TARMOQ PAKETLARINI FILTRLASHNING XUSUSIYATLARI

Tashev S.N.

Toshkent kimyo-texnologiya instituti Shahrisabz filiali Ijtimoiy-iqtisodiy fanlar kafedrasi mudiri sarvar.tashev@mail.ru

Har bir IP-paket qoidalar to‘plamiga mosligi bo‘yicha tadqiq etiladi. Bu qoidalar TCP/IP modelini tarmoq va transport sathi sarlavhalari tarkibi bo‘yicha aloqa ruxsatini o‘rnatadi, paketlarni harakatlanishini ham tahlil etadi. Paketlarni filtrlash quyidagilarni nazorat etadi:

- paket kelgan fizik interfeysni;
- IP (jo‘natuvchining IP-adresini);
- IP (qabul qiluvchining IP-adresini);
- transport sathining xilini (TCP, UDP, ICMP);
- manba va belgilangan adresning transport portlarini[1].

Paketlarni filtrlashda, agar paket qoidalarni qanoatlantirsa u tarmoq steki bo‘yicha keyinchalik ishlash va jo‘natish uchun ko‘chadi. Barcha kiruvchi paketlar filtrlashning berilgan qoidalari mosligiga tekshiriladi. Paketni tarmoq stekiga ko‘chirish uchun unga ruxsat beriladi yoki paket yo‘q qilinadi.

Bunday sxemada bir yoki bir necha tarmoq protokollarini tahlili uchun cheklangan komandalar to‘plami qo‘llaniladi, biroq bu sxema yadro muhitida tahlilni amalga oshiradi. Paketlarni filtrlash qanday amaliy protokol foydalanilishini ajratish imkoniga ega emas. Qoidalar ikki ro‘yxatdan iborat: ruxsat ro‘yxati va taqiq ro‘yxati. Tarmoq paketi ikkala ro‘yxat tekshiruvidan o‘tadi.

Paketlarni ishlash sxemasi va qoidalari quyidagicha:

- agar qoida ruxsat bersa, paketga ijozat beriladi;
- agar qoida taqiqlasa, paket yo‘q qilinadi;
- agar hech qanday qoida qo‘llanilmasa, paket yo‘q qilinadi.

Seans sathi shlyuzi. Seans sathida filtrlash texnologiyasining mohiyati shundan iboratki, shlyuz bitta uzelning barcha so‘rovlarini boshqa uzelga foydalanish uchun ushlab oluvchi vositachi sifatida ikki uzelni to‘g'ridan-to‘g'ri o‘zaro munosabatini inkor qiladi va bunday so‘rovlarning joizligini tekshirgandan keyin ulanishni o‘rnatadi. Shundan so‘ng seans sathi shlyuzi qo‘shimcha filtrlashsiz ikki uzel orasida bitta sessiya doirasida uzatilayotgan paketlarni nusxalaydi. Avtorizatsiyalangan ulanish o‘rnatilganidan keyin shlyuz maxsus ulanishlar jadvaliga tegishli axborotni kiritadi. Paketlarni filtrlash texnologiyasi turli xildagi himoya vositalarini yaratilishiga asos bo‘ldi va barcha turdagi marshrutizatorlarda amalga oshirilgan[2]. Bu texnologiyaning asosiy afzalliklari va kamchiliklari 1-jadvalda keltirilgan. Paketlarni filtrlashning afzalliklari va kamchiliklari

1-jadval

№	Afzalliklari	Kamchiliklari
1.	Ishlashning yuqori tezligi.	Amaliy sathni tahlillash imkoniyatining yo‘qligi.
2.	Amalga oshirishning soddaligi.	Adreslarni o‘zgartirib qo‘yishdan himoya yo‘q.
3.	Bu imkoniyat barcha marshrutizatorlarda va ko‘plab operatsion tizimlarda o‘rnatilganligi sababli qo‘shimcha moliyaviy xarajat talab qilmaydi.	Sozlashning va ma’murlashning qiyinligi.
4.	Past narx yoki erkin tarqatilishi (xarid qilinganda).	Qoidalar soni oshganda samaradorlik tushishi mumkin.
5.	Paketlar o‘tishida kichik to‘xtalish.	Tarmoq xizmatlari va protokollari to‘g'risida batafsil bilim talab etiladi.
6.	NAT sxemasi ichki IP-adreslarni yashiradi.	Ulanish holatining nazorati yo‘q.
7.	Tarmoqlararo ekran qurilma shaklida amalga oshirilishi mumkin.	Tarmoqlararo ekran qurilma shaklida amalga oshirilishi mumkin.

Seans yakunlanishi bilan bu haqidagi yozuv jadvaldan o‘chiriladi. Buzg'unchi tomonidan shakllantirilishi mumkin bo‘lgan va tugallangan ulanishga “taalluqli” keyingi barcha paketlar olib tashlanadi. Bu turdagi tarmoqlararo ekranlar paket yoki TCP-ulanishga

so‘rov ekanligi, yoki o‘rnatilgan ulanishga tegishligi, yoki ikki transport sathi orasida virtual ulanishga taalluqli ekanligini tekshiradi.

Foydalanilgan adabiyotlar ro‘yxati

1. T. Divya Rai, Ritu Verma “Packet Filtering Technique for Network Security” International Journal of Engineering Research & Technology (IJERT) Special Issue - 2015 ISSN: 2278-0181 ISNCESR-2015 Conference Proceedings

2. G‘ulomov Sherzod Rajaboevich, Mirzaeva Malika Bakhadirovna, Iminov Abdurasul Abdulatipovich. Port-Knocking Method for Enhancing Network Security. 2022 International Conference on “Information Science and Communications Technologies (ICISCT)”. Tashkent; Uzbekistan-2022. -4p.