TELEKOMMUNIKATSIYA TARMOQLARIDA XAVFSIZLIKNI TA'MINLASH MASALASINING DPI ASOSIDAGI YECHIMLARINI TAHLIL QILISH

Dilbar Turgunovna Normatova
Muhammad al-Xorazmiy nomidagi TATU,
"Telekommunikatsiya injiniringi" kafedrasi, katta o'qituvchi
Email: normatova_1972@mail.ru

Annotatsiya: *Ushbu maqolada telekommunikatsiya tarmoqlarida mavjud xafsizlik muammolari, tahdidlar va telekommunikatsiya tarmoqlarida xavfsizlikni ta'minlash masalasining DPI (Deep Packet Inspection) tushunchasi, tarmoqlar orasidagi ma'lumot almashinuvlarida, ma'lumotlarni to'plagan paketlarning ichki strukturasi va turli xususiyatlarini tahlil qilindi.*

Kalit so'zlar: *DPI, Bypass, Back-End, PCRF, SolarWinds, Ntopng, PRTG, Manage Engine OpManager, Netifyd.*

Abstract: *In this article, the existing security problems in telecommunication networks, threats and the concept of DPI (Deep Packet Inspection) of providing security in telecommunication networks, the internal structure and various characteristics of the packets that collect data in information exchanges between networks were analyzed.*

Keywords: *DPI, Bypass, Back-End, PCRF, SolarWinds, Ntopng, PRTG, Manage Engine OpManager, Netifyd.*

Аннотация: *В данной статье были проанализированы существующие проблемы безопасности в телекоммуникационных сетях, угрозы и концепция DPI(Deep Packet Inspection) обеспечения безопасности в*

телекоммуникационных сетях, внутренняя структура и различные характеристики пакетов, собирающих данные при информационном обмене между сетями.

Ключевые слова: *DPI, Bypass, Back-End, PCRF, SolarWinds, Ntopng, PRTG, Manage Engine OpManager, Netifyd.*

KIRISH

O‘zbekistonda DPI (Deep Packet Inspection) tizimlari, telekommunikatsiya tarmoqlarida xavfsizlikni ta’minlash uchun keng qo‘llaniladi. Bu tizimlar, tarmoqdagi ma’lumotlarni nazorat qilish va zararli dasturlar va xakerlarga qarshi kurashish uchun yordam berish uchun ishlatiladi.

O‘zbekiston Xalqaro aloqalar va telekommunikatsiya qo‘mitasi (MICT) DPI tizimlarini qo‘llagan holda, tarmoqdagi ma’lumotlarni nazorat qiladi va xavfsizlikni ta’minlaydi. Bu tizimlar, tarmoqda o‘tgan har bir paketni o‘z ichiga oladi va ma’lumotni tahlil qiladi. Bu tahlil asosida, zararli paketlar aniqlanadi va ularni yo‘qotish uchun kerakli harakatlar o‘tkaziladi.

O‘zbekistonda jamiyat xavfsizligi va tarmoq xavfsizligi mavzulari katta ahamiyatga ega. Hukumat, korxona va o‘quv markazlari o‘zlarining tarmoq xavfsizligi va maxfiylikni saqlash uchun DPI tizimlarini hamda boshqa xavfsizlik texnologiyalarini ishlatishni tavsiya qiladi. Bu, tarmoqdagi ma’lumotlarni himoya qilish va zararli dasturlar va xakerlarga qarshi kurashish uchun zarurdir.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

O‘zgaruvchi tashqi ta’sirlar (tarmoq ayrim elementlari xolatlarining o‘zgarishlari), tarmoq strukturasining o‘zgarishi (tarmoq ayrim uchastkalarining ishdan chiqarilishi va yangilarini ishga tushirilishi) va axborot yetkazishga talablarning qondirish sharoitlarida telekommunikatsiya tarmog‘ining normal rivojlanishi va ishlashini ta’minlash mos boshqaruv tizimlari orqali amalga oshiriladi.

Telekommunikatsiya tarmog‘ini, shuningdek uning katta qismlarini (ikkilamchi tarmoqlar, quyi tarmoqlar, uzellar, liniyalar va xakozo), o‘zaro “xizmat” axborotlari oqimlari (teskari aloqa) bilan bog‘langan va tashqi ta’sirlar ostida bo‘lgan, boshqarish obekti - OU (boshqariluvchi quyi tizim) va boshqaruvchi qurilmalar - UU (boshqaruvchi quyi tizim) jamlanmasi sifatida qarash mumkin

Xavfsizlikni boshqarish bazaviy elementlariga foydalanuvchilarni autentifikatsiyalash protseduralari, tarmoq resurslariga kirishni tayinlash va xuquqini tekshirish, shifrlash kalitlarini taqsimlash va qo‘llash, vakolatni boshqarish va xakozolar kiradi. Ko‘p xollarda bu guruxning funksiyalari tarmoqlarni boshqarish tizimlariga kiritilmaydi, lekin maxsus maxsulotlar (masalan, Kerberos autentifikatsiyalash va mualliflash, turli xil ximoya ekranlari, ma’lumotlarni shifrlash tizimlari) ko‘rinishida amalga oshiriladi, yoki operatsion tizimlar va tizimiy ilovalar tarkibiga kiritiladi.

Texnikaning ishonchliligi tushunchasining asosi bu raddiya tushunchasidir, texnikaning o‘z funksiyalarini bajarilishini davom ettira olmaslik xolatidir. Bu tushuncha nafaqat telekommunikatsiya apparaturasiga tegishli bo‘lib qolmasdan, komplekslarga ham, jumladan, telekommunikatsiya liniyalariga (kabelli, radioreleli va boshqalar) ham tegishlidir. Raddiya tushunchasi orqali shuningdek, ikki qutbli telekommunikatsiya tarmoqlarini ishonchliligini baholash maqsadga muvofiqdir. Bu xolda ikki qutbli telekommunikatsiya tarmog‘ining raddiyasi deyilganda, uning shunday xolati tushuniladiki, unda tarmoq qutblari orasida o‘tkazuvchanlik qobiliyati va aloqa sifati berilgan chegaraviy qiymatdan (talablardan) past bo‘ladi.

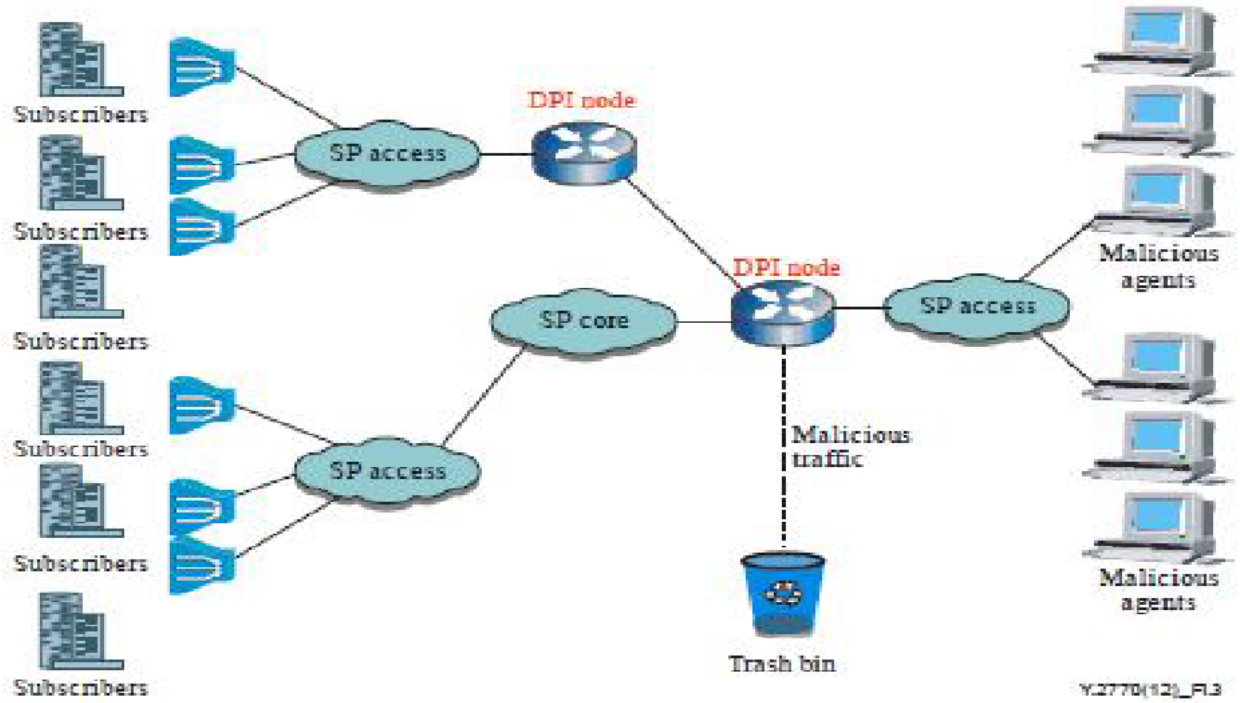
DPI (Deep Packet Inspection) texnologiyasi yangi zamonaviy texnologiya hisoblanib, IP asosida qurilgan paketli ma’lumot uzatish tarmoqlarida axborot paketlarini chuqur tekshirish va analiz qilish yo‘li bilan xavfsizlikni ta’minlash, trafikni boshqarish va xizmat ko‘rsatish sifatini nazorat qilish kabi dolzarb muammolarni hal etish maqsadida ishlab chiqildi.

Telekommunikatsiya provayderlari va hukumatlar DPI dan turli kontekstlarda foydalanadilar. Shimoliy Amerika, Evropa va Osiyodagi hukumatlar DPI dan o‘z

tarmoqlarini himoya qilish uchun foydalanishdan tashqari, kuzatuv va tsenzura kabi turli maqsadlar uchun foydalanadilar.

Deep Packet Inspection (DPI) - bu biznes va internet provayderingiz (ISP) tomonidan kiberhujumlarni aniqlash va to‘xtatish, foydalanuvchi xatti-harakatlarini kuzatish, zararli dasturlarni to‘xtatish va trafik turli shakllariga qarshi kurashish uchun muntazam ravishda foydalaniladigan paketli filtrlash turi. DPI IP-trafikni tahlil qilish va boshqarish va tarmoqning ko‘rinishini va real vaqtda dastur xabardorligini ta’minlash orqali real vaqt rejimida IP tarmoqlarini himoya qilishni osonlashtiradi [1].

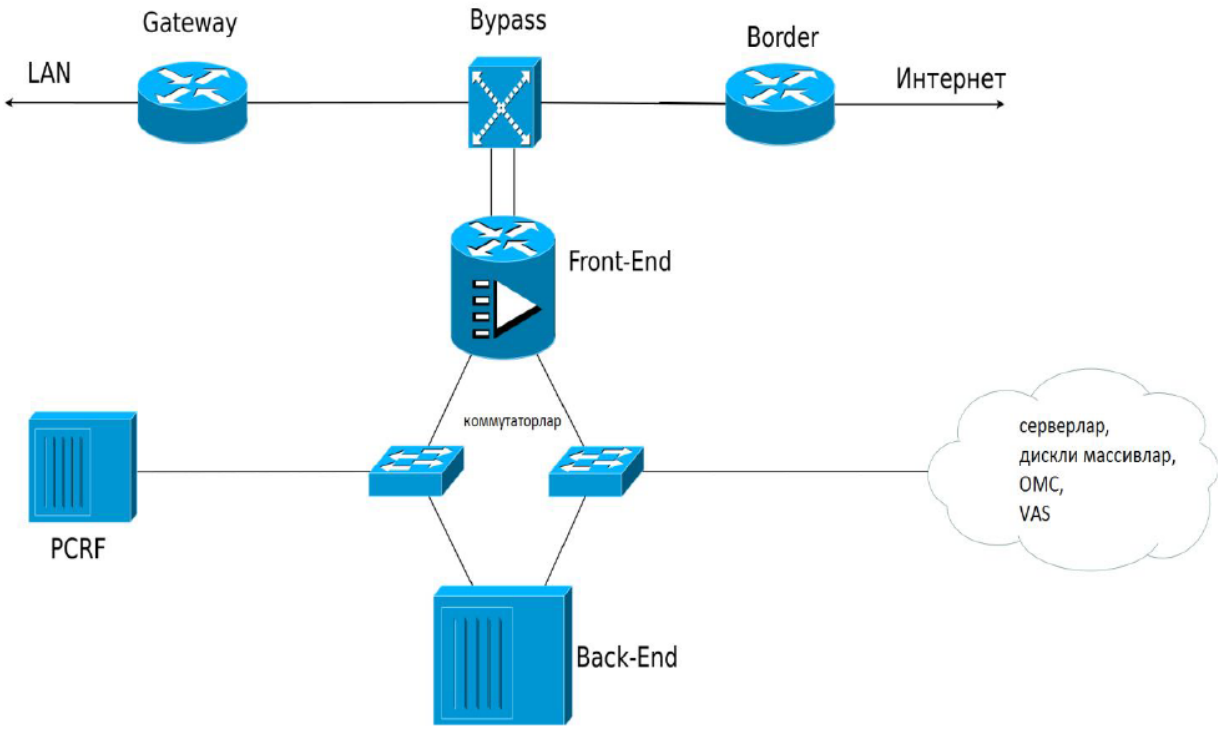
DPI texnologiyasi IP asosida qurilgan barcha turdagi paketli ma’lumot uzatish tarmoqlarida keng qo‘llanilishi mumkin. Tarmoqda joylashgan DPI qurilmasi OSI modelining hamma pog‘onasiga tegishli bo‘lgan barcha turdagi axborot oqimlari tarkibini chuqur tekshiradi.



1-rasm. DPI qurilmalarining ishlash prinsipi.

DPI tizimi aloqa operator tarmog‘ining chegarasiga qo‘yiladi. DPI texnik vositalari quyidagi komponentlardan tashkil topgan:

- ❖ Bypass;
- ❖ Front-End qurilmasi;
- ❖ Back-End qurilmasi;
- ❖ PCRF-serveri (Policy and Charging Rules Function);
- ❖ komponentlar orasida aloqani ta’minlaydigan kommutatorlar;
- ❖ serverlar (qo‘shimcha);
- ❖ disk massivlari (qo‘shimcha);
- ❖ VAS qurilmasi (Value Added Services – spam va viruslar tekshiruvi) (qo‘shimcha). Umumiy sxemasi 1-rasmdagi ko‘rinishga ega.



2-rasm. DPI tizimining tipik sxemasi

Birinchi bo‘lib tarmoqqa Bypass, keyin esa unga Front-End ulanadi. Bypass ikkita ishlash rejimiga ega:

1. Himoya. Trafik to‘g‘ri liniyaga o‘tib ketadi va Front-End qurilmasiga uzatilmaydi.

2. Ishchi. Trafik Front-End qurilmasiga uzatiladi.

Front-End ishdan chiqqanda, uning portlariga ulangan kabel shikastlanganda, DPI texnik vositalari elektr ta’minotidan uzilib qolganda Bypass himoya rejimiga o‘tadi. Bypass elektr yoki optik turda bo‘lishi mumkin. Elektr Bypass relega asoslangan bo‘lib, mis simlar ulashga mo‘ljallangan va ma’lumot uzatish tezligi 1 Gbit/s gacha bo‘ladi. Optik Bypass bir necha afzalliklarga ega: ma’lumot uzatish tezligi 10 Gbit/s gacha, trafikni akslantirish imkoniyati yuzaga keladi (trafik to‘g‘ri kanal bo‘yicha ketayotganda uning nusxasi Front-End ga uzatiladi, trafik bilan hech qanday amallarni bajarish imkoniyati mavjud bo‘lmasada, statistika olib borish mumkin bo‘ladi). Front-End qurilmasida paketlar OSI modelinig kanal sathidan amaliy sathigacha tahlil qilinadi [2].

NATIJALAR

Paketni chuqur tekshirish tarmoq foydalanuvchilari tushunchasini va biznes xavfsizligini sezilarli darajada yaxshilaydi. Uzluksiz DPI xavfsizlik guruhlariga evristik va xatti harakatlarga asoslangan tahlillarni birlashtirib, paketning butun dastur yuklamasini sinchkovlik bilan tahlil qilish va tekshirish va trafik seanslarini qayta yig‘ish orqali xavfli va murakkab hujumlarni aniqlash imkonini beradi.

Uzluksiz DPI tarmoq faolligini aniqlash va trafikni kuzatishda yordam beradi. Natijada, korxonalar shaxsiy ma’lumotlarning tarmoqdan chiqishini to‘xtatuvchi va ma’lumotlar sizib chiqishi sodir bo‘lganda ogohlantirishlarni oladigan siyosatlarni amalga oshirishi mumkin.

Har yili bozorga yana millionlab IoT narsalar interneti qurilmalari qo‘shiladi va ularning aksariyati xavfsizlik-dizayn tamoyillari yordamida ishlab chiqilmagan. Buzg‘unchilikdan himoya qilish uchun o‘rnatilgan xavfsizlik choralari mavjud emas. Uzluksiz DPI xavfsizlik guruhlarini IoT xavfsizligi masalalari bo‘yicha o‘rgatish orqali IoT DDoS va botnet hujumlarining oldini olishga yordam beradi.

MUHOKAMA

DPI (Deep Packet Inspection) asosidagi xavfsizlik devori har bir paket mazmuni asosida tarmoq trafigini kuzatuvchi va filtrlaydigan tarmoq xavfsizligi qurilmasidir. Faqat paket sarlavhasi ma'lumotlarini tekshiradigan an'anaviy xavfsizlik devori texnologiyasidan farqli o'laroq, DPI xavfsizlik devorlari zararli trafikni aniqlash va blokirovka qilish uchun har bir paketning butun tarkibini tekshiradi.

DPI xavfsizlik devorlari an'anaviy xavfsizlik devori texnologiyasi tomonidan o'tkazib yuborilishi mumkin bo'lgan zararli dasturlar, viruslar va boshqa zararli trafik turlari kabi tahdidlarni aniqlash va blokirovka qilishda ayniqsa samarali. Ular, shuningdek, ruxsatsiz fayllarni uzatish, tasdiqlanmagan ilovalardan foydalanish va tarmoqdan noto'g'ri foydalanishning boshqa turlari kabi korporativ siyosatlarni buzadigan tarmoq trafigini aniqlashi va bloklashi mumkin. DPI xavfsizlik devorlari cheklovlarsiz emas. Ular resurs talab qilishi mumkin, real vaqtda tarmoq trafigini tahlil qilish uchun katta ishlov berish quvvati va xotirani talab qiladi. Bu, ayniqsa, katta hajmli tarmoqlarda ishlash muammolariga olib kelishi mumkin. Bundan tashqari, shifrlangan trafikning ba'zi turlarini tekshirish qiyin bo'lishi mumkin, bu ma'lum stsenariylarda DPI xavfsizlik devorlari samaradorligini cheklaydi.

DPI xavfsizlik devorlari turli stsenariylarda, masalan, korporativ tarmoqlarda kiberhujumlardan himoyalanish va korporativ siyosatni qo'llashda, josuslik va boshqa xavfsizlik tahdidlaridan himoyalanish uchun hukumat tarmoqlarida va xizmat ko'rsatuvchi provayder tarmoqlarida boshqarish va tarmoq trafigini optimallashtirish uchun ishlatilishi mumkin.

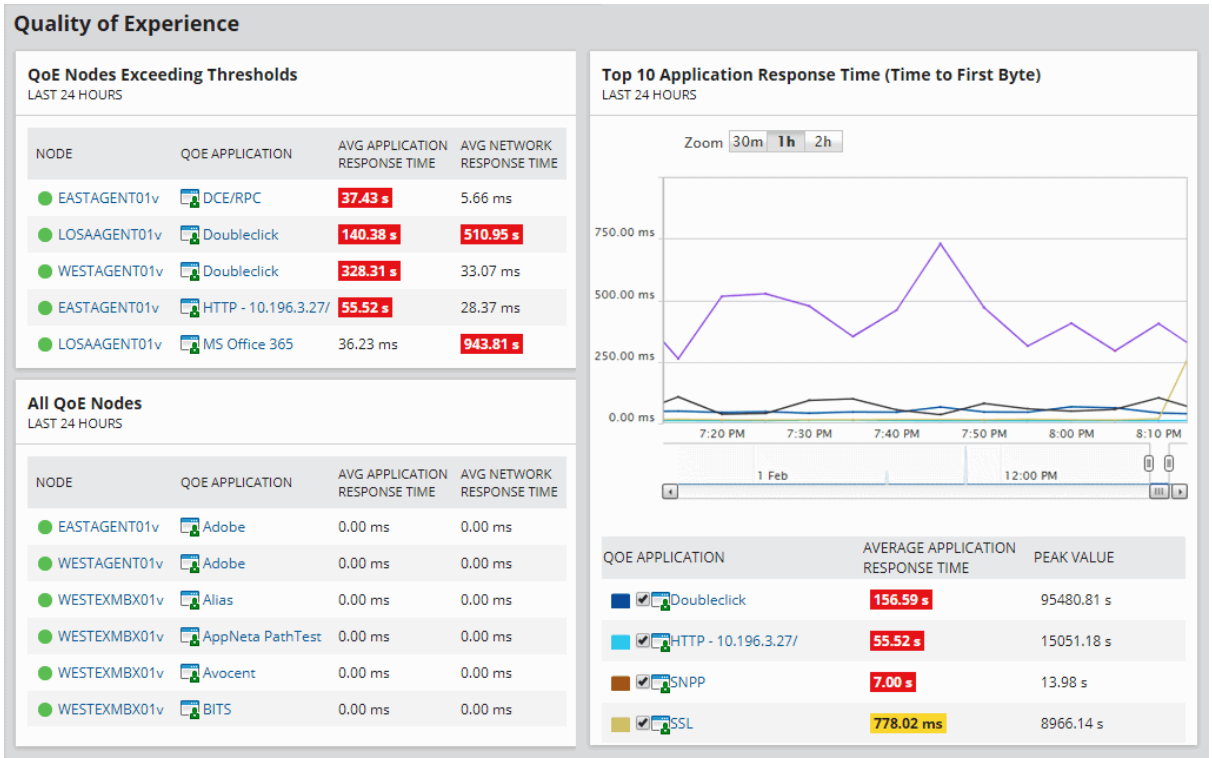
Deep Packet Inspection (DPI) tahlil qilish uchun bir qancha dasturiy ta'minot va vositalar kerak bo'lishi mumkin, chunki DPI tahlili bir tarmoqning xavfsizligini nazorat qilish, tarmoq trafikini ko'rsatish va tarmoqning ishlaydiganligini aniqlash uchun yordam beradi.

Quyidagilar DPI uchun eng mashhur chuqur paketlarni tekshirish vositalarini hisoblanadi:

1. SolarWinds – Network Perfomance Monitor
2. Ntopng bilan nDPI
3. PRTG bilan Paessler Packet Sniffing
4. Manage Engine OpManager
5. Netifyd

Endi esa bu dasturiy vositalarning tavsifi, afzalliklari va kamchiliklarini ko‘rib o‘tamiz.

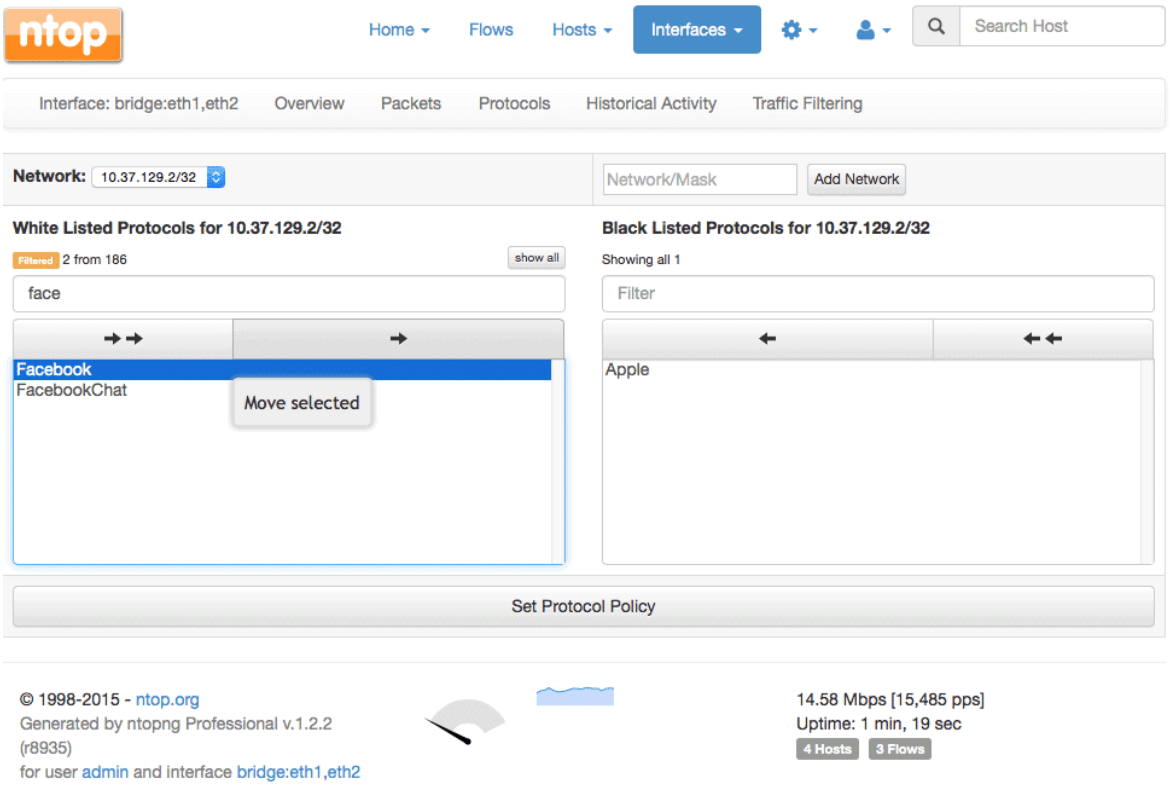
1. SolarWinds – Network Perfomance Monitor



3-rasm. SolarWinds NPM dasturiy vositasi bilan ishlash oynasi

SolarWinds dan "NPM" Network Perfomance Monitor (tarmoq ishlashi monitori) DPI va tarmoq trafigini tahlil qilishi mumkin.

Ntopng bilan nDPI



4-rasm. Ntopning dasturiy vositasi bilan ishlash oynasi

Ntop - bu tarmoq monitoringi to‘plami. Unda Packet Capture, Traffic Recording, Network Probe, Traffic Analysis va DPI uchun turli mahsulotlar mavjud. NTop dan DPI Ntopng yordamida nDPI tomonidan amalga oshiriladi .

nDPI mashhur OpenDPI-ga asoslangan ochiq manba va kengaytiriladigan DPI kutubxonasi. Tarmoq ma’muri ushbu vositadan ma’lum trafik oqimlarini, xostlarni yoki tarmoq protokollarini bloklash uchun foydalanishi mumkin.

Ammo nDPI faqat kutubxona bo‘lgani uchun qoidalarni bajarish uchun u ntopng va nProbe cento kabi boshqa ilovalar bilan ishlatilishi kerak.

Ntopng - bu holat va unumdorlikni ko‘rsatish uchun tarmoq interfeysidan trafikni passiv to‘plashi mumkin bo‘lgan veb-interfeys monitoringi vositasi.

Ntopng va ndpi bilan siz L7 siyosatlarini qo‘llashingiz mumkin, masalan, tarmoq quyi tarmog‘idagi maxsus ilovalar trafigini shakllantirish.

Netifyd DPI texnologiyasidan dastur qatlamida paketlarni ochish, HTTPS sertifikatlariga qarash va Youtube, Facebook, Netflix va boshqalar kabi vebsaytlar/ilovalarni aniqlash imkonini beradi.

Netifyd trafikni passiv tarzda ushlaydi, ya'ni u trafikni bloklamaydi, filtrlamaydi yoki manipulyatsiya qilmaydi. Netifyd boshqa vositalarga DPI xizmatlarini taqdim etadi. Keyin ushbu trafik paketlari paket oqimlarini aniqlash uchun nDPI protokoli orqali skanerdan o'tkaziladi. **Netifyd orqali (DPI) chuqur paketli tekshiruvni amalga oshirish.** Netifyd -protokol bo'yicha paketlar bo'yicha statistikani to'plashi mumkin bo'lgan bepul paketlarni yig'ish tizimi. Bu to'liq paketlarni tahlil qilish vositasi emas, balki ma'lumotlarni yig'ish agenti. Siz Netfyd to'playdigan yozuvlarni topshirishni va ularni ma'lumotlarni tahlil qilish tizimiga yuborishni tanlashingiz mumkin.

Netifyd paketlarni ushlaydi, lekin u ma'lumotlarni sharhlash yoki trafikni shakllantirish yoki protokollarni bloklash bo'yicha harakatlarni bajarish uchun tahlil funktsiyalarini o'z ichiga olmaydi [2,3].

XULOSA

DPIga asoslangan tarmoq trafigini tekshiruvchi dasturiy ta'minot vositalarini baholashni taqdim etadi.

Bizning tahlilimizga ko'ra SolarWinds NPM trafik tasnifi uchun eng ishonchli yechim hisoblanadi. Uning yuqori darajadagi trafik monitoringi, hujum aniqlash va nazorat imkoniyatlari tarmoqdagi xavfsizlikni oshirishda yordam beradi. DPI tahlilining telekommunikatsiya tarmoqlarida xavfsizlikni ta'minlashdagi o'rni va roli batafsil tahlil qilindi. DPI texnologiyasi tarmoq trafikini batafsil va tafsilotli tahlil qilish imkonini beradi. Bu tahlil jarayoni qo'llanilgan ma'lumot paketlarini yoki paketlarga tegishli metamatematik malumotlarni qayta qurish, qayta tiklash va tahlil qilishdan iborat bo'ladi. Buning natijasida tarmoqdagi har bir paketni xavfsizlik darajasini oshirish, xavfli yo'nalishlarni aniqlash va xavfsizlik cheklovlari uchun muvaffaqiyatli foydalanish imkoniyatiga ega bo'lamiz.

Tarmoq xavfsizlikni ta’minlash uchun DPI asosidagi mavjud yechimlar tahlil qilindi. Bu yechimlar, tarmoqdagi xavfli yo‘nalishlarni aniqlash, zararli kodlarni identifikatsiya qilish, trafikni monitoring qilish, xavfli faoliyatni identifikatsiya qilish va tahlil ma’lumotlarini tahrirlash imkoniyatlarini o‘z ichiga oladi. Bir necha eng yaxshi DPI dasturiy vositalari (masalan, SolarWinds, Ntopng, ManageEngine, Netifyd) taqqoslandi. Ularning bir-biridan farqli jihatlari, ustunliklari, funktsiyalari, narxlari, qulayliklari tahlil qilindi va foydalanuvchilar tomonidan bildirilgan fikrlar hisobga olindi.

DPI dasturiy vositalari yordamida tarmoqdagi xavfsizlik holatini baholashning qanday amaliy usullari mavjudligi va ularning natijalari tahlil qilindi. Bu baholash, xavfsizlik statistikasi, tahlil ma’lumotlari orqali tushuntirildi. DPI tahlilining xavfsizlik strategiyalarini rivojlantirishga qanday yordam berishi tahlil qilindi. DPI dasturiy vositalari orqali xavfsizlikning keyinchalik oshirilishi, qo‘shimcha cheklovlarni qo‘yish, xavfli yo‘nalishlarga tezroq reaksiya ko‘rsatish va xavfsizlik sohalari uchun DPI texnologiyalaridan foydalanish bo‘yicha xulosa va tavsiyalar berildi.

ADABIYOTLAR RO‘YXATI

1. Hannah Bartus.(2018). Deep Packet Inspection: A Key Issue for Network Security.

In book: Information Technology - New Generations (pp.89-92).

2. Abusukhon A. & Yu, F. R. (2017). A Survey on Traffic Classification and Its Applications to Deep Packet Inspection.

3. Tamer Abuhmed, David Mohaisen, Daehun Nyang. (2008) A Survey on Deep Packet Inspection for Intrusion Detection Systems.

4. Mykola Beshley, Krzysztof Przystupa. (2020). A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection.