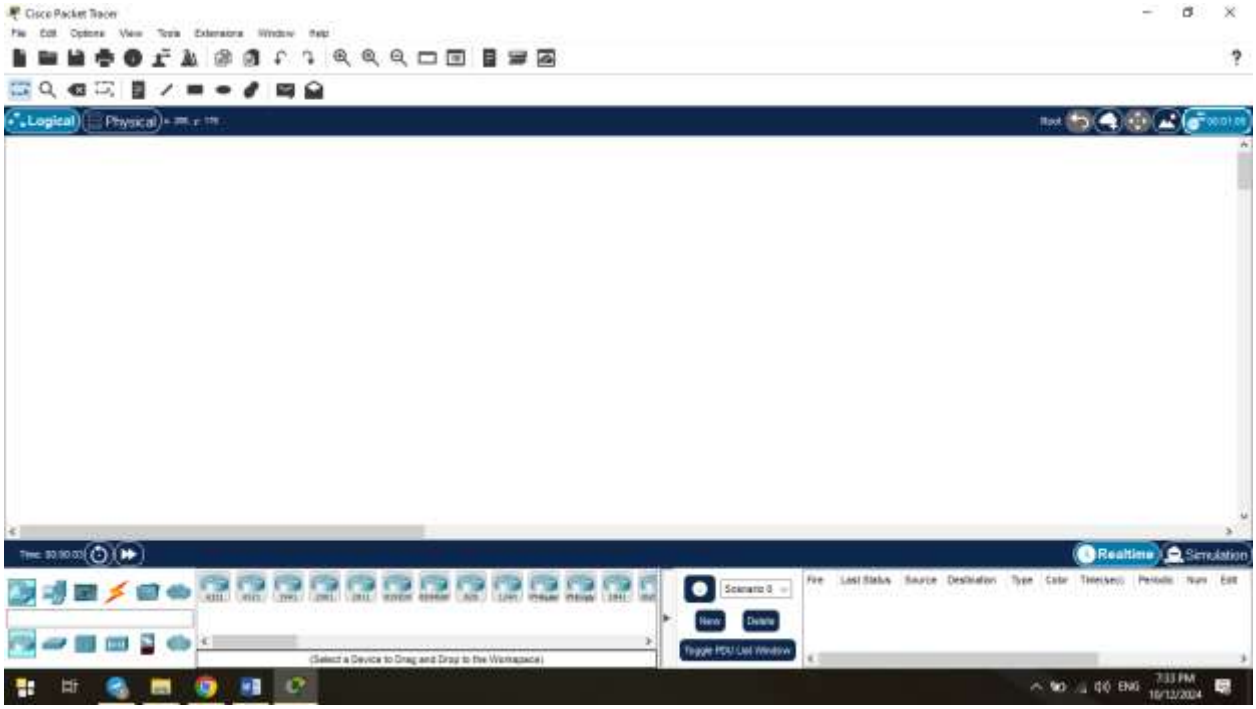
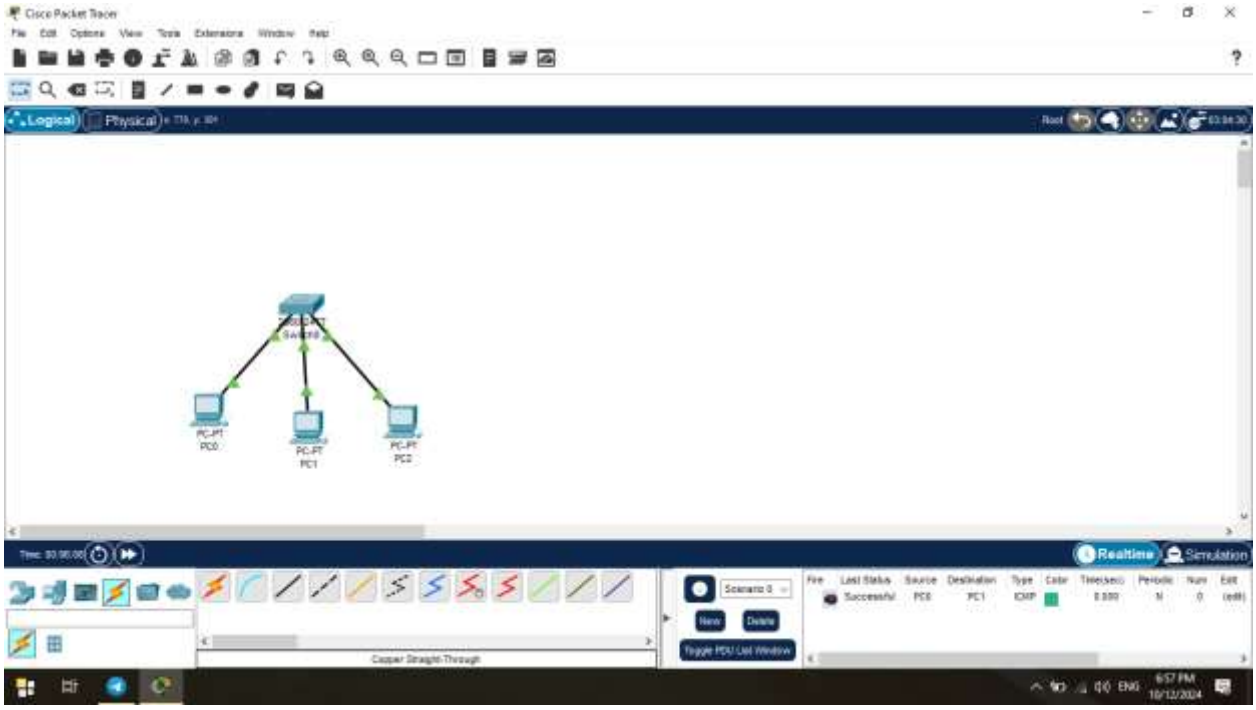
6-amaliy mashg'ulot.

Cisco Paket Trascer o'rnatish

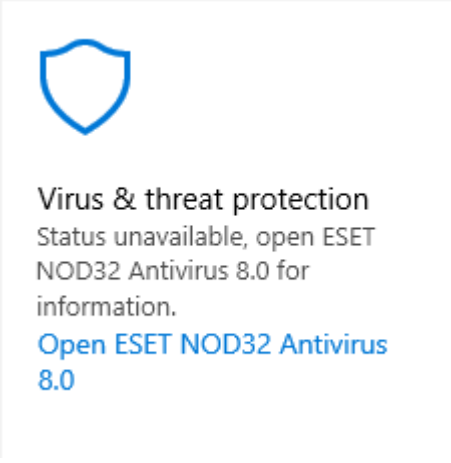




Tayyor.

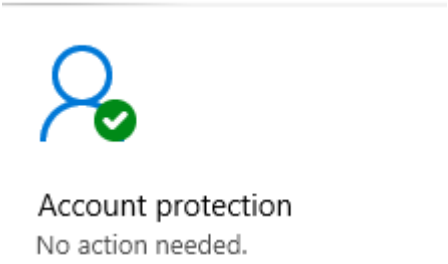
7-amaliy mashg'ulot.

Tarmoqlararo ekran vositasi yordamida tarmoq himoyasini qurish: Comodo firewall misolida



Virus threat protection - Virus kompyuter va boshqa jihozlarni tahdid dasturlari, viruslar, troyanlar, boshqa zararli kodlardan himoya qilish uchun texnologiya va ta'minot funksiyasidir. unga tegishli:

1. **Zararli dasturiy ta'minot : Qurilma ichida yoki internetdan kiruvchi zararli fayllarni tekshirib, aniqlaydi. Bu orqali zararli kodlar qurilmaga o'rnashib olishi oladi.**
2. **Real-time himoya qilish : Kompyuteringiz ishlayotganda yangi fayllarni va o'zgartirilgan fayllarni darhol tekshirib ko'ring**
3. **Fayllarni skanerlash : 4. Karantin qilish : 5. Onlayn shunday :**



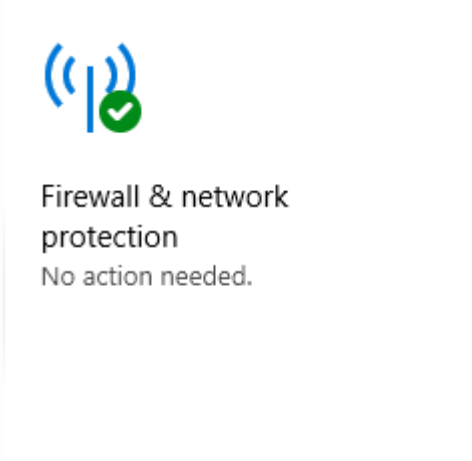
Account Protection – bu foydalanuvchi hisoblarini (masalan, elektron pochta, ijtimoiy tarmoqlar, bank hisoblari va boshqa onlayn foydalanish) turli yordam-xatarlardan himoya qilish usullarini o'z ichiga olgan qo'zg'atuvchi omillar majmuasidir. Bu foydalanuvchining shaxsiy ma'lumotlari va hisob ma'lumotlarini himoya qilish, ularni buzib kirish yoki ruxsatsiz kirishdan ko'rish uchun.

Hisobni himoya qilish bo'yicha tizim:

1. Kuchli parol : samaralilar oson topiladigan yoki mumkin bo'lgan parollardan emas, balki murakkab, uzun va raqam, harflar va maxsus belgilarni o'z ichiga olgan parollardan olib yurishi kerak.
2. Ikki faktorli a autentifikatsiya (2FA) : Hisobga kirishda parol bilan bir qatorda qo'shimcha yordam sifatida SMS, email orqali yuboriladigan kod yoki autentifikatsiya ilovasi orqali talab qilish. Buni ruxsatsiz kirishdan ishonchli hisob qiladi.
3. Kirish harakatlarini kuzatish : Ko'plab tizimlar foydalanuvchi hisoblariga kirish joyi, vaqti, va quvvatlangan qurilmalarni kuzatib boradi. Agar shubhali yoki noma'lum qurilma yoki joydan kirishga urinish bo'lsa, foydalanuvchiga yuboriladi yoki hisob vaqtincha bloklanadi.
4. Shubhali faoliyatdan himoya : Shubhali yoki noodatiy harakat paydo bo'lsa, tizim avtomatik hisobni himoyalash dasturini ishga tushiradi.
5. Parolni qayta tiklash jarayonining tiklanishi : Parolni unutgan foydalanuvchilarga parolni qayta tiklash uchun tiklanish jarayonini taqdim etadi. yordam, bu jarayon emaili yoki SMS orqali amalga oshirish.

6. Shaxsiy ma'lumotlarni shifrlash : Ma'lumotlar shifrlanganda, hisob taqdirda ham ruxsatsiz odamlardan foydalana olmaydi.

Hisoblarni himoya qilish hisoblarni xakerlik hujumlari, phishing, va boshqa zararli faoliyatlardan himoya qilish uchun juda oson. Shu orqali o'z shaxsiy va ma'lumotlarini saqlab qolishlari mumkin.



Firewall network protection - bu tarmoqni ruxsatsiz kirish, zararli dasturlar va boshqa kiber tahdidlardan himoya qilishga yordam beradigan xavfsizlik chorasi. Xavfsizlik devori ichki tarmog'ingiz (ishonchli tarmoq) va tashqi tarmoqlar (masalan, Internet) o'rtasida to'siq bo'lib, xavfsizlik qoidalari to'plami asosida kiruvchi va chiquvchi tarmoq trafigini filtrlaydi. Xavfsizlik devori himoyasi qanday ishlashi va nima uchun bu essentia haqida qisqacha ma'lumot

1. Firewall turlari

- Paketli filtrlovchi xavfsizlik devorlari :
- Davlat tekshiruvi xavfsizlik devorlari : faol ulanishni kuzatadi
- Proksi-serverlar : ishlaydi
- Keyingi avlod xavfsizlik devorlari (NGFW) : taroq
- Bulutga asoslangan xavfsizlik devorlari (xizmat sifatidagi xavfsizlik devori) : Pro

2. Faervol qoidalari va siyosatlari

- Xavfsizlik devorlari qanday trafikka ruxsat etilgan yoki rad etilganligini belgilaydigan qoidalar to'plamiga asoslanadi.

Ushbu qoidalar turli mezonlar uchun moslashtirilishi mumkin, jumladan:

- Manba va maqsad IP manzillari : C
- Port raqamlari va protokollari : Filt
- Ilovalar :

- Qattiq, aniq belgilangan qoidalarni o'rnatish ruxsatsiz kirishni minimallashtirishga va potentsial hujumlarni kamaytirishga yordam beradi

3. Faervolni joylashtirish

- Perimetr xavfsizlik devorlari: joy
- Ichki xavfsizlik devorlari :
- Xostga asoslangan xavfsizlik devorlari: Insta

4. Kengaytirilgan himoya uchun xavfsizlik devori xususiyatlari

- Intrusionlarni aniqlash va oldini olish tizimlari (IDPS) :
- Virtual xususiy tarmoqni (VPN) qo'llab-quvvatlash: A
- Chuqur paketli tekshiruv (DPI) : An
- Yagona tahdidlarni boshqarish (UTM): Co

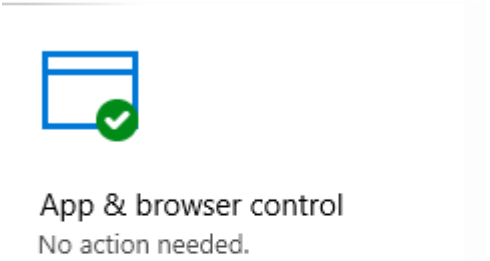
5. Faervolga texnik xizmat ko'rsatish va boshqarish

- Muntazam ravishda
- Xavfsizlik devori dasturiy ta'minoti va proshivkasini muntazam yangilab turish ularda eng so'nggi xavfsizlik xususiyatlari va zaifliklar uchun tuzatishlar mavjudligini ta'minlashga yordam beradi.

6. Nima uchun xavfsizlik devori himoyasi muhim?

- Ruxsatsiz kirishni oldini oladi : Bl
- Zararli dasturlar va virus hujumlarini yumshatadi :
- Nozik ma'lumotlarni himoya qiladi: Redu
- Umumiy tarmoq xavfsizligini oshiradi : ta'minlaydi

Kuchli xavfsizlik devori strategiyasi dasturiy ta'minotni muntazam yangilash va xodimlarni o'qitish kabi qo'shimcha xavfsizlik amaliyotlari bilan birgalikda tashkilotning cyb-ni sezilarli darajada kuchaytirishi mumkin.



App & browser control – bu Windows ilovasidagi (Windows Security) bir funksiyadir. U kompyuteringizda foydalanilayotgan dasturlar va internet brauzerlari orqali narsalarni aniqlash va aniqlash uchun mo'ljallangan. Ush funksiya zararli dastur va saytlar, phishing, va boshqa zararlardan himoya qilish uchun yordam beradi. **Dastur va brauzerni boshqarish** o'z ichiga oladi: 1. **SmartScreen filtri**: Bu vosita foydalanuvchi internet orqali olingan noma'lum yoki zarar dasturlardan olinadi. Zarar, zararli yoki phishing saytlari aniqlab, foydalanuvchi kirishadi va ushbu saytlarga kirishadi. SmartScreen filtri Windows dasturlari va Microsoft Edge brauzerida ishlaydi.

2. ** Ekspluatatsiya

Device security - deganda kompyuterlar, smartfonlar, planshetlar va boshqa apparat vositalari kabi elektron qurilmalarni turli tahdidlardan himoya qilish uchun mo'ljallangan chora-tadbirlar va texnologiyalar majmui tushuniladi. Qurilma xavfsizligining maqsadi maxfiy ma'lumotlarni himoya qilish, ruxsatsiz kirishni oldini olish va zararli dasturlardan va

kiberhujumlardan himoya qilishdir. Qurilma xavfsizligining asosiy tarkibiy qismlariga quyidagilar kiradi:

1. ** Zararli dasturlardan himoya qilish**: qurilmaga zarar etkazishi mumkin bo'lgan viruslar, troyanlar va boshqa zararli dasturlarni aniqlash va yo'q qilish uchun antivirus dasturlari va zararli dasturlarga qarshi vositalardan foydalanish.

2. ** Ma'lumotlarni shifrlash**: qurilmada saqlangan maxfiy ma'lumotlarni ruxsatsiz kirishdan himoya qilish uchun shifrlash, hatto ma'lumotlar buzilgan taqdirda ham uni osongina o'qib bo'lmasligini ta'minlash.

3. ** Kirishni boshqarish**: qurilmaga va uning ma'lumotlariga kim kira olishini boshqarish uchun kuchli parollarni, biometrik autentifikatsiyani (barmoq izi yoki yuzni aniqlash kabi) va ikki faktorli autentifikatsiyani (2FA) amalga oshirish.

4. ** Xavfsiz yuklash**: qurilmani faqat ishonchli dasturlardan foydalanishni boshlaydigan, yuklash jarayonida ruxsatsiz yoki zararli dasturlarning ishlashiga yo'l qo'ymaydigan jarayon.

5. ** Muntazam yangilanishlar**: ma'lum zaifliklardan himoya qilish uchun operatsion tizim va ilovalarni so'nggi xavfsizlik yamoqlari bilan yangilab turish.

6. ** Tarmoq xavfsizligi**: VPN (Virtual xususiy tarmoqlar) dan foydalanish va tarmoqlarga ruxsatsiz kirishdan himoya qilish kabi xavfsiz ulanishlarni ta'minlash.

7. ** Jismoniy xavfsizlik**: o'g'irlikning oldini olish uchun qulflardan foydalanish, xavfsiz saqlash yoki joylashuvni kuzatish kabi qurilmani jismoniy himoya qilish choralarini ko'rish.

Qurilma xavfsizligi foydalanuvchi maxfiyligini himoya qilish, shaxsiy va moliyaviy ma'lumotlarni ta'minlash va qurilmaning

yaxlitligini saqlash uchun juda muhimdir. Bu shaxslar va tashkilotlar uchun umumiy kiberxavfsizlik strategiyasida muhim rol o'ynaydi.

Device performance & health
No action needed.

Device performance & health - kompyuter yoki mobil qurilmaning umumiy ishlashi va holatini anglatadi, uning ganchalik yaxshi ishlashiga va uning optimal ishlashiga e'tibor beradi. Bu jihat turli ko'rsatkichlarni kuzatish va uzluksiz ishlash va uzoq umr ko'rish uchun qurilmaning apparat va dasturiy komponentlari haqida tushuncha berishni o'z ichiga oladi.

Qurilmaning ishlashi va sog'lig'ining asosiy tarkibiy qismlariga quyidagilar kiradi:

1. ** Ishlash monitoringi**: CPU, RAM, diskdan foydalanish va boshqa resurslarning ishlashini kuzatadigan vositalar va yordamchi dasturlar. Bu qurilmani sekinlashtirishi mumkin bo'lgan muammolar yoki muammolarni aniqlashga yordam beradi.

2. ** Disk salomatligi**: ma'lumotlar yo'qolishiga olib kelishi mumkin bo'lgan yomon tarmoqlar yoki diskdagi nosozliklar kabi muammolarni aniqlash uchun saqlash disklari (HDD, SSD) holatini kuzatish.

3. ** Tizim yangilanishlari**: operatsion tizim va ilovalarning so'nggi versiyalariga yangilanishini ta'minlash. Yangilanishlar ko'pincha ishlashni yaxshilash, xatolarni tuzatish va xavfsizlik yamoqlarini o'z ichiga oladi.

4. ** Resurslarni boshqarish**: qurilmaning haddan tashqari yuklanmasligini ta'minlash uchun ishlaydigan jarayonlar va

dasturlarni boshqarish. Bunga resurslarni iste'mol qiladigan keraksiz dasturlar yoki xizmatlarni o'chirish kiradi.

5. ** Haroratni kuzatish**: qizib ketishning oldini olish uchun qurilmaning ish haroratini tekshirish, bu vaqt o'tishi bilan ishlashni yomonlashtirishi va qismlarga zarar etkazishi mumkin.

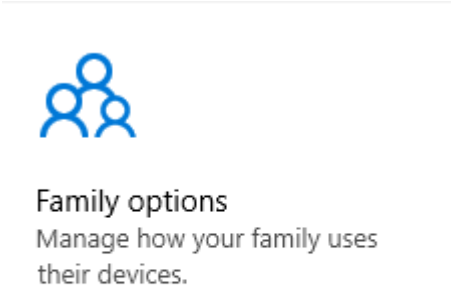
6. ** Batareya salomatligi**: portativ qurilmalar uchun batareyaning ishlashi va uzoq umr ko'rishini baholash, qurilma zaryadni samarali ushlab turishi va kutilganidek ishlashini ta'minlash.

7. ** Zararli dastur va xavfsizlikni tekshirish**: qurilmaning ishlashiga ta'sir qilishi va ma'lumotlar yaxlitligini buzishi mumkin bo'lgan zararli dastur va boshqa xavfsizlik tahdidlarini muntazam ravishda skanerlash.

8. ** Foydalanuvchi tajribasini optimallashtirish**: keraksiz fayllarni tozalash, ishga tushirish dasturlarini optimallashtirish va disklarni birlashtirish (an'anaviy qattiq disklarda) kabi foydalanuvchi tajribasini yaxshilash uchun tavsiyalar yoki vositalarni taqdim etish.

9. ** Diagnostika vositalari**: apparat va dasturiy ta'minot muammolarini aniqlashga yordam beradigan, foydalanuvchilarga ishlashni yaxshilash uchun amaliy tushunchalarni beradigan o'rnatilgan vositalar.

Qurilmaning ishlashi va sog'lig'ini saqlash qurilmaning muammosiz, samarali va xavfsiz ishlashini ta'minlash, foydalanuvchilarga yaxshi tajribadan bahramand bo'lish va qurilmalarining ishlash muddatini uzaytirish uchun juda muhimdir.



Family options - odatda oilalarga o'z oila a'zolarining, xususan bolalarning raqamli faoliyatini boshqarish va nazorat qilish imkonini beruvchi operatsion tizimlar yoki dasturiy ta'minot tomonidan taqdim etilgan xususiyatlar va vositalar to'plamini anglatadi. Ushbu variantlar onlayn xavfsizlikni oshirish, mas'uliyatli raqamli xatti-harakatlarni rag'batlantirish va ota-onalarga farzandlarining texnologiyadan foydalanishini nazorat qilish vositalarini taqdim etish uchun mo'ljallangan.

Ko'pincha oilaviy variantlarga kiritilgan asosiy xususiyatlar:

1. ** Ota-ona nazorati**: ota-onalarga farzandlari kirishi mumkin bo'lgan kontentga cheklovlar qo'yishga imkon beruvchi vositalar, masalan, nomaqbul veb-saytlarni bloklash yoki qurilmalarda ekran vaqtini cheklash.

2. ** Ekran vaqtini boshqarish**: ota-onalar uchun bolalar qurilmalar yoki maxsus ilovalarga qancha vaqt sarflashlari mumkinligi bo'yicha kunlik chegaralarni belgilash imkoniyatlari, bu ekran vaqti va boshqa tadbirlar o'rtasida sog'lom muvozanatni saqlashga yordam beradi.

3. ** Faoliyat monitoringi**: bolalar o'z qurilmalaridan qanday foydalanayotgani, jumladan, qaysi ilovalardan va qancha vaqt foydalanayotgani haqida hisobotlarni taqdim etuvchi xususiyatlar ota-onalarga farzandlarining raqamli odatlari haqida ma'lumot berish imkonini beradi.

4. ** Ilovalarni boshqarish**: bolalar yuklab olishi yoki foydalanishi mumkin bo'lgan maxsus ilovalarni tasdiqlash yoki bloklash, ularning yoshiga mos kontent bilan ishlashini ta'minlash.

5. ** Joylashuvni kuzatish**: mobil qurilmalar uchun bu xususiyat ota-onalarga farzandlarining jismoniy joylashuvini kuzatishda yordam beradi, ayniqsa yosh bolalar uchun qo'shimcha xavfsizlik qatlamini ta'minlaydi.

6. ** Oilaviy almashish**: oila a'zolari o'rtasida ilovalar, o'yinlar, obunalar yoki xizmatlarni almashish imkoniyatlari, bu oilalarga birgalikda kontentga kirishni osonlashtiradi.

7. ** Hisobni boshqarish**: bolalar uchun foydalanuvchi hisoblarini yaratish va boshqarish vositalari, har bir oila a'zosining shaxsiy sozlamalari va kirish huquqlariga ega bo'lishini ta'minlash.

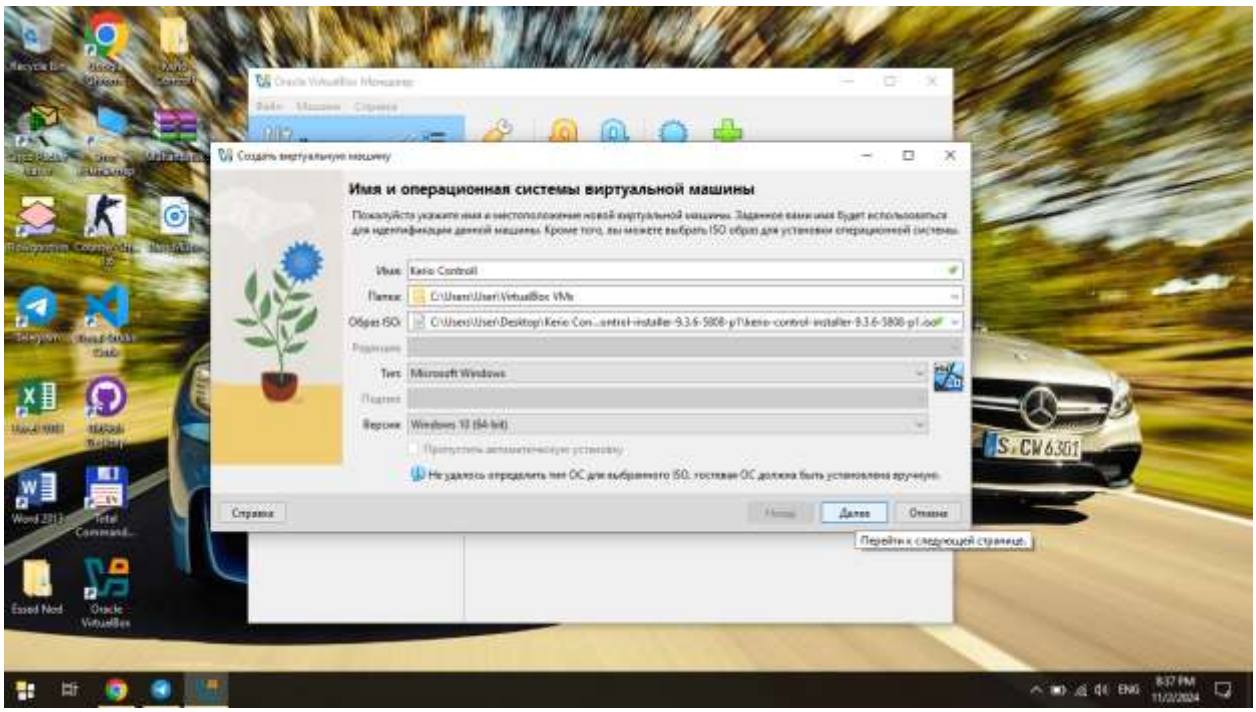
8. ** Aloqa monitoringi**: ota-onalarga xabar almashish ilovalari yoki ijtimoiy media platformalari orqali aloqalarni kuzatishga imkon beruvchi xususiyatlar xavfsiz o'zaro ta'sirlarni ta'minlashga yordam beradi.

9. ** Xavfsizlik resurslari**: onlayn xavfsizlik, raqamli savodxonlik va oilada sog'lom texnik odatlarni qanday tarbiyalash haqida manbalar va ma'lumotlarga kirish.

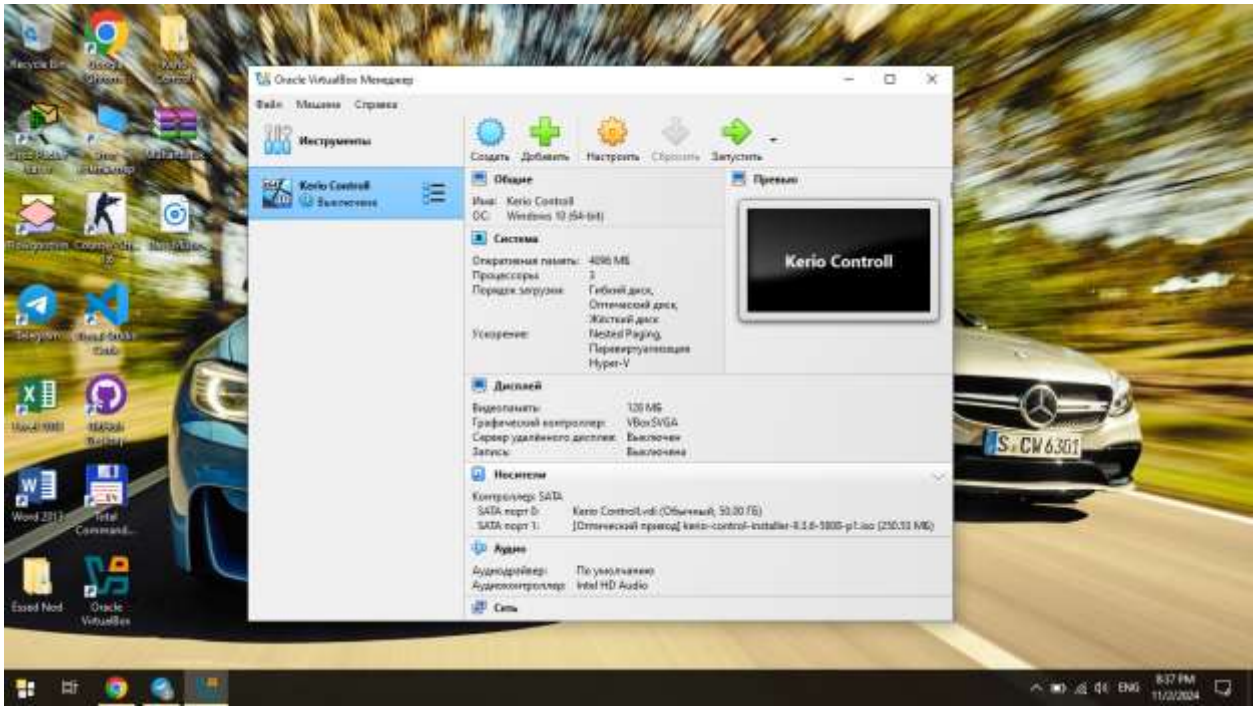
Ushbu oilaviy imkoniyatlar ota-onalarga farzandlari uchun xavfsizroq va boshqariladigan raqamli muhitni yaratishga yordam beradi, shu bilan birga texnologiyadan mas'uliyatli va muvozanatli foydalanishni rag'batlantiradi. Ularni ko'pincha derazalar, macOS kabi operatsion tizimlarda yoki Android va iOS kabi mobil platformalarda, shuningdek, oilani boshqarish uchun mo'ljallangan turli xil uchinchi tomon dasturlarida topish mumkin.

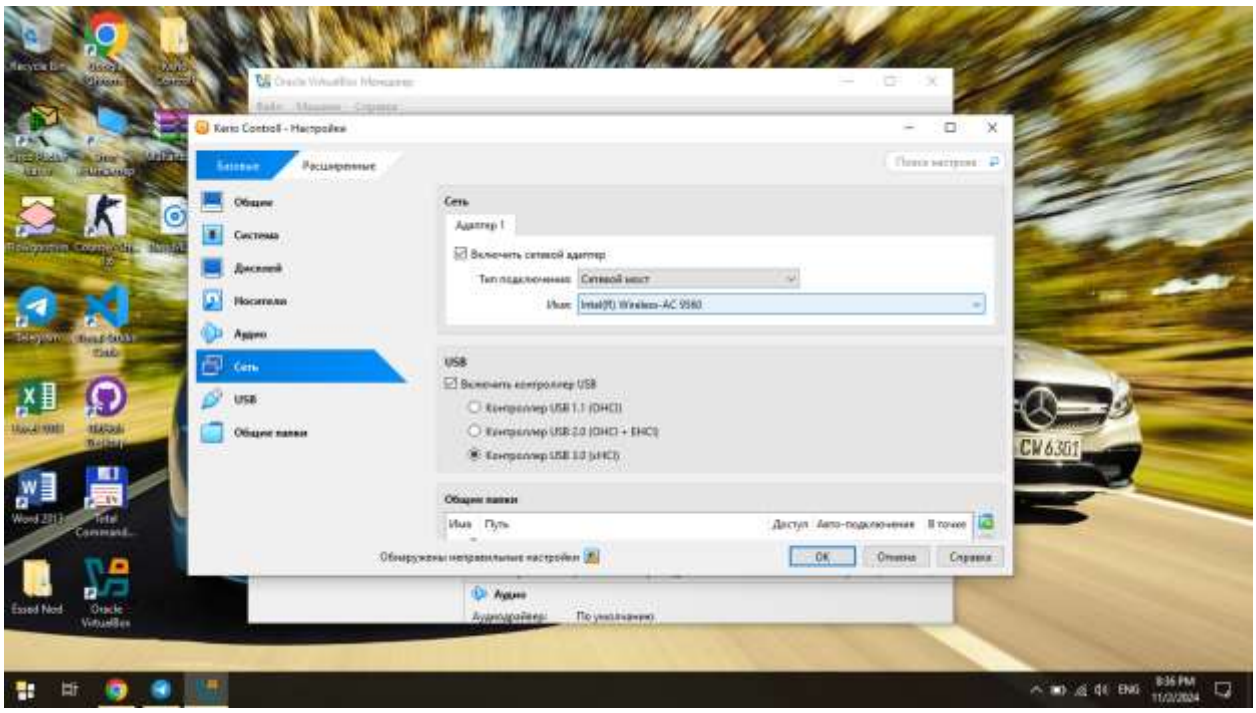
8-amaliy mashg‘ulot.

Tarmoqlararo ekran vositasi yordamida tarmoq himoyasini ko‘rish: Kerio Control firewall misolida

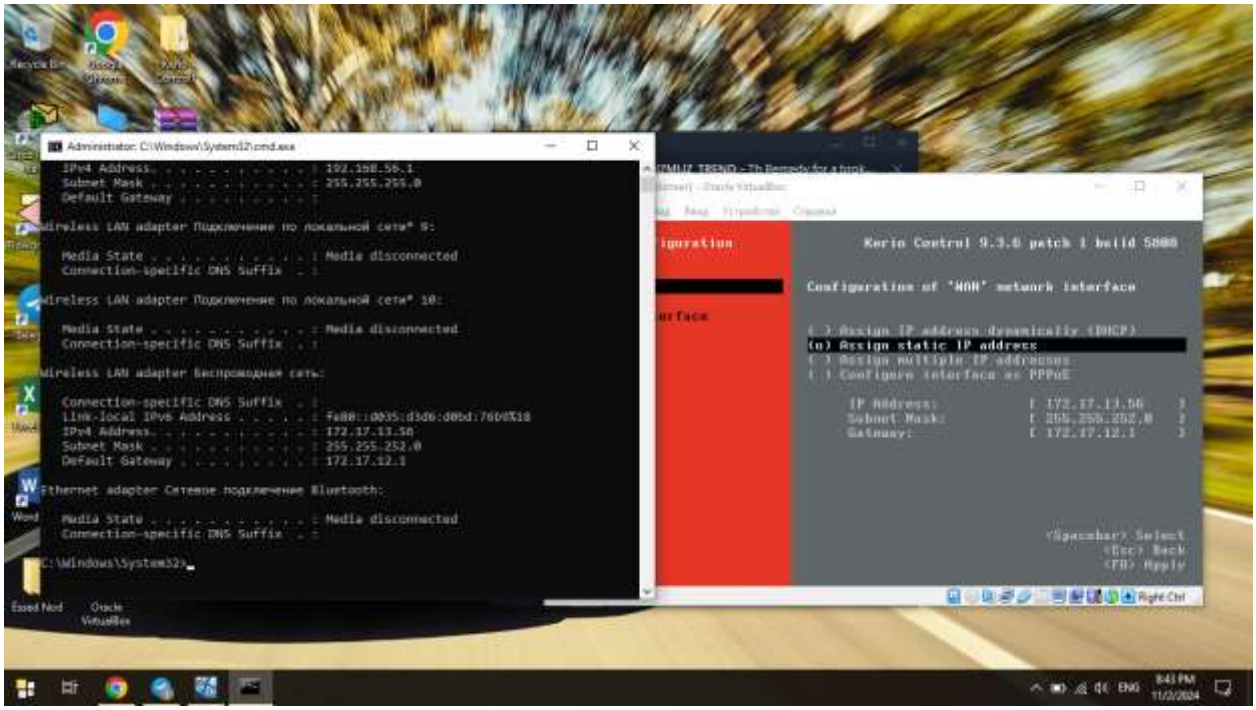


Oracle VirtualBox dasturini sozdat qilamiz.

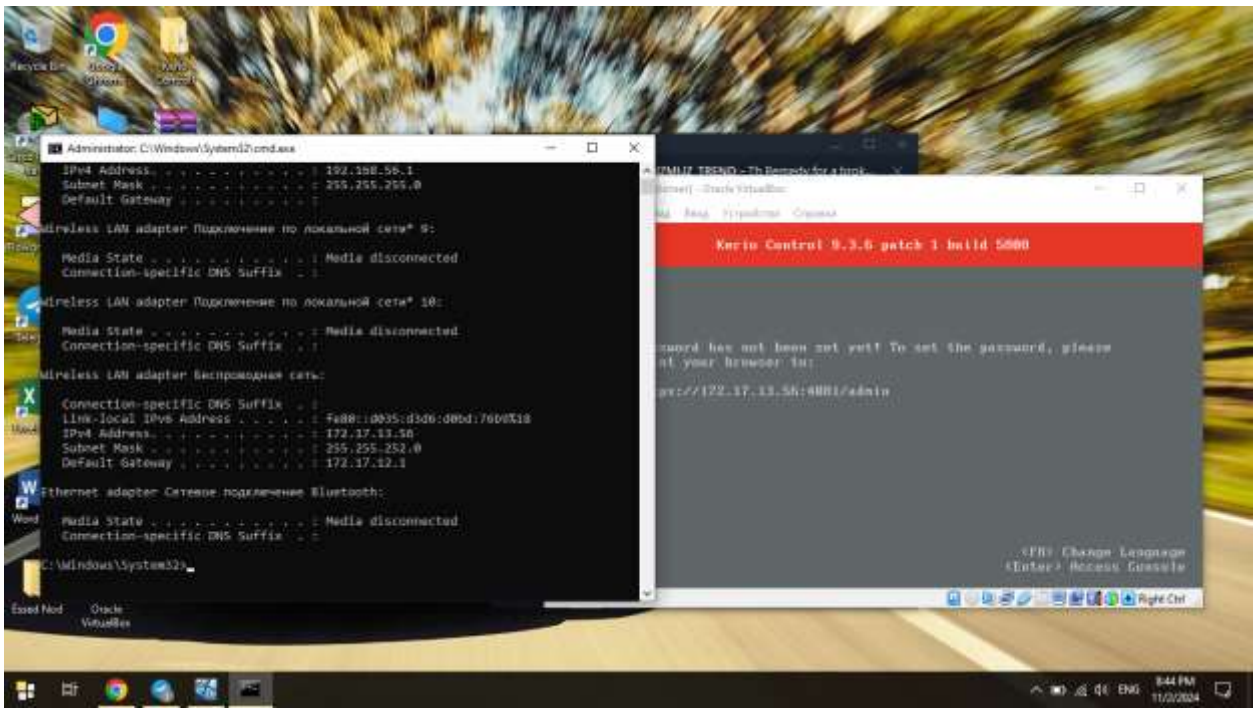




Kerio Controll dasturini sozlab olamiz.



Kerio Control o'rnatildi kompyuter bn iPv4 Adrees ni bir xilga keltiramiz.



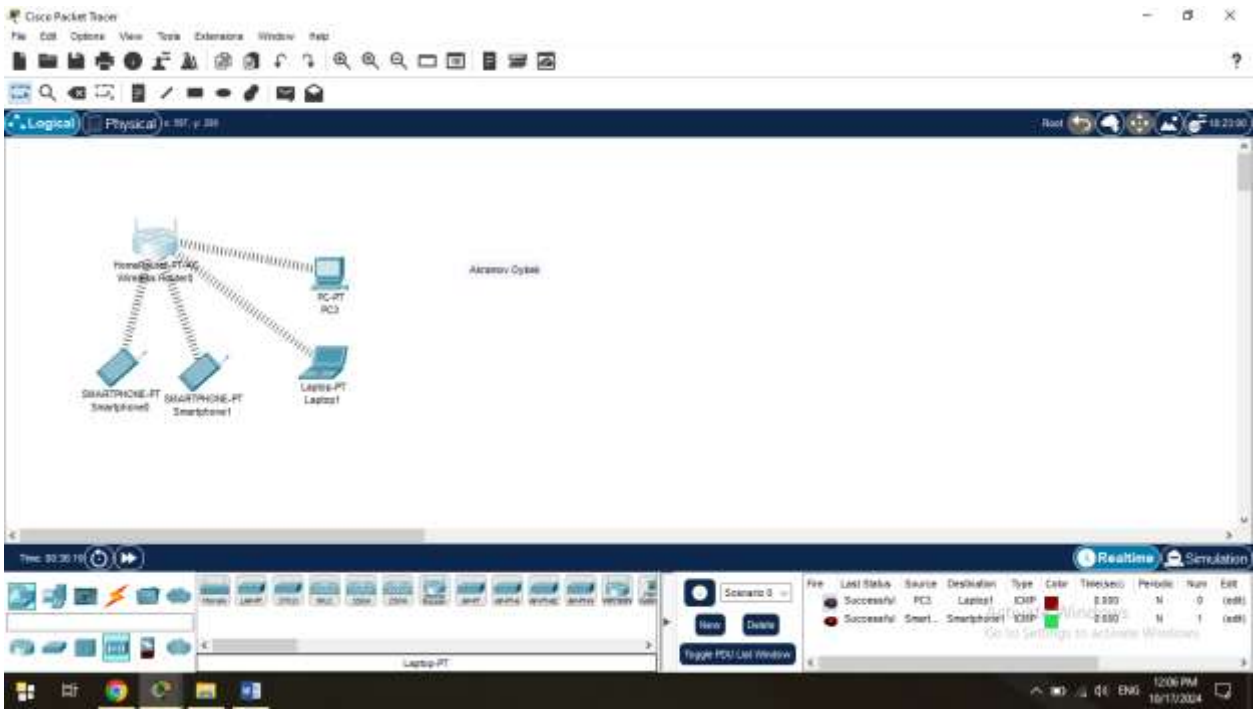
Tayyor.

9-amaliy mashg'ulot.

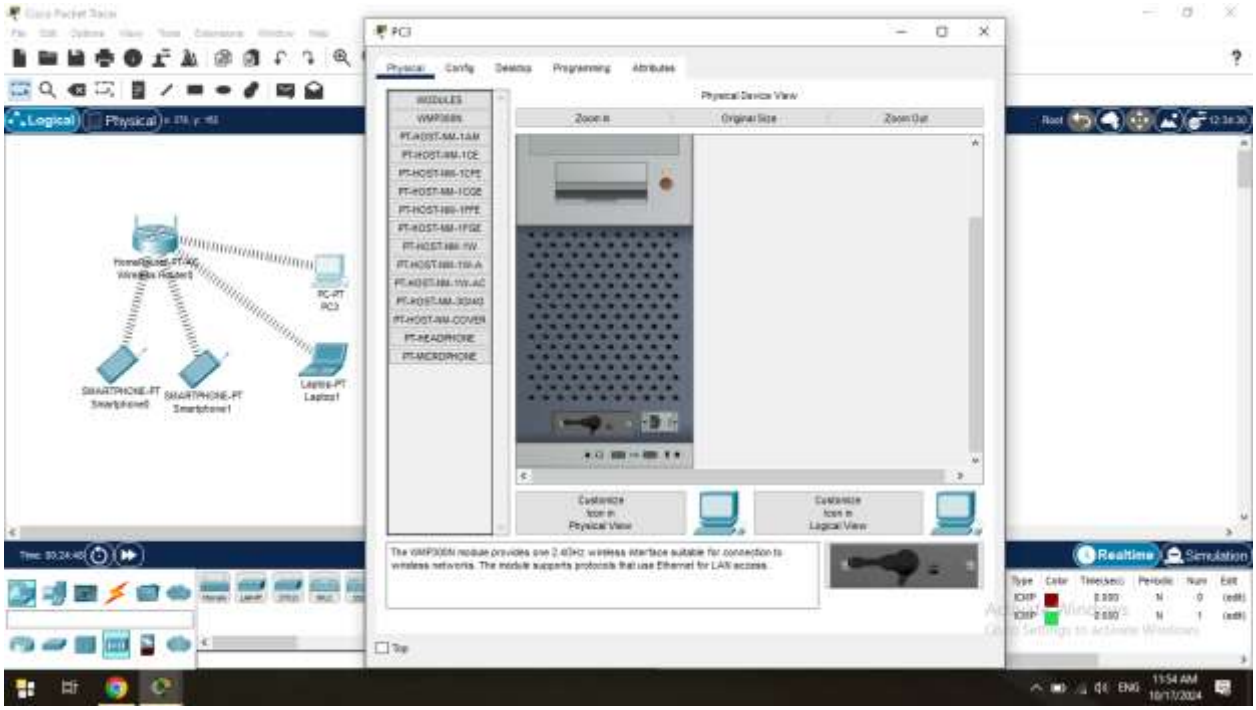
Xavfsiz Wi-Fi simsiz tarmog'ini qurish.

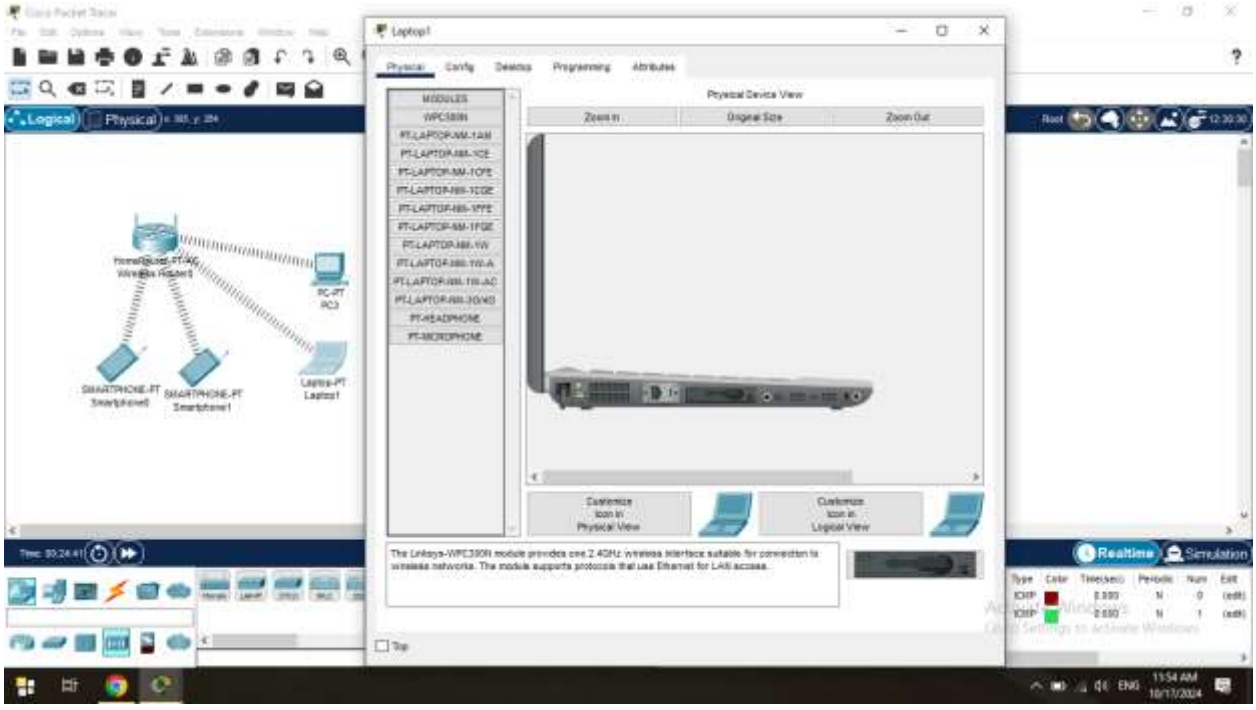
1 ta roter, 2 ta smartfon, 1 ta kompyuter, 1 ta notebook olamiz.

Ularni roterga ulaymiz.

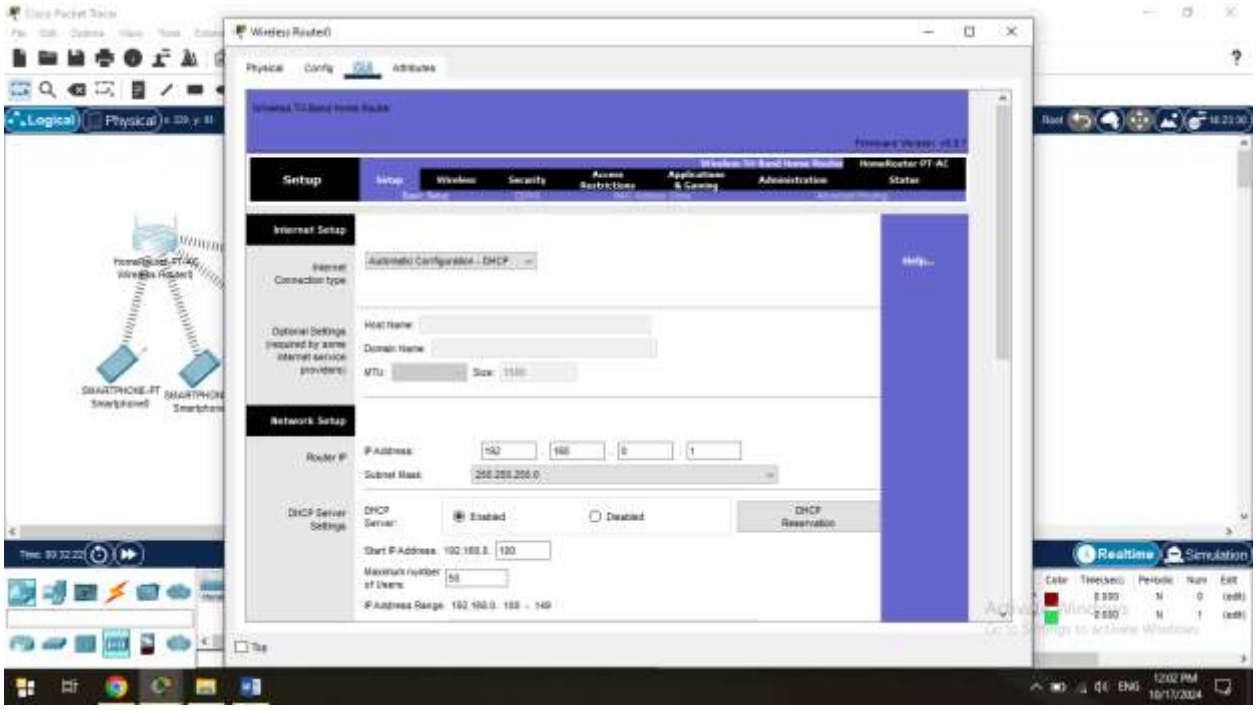


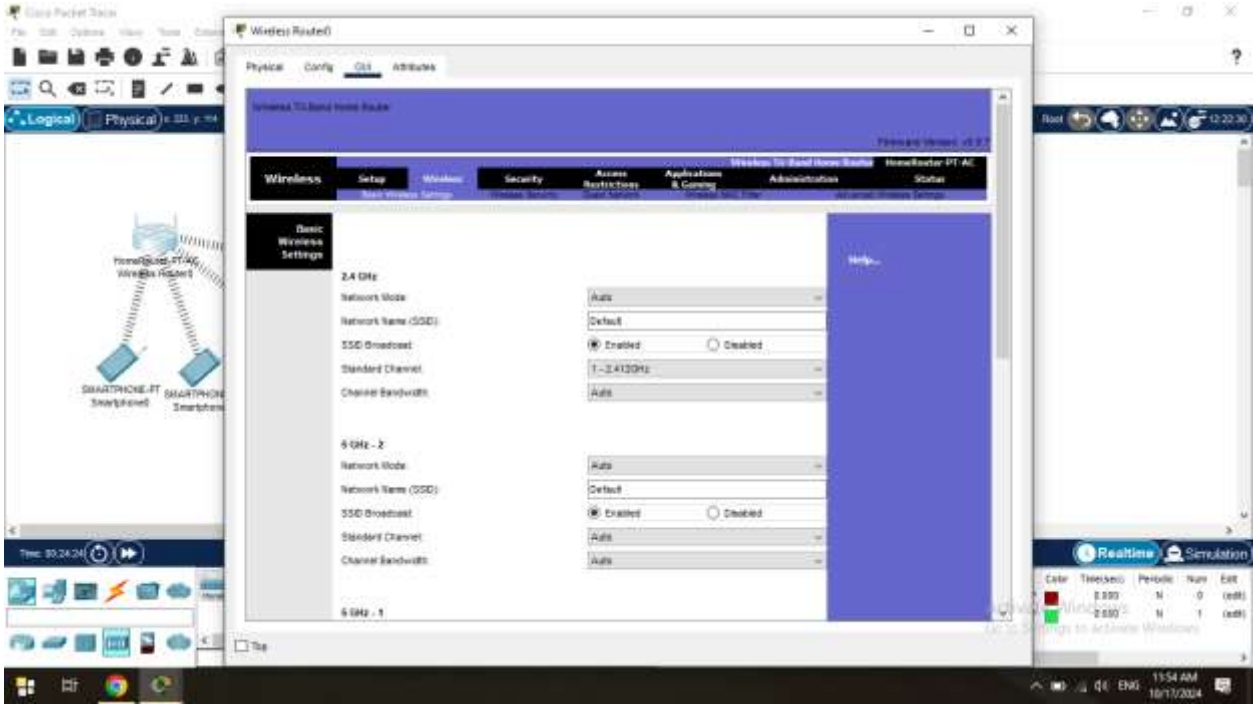
Kompyuter va Notebookni roterga ulash jarayoni.



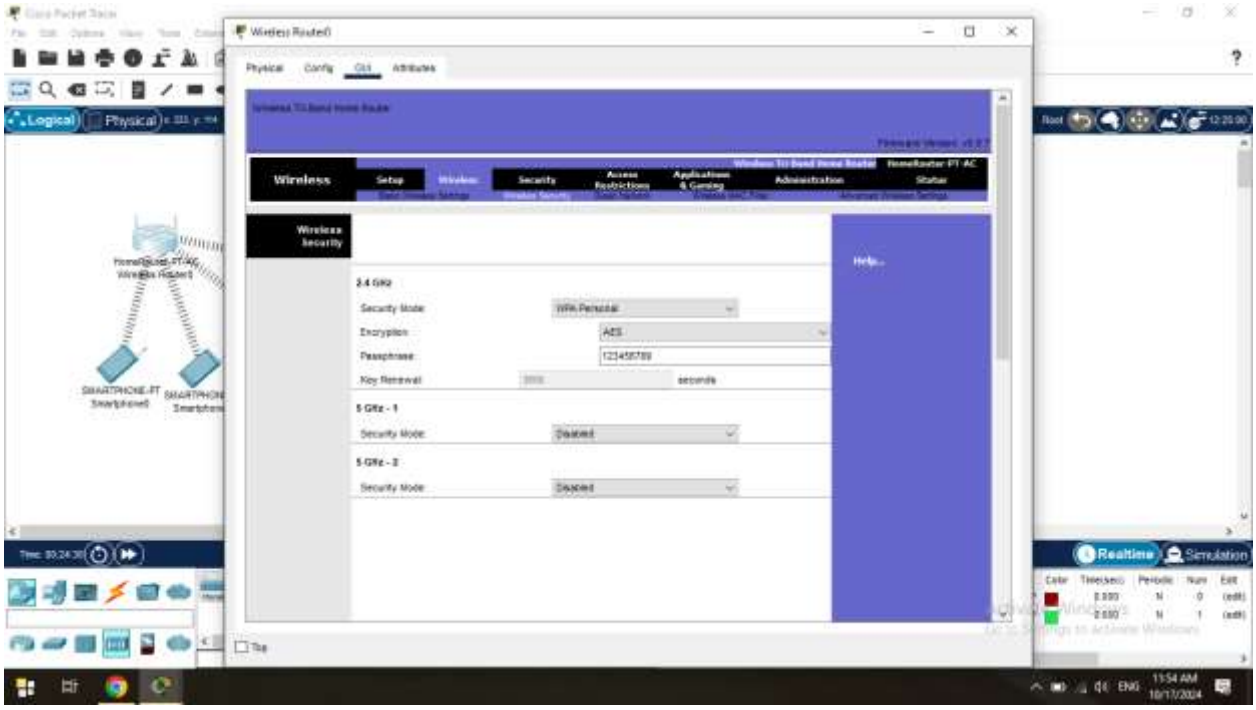


Roter ichidagi Setup oynasi hech qayeriga o‘zgarish kiritmadik.





Wirelles oynasidagi Wirelles security tugmasini bosib. Security Mode da turgan Disabledni WPA Personal ga o‘zgartiramiz.



10-amaliy mashg‘ulot.

Kiberxavfsizlikda risklarni baholashni o‘rganish

Akramov Education

1-Jadval Tahdidni amalga oshirish ehtimolini baholash

Hujum ehtimoli	Tavsif	Ehtimollik qiymati
1 Juda past	Tahdid deyarli sodir bo'lmaydi	[0; 0,25)
2 past	Bu tahdid amalga oshishi ehtimoldan yuqori emas	[0,25; 0,5)
3 O'rta	Tahdid ehtimoli teng darajada bo'lishi mumkin	0,5
4 Yuqori	Ehtimol, bu tahdid amalga oshishi mumkin (oldin voqealar bo'lgan), yoki shunga o'xshash tahdidlar	(0,5; 0,75]

	ba'zida oldin sodir etilganligini ko'rsatuvchi statistik ma'lumotlar yoki boshqa ma'lumotlar yoki tajovuzkorning o'ziga xos sabablari bo'lishi mumkinligi haqida dalillar bo'lishi mumkin.	
5 Juda yuqori	Ehtimol, tahdid amalga oshadi. Hodisa sodir bo'lishi mumkinligini ko'rsatadigan hodisalar, statistik ma'lumotlar yoki boshqa ma'lumotlar yoki tajovuzkorning bunday harakatga jiddiy sabablari yoki sabablari bo'lishi mumkin.	(0,75; 1]

2 -jadval - zaifliklar orqali tahdidni amalga oshirish ehtimolini baholash

Hujum ehtimoli	Tavsif	Ehtimollik qiymati
1 Yuqori	Zaiflikdan foydalanish oson va himoyasiz yoki umuman yo'q	(0,75; 1]
2 O'rta	Zaiflikdan foydalanish mumkin, lekin ba'zi himoya mavjud	[0,35; 0,75)
3 Past	Zaiflikdan foydalanish qiyin va yaxshi himoya mavjud	[0; 0,35)

3 -jadval - Axborot ob'ekti xavfini tahlil qilish natijalari

Zaiflik nomi	Tahdid nomi	Tahdid ehtimoli	Xavfsizlikning amalga oshirilishi ehtimoli	Risk,
Parollar	Xodimlar	(0,5; 0,75]	[0,35; 0,75)	(0.175;0.5625]
Texnika	Iqtisodiy inqiroz	(0,5; 0,75]	[0,35; 0,75)	(0.175;0.5625]

4 -jadval - Zarar darajasini baholash

Zarar darajasi	Tavsif
1 kichik (1000 AQSh dollaridan kam)	Tez tiklanadigan moddiy boyliklarning ozgina yo'qotilishi yoki kompaniyaning obro'siga ozgina ta'sir ko'rsatishi
2 o'rtacha (1000 dan 5000 AQSh dollarigacha)	Moddiy aktivlarning sezilarli darajada yo'qolishi yoki kompaniyaning obro'siga o'rtacha ta'sir ko'rsatishi
3 O'rtacha (5000 dan 10,000 USD gacha)	Moddiy boyliklarning sezilarli darajada yo'qolishi yoki kompaniyaning obro'siga jiddiy zarar yetkazilishi
4 Katta (10,000 $ dan 30,000 $ gacha)	Moddiy boyliklarning katta yo'qotilishi va kompaniyaning obro'siga katta zarar
5 Kritik (30000 $ dan yuqori.)	Moddiy aktivlarning keskin yo'qolishi yoki kompaniyaning bozorda obro'sining to'liq yo'qolishi, bu uning keyingi faoliyatiga to'sqinlik qiladi.