Дәріс №9: Желіаралық экрандар және олардың түрлері

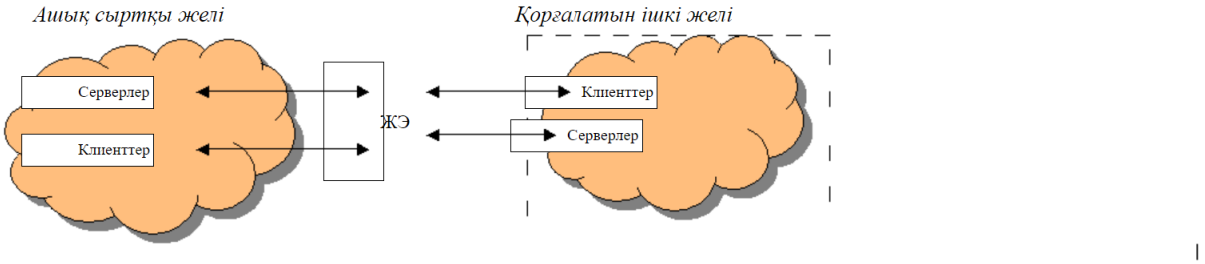
Желіаралық экран - ***брандмауэр*** немесе ***firewall*** - арнайы желіаралық қорғаныс комплексі.

Желіаралық экран ортақ желіні екіге бөлуге және ортақ желінің бір облысынан екінші облысының шекарасынан берілгендер пакетінің өту шаттарын анықтайтын ережелер жиынтығын іске асыруға мүмкіндік береді. Мұндай шекаралар мекеменің жергілікті желісі және Internet ауқымды желісі арасында жүргізіледі.

Әдетте желіаралық экран Internet ауқымды желісінен мекеменің ішкі желісін бұзып кіруден қорғайды, мекеменің жергілікті желісіне қосылған корпоративті интражелідегі шабуылдан қорғау үшін де қолданыла береді. Желіаралық экран технологиясы корпоративті желілерді сыртқы кауіп қатерден қорғайтын ең алғашқы технологиялардың бірі.

Көптеген мекемелерде желіаралық экран – орнату ішкі желіні қорғаудың ең қажетті шарты болып табылады.

Санкцияланбаған желіаралық бұзуға қарсы тұру үшін желіаралық экран ішкі болып табылатын мекеменің қорғалатын желісі және сыртқы қарсылас желінің арасында орналасуы керек (1 - сурет). Соған қарамастан осы желілер арасындағы қарым қатынастар желіаралық экран арқылы жүзеге асырылуы тиіс. Желіаралық экран жалпы қорғалатын желі құрамына кіреді.



1 – сурет. Желіаралық экранның қосылу схемасы

Бірнеше түйіндерді бірден шешетін желіаралық экран, мыналарды жүзеге асырады:

- Корпоративті желінің ішкі ресурстарына сыртқы қолданушылардың кіруін шектеу жұмысы (қорғалатын желіге байланысты). Мұндай пайдаланушыларға серіктестер, жойылған қолданушылар, хакерлер және де сол мекеменің желіаралық экран қорғайтын берілгендер қорын алғысы келетін жұмысшыларын жатқызуға болады.
- Сыртқы ресурстарға қорғалатын желінің қолданушыларының кіруін шектемеу мәселесі. Бұл мәселені шешу, мысалы қызмет бабының орындалуын қажет етпейтін серверлерге кіруді қадағалауға мүмкіндік береді.

Осы кезге дейін жалпыға мойындалған бір ғана желіаралық экран классификациясы жоқ. Оларды мысалға келесі негізгі белгілері бойынша классификациялауға болады:

OSI моделінің деңгейінде функционалдау:

- Пакет сүзгіші *(screening* – экрандалатын маршрутизатор*)*;
- Сеанстық деңгей шлюзі (экрандалатын көлік);
- Қолданбалы шлюз *(aplication gateway);*
- Эксперттік деңгей шлюзі *(stateful inspection firewall).*

Қолданылатын технология бойынша:

- Протокол жағдайын қадағалау *(stateful inspection);*
- Орадағы модульдер *(proxy).*

Орындалуы бойынша:

- Программа – аппараттық;
- Программалық.

Қосылу схемасы бойынша:

- Желіні қорғаудың ортақ схемасы;
- Қорғалатын жабық және қорғалмайтын ашық желі сегменттерінің схемасы;
- Бөлек жабық қорғау мен ашық желі сегментінің схемасы.

Ақпараттық ағымдарды сүзгілеу олардың экран арқылы таңдап өткізу кейбір түрлендірулердің жасалуынан тұрады. Сүзгілеу таңдалған қауіпсіздік ережелеріне сәйкес, желіаралық экранға алдын ала жүктелген ережелер арқылы жүзеге асады. Сондықтан да желіаралық экранды ақпараттық ағымды өңдейтін сүзгі ретінде қарастырған ыңғайлы.

Фильтрдің әрқайсысы бөлек сүзгілерді мына жолдармен интерпретациялау үшін арналған:

1. интерпретацияланатын критерий ережелеріне сәйкес ақпаратты анализдеу, мысалы қабылдаушы адресі бойынша және ақпарат арналған жіберушіге немесе түсініктеме түріне.

2. интерпретацияланатын ереженің біреуі негізінде келесі шешімдерді қабылдау:

- берілгендерді тастап кетпеу;
- алушы атынан берілгендерді өңдеу және жіберушіге қорытындыны жіберу;
- анализді жалғастыру үшін берілгендерді келесі сүзгіге жіберу;
- келесі фильтрлардан берілгендерді өткізіп жіберу.

Сүзгілеудің ережесін жалғастырушы функциясына жататын қосымша іс - әрекеттерде бере алады, мысалға берілгендерді өңдеу, оқиғаларды тіркеу және т.б. Соған байланысты сүзгілеу ережесі орындалуына байланысты шарттарды анықтайды:

- алдағы берілгендердің жіберілуін шектеу немесе шешу;

- қосымша қорғаныс функцияларының орындалуы;

Ақпараттық ағымның талдауының критерийлері ретінде келесі шамалар қолданыла алады:

- желілік адрестерден, индикаторлардан, интерфейс адресінен, порттар номерінен және де басқа мәні бар берілгендерден тұратын хабарламалар пакетінің қосымша өрістері;
- мысалы компьютерлік вирустың бар жоғына тексеретін хабарлама пакеттерінің құрамы;
- ақпараттық ағымның сыртқы мінездемелері, мысалы уақытша, жиілік мінездемелер, берілгендердің көлемі және т.б.

Қолданылып отырған анализ критерийлері сүзгілеу жүзеге асырып жатқан OSI моделінің деңгейіне байланысты болады. Жалпы жағдайда желіаралық экран сүзгілеуден өткізіп жатқан пакеттің неғұрлым OSI моделінің деңгейі жоғары болса, соғұрлым ол қамтамасыз ететін қорғаныс деңгейі де жоғары болады.

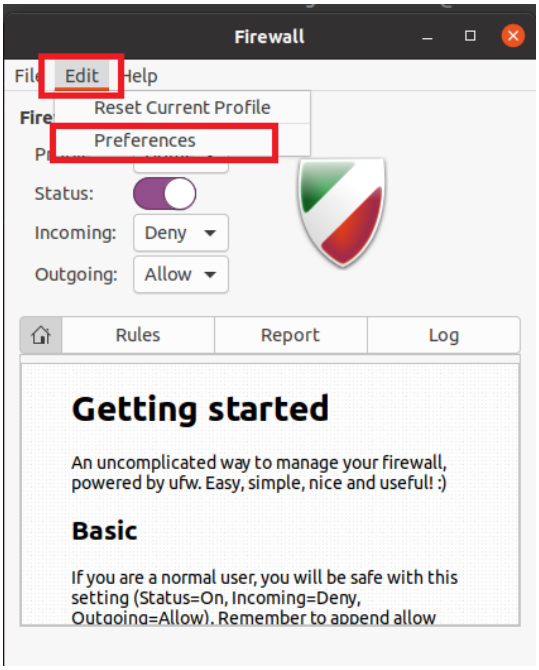
Желіаралық экран жалғаушы функциясы экрандалатын агент немесе *жалғаушы* - *программа* деп аталатын арнайы программалар арқылы орындалады. Бұл программалар резидентті болып табылады және ішкі және сыртқы желілер арасындағы ретсіз ақпарат алмасуға рұқсат бермейді.

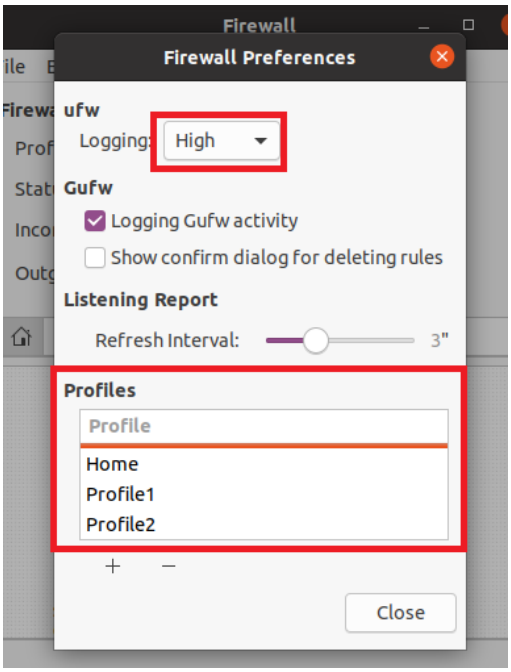
Үнсіз келісім бойынша Ubuntu жүйесінде орнатылған желіаралық экран – **Uncomplicated Firewall – ufm** – қарастырайық:

Желіаралық экранды орнату командасы

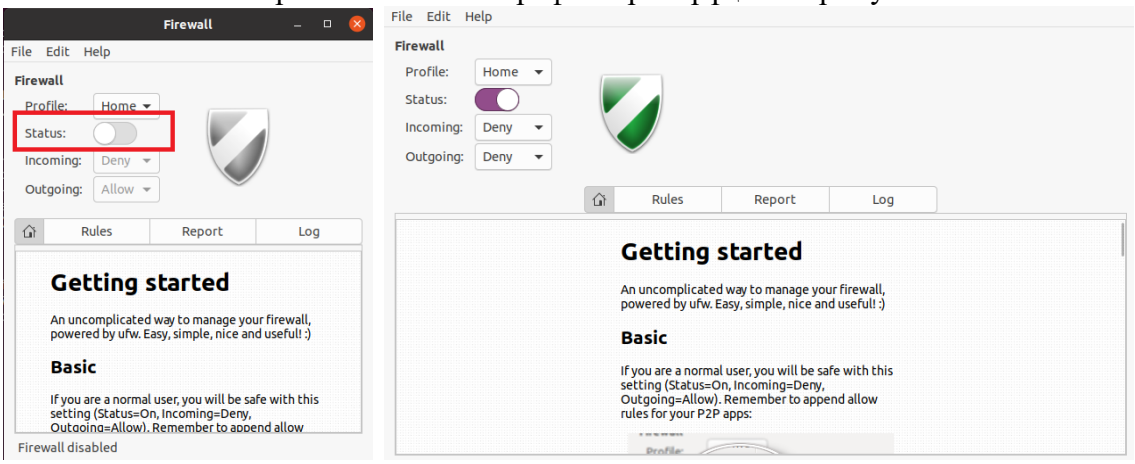
Қосымшадан желіаралық экранды жүктейміз

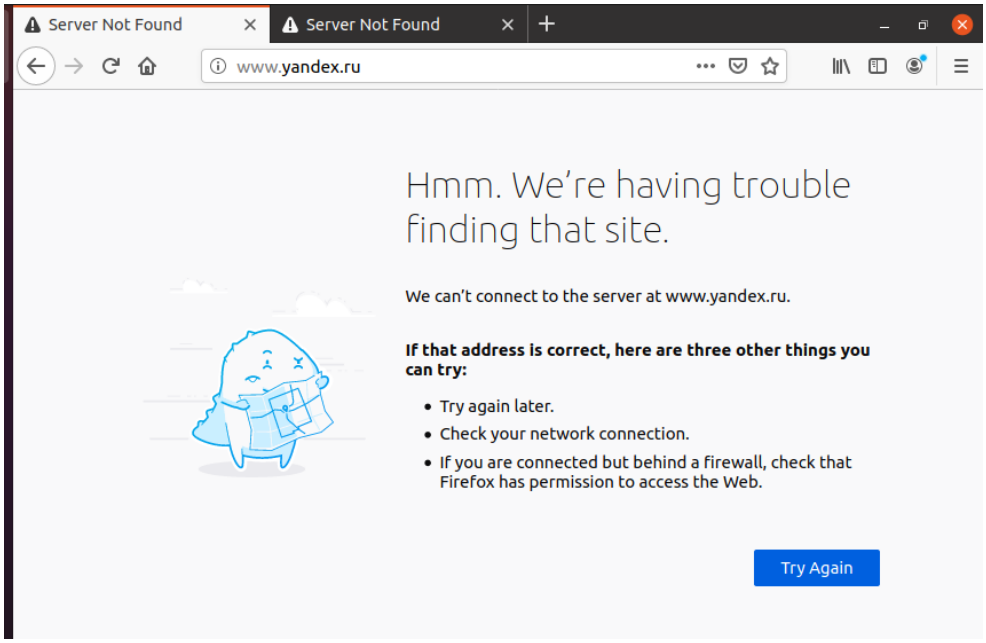
«Edit-Preferences» (Правка - Настройка) командасы арқылы желіаралық экранның жалпы қасиеттер бөлімін дайын режімдер арқылы өзгерте аламыз. Кіріс және шығыс трафиктеріне қарай ғана қасиеттер өзгереді.

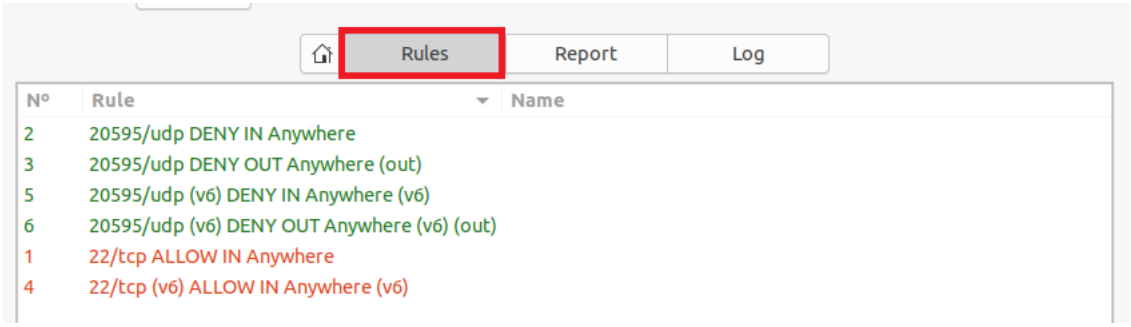


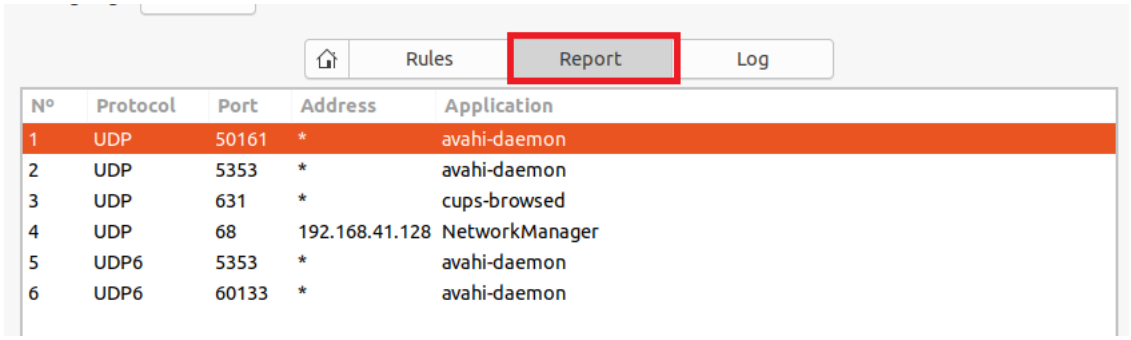


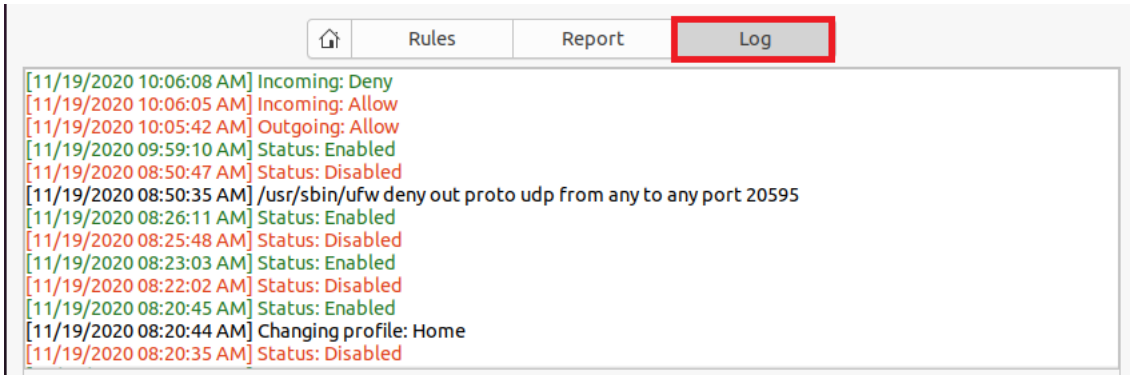
Кіріс және шығыс трафиктеріне рұқсат бермеу



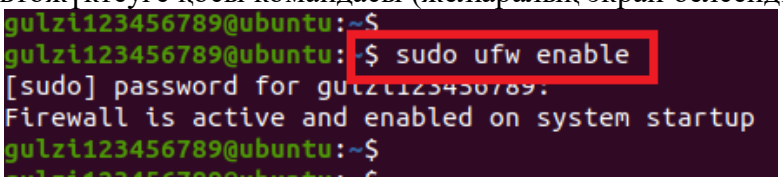

Server Not Found
Server Not Found
www.yandex.ru
Hmm. We're having trouble finding that site.
We can't connect to the server at www.yandex.ru.
If that address is correct, here are three other things you can try:
Try again later.
Check your network connection.
If you are connected but behind a firewall, check that Firefox has permission to access the Web.
Try Again


Rules
Report
Log
N°
Rule
Name
2 20595/udp DENY IN Anywhere
3 20595/udp DENY OUT Anywhere (out)
5 20595/udp (v6) DENY IN Anywhere (v6)
6 20595/udp (v6) DENY OUT Anywhere (v6) (out)
1 22/tcp ALLOW IN Anywhere
4 22/tcp (v6) ALLOW IN Anywhere (v6)

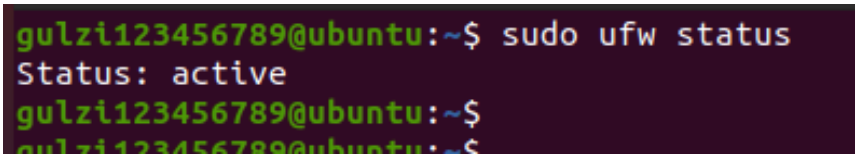

Rules
Report
Log
N° Protocol Port Address Application
1 UDP 50161 * avahi-daemon
2 UDP 5353 * avahi-daemon
3 UDP 631 * cups-browsed
4 UDP 68 192.168.41.128 NetworkManager
5 UDP6 5353 * avahi-daemon
6 UDP6 60133 * avahi-daemon

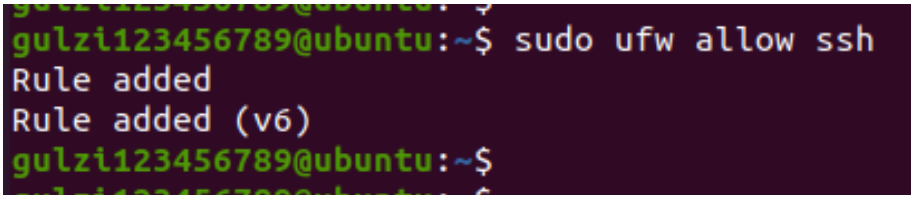

Rules
Report
Log
[11/19/2020 10:06:08 AM] Incoming: Deny
[11/19/2020 10:06:05 AM] Incoming: Allow
[11/19/2020 10:05:42 AM] Outgoing: Allow
[11/19/2020 09:59:10 AM] Status: Enabled
[11/19/2020 08:50:47 AM] Status: Disabled
[11/19/2020 08:50:35 AM] /usr/sbin/ufw deny out proto udp from any to any port 20595
[11/19/2020 08:26:11 AM] Status: Enabled
[11/19/2020 08:25:48 AM] Status: Disabled
[11/19/2020 08:23:03 AM] Status: Enabled
[11/19/2020 08:22:02 AM] Status: Disabled
[11/19/2020 08:20:45 AM] Status: Enabled
[11/19/2020 08:20:44 AM] Changing profile: Home
[11/19/2020 08:20:35 AM] Status: Disabled

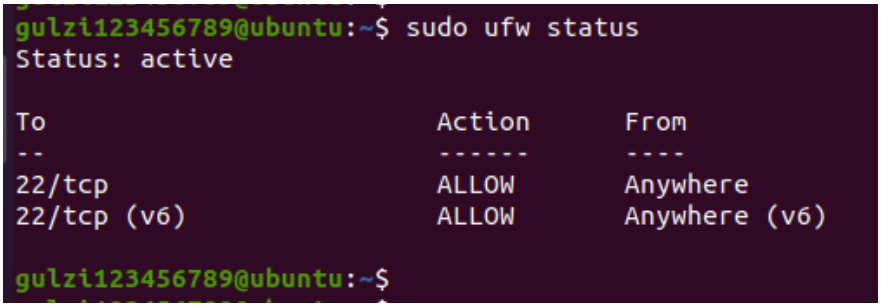
Автожүктеуге қосы командасы (желіаралық экран белсенді)



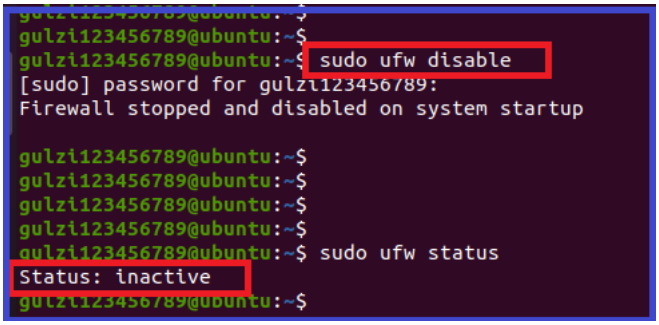
Желіаралық экран белсенді хабарламасы





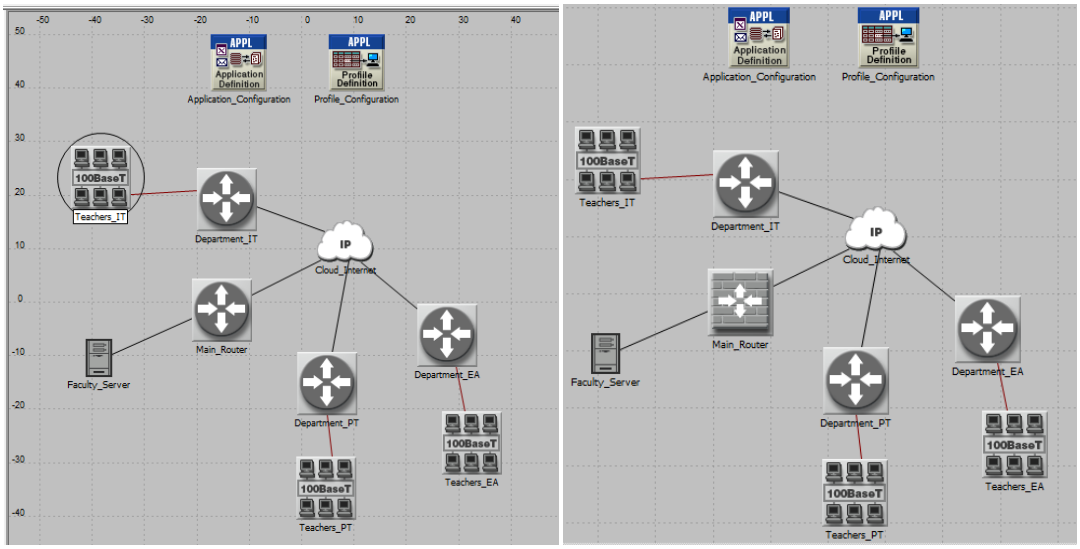


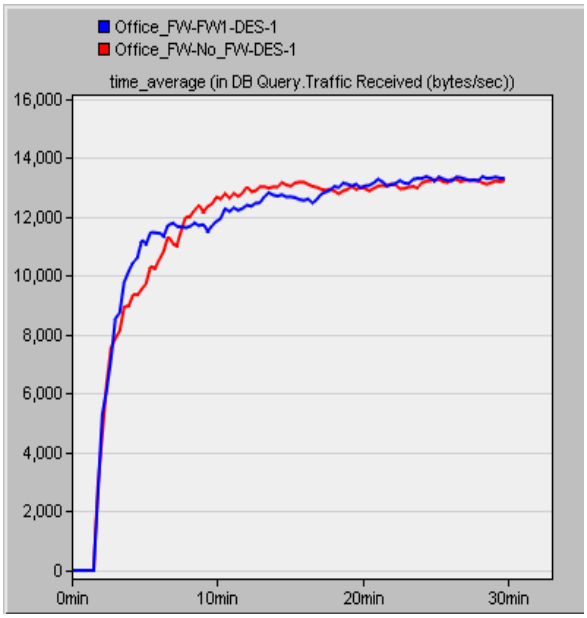
IPTABLES

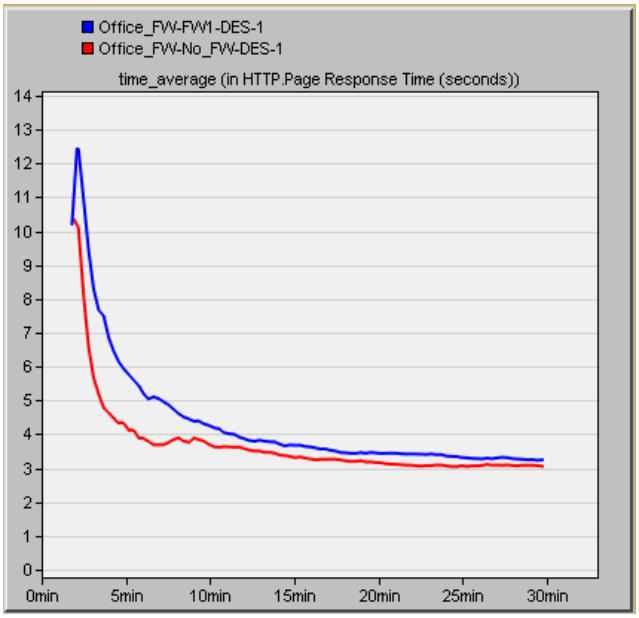


```
root@ubuntu:/home/gulzi123456789# iptables -h
iptables v1.8.4

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)

Commands:
Either long or short options are allowed.
  --append  -A chain            Append to chain
  --check   -C chain            Check for the existence of a rule
  --delete  -D chain            Delete matching rule from chain
  --delete  -D chain rulenum
                                Delete rule rulenum (1 = first) from chain
  --insert  -I chain [rulenum]
                                Insert in chain as rulenum (default 1=first)
```

Ішкі желіден сыртқы желіге немесе керісінше қол жеткізу қажет болған жағдайда, ең алдымен желіаралық экран компьютерде функционалдайтын жалғаушы – программамен логикалық байланыс орнатылуы қажет. Жалғаушы программа сұралған желіаралық байланысты тексеріп, ол шешілетін болса өзі керекті компьютермен байланыс орнатады. Әрі қарай ішкі және сыртқы желі компьютерлері арасындағы байланыс программалық жалғауыш арқылы жүзеге асады, ол өз кезегінде келген ақпаратты сүзгіден өткізіп, басқа да қорғаныс функцияларын орындайды.







Желіаралық экран жалғауыш-программа көмегінсіз сүзгілеу функциясын жүзеге асыра алады, бұл жағдайда ол ішкі және сыртқы желі арасында мөлдір өзара байланысты қамтамасыз етеді. Сонымен қатар жалғауыш-программа хабарламаларды сүзгілеуден өткізуді жүзеге асыра алмауы да мүмкін.