

23-Laboratoriya ishi Mavzu: Antivirusni o'rnatish

Biz har doim Panda mahsulotimizning so'nggi versiyasini Panda hisobimizdan yuklab olishimiz mumkin. Faqat quyidagi amallarni bajaring:

1. Faollashtirish kodimizni tayyorlang.
2. Panda hisobini yarating va agar bizda allaqachon mavjud bo'lsa, unga kirish uchun elektron pochta manzilimizni (login) va parolimizni kiriting:
<https://myaccount.pandasecurity.com>
3. Mahsulotimizni tanlaymiz. Agar mahsulotimizni topa olmasak, " **Menda kod bor** " tugmasini bosish orqali faollashtirish kodimizni kiriting :

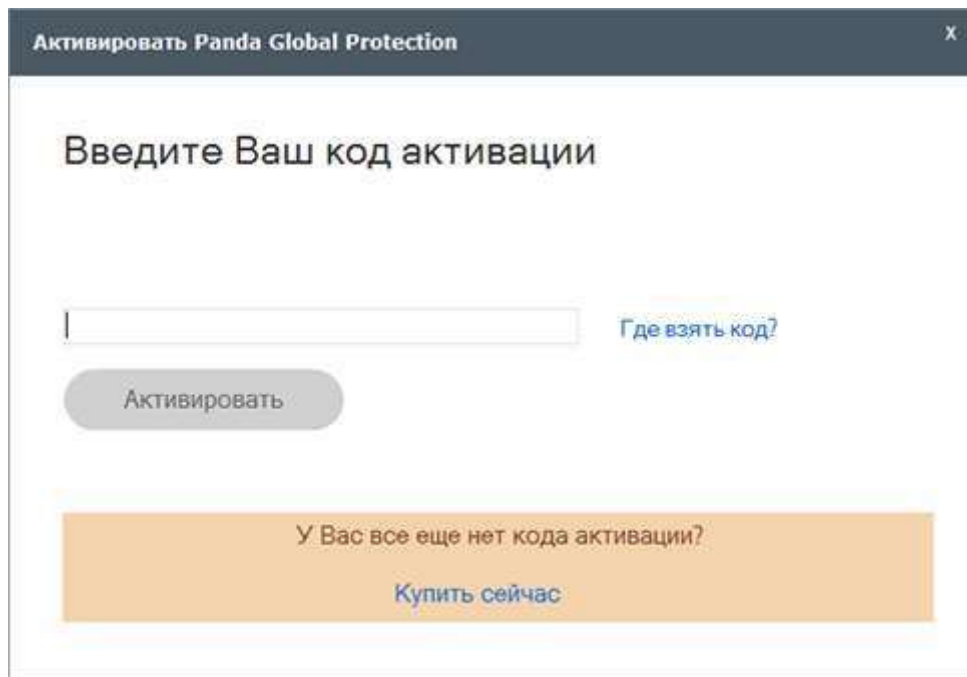


4. Endi o'rnatish faylini yuklab olish uchun bulut belgisini bosing.

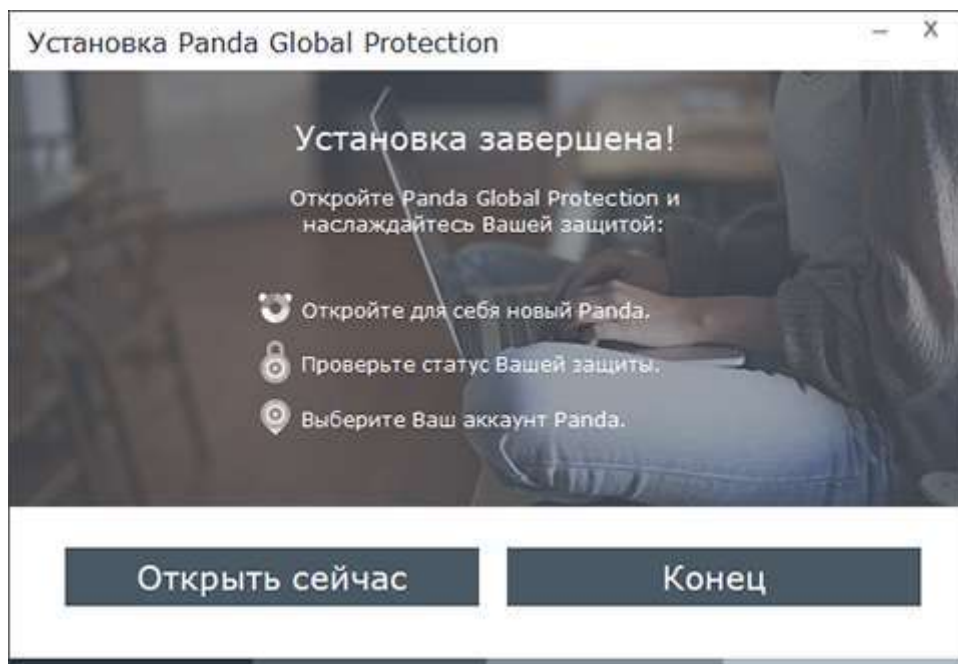


5. Biz yuklab olgan Panda fayliga ikki marta bosing va o'rnatish ustasiga amal qiling.

Sehrgarning birinchi ekranida [faollashtirish kodimiz matn maydonida](#) bo'ladi. Aks holda, agar u erda bo'lmasa, uni kiriting va davom eting.



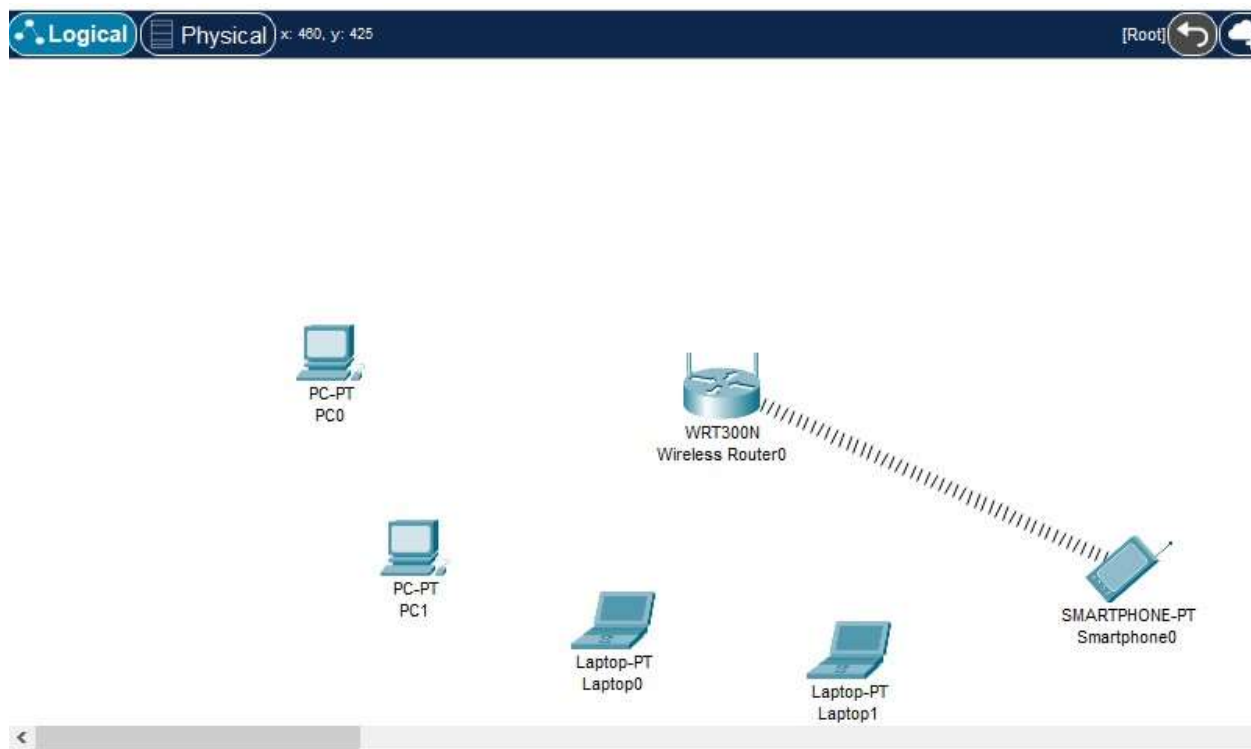
6. O'rnatish jarayonini yakunlash va Panda hisob qaydnomakni o'rnatishni davom ettirish uchun **Hozir ochish** tugmasini bosing .



24 – LABORATORIYA ISHI MAVZU: TARMOQ MUAMMOLARINI IZLASH VA BARTARAF ETISH: SIMSIZ TARMOQ ROUTERIDA MAC – ADRESLAR FILTLASH

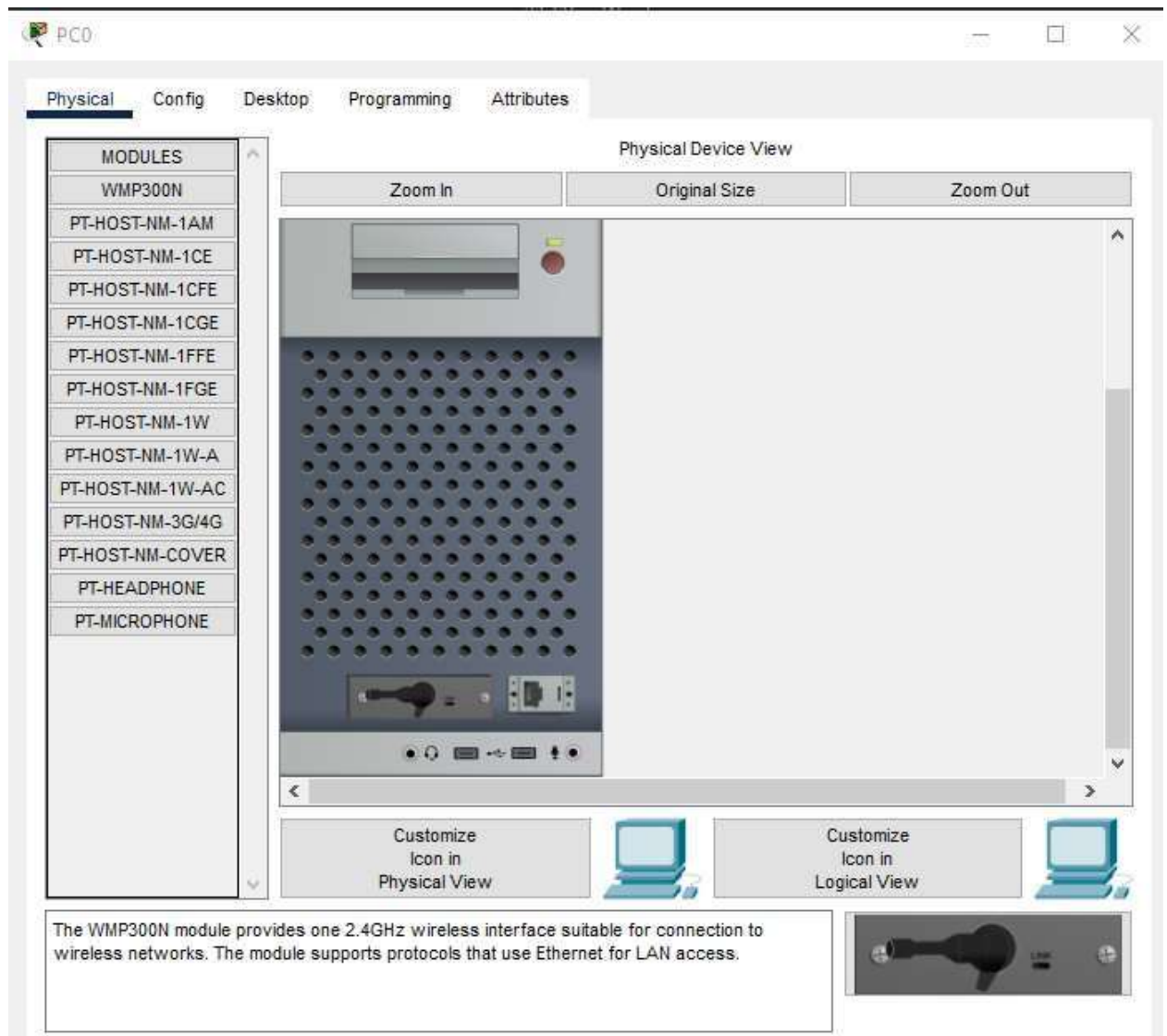
Cisco Packet Tracer dasturida simsiz routerlani MAC manzil bo'yicha filtrlash.

Dastlab Cisco Packet Tracer dasturi ishga tushiriladi va rasmdagi kabi kompyuterlar, noutbooklar va simsiz router tanlab olinadi.

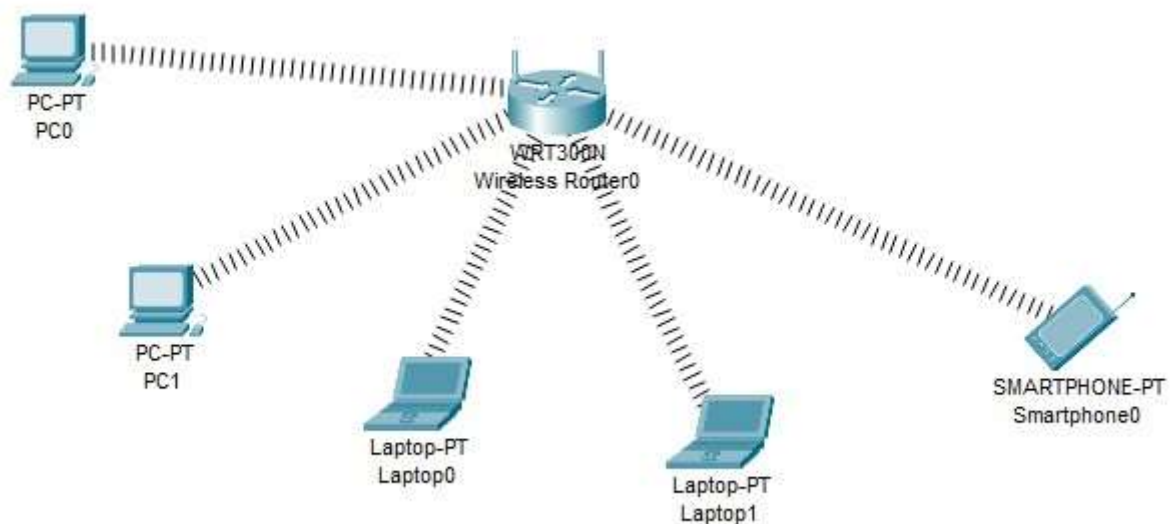


Kompyuter va noutbooklarni simsiz routerga ulanish uchun qurilmalarda simsiz adapterni ulab qo'yish kerak. Buning uchun kompyuter tanlanadi. "Physical" bo'limiga o'tiladi:

1. Kompyuter o'chiriladi;
2. Kompyuter pastki qismidagi Ethernet adapter olinadi;
3. Simsiz tarmoq adapter kompyuterga joylanadi va kompyuter qayta yoqiladi.



Shu tariqa qolgan qurilmalarga ham simsiz tarmoq adapter joylanadi. Natijada hamma qurilmalar simsiz routerga ulangani aks etadi.



Simsiz routerlarda kompyuter, noutbooklarni MAC manzili bo'yicha filtrlash uchun. Qurilmalarni MAC manzili yozib olinadi. Kompyuterga o'tiladi. "Deskop", "Командная строка" tanlanadi. Oynaga **ipconfig /all** buyrug'i kiritiladi.

Hosil bo'lgan ma'lumotlardan "Physical Address" dagi ma'lumot nusxa olinadi.

```
C:\>ipconfig /all

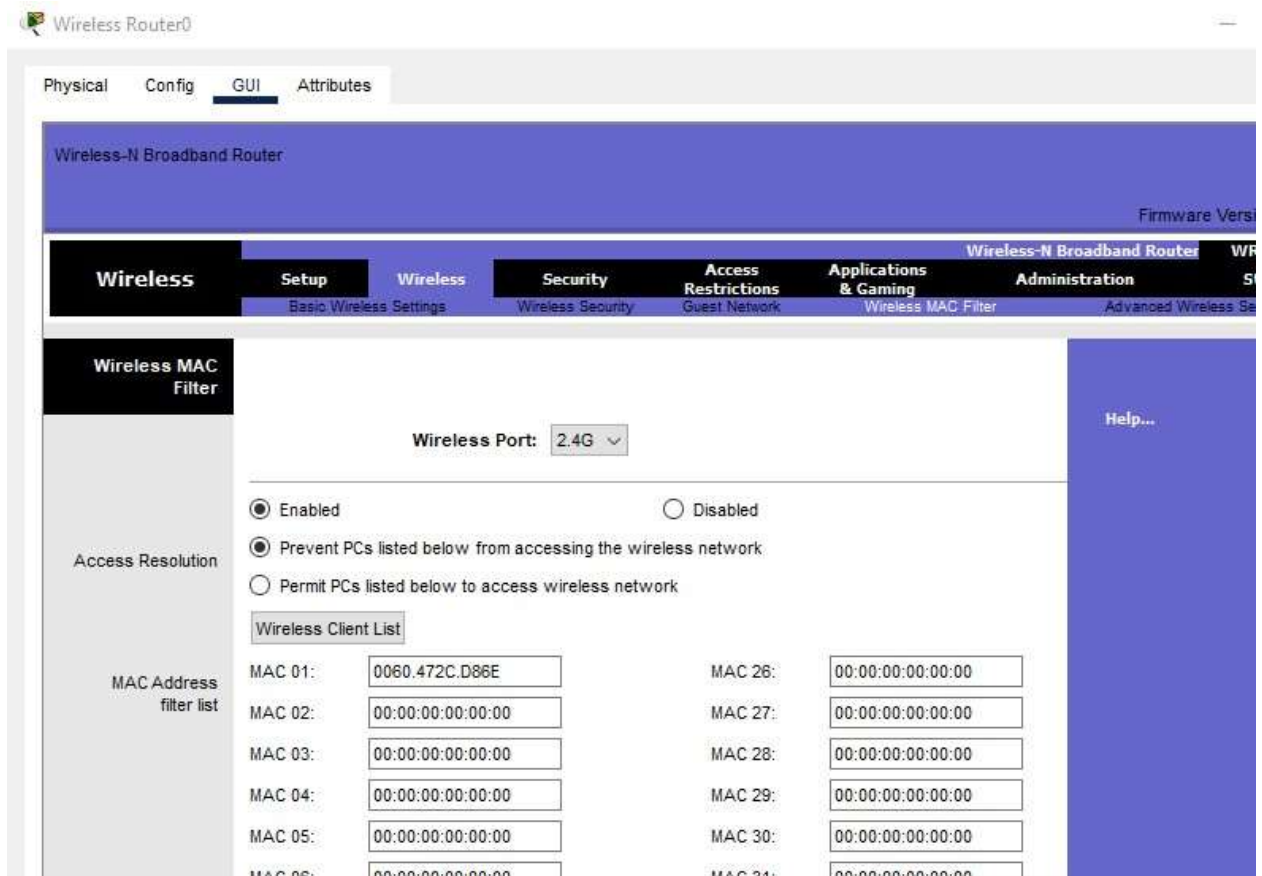
Bluetooth Connection: (default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 000C.85A7.5486
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                        0.0.0.0
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-75-89-05-8C-00-60-47-2C-D8-6E
    DNS Servers.....: ::
                        0.0.0.0

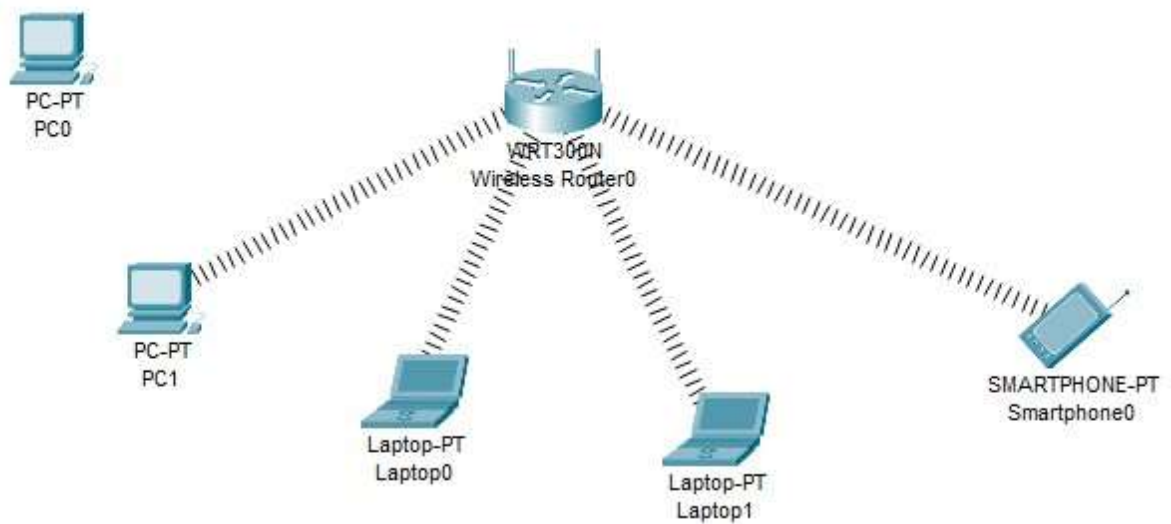
Wireless0 Connection:

    Connection-specific DNS Suffix...:
    Physical Address.....: 0060.472C.D86E
    Link-local IPv6 Address.....: FE80::260:47FF:FE2C:D86E
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                        0.0.0.0
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-75-89-05-8C-00-60-47-2C-D8-6E
    DNS Servers.....: ::
                        0.0.0.0
```

Simsiz router tanlanadi. 1. "GUI" bandi tanlanadi. 2. "Wireless" qismiga o'tiladi. 3. "Wireless MAC Filter" tanlanadi. 4. "Enabled" belgilanadi. 5. MAC 01 oynaga birinchi kompyuter MAC manzili kiritiladi. Jarayon yakunlangach saqlash tugmasi bosiladi.



Natija birinchi kompyuter simsiz routerga ulana olmay qoladi.



25-LABORATORIYA ISHI

MAVZU: TARMOQ MUAMMOLARINI IZLASH VA BARTARAF ETISH: WEP VA WPA PROTOKOLINI SOZLASH.

Nazariy qism

Simsiz tarmoq Wi-Fi ulanish nuqtasini himoya qilish muhim hisoblanadi. Sababi xavfsizlik ta'minlanmasa, kimdir sizning tarmoqdan axborot almashishda tizimingizni buzishi yoki tarmoq orqali noqonuniy harakatlarni amalga oshirishi mumkin. Wi-Fi protokollari - bu Wi-Fi simsiz axborot almashinishda xavfsiz kirishni ta'minlash uchun ishlab chiqilgan standartdir. Wi-Fi protokollari tarmoq bo'ylab harakatlanayotganda ma'lumotlarni shifrlaydi. Shifrini ochish kaliti bo'lmagan odam tarmoqqa ulana olmaydi va aloqa ma'lumotlarini o'qiy olmaydi.

Barcha protokollar sizmsiz tarmoq xavfsizligini ta'minlash uchun ishlab chiqilgan. Ushbu protokollarning har biri o'zining afzalliklari va kamchiliklariga ega. Foydalanuvchi tegishli protokolni tanlashi kerak.

Shuni yodda tutish kerakki, simsiz tarmoqlar mutloqo xavfsiz emas, chunki simsiz signallarning fazoda tarqalishini nazorat qilib bo'lmaydi. Shuning uchun ma'lumotlarni buzish yoki o'qish xavfini kamaytiradigan eng yaxshi xavfsizlik protokolini tanlash muhimdir.

WEP (Wired Equivalent Privacy)

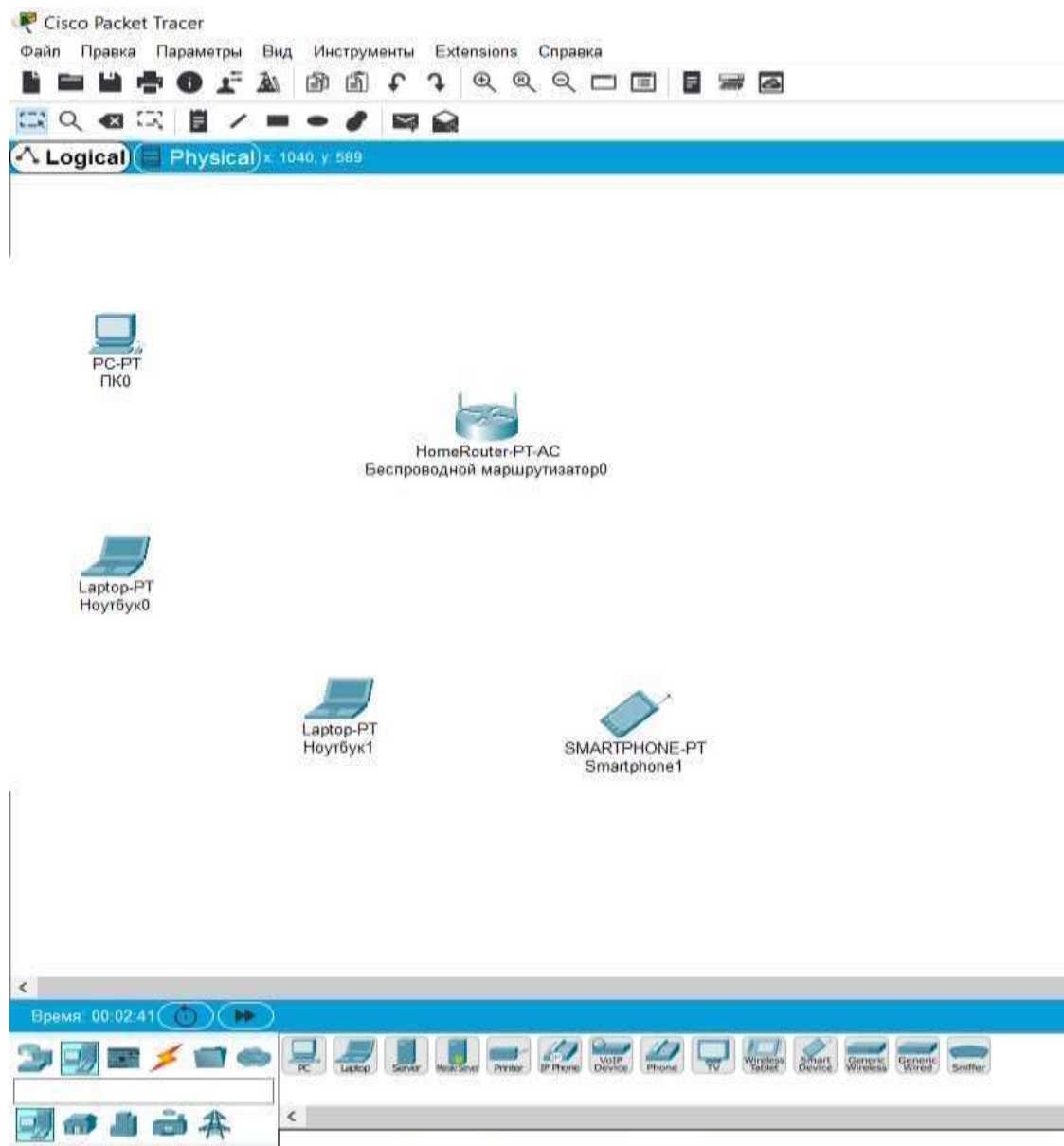
WEP (Wired Equivalent Privacy)— Wi-Fi tarmoqlari xavfsizligini ta'minlash uchun ishlab chiqilgan dastlabki algoritm. Maxfiylikni ta'minlash va foydalanuvchilarning uzatilgan ma'lumotlarini ushlab qolishdan himoya qilish uchun ishlatiladi. WEP-40 va WEP-104 ikkita versiyasi mavjud, ular faqat kalit uzunligi bilan farqlanadi. Hozirgi vaqtda ushbu texnologiya eskirgan, hakerlar bir necha daqiqada buzib kirishi mumkin. Biroq, u keng foydalanishda davom etmoqda.

WPA va WPA2 (Wi-Fi Protected Access) - simsiz qurilmalar uchun yangilangan sertifikatlash dasturi. WPA texnologiyasi WEP simsiz Wi-Fi tarmoq xavfsizligi texnologiyasini almashtiradi. WPA-ning afzalliklari ma'lumotlar xavfsizligining mustaxkamlanganligi va simsiz tarmoqlarga kirishning kuchaytirilgan nazoratidir. Muhim xususiyat ko'plab simsiz qurilmalar, ham apparat, ham dasturiy ta'minot o'rtasidagi muvofiqlikdir. Hozirgi vaqtda WPA va WPA2 Wi-Fi Alliance tomonidan ishlab chiqilgan va foydalanilmoqda.

WPA 802.1X standartlarini, shuningdek EAP (Extensible Authentication Protocol -kengaytirilgan autentifikatsiya protokoli) ni qo'llab-quvvatlaydi. Shuni ta'kidlash kerakki, WPA2 AES (Advanced Encryption Standard) ga muvofiq shifrlashni qo'llab-quvvatlaydi, bu WEP RC4-ga nisbatan bir qator afzalliklarga ega, masalan, yanada mustahkam kriptografik algoritm.

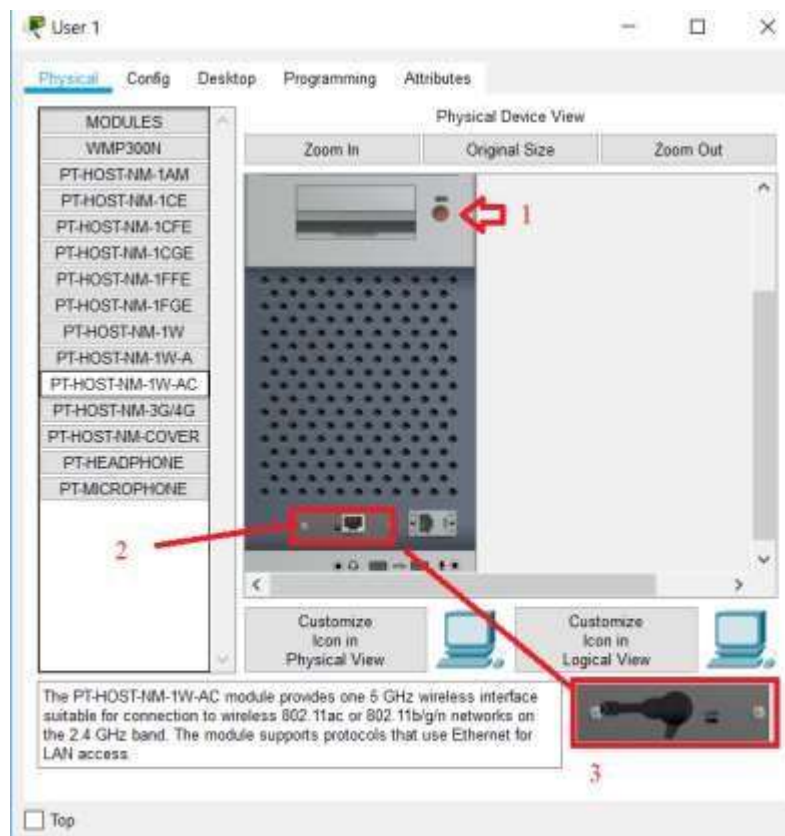
Cisco Packet Tracer dasturida simsiz routerlarida WEP, WPA, WPA2 protokolini sozlash

Dastlab Cisco Packet Tracer dasturi ishga tushiriladi va rasmdagi kabi kompyuterlar, noutbooklar, smartfon va sizmiz router tanlab olinadi.

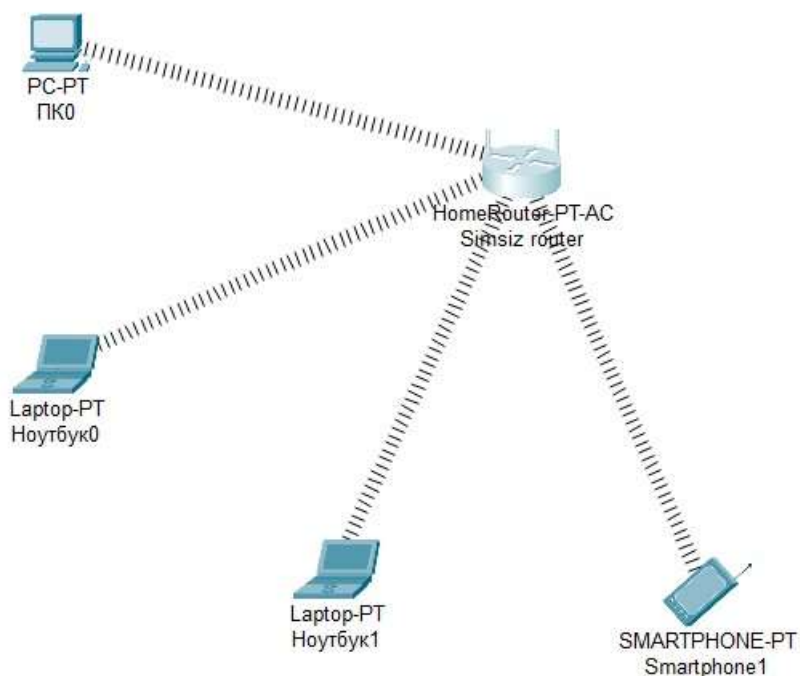


Kompyuter va noutbooklarni simsiz routerga ulanish uchun qurilmalarda simsiz adaptarni ulab qo'yish kerak. Buning uchun kompyuter tanlanadi. "Physical" bo'limiga o'tiladi:

1. Kompyuter o'chiriladi;
2. Kompyuter pastki qismidagi Ethernet adapter olinadi;
3. Simsiz tarmoq adapter kompyuterga joylanadi va kompyuter qayta yoqiladi.

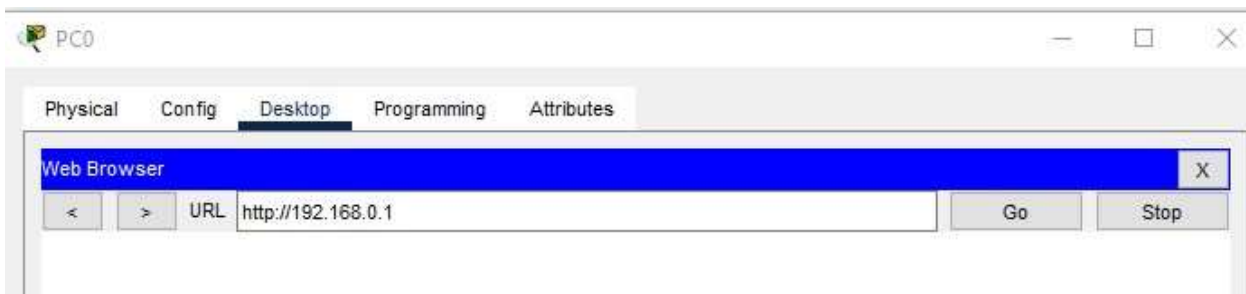


Shu tariqa qolgan qurilamalarga ham simsiz tarmoq adapter joylanadi. Natijada hamma qurilamalar simsiz routerga ulangani aks etadi.

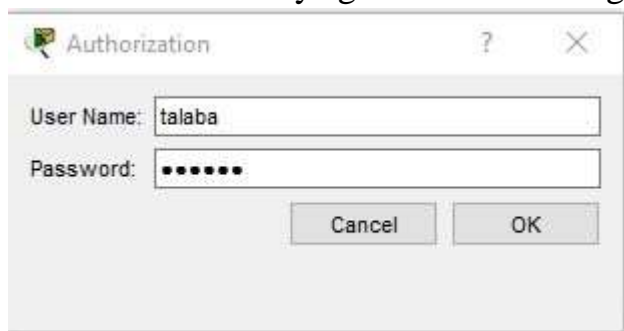


1. Kompyuter tanlanadi.

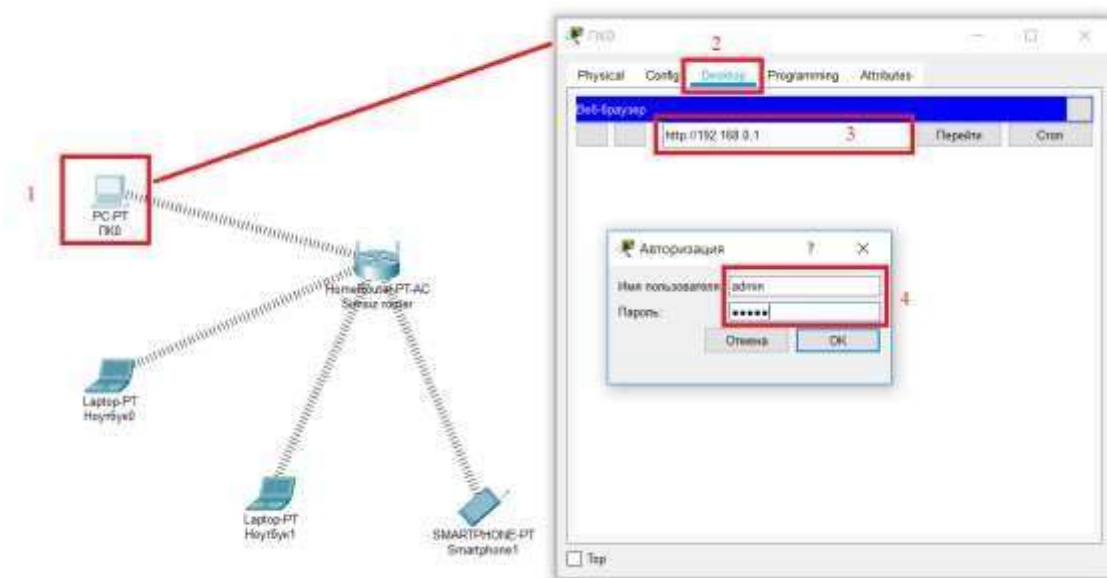
2. “Desktop” bo’limiga o’tiladi. “Web brauzer” bosiladi.
3. Manzillar oynasiga http://192.168.0.1 manzil kiritiladi.



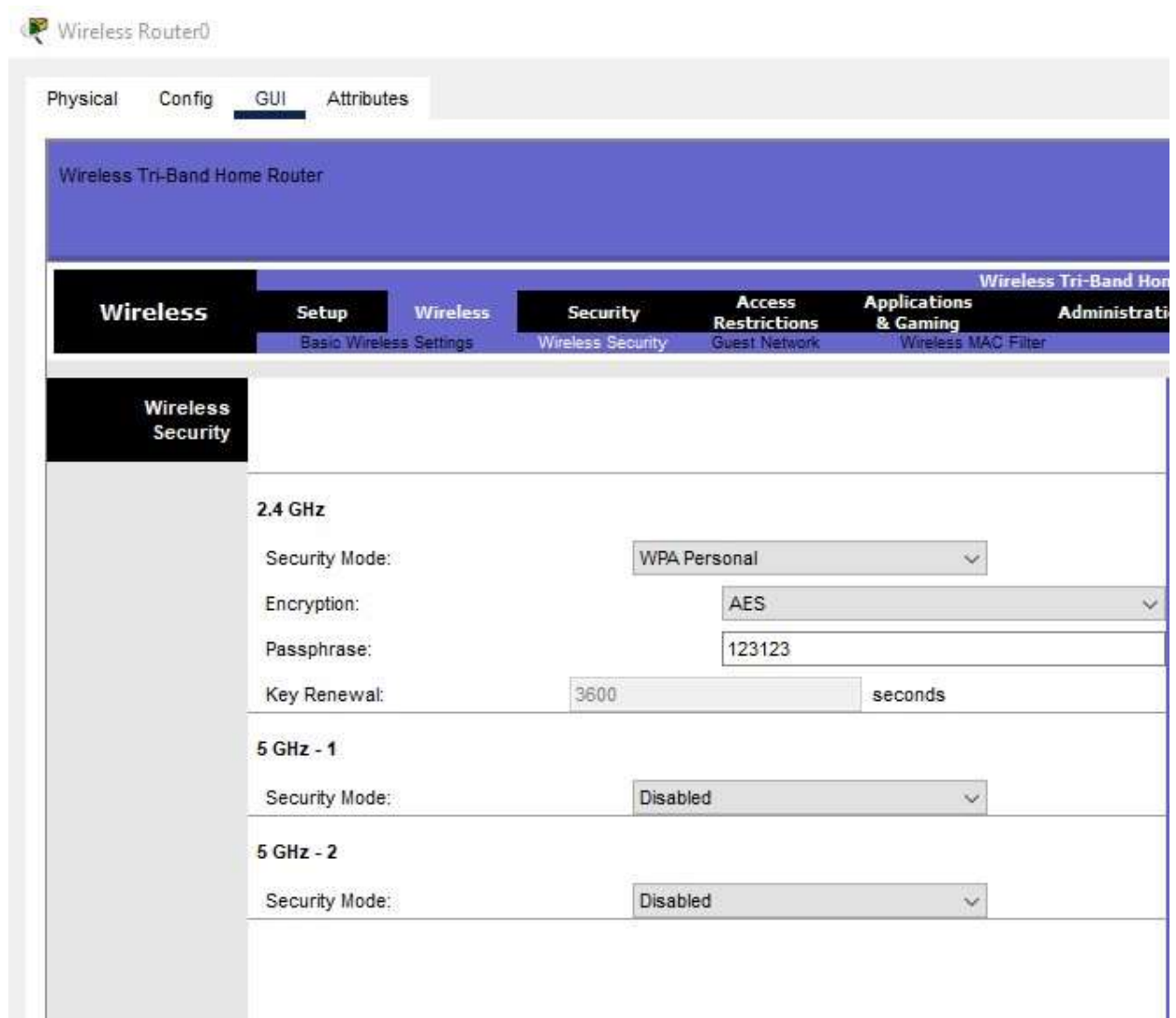
4. Simsiz router interfeysiga kirish uchun login va parol kiritish so’raladi.



5. Foydalanuvchi wi-fi admin va parolini kiritadi va OK tugmasi bosiladi.



Wi-Fi interfeysiga o’tilgach “Wireless” tanlanadi, keyin “Wireless Security” belgilanadi. Shifrlash turini AES tanlanadi. Parol oynasiga parol kiritiladi. Masalan: “0123456789”. So’ngra saqlash tugmasi bosiladi.



Natijada qurilamalar simsiz routerga parolni kiritish orqali ulana oladi. 26-laboratoriya

Mavzu: FIREWALL DASTURIY VOSITASINI O'RNATISH VA SOZLASH

Xavfsizlik devori nima?

Xavfsizlik devori - bu barcha kiruvchi va chiquvchi tarmoq trafigini kuzatuvchi va filtrlaydigan va tarmoqqa/tarmoq ichida ruxsatsiz kirishning oldini oladigan qurilma. Tarmoq va dastur xavfsizligini ta'minlashda xavfsizlik devori eng muhim himoya chizig'i hisoblanadi. Har bir xavfsizlik devorida tarmoq ichidagi ma'lumotlar turiga ruxsat berish uchun oldindan belgilangan qoidalar to'plami mavjud; shunga ko'ra, u tarmoq ichidagi kiruvchi trafikka ruxsat beradi yoki rad etadi.



Xavfsizlik devori turlari

Xavfsizlik devori apparat yoki dasturiy ta'minot bo'lishi mumkin.

Uskuna xavfsizlik devori trafikni filtrlash usuliga qarab OSI modelining tarmoq, transport va amaliy qatlamlarida ishlashi mumkin. Agar xavfsizlik devori IP-manzil asosida trafikni filtrlasa, u tarmoq sathida ishlaydi. Agar xavfsizlik devori port raqami asosida trafikni filtrlasa, u transport qatlamida ishlaydi va agar xavfsizlik devori protokol holati yoki ma'lumotlarini tekshirsa, u holda u dastur sathida ishlaydi.

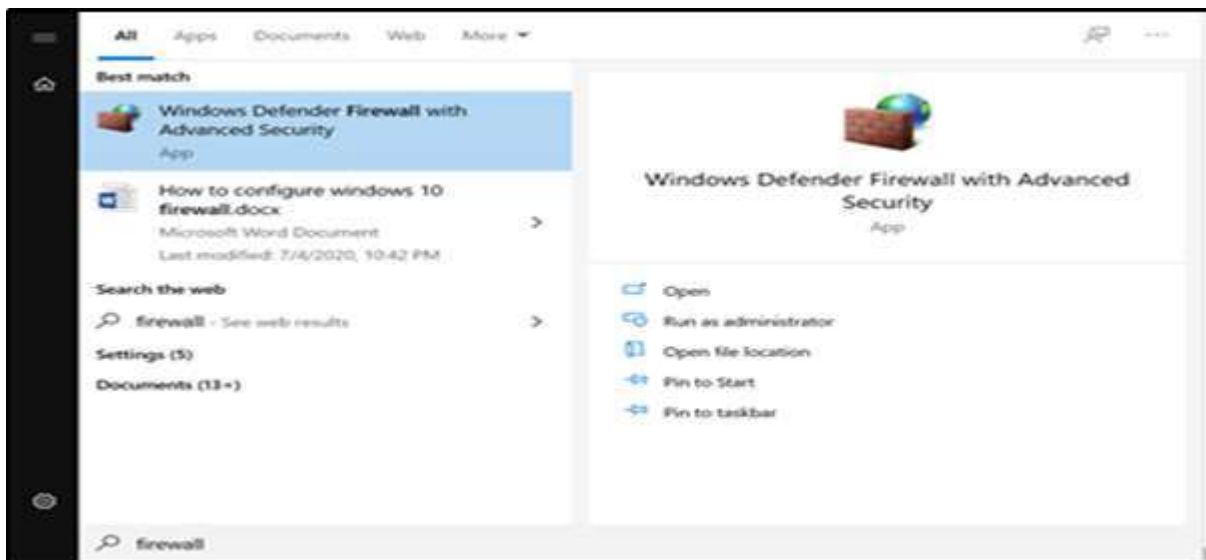
Dasturiy ta'minot xavfsizlik devorlari odatda sukut bo'yicha operatsion tizimga o'rnatilgandir. Mashinada har qanday operatsion tizim (Windows, Mac yoki Linux) o'rnatilganda ular paket sifatida o'rnatiladi, lekin ular unchalik samarali emas va apparat xavfsizlik devorining har tomonlama himoyasini ta'minlamaydi. Har doim korporativ muhitda xavfsizlik devorlarining ikkala turini va shaxsiy tizimlar/noutbuklarda dasturiy xavfsizlik devorlaridan foydalanish tavsiya etiladi.

Windows 10 da xavfsizlik devorlarini sozlash

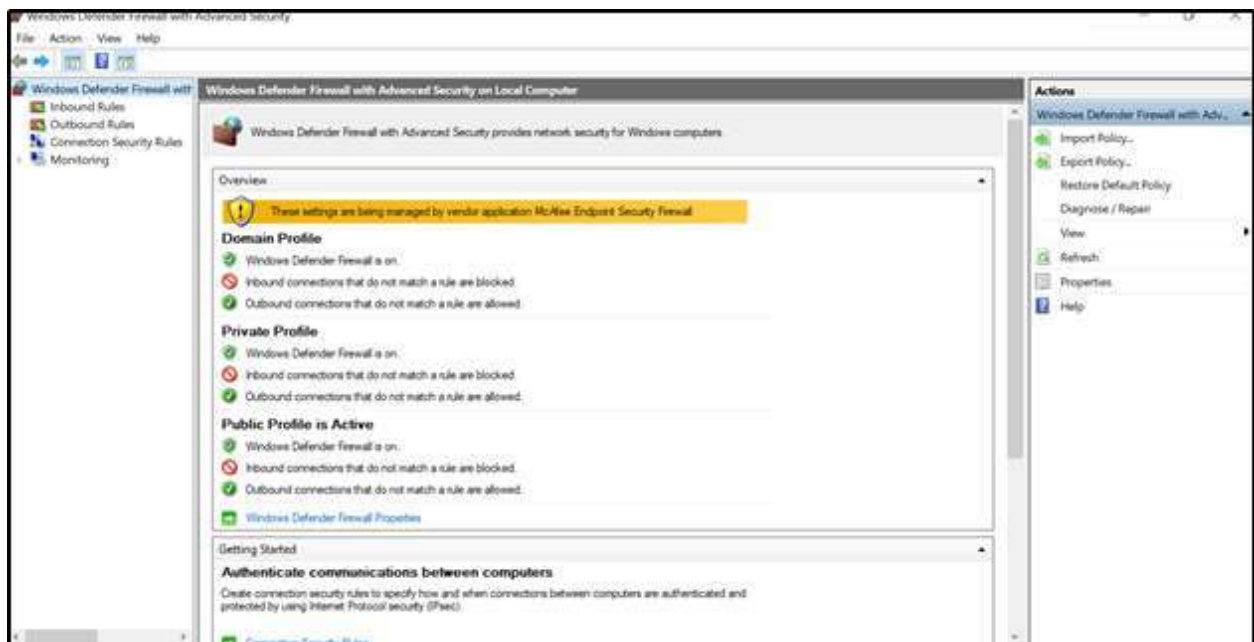
Windows shaxsiy darajada keng qo'llanilganligi sababli, ushbu maqola Windows-da xavfsizlik devorlarini sozlash uchun maxsus yozilgan.

Windows 10 xavfsizlik devorida har qanday maxsus portni ochish uchun bu qadamlar:

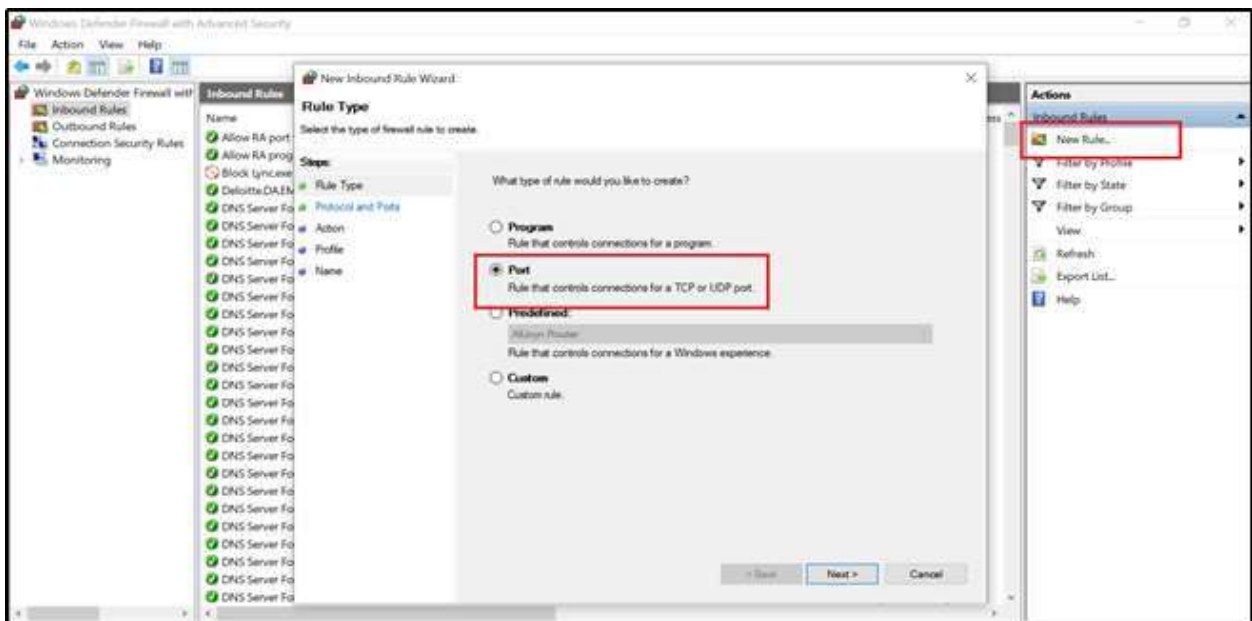
- 1) Quyida ko'rsatilganidek, "xavfsizlik devori" ni qidiring va Windows Defender xavfsizlik devorini bosing:



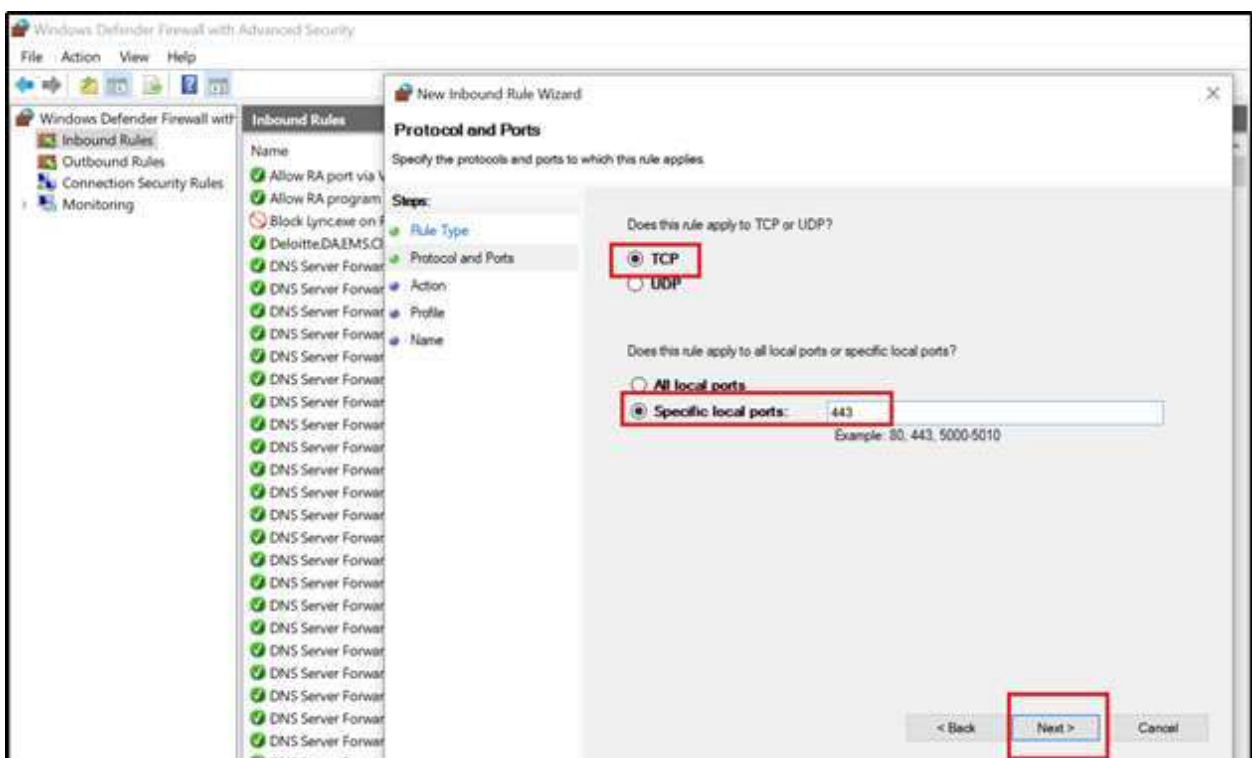
2) Ko'rsatilganidek, Inbound Rules-ni bosing.



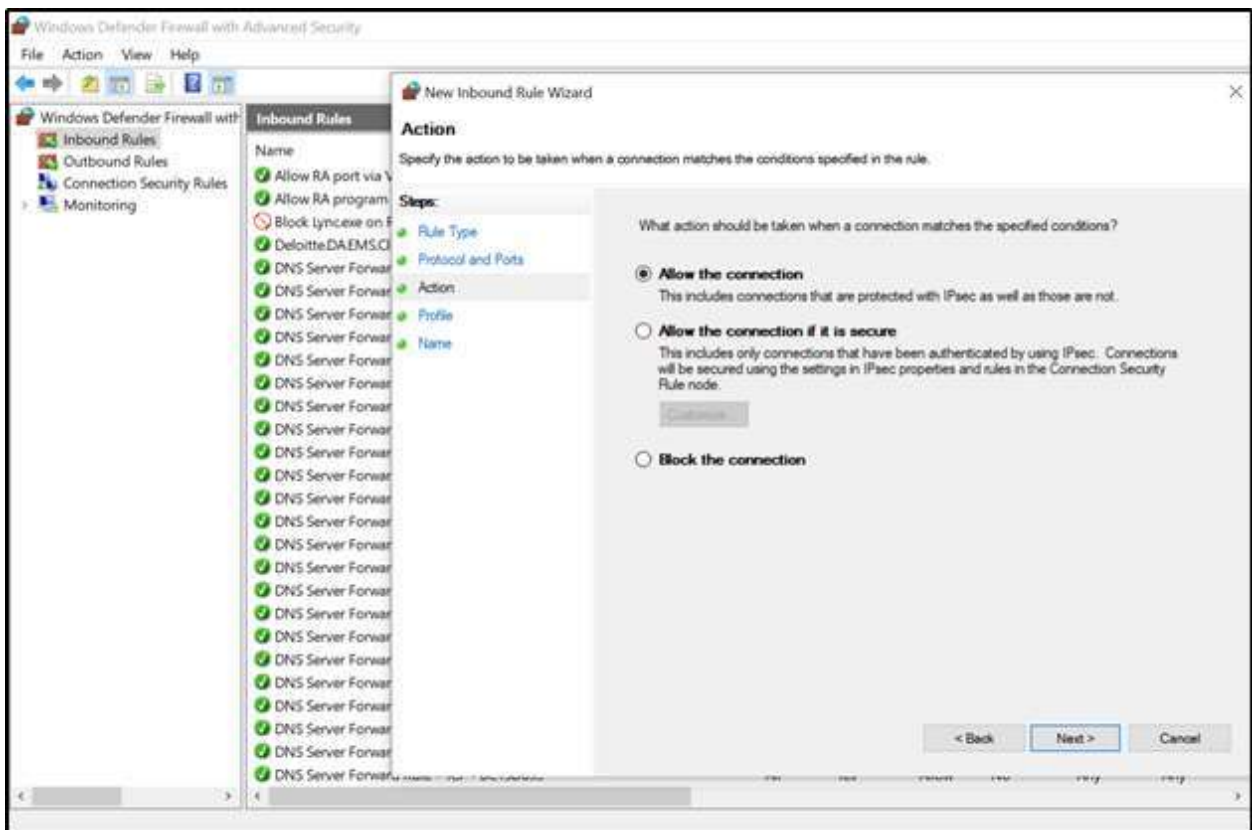
3) Yangi qoidani bosing, portni tanlang va ko'rsatilganidek, Keyingiga bosing:



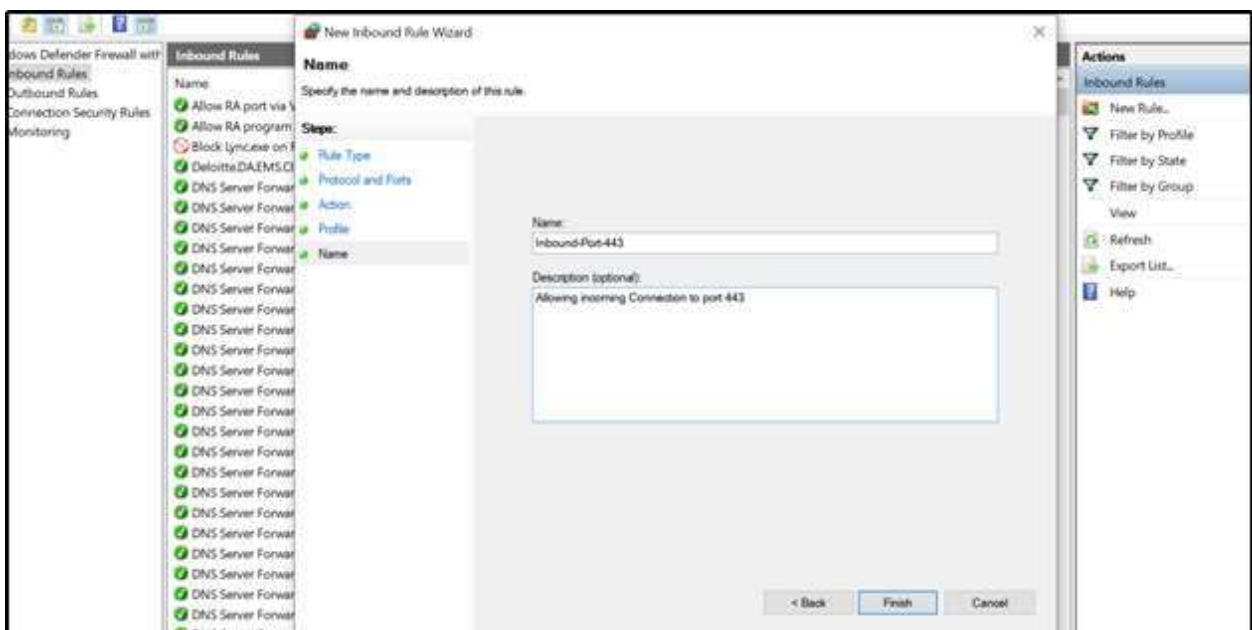
4) Muayyan port raqamini kiriting. Bu holda, bu 443. Keyingiga bosing.



5) Agar kerak bo'lsa, ulanishga ruxsat bering yoki blokirovka qiling.



6) Qoida va tavsifni kerak bo'lganda nomlang.



7) Chiquvchi ulanishga ruxsat berish uchun bir xil amallarni bajarish kerak. Ibosqichda Kiruvchi qoidalarni tanlash o'rniga Chiqish qoidalarini tanlang va yuqoridagi kabi amallarni bajaring.

Windows 10 da ma'lum bir port uchun har qanday ulanishga ruxsat berish yoki rad etish uchun sozlash juda oson.

27-Laboratoriya ishi

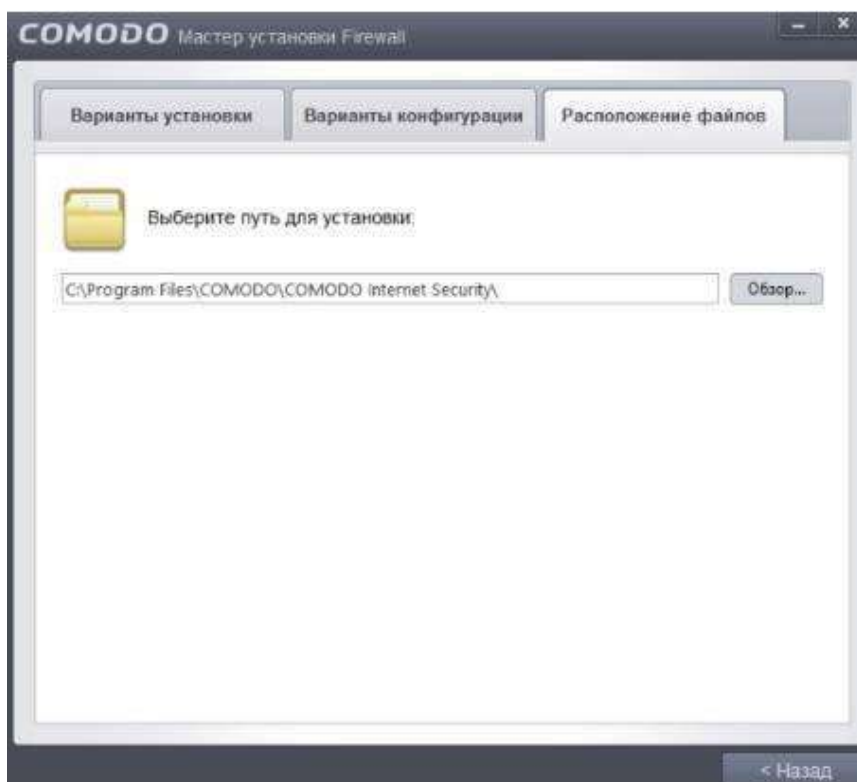
Мавзу: **FIREWALL DASTURIY VOSITASINI O‘RNATISH VA SOZLASH: COMODO INTERNET SECURITY FIREWALL DASTURINI O‘RNATISH VA UNI SOZLASH**

O'rnatish konfiguratsiyasi

Keyinchalik, konfiguratsiya parametrlari yorlig'i haqida:



Agar siz xavfsizlik devorlari bilan ishlashni yaxshi bilmasangiz, bu erda tasdiq belgisini qoldirishga arziydi. Bu sizga keraksiz konfiguratsiyalar va bildirishnomalardan qochish imkonini beradi, biroq ayni paytda **Comodo Firewall statistik ma'lumotlarga asoslanib siz uchun** ba'zi qarorlar qabul qiladi (masalan, ma'lum oddiy ilovalar uchun ulanishga ruxsat berish - **brauzerlar kabi** - va ma'lum zararli yoki shubhali ilovalarni rad etish).



Xo'sh, oxirgi yorliq xavfsizlik devorini o'rnatish fayllari joylashuvini tanlash imkonini beradi. Siz odatdagidek standartni qoldirishingiz yoki o'zingiznikini belgilashingiz mumkin. Keyin, " **Orqaga** " tugmasini bosib va oxirgi bosqichga qayting, bu erda biz birinchi katakchalarni olib tashladik va " **O'rnatishni sozlash** " tugmasini bosdik, bu erda o'z navbatida " **Oldinga** " tugmasini bosib.

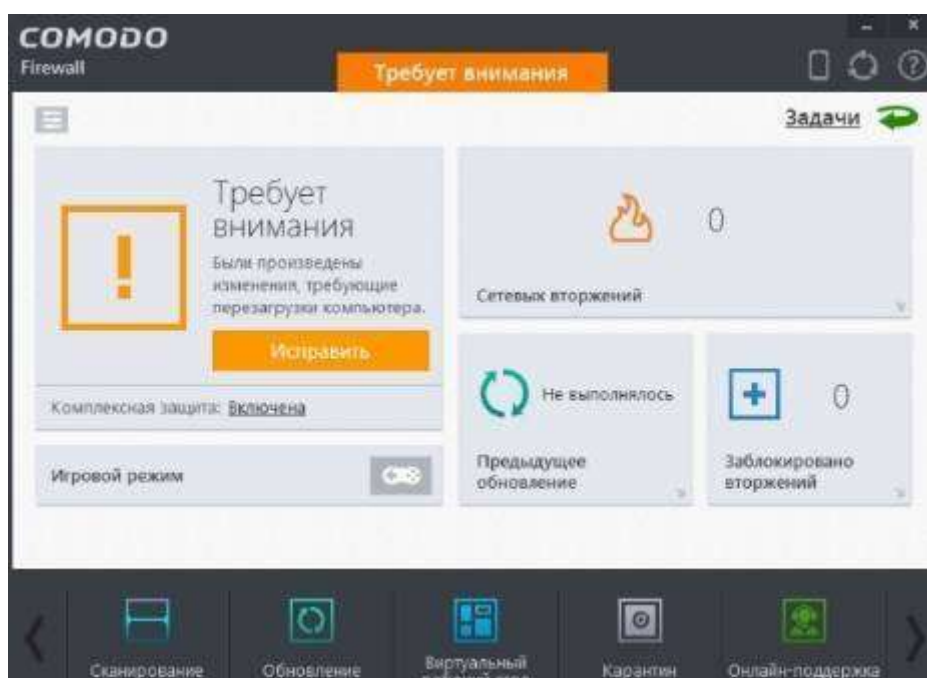
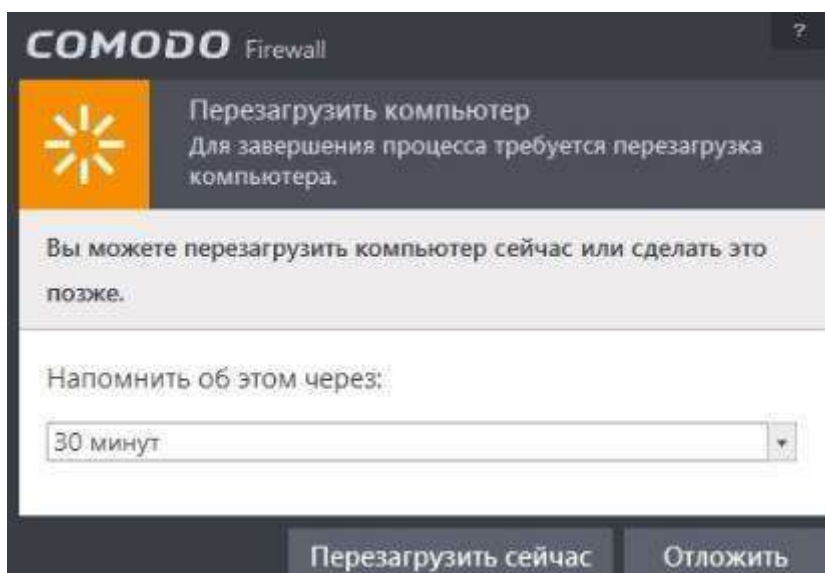


Keyinchalik, biz tasdiqlash qutilari bilan kurashishni davom ettiramiz, chunki bizga **Yandex elementlarini o'rnatish taklif etiladi** , **Yandex** -ni asosiy va umuman boshqa hamma narsaga aylantiring. An'anaga ko'ra, **biz** barcha katakchalarni olib tashlaymiz, albatta, sizga kerak bo'lmasa **Yandex** , va " **Roziman. O'rnatish** " tugmasini bosning.



Shundan so'ng, bepul litsenziya olish va **COMODO Firewall -ni o'rnatish jarayoni boshlanadi** .

Jarayonning oxiri, aslida, kutishga to'g'ri keladi, shundan so'ng xavfsizlik devori zudlik bilan qichqiradi va e'tiborni talab qilishni, qayta ishga tushirishni va boshqa narsalarni boshlaydi va buni bir vaqtning o'zida bir nechta oynada amalga oshiradi:



Xo'sh, siz imtiyozlarga berilishingiz va qayta ishga tushirishga ruxsat berishingiz kerak (sizga kerak bo'lgan hamma narsani yopganingizdan va ish jarayonini saqlaganingizdan so'ng), aks holda xavfsizlik devori normal ishlaymaydi va umuman, sizga ruxsat bermaydi.

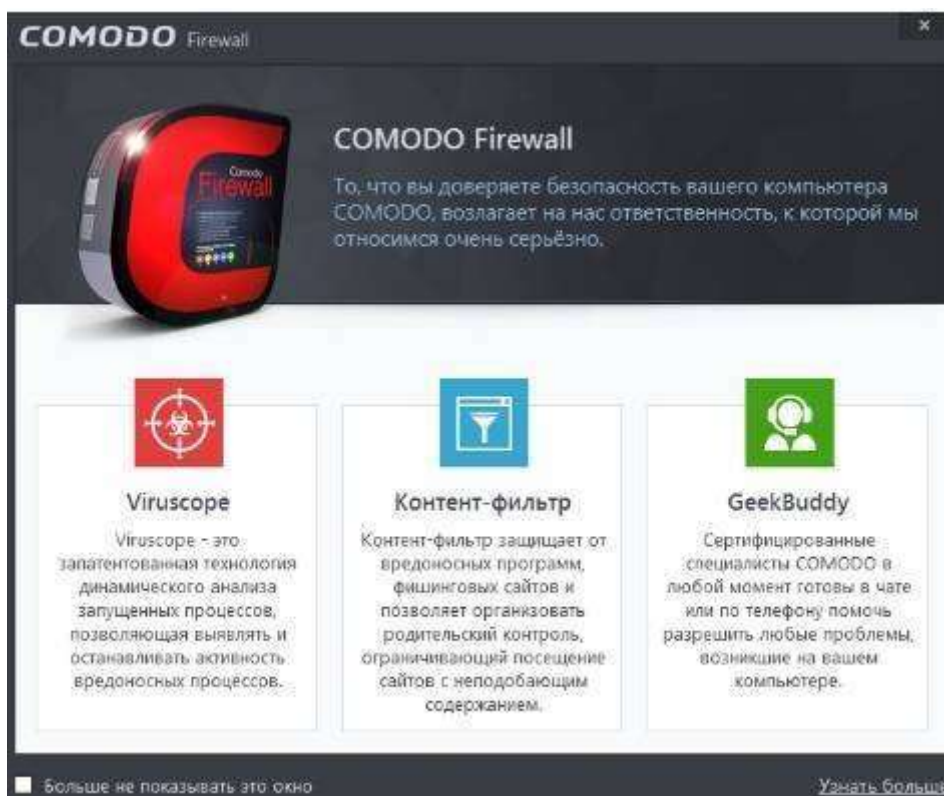
Qayta ishga tushirgandan so'ng, biz foydalanish va keyingi konfiguratsiya bilan shug'ullanamiz.

Dastlabki ishga tushirish va sozlash

O'rnatishdan so'ng, ehtimol siz darhol dasturning kichik (yon) oynasini, **Comodo sizni qanday himoya qilishi haqida bildirishnomani** va avtomatik ravishda ochiladigan ishlab chiquvchining sayтини ko'rasiz. Agar hamma narsa yaxshi bo'lsa, unda hamma narsa shunday ko'rinadi:

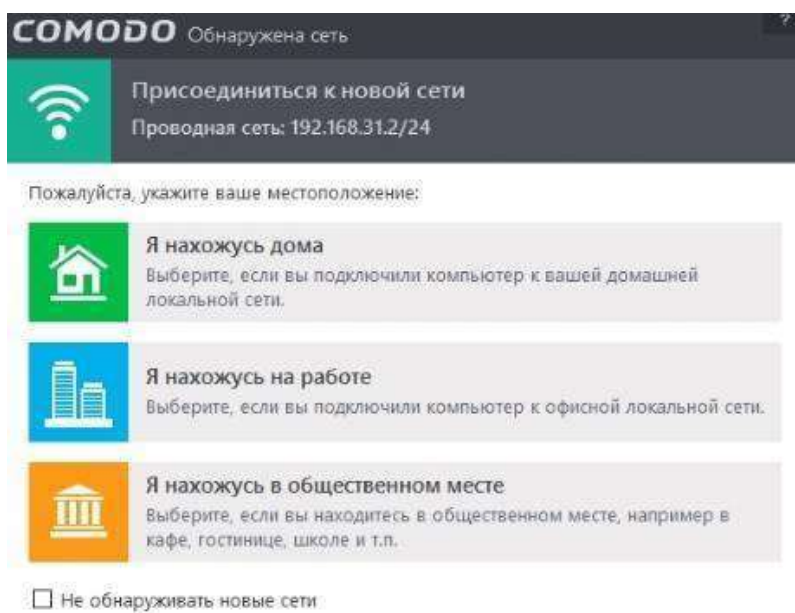


Bu oynani boshqa ko'rsatma " katagiga belgi qo'yishingiz mumkin , chunki bunga ehtiyoj yo'q, o'z-o'zini tarbiyalashdan tashqari:



xavfsizlik darajasiga va ichki sozlamalarga bog'liq bo'lgan elementlar to'plamiga

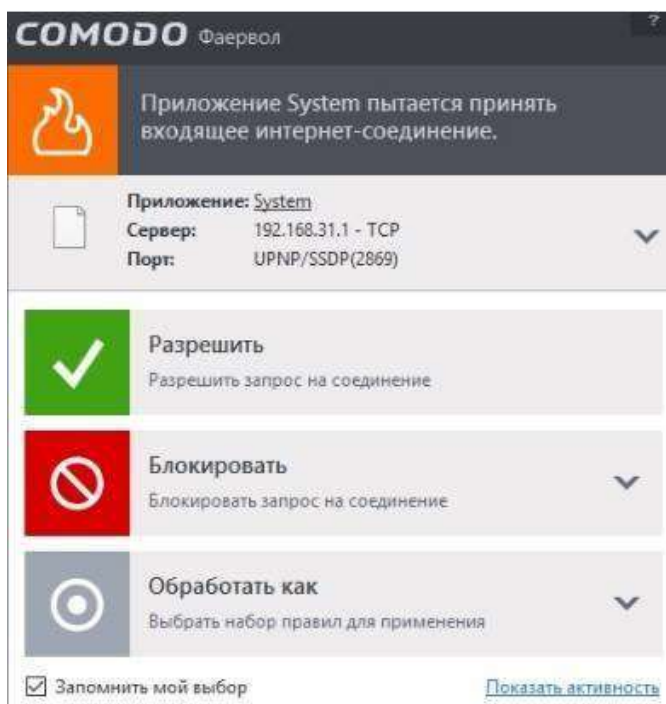
ega bo'lgan tarmoq haqida xabar olasiz :



Tanlovni oqilona qilish kerak, to'g'rirog'i, qayerdan turib, halol tan olish kerak. Yoki, agar sizda ba'zi xavotirlar bo'lsa va maxfiylik darajasi haqida qayg'urayotgan bo'lsangiz, uchinchi bandni, ya'ni " **Men jamoat joyidaman** " ni himoya qilish nuqtai nazaridan eng kuchlisi sifatida tanlang.

Comodo xavfsizlik devori so'rovlarini boshqarish

Ikkinchi turdagi bildirishnomalar turli dasturlarning biror narsa yoki kimdir bilan ulanishga urinishlari, shuningdek, biron bir sababga ko'ra biror narsa qilish haqida bo'ladi. Bu shunday ko'rinadi:

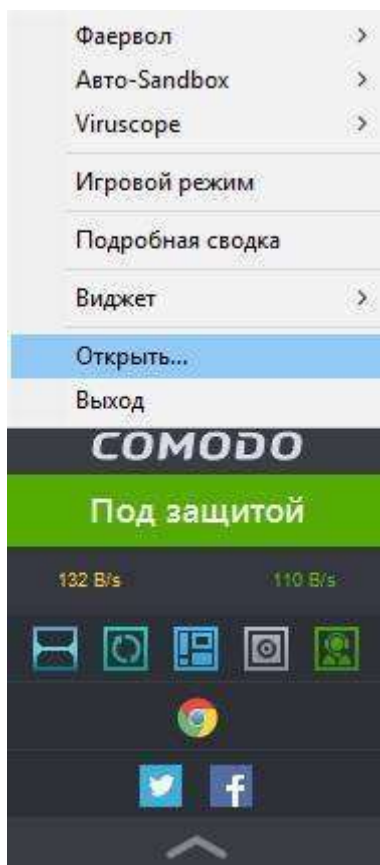


Bunday so'rovlarni qayta ishlash mantig'i oddiy: agar siz qanday dastur (masalan, brauzer) biror narsaga ulanishga yoki biror narsani bajarishga harakat qilayotganini bilsangiz, unda siz nima ekanligini umuman bilmasangiz, harakatni bajarishga ruxsat berasiz. bema'nilik sodir bo'lmoqda (internetdagi qidiruvdan foydalangandan keyin ham va hokazo), ya'ni dastur qoidalaridan biriga muvofiq blokirovka qilish yoki qayta ishlash mantiqan.

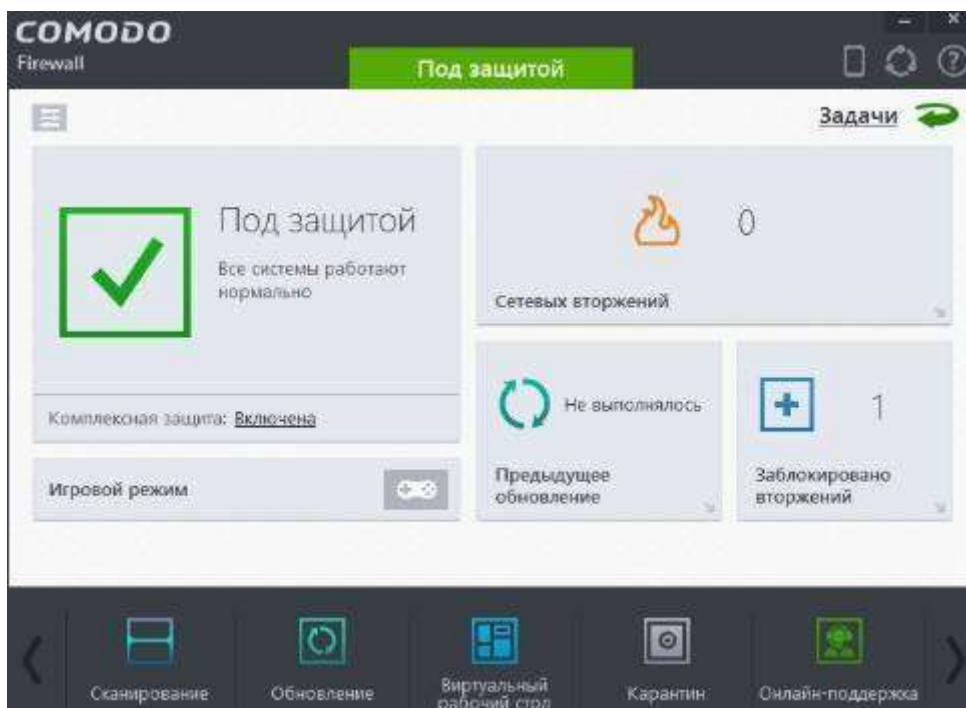


Keyinchalik, dasturning asosiy oynasiga o'tish mantiqan. Buni kichik oyna (sichqonchaning o'ng tugmasi - " **Ochish** ") yoki laganda belgisi (ikkinchisi trafik yoki xavfsizlik devori logotipini ko'rsatish uchun o'zgartirishi mumkin) yordamida amalga oshirish mumkin:



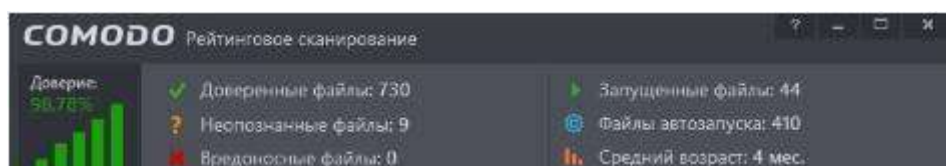
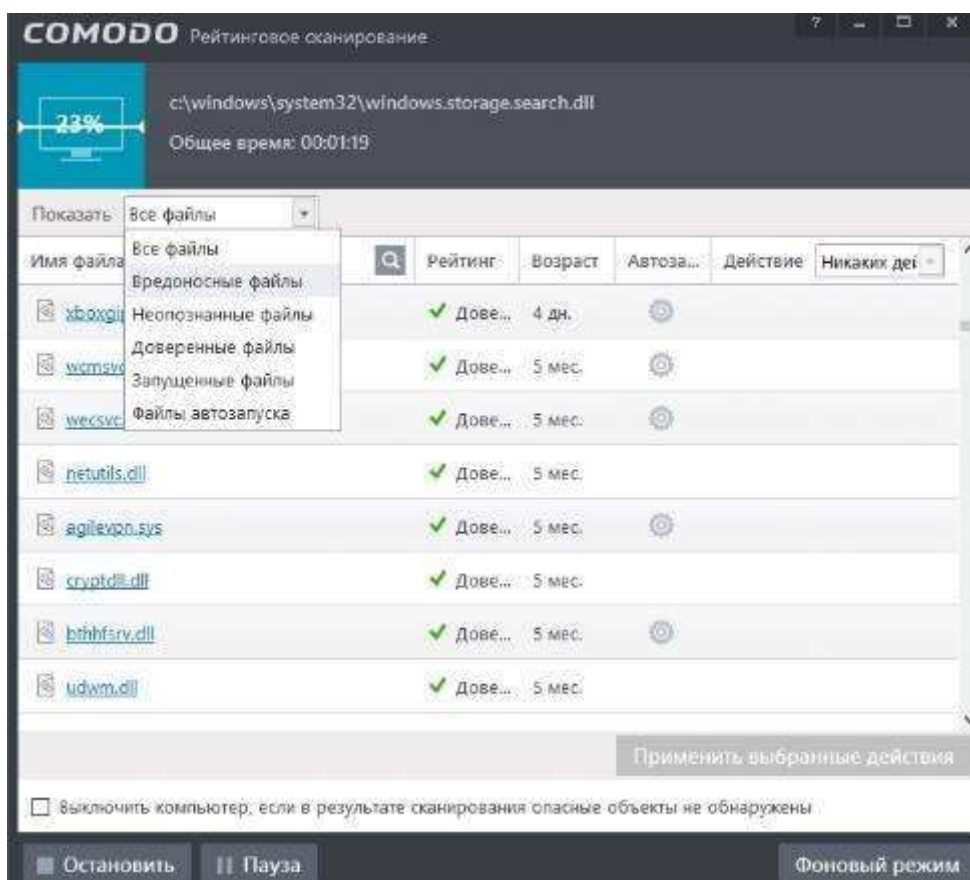


Dasturning asosiy oynasi juda vizual, o'rta darajada ixcham ko'rinadi va aslida kerakli ma'lumotlarning ko'p qismini o'z ichiga oladi. Yangilash jarayonidan boshlash mantiqiy bo'lishi mumkin, garchi siz dasturni ishlab chiquvchining saytidan o'rnatgan bo'lsangiz, u holda versiya dastlab eng so'nggi bo'lishi kerak:



Tugmalar hammasi standart bo'lib, ularning har biri tegishli funkcionallik uchun javobgardir. Masalan, " **Scan** " tugmasi , aslida, kompyuteringizni tahdidlar uchun

skanerlash va tizimda qanday fayllar mavjudligi va ularga ishonish kerakligi haqida batafsil ro'yxat-hisobotni chiqarish imkonini beradi:



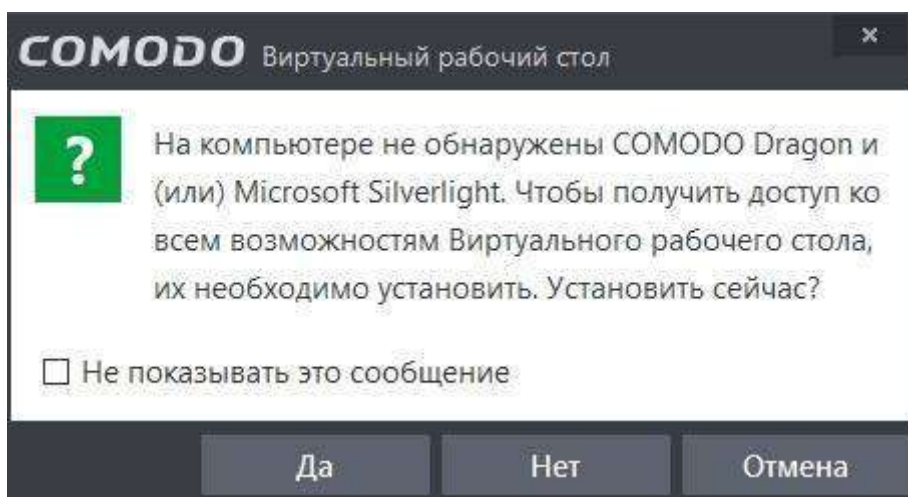
Biz allaqachon yangilanishlar haqida gapirgan edik, shuning uchun biz qo'shimcha **ekran tasvirini olmaymiz**, chunki yangilanish yangilanish uchun javobgardir va bu borada hech qanday murakkab narsa yo'q. [tarkibga qaytish](#) ↑

Izolyatsiya qilingan muhit va boshqa tafsilotlar

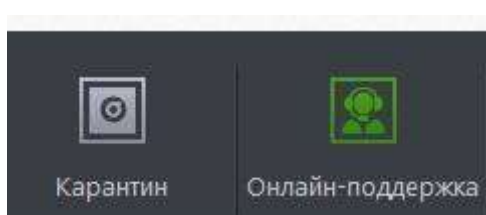
Virtual ish stoli tugmasi xavfli joylarda yurishingiz mumkin bo'lgan izolyatsiya qilingan muhitni ishga tushirishga imkon beradi.



Mantiqiy va ishlash printsiplari nuqtai nazaridan, u Windows funksionalligiga asoslangan bunday **VirtualBoxga o'xshaydi, shuningdek**, kengaytirilgan, o'rtacha kattalar shaklida sandboxga (masalan, **Sandboxie**) juda o'xshaydi. Juda foydali narsa, biz paranoidlar uchun tavsiya qilamiz.



Tegishli tugma yordamida ish stollari o'rtasida tez va juda og'riqsiz o'tish mumkin bo'ladi, bu qulay. Aytgancha, yuqorida aytilganlarning barchasini o'rnatish (**Silverlight** va **Comodo Dragon**) to'liq ish uchun zaruriy funktsiya emas, lekin shunday tavsiya etiladi.

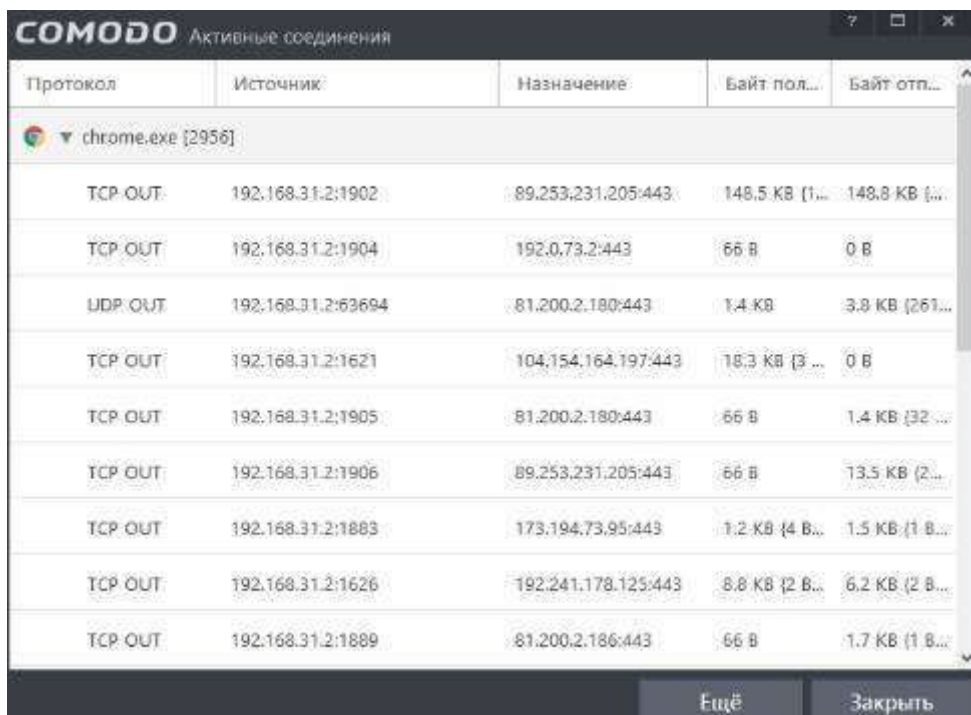


Karantin yorlig'i karantin, onlayn yordam uchun onlayn yordam uchun javobgardir. Umuman olganda, g'ayrioddiy narsa yo'q va biz ular haqida to'xtalmaymiz. Yuqori chap burchakdagi tugma nima sodir bo'layotganining batafsil xulosasini ko'rish imkonini beradi:



Ya'ni, kiruvchi va chiquvchi ulanishlar sonini ko'ring, jarayonlarni blokirovka qiling, barcha turdagi Auto -**Sandbo** x, **HIPS** va **Viruskopni yoqing yoki o'chiring** va allaqachon bloklangan, izolyatsiya qilingan va hokazolarni boshqaring.

Tegishli, aytaylik, havolani bosish sizga ma'lumotni batafsilroq ko'rish yoki sozlamalarni ochish imkonini beradi. Masalan, tizimdagi ulanishlar haqidagi ma'lumotlar qanday ko'rinishga ega (**TCPViewni eslatadi** va hokazo):



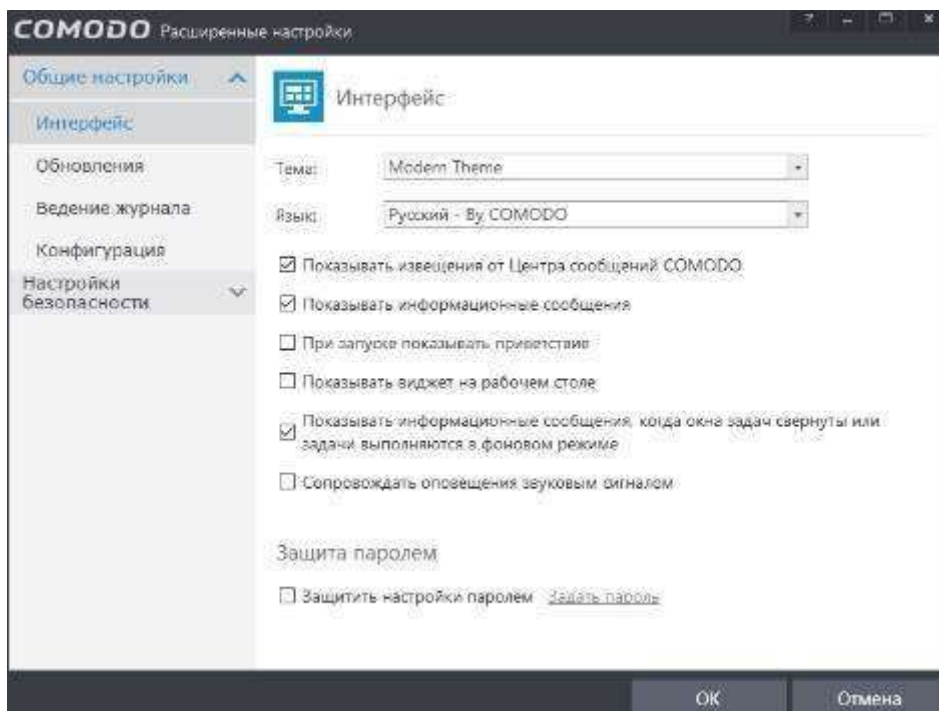
Протокол	Источник	Назначение	Байт пол...	Байт отп...
chrome.exe [2956]				
TCP OUT	192.168.31.2:1902	89.253.231.205:443	148.5 KB (1...	148.8 KB (...)
TCP OUT	192.168.31.2:1904	192.0.73.2:443	66 B	0 B
UDP OUT	192.168.31.2:63694	81.200.2.180:443	1.4 KB	3.8 KB (261...
TCP OUT	192.168.31.2:1621	104.154.164.197:443	18.3 KB (3 ...)	0 B
TCP OUT	192.168.31.2:1905	81.200.2.180:443	66 B	1.4 KB (32 ...)
TCP OUT	192.168.31.2:1906	89.253.231.205:443	66 B	13.5 KB (2...
TCP OUT	192.168.31.2:1883	173.194.73.95:443	1.2 KB (4 B...	1.5 KB (1 B...
TCP OUT	192.168.31.2:1626	192.241.178.125:443	8.8 KB (2 B...	6.2 KB (2 B...
TCP OUT	192.168.31.2:1889	81.200.2.186:443	66 B	1.7 KB (1 B...

Xavfsizlik devori havolasini bosish, masalan, sozlamalar yorlig'ini va tegishli pastki yorliqni ochishga imkon beradi, ammo bu erda biz kerakli joyga o'tish orqali umuman barcha **sozlamalarni boshqarishimiz mumkin** (masalan, " **Umumiy sozlamalar** " - " **Interfeys** "). Keling, ularni qisqacha ko'rib chiqaylik.

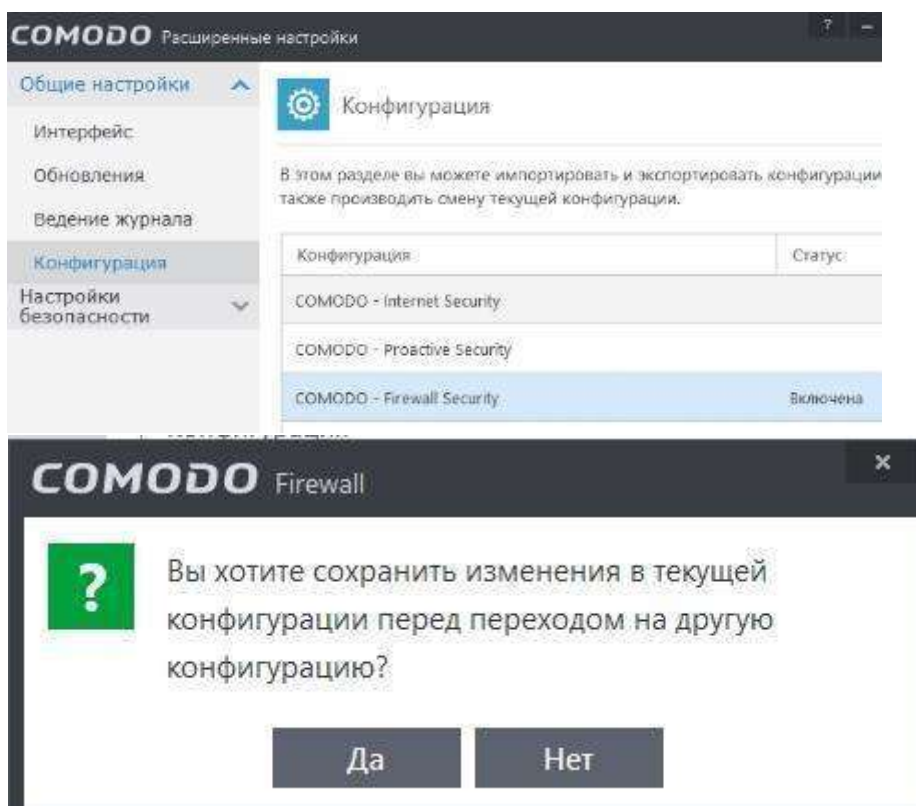
[tarkibga qaytish ↑](#)

Kengaytirilgan sozlash va foydalanish

Interfeysli yorliq, g'alati darajada, interfeys uchun javobgardir. Majburiy emas, siz mavzuni, yana tilni va boshqa dumlarni sozlashingiz mumkin. Bu erda uzoq davom etadigan ovozni, salomlashishni, barcha turdagi bildirishnomalarni va boshqa bezovta qiluvchi funktsiyalarni o'chirish tavsiya etiladi:

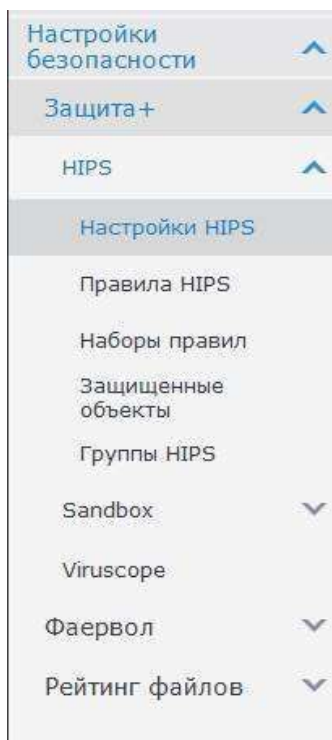


Yangilanishlar mavjud bo'lgan yorliq yangilanishlar chastotasi va jurnal uchun, mantiqiy bo'lsa, jurnalning o'lchami, uni qayta yaratish va hokazolar uchun javobgardir. Bularning barchasi mantiqiy, sodda va o'rnatish oddiy, rus tilida yaxshi, o'ylaymanki, siz buni tushunasiz.



Konfiguratsiya yorlig'ida siz har qanday tayyor konfiguratsiyani yoqishingiz yoki o'chirib qo'yishingiz mumkin. Bu juda va juda qulay va o'tish paytida u mavjud va o'zgartirilgan konfiguratsiyani saqlashga imkon beradi, ya'ni vaziyatga qarab

xavfsizlik darajasini o'zgartirishingiz mumkin. To'g'ri, almashtirish qayta ishga tushirishni talab qiladi, bu umuman mantiqiydir.

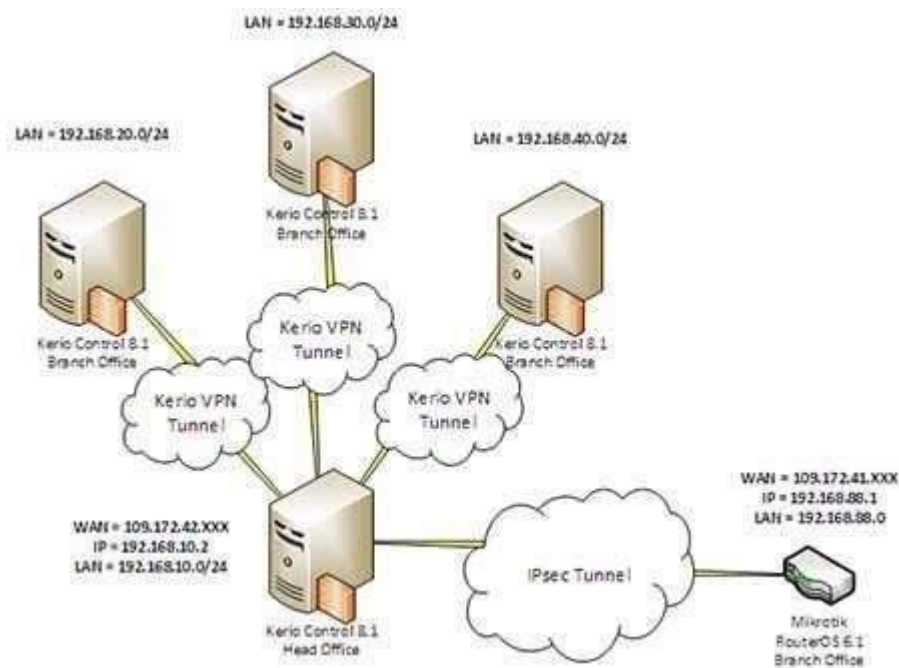


28-29-Laboratoriya ishi

Mavzu: **FIREWALL DASTURIY VOSITASINI O'R NATISH VA SOZLASH:**
KERIO CONTROL TARMOQLARARO EKRAN DASTURINI O'R NATISH VA
SOZLASH

Kerio Control dasturini o'rnatish va sozlash. Kerio Control dasturida lokal
tarmoqni boshqarish Nazariy qism:

Kerio Control - Internet tarqatilishini sozlash.



Trafikning taqsimlanishini to'g'ri sozlash uchun siz Internetga ulanish turini tanlashingiz kerak.

Eng mos keladigan har bir lokal tarmoq uchun tuzilgan. Doimiy kirish ulanishi mumkin, bu funktsiya bilan Internetga doimiy ulanish mavjud.

Agar kerak bo'lsa, ikkinchi variant ulanish bo'lishi mumkin - kerak bo'lganda dastur o'zi ulanishni o'rnatad.

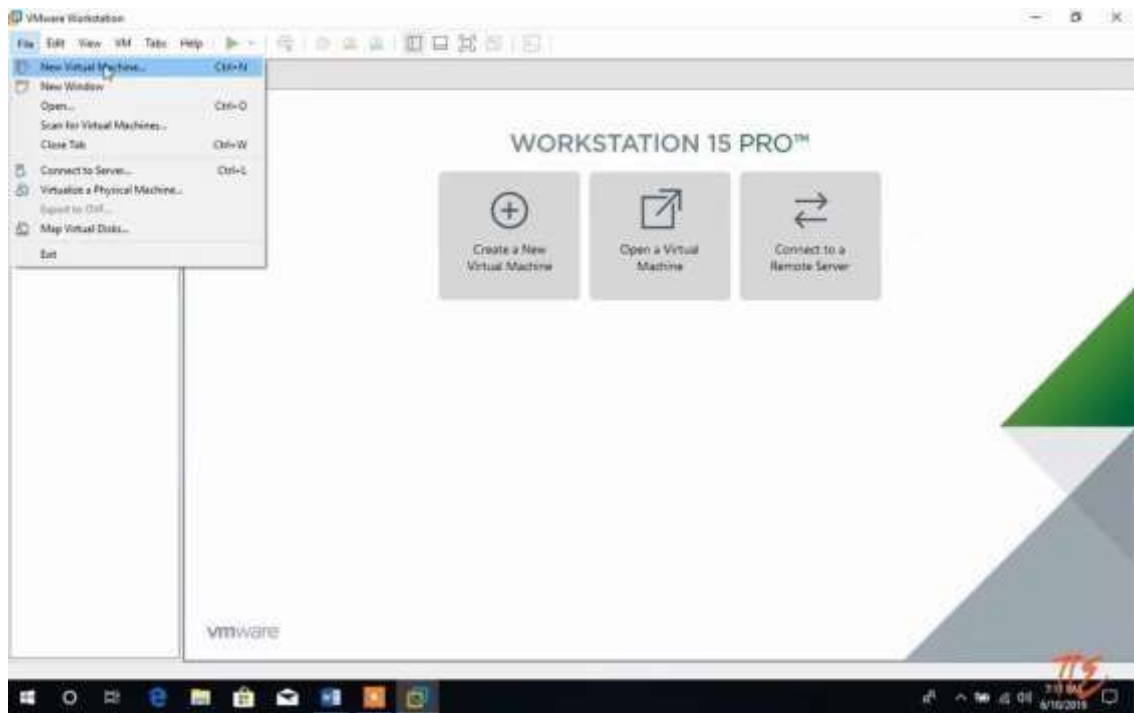
Ikkita ulanish mavjud, Kerio Control Internetga ulanishini yo'qotsa, boshqa kanalga qayta ulanishni yaratadi.

Agar sizda ikkita yoki undan ortiq Internet-kanal mavjud bo'lsa, ulanishning to'rtinchi turini tanlashingiz mumkin. Yuk barcha kanallar bo'yicha teng ravishda taqsimlanadi.

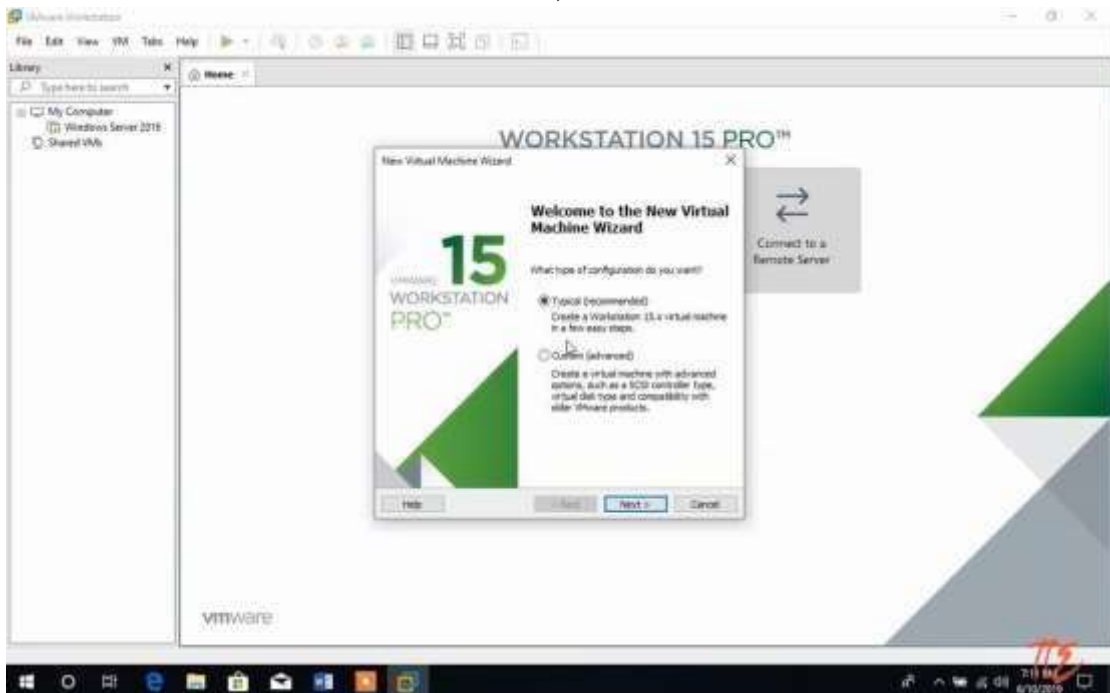
Nazariy qism:

VMware muhitida Kerio Control dasturini o'rnatish

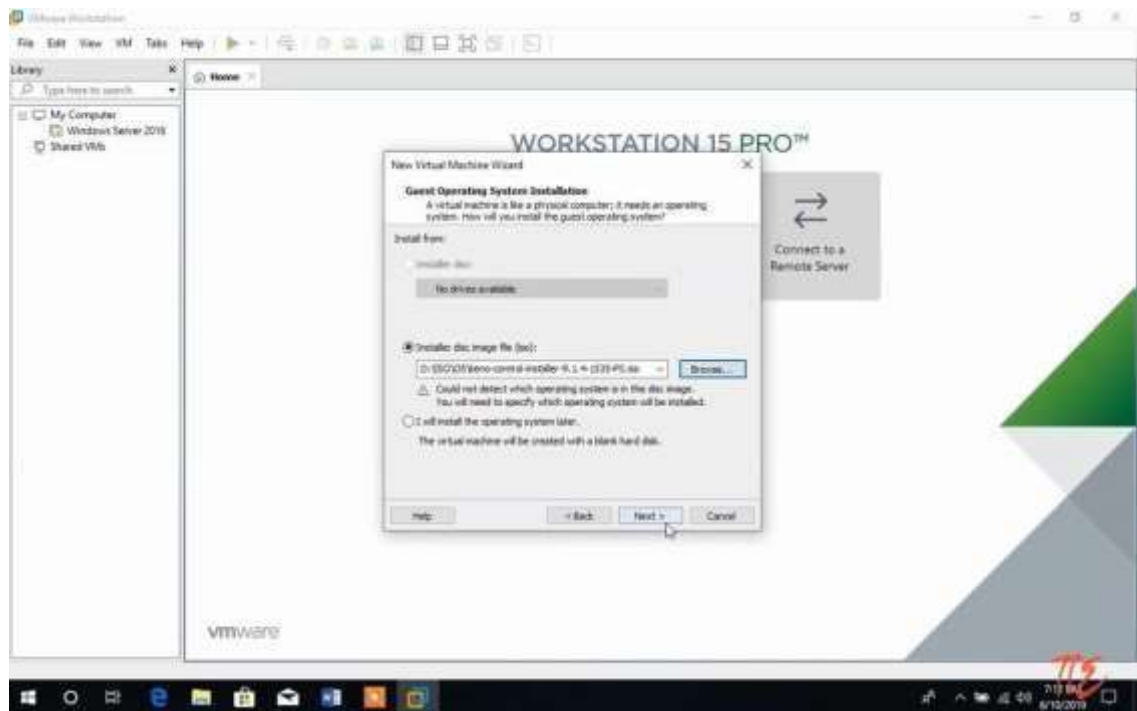
1. VMwareni ishga tushirib, yangi virtual mashina yaratishni bosamiz:



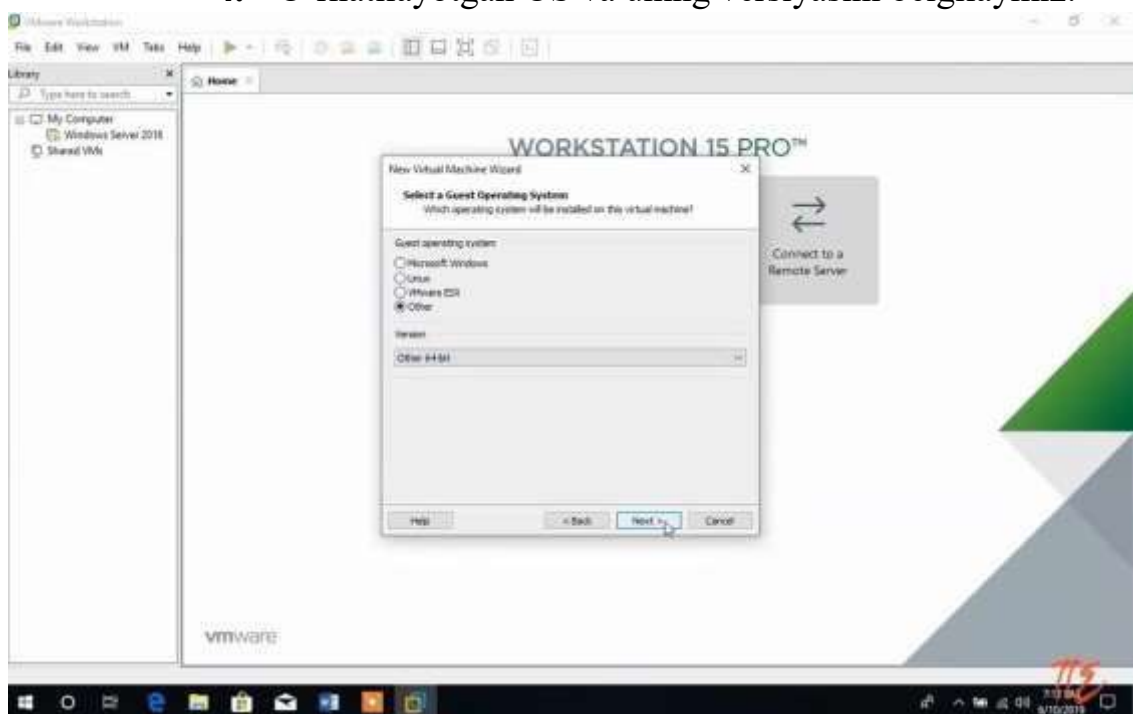
2. Birinchisini tanlab, Next ni bosamiz:



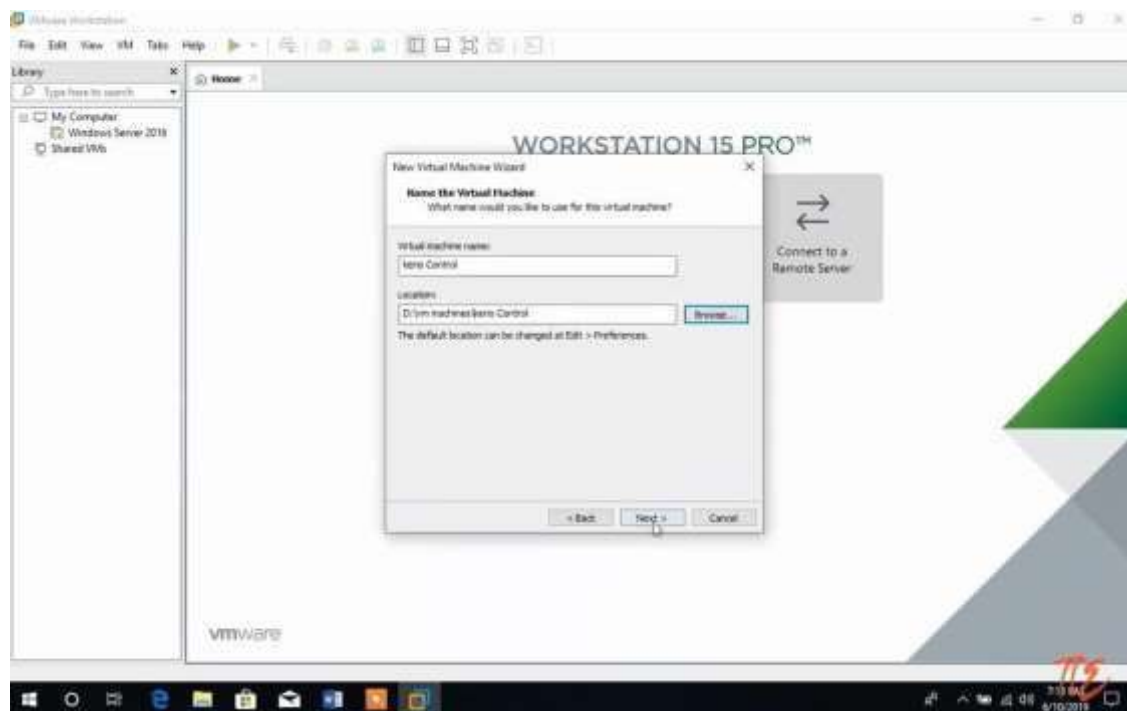
3. Kerio Control dasturining kompyuterimizda joylashgan o'rnini ko'rsatib qo'yamiz:



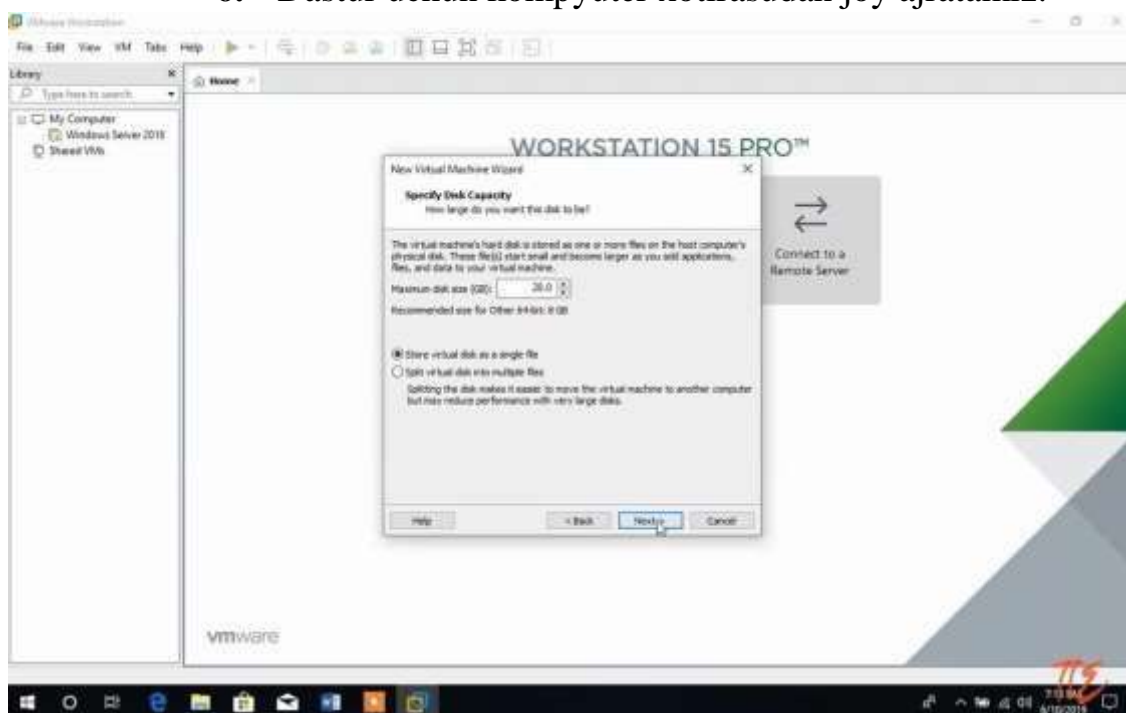
4. O'rnatilayotgan OS va uning versiyasini belgilaymiz:



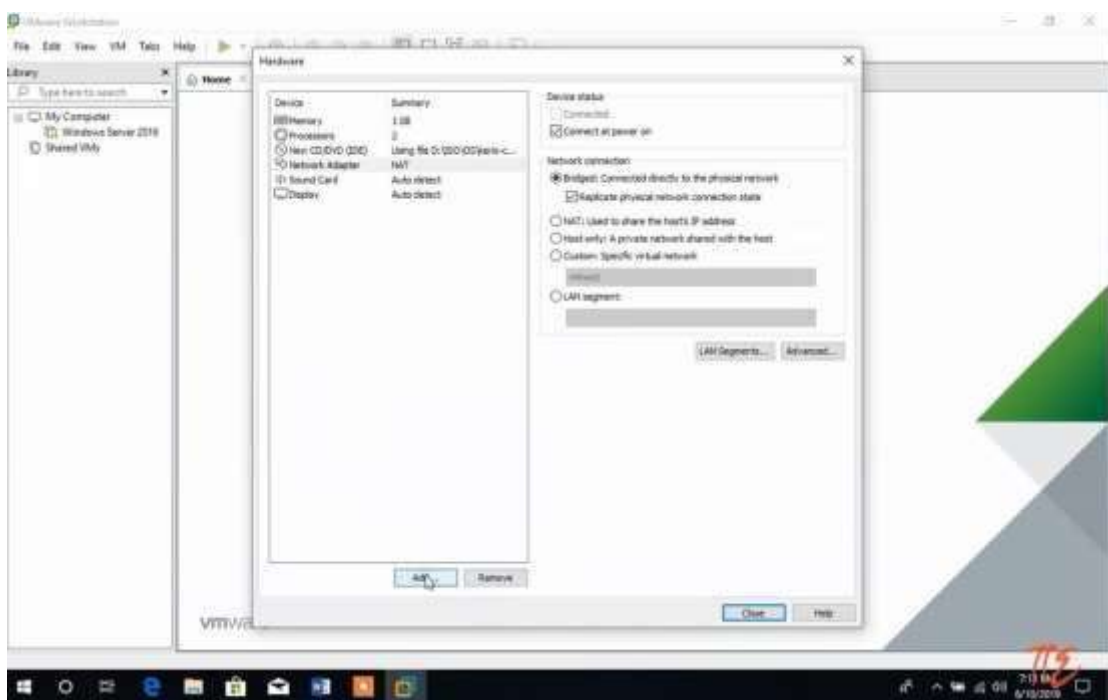
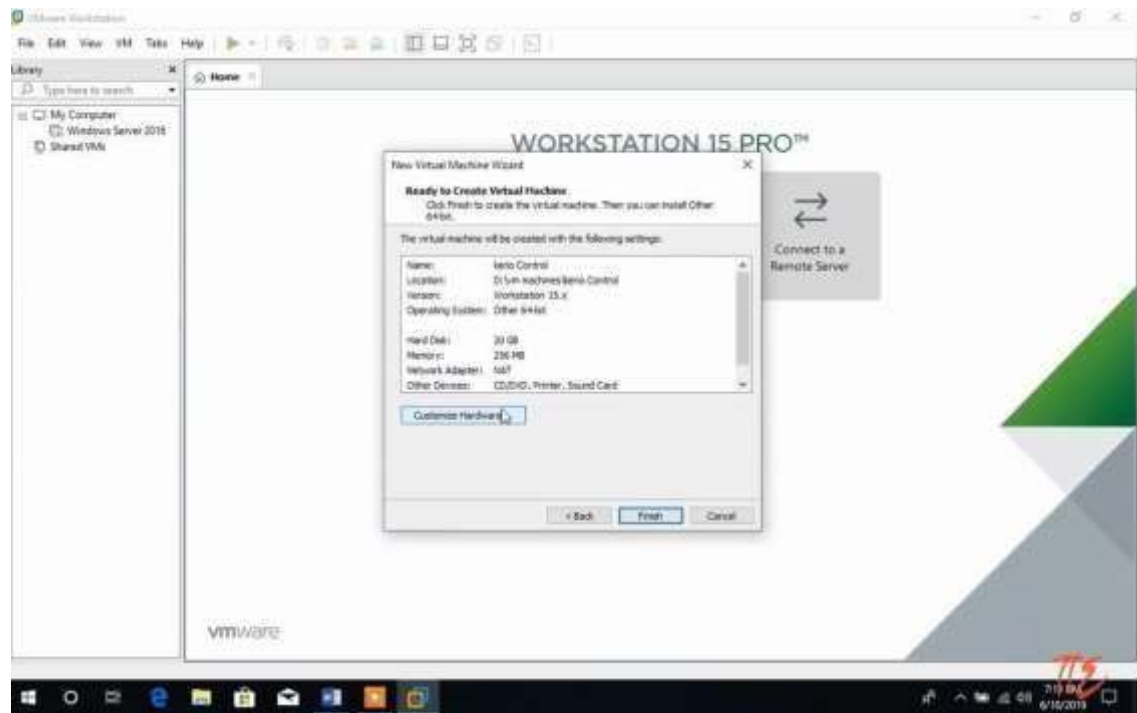
5. Virtual dasturimizga nom beramiz:

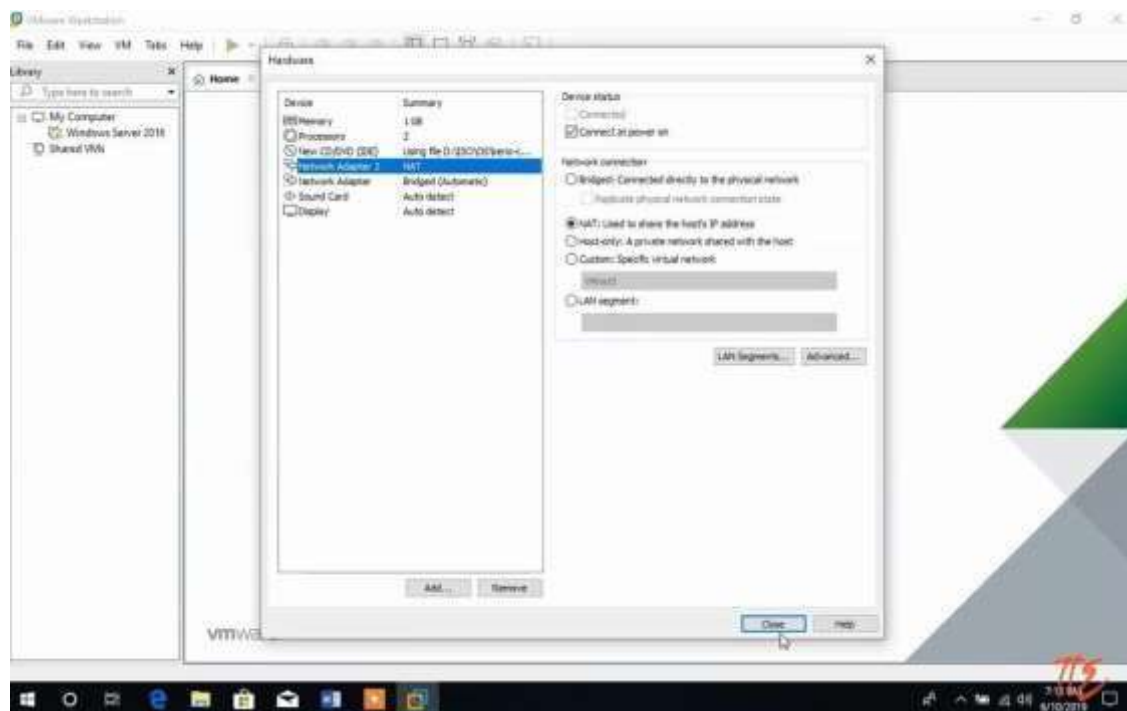


6. Dastur uchun kompyuter xotirasudan joy ajratamiz:

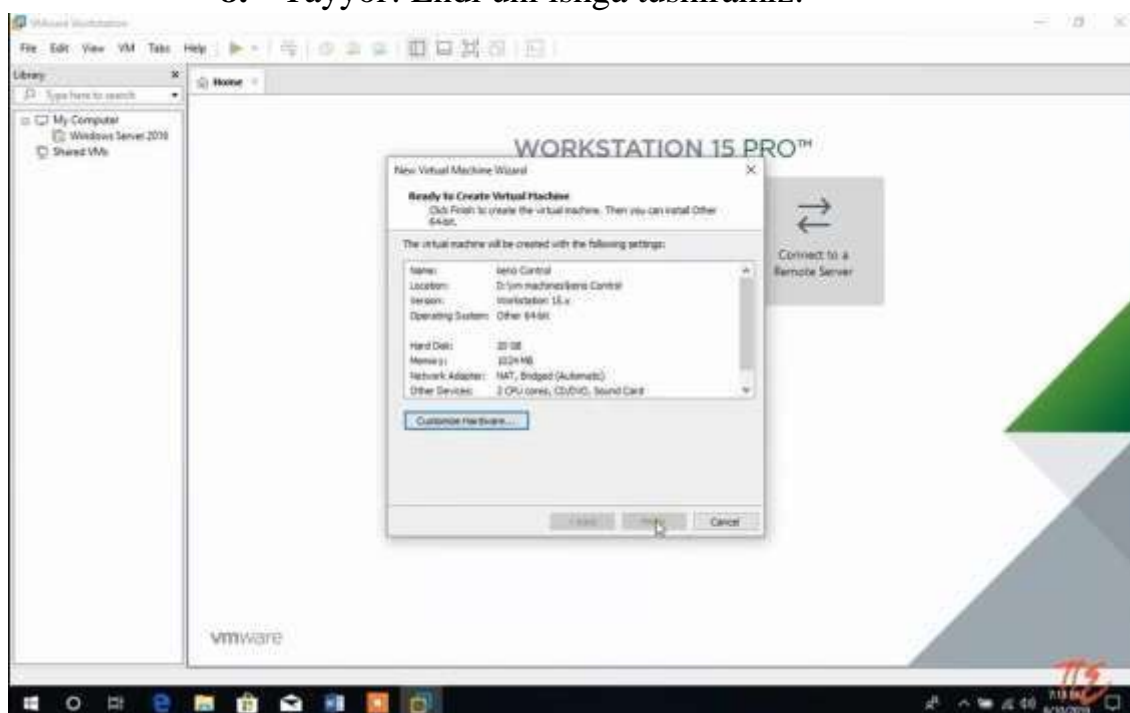


7. Muhit yaratildi. Endi uni ba'zi joylarini sozlab olamiz:

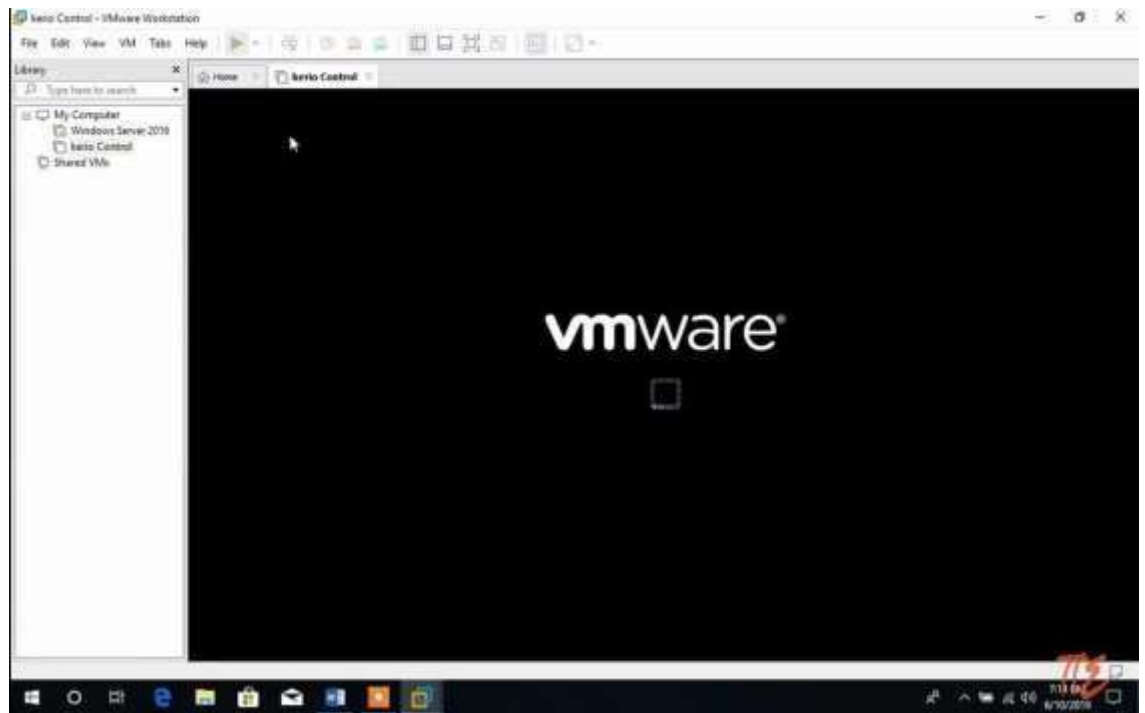




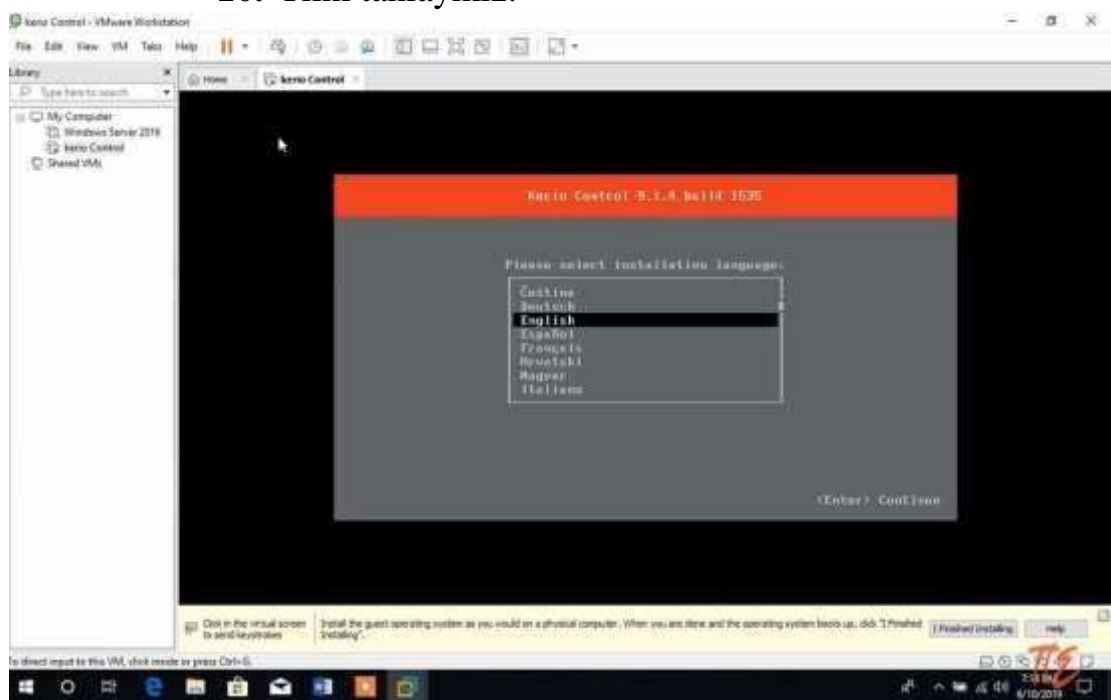
8. Tayyor! Endi uni ishga tushiramiz:

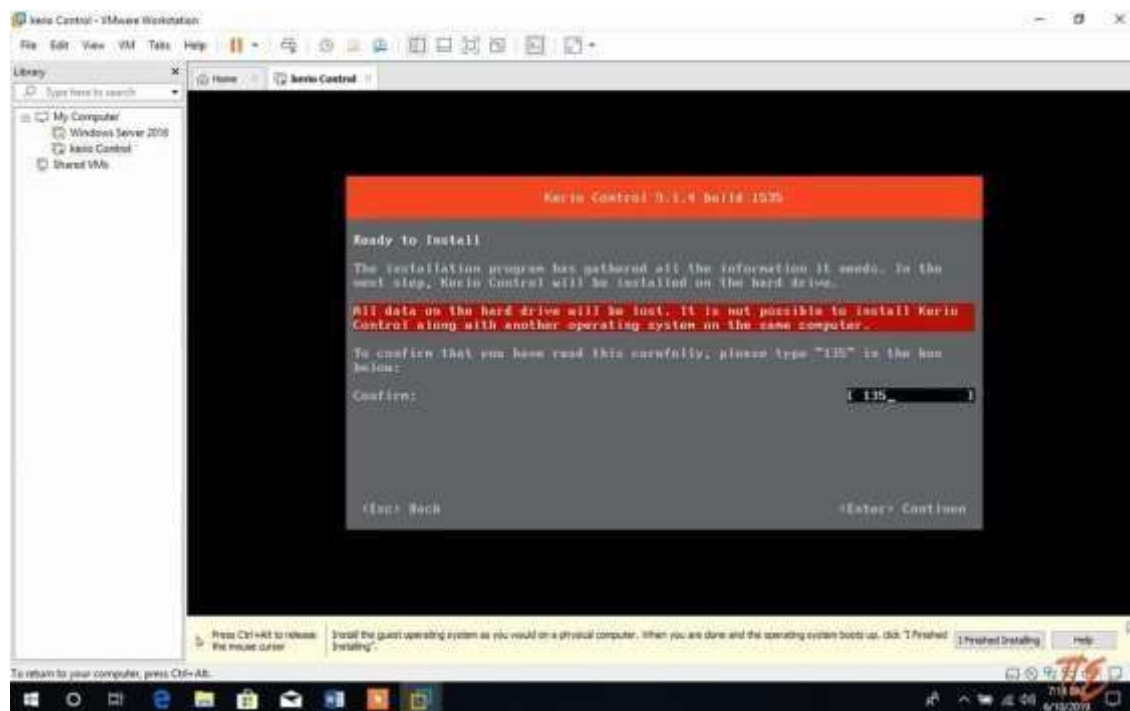


9. Dastur ishlashni boshladi:

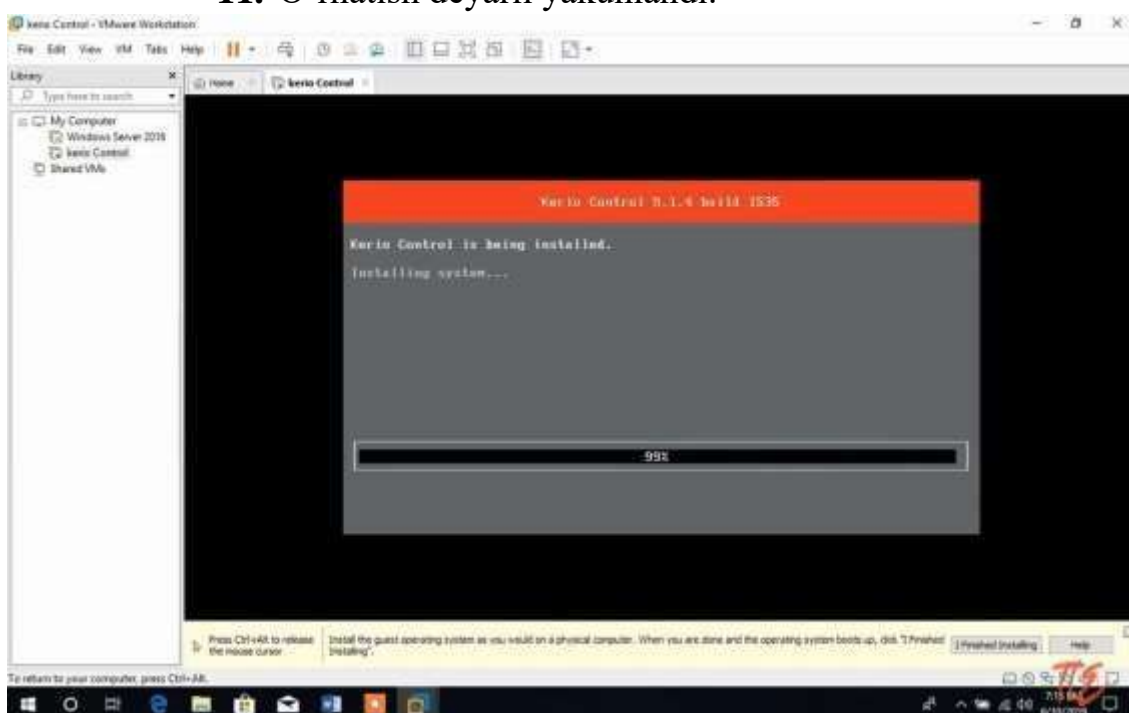


10. Tilni tanlaymiz:

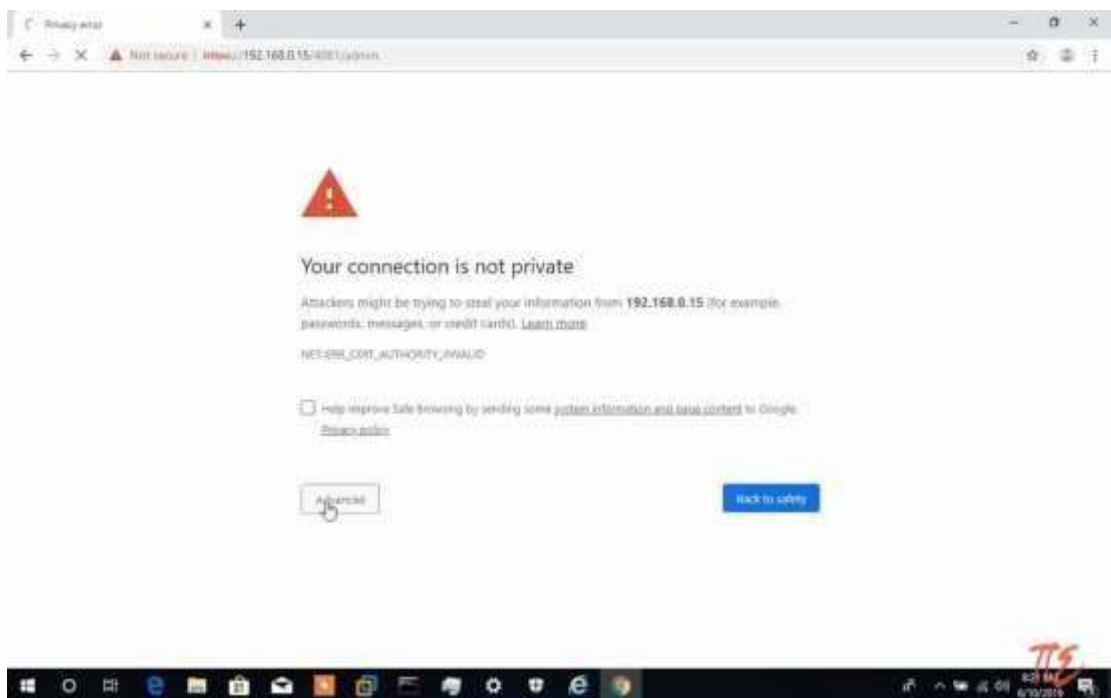
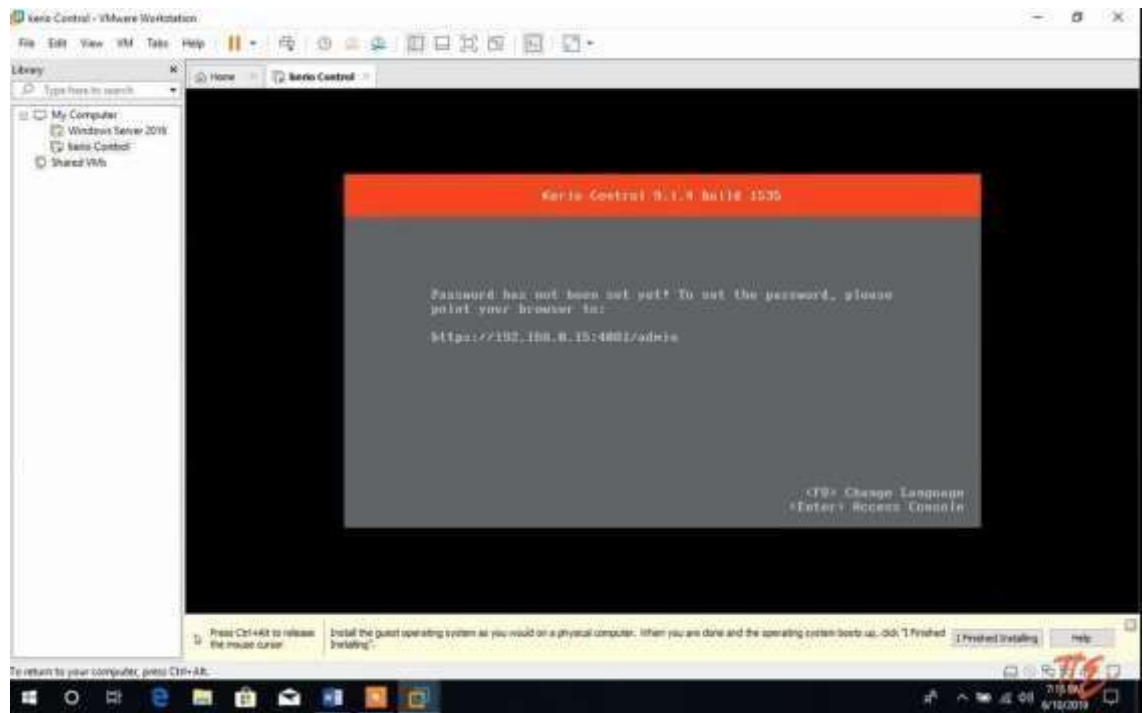


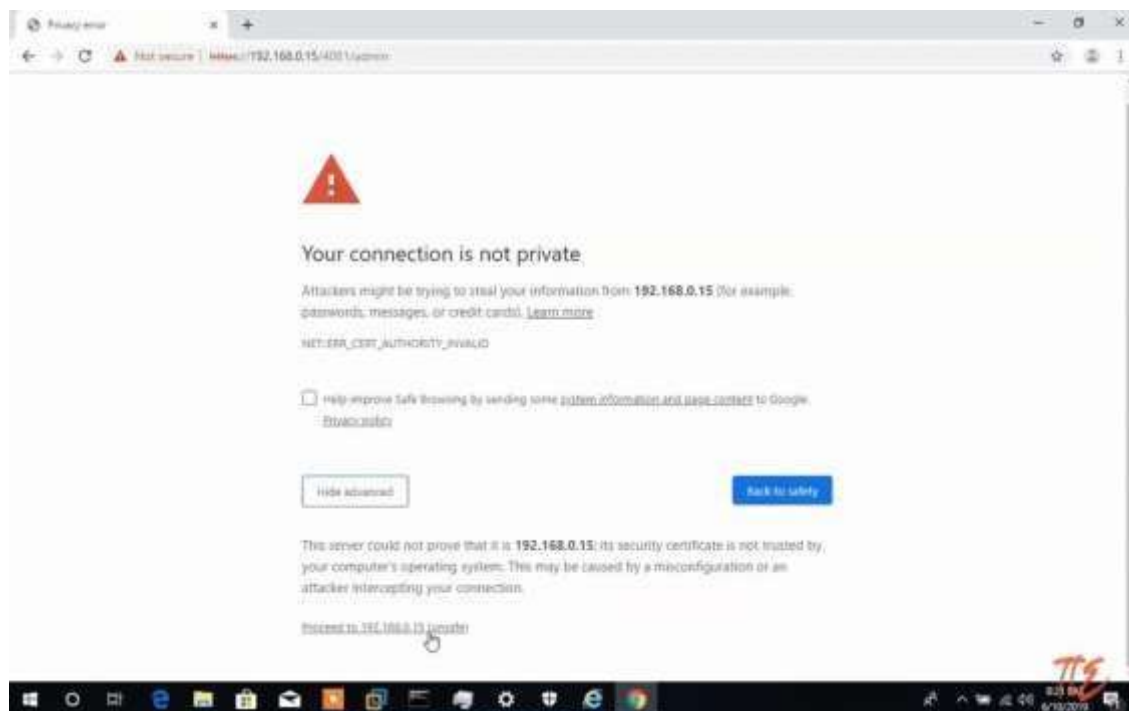


11. O'rnatish deyarli yakunlandi:

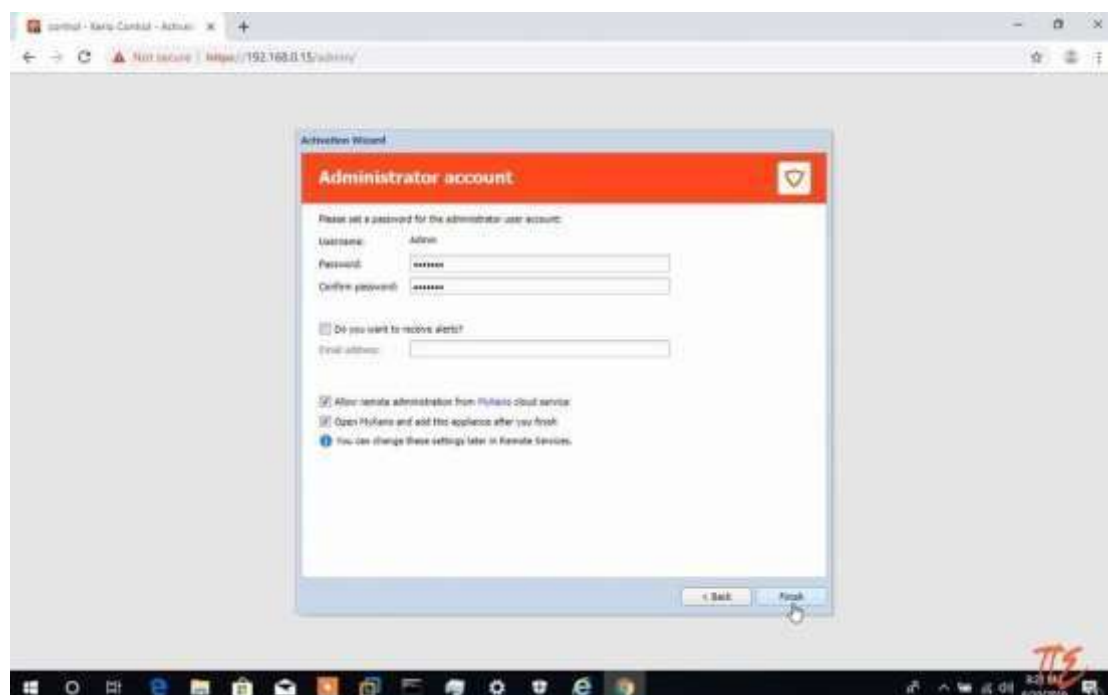


12. Ko'rib turganimizdek u bizga IP-manzil berdi. Uni brauzerga kiritib olami:

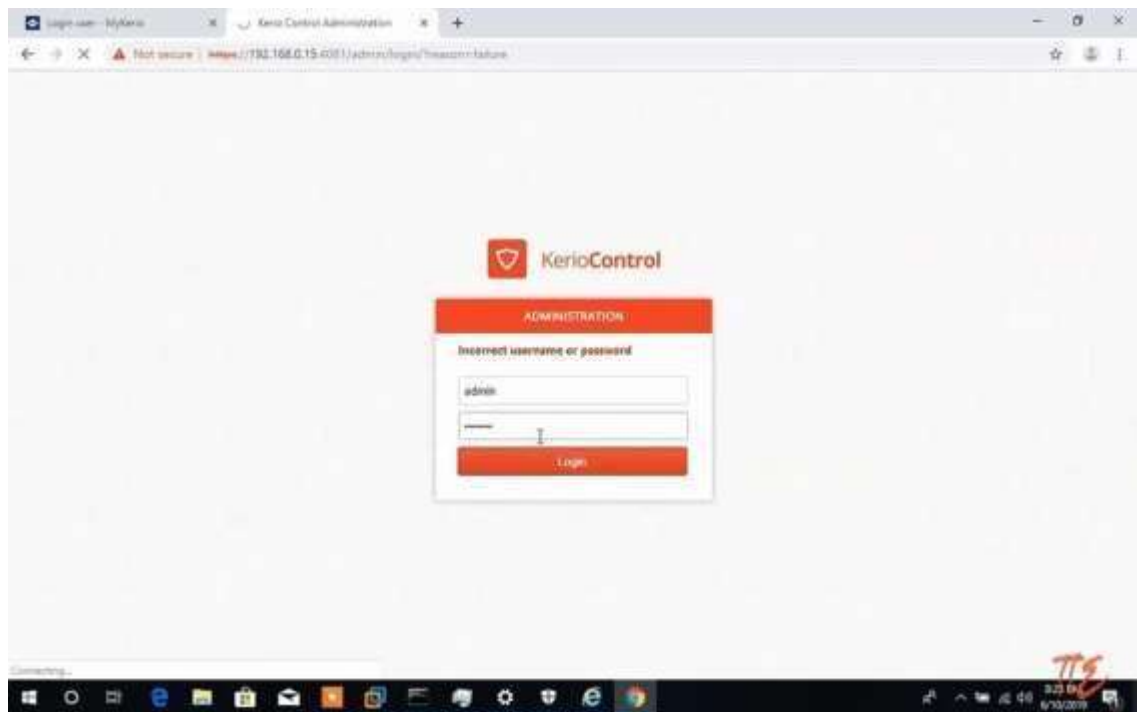




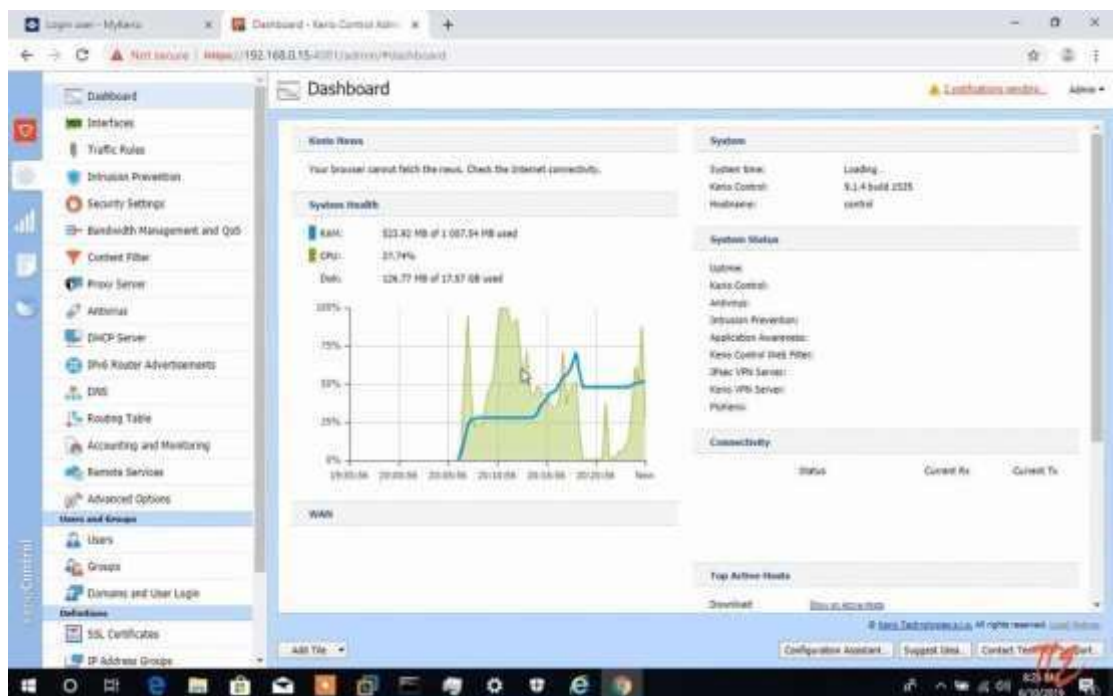
13. Dasturga kirdik. Uni ximoyalash uchun username va parol kiritib qo'yamiz:



14. Keyingi qadamda hosil bo'lgan oynaga yuqorida kiritgan username va parolimizni kiritamiz:



15. Dasturga kirdik. Quyida uning interfeysini ko'rishimiz mumkin. Endi chap paneldagi menyularga kirib tizimga har xil ximoyalar va cheklovlar qo'yishimiz mumkin bo'ladi:



30-LABORATORIYA ISHI

Mavzu: IDS/IPS dasturiy ta'minotini o'rnatish va sozlash.

Ishdan maqsad: Kirishni aniqlash va oldini olish tizimlari qanday himoyalanganligi to'g'risida tushuncha olish. SNORT-dan foydalanishni o'rganish.

Nazariy ma'lumot

Hujumni aniqlash tizimi (IDS) - bu kompyuter tizimiga yoki tarmoqqa ruxsatsiz kirish yoki ularni asosan Internet orqali ruxsatsiz boshqarish faktlarini aniqlash uchun mo'ljallangan dasturiy ta'minot yoki apparat vositasi.

Tarmoqning kirib kelishini aniqlash tizimi (NIDS) - bu DoS hujumlari, portni skanerlash yoki hatto tarmoqqa kirish urinishlari kabi zararli harakatlarni kuzatadigan kirishni aniqlash tizimi.

Passiv identifikatorlarda xavfsizlik buzilishi aniqlanganda, qoidabuzarlik to'g'risidagi ma'lumotlar dasturlar jurnaliga yoziladi va xavfli aloqa signallari konsolga va / yoki tizim ma'muriga ma'lum aloqa kanali orqali yuboriladi. Hujumni oldini olish tizimi (IPS) deb ham ataladigan faol tizimda IDS buzilishga javoban ulanishni tashlab yoki tajovuzkordan trafikni blokirovka qilish uchun xavfsizlik devorini qayta tuzadi. Javob berish harakatlari avtomatik ravishda yoki operator buyrug'i bilan amalga oshirilishi mumkin.

IPS / IDS - Kirishni aniqlash va oldini olish tizimlari

IDS Intruzion Detection System - kirishni aniqlash tizimi degan ma'noni anglatadi. IPS yoki kirib kelishning oldini olish tizimi bu tajovuzni oldini olish tizimidir. An'anaviy himoya vositalari bilan taqqoslaganda - antivirus, spam-filtrlar, xavfsizlik devorlari - IDS / IPS tarmoq himoyasini ancha yuqori darajada ta'minlaydi.

Antivirus fayllarni, spam-filtr xabarlarini, xavfsizlik devori IP-ulanishlarni tahlil qiladi. IDS / IPS ma'lumotlar va tarmoq xatti-harakatlarini tahlil qiladi.

IDS arxitekturasini va texnologiyasi

IDS printsipli transport tahlili asosida tahdidlarni aniqlashdan iborat, ammo keyingi harakatlar administratorida qoladi. IDS tizimlari o'rnatish joyiga va ishlash printsipliga ko'ra turlarga bo'linadi. Sayt identifikatorlari turlari

Ushbu sohada eng keng tarqalgan ikki turdagi IDS:

Sayt identifikatorlari turlari

Ushbu sohada eng keng tarqalgan ikki turdagi IDS:

- Tarmoqqa kirishni aniqlash tizimi (NIDS),
- Xostga asoslangan kirishni aniqlash tizimi (HIDS).

Birinchisi tarmoq darajasida ishlaydi, ikkinchisi esa faqat bitta xost darajasida ishlaydi.

Tarmoq hujumlarini aniqlash tizimlari (NIDS)

NIDS texnologiyasi tizimni strategik muhim tarmoq joylarida o'rnatish va barcha tarmoq qurilmalarining kirish/chiqish trafigini tahlil qilish imkonini beradi. NIDS, kanal darajasidan ilovalar darajasiga qadar har bir paketga "qarash" orqali chuqur darajadagi trafikni tahlil qiladi.

NIDS xavfsizlik devori yoki xavfsizlik devori farq qiladi. Xavfsizlik devori faqat tarmoqdan tashqarida keladigan hujumlarni aniqlaydi, NIDS esa ichki tahdidni aniqlay oladi.

Tarmoq hujumlarini aniqlash tizimlari butun tarmoqni nazorat qiladi, bu esa qo'shimcha echimlarga pul sarflamaslikka imkon beradi. Biroq, kamchiliklar mavjud: NIDS ko'plab resurslarni iste'mol qilib, barcha tarmoq trafigini kuzatib boradi. Trafik miqdori qanchalik ko'p bo'lsa, CPU va RAM resurslariga bo'lgan ehtiyoj qanchalik baland. Bu ma'lumotlar almashinuvining sezilarli kechikishiga va tarmoq tezligini pasayishiga olib keladi. Katta miqdordagi ma'lumot, shuningdek, tizimni ba'zi paketlarni o'tkazib yuborishga majbur qilib, NIDSNI "bezovta qilishi" mumkin, bu esa tarmoqni zaiflashtiradi.

Host intrusion Detection tizimi (HIDS)

Tarmoq tizimlariga muqobil-host. Bunday tizimlar tarmoq ichida bitta uy egasiga o'rnatiladi va faqat uni himoya qiladi. HIDS shuningdek, barcha kiruvchi va chiquvchi paketlarni tahlil qiladi, lekin faqat bitta qurilma uchun. HIDS tizimi fayl snapshotlarini yaratish tamoyiliga asoslangan: joriy versiyaning rasmini oladi va uni avvalgi bilan taqqoslaydi, shu bilan mumkin bo'lgan tahdidlarni aniqlaydi. HIDS tarmoqdagi muhim mashinalarga kamdan-kam hollarda konfiguratsiyani o'zgartiradigan yaxshiroqdir.

Snort - bu bepul, ochiq manbali, tarmoqqa asoslangan kirib borishni oldini olish tizimi (IPS) va kirishni aniqlash tizimi (IDS), bu IP-tarmoqlarda paketlarni ro'yxatdan o'tkazish va real vaqtda trafik tahlilini amalga oshirishi mumkin.

Tizimga kirish, tahlil qilish, tarkibni qidirishni amalga oshiradi va bir qator hujumlarni va zondlarni faol ravishda blokirovka qilish yoki passiv ravishda aniqlash uchun keng foydalaniladi, masalan, buferdan oshib ketishga urinishlar, yashirin portni skanerlash, veb-ilovalar hujumlari, SMB problari va OSni aniqlash tizimlari. Dastur asosan tajovuzni oldini olish uchun ishlatiladi, agar ular paydo bo'lsa hujumlarni bloklaydi.

Snort oddiy, ammo moslashuvchan va kuchli tilda yozilgan qoidalardan foydalanadi. Yodda saqlash oson bo'lgan bir qator umumiy yozuv tamoyillari mavjud.

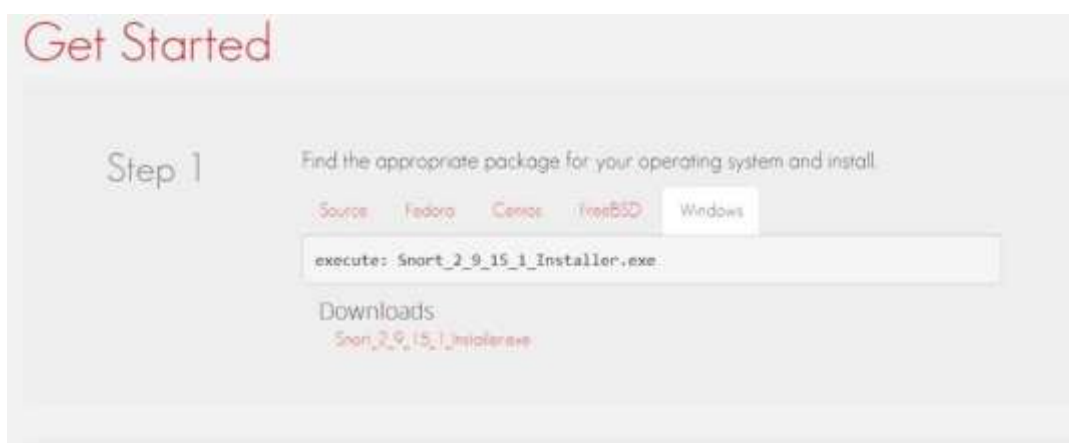
Snort qoidalari ikki qismdan iborat: qoida sarlavhasi va qoida parametrlari. Sarlavhada harakatning tavsifi, aloqa protokoli, IP-manzillar, tarmoq maskalari va manba va manzil portlari mavjud. Qoida parametrlari ogohlantiruvchi xabarni saqlaydi, shuningdek, agar qoida ishga tushirilsa, aniqlangan paketning qaysi qismi qayta ishlanishi kerakligi haqida ma'lumot.

Avvalo, snort.org rasmiy saytiga o'tiladi. Dastur to'liq bepul bo'lgani uchun, litsenziya talab qilinmaydi.

Get Started tugmasi bosiladi



Matn buyruqlari bo'lgan oyna ochiladi, u erda biz operatsion tizimimizni yuqori yorliqlarda tanlaymiz (bu holda Windows) va dastur faylini yuklaymiz (Installer.exe).



Yordamchi dasturlarni o'rnatish

Windows uchun oxirgi snort oynasida Winpcap yordam dasturi uchun tanqli tarmoq administratorlarini o'rnatishingizni so'raydi. Bu sizning tarmoq kartangizni monitor rejimiga o'tishga, ya'ni protokollar to'plamini chetlab o'tib, paketlarni uzatish va qabul qilishga imkon beruvchi. Ushbu yordamchi dastur ham bepul, shuning uchun uni winpcap.org rasmiy saytidan yuklab olinadi o'rnatiladi.



Ikkinchi yordamchi dastur - bu fayllarni ochish uchun zarur bo'lgan maxsus yuqori siqishni nisbati arxivi. 7-Zip arxivatorini 7-zip.org rasmiy saytidan yuklab olinadi va o'rnatiladi.

Shunday qilib, o'rnatuvchi yuklab olinadi va o'rnatiladi, yordamchi dasturlar ham ta'minlanadi. Ammo grafik qobiq yo'qligi sababli, biz snort ishlaydigan maxsus qoidalarni yuklashimiz kerak. snort.org rasmiy saytiga qaytib, "Rules" tugmasi bosiladi.

