**Laboratoriya №7**

**Tarmoq resurslaridan foydalanishni cheklash va ochiq aloqa kanallari orqali uzatiluvchi ma'lumotlarni himoyalashda tarmoqlararo ekran dasturini o'rnatish va sozlash**

***Ish maqsadi:****malumotni* ochiq aloqa kanallari orqali uzatish va tarmoq resurslariga kirishni cheklash vaqtida tarmoqlararo ekran dasturiy ta'minotini va utilitalarini o'rnatish va sozlash bo'yicha amaliy ko'nikmalarga ega bo'lish.

***Topshiriq:*** tarmoqlararo ekran dasturiy ta'minotini o'rnatish va sozlash. O'rnatilgan tarmoqlararo ekran dasturiy ta'minotini sozlash va tarmoq resurslaridan foydalanishni cheklash.

Tarmoqlararo ekran (xavfsizlik devori) nima

**Tarmoqlararo ekran (Brandmauer)**  yoki **Tarmoqlararo ekran (Firewall) - bu**  Kompyuteringizni viruslardan himoya qilish maqsadi bo'lgan kompyuter dasturi. Tarmoqlararo ekran operatsion tizimga kiradigan tarmoq trafigini kuzatib boradi va foydalanuvchining shaxsiy ma'lumotlariga kirishga urinayotgan zararli dasturlarni to'xtatishga yordam beradi. Bundan tashqari, Firewall va Firewall atamalari yana bir ta'rifga ega. Ushbu atamalar yong'in kapital devorlari deb ataladi, ular nazariy jihatdan zich binolarda uylarni yong'inlardan himoya qilishi kerak.

Tarmoqlararo ekran (xavfsizlik devori) nima o'zi - oddiy so'zlar bilan ma'nosi, ta'rifi.

**Oddiy so'zlar bilan aytganda, Tarmoqlararo ekran (Xavfsizlik devori) bu**  Internetda qabul qilingan va yuborilgan ma'lumotlarni doimiy ravishda skanerlaydigan maxsus himoya kompyuter dasturlari. Tasavvur qilib aytadigan bo'lsak, bu kompyuterni Internet xavfidan himoya qiluvchi virtual devorlar: viruslar, rootkitlar, josuslik dasturlari va boshqalar. Shuni ta'kidlash kerakki, tarmoqlararo ekran sizning kompyuteringiz uchun yagona yoki eng ishonchli himoya manbai emas. Qoida tariqasida, eng katta xavfsizlikni ta'minlash uchun tarmoqlararo ekran (Firewall) har doim antivirus va piyodalarga qarshi dasturlar bilan birgalikda ishlaydi.

Ko'pgina hollarda, tarmoqlararo ekran to'g'ridan-to'g'ri ishlaydigan dastgohda (kompyuter) o'rnatiladi, lekin ba'zida, ko'plab kompyuterlar mavjud bo'lgan turli ofislarda bo'lgani kabi, tarmoqlararo ekran jismoniy qurilma shaklida ( *ammo keyinchalik bu haqida ko'proq*) Windows operatsion tizimining foydalanuvchilari uchun xavfsizlik devorini o'zlari o'rnatishga hojat yo'q ( *alohida-alohida*), chunki dastlab OT o'ziga xos xususiyatga ega - **Windows xavfsizlik devori**.

Tarmoqlararo ekran - bu qanday ishlaydi, sodda so'zlar bilan aytganda.

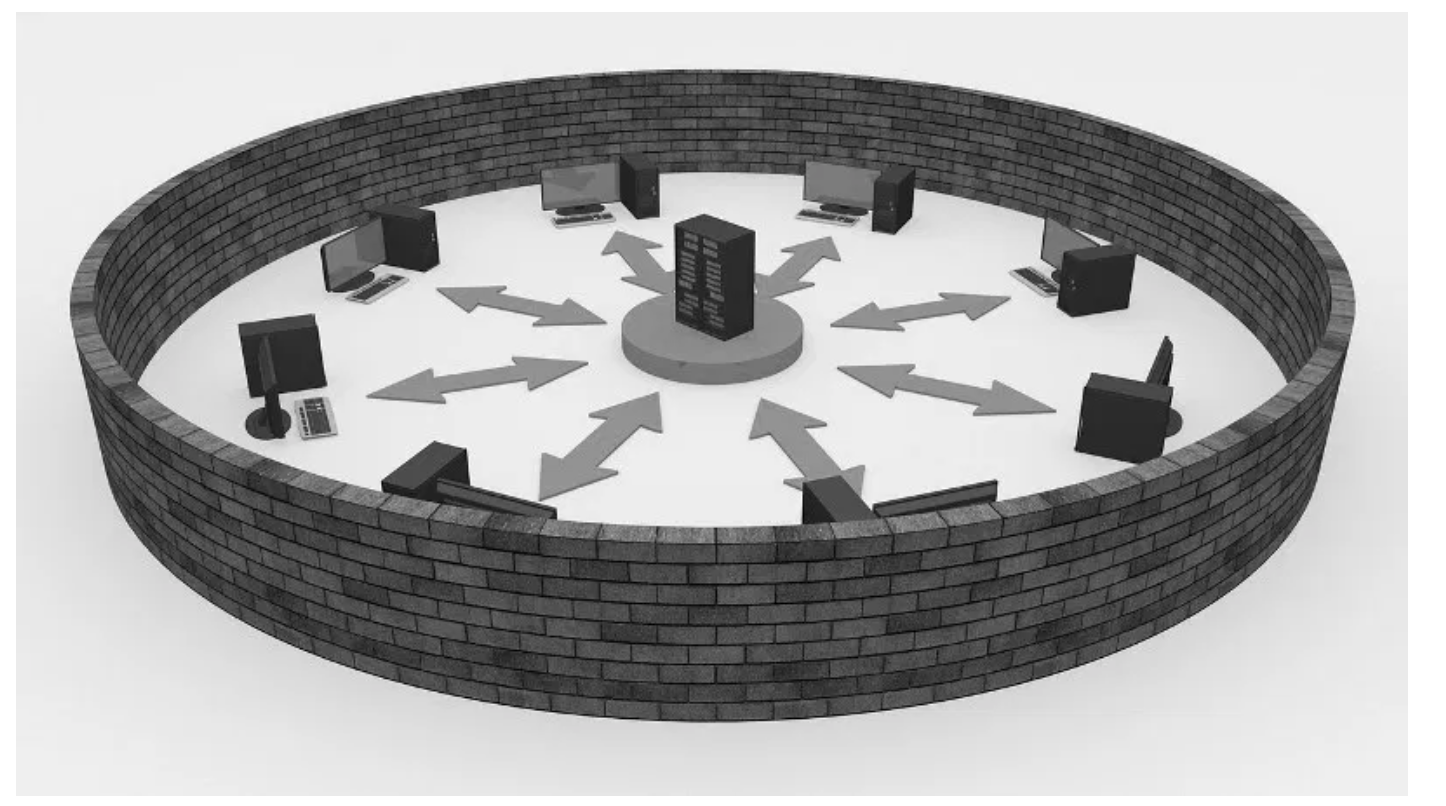
Murakkab texnik tafsilotlarni aniqlamasdan, tarmoqlararo ekran quyidagicha ta'riflanishi mumkin. Foydalanuvchi brauzer yoki kompyuter o'yini kabi Internetga tegishli dasturni ishga tushirganida, kompyuter uzoq veb-saytga ulanadi va foydalanuvchining kompyuter tizimi haqida ma'lumot yuboradi. Biroq, ma'lumotlar yuborilish yoki qabul qilinishidan oldin, u tarmoqlararo ekran orqali o'tadi ( *xavfsizlik devori*), bu erda, belgilangan parametrlarga qarab, ma'lumotlar o'tkazib yuboriladi yoki to'xtatiladi.

Tasavvur qilib aytganda, tarmoqlararo ekran o'z ish jarayonida kompyuterga eksport qilinadigan va olib kiriladigan barcha narsalarni nazorat qiladigan chegara qo'riqchisi yoki bojxona xodimi vazifasini bajaradi. Bundan tashqari, uning vazifalariga ma'lumotlar paketlarini kerakli parametrlarga muvofiqligini tekshirish kiradi. Shunday qilib, tarmoqlararo ekran allaqachon o'rnatilgan zararli dasturlarning, masalan troyan otlari va boshqa josus dasturlarning ishini to'xtatishga yordam beradi. Oddiy so'z bilan aytganda, ekran shunchaki ushbu dasturlar tomonidan to'plangan ma'lumotlarni Internetga o'tkazmaydi. Ammo, bu, albatta, nazariy jihatdan, chunki bunday buzish dasturlari doimiy ravishda takomillashtirilib, xavfsizlik devorlarini buzishni o'rganmoqda.

Qurilma tarmoqlararo ekran va tarmoq xavfsizligi usullari nima?

**Uskuna tarmoqlararo ekran**  Ruxsatsiz kirishdan himoya qilishning ma'lum rivojlangan usullaridan foydalangan holda kompyuterni yoki tarmoqni Internetga ulaydigan jismoniy qurilma. Simli marshrutizatorlar, keng polosali shlyuzlar va simsiz yo'riqnoma tarmoqdagi har bir kompyuterni himoya qiladigan apparat devorlarini o'z ichiga oladi. Uskuna tarmoqlararo ekran tarmoqni himoya qilish uchun turli xil xavfsizlik turlaridan foydalanadi: paketlarni filtrlash, paketli holatni tekshirish, tarmoq manzili tarjimasi va dastur darajasidagi shlyuzlar.

**Paketli filtrlash devori**  Tizimga yuborilgan va undan kelgan barcha ma'lumot paketlarini tekshiradi. U tarmoq ma'muri tomonidan belgilangan qoidalar to'plamiga asoslangan ma'lumotlarni yuboradi. Ushbu apparat tarmoqlararo ekran paketning sarlavhasini tekshiradi va paket manbai manzili, tayinlanishi va portiga qarab filtrlaydi. Agar paket qoidalarga rioya qilmasa yoki blokirovka qilish mezonlariga javob bermasa, kompyuter yoki tarmoq orqali o'tishga yo'l qo'yilmaydi.

 **Paketlarni dinamik filtrlash**  yoki davlat paketli tekshiruvi, bu yanada himoya qilish usuli. Ushbu xavfsizlik devori u bilan nima qilish kerakligini aniqlash uchun paket qaerdan kelganligini boshqaradi. Bu ma'lumot ko'proq ma'lumot olish uchun so'rovga javoban yuborilganligini yoki u faqat o'z-o'zidan paydo bo'lganligini tekshiradi. Belgilangan ulanish holatiga mos kelmaydigan paketlar rad qilindi.

 Xavfsizlikni ta'minlashning yana bir usuli - bu tarmoq manzili tarjimasi yo'riqchisi (NAT). U Internetga kirish uchun hammaga taqdim etiladigan kompyuterni yoki tashqi dunyodan kompyuterlar tarmog'ini yashiradi. Xavfsizlik devori IP manzili ushbu stsenariyda yagona haqiqiy manzil va tarmoqdagi barcha kompyuterlar uchun berilgan yagona IP-manzil. Tarmoq ichidagi har bir kompyuterga faqat tarmoq ichida amal qiladigan o'z IP-manzili beriladi. Ushbu himoya optsiyasi juda samarali, chunki u ma'lumot paketlarini yuborish va olish uchun faqat bitta umumiy IP-manzildan foydalanish imkoniyatini ta'minlaydi. Bu, o'z navbatida, zararli dasturlarni joriy qilish imkoniyatini kamaytiradi. Ushbu apparat xavfsizlik devori odatda ishlaydigan yagona funktsiyaga ega bo'lgan tarmoqdagi alohida kompyuterda amalga oshiriladi. Bu juda murakkab va xavfsizlik devorlarining eng xavfsiz turlaridan biri hisoblanadi.

## Xavfsizlik devorlaridagi asosiy muammolar.

Xavfsizlik devorini ishlatishda bir nechta keng tarqalgan muammolar mavjud. Eng keng tarqalgan muammo shundaki, zararli dasturlarga qo'shimcha ravishda, xavfsizlik devori ko'pincha bizga kerak bo'lgan oddiy trafikni bloklaydi. Ba'zi veb-saytlar cheklangan kirish huquqiga ega yoki noto'g'ri ochilganligi sababli ochilmasligi mumkin. Ko'pincha tarmoq o'yinlari bilan bog'liq muammolar mavjud, chunki xavfsizlik devori bunday trafikni zararli deb biladi va dasturlarning ishlashini bloklaydi. Shunga asoslanib shuni ta'kidlash kerakki, xavfsizlik devori juda foydali bo'lsa-da, lekin u taqiqlari bilan hayotni buzmasligi uchun uni to'g'ri sozlash kerak.

  Toifalar: ,    / dan

Har qanday operatsion tizim hech bo'lmaganda bir oz himoyaga ega bo'lishi kerak. Windows-da ikkita butun himoya funktsiyasi mavjud - xavfsizlik devori (xavfsizlik devori) va Windows Defender. "Xavfsizlik devori" tushunchasi bir nechta ma'noga ega, ammo xavfsizlik devori versiyasi ushbu maqolada ko'rib chiqiladi.

Xavfsizlik devori nima?

Xavfsizlik devori (xavfsizlik devori) - Windows tizimidagi xavfsizlik devori, Internetga va mahalliy tarmoqlarga kompyuterga ruxsatsiz kirishning oldini oladi, shuningdek, ilovalarga tarmoqqa ulanishni taqiqlaydi yoki ruxsat beradi.

Oddiy so'zlar bilan aytganda, xavfsizlik devori - bu faqat ruxsat berilganlar uchun ochiladigan devor yoki yopiq eshik. Windows-da, odatda Internet bilan aloqa qiladigan dasturiy ta'minotga cheklovlar qo'yiladi. Endi biz "xavfsizlik devori" tushunchasini aniqladik, ammo kompyuterni himoya qilish uchun uni qanday qilib to'g'ri sozlash kerak?

Windows 10-da xavfsizlik devori (xavfsizlik devori) ni qanday sozlash kerak?

Ofislarda tizim ma'muri buni amalga oshiradi, shuning uchun xavfsizlik dasturlarini sozlash ko'nikmalariga ega bo'lish shart emas. Uyda, har kim kompyuter parametrlarini xohlagancha o'zgartirishi mumkin, ammo sababga ko'ra.

**Xavfsizlik devori nima?**

Ingliz tilidan tarjima qilingan so'z **xavfsizlik devori**  , "yonayotgan devor" deb tarjima qilingan. Ko'p foydalanuvchilar buni devor yoki deb atashadi **xavfsizlik devori**  . Odamlar ko'pincha xavfsizlik devori shunchaki devor yoki devor deb atashadi.

Xavfsizlik devori nima ekanligini va nima uchun kerakligini tushunaylik. Xavfsizlik devori tarmoq va kompyuter o'rtasida biron bir to'siqni ta'minlaydi yoki boshqacha qilib aytganda filtrdir. Ushbu dastur kompyuter ulanishlarini kuzatadi, ularni tahlil qiladi va ushbu ulanishga ruxsat berish yoki qilmaslik to'g'risida qaror qabul qiladi. Ya'ni, dastur faqat foydalanuvchining o'zi ruxsat bergan narsalarni o'tkazib yuboradi. Hech kim mutlaq kafolat berolmasligi aniq, ammo agar kimdir sizning kompyuteringizni buzishga harakat qilsa, devor unga aniq to'siq bo'ladi. Bu hali ham xakerning tajribasiga bog'liq bo'ladi.

Xavfsizlik devorining oddiy tushunchalarini sizning uyingiz bilan taqqoslash mumkin. Uyning eshiklari bor. Siz barcha eshiklarni yopiq holda saqlaysiz va siz hamma ochiq eshikdan sizga kelishi mumkinligini aytmoqchisiz. O'xshashlik bilan, hech kim sizning kompyuteringizga shunchaki kira olmasligiga ishonch hosil qilishingiz kerak - uni boshqaring va undan turli xil ma'lumotlarni oling. Uyning eshiklarida qulflar mavjud. Do'stingizga kirish uchun siz qasrni ochasiz. Xavfsizlik devori ham ishlaydi. U Internetga o'tish yoki Internetdan faqat siz unga ruxsat bergan dasturlarni ishlata oladi. Boshqa barcha dasturlar Internetdan kirish va chiqish uchun blokirovka qilinadi.  
Ma'lum bo'lishicha, siz kompyuter va Internet o'rtasida qorovulni qo'ysangiz, bu sizga kerakli va muhim bo'lgan narsalarni ta'minlaydi, qolganlarini kechiktiradi.

Kompyuterni maksimal darajada himoya qilish uchun siz to'g'ri sozlamalarni o'rnatishingiz kerak. Faqatgina unga muhtoj bo'lgan dasturlarga ulanishga ruxsat berish tavsiya etiladi. Va dastur bo'lishi kerak bo'lsa **faqat o'sha portlarga kirish** u uchun ishlaydi Bir qarashda, bu murakkab tuyuladi, ammo xavfsizlik devorlaridagi konfiguratsiya yordamchilari mavjud va ular yordamida sozlash jarayonini soddalashtiradi. Asosiysi, jarayonda paydo bo'ladigan xizmat xabarlarini diqqat bilan o'qish.

Xavfsizlik devori ikki xil devorga ega - shaxsiy va korporativ. Shaxsiy devor - bu shaxsiy kompyuterga o'rnatilgan dastur va Internet va mahalliy tarmoq o'rtasidagi shlyuzga korporativ xavfsizlik devori o'rnatilgan dastur.

Shaxsiy xavfsizlik devorida o'rnatilgan o'quv rejimi mavjud, uning yordamida dasturning ishlashini va ulanishga ruxsat berilgan va taqiqlangan narsalarni tushunish oson. Agar kompyuterdagi dastur xavfsizlik devori uchun mos bo'lmasa, unda tizim xabari paydo bo'ladi va foydalanuvchi ulanish yoki rad etishni o'zi o'zi hal qila oladi. Bugungi kunda etarli darajada shaxsiy xavfsizlik devorlari va ular orasida eng mosini tanlang. Ular turi, interfeysi, pullik va bepul farq qiladi, ammo aslida deyarli farq qilmaydi. Ya'ni, siz foydalanish uchun qulayroq bo'lgan dasturni tanlaysiz.

Korporativ xavfsizlik devorlari tizim ma'muri tomonidan sozlangan, u butun tarmoqni hujumlardan himoya qiladi.  
LeakTest yordam dasturi yordamida xavfsizlik devori dasturining ishlashini tekshirishingiz mumkin. Buning uchun yordam dasturini ishga tushiring, "Test" ni bosing va keyin xavfsizlik devori so'roviga javob berishingiz kerak, "Bir marta ruxsat berish" ga javob bering. Dastur sizga aytishi kerak - "Xavfsizlik devori kirib ketdi". Bu Internetga ulanishni va sinov uchun ishlatiladigan serverni tekshirish uchun kerak. Keyin "Test" tugmachasini bosamiz va xavfsizlik devori dasturining talabiga "Bir marta rad eting" degan javobni beramiz. Dastur "ulanib bo'lmadi" degan xabarni berishi kerak, bu esa xavfsizlik devori ulanishni bloklaganligini anglatadi.

Keyin, LeakTest dasturining EXE fayli brauzer nomiga mos ravishda o'zgartirilishi kerak, agar Internet Explorer uchun bu IEXPLORE.EXE bo'lsa, Opera uchun bu OPERA.EXE, boshqa brauzerlar uchun esa "Boshlash" bandidagi yorliqning xususiyatlaridan nom qidirish kerak. Va siz ulanishni o'rnatmoqchi bo'lganingizda yoki ulanishni o'rnatganingizda, xavfsizlik devori sizni dastur bu qoida uchun yaratilgan dastur emasligi haqida ogohlantiradi. Agar bunday ogohlantirish bo'lmasa va ulanish o'rnatilsa, ya'ni "Xavfsizlik devori kirib ketdi" xabari paydo bo'lsa, har qanday virus faylni shunchaki qayta nomlash orqali xavfsizlik devorini chetlab o'tishi mumkin, ya'ni bu xavfsizlik devori zudlik bilan boshqasiga o'zgartirilishi kerak.

A **xavfsizlik devorini tekshiring**  kompyuteringizga o'rnatilgan bizning veb-saytimizda bo'lishi mumkin.

Agar siz Internetga ulangan kompyuterni qanday himoyalashga qiziqsangiz, xavfsizlik devori nima degan savol tug'ilgandir.

**Xavfsizlik devori**  (ingliz firewall - yong'in devori), bu xavfsizlik devori (nemis markasimeyridan bir xil tarjima), u xavfsizlik devori - tarmoq trafigini filtrlaydigan, tarmoq qismlari yoki alohida tugunlar uchun himoya funktsiyasini bajaradigan dasturiy ta'minot yoki dasturiy vositaning tarkibiy qismi.  
  Uning ishi davlat chegarasidagi nazorat punktiga yoki yopiq hududga kirish joyidagi xavfsizlik postiga o'xshaydi.

  Ish printsipi

Xavfsizlik devori trafikni ketma-ket oqadigan filtrlar to'plami deb hisoblash mumkin. Har bir filtr oqim elementlarini ma'lum bir qoidaga muvofiqligini tekshiradi. Filtrlash qoidalari (qoidalar to'plami) qaysi paket ekranni kesib o'tishini (ishlashga ruxsat berish - "ruxsat berish") belgilaydi va o'chirib tashlanadi (xizmat mavjud emasligi to'g'risida ogohlantirishsiz "operatsiyani rad etish -" rad qilish yoki bildirish bilan "rad etish").

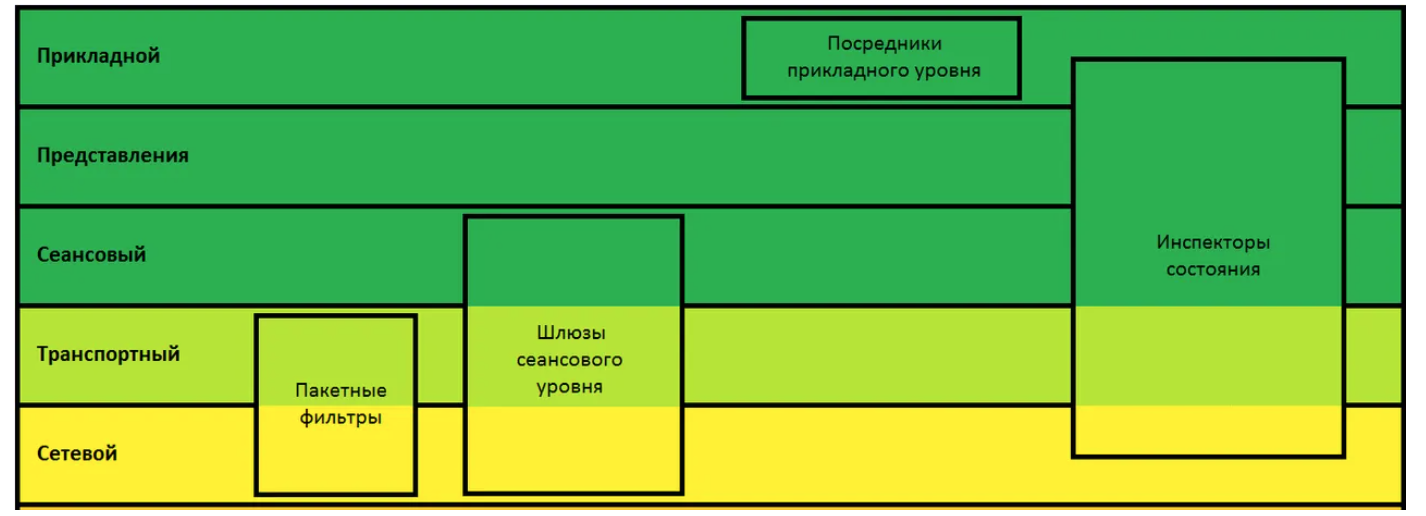
Paketlarni tanlash ikkita printsipdan biriga muvofiq amalga oshiriladi:

1. Taqiqlanmagan hamma narsa o'tadi. Qoidalarda o'tkazib yuborib bo'lmaydigan paketlarning belgilari ko'rsatilgan.
2. Faqat ruxsat berilgan narsalar o'tadi. Qoidalarda qaysi paketlarni tashlab yuborish mumkinligi ko'rsatilgan.

Ikkinchi printsip tizimni boshqarishni murakkablashtirish hisobiga ko'proq xavfsizlikni ta'minlaydi.

Ekran qaysi tarmoq protokollarining ishlash darajasiga qarab, uni quyidagi turlardan biriga bog'lash mumkin:

* paketli filtrlar (paketlarning sarlavhalarini tahlil qilish (lekin uzatilmagan ma'lumotlarni tahlil qilish), parchalangan paketlarga va ma'lumotlarni soxtalashtirishga, masalan, IP-manzil buzib ko'rsatishga moyil);
* seans darajasidagi shlyuzlar (ular himoyalangan xost va boshqa tarmoq tugunlari o'rtasida vositachilar rolini o'ynaydilar, paketlarni faqat o'rnatilgan aloqada uzatadilar, oldingi tur singari, paketlarning tarkibini tahlil qilmaydilar, bu zaiflik bo'lishi mumkin);
* dastur darajasidagi vositachilar (shuningdek, ulanishda vositachilar sifatida ham ishlaydi, lekin qo'shimcha ravishda uzatilayotgan ma'lumotlarni tahlil qila oladilar, istalmagan buyruqlarni bloklaydilar, avvalgilariga qaraganda ancha ishonchli, ammo ko'proq resurs talab qiladilar);
* davlat inspektorlari (yuqoridagi turlarning qo'shilishi, ularning foydasiga o'zgartirilgan).



Firewallda shifrlangan yoki tunnelli trafik qiyin bo'lishi mumkin, uni filtrga muvofiqligini tahlil qilib bo'lmaydi. Bunday holatlarda bunday ma'lumotlarni o'chirib tashlash eng xavfsiz echim bo'ladi.

Shaxsiy xavfsizlik devori xavfsizlik devorlaridagi kabi ishlaydi, lekin bir qator xususiyatlarga ega:

* qaysi dastur tarmoqqa ulanishga harakat qilayotganini aniqlash qobiliyati;
* turli foydalanuvchilar uchun turli xil qoidalar;
* barcha dasturlar uchun tarmoq faoliyatining ruxsatnomalari va taqiqlarini qo'lda sozlash imkonini beradigan "o'quv rejimi" mavjudligi.

Taniqli xavfsizlik devori dasturlariga misollar

Operatsion tizimda o'rnatilgan himoyachi mavjud va ko'plab antivirus dasturlari o'z ichiga xavfsizlik devori o'rnatilgan, ammo bu sizning xohishingiz bilan xavfsizlik devori tanlash, o'rnatish va sozlashingizga xalaqit bermaydi.

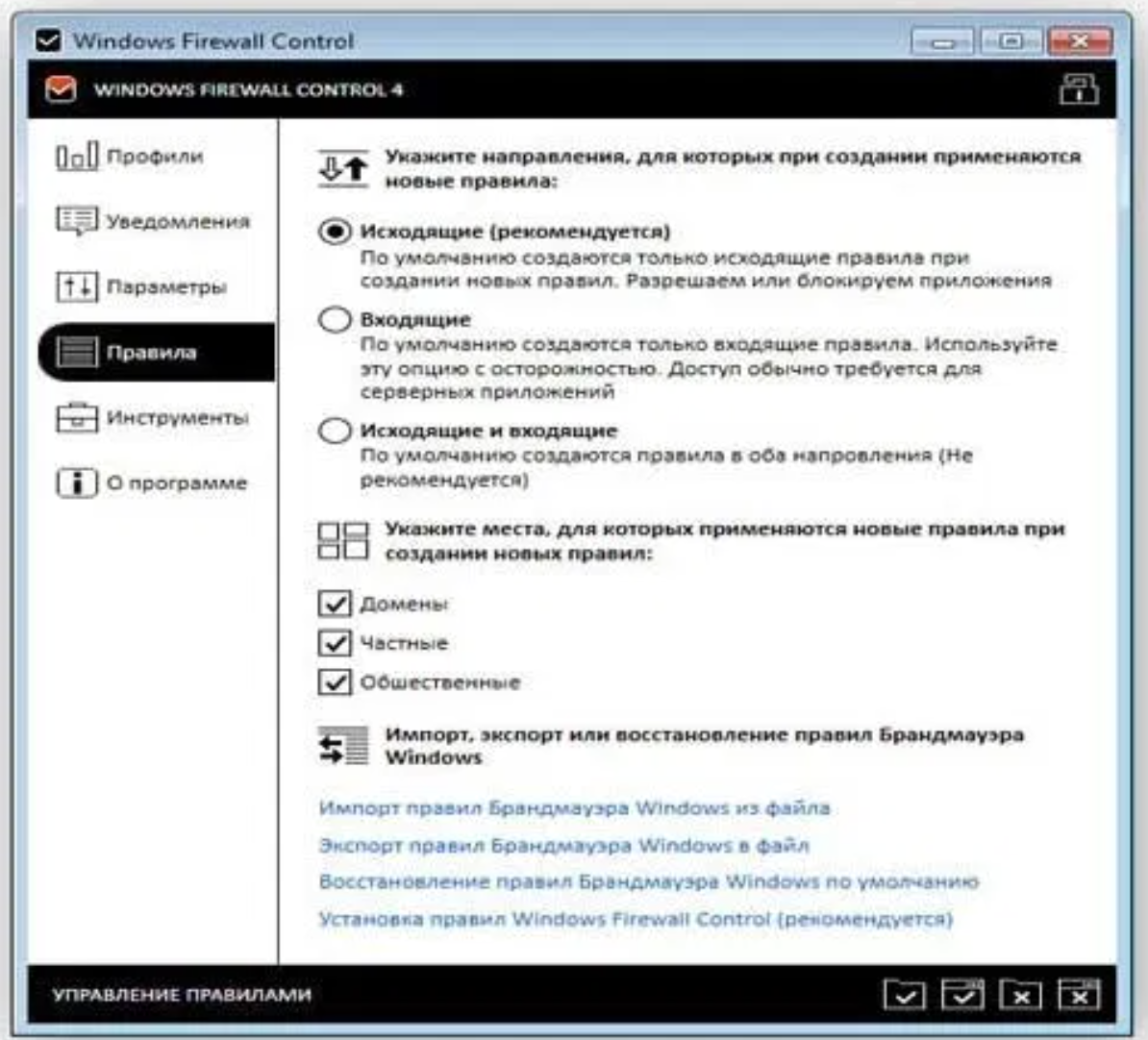
Windows uchun mashhur bepul xavfsizlik devorlari:

* Comodo Firewall
* Outpost Firewall Bepul;
* ZoneAlarm Free Firewall;
* PC Tools Firewall Plus;
* Emsisoft Online Armor Free;
* Xususiy temiryo‘l
* TinyWall (boshqalar singari mashhur emas, lekin tizimga o'rnatilgan xavfsizlik devori bilan ziddiyat qilmaydi va troyanlarga qarshi samarali).

  Windows uchun xavfsizlik devori qanday sozlanadi?

**Xavfsizlik devori sozlamalari**  - murakkab vazifa, uni amalga oshirish uchun sizga bilimlar to'plami kerak. Himoya qilishni ta'minlaydigan va ayni paytda foydali dasturlarning ishiga xalaqit bermaydigan filtr qoidalarining izchil to'plamini ishlab chiqish kerak. Har bir qoida bir qator xususiyatlarga ega va ularning barchasi to'g'ri o'rnatilishi kerak.

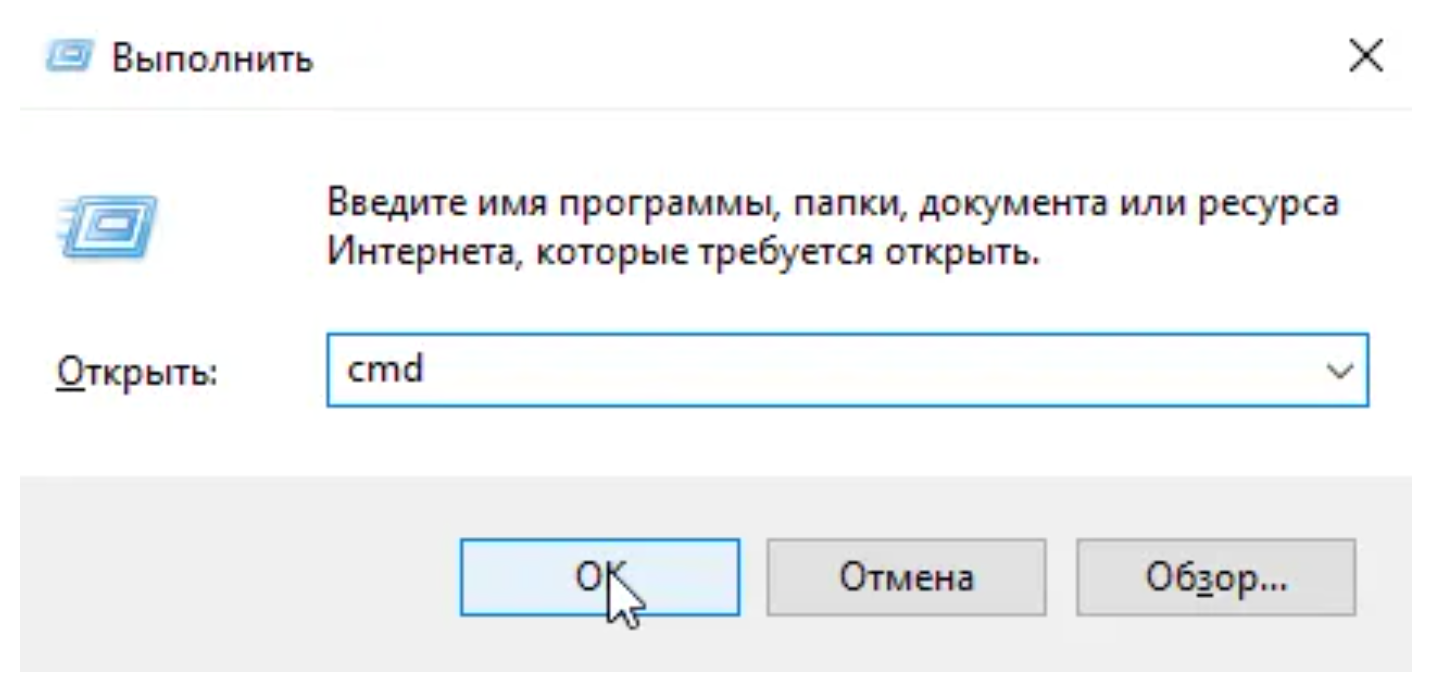
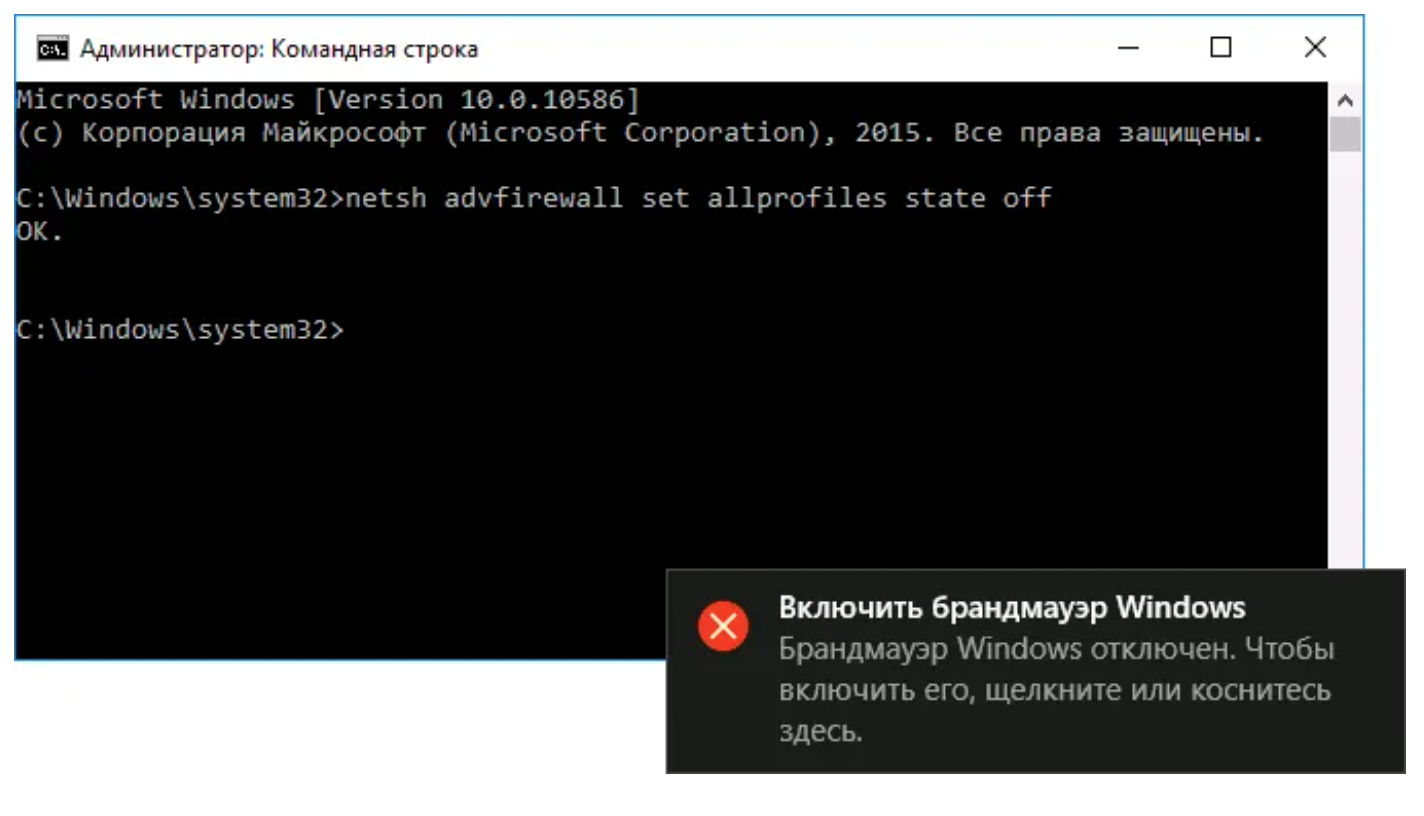
Vazifani soddalashtirish uchun bir qator usullar mavjud:

 Alohida dasturlarga kirishga qanday ruxsat berilishini alohida ko'rib chiqamiz:

## Windows-da xavfsizlik devori qanday o'chiriladi?

Boshqa to'liq xavfsizlik devoridan foydalanganda, o'rnatilgan o'chirilgan bo'lishi mumkin.

Eng tezkor usul bu buyruq satridan foydalanish:

  Agar kerak bo'lsa, yoqish uchun buyruq quyidagicha ko'rinadi.

***netsh advfirewall allprofiles holatini yoqdi***

Aksariyat foydalanuvchilar bugungi kunda yaxshi antivirus dasturlarini o'zlarining kompyuterlariga o'rnatilgan xavfsizlik devori bilan o'rnatadilar. Shu bilan birga, har bir kishi o'zi uchun eng mos variantni tanlaydi. Pulli ham, bepul ham kommunal xizmatlar mavjud. Ularning barchasi tizimni ishonchli himoya qiladi.

Agar sizga Windows xavfsizlik devorini o'chirib qo'yish tavsiya qilinsa, chunki u uchinchi tomon dasturiga zid kelishi, turli dasturlarni blokirovka qilishi va Internet tezligiga ta'sir qilishi mumkin. Ammo boshqa hollarda, xavfsizlik devorini o'chirish zararli dasturlarning tizimga kirishiga olib kelishi mumkin, shuning uchun buni amalga oshirish juda istalmagan.

Nega menga xavfsizlik devori kerak?

Ingliz tilidan tarjima qilingan "xavfsizlik devori" so'zi "olov devori" (olov - olov, devor - devor) degan ma'noni anglatadi. Darhaqiqat, Windows-ga o'rnatilgan ushbu dastur turli xil qurtlar, troyanlar va boshqa viruslar uchun to'siq bo'lib xizmat qiladi. Xavfsizlik devori (xavfsizlik devori yoki xavfsizlik devori) Internet-trafikni filtrlaydi va faqat dastur tomonidan ruxsat etilganlardan o'tadi.

Shunisi e'tiborga loyiqki, bepul Windows-ning xavfsizlik devori, shuningdek pullik xavfsizlik devori ham mavjud. Aslida, "mahalliy" versiya, ayniqsa Windows 7-dan boshlab, kompyuteringizni yuqori sifatli himoya qilishni ta'minlaydi, ammo agar xohlasangiz, siz pullik dasturni sotib olishingiz mumkin. Bunday holda, uchinchi tomon xavfsizlik devorini o'rnatayotganda, o'rnatilgan Windows-ni o'chirishingiz kerakligini unutmang.

Windows-ning turli xil versiyalarida uni qanday va qanday o'chirish haqida quyida o'qing.

Windows XP Xavfsizlik devorini o'chirish

Xavfsizlik devorini "amal qilish muddati" da quyidagicha o'chirib qo'yishingiz mumkin. "Boshlash" menyusiga o'ting va "Boshqarish paneli" ni tanlang. Bu erda siz "Xavfsizlik devori" bo'limiga o'tishingiz kerak. Umumiy ko'rinishida O'chirish parametrining yonidagi katakchani o'rnating va OK ni bosing.

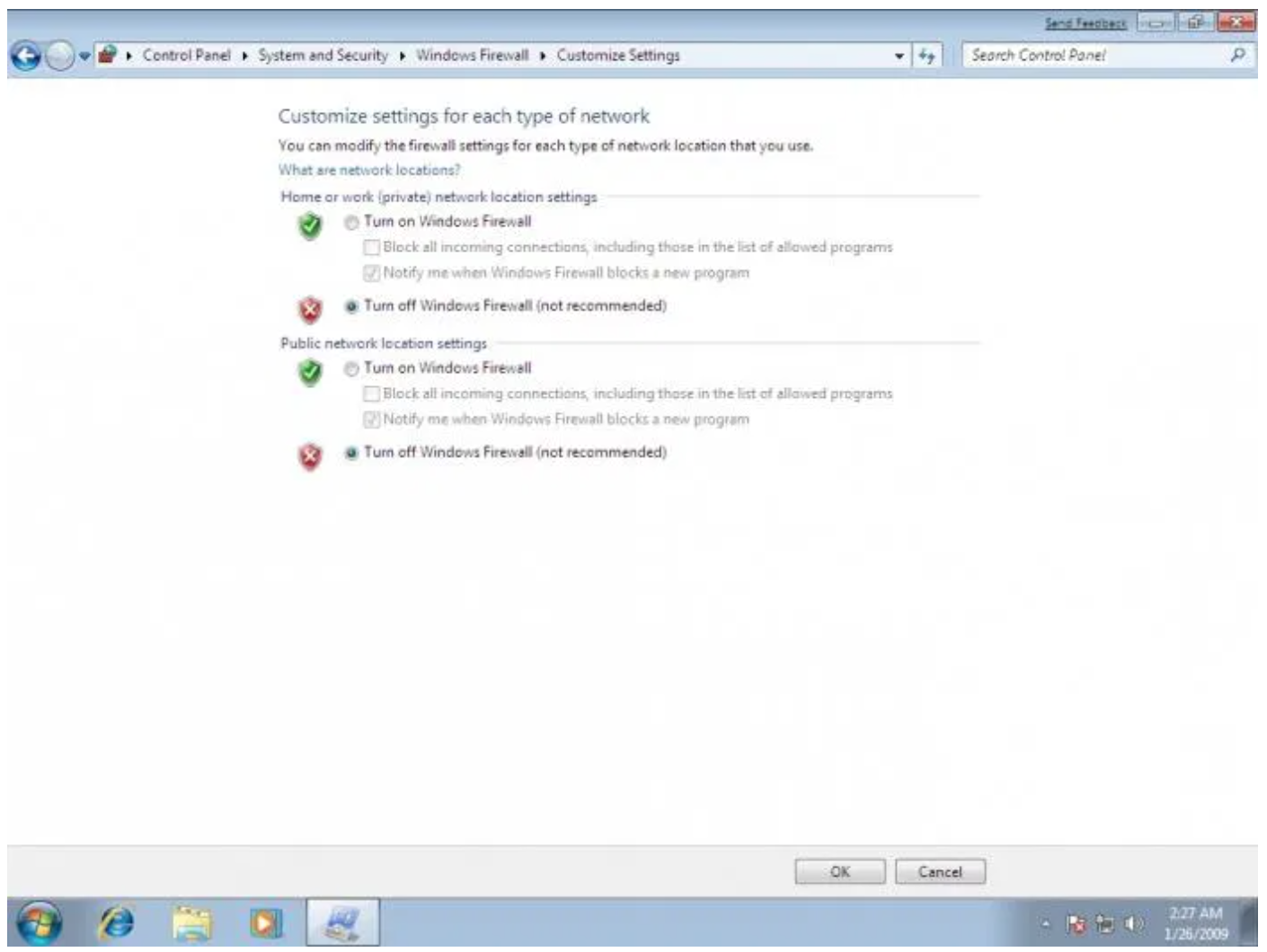
 Aytgancha, Windows XP (SP 1) da xavfsizlik devori normal himoyani ta'minlamadi, bunga qo'shimcha ravishda, ko'p foydalanuvchilar Internetda vaqt o'tkazish paytida kompyuterga tajovuzkorlar tomonidan hujum qilinishi mumkinligini tushunishmagan. Natijada ko'plab noxush holatlar ro'y berdi, ammo SP 2 chiqqandan keyin vaziyat ancha yaxshilandi.

Shunday qilib, endi sizda fikr bor va uni Windows XP-da qanday o'chirish kerak.

Xavfsizlik devori Windows 7. Qanday qilib o'chirish kerak?

"Yetti" ichiga o'rnatilgan xavfsizlik devori avvalgilariga qaraganda ancha ishonchli. Biroq, yuqorida aytib o'tilganidek, ko'plab foydalanuvchilar o'zlarining xavfsizlik devorlariga ega bo'lgan antivirus dasturlarini o'rnatishni afzal ko'rishadi. Ehtimol, bu to'g'ri qaror. Xavfsizlik devori nima va uni "ekshirka" da qanday o'chirish kerak, siz allaqachon bilasiz. Ammo Windowsning ettinchi versiyasi o'rnatilgan bo'lsa nima bo'ladi? Aslida, siz hech qanday chuqur kompyuter bilimiga muhtoj emassiz, chunki "ettitada" xavfsizlik devorini o'chirish Windows XP-da bo'lgani kabi oson.

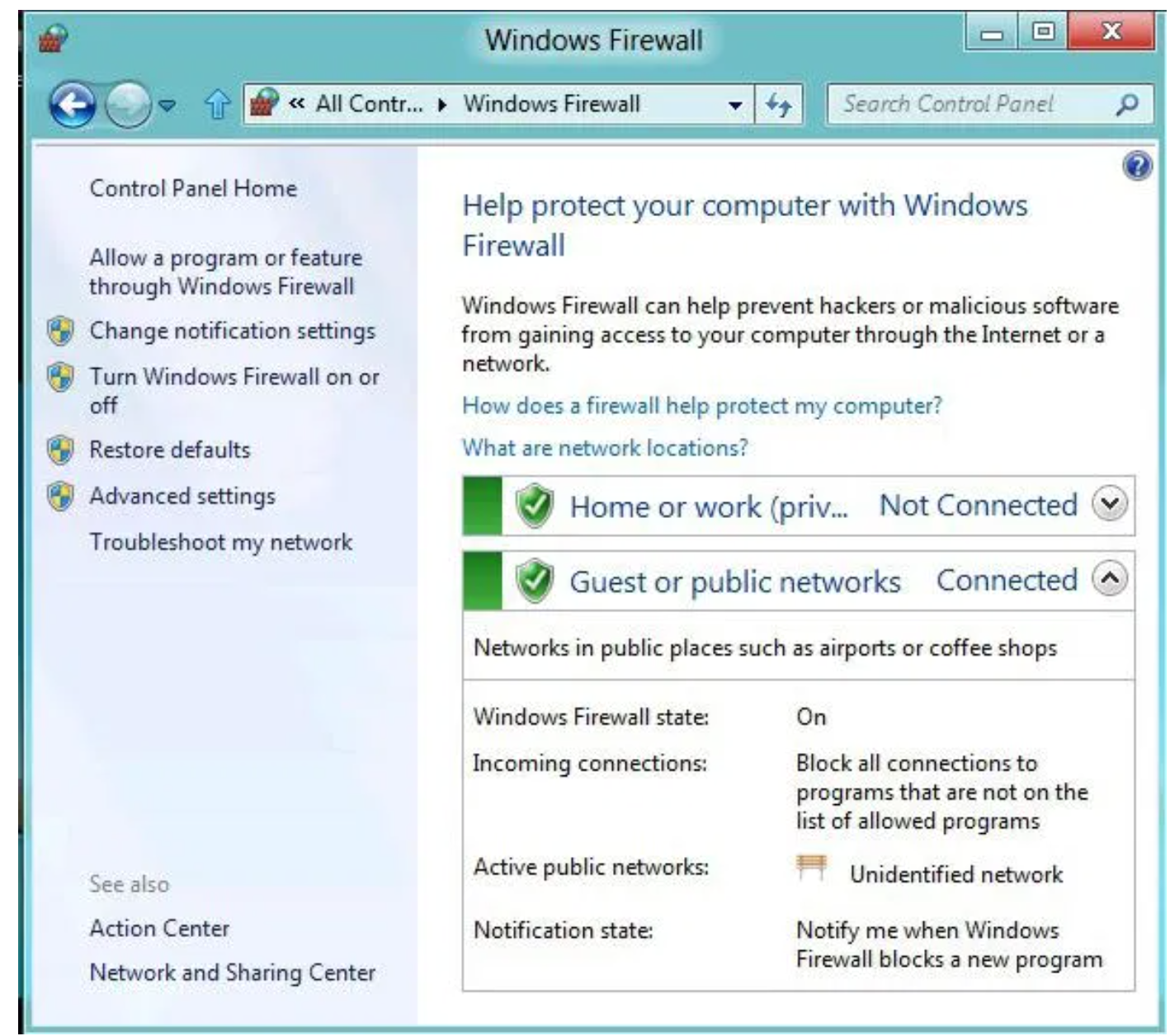
"Ishga tushirish" va "Boshqarish paneli" ni bosing. Ko'rish parametrlarida Kichik Icons-ni tanlang. "Xavfsizlik devori" bo'limiga o'ting. Chapda, "xavfsizlik devorini yoqing yoki o'chiring" havolasini toping va ustiga bosing. Xavfsizlik devorini o'chirib qo'yadigan parametrlar yonidagi katakchalarni o'rnating.

 Ko'rib turganingizdek, xavfsizlik devori nima ekanligini va uni Windows 7-da qanday o'chirib qo'yishni bilib olgandan so'ng, siz ushbu protsedurani bir daqiqada bajarishingiz mumkin.

G8-da xavfsizlik devorini o'chirish

Agar Windows 8 qurilmangizga o'rnatilgan bo'lsa, u holda "mahalliy" xavfsizlik devori o'chirilishi uchun quyidagi amallarni bajaring:

* ish stolida bo'lganingizda, "Ishga tushirish" RMB-ni bosing;
* u "Boshqarish paneliga" borishingiz kerak bo'lgan joyda ochiladi;
* "Xavfsizlik devori" bo'limini tanlang (undan oldin "Kichik nishonchalar" ni tanlang);
* chapdagi menyuda xavfsizlik devorini yoqish yoki o'chirishga imkon beradigan havolani bosing;
* kerakli variantga qarshi katakchalarni o'rnating.

 Endi siz xavfsizlik devori nima ekanligini va uni Windows 8-da qanday o'chirishni bilasiz.

Agar sizda kompyuteringizni zararli dasturlardan himoya qiladigan boshqa dastur bo'lmasa, o'rnatilgan Windows-ning himoya devorini o'chirmang. Albatta, xavfsizlik devori ba'zan ba'zi dasturlarni blokirovka qilishga xalaqit beradi, ammo u shunday tuzilganki, tajovuzkor tomonidan hujum qilish xavfi kamayadi.

Agar sizda o'z xavfsizlik devori bo'lsa, "tabiiy" Windows Firewall-ni o'chirib qo'yganingizga ishonch hosil qiling, chunki nizolar bo'lishi mumkin.

Agar standart shubha tug'dirsa (u juda kamdan-kam hollarda), siz uchinchi tomon xavfsizlik devorini o'rnatishingiz mumkin. Shunga qaramay, bunday dasturlarni shubhali obro'ga ega saytlardan yuklab olish juda istalmaganligini unutmang.

Xulosa

Shunday qilib, siz xavfsizlik devori nima ekanligini va Windows-ning mashhur versiyalarida uni qanday o'chirishni bilib oldingiz. Ko'rib turganingizdek, harakatlar ketma-ketligi deyarli bir xil. Qaysi OS o'rnatilganidan qat'iy nazar, siz ushbu operatsiyani o'zingiz bajarishingiz mumkin.