Зертханалық сабақ №12:Linux ОЖ негізіндегі IPTABLES пакеттік сүзгісі

Iptablesутилитасы-Linux операциялықжүйелерінеарналғанбрандмауэр. Iptables ережелерінқолданаотырып, трафиктіңөтуінеруқсатберугенемесебұғаттауғаболады. Ағымдағымашинаменбайланысорнатуғатырысқанкезде, iptables бұлжағдайданеістеукеректігінтүсінуүшінтізімдегіережелертізімінқарайды. Егерережеболмаса, әдепкіәрекеторындалады.

Ережелертізбегі

Ережелержиынтығытізбектердеқалыптасады, негізгіжәнежекетізбектербар. Негізгітізбектертізімі:

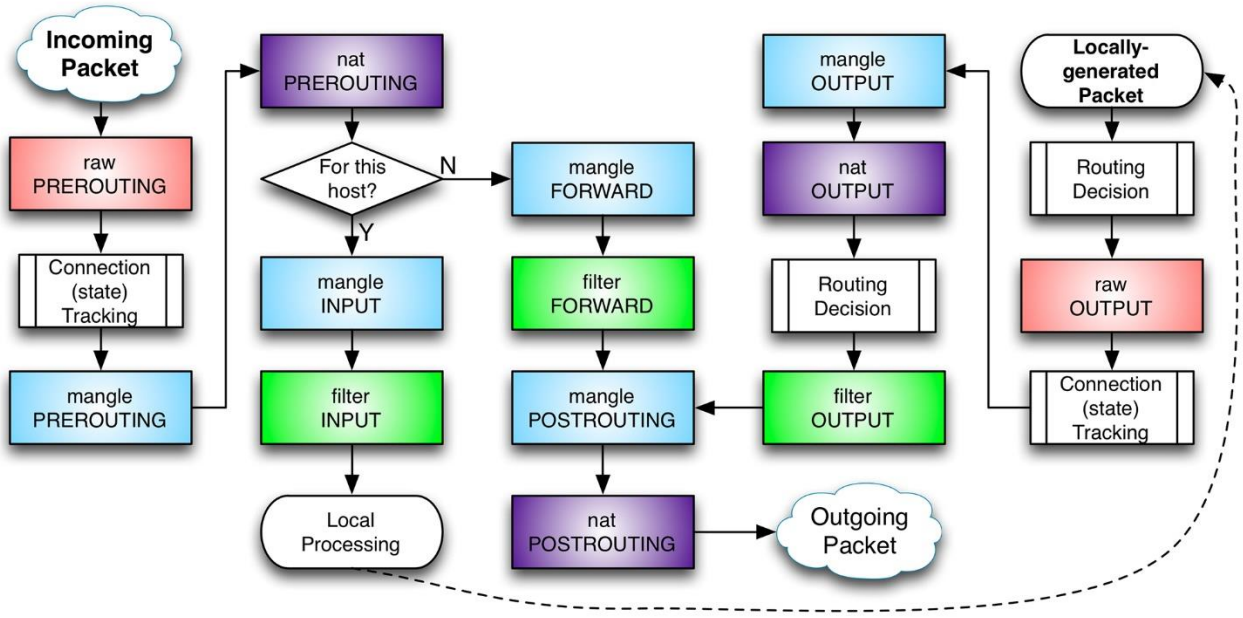
* PREROUTING-осытізбектегіережелержелілікинтерфейскесырттанкелетінбарлықпакеттергеқолданылады

* INPUT-хосттыңөзіненемесеосыхосттағыпроцескеарналғанпакеттергеқолданылады

* FORWARD-хостарқылыөтетінтранзиттікпакеттергекідіріссізқолданылатынережелер

* OUTPUT-хосттыңөзінемесеосыхосттағыпроцестержасағанпакеттергеқолданылады

* POSTROUTING-берілгенхосттыңжелілікинтерфейсіненкетуікерекпакеттергеқолданылады



Iptables кестелері

Iptables — теережелертізбегініңүстіндеабстракцияныңтағыбірдеңгейібар-кестелер. Кестелерпакеттердеәртүрліәрекеттердіорындауғаарналған, мысалы, өзгертунемесесүзу:

* raw-шикіпакеттерменжұмысістеугеарналған, оларәліөңделмеген

* mangle-әртүрліпакеттақырыптарынөзгертугеарналған

* Nat-сервермаршрутизаторретіндепайдаланылса, Nat жұмысынқамтамасызетеді

*filter-әдепкібойыншапайдаланылатынпакеттердісүзугеарналғаннегізгікесте

Жұмыс принципі

Кіріспакетінбрандмауэр mangle кестесіндегі PREROUTING тізбегіненөңдейбастайды. Соданкейінол nat кестесінің PREROUTING тізбегіережелеріменөңделеді. Бұлкезеңдепакеттіңмақсатынөзгерту (DNAT) қажетпе, жоқпатексеріледі. Тағайындаудықазірөзгертумаңызды, өйткеніпакеттіңбағыты PREROUTING тізбегіненшыққаннанкейінбірденанықталады. Осыданкейінол INPUT тізбегіне (егерпакеттіңмақсатыосыкомпьютерболса) немесе FORWARD (егероныңмақсатыжелідегібасқакомпьютерболса) жіберіледі.

Егерпакеттіңмақсатыбасқакомпьютерболса, ондапакет Mangle және filter кестелерінің FORWARD тізбегіережелеріменсүзіледі, соданкейіноған POSTROUTING тізбегіережелеріқолданылады. Бұлкезеңде SNAT/MASQUARADE (көздіауыстыру/жасыру) қолдануғаболады. Осыәрекеттерденкейінпакет (егераманқалса) желігежіберіледі.

Егерпакеттіңмақсатыбрандмауэрібаркомпьютердіңөзіболса, ондабағыттауданкейінол Mangle және filter кестелерініңкірістізбегіережелеріменөңделеді. Тізбектеröткенжағдайдапакетқосымшағаберіледі.

Бағдарламабрандмауэрменжұмысістегенкезде, сұрауғажауапберединемесеөзініңпакетінжібереді, соданкейінол filter кестесіңШығыстізбегіменөңделеді. Соданкейіноған NAT кестесіңшығутізбегініңережелеріқолданылады — DNAT (мақсаттыөзгерту) қажетпе, жоқпа, соныанықтауүшін. Әріқарай, пакет filter кестесіңШығыстізбегіменсүзіледіжәне SNAT және QoS қолданаалатын POSTROUTING тізбегіндеқолжетімді. POSTROUTING сәттіöткенжағдайдапакетжелігешығады.

Iptables утилитасы

Iptables утилитасының синтаксисі:

```
$sudoiptables [-t таблица] команда [критерий действие]
```

Копировать

Егер кесте көрсетілмесе, filter кестесі қабылданады. Командалар келесідей болуы мүмкін:

- - A (немесе --append) - ережені тізбекке қосыңыз
- - D (немесе --delete) — ережені тізбектен алып тастаңыз
- - I (немесе --insert) - ережені көрсетілген нөмірдің астына тізбекке салыңыз
- - L (немесе --list) — берілген тізбектің барлық ережелерін көрсету
- - F (немесе --flush) — берілген тізбектің барлық ережелерін тазалаңыз (кестелер)
- - N (немесе --new-chain) — жаңа тізбек жасаңыз
- - X (немесе --delete — chain) - тізбекті жою
- - P (немесе --policy) - тізбектің әдепкі әрекетін орнатыңыз
- Келесі қосымша опциялар бар:

- * — v (немесе --verbose) - хабарламалардың егжей-тегжейін көбейтіңіз, --list командасымен көрсетілген кезде интерфейс атауы, ережелер параметрлері және TOS маскалары көрсетіледі.
-
-
  - * — n (немесе --numeric)-IP мекенжайлары мен порт нөмірлерін сандық түрде шығарып, оларды символдық атауларға айналдыруға жол бермейді.
  - * --line-numbers — --list пәрменімен ережелер тізімін көрсету кезінде жол нөмірлерін көрсету (жол нөмірі тізбектегі ереже позициясына сәйкес келеді).
  - Қызметтік бағдарламаны пайдалану мысалдары:
  -
- $sudoiptables -F# сбросить все правила в таблице filterКопировать

```
$sudoiptables -tnat -F#nat кестесіндегі барлық ережелерді қалпына келтіруКопировать
$sudoiptables -L --line-numbers#нөмірленген filter кестесіндегі барлық ережелерді қарауКопировать
$sudoiptables -L -v --line-numbers#нөмірленген filter кестесіндегі барлық ережелерді қараңыз (толығырақ)Копировать
$sudoiptables -tnat -L --line-numbers#Nat кестесіндегі барлық ережелерді нөмірлеу арқылы қараңызКопировать
$sudoiptables -DINPUT3  #filter кестесіндегі input тізбегіндегі ережені нөмір бойынша жойыңызКопировать
$sudoiptables -IINPUT -ptcp --dport 80 -jACCEPT#filter кестесіндегі енгізу тізбегінің басына ережені енгізуКопировать
$sudoiptables -AINPUT -ptcp --dport 80 -jACCEPT#сүзгі кестесіндегі енгізу тізбегінің соңына ереже қосыңызКопировать
$sudoiptables -IINPUT 3 -ptcp --dport 80 -jACCEPT#сүзгі кестесіндегі ережені енгізу тізбегінің үшінші орнына салыңыз
```

Әдеттегі әрекет

Брандмауэрді орнатуды бастамас бұрын, әдепкі ережелер тізбегінің әрекеті қандай болуы керек екенін шешу керек. Басқаша айтқанда, егер Байланыс конфигурацияланған ережелердің кез-келгеніне сәйкес келмесе, iptables не істеу керек?

Бастапқыда, filter кестесінің барлық үш тізбегі әдепкі бойынша трафикті қабылдауға мүмкіндік береді

```
$sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
targetprotoptsourcedestinationКопировать
```

Егербірнәрсеөзгерсе, ендісізбұрынғыпараметрлердіқайтаруыңызкерекболса, мұныпәрмендердіңкөмегіменжасайаласыз:

```
$sudoiptables -PINPUTACCEPT
```

```
$sudo iptables -P OUTPUT ACCEPT
$sudoiptables -PFORWARDACCEPTКопировать
```

Сізбасқажолменжүреаласызжәнеалдыменбарлықтрафиккетыйымсалып, соданкейінонытаңдамалытүрдешешеаласыз:

```
$sudo iptables -P INPUT DROP
$sudo iptables -P OUTPUT DROP
$sudoiptables -PFORWARDDROPКопировать
```

Байланыстарәрекеттер

Әдепкімінез-құлықтыорнатқаннанкейін, iptables нақтыпакетпеннеістеукеректігінтүсінуіүшінтрафиктібасқаруережелерінжасауғакірісугеболады.

* ACCEPT-пакетосытізбектеншығып, келесігежіберіледі

* DROP-пакеттітастаңыз, пакеткелесітізбеккеберілмейді

* REJECT-пакеттітастаңыз, пакетжіберушісінеқатетуралыхабарлаңыз

* SNAT-пакеттегі, NAT кестесінің POSTROUTING және OUTPUT тізбектеріндегі IP мекенжайынауыстыру

* DNAT-пакетте, nat кестесінің PREROUTING тізбегінде (кейде — OUTPUT-та) тағайындалған ip мекенжайынауыстыру)

* LOG - пакеттіжурналфайлынажазыңыз (syslog демонынажіберіледі) жәнеқалғанережелерменөңдеңіз

* MASQUERADE-SNAT сияқты, бірақдинамикалық ip-мекен-жайыбарқосылыстарүшін, nat кестесінің POSTROUTING тізбегінде

* MARK-пакеткебелгіқойыңызжәнеқалғанережелерменөңдеңіз

Пакеттергеарналғанкритерийлер

Жалпықритерийлер-кез-келгенережедеқолдануғаболады, олархаттаманыңтүрінебайланыстыемесжәнекеңейтумодульдерінжүктеудіқажететпейді:

- * - p (немесе --protocol) - Протоколтүрінкөрсетуүшінқолданылады (all, icmp, tcp, udp)
- • - s (немесе --source) — көздің ip мекенжайынкөрсетуүшінқолданылады; жалғыз ip мекенжайын (10.10.10.10) немесе IP мекенжайларыныңауқымын (10.10.10.0/24) көрсетугеболады)
- • - d (немесе — destination)-тағайындалғанжердің ip мекенжайынкөрсетуүшінқолданылады; жалғыз ip мекенжайын (10.10.10.10) немесе IP мекенжайларыныңауқымын (10.10.10.0/24) көрсетугеболады)
- * - i (немесе --in — interface) - пакеталынғанинтерфейстек INPUT, FORWARD және PREROUTING тізбектеріндеруқсатетіледі; бұлкритерийболмағанжағдайдакезкелгенинтерфейсболжанады

- * - o (немесе — out-interface) - пакетжіберілетінинтерфейстек OUTPUT, FORWARD және POSTROUTING тізбектеріндеруқсатетіледі; бұлкритерийболмағанкездекез-келгенинтерфейсқабылданады
- Жасырынкритерийлер - кеңейтумодульдерінтолығыменжүктейдіжәне --protocol критерийінкөрсеткенкездеқолжетімдіболады. Олардың кейбірін қарастырайық:
- • - p tcp --sport (немесе --source-port)-TCP пакеті жіберілген бастапқы порт. Параметр ретінде порт нөмірі немесе желі қызметінің атауы көрсетілуі мүмкін.
- * Қызмет атаулары мен порт нөмірлерінің сәйкестігін /etc/services файлынан табуға болады. Порт нөмірлері ең аз және ең көп нөмірлерден интервал түрінде берілуі мүмкін.
- • - p tcp --dport (немесе --destination-port) — TCP пакеті жіберілетін порт немесе порт ауқымы. Дәлелдер --source-port үшін бірдей форматта берілген.
- • - p udp --sport (немесе --source-port)-UDP пакеті жіберілген бастапқы порт. Параметр ретінде порт нөмірі немесе желі қызметінің атауы көрсетілуі мүмкін. Қызмет атаулары мен порт нөмірлерінің сәйкестігін /etc/services файлынан табуға болады. Порт нөмірлері ең аз және ең көп нөмірлерден интервал түрінде берілуі мүмкін.
- • - p udp --dport (немесе --destination-port) — UDP пакеті жіберілетін порт немесе порт ауқымы. Дәлелдер --source-port үшін бірдей форматта берілген.
- Айқын критерийлер-m немесе --match опциясы арқылы кеңейту модульдерін нақты жүктеуді қажет етеді. Мысалы, егер Сіз мемлекеттік критерийді қолдануды жоспарласаңыз, онда сіз нақты көрсетуіңіз керек-m күйі қолданылатын критерийдің сол жағында. Олардың кейбірін қарастырайық:
- • — m conntrack --ctstate STATES-қосылукүйініңбелгісінтексереді: NEW, ESTABLISHED, RELATED және INVALID. Жаңакүйпакеттіңжаңақосылымдыашатынынеместепакетбірбағыттыағынғажататынынбілдіреді. ESTABLISHED күйіпакеттіңорнатылғанқосылымғатиесіліекенінкөрсетеді, оларқылыпакеттерекібағыттадажүреді. RELATED күйіпакеттіңбұрыннанбарқосылымғатиесіліекенінкөрсетеді, бірақолжаңақосылымдыашады. INVALID күйіпакеттіңбелгісізағынменнемесеқосылымменбайланыстыекенінжәнедеректерденемесетақырыптақатеболуымүмкінекенінбілдіреді.

• - m state-state STATES (ескірген, ұсынылмайды) — байланыскүйініңбелгісінтексереді: жаңа, ескірген, RELATED жәнежарамсыз.

• - m multiport --source-port PORTS-Шығыспорттарыныңтізімінкөрсетугеқызметететеді, сіз 15 түрліпорттардыкөрсетеаласыз. Тізімдегіпорттардыңатауларыбір-бірінеңүтірменбөлінуікерек, тізімдегібосорындарғажолберілмейді. Онытек p TCP немесе-p udp өлшемдеріменбіргеқолдануғаболады. Негізінен --source-port әдеттегіөлшемініңкеңейтілгеннұсқасыретіндепайдаланылады.

• - m multiport --destination — port PORTS-кіріспорттарыныңтізімінкөрсетугеқызметететеді, сіз 15 түрліпорттардыкөрсетеаласыз. Тізімдегіпорттардыңатауларыбір-бірінеңүтірменбөлінуікерек, тізімдегібосорындарғажолберілмейді. Онытек p TCP немесе-p udp өлшемдеріменбіргеқолдануғаболады. Негізіненәдеттегі --destination-port критерийініңкеңейтілгеннұсқасыретіндеқолданылады.

• - m multiport --port PORTS-пакеттіңШығысжәнекіріспортынтексереді. Аргументтерформаты --source-port және --destination-port өлшемдерінеұқсас. Бұлкритерийекібағыттағыпорттардытексереді, егеркритерийберілгенболса-m multiport --port 80 — оныңастына 80 портынан 80 портынабаратынпакеттертүседі.

* - m mac — Mac-source MAC-Mac-пакеттіXX:XX:XX:XX:XX:XX: XX форматындабергенжеліліктүйіннің MAC мекен-жайы. Бұлтек PREROUTING, FORWARD және INPUT тізбектеріндежәнебасқажердемағынасыбар.

• - m iprange --src-range IP-IP-көздің ip мекенжайларыныңауқымынкөрсетугемүмкіндікбереді, мысалы 192.168.1.10-192.168.2.20

• - m iprange --dst-range IP-IP-192.168.1.10-192.168.2.20 сияқтытағайындалған ip ауқымынкөрсетугемүмкіндікбереді

Байланыскүйініңкритерийі

Жоғарыдаайтылғандай, көптегенпротоколдарекіжақтыбайланыстықажететеді. Мысалы, SSH қосылуларынаруқсатбергіңізкелсе, INPUT тізбегінеде, OUTPUT тізбегінедеережелеркосуыңызкерек. Егерсізтексервергекіретін SSH қосылуларынаруқсатбергіңізкелсе (яғнитек SSH арқылысервергеқосылумүмкіндігіболса) ше? OUTPUT тізбегінеережеқосушығатын SSH қосылуларынамүмкіндікбередіме (яғнисерверден SSH арқылыбасқахостқақосылуғаболады)?

Мұндайжағдайларүшінбайланыскүйлеріқолданылады. Оларсізгебелгілібірбағыттағыбайланыстарғағанаруқсатетілгенекіжақтыбайланыстысипаттауғамүмкіндікбереді. Төмендегімысалда 10.10.10.10 хостынан SSH қосылыстарыруқсатетілген, бірақсолхостқа SSH қосылыстарытыйымсалынған. Алайда, байланысорнатылғанжағдайда, жүйеге SSH арқылыақпаратжіберугеруқсатетіледі, бұлхосттарарасындағы SSH байланысынмүмкінетеді:

```
$sudo iptables -A INPUT -p tcp --dport 22 -s 10.10.10.10 -m state --state
NEW,ESTABLISHED -j ACCEPTКопировать
$sudo iptables -A OUTPUT -p tcp --sport 22 -d 10.10.10.10 -m state --state
ESTABLISHED -j ACCEPTКопировать
```

Өзгерістердісақтау

Ережелертізбегінеенгізілгенөзгертулерқайтажүктеукезіндежоғалады, сондықтанолардыпәрмендіпайдаланыпфайлғасақтауқажет:

```
$sudo /sbin/iptables-save > /etc/iptables.rulesКопировать
$cat /etc/iptables.rulesКопировать
# Generated by iptables-save v1.6.1 on Sat Feb 15 11:58:32 2020
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -p udp -m udp --sport 53 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --sport 53 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 80 -j ACCEPT
```

```
-A OUTPUT -p tcp -m tcp --sport 443 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Sat Feb 15 11:58:32 2020Копировать
```

Қайтажүктеуденкейінережелерді/etc/iptables.rules файлынанкелесіпәрмендіқалпынакелтіругеболады:

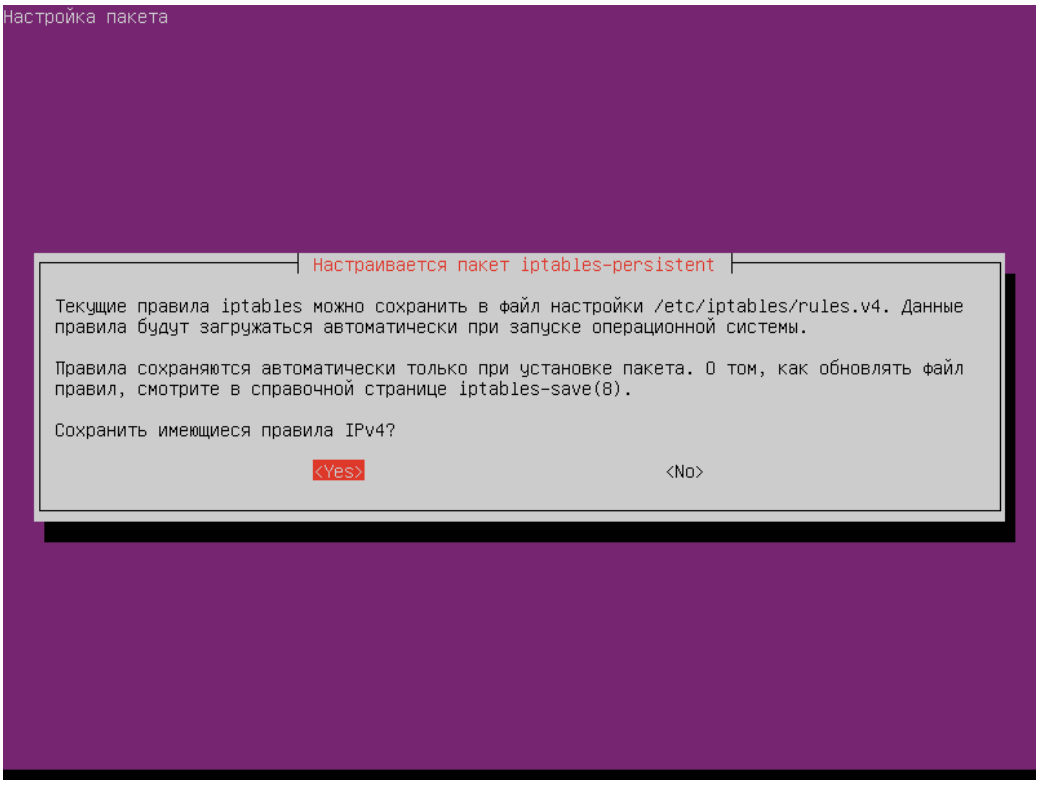
```
$sudoiptables-restore< /etc/iptables.rulesКопировать
```

Автоматтыжүктеуережелері

Әрқайтажүктелгенненкейінережелердіқолменқалпынакелтіруыңғайсызекенітүсінікті. Сондықтанбізiptables-persistent пакетінорнатамыз:

```
$sudoaptinstalliptables-persistentКопировать
```

- Буманыорнатқанкездесізден iptables қолданыстағыережелерінсақтаусұралады:
- • IPv4 үшін /etc/iptables/rules.v4 файлына
- • IPv6 протоколыүшін/etc/iptables/rules.v6 файлына



Енді ережелерге өзгертулер енгізілгеннен кейін, сіз ағымдағы күйді /etc/iptables/rules.v4 файлына сақтауыңыз керек, сонда бұл күй қайта жүктелгеннен кейін қалпына келтіріледі:

```
$sudo iptables-save > /etc/iptables/rules.v4Копировать
```

Буманыорнатқаннанкейінnetfilter-persistent.serviceжаңақызметіқосылады, олжүктеукезіндеiptables ережелерінқалпынакелтіреді:

```
$systemctl status netfilter-persistent.service
● netfilter-persistent.service - netfilter persistent configuration
   Loaded: loaded (/lib/systemd/system/netfilter-persistent.service;
enabled; vendor preset: enabled)
   Active: active (exited) since Wed 2020-02-05 10:08:52 MSK; 27s ago
 Main PID: 3769 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 2317)
   CGroup: /system.slice/netfilter-persistent.service

фев 05 10:08:52 ubuntu-iptables systemd[1]: Starting netfilter persistent
configuration...
фев 05 10:08:52 ubuntu-iptables systemd[1]: Started netfilter persistent
configuration.Копировать
```

Судя по всему, скоро пакет `iptables-persistent` будет заменен на пакет `netfilter-persistent` (сейчас он устанавливается как зависимость при установке `iptables-persistent`).

Барлық ережелерді алып тастау

`Filter`кестесінің барлық конфигурацияланған ережелерін жою үшін келесі пәрменді қолдануға болады:

```
$sudoiptables -FКопировать
```

Nat кестесінің барлық теңшелген ережелерін жою үшін пәрменді пайдалануға болады:

```
$sudoiptables -tnat -FКопировать
```

Веб-серверді конфигурациялауға арналған мысал

1. OUTPUTүшін ACCEPTсаясаты

Ең алдымен, біз әдепкі саясатты орнаттық:

```
$sudo iptables --policy INPUT DROP
$sudo iptables --policy OUTPUT ACCEPT
$sudo iptables --policy FORWARD DROPКопировать
```

Loopback интерфейсі арқылы трафикке рұқсат етіңіз (ping localhost үшін жұмыс істейді):

```
$sudo iptables -A INPUT -i lo -j ACCEPTКопировать
```

Көптегенқосымшаларөзараалмасуүшінкеріциклинтерфейсінпайдаланадыжәнеосыережесізмұндайқосымшалардыңжұмысыбұзылады.

Егерсізорнатуғаөтефанатикалықемесболсаңыз, ондасіз ICMP протоколыныңжұмысынаруқсатбереаласыз (ping және traceroute жұмысістейді):

```
$sudo iptables -A INPUT -p icmp -j ACCEPTКопировать
```

ICMP (желіаралық басқару хабарламаларының ХАТТАМАСЫ) - TCP/IP хаттамаларының стекіне кіретін желілік хаттама. Негізінен, ICMP қате туралы хабарламаларды және деректерді беру кезінде пайда болған басқа ерекше жағдайларды жіберу үшін қолданылады.Утилита `ping`, служащаядляпроверкивозможностидоставкиIP-пакетов, используетICMP-сообщениястипом 8 (эхо-запрос) и 0 (эхо-ответ). Утилита `traceroute`, отображающая путь следования IP-пакетов, использует ICMP-сообщения с типом 11.

Біздің серверге DNS серверлерінен жауап алуға рұқсат береміз:

```
$sudo iptables -A INPUT -p udp --sport 53 -m state --state ESTABLISHED -j
ACCEPT
$sudo iptables -A INPUT -p tcp --sport 53 -m state --state ESTABLISHED -j
ACCEPTКопировать
```

Көпжағдайда UDP протоколы DNS хабарламаларыүшінқолданылады. Бірақ егер хабарлама 512 Байттан асса-TCP протоколы қолданылады. DNS серверлері 53 портында жұмыс істейді, сондықтан кіріс TCP және UDP трафигіне рұқсат береміз, ол source port 53-пен бірге келеді. Сонымен қатар, біз бұл трафикті біздің серверден сұрауға жауап ретінде түсіндіреміз.

HTTP, HTTPS және SSH порттарына кіріс қосылымдарын рұқсат етіңіз:

```
$sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
$sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
$sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPTКопировать
```

Біздіңвеб-сервер (Apache немесе Nginx) 80 және 443 порттарын, ал SSH сервері 22 портынтыңдайды. Сондықтанбізdestination port 80, 443 және 22-гекелетін TCP трафигінеруқсатбереміз..

Пакеттерді apt утилитасыарқылыорнатуғажәнежаңартуғаболады:

```
$sudo iptables -A INPUT -p tcp --sport 80 -m state --state ESTABLISHED -j
ACCEPTКопировать
```

Біздекез-келгенШығыстрафиккеруқсатетіледі, сондықтанapt утилитасырепозиторийсерверінесұраныстаржібереалады. Бірақоғанәлідежауапалукерек, сондықтанбізкіріс TCP трафигінsource port 80-менбіргежібереміз. Соныменқатар, бізбұлтрафиктібіздіңсерверденсұрауғажауапретіндетүсіндіреміз.

Ендісізқосылғанережелердіпәрменментексереаласыз:

```
$sudo iptables -L -v --line-numbers
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source       destination
1      272 27773 ACCEPT     all  --  lo     any     anywhere     anywhere
2       22  1848 ACCEPT     icmp --  any    any     anywhere     anywhere
3       12  1975 ACCEPT     udp  --  any    any     anywhere     anywhere
udp spt:domain state ESTABLISHED
4        0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp spt:domain state ESTABLISHED
5       18  2313 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:http
6        0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:https
7     2091  140K ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:ssh
8       10  1308 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp spt:http state ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 6 packets, 772 bytes)
```

```
num   pkts bytes target     prot opt in     out     source
destination
```
Копировать

2. OUTPUT үшін DROPсаясаты

БұлжағдайдаINPUT тізбегініңбарлықережелерібірдейболады, бірақOUTPUT тізбегіүшінережелердіқосукерек. Сонымен, біріншіқадам-әдепкісаясаттыорнату:

```
$sudoiptables --policyINPUTDROP
$sudo iptables --policy OUTPUT DROP
$sudo iptables --policy FORWARD DROP
```
Копировать

Loopbackинтерфейсі арқылы трафикке рұқсат береміз :

```
$sudo iptables -A INPUT -i lo -j ACCEPT
$sudo iptables -A OUTPUT -o lo -j ACCEPT
```
Копировать

ICMP протоколының жұмысына рұқсат береміз (ping жәнеtracerouteжұмыс жасайды):

```
$sudo iptables -A INPUT -p icmp -j ACCEPT
$sudo iptables -A OUTPUT -p icmp -j ACCEPT
```
Копировать

Біздіңсерверге DNS серверлерінесұрауларжіберугеруқсатбереміз:

```
$sudo iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
$sudo iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
```
Копировать

Біздіңсерверге DNS серверлерінесұрауларжіберугемүмкіндікбереміз:

```
$sudo iptables -A INPUT -p udp --sport 53 -m state --state ESTABLISHED -j
ACCEPT
$sudo iptables -A INPUT -p tcp --sport 53 -m state --state ESTABLISHED -j
ACCEPT
```
Копировать

HTTP, HTTPS және SSH порттарынакірісқосылымдарынрұқсатетіңіз:

```
$sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
$sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
$sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```
Копировать

Пакеттерді HTTP, HTTPS және SSH порттарынанжіберугеруқсатетіңіз:

```
$sudo iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
$sudo iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT
$sudo iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
```
Копировать

Пакеттердіapt утилитасыарқылыорнатуғажәнежаңартуғаболады:

```
$sudo iptables -A INPUT -p tcp --sport 80 -m state --state ESTABLISHED -j
ACCEPT
$sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
```
Копировать

Ендісізқосылғанережелердіпәрменментексереаласыз:

```
$sudo iptables -L -v --line-numbers
Chain INPUT (policy DROP 6 packets, 623 bytes)
num   pkts bytes target     prot opt in     out     source       destination
```

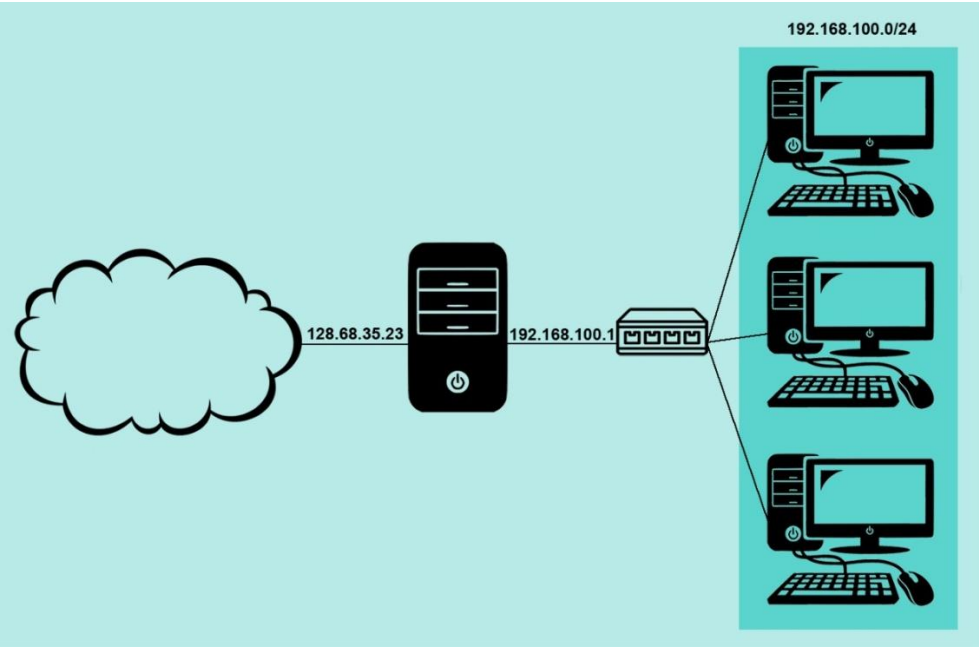
```
1        53  5876 ACCEPT     all  --  lo     any     anywhere     anywhere
2         0     0 ACCEPT     icmp --  any    any     anywhere     anywhere
3        16  2808 ACCEPT     udp  --  any    any     anywhere     anywhere
udp spt:domain state ESTABLISHED
4         0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp spt:domain state ESTABLISHED
5        35  3480 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:http
6         0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:https
7       936 63201 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:ssh
8        50 92195 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp spt:http state ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source       destination

Chain OUTPUT (policy DROP 6 packets, 772 bytes)
num   pkts bytes target     prot opt in     out     source       destination
1        53  5876 ACCEPT     all  --  any    lo      anywhere     anywhere
2         0     0 ACCEPT     icmp --  any    any     anywhere     anywhere
3        16  1244 ACCEPT     udp  --  any    any     anywhere     anywhere
udp dpt:domain
4         0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:domain
5        18 22936 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp spt:http
6         0     0 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp spt:https
7       657 80901 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp spt:ssh
8        69  4613 ACCEPT     tcp  --  any    any     anywhere     anywhere
tcp dpt:http
```


Маршрутизатордың настройкасы

Екі желілік интерфейсі бар компьютер бар. Бірінші eth0 интерфейсі интернетті қарайды және 128.68.35.23 ақ IP мекен-жайы бар. Екінші интерфейс eth1 жергілікті желіге қарайды және 192.168.100.1 IP мекен-жайы бар.



Интернетке қол жетімділік (SNAT)

Бұл компьютер 192.168.100.0 / 24 Жергілікті желісінен барлық компьютерлер үшін Интернетке шығуды қамтамасыз етуі керек. Әдепкі бойынша, транзиттік трафик өшірілген, сондықтан /etc/sysctl файлын өңдеңіз.conf:

```
$sudonano /etc/sysctl.conf
net.ipv4.ip_forward=1
```

Параметрлер күшіне енуі үшін:

```
$sudosysctl -p
```

Енді `iptables ті` орнатамыз:

```
$sudoiptables -PFORWARDDROP
$sudo iptables -A FORWARD -i eth1 -o eth0 -s 192.168.100.0/24 -j ACCEPT
$sudo iptables -A FORWARD -i eth0 -o eth1 -d 192.168.100.0/24 -j ACCEPT
```

Осылайша, біз IP мекен-жайларыүшінтранзиттікпакеттергеруқсатбердік, алқалғандарынатыйымсалынды. Ендібіз SNAT-ті (бастапқыадрестіауыстыру) конфигурациялаймыз, бұлжелідегібарлыққомпьютерлерге128.68.35.23 бір IP-адресарқылыИнтернеткеқосылуғамүмкіндікбереді.

```
$sudo -t nat iptables -A POSTROUTING -s 192.168.100.0/24 -o eth0 -j SNAT --
to-source 128.68.35.23
```

Ішкіжелігеқолжетімділік(DNAT)

Желіішінде192.168.100.2 IP-мекен-жайыбаркомпьютербар, оған RDP арқылыинтернеттенқолжетімділікқажет. Біздіңжергіліктіжелімізгебарлықсұраулар128.68.35.23 IP мекен-жайыбарeth0интерфейсінекеледі. 3389 портынабаратындардытаңдап, оларды192.168.100.2мекен-жайынажібереламыз (DNAT - алушыныңмекен-жайынауыстыру):

```
$sudo iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 3389 -j
DNAT --to-destination 192.168.100.2
```

Өзіндік жұмыстар:

I) Берілген команда нәтижелерін анықтаңыз:

1)
```
root@gulzinat-VirtualBox:/home/gulzinat# iptables -t filter --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

2)
```
root@gulzinat-VirtualBox:/home/gulzinat#
root@gulzinat-VirtualBox:/home/gulzinat# iptables -t mangle --list
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
root@gulzinat-VirtualBox:/home/gulzinat#
```

3)
```
root@gulzinat-VirtualBox:/home/gulzinat# iptables -t nat --list
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
root@gulzinat-VirtualBox:/home/gulzinat#
```

4)
```
root@gulzinat-VirtualBox:/home/gulzinat#
root@gulzinat-VirtualBox:/home/gulzinat# iptables -t raw --list
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@gulzinat-VirtualBox:/home/gulzinat#
```

5)
```
root@gulzinat-VirtualBox:/home/gulzinat# sudo iptables -P FORWARD DROP
```

6)
```
root@gulzinat-VirtualBox:/home/gulzinat# sudo iptables -A INPUT -s 10.10.10.10
-j DROP
```

7)
```
root@gulzinat-VirtualBox:/home/gulzinat#
root@gulzinat-VirtualBox:/home/gulzinat# sudo iptables -A OUTPUT -s 10.10.10.10
 -j DROP
root@gulzinat-VirtualBox:/home/gulzinat#
```

8)
```
root@gulzinat-VirtualBox:/home/gulzinat# iptables -L | grep policy
```

9)
```
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
root@gulzinat-VirtualBox:/home/gulzinat#
```

10)
```
root@gulzinat-VirtualBox:/home/gulzinat#
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
root@gulzinat-VirtualBox:/home/gulzinat#
```

11)
```
root@gulzinat-VirtualBox:/home/gulzinat#  iptables -A INPUT -s 10.10.10.0/24
 -j DROP
root@gulzinat-VirtualBox:/home/gulzinat#
```

12)
```
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       all  --  10.10.10.10          anywhere
DROP       all  --  10.10.10.0/24        anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
root@gulzinat-VirtualBox:/home/gulzinat#
```

13)
```
┌──(gulzi㉿gulzi)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport ssh -s 10.10.10.10 -j DROP
```

14)
```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  10.10.10.10          anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

┌──(gulzi㉿gulzi)-[~]
└─$
```

15)
```
┌──(root㉿gulzi)-[/home/gulzi]
└─# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       10.10.10.10          0.0.0.0/0            tcp dpt:22
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

16)
```
┌──(root㉿gulzi)-[/home/gulzi]
└─# iptables -n -L -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  *      *       10.10.10.10          0.0.0.0/0            tcp dpt:22
2        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
```

17)

```
┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -P INPUT DROP

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -P FORWARD DROP

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -P OUTPUT ACCEPT

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -A INPUT -m state --state NEW,ESTABLISHED -j  ACCEPT

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -L -v -n
Chain INPUT (policy DROP 39 packets, 1248 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       10.10.10.10          0.0.0.0/0           tcp dpt:22
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   25   800 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

18)

```
┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -A INPUT -p tcp --dport 80 -j DROP

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -A INPUT -i eth1 -p tcp --dport 80 -j DROP

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       tcp  --  10.10.10.10          anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state NEW,ESTABLISHED
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

19)

```
┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -A INPUT -p tcp -s 192.168.244.144 --dport 80 -j DROP

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --dport 80 -j DROP

┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       tcp  --  10.10.10.10          anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state NEW,ESTABLISHED
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  192.168.244.144      anywhere             tcp dpt:http
DROP       tcp  --  192.168.1.0/24       anywhere             tcp dpt:http

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

20)

```
┌──(root💀 gulzi)-[/home/gulzi]
└─# iptables -A INPUT -m mac --mac-source AA:0F:EA:81:03:18 -j DROP
```

21)

```
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh MAC AA:0F:EA:81:03:18
DROP       all  --  anywhere             anywhere             MAC AA:0F:EA:81:03:18
```

22)
```
┌──(root💀gulzi)-[/home/gulzi]
└─# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

┌──(root💀gulzi)-[/home/gulzi]
└─# iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP

┌──(root💀gulzi)-[/home/gulzi]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       tcp  --  10.10.10.10          anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state NEW,ESTABLISH
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  192.168.244.144      anywhere             tcp dpt:http
DROP       tcp  --  192.168.1.0/24       anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh MAC AA:
DROP       all  --  anywhere             anywhere             MAC AA:0F:EA:81:03:
DROP       icmp --  anywhere             anywhere             icmp echo-request
DROP       icmp --  anywhere             anywhere             icmp echo-request
```

23)
```
┌──(root💀gulzi)-[/home/gulzi]
└─# ls /lib/modules/$(uname -r)/kernel/net/ipv4/netfilter/
arptable_filter.ko  iptable_raw.ko       ipt_REJECT.ko         nf_log_arp.ko         nf_socket_ipv4.ko
arp_tables.ko       iptable_security.ko  ipt_rpfilter.ko       nf_log_ipv4.ko        nft_dup_ipv4.ko
arpt_mangle.ko      ip_tables.ko         ipt_SYNPROXY.ko       nf_nat_h323.ko        nft_fib_ipv4.ko
iptable_filter.ko   ipt_ah.ko            nf_defrag_ipv4.ko     nf_nat_pptp.ko        nf_tproxy_ipv4.ko
iptable_mangle.ko   ipt_CLUSTERIP.ko     nf_dup_ipv4.ko        nf_nat_snmp_basic.ko  nft_reject_ipv4.ko
iptable_nat.ko      ipt_ECN.ko           nf_flow_table_ipv4.ko nf_reject_ipv4.ko
```

24)
```
┌──(root💀gulzi)-[/home/gulzi]
└─# netstat -n --tcp | grep SYN_RECV
```

II) Сөйлемді толықтырыңыз:

1) ... – үнсіз келісім бойынша Iptables кестесі.
2) **sudo iptables -F** - команда қызметі қандай?
3) Команда нәтижесі қандай: **sudo /sbin/iptables-save**
4) Байланысқа рұқсат беру (Iptables) командасы
5) Байланысқа мән бермеу (Iptables) командасы
6) Байланысты бұғаттау (Iptables) командасы
7) IP адресті анықтау командасын көрсетіңіз
8) Сервердегі ашық қосылымдардың тізімін көрсететін ... командасы Syn шабуылы туралы анықтау үшін қызмет етеді.