TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI VA UNING FILIALLARI O‘RTASIDA VPN(VERTUAL PRIVATE NETWORK)NI TARMOQ DARAJASIDA KO’TARISH

Radjabova Madina Shavkatovna
Toshkent axborot texnologiyalari unversitetining “Kiberxavfsizlik va kriminalistika ” kafedrasi o’qituvchi-stajyor
Abdullayev Ibrohim Ko‘palboy o‘g‘li
Mirzanazarov Mehridil Shamsiddin o’g’li kiberxavfsizlik fakulteti 2-kurs 730-21 guruh talabalari

Anatatsiya: *Maqola hozirgi globallashuv hamda fan, texnika va texnologiyalarni tezkor rivojlanishi davrida konfidensial va shaxsiy ma‘lumotlarni ishonchli saqlash, tashkilot, korxona va banklarda turli xavflarni oldini olishni cisco qurilmalari yordamida amaliy tarzda ta‘minlashni ko‘rib chiqamiz.*

Анатация: *В статье в эпоху современной глобализации и бурного развития науки, техники и техники мы рассмотрим практический способ обеспечения надежного хранения конфиденциальных и персональных данных, предотвращения различных рисков в организациях, предприятиях и банках с помощью устройств cisco.*

Anatation: *The article provides concrete examples of the importance of using mathematical apparatus to obtain precise and rapid solutions in the current era of globalization and the rapid development of science, engineering and technology, and the application of complex number theory in mathematics to electrical engineering.*

Ushbu maqola hozirgi globallashuv, fan, texnika va texnologiyalarni tezkor rivojlanishi davrida konfidensial va shaxsiy ma‘lumotlarni ishonchli saqlash, tashkilot, korxona va banklarda turli xavflarni oldini olishni cisco qurilmalari yordamida amaliy tarzda ta’minlashda katta ahamiyat kasb etadi. Ayniqsa hozirgi raqamli xujumlar ko‘payayotgan bir vaqtda unga qarshi ko‘plab ximoya vositalarini qo‘llash maqsadga muvofiqdir. Ushbu maqolada VPN (Vertual private network – shaxsiy ximoyalangan tarmoq)ni site-to-site VPN turini tarmoq tarjasida routerda ko‘taramiz.

Site-to-site texnoligiyasi tarmoqlar o‘rtasida VPN kanal ko’tarish uchun ishlatiladi. Ya’ni markaz-filial o‘rtasida ishonchli aloqani taminlashdir. Site-to-site VPN tunneli trafikni bir uchida shifrlaydi va uni umumiy Internet orqali boshqa saytga yuboradi, u yerda shifrlangan va belgilangan manzilga yo‘naltiriladi. Site-to-site VPN-lar ko‘plab tashkilotlar tomonidan qo‘llaniladi. Buning sababi shundaki, ular korxonalar va ularning xodimlariga bir qator imtiyozlar beradi. Tashkilotlar odatda LAN ichidagi qurilmalar uchun ichki IP-manzil diapazonlaridan

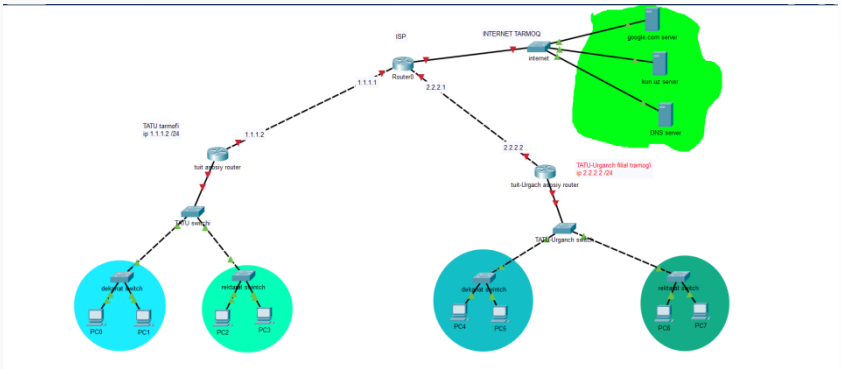
foydalanadilar. Ushbu manzillar umumiy Internetdan kirish uchun tashqi IP manzillarga aylantirilishi kerak.

Site-to-site VPN-lar bilan bir LANdan ikkinchisiga trafik “ichki” bo'lib qoladi, ya'ni barcha saytlar bir-birining resurslari uchun ichki manzillardan foydalanishi mumkin bo‘ladi. Yana bir afzalligi shundaki masofaviy foydalanuvchilarga tarmoqqa xavfsiz kirishni ta'minlaydi. Site-to-site texnologiyasi l2l deb ham ataladi.

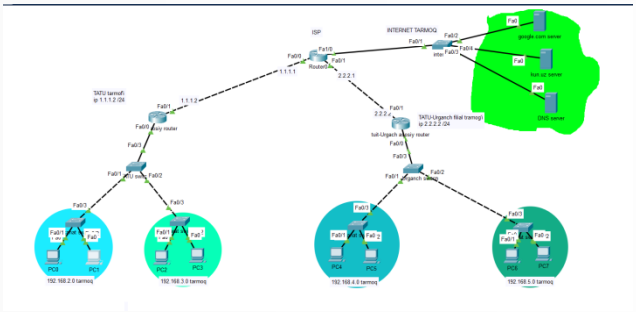
Site-to-site texnologiyasini ikkita fazada bo‘lgan xolda quramiz. Birinchi fazada VPN qaysi siyosatlar asosida ishlaydi, qanday shifrlash (encryption), qanday hash funsiya,authentificatsiya (dfhelmn), ikki tomon bir birini tanib olish va kalitlarni almashinishi uchun dastlabki key (kalit) beriladi, berilgan kalitlarning amal qilish muddatlari (lifetime) beriladi. Qisqacha aytganimizda biz bilgan ruchkani qobiqini ya’ni VPN ning tunnelini birinchi bosqichda qurib olamiz. Ikkinchi bosqichda asosiy protocol ipsec – VPN tunnel ichidagi pasta yoritiladi. Encryption, hash, ACL kimlar uchun huquq berishni belgilaymiz va VPN dan foydalanishini, crypto carta yaratiladi portlarga biriktiladi.

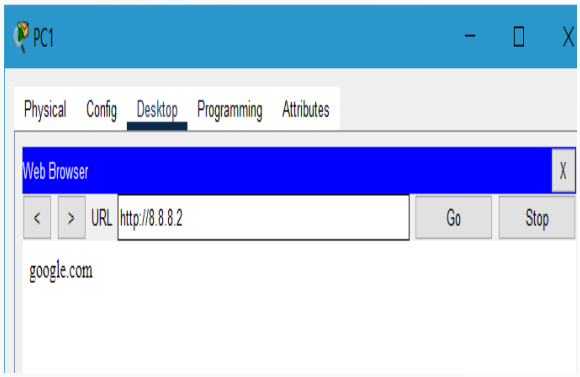
Endi amaliy qismga o‘tsak. Hozir VPN tarmoq orqali TATU univarsitatini uning Urganchdagi filiali bilan ulaymiz. Bunda markazdan turib filiallardagi local tarmoqni nazorat qilishimiz, konfidensial malumotlarni ishonchli yuborishimiz mumkin bo‘ladi.

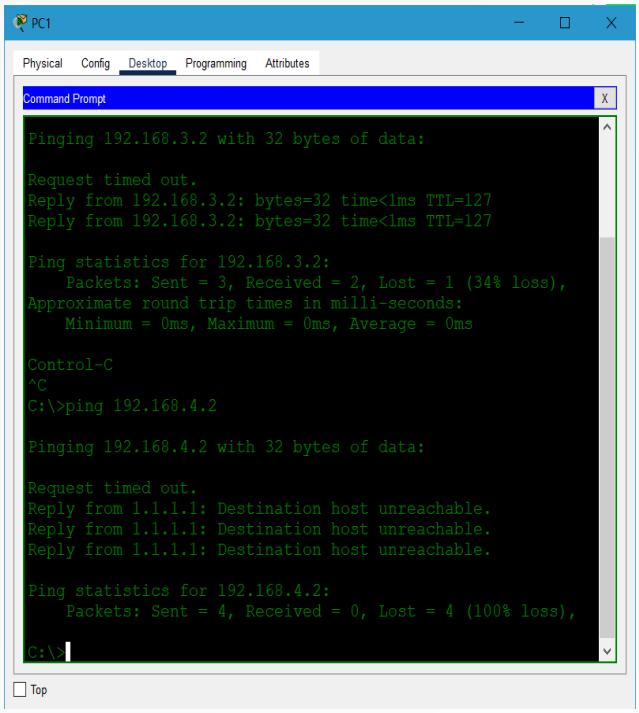
1. VPN tarmoqni routerda quramiz.



Tarmoqni kichikroq topologiya asosida chizdim. Hozirgi vazifamiz TATU dekanat va TATU-Urganch filialdagi dekanat oragidagi aloqani tiklashdan iborat.







Tarmoq to‘liq qurildi. Hamma komyuterlar internetga chiqyapti. Lekin filial bilan aloqa yo‘q.

Chunki local ip global tarmoqda mashurutini ta’minlanmaydi.

TATUning asosiy routeridan kod yozamiz.

1.1 crypto isakmp policy 1 - IPsec xavfsizligini qanday tuzish haqida kelishib oluvchi isakmp protocolining siyosati. Texnologik tunnel yaratyapmiz.

1.1.1Encryption aes – aes shifrlash algoritmi yordamida shifrlanadi.

1.1.2 Hash sha – Sha hesh funksiyadan foydalanadi.

1.1.3 Authentication pre-share – malumot almashinishda SSL sertifikatidan foydalanish

1.1.4 Group 2 – Diffie-Hellman ni 2-versiyasidan foydalaniladi.

1.1.5 Lifetime 86400 – tunneling ishlab berish vaqti (s).

1.2 crypto isakmp key kalit address 2.2.2.2 – kalitlar tanlanadi, yani shifrlaydigan va shifrni yechadidan kalitlar. Va peer address – narigi tomon internetga chiqadigan ip addressi yoziladi.

Mana shu yerda 1-faza tugaydi. Endi 2-fazani ko‘ramiz.

2.1 crypto ipsec transform-set TS esp-aes esp-sha-hmac – shifrlash algoritmi va hesh funsiya pastaga biriktirilyapti

2.2 ip access-list extended for-vpn – VPN uchun kengaytirilgan access list tuzamiz.

2.2.1 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 TATU dekanat aloqasi TATU-Urganch filial dekanati bilan aloqa qilishini aytamiz.

2.3 Crypto map karta 10 ipsec-isakmp – endi kriptokarta tuzib olamiz

2.3.1 match address for-vpn – biz tuzgan access-listni kriptokartaga biriktiryapmiz.

2.3.2 Set peer 2.2.2.2 – peer address ham biriktiriladi.

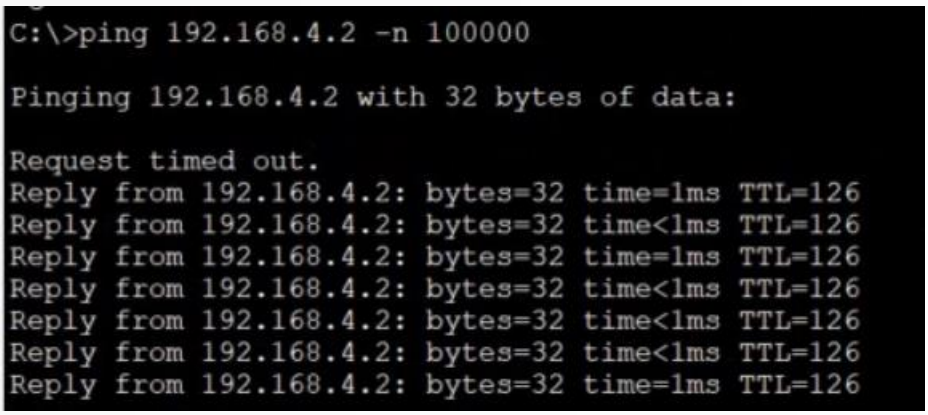
2.3.3 set transform-set TS

2.3.4 set security-association lifetime seconds 86400 – vpn ishlash vaqti.

2.4 interface fastEthernet 0/1 – internetga qaragan portga kiramiz.

2.4.1 crypto map karta – unga kriptokartani biriktiramiz.

Ikkinchi TATU-Urganch asosiy routerida ham huddi shu narsa yoziladi. Bitta farqi access-list tuzayotganda ip diapazonlar o‘zgartiriladi.



Va mana ko’rishimiz mumkin 192.168.2.0 tarmoqdan 192.168.4.0 tarmoq aloqaga kirishyapdi.

FOYDALANILGAN ADABIYOTLAR:

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov Kiberxavfsizlik asoslari. O‘quv qo‘llanma. – T.: <<Iqtisod Moliya>>, - 2021.

2. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. – T.: <<Aloqachi>>, - 2008.

3. Candace Leiden, Marshall Wilensky “TCP/IP For Dummies” – 2009.

4. “Internet Protocol Transition Workbook” – 1982.

5. Douglas Comer “The Internet Book: Everything You Need to Know about Computer…” – 2018.

6. Ko-yi Lu “Internet Protocol Version 6” – 2005.

7. Internet saytlari: https://www.books.google.com

8. https://www.bookauthority.org

9. https://www.cloudflare.com