YANGI O‘ZBEKISTON, YANGI TADQIQOTLAR JURNALI
Volume 2 Issue 1 03.01.2025
https://phoenixpublication.net/ Online ISSN: 3030-3494

CISCO ROUTERLARDA NAT YECHIMINI TADBIQ QILISH
IMPLEMENTATION OF NAT SOLUTION ON CISCO ROUTERSВНЕДРЕНИЕ NAT РЕШЕНИЯ НА МАРШРУТИЗАТОРЫ CISCO

Murodov Ne’mat Qahramon o’g’li
Babaqulov Bekzod Mamatqulovich
Mirzo Ulug’bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali Axborot xavfsizligi (sohalar bo‘yicha) 3-kurs talabasi
nematmurodov231@gmail.com
b_babaqulov@jbnuu.uz
tel: +998904939933

Annotatsiya: *Ushbu maqolada Cisco routerlarida NAT (Network Address Translation) texnologiyasini tadbiq qilish usullari va uning tarmoq xavfsizligini ta'minlashdagi o'rni ko'rib chiqiladi. Tadqiqot davomida NAT ishlash tamoyillari, konfiguratsiya jarayoni hamda uning tarmoq samaradorligini oshirishdagi roli tahlil qilingan. Amaliy natijalar NAT yordamida manzillarni qayta xaritalash va tarmoqdagi manzillarni yashirish orqali xavfsizlikni oshirish mumkinligini ko'rsatadi. Maqola Cisco qurilmalarida NATni muvaffaqiyatli tadbiq qilish uchun qo'llaniladigan aniq yechimlar va tavsiyalarni ham o'z ichiga oladi.*

Kalit so‘zlar: *NAT, Cisco router, tarmoq xavfsizligi, IP manzilni qayta xaritalash, tarmoq samaradorligi, NAT konfiguratsiyasi, tarmoq texnologiyalari, routing va switching, tarmoq arxitekturasi, internet ulanishi, tarmoq protokollari, PAT (Port Address Translation), statik NAT, dinamik NAT, tarmoq boshqaruvi, tarmoq optimizatsiyasi, tarmoq muammolarini bartaraf etish.*

Abstract: *This article examines the methods of implementing NAT (Network Address Translation) technology on Cisco routers and its role in ensuring network security. The study analyzes the principles of NAT operation, the configuration process, and its role in enhancing network efficiency. Practical results demonstrate that NAT can improve security by remapping addresses and hiding network addresses. The article also includes specific solutions and recommendations for successfully implementing NAT on Cisco devices.*

Keywords: *NAT, Cisco router, network security, IP address mapping, network efficiency, NAT configuration, network technologies, routing and switching, network architecture, internet connectivity, network protocols, PAT (Port Address Translation), static NAT, dynamic NAT, network management, network optimization, troubleshooting network issues.*

Аннотация: *В данной статье рассматриваются методы внедрения технологии NAT (Network Address Translation) на маршрутизаторах Cisco и её роль в обеспечении сетевой безопасности. В исследовании анализируются принципы работы NAT, процесс настройки и его роль в повышении эффективности сети. Практические*

результаты показывают, что NAT может повысить безопасность за счёт переназначения адресов и скрытия сетевых адресов. Статья также содержит конкретные решения и рекомендации по успешной реализации NAT на устройствах Cisco.

Ключевые слова: *NAT, маршрутизатор Cisco, сетевая безопасность, переназначение IP-адресов, эффективность сети, настройка NAT, сетевые технологии, маршрутизация и коммутация, архитектура сети, подключение к интернету, сетевые протоколы, PAT (Port Address Translation), статический NAT, динамический NAT, управление сетью, оптимизация сети, устранение проблем в сети.*

Kirish.

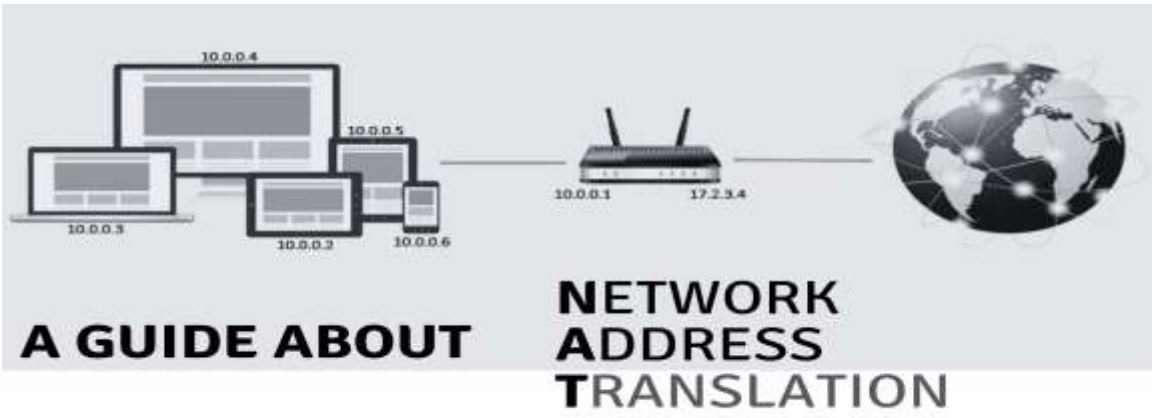
Bugungi kunda global tarmoq infratuzilmasining rivojlanishi va internetga ulanadigan qurilmalar sonining ortishi bilan IP manzillarni samarali boshqarish va tarmoq xavfsizligini ta'minlash masalalari tobora dolzarb bo‘lib bormoqda. IPv4 manzillarining cheklanganligi sababli NAT (Network Address Translation) texnologiyasi zamonaviy tarmoqlarni boshqarishning ajralmas qismiga aylandi. Ushbu texnologiya, bir tomondan, tarmoqdagi ichki qurilmalar uchun manzillarni qayta xaritalash orqali internet manzillarini tejash imkonini bersa, boshqa tomondan, tarmoq xavfsizligini oshirish va ichki manzillarni yashirish imkoniyatini yaratadi.

Cisco routerlari NAT texnologiyasini amalga oshirishda tarmoq administratorlari orasida keng qo‘llaniladigan asosiy vositalardan biri hisoblanadi. Ular NAT konfiguratsiyasi va boshqaruvini yuqori darajada soddalashtiradi va samaradorligini ta’minlaydi. Shu bilan birga, Cisco qurilmalari orqali NATni samarali tadbiq etish tarmoqning barqaror ishlashiga, xavfsizlik darajasining oshishiga hamda muhandislik resurslaridan oqilona foydalanishga xizmat qiladi.

Ushbu maqolada NATning ishlash tamoyillari, Cisco routerlarida NAT texnologiyasini amalga oshirish usullari, konfiguratsiya jarayoni va uning tarmoq samaradorligi hamda xavfsizlikni oshirishdagi roli batafsil o‘rganiladi. Tadqiqotning asosiy maqsadi – Cisco routerlarida NATni muvaffaqiyatli qo‘llash bo‘yicha amaliy tajribalar va tavsiyalarni taqdim etishdan iborat.

NAT (Network Address Translation)

Internet kengroq qo'llanilganda, ko'proq qurilmalar ulanadi va IP-manzillarning mavjudligi jiddiy muammoga aylanadi, tarmoq manzillarini tarjima qilish juda muhim texnologiyadir. NAT aslida ba'zi vaziyatlarda muammoni juda yaxshi hal qiladigan "vaqtinchalik echim" dir. Uzoq muddatda IP protokolining keyingi avlodi IPv6 yechim bo'lishi mumkin.



1-rasm. *NAT*

Router orqali tranzit paytida IP-paketlar sarlavhasini o'zgartirish orqali Internet protokoli (IP) manzilini boshqasiga ko'rsatish usuli tarmoq manzilini tarjima qilish (NAT) deb nomlanadi. Ushbu texnikaning bir qismi sifatida NAT sozlamalari butun tarmoq uchun faqat bitta IP-manzilni tashqi dunyoga ko'rsatishi mumkin, bu asosan butun ichki tarmoqni maskalashi va xavfsizlikni qo'shishi mumkin. Tarmoq manzilini tarjima qilish odatda masofaviy kirish stsenariylarida qo'llaniladi, chunki u manzilni saqlash va xavfsizlikni oshiradi. Bu xavfsizlikni yaxshilaydi va kompaniya talab qiladigan sonini kamaytiradi .

NAT qanday ishlaydi ?

Sizning uy routeringizga ulangan noutbukingiz bor deb taxmin qiling. Kimdir o'z noutbukida sevimli restoraniga yo'nalish qidirmoqda. Ushbu so'rov paket sifatida noutbukdan routerga yuboriladi, so'ngra uni internetga yo'naltiradi. Biroq, marshrutizator birinchi navbatda chiquvchi IP-manzilni shaxsiy mahalliy manzildan ommaviy manzilga o'zgartirishi kerak.

Qabul qiluvchi server, agar paket shaxsiy manzilga ega bo'lsa, ma'lumotni qayerga qaytarib yuborishni bilmaydi - bu jismoniy pochta jo'natish va qaytarish xizmatini izlashga o'xshaydi, lekin anonim qaytish manzilini taqdim etadi. Ma'lumot noutbukga NAT tufayli noutbukning shaxsiy manzili emas, balki routerning umumiy manzili yordamida qaytariladi.

Tarmoq manzillarini tarjima qilish xavfsizlikni qanday yaxshilaydi ?

Bu birinchi navbatda xavfsizlik uchun noaniqlik haqida. NAT qurilmasi barcha tarmoq qurilmalarini NAT qurilmasining yagona IP-manzilidan chiqayotgandek qilib “yashiradi”.

Barcha tizimlar tarmoq ichida o'z IP manziliga ega bo'lsa-da, Internetning qolgan qismi bilan o'zaro aloqada bo'lganda, ular ichki qurilmalar xaritasiga ega bo'lgan NAT orqali o'tadilar. Natijada, NAT qaysi qurilma internet-trafikni uzatishni biladi.

Biroq, tarmoqdan tashqarida NAT IP manzili ko'rinadigan yagona narsa; har qanday ichki qurilmalarning ichki IP-manzillarini aniqlashning to'g'ridan-to'g'ri, oddiy usuli yo'q.

Boshqa tomondan, NAT haqiqiy xavfsizlik qurilmasi emas. U ichki IP-manzillarni maskalashi mumkin, ammo u zararli trafikka ta'sir qilmaydi. Natijada, tajovuzkor NAT ga

oddiygina zararli dastur yuborishi mumkin, u NAT ning qurilmalarning tarmoq xaritasiga kirish huquqini oladi yoki infektsiyaga qarab to'g'ridan-to'g'ri ichki qurilmaga o'tadi.

Shuning uchun NAT ga qo'shimcha ravishda sizga xavfsizlik devori kerak bo'ladi . NAT asosan tizim boshqaruvchilari tomonidan Internetga tarmoq tiqilib qolishini kamaytirish uchun ishlatiladi; Internet orqali kirish mumkin bo'lgan o'z IP-manziliga ega bo'lgan har bir tizim o'rniga, muammolarni bartaraf etish va tizimni sozlashda yordam beradigan yagona IP-manzil ishlatiladi.

Tarmoq manzillarini tarjima qilish tarixi nima ?

Internet protokoli spetsifikatsiyasi nashr etilgandan keyin Internet tez o'sdi. 1991 yilda RFC 1287 (Internet muhandisligi bo'yicha ishchi guruhi tomonidan ishlab chiqarilgan RFClar kompyuter tarmoqlarining ko'p jihatlarini qamrab oldi.) "Kelajak Internet arxitekturasi sari" nashri chiqdi va bu, ehtimol, IP-manzillar maydonining tugashi masalasini ko'targan birinchi RFC bo'lishi mumkin. yaqin kelajak.

1992 yil may oyida nashr etilgan RFC 1335 ichki IP-manzillardan (shuningdek, shaxsiy IP-manzillar sifatida ham tanilgan) IP-manzillar tugashiga yechim sifatida foydalanishning batafsil tavsifini beradi. NAT kontseptsiyasini tavsiflovchi birinchi maqola "IP Internetni manzilni qayta ishlatish orqali kengaytirish" 1993 yil yanvar oyida "Computer Communication Review" nashrida paydo bo'ldi va bir yildan so'ng RFC 1663 nomi bilan nashr etildi.

NAT turlari qanday ?

Tarmoqlarda turli xil NAT turlari qo'llaniladi. Ushbu NATlar turli maqsadlarda qo'llaniladi. Ushbu NAT turlarining har biri quyida keltirilgan.

1. Statik NAT
2. Dinamik NAT
3. Port manzilini tarjima qilish (PAT)

1. Statik NAT

Tarmoq trafigi statik tashqi IP manzildan ichki IP manzilga yoki statik NAT orqali tarmoqqa ko'rsatiladi. U haqiqiy manzillarni statik tarzda xaritalangan manzillarga aylantiradi. Statik NAT tarmoq qurilmalarini ro'yxatdan o'tmagan shaxsiy IP-manzilga ega shaxsiy LAN orqali internetga ulaydi.

Bir IP quyi tarmog'idan ikkinchisiga birma-bir xaritalash statik NAT tomonidan aniqlanadi. Bir yo'nalishda xaritalash maqsad IP-manzil tarjimasini, ikkinchisida esa manba IP-manzil tarjimasini o'z ichiga oladi. Virtual xost IP-manzili NAT qurilmasining asl manzili bo'lsa, xaritalangan manzil esa haqiqiy xost IP-manzilidir.

Ulanishlar tarmoqning har ikki tomonida statik NAT orqali paydo bo'lishi mumkin, lekin tarjima birma-bir yoki bir xil o'lchamdagi manzillar bloklari o'rtasida cheklangan. Har bir shaxsiy manzilga umumiy manzil belgilanishi kerak. Manzil hovuzlari talab qilinmaydi.

Quyidagi tarjima turlari ham statik NAT tomonidan qo'llab-quvvatlanadi:

- Bir nechta IP-manzillar va port diapazonlarini bitta IP-manzilga va boshqa port diapazoniga moslashtirish uchun.
- Muayyan IP manzil va portning IP manzili va portini o'zgartirish uchun.

2. Dinamik NAT

Shaxsiy IP-manzil dinamik NAT-da NAT hovuzi sifatida tanilgan umumiy IP-manzillar guruhidan umumiy IP-manzilga ko'rsatiladi. Shaxsiy IP-manzil va umumiy IP-manzil o'rtasidagi yakkama-yakka xaritalash dinamik NAT orqali o'rnatiladi . Umumiy IP-manzil NAT routerining uchida aniqlangan IP-manzillar to'plamidan tanlanadi. Umumiy va shaxsiy xaritalash NAT hovuzida mavjud bo'lgan umumiy IP manziliga qarab farq qilishi mumkin.

Dinamik NAT, ichki ro'yxatdan o'tmagan manzillar va tashqi ro'yxatdan o'tgan manzillar o'rtasida birma-bir tarjimani yaratadigan statik NATdan farqli o'laroq, bir nechta ichki manzillar bir xil umumiy manzildan foydalanadigan ko'p-bir tarjimani yaratadi. Dinamik NAT besh qiymatni (manba manzili, manba porti, maqsad manzili, maqsad port va protokol) saqlaydigan har bir TCP yoki UDP ulanishi uchun holat jadvalini saqlash orqali IP-manzil ziddiyatlarini bartaraf qiladi.

3. PAT

Mahalliy tarmoqdagi (LAN) bir nechta qurilmalar tarmoq manzillarini tarjima qilish (NAT) ning kengaytmasi bo'lgan Port manzillari tarjimasi (PAT) yordamida bitta umumiy IP manzilga ko'rsatilishi mumkin. PAT ning maqsadi IP manzillarini saqlashdir.

Ko'pgina uy tarmoqlarida PAT ishlatiladi. Bunday holda, Internet-provayder (ISP) uy tarmog'idagi routerga bitta IP-manzilni tayinlaydi. Router ushbu tarmoqdan Internetga ulanganda X kompyuteriga port raqamini ajratadi. Keyin ichki IP manzili bunga qo'shiladi. Natijada X kompyuteri o'zining noyob manzilini oladi. Y kompyuteri X kompyuteri bilan bir vaqtda internetga ulanganda, marshrutizator unga alohida port raqamini beradi.Ikkala mashina ham bir xil umumiy IP manzilga ega va bir vaqtning o'zida internetga ulanadi. Boshqa tomondan, marshrutizator har doim qaysi paketlarni jo'natish kerakligini va ular qaerga ketishi kerakligini biladi. Shaxsiy kompyuterlarning ichki manzillari har xil.

NAT ning qanday afzalliklari bor ?

Quyida NAT ning ba'zi afzalliklari keltirilgan:

- Manzilni saqlash: NAT qonuniy ro'yxatdan o'tgan IP manzillarini saqlab qoladi va ularning tugashini oldini oladi.
- Tarmoq manzilini tarjima qilish xavfsizligi: Umumiy tarmoqdan qurilma IP-manzilini maskalash orqali NAT foydalanuvchilarga hatto trafikni uzatish va qabul qilishda ham internetdan kattaroq xavfsizlik va maxfiylik bilan foydalanish imkonini beradi. Foydalanuvchilar NAT tezligini cheklashdan marshrutizatordagi NAT operatsiyalari sonini hamda NAT tarjimalari sonini cheklash uchun foydalanishlari mumkin. Bu nafaqat NAT manzillaridan qanday foydalanishni nazorat qilish imkonini beradi, balki qurtlarni , viruslarni va xizmat ko'rsatishni rad etish (DoS) hujumlaridan qochishga yordam beradi. Dinamik NAT dan foydalanish avtomatik ravishda ichki tarmoq va internet o'rtasida xavfsizlik devori yaratadi. Trafik jurnali va filtrlash ba'zi NAT routerlarida mavjud.
- Moslashuvchanlik: NAT moslashuvchan; u, masalan, umumiy simsiz LAN sozlamalarida ishlatilishi mumkin. Ba'zi hollarda kiruvchi xaritalash yoki statik NAT tashqi qurilmalarga stub domenidagi kompyuterlarga ulanish imkonini beradi.

- Oddiylik: Tarmoq o'zgarganda yoki birlashganda manzillarni qayta raqamlashning hojati yo'q. Tarmoq manzillarini tarjima qilishdan foydalanib, ichki tarmoq serverlari uchun TCP yuk balansini muvofiqlashtirish uchun ichki tarmoq virtual xostini qurishingiz mumkin.
- Tezlik: NAT proksi-serverlardan farqli o'laroq, maqsad va manba kompyuterlar uchun shaffof bo'lib, tezroq to'g'ridan-to'g'ri aloqa qilish imkonini beradi. Bundan tashqari, proksi-serverlar ko'pincha OSI Reference Modelining transport darajasida yoki undan yuqoriroqda ishlaydi , bu ularni tarmoq sathida yoki 3-qatlamda ishlaydigan tarmoq manzillarini tarjima qilishdan sekinroq qiladi.
- Masshtablilik: DHCP server kerak bo'lganda ro'yxatdan o'tmagan IP manzillarini stub domeni uchun tarqatadi va NAT va dinamik xost konfiguratsiya protokoli (DHCP) birgalikda samarali ishlaydi. Masshtabni kengaytirish osonroq, chunki DHCP sozlagan IP-manzillarning mavjud diapazonini kengaytirishingiz mumkin, chunki sizning talablaringiz oshib borishi bilan IANA-dan ko‘proq IP-manzillarni so‘rash o‘rniga darhol ko‘proq tarmoq kompyuterlari uchun joy yaratishingiz mumkin.
- Multi-homing: Multi-homing yoki ko'plab internet ulanishlariga ega bo'lish ishonchli ulanishni saqlashga yordam beradi va aloqa uzilib qolganda o'chirish ehtimolini kamaytiradi. Bu, shuningdek, bitta ulanishdan foydalanadigan mashinalar sonini cheklash orqali yukni muvozanatlash imkonini beradi. Ko'p xonadonli tarmoqlar tez-tez ko'plab Internet-provayderlarga ulanadi, ularning har biri tashkilotga bir qator IP-manzillar yoki bitta IP-manzilni tayinlaydi. Turli xil tarmoq manzillarini tarjima qilish protokollaridan foydalanadigan tarmoqlar o'rtasida marshrut qilish uchun marshrutizatorlar tarmoq manzillarini tarjima qilishdan foydalanadilar. Ko'p uyli tarmoqdagi marshrutizator TCP/IP protokollar to'plamining bir qismi bo'lgan chegara shlyuzi protokoli (BGP) yordamida aloqa qiladi; stub domeni tomoni ichki BGP yoki IBGP dan foydalanadi va marshrutizatorlar tashqi BGP yoki EBGP yordamida bir-biriga ulanadi. Agar ISPga ulanishlardan biri muvaffaqiyatsiz bo'lsa, multi-homing barcha trafikni boshqa routerga yo'naltiradi.

NAT ning kamchiliklari

NAT dan foydalanishning ba'zi kamchiliklari mavjud:

- Ba'zi real vaqt ilovalari tarmoq manzili tarjimasi ta'minlamaydigan haqiqiy uchdan oxirigacha aloqani talab qiladi: Turli xil real vaqtda ilovalar real vaqtda ma'lumotlar paketlarini almashish uchun mantiqiy tunnel yaratishni talab qiladi. Bu proksi-server kabi oraliq vositalardan foydalanmasdan tez va uzluksiz ulanishni talab qiladi, bu esa aloqa jarayonini murakkablashtirishi va sekinlashtirishi mumkin.
- NAT tunnel protokollarining ishlashini murakkablashtiradi: Proksi-server orqali o'tadigan har qanday aloqa sust va uzilishlarga moyil bo'lishi mumkin. Ba'zi muhim ilovalarda bunday kamchiliklarga yo'l qo'yilmaydi. Telemeditsina va telekonferentsiya ikkita misoldir. Bunday ilovalar tarmoq manzillarini tarjima qilishni aloqa tarmog'idagi to'siq sifatida ko'radi, bu esa oldini olish mumkin bo'lgan uchdan-end ulanish buzilishlariga olib keladi.

- NAT Internet orqali internet aloqasi uchun zaxira marshrut bo'lib xizmat qiladi: IPv4 manzil maydonining etishmasligi va xavfsizlik muammolari tarmoq manzillarini tarjima qilish jarayonining keng tarqalgan jozibasi va keyinchalik amalga oshirilishi ortidagi harakatlantiruvchi kuchlar edi. IPv6 protokoli ushbu ikkala qiyinchiliklarni to'liq hal qildi. IPv6 asta-sekin IPv4 o'rnini bosganligi sababli, tarmoq manzilini tarjima qilish protsedurasi keraksiz va eskirgan bo'lib, IPv6 tarmoqlarida endi kerak bo'lmaydigan xizmatlar uchun qimmatli tarmoq resurslarini isrof qiladi.

NAT ga misollar

NAT tarmoq manzilini tarjima qilish misoli sifatida, ichki xost tashqi dunyoda maqsadli tarmoq manzilini tarjima qilish veb-server manzili bilan o'zaro aloqada bo'lishni xohlashi mumkin. Keyingi aloqa uchun NAT shlyuz routeriga ma'lumotlar to'plami yuboriladi.

Paket tarjimaga yaroqliligini baholash uchun NAT shlyuzi routeri paketning manba IP-manzilini bilib oladi va uni jadvalda qidiradi. U kirishni boshqarish ro'yxatida (ACL) ichki tarmoq tarjimasi uchun autentifikatsiya qilingan xostlarni topishi va keyin ichki mahalliy IP manzilidan ichki global IP-manzilni ishlab chiqarish orqali tarjimani yakunlashi mumkin.

Nihoyat, tarjimani NAT jadvaliga saqlagandan so'ng, NAT shlyuzi routeri paketni o'z manziliga yo'naltiradi. Internetning veb-serveri so'rovga javob berganida, paket routerning global IP manziliga qaytadi. NAT jadvali yordamida marshrutizator qaysi tarjima qilingan IP-manzil qaysi global manzilga mos kelishini aniqlay oladi, uni ichki mahalliy manzilga o'zgartiradi va ma'lumotlar paketini shu manzildagi xostga uzatadi. Hech qanday moslik aniqlanmasa, ma'lumotlar paketi o'chiriladi.

NAT asboblari va dasturlari nima ?

Xavfsizlik devori yoki marshrutizatordan foydalanish mumkin, odatda bular NATni amalga oshirish uchun umumiy foydalanishga mo'ljallangan qurilmalardir. NAT amalga oshirilgandan so'ng, NAT yozuvlarini qanday qidirishingiz mumkin. Ushbu sarlavha ostida biz NAT qidirish vositalarini ko'rib chiqamiz.

Filtrlash, toifalarga ajratish va chiqishni soddalashtirishning turli usullarini taqdim etish orqali NAT qidiruv vositasi ma'murlarga muammolarni bartaraf etish va NAT yozuvlarini saqlashda yordam beradi (ko'pincha qurilmaga ulanmasdan).

7 ta eng yaxshi NAT qidirish vositalari va dasturlari quyidagilar:

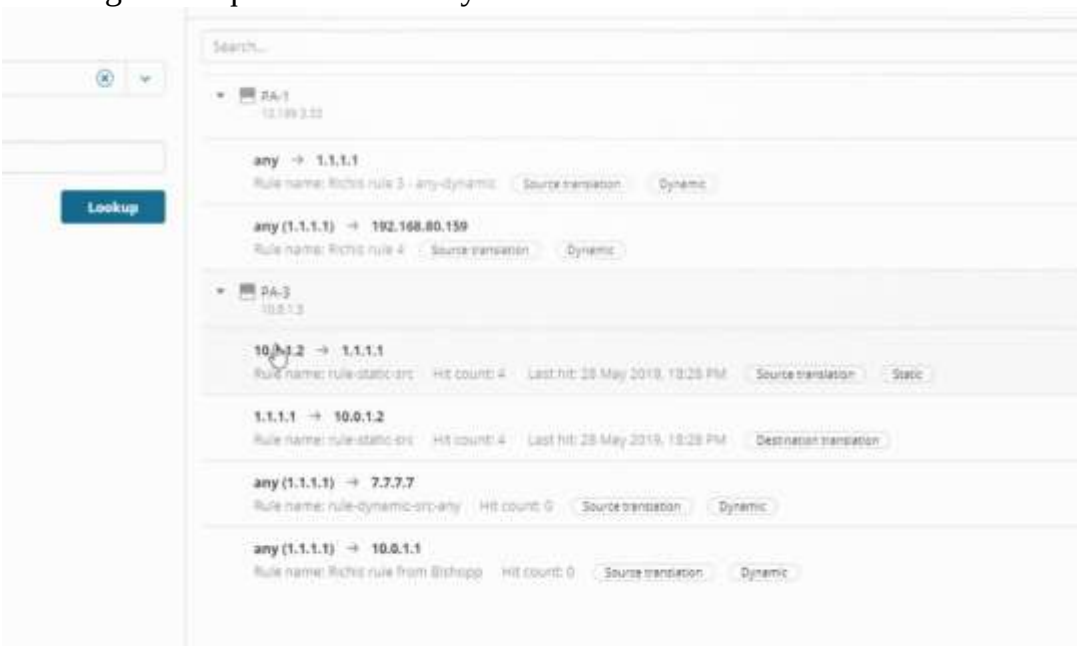
1. SolarWinds NAT qidirish vositasi
2. Netstat-nat
3. Cisco'ning IOS "ip nat tarjimasini ko'rsatish"
4. FortiGate xavfsizlik devorlari uchun FortiView
5. OpenBSD PF uchun pfctl
6. pfSense dasturi WebGUI
7. Juniper's J-Web

1. SolarWinds NAT qidirish vositasi

Har qanday IP-manzil uchun dastur NAT siyosatlari va ular bilan bog'liq xavfsizlik devorlari ro'yxatini qaytaradi.

Dasturiy ta'minot juda kengaytirilishi mumkin va u ma'murlarga keng qamrovli NAT siyosat ro'yxatlarini yaratishda yordam berishi mumkin.

Ushbu ro'yxatlar IP-manzil ziddiyatlarini, NAT siyosatlari yoki qoidalarining bir-biriga mos kelishini, xavfsizlik devori tarjimasining umumiy muammolarini va har qanday o'lchamdagi tarmoqlarni tuzatishda yordam beradi.



Shakl 2. Solarwinds NAT qidirish vositasi

2. Netstat- nat

Netstat-nat - bu tarmoq trafigini kuzatuvchi kichik C ilovasi. U Linux yadrolari > 2.4.x tarkibiga kiritilgan netfilter/iptables tomonidan boshqariladigan NAT ulanishlarini ko'rsatadi. Ilova o'z ma'lumotlarini netfilterning vaqtinchalik konntrack-xotirasidan, "/proc/net/ip conntrack" yoki "/proc/net/nf conntrack" dan oladi.netfilter.org

Linux dasturiy ta'minoti "netstat-nat" iptables yoki netfiltrlar tomonidan boshqariladigan barcha NATed ulanishlarini ko'rsatadi . Siz netstat-nat dan foydalanishingiz mumkin;

- Faqat SNAT, DNAT yoki ikkala havola ko'rsatilishi mumkin.
- Barcha NAT ulanishlari ko'rsatiladi.
- Natijalarni protokol raqami bo'yicha filtrlang.
- Natijalarni manbaning IP manzili asosida filtrlang.
- Berilgan IP-manzil yoki xost nomidan ulanishlarni ko'rsatish.
- NAT ulanishlari tartiblangan bo'lishi kerak.

Debian, Ubuntu, Suse va Redhat kabi mashhur Linux distribyutorlari yordam dasturini qo'llab-quvvatlaydi. Netstat-nat bir nechta argumentlarni oladi (lekin kerak emas).

Parametrlar	Ta'riflar
-h	yordamni ko'rsatadi
-n	IP/portlarni xost/port nomlariga ajratmang.
-p 'protocol'	protokol tanlash bilan NAT ulanishlarini ko'rsatish.

Parametrlar	Ta'riflar
-s 'source host'	manba IP/xost nomi bo'yicha ulanishlarni ko'rsatish.
-d 'destination host'	ulanishlarni maqsad IP/xost nomi bo'yicha ko'rsatish
-S	SNAT ulanishlarini ko'rsatish
-D	DNAT ulanishlarini ko'rsatish
-L	faqat NAT qutisiga ulanishlarni ko'rsatish (SNAT va DNAT ko'rsatishni o'chiradi)
-R	faqat NAT qutisi orqali yo'naltirilgan ulanishlarni ko'rsatish (SNAT va DNAT ko'rsatilmaydi)
-x 'source host'	DNAT ulanishlarini ko'rsatish
-o	chiziqli chiqish sarlavhasi
-N	NATing iface uchun NAT qutisiga ulanish ma'lumotlarini (IP va port) ko'rsatish (faqat SNAT va DNAT bilan amal qiladi)
-v	versiya
-r	ulanishlarni tartiblash

3. Cisco’ning IOS “ip nat tarjimasini ko‘rsatish ”

Agar NAT muhitida IP-ulanish bilan bog'liq muammolar mavjud bo'lsa, muammoga nima sabab bo'lganini aniqlash qiyin bo'lishi mumkin. NAT ko'pincha, aslida, asosiy muammo bo'lganida ayblanadi. Cisco muhitida quyidagi buyruq yordamida muammoni osongina bartaraf etishingiz mumkin.

```
show ip nat translation
```

First, determine that NAT is working correctly. You know from the configuration that the Router 4 IP address (10.10.10.4) is supposed to be statically translated to 172.16.6.14. You can use the **show ip nat translation** command on Router 6 to verify that the translation does exist in the translation table:

```
router-6# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.6.14        10.10.10.4         ---                ---
```

3-rasm. Cisco routerda ip nat tarjima buyrug'ini ko'rsating

4. FortiGate xavfsizlik devorlari

FortiGate xavfsizlik devorlari uchun asosiy ro'yxatga olish vositasi FortiView hisoblanadi. U bir nechta asboblar panelidagi (ilovalar, Wi-Fi, veb-saytlar va boshqalar) joriy va tarixiy jurnallarni ko'rsatadi.

FortiView - bu real vaqt rejimi va tarixiy ma'lumotlarni yagona ko'rinishda birlashtirgan yagona tarmoq monitoringi tizimi. U tarmoq tahdidlarini qayd etishi va kuzatishi,

ma’lumotlarni bir necha darajadagi filtrlashi va boshqa narsalar qatori ma’muriy faoliyatni kuzatishi mumkin.

Konsollarda FortiView foydalanuvchi identifikatori yoki mahalliy IP manzili, ilova va boshqa variantlar bo'yicha ma'lum vaqtga ko'rinishni toraytirish uchun bir nechta filtrlardan foydalanish imkonini beradi. Tarmoq miqyosidagi foydalanuvchilar guruhida yoki individual foydalanuvchilar darajasida siz undan foydalanuvchi yuklash/yuklab olish yoki tomosha qilingan YouTube videolari kabi trafik faolligini tekshirish uchun foydalanishingiz mumkin. U ma'lumotlarning matnli va vizual tasvirini beradi.

Agar siz aniq NAT manzilini qidirsangiz, jurnallarni qidirishingiz va filtrlashingiz mumkin.

5. OpenBSD PF

Paketlarni filtrlashni boshqarish pfctl buyrug'i bilan ifodalanadi. Bu paketli filtr qurilmasi bilan aloqa o'rnatadigan dastur va u faqat OpenBSD PF uchun.

pfctl buyrug'i paketlarni filtrlash (yoki xavfsizlik devori) qurilmasining konfiguratsiyasi va qoidalarini o'zgartirishi, shuningdek, holat ma'lumotlarini olishi mumkin.

Bu juda ishonchli va ko'p sonli buyruqlarni taklif qiladi.

Pfctl yordam dasturi bilan joriy faol NAT tarjimalarini ko'rish uchun buyruqqa (-s state) opsiyasini qo'shing.

Quyidagi buyruq barcha faol NAT seanslari ro'yxatini ko'rsatadi.

```
pfctl -s state
```

6. pfSense® WebGUI

Siz pfSense® WebGUI dasturiy ta'minotida barcha xavfsizlik devori va NAT holatlari ro'yxatini ko'rishingiz mumkin , unga quyidagilar kiradi:

- Davlat interfeysda bog'langan.
- Protokol: bu holat yuzaga kelishiga sabab bo'lgan protsedura.
- Kelib chiqishi va yakuniy manzili. NATtingdan oldin va keyin, IP manzili. Yo'nalish o'q bilan ko'rsatiladi (chiqishga kiruvchi yoki aksincha).
- Shtat: Shtatning ulanish holati. Bular protokolga qarab farqlanadi.
- Paketlar: holatga mos keladigan manbadan manzilgacha bo'lgan paketlar soni.
- Baytlar: boshidan oxirigacha paketdagi baytlarning umumiy soni.

Sessiya ro‘yxati siz qidirayotgan narsani topish uchun juda katta bo‘lsa, holat filtrlari yordam berishi mumkin. Bu filtrlar muayyan qidiruv parametrlari asosida tezkor qidiruvni amalga oshirishda yordam beradi.

7. Juniper's J- Web

Juniper's SRX Series Services Gateways uchun veb-foydalanuvchi interfeysi J-Web deb ataladi.

Ushbu yordamchi dastur yordamida xavfsizlik devorini kuzatish, sozlash va muammolarni bartaraf etish uchun HTTPS dan foydalanishingiz mumkin. J-Web GUI JunOS CLI ga bo'lgan ehtiyojni yo'q qiladi.Siz J-Web interfeysining NAT seanslari va

qoidalar maydoni ostida NAT ni sozlashingiz mumkin .Shuningdek, u barcha joriy NAT tarjimalari hamda ularni boshqaradigan siyosatlarni ko'rsatadi.

Haqiqiy vaqtda ma'lumotni o'rganayotganda siz filtrlarni (yoki tarixiy) ham qurishingiz mumkin.

Tarmoq manzillarini tarjima qilish jadvali nima ?

Mahalliy tarmoqda (LAN) barcha xostlar bir xil umumiy IP-manzilni qanday ulashadi? Tarmoq manzili tarjimasi (NAT) IP manzillari va port raqamlarini qayta tayinlaydi va ushbu qayta tayinlanishlarni kuzatib borish uchun NAT tarjima jadvalidan foydalanadi.

Router mahalliy xostdan umumiy IP-manzilli paketni olganida, u manba IP-manzilini Internet IP-manziliga o'zgartiradi va manba port raqamini o'zgartiradi, shuning uchun paketlarni qaysi localhost jarayoniga etkazib berishni biladi. Tarjima jadvali ushbu qayta topshiriq bilan yangilanadi.

NAT mahalliy tarmoqdagi Internetga ulanishni talab qiladigan har qanday jarayonga yangi IP-manzil va port raqamini tayinlaydi. Tarmoq manzilini tarjima qilish jadvali har bir qayta tayinlash bilan yangilanadi.

FOYDALANILGAN ADABIYOTLAR:

1. **Cisco Systems.** (2023). *Cisco NAT Configuration Guide*. Cisco. https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/rpcfg/64x/b-bgp/b-bgp-64x-book/b-bgp-64x/chapter-13.pdf
2. **Elam, M. & Duong, T.** (2022). *Network Address Translation (NAT) and Its Importance in Network Security*. Wiley Network Security.
3. **Liu, W.** (2021). *Configuring NAT on Cisco Routers for Security and Performance*. Network World, 39(6), 45-52.
4. **Forouzan, B. A.** (2022). *Data Communications and Networking*. 5th edition. McGraw-Hill.
5. **Palmer, D.** (2023). *Introduction to NAT and PAT on Cisco Routers*. TechNet, 34(1), 77-84.
6. **U.S. Department of State.** (2023). *Cybercrime Prevention and Detection: A Practical Guide*. State.gov. (Available at: State.gov)

Foydalanilgan internet sahifalari:

1. Cisco Systems. "What is NAT?" Rasmiy sayt: https://www.cisco.com
2. NetworkLessons. "Cisco NAT Configuration Guide." Manba: https://networklessons.com
3. PacketLife.net. "NAT Explained." Hujjatlashgan qo‘llanma: https://packetlife.net
4. TechTarget. "Network Address Translation (NAT): An Overview." Maqola: https://www.techtarget.com
5. HowToNetwork. "Configuring NAT on Cisco Routers: A Step-by-Step Guide." Manba: https://howtonetwork.com