CISCO PACKET TRACER SIMULYATORIDA IOT ASOSIDAGI AQLLI TIZIMNING XAVFSIZLIGINI IPSEC ORQALI TA'MINLASH

Jumaboyev T.A,

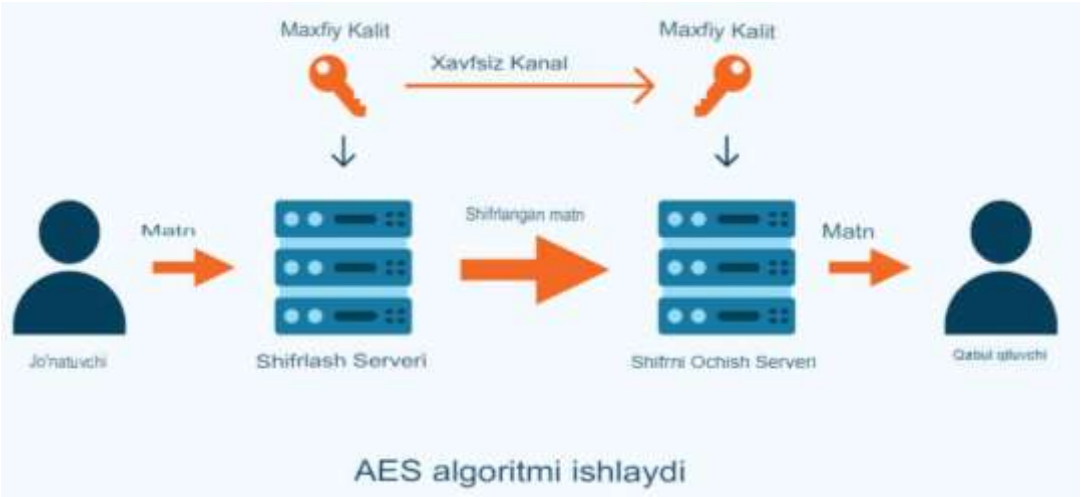
Nizamov A.N,

Djo'rayev.A.A.

Muhammad Al-Xorazmiy Nomidagi TATU Samarqand filiali o'qutuvchilar

AES (Advanced Encryption Standard) shifrlash algoritmi ko'plab tarmoq qurilmalarida va turli xil texnologiyalarda qo'llaniladi. Uning keng tarqalishi xavfsizlikni ta'minlaydigan ishonchli va samarali usul sifatida tan olinganligi bilan bog'liq. Quyida AES algoritmining qo'llanilishi haqida ba'zi misollar keltirilgan:

Xavfsizlik Kameralari va Boshqa Nazorat Tizimlari. Xavfsizlik Kameralari, ko'pincha bu kameralar yuborilayotgan video ma'lumotlarini shifrlash uchun AESdan foydalanadi, bu esa ma'lumotlarni noqonuniy kuzatuvdan himoya qiladi.

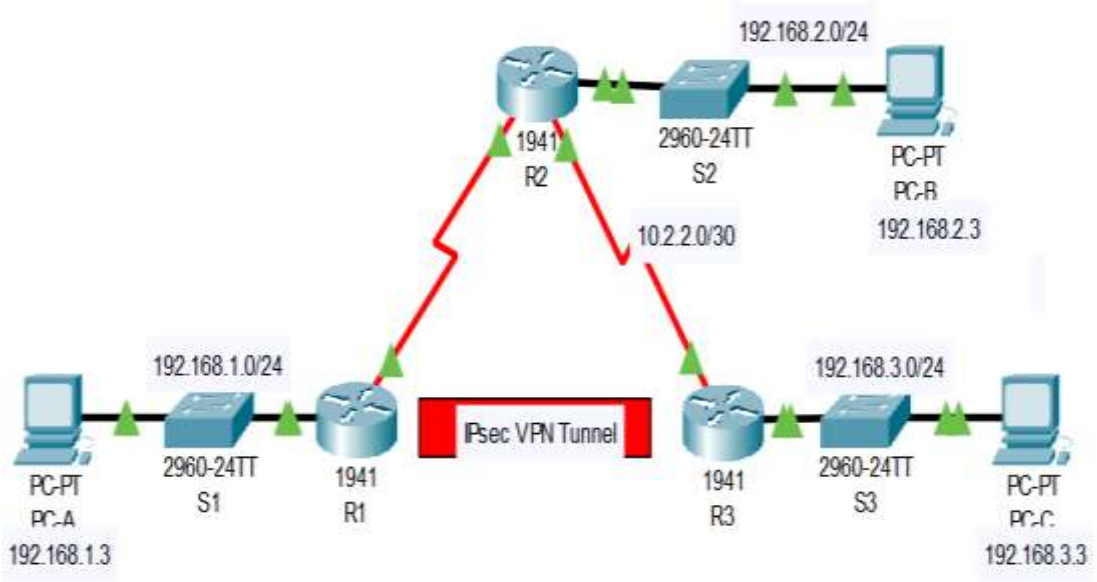


1-rasm. AES algoritmi yordamida tarmoq qurilmalari ishlashi

Ma'lumotlar Markazlari va Serverlar (Disk Shifrlash Tizimlari). AES, korporativ darajadagi disk shifrlash yechimlarida, masalan, Microsoft BitLocker va Apple FileVault kabi tizimlarda qo'llaniladi. Bu yechimlar ma'lumotlarni saqlash vositalarini to'liq disk shifrlash orqali himoya qiladi.

Smartfonlar va Planshetlar. iOS va Android kabi mobil operatsion tizimlar AESni ma'lumotlarni, jumladan, foydalanuvchi ma'lumotlari va ilovalar tomonidan yaratilgan ma'lumotlarni shifrlash uchun ishlatadi.

AESning keng qo'llanilishi uning yuqori xavfsizlik darajasidan va algoritmining turli xil amaliy qurilmalar va dasturlarga moslashuvchanligidan kelib chiqadi. Bu shifrlash algoritmi, xavfsizlik talablariga javob bera oladigan, ishonchli va sinovdan o'tgan usul sifatida tanilgan.



2-rasm. VPN IPsec tuneli asosidagi tarmoq topologiyasi

Packet Tracer - CLI yordamida Sayt-sayt IPsec VPN-ni sozlash va tekshirish

1-jadval

Manzillar jadvali

Qurilma	Interfays	IP Address	Tarmoq maskasi	Shlyuz	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Maqsadlar

• Tarmoqdagi ulanishni tekshirish.

• R1-ni R3 bilan o’zaro IPsec VPN-ni qo'llab-quvvatlash uchun sozlash.

Fon / Ssenariy

2-jadval

ISAKMP 1-bosqich siyosat parametrlari

Parameterlar		R1	R3
Kalit usuli	Qo’lda yoki ISAKMP	ISAKMP	ISAKMP
Shifrlash algoritmi	DES, 3DES, yoki AES	AES 256	AES 256
Hash algoritmi	MD5 yoki SHA-1	SHA-1	SHA-1
Autentifikatsiya usuli	Kalit asosida yoki RSA	oldindan bo'lishilgan	oldindan bo'lishilgan
Kalit almashinish	DH guruhi 1, 2, yoki 5	DH 5	DH 5
IKE SA kalit	86400 sekund	86400	86400
ISAKMP kalit		vpnpa55	vpnpa55

Eslatma: Qalin harflar bilan yozilgan parametrlar standartdir. Faqat qalin bo'lmagan parametrlar aniq sozlanishi kerak.

3-jadval

IPsec Phase 2 siyosat parametrlari

Parameterlar	R1	R3
Nomni o’rnatmoq	VPN-SET	VPN-SET
ESP Shifrlash	esp-aes	esp-aes
ESP Autentifikatsiya	esp-sha-hmac	esp-sha-hmac
Tugun IP manzili	10.2.2.2	10.1.1.2
Shifrlangan marshrut	access-list 110 (manba 192.168.1.0 manzil 192.168.3.0)	access-list 110 (manba 192.168.3.0 manzil 192.168.1.0)
Shifrlash xarita nomi	VPN-MAP	VPN-MAP
SA O’rnatish	ipsec-isakmp	ipsec-isakmp

1-qism: R1 da IPsec parametrlarini sozlash

Qadam 1: Tarmoqqa ulanishni tekshirish.

PC-A dan PC-C ga ping qilish.

Qadam 2: Xavfsizlik texnologiyasini yoqish.

a. R1 da show version buyrug‘ini bajarib, Xavfsizlik Texnologiyasi paketi litsenziya ma’lumotlarini ko‘rish.

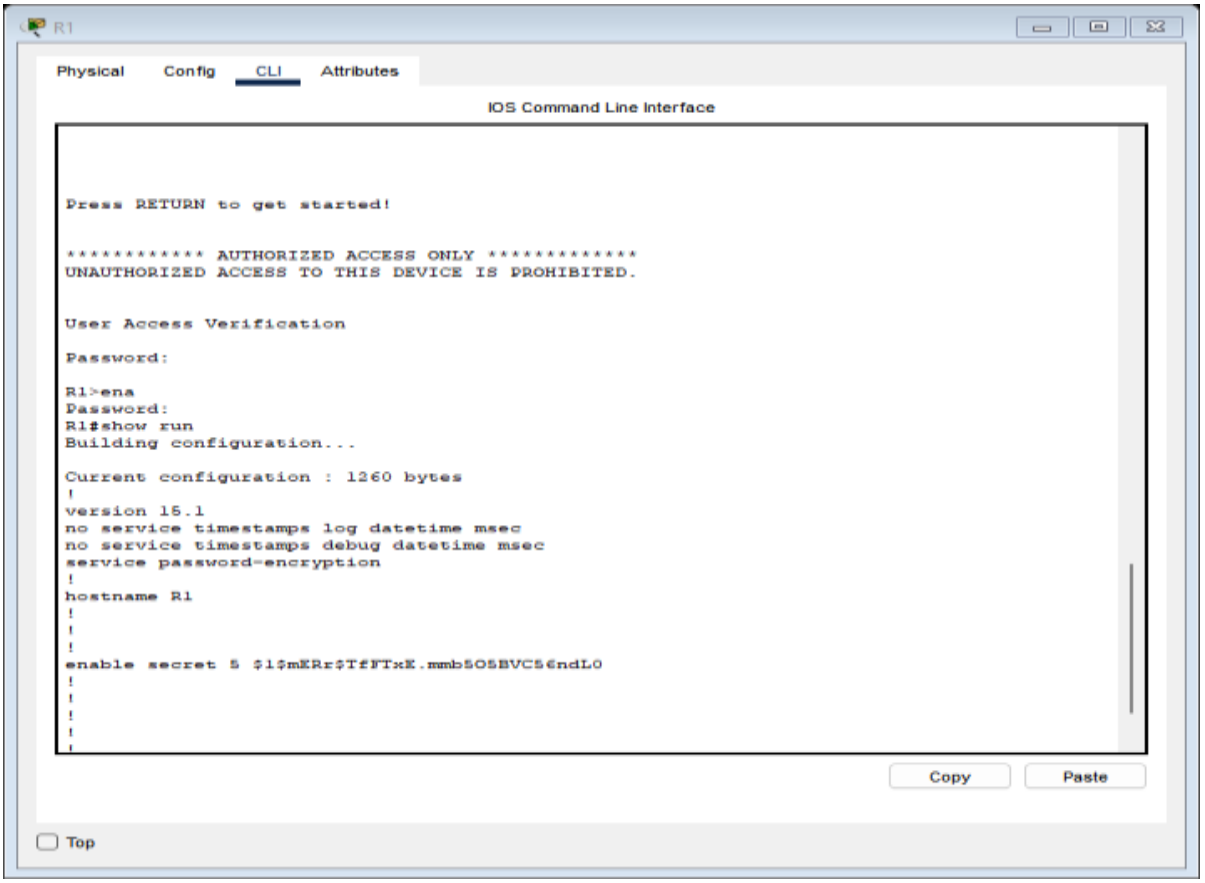
b. Agar Xavfsizlik Texnologiyasi paketi yoqilmagan bo‘lsa, quyidagi buyruqni bajarib paketni yoqing.

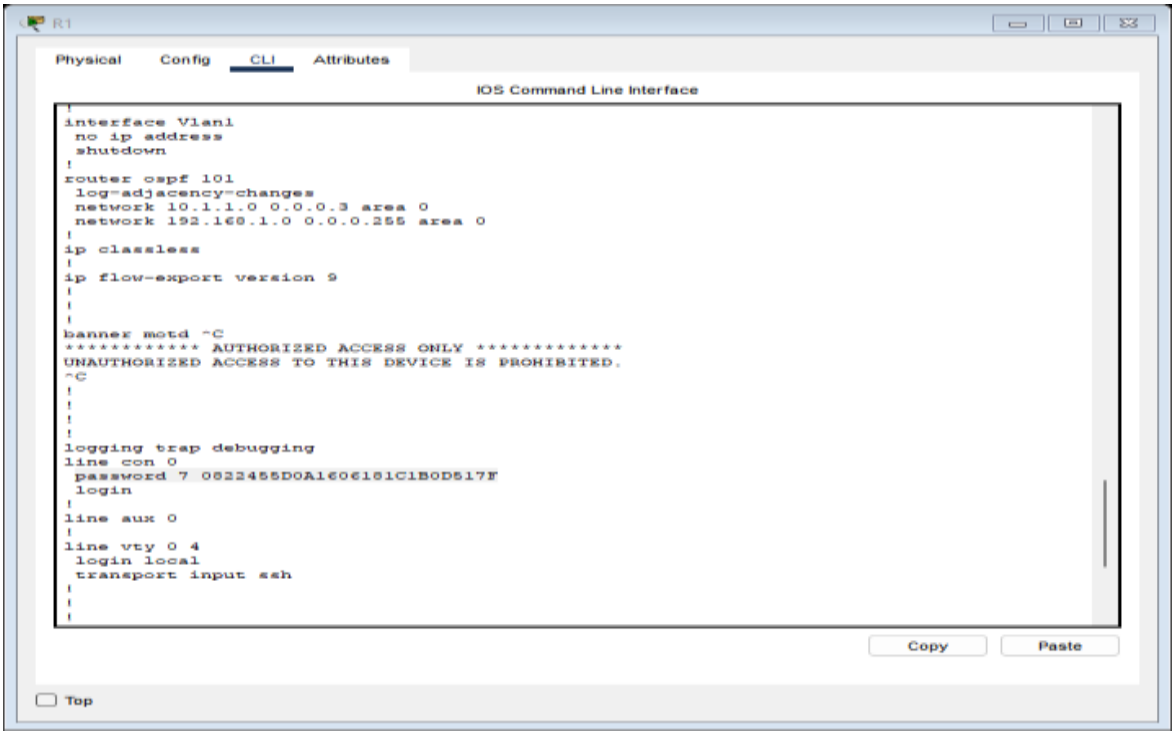
R1(config)# license boot module c1900 technology-package securityk9

c. Foydalanuvchi litsenziya kelishuvini qabul qiling.

d. Yurgizilayotgan konfiguratsiyani saqlang va marshrutizatorni qayta yuklang, shunda xavfsizlik litsenziyasi yoqiladi.

e. show version buyrug‘i yordamida Xavfsizlik Texnologiyasi paketining yoqilganligini tekshiring.





4-rasm. R1 router konfiguratsiyasi (Shifrlash yoqilgan)

1-qadam: Qiziqarli trafik bo'lmagan holda tunnelni tekshiring.

R1 da show crypto ipsec sa buyrug‘ini bajarib, qadoqlangan, shifrlangan, qadoqdan chiqarilgan va shifrdan ochilgan paketlar sonining hammasi 0 ekanligiga e'tibor bering.

2-qadam: Qiziqarli trafik yarating.

PC-A dan PC-C ga ping qiling.

3-qadam: Qiziqarli trafikdan keyin tunnelni tekshiring.

R1 da, show crypto ipsec sa buyrug‘ini qayta bajarib, paketlar sonining 0 dan ko'p ekanligiga e'tibor bering, bu IPsec VPN tunneli ishlayotganligini ko'rsatadi.

4-qadam: Qiziqarli bo'lmagan trafik yarating.

PC-A dan PC-B ga ping qiling. Diqqat: R1 marshrutizatoridan PC-C ga yoki R3 dan PC-A ga ping qilish qiziqarli trafik hisoblanmaydi.

5-qadam: Tunnelni tekshiring.

R1 da, show crypto ipsec sa buyrug‘ini qayta bajarib, paketlar sonining o'zgarmaganligiga e'tibor bering, bu qiziqarli bo'lmagan trafik shifrlanmaganligini tasdiqlaydi.

FOYDALANILGAN ADABIYOTLAR RO’YXATI

1. Rajiv Irungbam, The Model of Smart Cities in Theory and in Practice. Journal for Studies in Management and Planning, April 2016.

2. Dirks, S and Keeling, M. A Vision of Smarter Cities. IBM Institute for Business Value. 2009. URL: 03.

3. World development report: digital dividends. International Bank for Reconstruction and Development/The World Bank. 2016. URL: openknowledge.worldbank.org/bitstream/handle/10986/23347/9781464806711.pdf

4. N.B. Usmanova Ma’lumot uzatish tizimlari va tarmoqlari. O‘quv qo‘llanma. Toshkent TATU.2006 yil

5. Хелд Г. Технологии передачи данных. 7-е изд. -СПб Питер, К.: Изд. Группа BHV, 2003год