TARMOQ QURILMALARNING HAVSIZLIK IMKONIYATLARI VA ULARNING HIMOYA VOSITALARI TAHLILI

G'ulomov Sherzod Rajaboyevich[1], Nozimov Adxam Akramovich[2]

[1]*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, E-mail: sherzod.gulomov@tuit.uz*
[2]*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, E-mail: adkhamnozimov@gmail.com*

K A L I T S O ' Z L A R

VPN, FREESCO, IkuaiOS, Open-wrt, DD-WRT, Asus-Merlin, Firmware, Cisco IOS, ARM, Firewall, IDS-IPS, DLP, DPI, TP-Link, Zyxel, Vyatta, Juno, Embedded system, Router OS, Mikrotik, VipNet, arxitektura, Zebra, xorp, Quagga, Bird, GRE, MacSec, mini kompyuter, programmator, apparat-dasturiy, operatsion tizim, tizimlash, tizimli dasturlash.

A N N O T A T S I Y A

Mazkur maqolada Linux tizimi bilan bog'liq tadqiqot ishlar natijalarini taqdim etiladi. Linuxning kuchli tarmoq havfsizlik imkoniyatlaridan foydalanadigan dasturiy ta'minotlar imkoniyatlari haqida holda missollar keltirilgan. Bundan tashqari Linuxni ixtisoslashtirilgan qurilmalarga yoki marshrutizatorlarga o'tkazish tafsilotlari muhokama qilinadi. Jumladan, Linuxni o'rnatilgan tizim qurilmasigaga o'tkazish natijasida ishlash smaradorligi va uning samarali o'rnatish usullari yuzasidan takliflar va amalga oshirilgan natijalari yoritilgan.
Ushbu maqola kompyuter tarmoqlari xavfsizligi masalalari bilan bog'liq shug'ullanuvchi IT mutaxassislari uchun foydali bo'lishi mumkin.

I. Kirish

Bugungi kunda IP routerlar yoki IP tarmoq qurilmalari Internet yoki Global tarmoq foydalnishda eng muhim vazifalarini belgilab beradi.

Marshruztizator yoki router- bu apparat qurilmasi bo'lib, tarmoq satxida ikki yoki undan ortiq qurilmani aloqa o'rantishi, hamda qurilma tarmoq transport vositasi vazifasini bajarib beradi.

Router qurilmalarini ishlab chiqishda aksariyati qurilmaning ichki tizimida Linux operatsion tizimidan foydalanish va ularning himoya havfsizlik dasturiy ta'minotlarini imkoniyatlari qo'lanilmoqda. Yangi avlod routerni ishlab chiqish «Cisco, Mikrotik, Eltex» qurilmadagidek judda muhimdir. Shuning uchun ham, router qurilmaning ichki tizimi va imkoniyatlari tahlil qilish muhim masalardan biri hisoblanadi.

Bugungi kunda tarmoq mashrutizator qurilmaning ichiki operatsion tizimi turli hil tizimlarni uchratishimiz va ko'rishimiz mumkin.

Tarmoq marshrutizator qurilmasini ichiki tizimida eng muhim jihatlaridan biri, Bu:

- Kiberhujumlardan oldini olish imkoniyatini ishlab chiqish (Firewall, IDS/IPS)
- Tarmoq xavfsizlik protokolarni qolanilishi kriptografik akslanitirish orqali malumotlarni uzatish-qabul qilish imkoniyatini ishlab chiqish (GRE, VLAN, VPN protokolar)

Foydalanuvchilarning yangi va yanada ko'p funksiyonal IP mashrutizatorlarni ishlab chiqish judda qiyindir va mukamal hisoblanadi. Zamonaviy IP marshrutizatorlarni ishlab chiqishda qulayligi, ishonchligi, arzonligi, elektr ta'minotini kam quvvat sarflanishini hamda ixchamligini ta'minlash kerak bo'ladi.

So'ngi yillarda yangi avlod tarmoq marshrutizatorli Linux tizimiga asoslangan ko'p processorli arxitekturali, ARM plata texnalogiyasiga asoslangan ta'minlovchi qurilmalar joriy etilmoqda.

Shu o'rinda, qurilmalarni qayta "dasturlash» va "kiprografik algortim» qo'shish imkoniyatlarini

© *G'ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*

yartish mumkinligi to‘g‘risida tadqiqot ishlar olib borilmoqda.

Shu munosabati bilan, ushbu maqolada asosiy maqsadimiz marshrutizator ishlab chiqishda Opertasion tizimini, arxitekturasini o‘rganish va boshqa qurilmalar tizimlar bilan taqoslash, hamda imkoniyatlarini ko‘rib o‘tiladi.

II. Router bu nima va uning axborot xavfsizlikda qo‘lanilishi

Router bu nima ?

Marshruztizator yoki router- bu apparat qurilmasi bo‘lib, tarmoq satxida ikki yoki undan ortiq qurilmani aloqa o’rantishi, hamda qurilma tarmoq transport vositasi vazifasini bajarib beradi.

Router marshrutizasiya jadvaliga asoslangan holda ishlaydi. U ikki hil ko’rinishda bo’ladi:

- dinamik marshrutizasiya
- static marshrutizasiya

Dinamik marshrutizasiya, ko‘rinishidan qulay, uni sozlash shart emas. U o‘ziga ulangan barcha qurilmalar tog‘risida ma’lumotni saqlaydi. Vaqti – vaqti bilan tarmoqqa paketlar jo‘natib turadi va ulardan qaytgan javob orqali tarmoqni hotirasida quradi.

Statik marshrutizasiya esa tarmoq havfsizligining barcha talablariga javob beradi. Unda tarmoq marshruti avvaldan yozib qo‘yiladi. Barcha paketlar ushbu mashrutlash yo‘li bo‘yicha harakat qiladi.

Hozirgi kunda marshrutizator ishlab chiqaruvchi firmalar soni kundan kunga ko‘payib bormoqda. Misol tarqiasida Cisco, Tp-link, D-link, Tenda, Zyxell, Fast, Telmax va boshqalar shular jumlasidan ko‘rishimiz mumkin.

Marshrutizator axborot xavfsizlikda qo‘lanilishi vositalari

Marshrutizator nafaqat ikki tarmoqni bir biri bilan bog‘lab beradi, hamda lokal tarmog‘ingizni tashqi hujumlardan himoya vazifasini ham bajarib bera oladi.

Aksariyat marshrutizatorlar ichki tizimida qo‘shimcha himoya dasturiy vositalariga o‘rnatilgan bo‘ladi. Ular quyidagilar:

- IDS/IPS axborotni tashqi havfdan himoyalanish tizimi
- Firewall tizimi
- VPN tunel vositasi

Firewall

Faervollar yoki Firewall - bu oldindan belgilangan xavfsizlik qoidalari asosida kiruvchi va chiquvchi tarmoq trafigini kuzatish va filtrlash uchun mo‘ljallangan tarmoq xavfsizlik qurilmalari. Xavfsizlik devori printsipida ishlovchi dasturiy ta’minot ichki tarmoq va tashqi Internet o‘rtasida to‘siq bo‘lib, u orgali o‘tadigan barcha ma’lumotlar paketlarini tahlil qilish va tarmoq administratori tomonidan belgilangan xavfsizlik siyosatini buzuvchi trafikni blokirovka qilanadi.

Faervollar tarmoq trafigini boshqarish uchun turli usullardan foydalanadi, jumladan paketlarni filtrlash, holatni tekshirish va nazorat olib borishdir. Paketni filtrlashda har bir paketning sarlavhasi ma’lumotlarini tekshiradi, uning manbasini, manzilini, protokoli va port raqamini aniqlanadi va oldindan belgilangan qoidalarga muvofig trafikni blokirovka qilish yoki ruxsat berishni o‘z ichiga oladi. Boshqa tomondan, sozligni tekshirishda tarmoq ulanishlari holatini nazorat qiladi va faqat ruxsat berilgan trafikni o‘tkazishga imkon beradi. Ilova qatlamini filtrlash paketlar tarkibini HTTP yoki FTP kabi ma’lum dastur protokollariga mos kelishiga ishonch hosil qilish uchun tekshiradi.

Faervollardan kichik biznes, yirik korporatsiyalar va davlat idoralari kabi turli xil muhitlarda foydalanish mumkin. Ular har qanday tarmoq xavisizligi arxitekturasining muhim tarkibiy qismidir, chunki ular ruxsatsiz kirishni oldini olish, zararli dasturlarni aniqlash va blokirovka qilish hamda nozik ma’lumotlani o‘g‘irlik yoki yo‘qolishidan himoya qilishga yordam beradi.

Kichik biznesda kompaniyaning ichki tarmog‘ini tashqi tahdidlardan himoya qilish uchun xavfsizlik devoridan foydalanish mumkin. Bu xavfsizlikka xavf tug‘dirishi mumkin bo‘lgan

© *G‘ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*

ayrim turdagi trafikni bloklashni o‘z ichiga olishi mumkin, masalan, foydalanuvchi bilan fayl almashishda yoki ijtimoiy tarmog‘ida saytlaridan foydalanganda bloklanadi.

Katta kompaniyada tarmog‘ning turli qismlariga kirishni nazorat qilish uchun xavisizlik devoridan foydalanish mumkin, bu xodimning roli va kirish darajasiga bog‘liq. Misol uchun, sotuvchi kompaniyaning mijozlar ma‘lumotlar bazasiga kirishi mumkin, ammo moliyaviy tizimga kira olmaydi.

Davlat idorasida maxfiy ma‘lumotlarni roxsatsiz kirishdan himoya gilish uchun xavfsizlik devoridan foydalanish mumkin. Bunga ma’lum mamlakatlardan trafikni blokirovka qilish yoki ruxsat darajalariga qarab ma’lum turdagi ma’lumotlarga kirishni cheklash mumkin.

Xavfsizlik devorlarining bir nechta turlari mavjud, jumladan:

- Tarmoq xavfsizlik devorlari:

Bu xavfsizlik devorining eng keng tarqalgan turi bo‘lib, butun tarmoqni himoya qilish uchun mo‘ljallangan.

Ular apparat xavisizlik devori yoki dasturiy xavfsizlik devori bo‘lishi mumkin.

- Xostga asoslangan xavisizlik devorlari:

Ular alohida kompyuterlar yoki serverlarga o‘matiladi va ma’lum bir qurilmaga va undan keladigan trafikni boshqarish uchun ishlatiladi.

- Ilova xavfsizlik devorlari: Bular web yoki elektron pochta serverlari kabi ba’zi ilovalarni tashqi tahdidlardan himoya qilish uchun mo’ljallangan.
- Keyingi avlod xavfsizlik devorlari:

Bular hujumning oldini olish, paketlarni chuqur tekshirish va ilg‘or kiber tahdidlardan kengroq himoya qilish uchun SSL foydalanish orqali kabi ilg‘or xususiyatlamni o‘z ichiga oladi.

IDS/IPS tizimi

Tarmoqqa asoslangan IDS tizimlari (NIDS - Network intrusion-detection systems). Tarmoqqa asoslangan IDS tizimlari tarmoq trafigida kiberhujumlarni aniqlashga qaratilgan. NIDS tarmoq ulanishi darajasida ishlaydi va tarmoq adapteri orqali o‘tadigan barcha trafikni tahlil qiladi. Bu IDS tizimiga kiberhujum xost yoki dasturga yetib borishidan oldin aniqlash imkonini beradi. Bu tarmoqqa asoslangan IDS tizimini tarmoq tahdidlarini aniqlashda samaralidir.

IDS (Intrusion Detection System) - bu tarmoqlarni kuzatish va ruxsatsiz kirish, zararli harakatlar yoki boshqa shubhali hodisalarni aniqlash uchun qo‘llaniladigan kiberhujumni aniqlash tizimidir.

IPS (Intrusion Prevention System) - bu IDS ga o‘xshash ishlaydigan, lekin real vaqt rejimida ruxsatsiz harakatlarni avtomatik ravishda blokirovka qilish hususiyatini o‘z ichiga olgan kiberhujumni oldini olish tizimi hisoblanadi. IPS kiberhujumlarga tez va samarali javob berish, zaifliklarni bloklash va muhim resurslarni himoya qilish uchun ishlatiladi.

IPS tizimlari axborot tizimlarini kiberhujumlardan himoya qilishning muhim qismidir. Ular tarmoq paketlari darajasida ishlaydi va kompyuter tarmog‘iga yoki uning tugunlariga qilingan kiberhujumlarni aniqlash va bloklash uchun qo‘llaniladi.

VPN

VPN – shaxsiy virtual tarmoq (SHVT) protokoli deb ataladi, u albatta shaxsiy himoyalangan tarmoq ko‘rsatkichlariga ega.

VPNning boshqa tarmoqlardan asosiy farqi, bu uning boshqa tarmoqlardan ajralganligidadir. Ajralganligini ko‘rsatuvchi ko‘rsatkichlar quyidagilardan iborat:

- istalgan mustaqil tarmoq texnologiyasini tanlay olish:
- tanlash imkoniyati ishlab chiqish
- chiqaruvchining qurilmalarini imkoniyati bilan chegaralanishi mumkin;
- mustaqil manzillash tizimi. VPN da manzil tanlashda cheklanish yoki, u istalgancha bo‘lishi mumkin;
- Shaxsiy aloqa kanallari avvaldan ma’lum kafolatlangan o‘tkazuvchanlik qobiliyatini korxona qurilmalari (global ulanishlar uchun) yoki

(cc) BY © *G‘ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*

kommutatsiya qurilmalar (lokal ulanishlar uchun) o‘rtasida ta’minlaydi;

- maksimal pog‘onadagi xavfsizlik. “Tashqi dunyo» bilan aloqa yo‘qligi butun tarmoq bo‘yicha axborotni “o‘g‘irlanishi» ehtimolligini kamaytiradi.

DPI (Deep paket inspection)

DPI – bu trafikni tartibga solish va paketlarni filtrlash, shuningdek statistik ma’lumotlarni to‘plash uchun tarmoq paketlarini ularning tarkibiga qarab tekshirish texnologiyasi hosablanadi. Xavfsizlik devorlaridan farqli taraflari, Deep Packet Inspection nafaqat paket sarlavhalarini, balki tarmoqa satxining OSI modelining ikkinchi (kanal) qatlamidan boshlab boshqa paketlarni ham tahlil qila oladi.

Bundan tashqari, Deep Packet Inspection texnologiyasi Internet-provayderlarni va davlat idoralarini turli xil trafik turlariga QoS texnalogiyasi foydalanib turli xil bloklash siyosatini qo‘llash imkoniyatiga ega, taqiqlangan manbalarga kirishni cheklash, tarmoq hujumlarini aniqlash va kompyuter viruslarining tarqalishini to‘xtatish imkonini beradi oladi. Deep Packet Inspection ba’zan BitTorrent kabi ba’zi protokollarni blokirovka qilish uchun foydalanib kelinmoqda. Deep Packet Inspection yordamida ma’lumotlarni yaratgan yoki olgan dasturni aniqlash va shu asosida har qanday harakatni monitoring olib borish mumkin. Deep Packet Inspection har bir Foydalanuvchini barchasini ulanish statistikasini alohida to‘plashi mumkin va bloklash imkoniyatini beradi.

Hozirgi kunda, marshrutizatorlarga o‘rnatilgan DPI texnalogiya echimlari tobora ommalashib bormoqda. Asosan Cisco, Juniper, SNR va boshqalar qurilmalarda ko‘rishmiz mumkin.

DLP (Data leakage prevention)

DLP- bu axborot tizimidan maxfiy ma’lumotlarning chiqib ketishini oldini olish texnologiyalari, shuningdek axborotni chiqib ketishidan oldini olish uchun texnik qurilmalar yoki dasturiy ta’minot hisoblandi.

DLP tizimlari himoyalangan axborot tizimini belgilangan kalit so‘zlar orqali ma’lumotlar oqimlarini tahlil qilishga asoslangan. Ushbu maxfiy ma’lumotlar oqimida aniqlanganda, tizimning faol himoya komponenti ishga tushiriladi va xabarning uzatilishi (paket, oqim, sessiya) bloklanadi.

III ichki operatsion tizim turlari

Operatsion tizimlar: Linux embedded, Openwrt, DD-wrt, Tomato, RouterOS, Juno OS, Vyatt OS, VyOS, Cisco iOS (XR-NS), Devil OS, Freesco OS, VipNet (Astra), OPENSense, Pfsense, IPFire Armbian Linux kabilar mavjud bo‘lib.

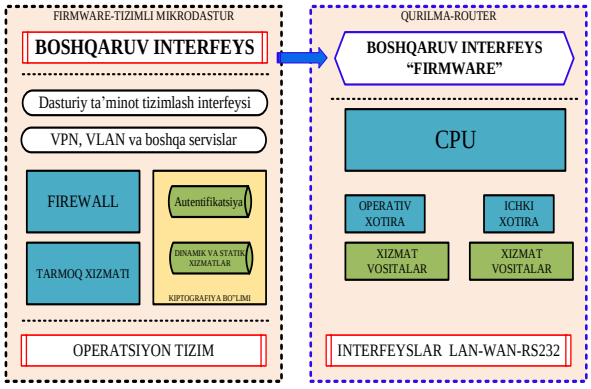
Quyidagilarni tasniflanishini ko‘rib chiqamiz.

Firmware

Tizimli mikrodasturlar- bu dasturiy ta’minot yoki qurilmaga o‘rnatilgan dasturiy ta’minot bo‘lib, tarmoq qurilmalarida yoki vositalarning tizimlarida mikrodatsurlar o‘rnatilga holda masalan Linux yadroli operatsion tizim qurilmani boshqarishga yordam beradi.

Ushbu tizimli mikrodasturlar asosan vositalarni yoki telekomunkatsyon qurilmalarini qayta dasturlash orqali ichki operatsion tizimini yangilash yoki yangi komponentlarini o‘rannatib qo‘yish imkoniyatini beradi.

Quyidagi rasmda Tizimli mikrodastur va operatsion tizimi bilan ishlash jarayonida marshrutizatorda foydalanish jarayoni yoritilgan.



1-rasm. Tizimli mikrodastur marshrutizatorda qo‘lanilishi.

Linux embedded

© *G‘ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*

Linux yadrosiga asoslangan operatsion tizimlar hisoblanib asosan elektronika vositalrida qo‘lanilib kelinmoqda hozirgi kunda ko‘plab vositalarda uchratishimiz mumkin masalan: IP-TV pristavkalar, Smart TV va Linux yadrosiga asoslangan operatsion tizimlar tarmoq uskunalari marshrutizatorlar kabi tobar foydalanilib ish jaroyonida qo‘lanilmoqda. Linux yardosiga asoslangan operatison tizimi judda keng meqiyosida tanilib bormoqda va axborot xavfsizlik jaroyonida qo‘lanilshida foydalalanib kelinmoqda.

Openwrt embedded system

OpenWrt (router yoki marshrutizatordan) Linuxga asoslangan o‘rnatilgan operatsion tizimlar uchun ochiq kodli loyiha bo‘lib, asosan tarmoq marshrutizatisyalash uchun o‘rnatilgan qurilmalarda foydalaniladi . Barcha komponentlar uy routerlarida mavjud bo‘lgan cheklangan xotira va xotiraga sig‘adigan darajada kichik bo‘lishi uchun optimallashtirilgan tizimdir.

OpenWrt interfeysi (terminal-shell) yoki web-interfeysli (LuCI) yordamida sozlamalr qilish imkoniyatiga egadir . opkg paketlarni boshqarish tizimi orqali yordamchi dasturiy ta’minotlar o‘rnatish uchun 8000 ga yaqin ixtiyoriy dasturiy paketlar mavjud.

OpenWrt har xil turdagi qurilmalarda ishlatish imkoniyatiga egadir, jumladan routerlarida, turar-joy shlyuz qurilmalar, smartfonlarda ishlashi mumkin. Shaxsiy kompyuterlar va noutbuklarda OpenWrt-ni tizimini ishga tushirish imkoniyatiga egadir.

DD-WRT embedded system

DD-WRT routerlar uchun Linuxga asoslangan dasturiy ta’minot va operatsion tizimi hisoblanadi. Dastlab Linksys WRT54G seriyasi uchun ishlab chiqilgan bo‘lsa, endi u turli xil modellarda ishlaydi. DD-WRT - bu ishlab chiqaruvchining original dasturiy ta’minoti Open-WRT tizimi asosida yaratilgan bo‘lib unga qo‘shimcha funktsiyalar va web-interfeysi takominlashtirilgan.

Tomato embedded system

Tomato - bu hamjamiyat tomonidan ishlab chiqilgan linux yadrosiga asoslangan tizmi bo‘lib, iste’molchi darajasidagi kompyuter tarmog‘i routerlari va Broadcom chipsetlari tomonidan quvvatlanadigan shlyuzlar uchun maxsus mikrodasturlar oilasi hisoblanadi.

Router OS

MikroTik mahsulotlaridan biri RouterOS, Linux-ga asoslangan tarmoq operatsion tizimi. RouterOS MikroTik RouterBoard routerlariga o‘rnatish uchun mo‘ljallangan bo‘lib.

Bundan tashqari, ushbu tizimni shaxsiy kompyuterga o‘rnatish mumkin, uni xavfsizlik devoir (Firewall), VPN server / client, QoS va boshqalar funktsiyalariga ega. RouterOS-ning bulutli virtual mashinalar uchun mo‘ljallangan Cloud Hosted Router deb nomlangan maxsus versiyasi ham mavjud.

Operatsion tizimda ko‘payib borayotgan xususiyatlar bilan bir necha darajadagi litsenziyalar mavjud.

Bundan tashqari, RouterOSni sozlash uchun grafik interfeysni ta’minlovchi Winbox deb nomlangan dastur mavjud. RouterOS bilan ishlaydigan qurilmalarga veb-interfeys, FTP , Telnet va SSH orqali ham kirish mumkin. Boshqaruv va monitoring uchun maxsus ilovalar yaratish imkonini beruvchi API ham mavjud.

Juno OS

Junos OS (Juniper Junos , Junos va JUNOS nomi bilan ham tanilgan) Juniper Networks marshrutlash, kommutatsiya va xavfsizlik qurilmalarida qo‘llaniladigan FreeBSD- ga asoslangan tarmoq operatsion tizimidir.

Vyatta OS

Vyatta - bu dasturiy ta'minotga asoslangan virtual router , virtual xavfsizlik devori va Internet protokoli tarmoqlari (IPv4 va IPv6) uchun VPN mahsulotlari . Vyatta-ni bepul yuklab olish mavjud. Tizim Quagga , OpenVPN va boshqa ko'plab tarmoq ilovalari bilan Debianga asoslangan ixtisoslashtirilgan Linux distribyutsiyasidir .

Juniper JUNOS yoki Cisco IOS ga o‘xshash standartlashtirilgan boshqaruv konsoli, webga asoslangan GUI va Linux tizimi buyruqlariga qo‘shimcha ravishda, tizim va ilovalarning konfiguratsiyasini ta’minlaydi. Vyattaning so‘nggi versiyalarida webga asoslangan boshqaruv interfeysi faqat obuna nashrida taqdim etiladi. Biroq, barcha funksiyalar KVM, ketma-ket konsol yoki SSH/telnet protokollari orqali mavjud. Dasturiy ta’minot standart x86-64 serverlarida ishlaydi.

Freesco OS

FREESCO (BEPUL ciSCO degan ma’noni anglatadi) 10 tagacha Ethernet / ARCNet / Token ring / ArLAN tarmoq kartalarini va 10 tagacha modemlarni qo’llab-quvvatlaydigan tijorat marshrutizatorlarini bepul va ochiq kodli router operatsion tizimidir .

VipNet

InfoTeKSning eng yaxshi rivojlanayotgan ViPNet texnologiyasi asoslangan qurilmalar bo‘lib, xavfsiz tarmoqda VPN yoki Firewall marshrutizator vositasi ishlab chiqarishadi.

virtual xususiy tarmoqlarni (VPN) va ochiq kalitlar infratuzilmasini (PKI) tashkil qilish uchun dasturiy ta’minot va apparat - dasturiy ta’minot ishlab chiqaradi;

xavfsizlik devorlari va shaxsiy himoya devorlari ishlab chiqaradi;

kompyuterlarda va tarmoqda saqlanadigan va qayta ishlanadigan ma’lumotlarni shifrlash vositalarini ishlab chiqaradi;

axborot xavfsizligi vositalarini markazlashtirilgan boshqarish va monitoring qilish tizimlarini ishlab chiqaradi;

uchinchi tomon ishlab chiquvchilarining amaliy tizimlariga (yuridik ahamiyatga ega hujjat aylanishi tizimlari, portallar va boshqalar) joylashtirish uchun axborotni kriptografik himoya qilish vositalarini ishlab chiqaradi;

ViPNet IDS kompyuter hujumlarini aniqlash uchun dasturiy va apparat tizimlari (yoki mustaqil tarmoq qurilmalarini) ishlab chiqaradi.

ikuaiOS

IkuaiOS - bu Linuxga asoslangan apparat va marshurutizator tarmoq operatsion tizimidir. Ushbu tizim axborot xavfsizligini ta’minlashda DPI texnalogiyasiga asoslangan va boshqa texnalogiya funksiyalari ega bo’lgan apparat va dasturiy ta’minot hisoblanadi.

Quyidagi funksiyonal imkoniyatlarga ega

- DPI texnalogiya orqali barcha xavfsizligini vazifalarni ta’minlaydi.
- Tarmoqni balanslashtirish va monitoring olib borish imkoniyatini ta’minlaydi.
- Himoyalangan aloqa kanalarini tashkil etish imkoniyatiga ega.
- Foydalanuvchilarni ushbu ulangan tarmoqda barcha turdagi qurlmalarni boshqarish va IDS-IPS tizimlarni ko’tarish, qurilmalarni masofadan boshqarish mumkin.

III. Marshrutizatorning arxitekturasi va uning tashkil etuvchilari

Marshrutizatorning arxitekturasi

Ushbu bo‘limda routerning marshrutiztsiya qilishning asosiy komponentlari va algoritm komponentlari hamda uning arxitekturasi yoritiladi.

Arxitektura 2-rasmdagi umumiy xotira arxitekturasi interfeyslar umumiy shina orqali umumiy xotiraga kirish saqlash mumkinligi ko'rsatadi.

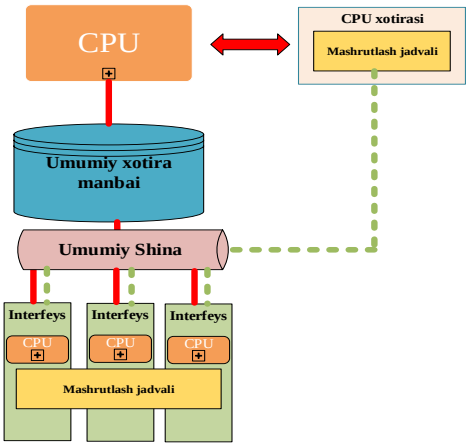
Ushbu arxitekturada bitta protsessor (CPU) o’zida ma’lumot va marshrutlash jadvallarini o‘ziga xos ajratilgan protsessor ichki xotirada saqlaydi.

Interfeyslar kerakli marshrutlash ma’lumotlarini yoki qarorlarini oladi, protsessorlarning umumiy xotirasi orqali bajariladi. Ushbu 2-rasmda boshqa turdagi arxitektura «ma’lumotlar o‘zaro faoliyatini» (cross bar datapath) deb nomlanuvchi jaryoni yoritilgan.

Aksariyati umumiy xotira, ushbu arxitekturada har bir interfeysida o‘zining ichki xotirasida (memory) va har bir kommandalarini, mashrutlash jadvalini (route inforamtion) mahalliy

(cc) BY © *G‘ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*

interfeysning (LAN-WAN interface) har biri o‘z xotirasida saqlaydi, keyinchalik uni foydalanish imkoniyatini yaratadi, o‘zgarishlar bo‘lsa uni qaytadan jadval xotirasiga saqlaydi.



2-rasm. Umumiy router arxitekturasi cross bar datapath va umumiy xotira manbai blok sxemasi

Marshrutizatorning dasturiy ta’minoti va uning arxitekturasi

Internet orqali uzatiladigan ma’lumotlarning turi va miqdori kundan-kunga oshib bormoqda. Bu hajm ortishi bilan yanada talab qiladigan murakkab tarmoq uskunalari ishlab chiqishga olib keladi, jumladan narxning oshishiga ham olib keladi.

Ayni paytda ochiq kodli dasturiy ta’minotlar axborot xavfsizligida va texnalogiyalarda qo‘llanilishi yangi turdagi qurilamalarni yartatishga yordam beradi. Ushbu yonalishda ko‘plab loyihalar shakllantirilmoqda va ishga tushirilmoqda, buning natijasida bir nechta ochiq kodli dasturiy ta’minotlar ishlab chiqildi. Misol tarqasida Zebra, XORP, Click, Quagga, BIRD va boshqalar kabi loyihalar amalga oshirilgani eslatib o‘tiladi. (3-rasm)

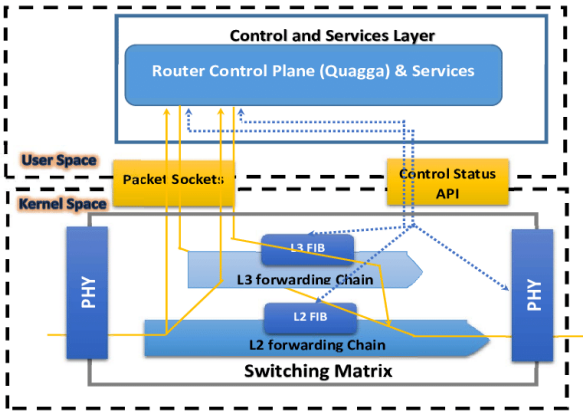
Zebra – dasturiy ta’minot marshrutizatsiyalash paketi bo‘lib, RIPv1,2, va OSPF v2, BGP v4, IPv4,6 protokolarni bilan ishlaydi. Zebra tizimi asosan Linux OTlar ishlaydi va qo‘laniladi.

XORP – bu ochiq kodli tarmoq dasturiy ta’minoti tarmoqlarni boshqarishda va rivojlantirishda qo‘laniladi. XORP bu boshqaruv tizimini (CLI) orqali boshqarishda komandalar bilan boshqariladi va protokolardan foydalaniladi.

Quagga – bu dasturiy ta’minot marshrutizatsiyalash paketi bo‘lib, RIPv1,2, va OSPF v2, BGP v4, IPv4,6 protokolarni bilan ishlaydi. Zebra va Quagga tizimi asosan Linux OTlar ishlaydi va qo‘laniladi va juda bir birga o‘xshaydi.

BIRD – bu dasturiy ta’minot marshrutlash vositasi asosan protokollarni qo‘shish va yangi tizimlarni foydalanish imkoniyatini beradi.

Click – bu ochiq kodli dasturiy ta’minot modul arxitekturasi dasturi bo‘lib asosan bu dastur Linux OTda yardrosini boshqarishda va sozlashda qo‘laniladi va IP marshrutlash qoidalarini yaratishda keng foydalaniladi.



3-rasm. Ochiq kodli router dasturiy ta’minotning arxitekturasi

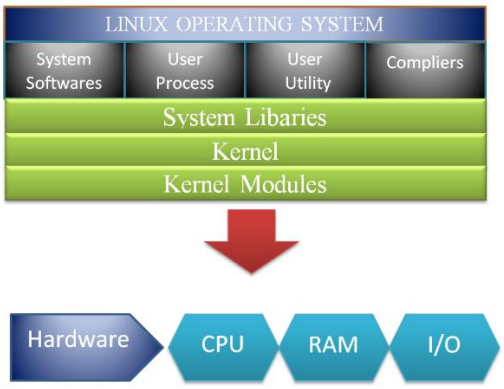
Bu sa'y-harakatlarning natijasi, yangi avlod routerlarning shakllanishiga sabab bo‘ldi. Asosan Open Software Router, Open Router va deb nomlanuvchi Ochiq kodli router misol qilamiz. Devil Linux kabi muvaffaqiyatli loyiha sifatida ochiq kodli dasturiy ta’minot/apparat tizimlari asosida ilmiy ishlar olib borilganini ko‘rishimiz mumkin, ushbu texnalogiyasida kompyuter arxitekturasi sifatida router yartishni imkoniyatini tashkil etilgan yuzasidan malumotlarga egamiz. (4-rasm)

Router vositalarini kompyuter asosida arxitekturasida foydalanish bir nechta afzalikllarini ko‘ramiz. Ular quyidagilar:

- Qurilmani ishlab chiqishda qiymati arzonligi
- Kompyuter arxitekturasida ishlab chiqilgan qurilma texnik hujjatlar va ichki imkoniyatlarni aniqligi

(cc) BY © *G‘ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*

- Kompyuterda arxitekturasida ishlab chiqilgan dasturiy ta'minotlar takominlashtirish imkoniyatiga egaligi



4-rasm. Linux OT asosida qurilgan router arxitekturasi.

IV. Xulosa

Xulosa qilib aytadigan bo‘lsak, mashruzatorlar yaratilishida Linux yadroli Operatsion tizimlar ko'plab uchratrmoqadamiz. Telekominikatsiya qurilma yaratilayotgan texnalogiyasida kiberhujumlarni oldini oluvchi yordamchi funksiyonal dasturiy ta'minotlar qo'lanilb kelinadi. Misol tariqasida CISCO, ikuaiOS, Juniper, Asus-merlin qurilmasi ichida barcha turdagi imkoniyatlar IDS-IPS, DLP, DPI, VPN kabi dasturlarni ko‘rishimiz mumkin yagona tizimda ishlaydi.

Zamonaviy kiberhujumlar butun dunyo bo‘ylab oddiy foydalanuvchilarni, hukumatlar uchun jiddiy xavf tug‘dirmoqda. Texnologiyaga qaramlik kuchayib borayotganligi kibertahdidlarning turlarini va ularning oldini olish uchun ko‘rilishi zarur bo‘lgan himoya choralarini qo‘llash juda muhimdir.

Kiberxavfsizlik bo‘yicha yagona bu texnik yechimi bu Marshrutizator yoki Firewall qurilmalar kabi texnalogik yechimlar qo‘llash va kiberhujumdan bartaraf etishdir.

Shuni takidlash joizki, respublikamizda ishlab chiqarilayotgan milliy vositasilarni shu texnalogiyaga asoslangan vositalar mavjud emas. Shu texnalogiyani mukammal o‘rganish tadbirlarini olib borish zarur, ularni amaliyotda tadbiq qilish, yaratish, maxsus sharoitlarda foydalanishda o‘z samarasini beradi.

Tadqiqot natijasida quyidagi xulosalar olindi:

1. Marshrutizatorlar mo'ljalangan Operatsion tizimlar ko‘plab turlari aniqlandi, ularni texnologiyasi, qurilmaning arxitekturasi va dasturiy ta'minot modullarni foydalangan holda milliy dasturiy ta'minotni ishlab chishda yordam beradi.

2. Apparat-dasturini ishlab chiqishda tarmoq kiberhujumlarining oldini olishga va ma'lumotlarni himoya qilishga yordam beradigan himoya vositalarini tahlil qilindi. Linux yadroli operatsion tizimda foydalnish imkoniyatlaridan qo'lanilmoqda va tashkil etiladi.

3. Programmator vositalarni protativ qurilmalar tizimli dasturlashda (Firmware upgrade) muayyan vaziyat uchun tizimni tanlashda e'tiborga olish kerak bo‘ladi.

4. VPN hosil qiluvchi qurilmalarda kriptografik akslantirishda algoritmlarni va kalit hosil qiluvchi generatorni qo'llanish metodlarni kengi tadqiqot ish faoliyatimizda tahlil qilish tavsiya etiladi.

5. O‘zbekiston Respublikasida joylashgan ishlab chiqaruvchi korxonalardan marshrutizator qurilmalarni o‘rganish va tizimli dasturlar o‘rnatish ustidan tadqiqot ishlar olib borish tavsiya etiladi.

Xulosa qilib aytish mumkinki, axborot xavfsizlik sohasida milliy VPN dasturiy ta'minotini tadbiq qilish bugungi kunda dolzarb masalalardan biri hisoblanadi. Yurtimizda ushbu sohada milliy VPN hosil qiluvchi dasturiy ta'minotlar yoki VPN hosil qiluvchi apparat-dasturiy ta'minotlar bo‘lmagan sababli o‘rganish ishlar olib borish muhimdir.

V.ADABIYOTLAR

1. M. Handley, O. Hodson, E. Kohler, Xorp: An open platform for network research, SIGCOMM Computer Communication Review 33 (1) (2003) 53–57.
2. Linux embedded system www.openwrt.org
3. Linux distributive OS for devices www.armbian.com

(cc) BY © *G'ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*

4. Openvpn server va kliyent tashkil etish maqolasi www.openvpn.com
5. J. Naous, G. Gibb, S. Bolouki, N. McKeown, Netfpga: Reusable router architecture for experimental research, in: Proceedings of the ACM Workshop on Programmable Routers for Extensible Services of Tomorrow, PRESTO '08, 2008, pp. 1–7.
6. Cisco router architecture, www.cisco.com/networkers/nw99 pres/601.pdf
7. Routers and wireless, http://www.mikrotik.com
8. Производство производства телекоммуникационных оборудование роутеров, USB модемов и прочее в Узбекистане. https://elius.uz/ru/
9. Производство мобильных и стационарных телефонов, а так-же умных часов, гаджетов, MI-FI роутеров, USB модемов с точкой доступа WI-FI и прочее в Узбекистане. https://idevice.uz/ru/
10. Intrusion Detection VS Prevention Systems, (2022) // https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems
11. Jungwon Kim, Peter J. Bentey. Immune system approaches to intrusion detection-a review. Future Generation Computer Systems, 116, 335-345.
12. Jairo a router technology of your attention, http://jairoproject.com/aboutus.html.
13. The bird internet routing daemon, http://bird.network.cz/.
14. Bsdrp router features, http://bsdrp.net/features.
15. Openbsd, http://www.openbsd.org/.
16. B. C. B. Chan, J. C. F. Lau, J. C. S. Lui, Opera: An open-source extensible router architecture for adding new network services and protocols, Journal of System and Software 78 (1) (2005) 24–36.
17. B.a.t.m.a.n. advanced documentation overview, http://www.openmesh.org/projects/batman-adv/wiki/Doc-overview.
18. Openbgpd, http://www.openbgpd.com/.
19. Vpn routers, http://www.sabaitechnology.com/vpn-routers/.
20. Network, http://demo.jairoproject.com/apps/basicNetwork/.
21. B. Bahrambeigy, M. Ahmadi, M. Fazlali, Bloom-bird: A scalable open source router based on bloom filter, in: 22nd Iranian Conference on Electrical Engineering (ICEE-2014), 2014, pp. 980–985.
22. R. Fatoohi, R. Singh, Performance of zebra routing software, in: IMSA, 2001, pp. 108–113. [23] K. Ishiguro, Gnu zebra, http://www.cs.virginia.edu/~cs458/material /zebramanual-Sept2002.pdf (September 2002).
23. V. Eramo, F. Miucci, M. Listanti, A. Cianfrani, S. Testa, Migration time experimental evaluation in a quagga based-software router, in: 2013 International Conference on Convergence (ICTC), 2013, pp. 80–83.
24. P. Jakma, D. Lamparter, Introduction to the quagga routing suite, IEEE Network 28 (2) (2014) 42–48.
25. S. Takov, A. Smiljani, Evaluation of is-is implemented in quagga.
26. M. R. Nascimento, C. E. Rothenberg, a. M. F. M. a. M. R. Salvador, Quagflow: Partnering quagga with openflow, SIGCOMM Computer Communication Review 40 (4) (2010) 441–442.

© *G'ulomov Sherzod Rajaboyevich, Nozimov Adxam Akramovich*