ISSN 2181-3187

TARMOQLARARO EKRANLARNING ASOSIY KOMPONENTLARI.

Shaydullayev Jahongir Qudrat o‘g‘li

Muhammad al-Xorazmiy nomidagi Toshkent

axborot texnologiyalari universiteti

Shaydullayevjahongir579@gmail.com

Annotatsiya: *Ushbu maqolada tarmoqlararo ekran (firewall) dasturlarining tarmoq xavfsizligi, Tarmoq xavfsizligini ta’minlash uchun firewall tizimlarining tashqi tahdidlardan, zararli dasturlardan, tarmoqga ruxsatsiz kirishlardan himoya qilishda asosiy vositalari sifatlari,Tarmoqning samarali va xavfsiz ishlashini ta'minlash uchun firewall konfiguratsiyasi va sozlamalari haqida fikr yuritilgan.*

Аннотация: *В статье рассматривается сетевая безопасность программ-брандмауэров, характеристики основных инструментов систем брандмауэров для обеспечения сетевой безопасности от внешних угроз, вредоносных программ и несанкционированного доступа в сеть, а также конфигурация и настройки брандмауэров для обеспечения эффективной и безопасной работы сети.*

Abstract: *This article discusses the network security of firewall programs, the characteristics of the main tools of firewall systems to ensure network security against external threats, malicious programs, and unauthorized access to the network, and the configuration and settings of firewalls to ensure the effective and secure operation of the network.*

Kalit so‘zlar: *Ekranlovchi marshrutizator, OSI modeli, IP, TCP/IP, UDP Seans sathi shlyuzi.*

ISSN 2181-3187

Ключевые слова: *экранирующий маршрутизатор, модель OSI, IP, TCP/IP, шлюз сеансового уровня UDP.*

Keywords: *Shielding router, OSI model, IP, TCP/IP, UDP Session layer gateway.*

Tarmoqlararo ekranlar tarmoqlararo aloqa xavfsizligini OSI modelining turli sathlarida madadlaydi. Bunda etalon modelning turli sathlarida bajariladigan himoya funksiyalari bir-biridan jiddiy farqlanadi. Shu sababli, tarmoqlararo ekranlar kompleksini, har biri OSI modelining alohida sathiga mo‘ljallangan, bo‘linmaydigan ekranlar majmui ko‘rinishida tasavvur etish mumkin.

Ekranlar kompleksi ko‘pincha etalon modelning tarmoq, seans, tatbiqiy sathlarida ishlaydi. Mos holda, quyidagi bo‘linmaydigan brandmauerlar farqlanadi (1.1-rasm).

- ekranlovchi marshrutizator;

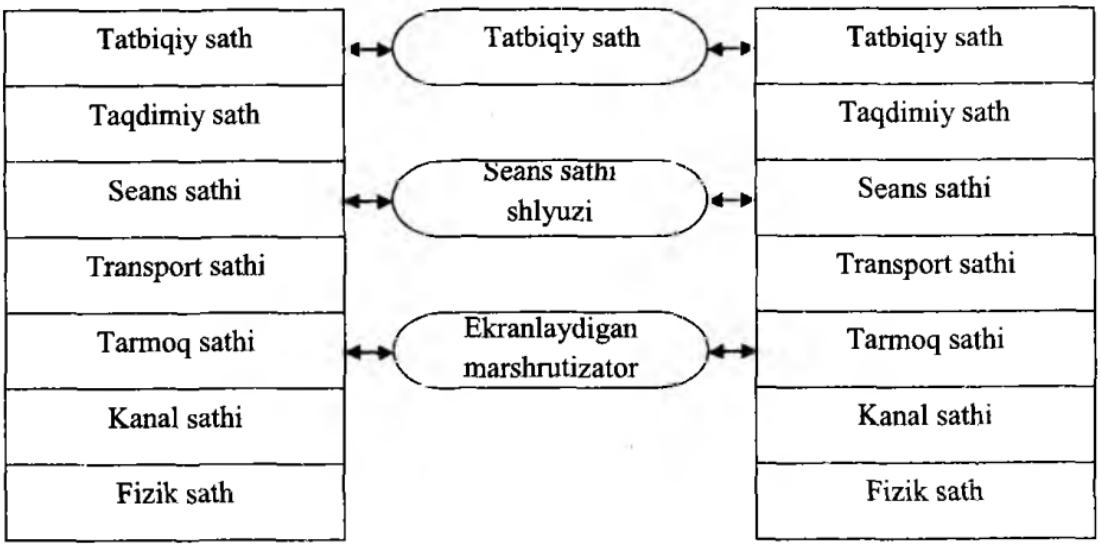
- seans sathi shlyuzi (ekranlovchi transport);

- tatbiqiy sath shlyuzi (ekranlovchi shlyuz).

Tarmoqlarda ishlatiladigan protokollar (TCP/IP, SPX/IPX) OSI etalon modeliga batamom mos kelmaydi, shu sababli sanab o‘tilgan ekranlar xili funksiyalarini amalga oshirishda etalon modelining qo‘shni sathlarini ham qamrab olishlari mumkin. Masalan, tatbiqiy ekran xabarlarning tashqi tarmoqqa uzatilishida ularni avtomatik tarzda shifrlashni hamda qabul qilinuvchi kriptografik bekitilgan ma’lumotlarni avtomatik tarzda rasshifrovka qilishni amalga oshirishi mumkin. Bu holda, bunday ekran OSI modelining nafaqat tatbiqiy sathida, balki taqdimiy sathida ham ishlaydi.

Seans sathi shlyuzi ishlashida OSI modelining transport va tarmoq sathlarini qamrab oladi. Ekranlovchi marshrutizator xabarlar paketini tahlillashda ularning nafaqat tarmoq, balki transport sathi sarlavhalarini ham tekshiradi.

ISSN 2181-3187



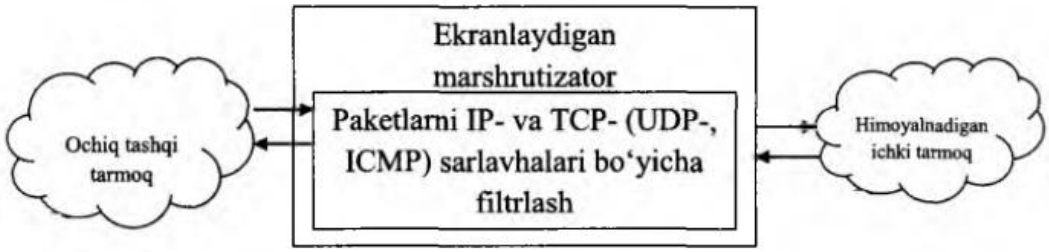
1.1-rasm. OSI modelining alohida sathlarida ishlaydigan tarmoqlararo ekranlar turi.

Yuqorida keltirilgan tarmoqlararo ekranlarning xillari o‘zining afzalliklari va kamchiliklariga ega. Ishlatiladigan brandmauerlarning ko‘pchiligi yoki tatbiqiy shlyuzlar, yoki ekranlovchi marshrutizatorlar bo‘lib, tarmoqlararo aloqaning to‘liq xavfsizligini ta’minlamaydi. Ishonchli himoyani esa faqat har biri - ekranlovchi marshmtizator, seans sathi shlyuzi hamda tatbiqiy shlyuzni birlashtiruvchi tarmoqlararo ekranlarning kompleksi ta’minlaydi.

Ekranlovchi marshrutizator (screeningrouter) (paketli filtr (packetfilter) deb ham ataladi) xabarlar paketini filtrlashga atalgan, ichki va tashqi tarmoqlar orasida shaffof aloqani ta’minlaydi. U OSI modelining tarmoq sathida ishlaydi, ammo o‘zining ayrim funksiyalarini bajarishida etalon modelining transport sathini ham qamrab olishi mumkin.

Ma’lumotlarni o‘tkazish yoki brakka chiqarish xususidagi qaror filtrlashning berilgan qoidalariga binoan har bir paket uchun mustaqil qabul qilinadi. Qaror qabul qilishda tarmoq va transport sathlari paketlarining sarlavhalari tahlil etiladi (1.6-rasm).

ISSN 2181-3187



1.2-rasm. Paketli filtrning ishlash sxemasi.

Har bir paketning IP- va TCP/UDP - sarlavhalarining tahlillanuvchi hoshiyalari sifatida quyidagilar ishlatilishi mumkin:

- jo‘natuvchi adresi;
- qabul qiluvchi adresi;
- paket xili;
- paketni fragmentlash bayrog‘i;
- manba porti nomeri;
- qabul qiluvchi port nomeri.

Birinchi to‘rtta parametr paketning IP-sarlavhasiga, keyingilari esa TCP-yoki UDP sarlavhasiga taalluqli. Jo‘natuvchi va qabul qiluvchi adreslari IP-adreslar hisoblanadi. Bu adreslar paketlarni shakllantirishda to‘ldiriladi va uni tarmoq bo‘yicha uzatganda o‘zgarmaydi.

Paket xili hoshiyasida tarmoq sathiga mos keluvchi ICMP protokol kodi yoki tahlillanuvchi IP-paket taalluqli bo‘lgan transport sathi protokolining (TCP yoki UDP) kodi bo‘ladi.

Paketni fragmentlash bayrog‘i IP-paketlar fragmentlashining borligi yoki yo‘qligini aniqlaydi. Agar tahlillanuvchi paket uchun fragmentlash bayrog‘i o‘matilgan bo‘lsa, mazkur paket fragmentlangan IP-paketning qismpaketi hisoblanadi.

ISSN 2181-3187

Manba va qabul qiluvchi portlari nomerlari TCP yoki UDP drayver tomonidan har bir jo'natiluvchi xabar paketlariga qo‘shiladi va jo‘natuvchi ilovasini hamda ushbu paket atalgan ilovani bir ma’noda identifikatsiyalaydi. Portlar nomerlari bo‘yicha filtrlash imkoniyati uchun yuqori sath protokollariga port nomerlarini ajratish bo‘yicha tarmoqda qabul qilingan kelishuvni bilish lozim.

Har bir paket ishlanishida ekranlovchi marshrutizator berilgan qoidalar jadvalini, paketning to‘liq assotsiatsiyasiga mos keluvchi qoidani topgunicha, ketma-ket ko‘rib chiqadi. Bu yerda assotsiatsiya deganda, berilgan paket sarlavhalarida ko‘rsatilgan parametrlar majmui tushuniladi. Agar ekranlovchi marshrutizator jadvaldagi qoidalarning birortasiga ham mos kelmaydigan paketni olsa, u, xavfsizlik nuqtayi nazaridan, uni yaroqsiz holga chiqaradi.

Paketli filtrlar apparat va dasturiy amalga oshirilishi mumkin. Paketli filtr sifatida oddiy marshrutizator hamda kiruvchi va chiquvchi paketlarni filtrlashga moslashtirilgan, serverda ishlovchi dasturdan foydalanish mumkin. Zamonaviy marshmtizatorlar har bir port bilan bir necha o‘nlab qoidalarni bog‘lashi va kirishda hamda chiqishda paketlarni filtrlashi mumkin.

Paketli filtrlarning kamchiligi sifatida quyidagilarni ko‘rsatish mumkin. Ular xavfsizlikning yuqori darajasini ta’minlamaydi, chunki faqat paket sarlavhalarini tekshiradi va ko‘pgina kerakli funksiyalarni madadlamaydi. Bu funksiyalarga, masalan, oxirgi uzellarni autentifikatsiyalash, xabarlar paketlarini kriptografik bekitish hamda ularning yaxlitligini va haqiqiyligini tekshirish kiradi. Paketli filtrlar dastlabki adreslarni almashtirib qo‘yish va xabarlar paketi tarkibini mxsatsiz o‘zgartirish kabi keng tarqalgan tarmoq hujumlariga zaif hisoblanadilar. Bu xil brandmauerlarni "aldash" qiyin emas - filtrlashga mxsat beruvchi qoidalarni qondiruvchi paket sarlavhalarini shakllantirish kifoya.

Ammo, paketli filtrlarning amalga oshirilishining soddaligi, yuqori unumdorligi, dasturiy ilovalar uchun shaffofligi va narxining pastligi, ularning hamma yerda

ISSN 2181-3187

tarqalishiga va tarmoq xavfsizligi tizimining majburiy elementi kabi ishlatilishiga imkon yaratdi.

Seans sathi shlyuzi (ekranlovchi transport deb ham yuritiladi) virtual ulanishlarni nazoratlashga va tashqi tarmoq bilan o‘zaro aloqa qilishda IP-adreslarni translyatsiyalashga atalgan. U OSI modelining seans sathida ishlaydi va ishlashi jarayonida etalon modelning transport va tarmoq sathlarini ham qamrab oladi. Seans sathi shlyuzining himoyalash funksiyalari vositachilik fimksiyalariga taalluqli.

Virtual ulanishlarning nazorati aloqani kvitirlashni kuzatishdan hamda o‘matilgan virtual kanallar bo‘yicha axborot uzatilishini nazoratlashdan iborat. Aloqani kvitirlashning nazoratida seans sathida shlyuz ichki tarmoq ishchi stansiyasi va tashqi tarmoq kompyuteri orasida virtual ulanishni kuzatib, so‘ralayotgan aloqa seansining joizligini aniqlaydi.

Bunday nazorat TCP protokolining seans sathi paketlarining sarlavhasidagi axborotga asoslanadi. Ammo TCP-sarlavhalani tahlillashda paketli filtr faqat manba va qabul qiluvchi portlarining nomerini tekshirsa, ekranlovchi transport aloqani kvirtirlash jarayoniga taalluqli boshqa hoshiyalarni tahlillaydi.

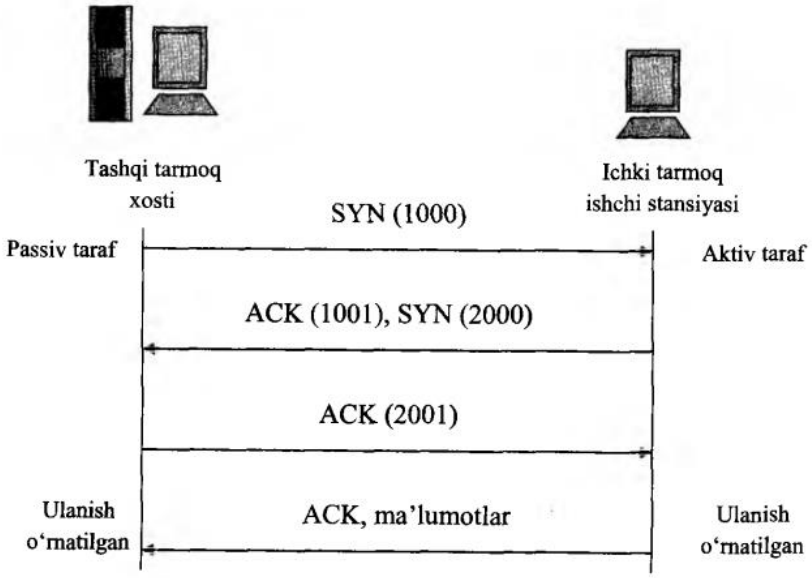
Aloqa seansiga so‘rovning joizligini aniqlash uchun seans sathi shlyuzi quyidagi harakatlarni bajaradi. Ishchi stansiya (mijoz) tashqi tarmoq bilan bog‘lanishni so‘raganida, shlyuz bu so‘rovni qabul qilib, uning filtrlashning bazaviy mezonlarini qanoatlantirishini, masalan, server mijoz va u bilan assotsiatsiyalangan ismning IP-adresini aniqlay olishini tekshiradi. So‘ngra shlyuz mijoz ismidan harakat qilib, tashqi tarmoq kompyuteri bilan ulanishni o‘matadi va TCP protokoli bo‘yicha kvitirlash jarayonining bajarilishini kuzatadi.

Bu muolaja SYN (Sinxronlash) va ACK (Tasdiqlash) bayroqlari orqali belgilanuvchi TCP-paketlarni almashishdan iborat (1.3-rasm).

SYN bayroq bilan belgilangan va tarkibida ixtiyoriy son, masalan, 1000 bo‘lgan TCP seansining birinchi paketi mijozning seans ochishga so‘rovi hisoblanadi. Bu

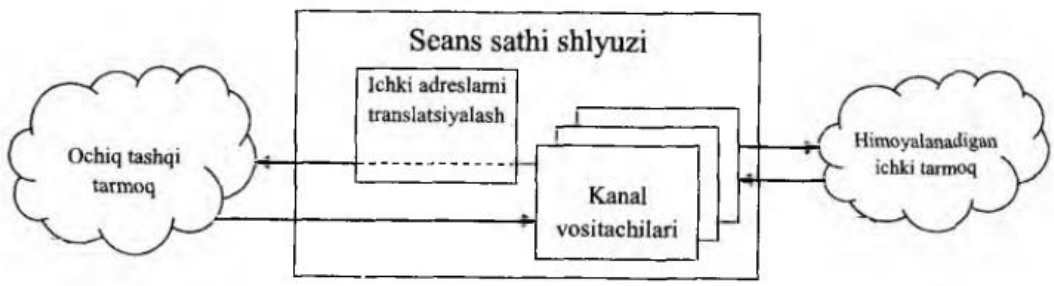
ISSN 2181-3187

paketni olgan tashqi tarmoq kompyuteri javob tariqasida ACK bayroq bilan belgilangan va tarkibida olingan paketdagidan bittaga katta (bizning holda 1001) son bo‘lgan paketni jo ‘natadi. Shu tariqa, mijozdan SYN paketi olinganligi tasdiqlanadi. So‘ngra teskari muolaja amalga oshiriladi: tashqi tarmoq kompyuteri ham mijozga uzatiluvchi ma’lumotlar birinchi baytining tartib raqami bilan (masalan, 2000) SYN paketini jo‘natadi, mijoz esa uni olganligini, tarkibida 2001 soni bo‘lgan paketni uzatish orqali tasdiqlaydi. Shu bilan aloqani kvirtirlash jarayoni tugallanadi.



1.3-rasm. TCP protokoli bo’yicha aloqani kvitirlash sxemasi.

Seans sathi shlyuzi (1.4-rasm) uchun so‘ralgan seans joiz hisoblanadi, qachonki aloqani kvirtirlash jarayoni bajarilishida SYN va ACK bayroqlar hamda TCP-paketlari sarlavhalaridagi sonlar o‘zaro mantiqiy bog‘langan bo‘lsa.



1.4-rasm. Seans sathi shlyuzining ishlash sxemasi.

ISSN 2181-3187

Ichki tarmoqning ichki stansiyasi va tashqi tarmoqning kompyuteri TCP seansining avtorizatsiyalangan qatnashchilari ekanligi hamda ushbu seansning joizligi tasdiqlanganidan so‘ng shlyuz ulanishni o‘rnatadi. Bunda shlyuz ulanishlarining maxsus jadvaliga mos axborotni (jo‘natuvchi va qabul qiluvchi adreslari, ulanish holati, ketma-ketlik nomeri xususidagi axborot va h.) kiritadi.

Shu ondan boshlab shlyuz paketlarni nusxalaydi va ikkala tomonga yo‘naltirib, o‘matilgan virtual kanal bo‘yicha axborot uzatilishini nazorat qiladi. Ushbu nazorat jarayonida seans sathi shlyuzi paketlarni filtrlamaydi. Ammo u uzatiluvchi axborot sonini nazorat qilishi va qandaydir chegaradan oshganida ulanishni uzishi mumkin. Bu esa, o‘z navbatida, axborotning ruxsatsiz eksport qilinishiga to‘siq bo‘ladi. Virtual ulanishlar xususidagi qaydlash axboroti to‘planishi ham mumkin.

Seans sathi shlyuzlarida virtual ulanishlarni nazoratlashda *kanal vositachilari* (pipeproxy) deb yuritiluvchi maxsus dasturlardan foydalaniladi. Bu vositachilar ichki va tashqi tarmoqlar orasida virtual kanallarni o‘rnatadi, so‘ngra TCP/IP ilovalari generatsiyalagan paketlarning ushbu kanal orqali uzatilishini nazoratlaydi.

Kanal vositachilari TCP/IPning muayyan xizmatlariga mo‘ljallangan. Shu sababli, ishlashi muayyan ilovalarning vositachi-dasturlariga asoslangan tatbiqiy sath shlyuzlari imkoniyatlarini kengaytirishda seans sath shlyuzlaridan foydalanish mumkin.

Seans sathi shlyuzi tashqi tarmoq bilan o‘zaro aloqada tarmoq sathi ichki adreslarini (IP-adreslarini) translyratsiyalashni ham ta’ minlaydi. Ichki adreslarni translyatsiyalash ichki tarmoqdan tashqi tarmoqqa jo‘natiluvchi barcha paketlarga nisbatan bajariladi.

Amalga oshirilishi nuqtayi nazaridan seans sathi shlyuzi yetarlicha oddiy va nisbatan ishonchli dastur hisoblanadi. U ekranlovchi marshmtizatomi virtual ulanishlarni nazoratlash va ichki IP-adreslarni translyatsiyalash funksiyalari bilan to‘ldiradi.

ISSN 2181-3187

Seans sathi shlyuzining kamchiliklari - ekranlovchi marshrutizatorlarning kamchiliklariga o‘xshash. Ushbu texnologiyaning yana bir jiddiy kamchiligi ma’lumotlar hoshiyalari tarkibini nazoratlash mumkin emasligi. Natijada, niyati buzuq odamlarga zarar keltiruvchi dasturlarni himoyalanuvchi tarmoqqa uzatish imkoniyati tug‘iladi. Undan tashqari, TCP-sessiyasining (TCPhijacking) ushlab 208 qolinishida niyati buzuq odam hujumlarini hatto ruxsat berilgan sessiya doirasida amalga oshirishi mumkin.

Amalda aksariyat seans sath shlyuzlari mustaqil mahsulot bo‘lmay, tatbiqiy sath shlyuzlari bilan komplektda taqdim etiladi.

Tatbiqiy sath shlyuzi (ekranlovchi shlyuz deb ham yuritiladi) OSI modelining tatbiqiy sathida ishlab, taqdimiy sathni ham qamrab oladi va tarmoqlararo aloqaning eng ishonchli himoyasini ta’minlaydi. Tatbiqiy sath shlyuzining himoyalash funksiyalari, seans sathi shlyuziga o‘xshab, vositachilik funksiyalariga taalluqli. Ammo, tatbiqiy sath shlyuzi seans sathi shlyuziga qaraganda himoyalashning ancha ko‘p funksiyalarini bajarishi mumkin:

- brandmauer orqali ulanishni o‘matishga urinishda foydalanuvchilarni identifikatsiyalash va autentifikatsiyalash;

- shlyuz orqali uzatiluvchi axborotning haqiqiyligini tekshirish;

- ichki va tashqi tarmoq resurslaridan foydalanishni cheklash;

- axborot oqimini filtrlash va o‘zgartirish, masalan, viruslarni dinamik tarzda qidirish va axborotni shaffof shifrlash;

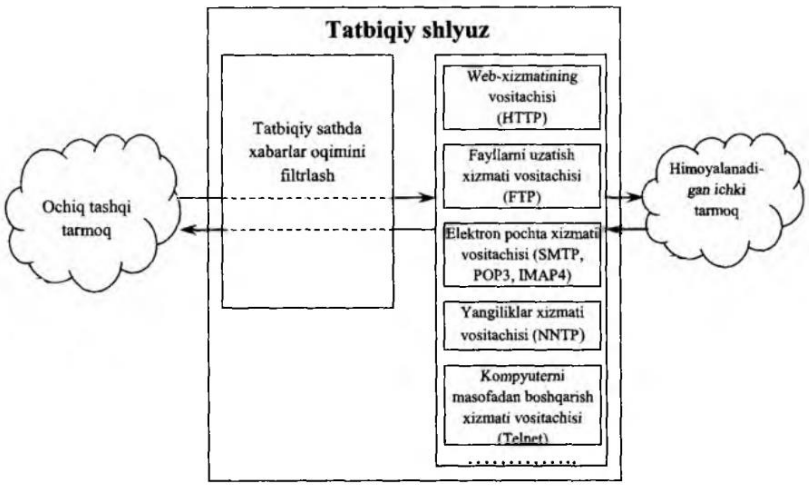
- hodisalarni qaydlash, hodisalarga reaksiya ko‘rsatish hamda qaydlangan axborotni tahlillash va hisobotlarni generatsiyalash;

- tashqi tarmoqdan so‘raluvchi ma’lumotlarni keshlash.

ISSN 2181-3187

Tatbiqiy sath shlyuzi funksiyalari vositachilik funksiyalariga taalluqli bo‘lganligi sababli, bu shlyuz universal kompyuter hisoblanadi va bu kompyuterda har bir xizmat ko‘rsatiluvchi tatbiqiy protokol (HTTP, FTP, SMTP, NNTP va h.) uchun bittadan vositachi dastur (ekranlovchi agent) ishlatiladi. TCP/IPning har bir xizmatining vositachi dasturi (applicationproxy) aynan shu xizmatga taalluqli xabarlarni ishlashga va himoyalash funksiyalarini bajarishga mo‘ljallangan.

Tatbiqiy sath shlyuzi mos ekranlovchi agentlar yordamida kiruvchi va chiquvchi paketlarni ushlab qoladi, axborotni nusxalaydi va qayta jo‘natadi, ya’ni ichki va tashqi tarmoqlar orasidagi to‘g‘ridan-to‘g‘ri ulanishni istisno qilgan holda, server-vositachi funksiyasini bajaradi (1.5-rasm).



1.5-rasm. Tadbiqiy shlyuzning ishlash sxemasi.

Tatbiqiy sath shlyuzi ishlatadigan vositachilar seans sathi shlyuzlarining kanal vositachilaridan jiddiy farqlanadi. Birinchidan, tatbiqiy sath shlyuzlari muayyan ilovalar (dasturiy serverlar) bilan bog‘langan, ikkinchidan, ular OSI modelining tatbiqiy sathida xabarlar oqimini filtrlashlari mumkin.

Tatbiqiy sath shlyuzlari vositachi sifatida mana shu maqsadlar uchun maxsus ishlab chiqilgan TCP/IPning muayyan xizmatlarining dasturiy serverlari - HTTP, FTP, SMTP, NNTP va h. - serverlaridan foydalanadi. Bu dasturiy serverlar brandmauerlarda rezident rejimida ishlaydi va TCP/IPning mos xizmatlariga taalluqli himoyalash

ISSN 2181-3187

funksiyalarini amalga oshiradi. UDP trafigiga UDP-paketlar tarkibining maxsus translyatori xizmat ko‘rsatadi.

Ichki tarmoq ishchi serveri va tashqi tarmoq kompyuteri orasida ikkita ulanish amalga oshiriladi: ishchi stansiyadan brandmauergacha va brandmauerdan belgilangan joygacha. Kanal vositachilaridan farqli holda, tatbiqiy sath shlyuzining vositachilari faqat o‘zlari xizmat qiluvchi ilovalar generatsiyalagan paketlarni o‘tkazadi. Masalan, HTTP xizmatining vositachi-dasturi faqat shu xizmat generatsiyalagan trafikni ishlaydi.

Agar qandaydir ilovada o‘zining vositachisi bo‘lmasa, tatbiqiy sathdagi shlyuz bunday ilovani ishlay olmaydi va u blokirovka qilinadi. Masalan, agar tatbiqiy sathdagi shlyuz faqat HTTP, FTP va Telnet vositachi-dasturlaridan foydalansa, u faqat shu xizmatlarga tegishli paketlarni ishlaydi va qolgan xizmatlarning paketlarini blokirovka qiladi.

Tatbiqiy sath shlyuzi vositachilari, kanal vositachilaridan farqli holda, ishlanuvchi ma’lumotlar tarkibini tekshirishni ta’minlaydi. Ular o‘zlari xizmat ko‘rsatadigan tatbiqiy sath protokollaridagi komandalarning alohida xillarini va xabarlardagi axborotlarni filtrlashlari mumkin.

Tatbiqiy sath shlyuzini sozlashda va xabarlarni filtrlash qoidalarini tavsiflashda quyidagi parametrlardan foydalaniladi: servis nomi, undan foydalanishning joiz vaqt oralig‘i, ushbu servisga bog'liq xabar tarkibiga cheklashlar, servis ishlatadigan kompyuterlar, foydalanuvchi identifikatori, autentifikatsiyalash sxemalari va h.

Tatbiqiy sath shlyuzi quyidagi afzalliklarga ega:

- aksariyat vositachilik funksiyalarini bajara olishi tufayli lokal tarmoq himoyasining yuqori darajasini ta’minlaydi;

ISSN 2181-3187

- ilovalar sathida himoyalash ko‘pgina qo‘shimcha tekshirishlarni amalga oshirishga imkon beradi, natijada dasturiy ta’minot kamchiliklariga asoslangan muvaffaqiyatli hujumlar o‘tkazish ehtimolligi kamayadi;

- tatbiqiy sath shlyuzining ishga layoqatligi buzilsa, bo‘linuvchi tarmoqlar orasida paketlarning to‘ppa-to‘g‘ri o‘tishi blokirovka qilinadi, natijada rad qilinishi tufayli himoyalanuvchi tarmoqning xavfsizligi pasaymaydi.

Tatbiqiy sath shlyuzining kamchiliklariga quyidagilar kiradi:

- narxining nisbatan yuqoriligi; - brandmauerning o‘zi hamda uni o‘matish va konfiguratsiyalash muolajasi yetarlicha murakkab;

- kompyuter platformasi unumdorligiga va resurslari hajmiga qo‘yiladigan talablarning yuqoriligi;

- foydalanuvchilar uchun shaffoflikning yo‘qligi va tarmoqlararo aloqa o‘matilishida o‘tkazish qobiliyatining susayishi.

Oxirgi kamchilikka batafsil to‘xtalamiz. Vositachilar server va mijoz orasida paketlar uzatilishida oraliq rolini bajaradi. Avval vositachi bilan ulanish o‘rnatiladi, so‘ngra vositachi adresat bilan ulanishni yaratish yoki yaratmaslik xususida qaror qabul qiladi. Mos holda tatbiqiy sath shlyuzi ishlashi jarayonida har qanday ruxsat etilgan ulanishni qaytalaydi. Natijada foydalanuvchilar uchun shaffoflik yo‘qoladi va ulanishga xizmat qilishga qo‘shimcha harajat sarflanadi.

Tatbiqiy sath shlyuzining foydalanuvchilar uchun shaffofligining yo‘qligi va tarmoqlararo aloqa o‘matilishida o‘tkazish qobiliyatining susayishi kabi jiddiy kamchiliklarini bartaraf etish maqsadida paketlarni filtrlashning yangi texnologiyasi ishlab chiqilgan. Bu texnologiyani ba’zida ulanish holatini nazoratlashli filtrlash (statefulinspection) yoki ekspert sathidagi filtrlash deb yuritishadi. Bunday filtrlash paketlar holatini ko‘p sathli tahlillashning maxsus usullari (SMLT) asosida amalga oshiriladi.

ISSN 2181-3187

Ushbu gibrid texnologiya tarmoq sathida paketlarni ushlab qolish va undan ulanishni nazorat qilishda ishlatiluvchi tatbiqiy sath axborotini chiqarib olish orqali ulanish holatini kuzatishga imkon beradi.

Ishlashi asosini ushbu texnologiya tashkil etuvchi tarmoqlararo ekran *ekspert sath brandmaueri* deb yuritiladi. Bunday brandmauerlar o‘zida ekranlovchi marshrutizatorlar va tatbiqiy sath shlyuzlari elementlarini uyg‘unlashtiradi. Ular har bir paket tarkibini berilgan xavfsizlik siyosatiga muvofiq baholaydilar.

Shunday qilib, ekspert sathidagi brandmauerlar quyidagilarni nazoratlashga imkon beradi:

- mavjud qoidalar jadvali asosida har bir uzatiluvchi paketni;

- holatlar jadvali asosida har bir sessiyani;

- ishlab chiqilgan vositachilar asosida har bir ilovani.

Ekspert sath tarmoqlararo ekranlarining afzalliklari sifatida ularning foydalanuvchilar uchun shaffofligini, axborot oqimini ishlashining yuqori tezkorligini hamda ular orqali o‘tuvchi paketlarning IP-adreslarini o‘zgartirmasligini ko‘rsatish mumkin. Oxirgi afzallik: IP-adresdan foydalanuvchi tatbiqiy sathning har qanday protokolining bunday brandmauerlardan hech qanday o‘zgarishsiz yoki maxsus dasturlashsiz birga ishlay olishini anglatadi.

Bunday brandmauerlarning avtorizatsiyalangan mijoz va tashqi tarmoq kompyuteri orasida to‘g‘ridan-to‘g‘ri ulanishga yo‘l qo‘yishi, himoyaning unchalik yuqori bo‘lmagan darajasini ta’minlaydi. Shu sababli, amalda ekspert sathini filtrlash texnologiyasidan kompleks brandmauerlar ishlashi samaradorligini oshirishda foydalaniladi. Ekspert sathning filtrlash texnologiyasini ishlatuvchi kompleks brandmauerlarga misol tariqasida Fire Wall-1 va ON Guardlarni ko‘rsatish mumkin.

Foydalanilgan adabiyotlar:

ISSN 2181-3187

1. S.K. Ganiyev, M.M. Karimov, K.A. Tashev. Axborot xavfsizligi. -T.: «Fan va texnologiya», 2017,372 bet.

2. “Journal of science-innovative research in Uzbekistan”, Volume 2, Issue 1, 2024. January.

3.GeeksForGeeks. https://www.geeksforgeeks.org/how-to-configure-firewalls-in-windows/?ref=header_outind. 2022, 28 Nov.