Практикалық сабақ №11:OSI моделінің желілік деңгейінің қауіпсіздігі

Желілік деңгейдегі басқару элементтері көбінесе байланысты қорғау үшін қолданылады, әсіресе Интернет сияқты жалпы желілерде, өйткені олар көптеген қосымшаларды бір уақытта өзгертпестен қорғауды қамтамасыз ете алады.

Алдыңғы тарауларда біз желінің қауіпсіздігін қамтамасыз ету үшін құпиялылық, бастапқы аутентификация, хабарламаның тұтастығы және авторлықтан бас тарту сияқты негізгі қауіпсіздік принциптерін қамтамасыз ететін көптеген нақты уақыттағы қауіпсіздік хаттамалары жасалғанын талқыладық.

Бұл хаттамалардың көпшілігі стандартты интернет-протоколдағы ішкі қауіпсіздіктің орнын толтыру үшін OSI протокол стекінің жоғары деңгейіне назар аударды. Олардың құндылығына қарамастан, бұл әдістерді кез-келген қосымшамен оңай жалпылауға болмайды. Мысалы, SSL HTTP немесе FTP сияқты қосымшаларды қорғау үшін арнайы жасалған. Бірақ қауіпсіз байланысты қажет ететін бірнеше басқа қосымшалар бар.

Бұл қажеттілік жоғары деңгейдегі барлық протоколдар оны өз пайдасына пайдалана алатындай етіп IP деңгейіндегі қауіпсіздік шешімін жасауға әкелді. 1992 жылы Интернет-инженерлік жұмыс тобы (IETF) "IPsec"стандартын анықтай бастады.

Осы тарауда біз IPSec протоколдарының осы танымал жиынтығын қолдана отырып, желілік деңгейде қауіпсіздікке қалай қол жеткізуге болатындығын талқылаймыз.

Желілік деңгейдегі қауіпсіздік

Желінің қауіпсіздігін қамтамасыз ету үшін жасалған кез-келген схема төмендегі диаграммада көрсетілгендей протокол стегінің белгілі бір деңгейінде орындалуы керек —

Қабат	**Байланыс хаттамалары**	**Қауіпсіздікхаттамалары**
Қолданбалы деңгей	HTTP FTP SMTP	PGP. S / MIME, HTTPS
Транспорттық деңгей	TCP / UDP	SSL, TLS, SSH
Желілік деңгей	IP	IPsec

Желілік деңгейдеқауіпсіздіктіқамтамасыз етуге арналған танымалплатформа-Internet Protocol Security (IPsec).

IPsec ерекшеліктері:

* IPsec TCP-мен тек транспорттық протокол ретінде жұмыс істеуге арналмаған. Ол UDP-мен, сондай-ақ ICMP, OSPF және т. б. сияқты IP-ден жоғары кез-келген хаттамамен жұмыс істейді.

* IPsec IP деңгейінде ұсынылған барлық пакетті, соның ішінде жоғары деңгейлі тақырыптарды қорғайды.

* Порт нөмірі бар жасырын жоғарғы деңгейлі тақырыптар болғандықтан, трафикті талдау қиынырақ.

* IPsec бір желілік объектіден басқа желілік объектіге жұмыс істейді. Сондықтан қауіпсіздікті жеке пайдаланушы компьютерлері / қосымшалары үшін өзгертулерді қажет етпестен қабылдауға болады.

* Желілік нысандар арасындағы қауіпсіз байланысты қамтамасыз ету үшін кеңінен қолданылатын IPsec хосттың қауіпсіздігін де қамтамасыз ете алады.

* IPsec — тің ең көп қолданылуы виртуалды жеке желіні (VPN) екі орын (шлюз-шлюз) арасында немесе қашықтағы пайдаланушы мен кәсіпорын желісі (хост-шлюз) арасында қамтамасыз ету болып табылады.

Қауіпсіздік функциялары

IPsec ұсынатын маңызды қауіпсіздік функциялары:

- Конфиденциалдылық
    - Байланыс түйіндеріне хабарламалардышифрлауға мүмкіндік береді.
    - Үшіншіжақтыңтыңдапалуыныңалдын алады.
- Бастапқы аутентификация және деректердің тұтастығы.
    - Қабылданған пакеттің іс жүзінде пакеттің тақырыбындағықайнаркөзі ретінде анықталғантарапбергенінекепілдік береді.

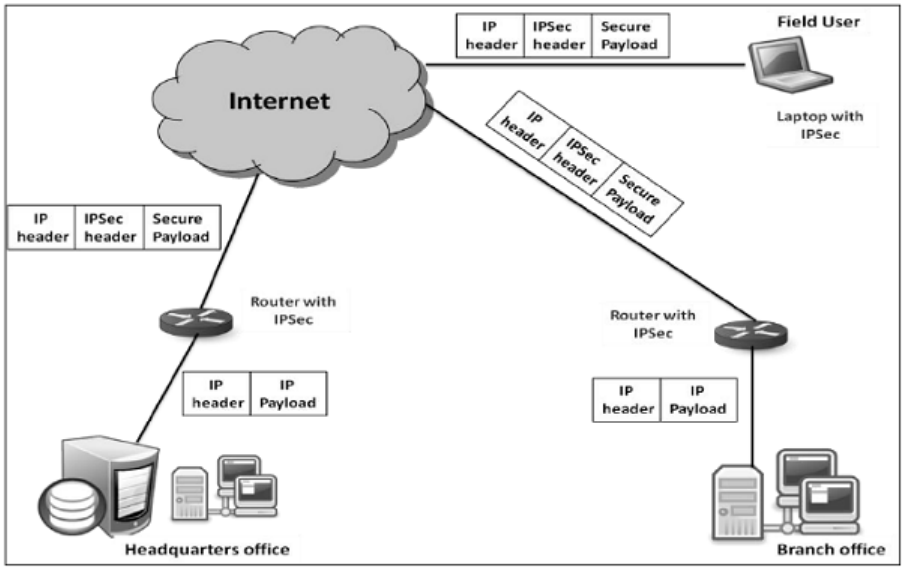
- Пакеттің өзгертілмегенін немесе басқашаболмағанынрастайды.

- Кілттікменеджмент.
  - Кілттердіңқауіпсізалмасуына мүмкіндік береді.
  - Қауіпсіздікшабуылдарыныңбелгілібіртүрлеріненқорғау.

Виртуалдыжекежелі

Ең дұрысы, кез-келген мекемеқауіпсіздіктіқамтамасыз ету үшін өзінің жеке байланыс желісіне ие болғысы келеді. Алайда, аумақтықбөлінгенаумақта осындай жеке желіні құру және қолдау өте қымбат болуы мүмкін. Бұл байланыс арналарының, маршрутизаторлардың, DNS және т. б. күрделі инфрақұрылымынбасқаруды қажет етеді.

IPsec мұндай мекемелер үшін виртуалды жеке желіні (VPN) іскеасырудың қарапайым механизмінұсынады. VPN технологиясы жалпыға қол жетімді интернет арқылы мекеменіңмекемеаралықтрафигінжіберуге, жалпыға қол жетімді Интернетке кірералдында трафикті шифрлауға және оны басқа Трафиктенлогикалық түрде бөлуге мүмкіндік береді. Жеңілдетілген VPN жұмысы келесі диаграммада көрсетілген —



IPsec-ке шолу

IPsec-бұл IP деңгейіндегі қауіпсіздікті қамтамасыз ететін протокол құрылымы / жиынтығы.

1990 жылдардың басында интернетті бірнеше институттар, негізінен академиялық мақсаттар үшін пайдаланды. Бірақ келесі онжылдықтарда Интернеттің өсуі желінің кеңеюіне және оны байланыс және басқа мақсаттар үшін пайдаланатын бірнеше ұйымдарға байланысты экспоненциалды болды.

Интернеттің жаппай өсуіне байланысты, TCP / IP протоколының ішкі қауіпсіздік әлсіздіктерімен қатар, Интернеттегі желінің қауіпсіздігін қамтамасыз ететін технологияға қажеттілік туындады. 1994 жылы интернет-сәулет кеңесі (IAB) "интернет-архитектурадағы қауіпсіздік"атты баяндама шығарды. Онда қауіпсіздік тетіктерінің негізгі бағыттары анықталды.

IAB аутентификацияны және шифрлауды IPv6, келесі буын IP-де негізгі қауіпсіздік функциялары ретінде енгізді. Бақытымызға орай, бұл қауіпсіздік мүмкіндіктері қазіргі IPv4 және футуристік IPv6-мен бірге жүзеге асырылуы үшін анықталды.

IPsec ішіндегі операциялар

IPsec пакетінде қауіпсіздік қызметтерінің толық жиынтығын қамтамасыз ететін екі бөлек операция бар деп болжауға болады. Бұл екі операция-IPsecCommunication және InternetKeyExchange.

- IPsec байланыс
    - Бұләдетте IPsec стандарттыфункциясыменбайланысты. Оғанинкапсуляция, шифрлаужәне IP-датаграммалардыхэштеужәнебарлықпакеттікпроцестердіөңдеукіреді.
    - Олбайланысушытараптарарасындаорнатылғанқолжетімдіқауіпсіздік қауымдастықтарына (SA) сәйкесбайланыстыбасқаруғажауапбереді.
    - Олаутентификациятақырыбы (AH) жәнеинкапсулаланған SP (ESP) сияқтықауіпсіздікпротоколдарынқолданады.
    - IPsec байланысыкілттердіқұруғанемесебасқаруғақатыспайды.

- IPsec байланысоперациясыныңөзіәдетте IPsec депаталады.

- Интернеттекілттерменалмасу (IKE)

  - IKE-бұл IPsec үшін қолданылатынавтоматты кілттерді басқару протоколы.
  - Техникалықтұрғыдан, кілттерді басқаруIPsecбайланысы үшін маңызды емес және кілттерді қолменбасқаруға болады. Алайда, кілттерді қолменбасқару үлкен желілер үшін қажет емес.
  - IKE IPsecкілттерін құруға және кілттерді орнату кезінде аутентификациянықамтамасыз етуге жауап береді. IPsec-ті кез-келген басқа кілттерді басқару протоколдары үшін пайдалануға болады, бірақ IKE әдепкібойынша қолданылады.
  - IKE InternetManagementAssociationKeyManagementProtocol (ISAKMP) белгілі бір кілт басқаруқұрылымыменқолданылатын екі протоколды (Oakley және SKEME) анықтайды.
  - ISAKMP IPsec-кетән емес, бірақ кез-келген протокол үшін SA құруға негіз береді.

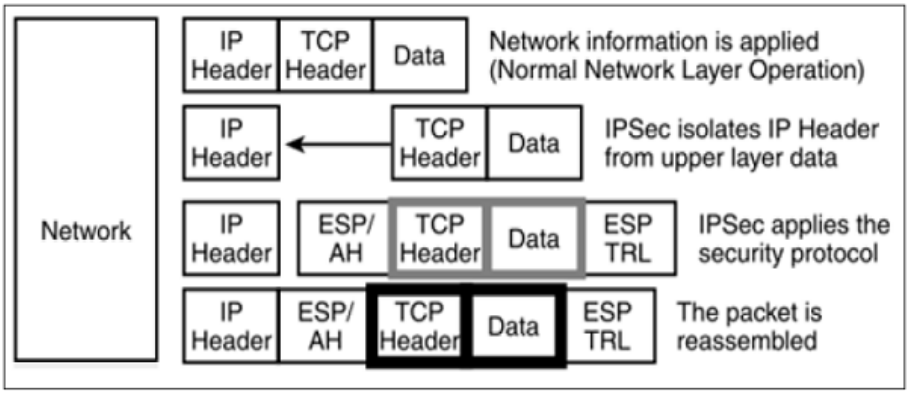
Бұл тарауданегізіненқауіпсіздікке қол жеткізу үшін пайдаланылатынIPsecбайланысы мен байланысты хаттаматалқыланады.

IPsec байланыс режимдері

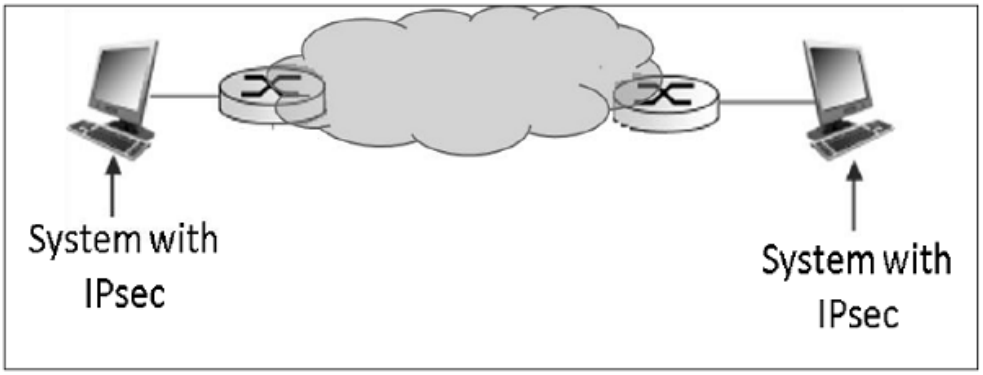
IPsecCommunication екі жұмыс режиміне ие; Транспорттық және туннельдітранспорттүрлері. Бұл режимдерді қажетті байланыс түріне байланысты комбинацияда немесе жеке пайдалануға болады.

Транспорттық режим

- IPsec жоғарғы деңгейденалынғанпакеттіинкапсулирлемейді.
- Бастапқы IP тақырыбысақталады және деректер жоғарғы деңгейпротоколындаорнатылған бастапқы атрибуттарнегізіндежіберіледі.
- Келесі диаграммада Протокол стекіндегі деректер ағыны көрсетілген.

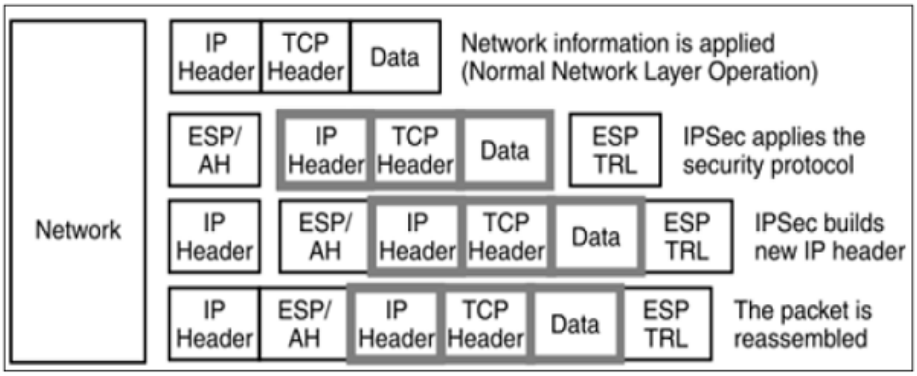


- Транспорттықрежимніңшектеулілігі - шлюзқызметтерінұсынумүмкінемес. Ол келесі суретте көрсетілгендей байланыс үшін сақталған.

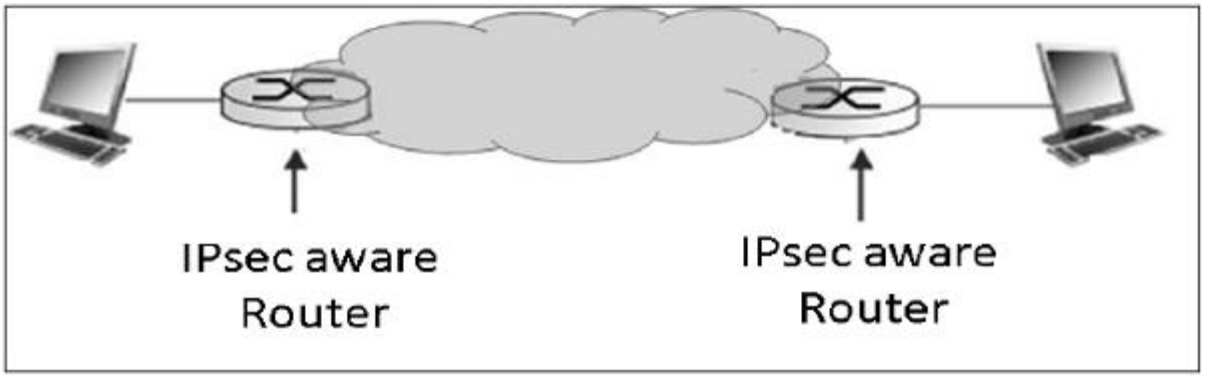


Туннельді режим

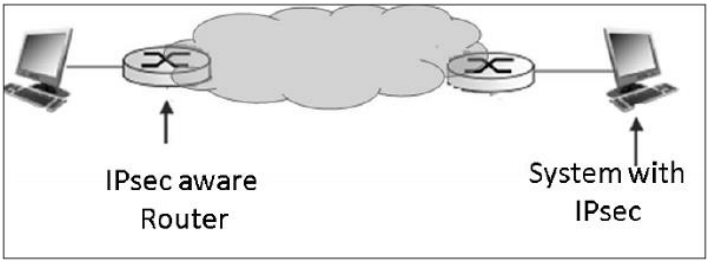
- Бұл IPsec режимі басқа қауіпсіздікқызметтеріменбіргеинкапсуляцияқызметтерінұсынады.
- Туннельрежимінде жұмыс істеген кезде жоғарғы деңгейдегі барлық пакетқауіпсіздікхаттамасынқолданаралдындаинкапсуляцияланады. Жаңа IP тақырыбықосылды.
- Келесі диаграммада Протокол стекіндегі деректер ағыны көрсетілген.



- Туннельрежимі әдетте шлюзәрекеттерімен байланысты. Инкапсуляция бірнеше сеанстарды бір шлюз арқылы жіберуге мүмкіндік береді.
- Туннельрежиміндегіәдеттегі байланыс келесі диаграммада көрсетілген.



- Соңғы нүктелерге келетін болсақ, олар тікелейтранспорттықдеңгейінеқосылады. Шлюзге жіберілген бір жүйенің датаграммасыинкапсуляцияланады, содан кейін қашықтағышлюзгежіберіледі. Қашықтағыбайланыстырылғаншлюз деректерді жояды және оныішкіжелідегі соңғы нүктегебағыттайды.
- IPsec көмегімен шлюзменбөлекторминалжүйесі арасында туннельрежимінорнатуға болады.



IPseспротоколдары

IPsec
қалағанқауіпсіздікқызметтерінұсынуүшінқауіпсіздікпротоколдарынқолданады. Бұлпротоколдар IPsec операцияларыныңнегізіболыптабылады, алқалғандары IPsec-теосыпротоколдардықолдауғаарналған.

Байланысобъектілеріарасындағықауіпсіздікқауымдастықтарыпайдаланылатынқ ауіпсіздікхаттамасыменорнатыладыжәнесақталады.

IPsec екіқауіпсіздікпротоколынанықтайды-аутентификациятақырыбы (AH) жәнеинкапсулаланғанжүктеме (ESP).

AH протоколыдеректердіңтұтастығыжәнекөздіңаутентификациясықызметінұсынады. Қосымшатұрақтылықтықамтамасызетеді. Алайда, бұлқұпиялылықтыңешқандайтүрінқамтамасызетпейді.

Аутентификациятақырыбы

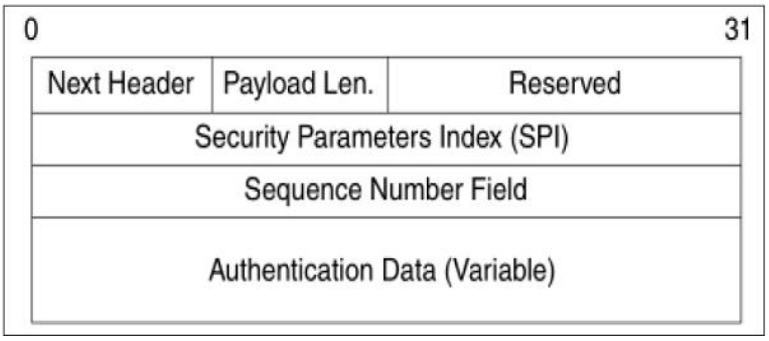
AH-бұлтақырыпқосуарқылыдейтаграммазмұнының барлығыннемесебірбөлігінаутентификациялаудықамтамасызететінхаттама.
Тақырыпдатаграммадағымәндернегізіндеесептеледі.
Есептеуүшіндатаграмманыңқандайбөліктеріқолданыладыжәнетақырыптықайжергеқоюөзараәрекеттесурежимінебайланысты (туннельнемесетранспорт).

AH протоколының жұмысытаңқаларлыққарапайым. Онытақылаусомасынесептеунемесеқателердіанықтауүшін CRC тексерулерінорындауүшінқолданылатыналгоритмдергеұқсасдепсанауғаболады.

AH тұжырымдамасыбірдей, қарапайымалгоритмніңорнына AH текөзараәрекеттесетінтараптарғабелгіліарнайыхэшалгоритміменқұпиякілттіқолданады.
Осымүмкіндіктердіанықтайтынекіқұрылғыарасындақауіпсіздікқауымдастығықұрылды.

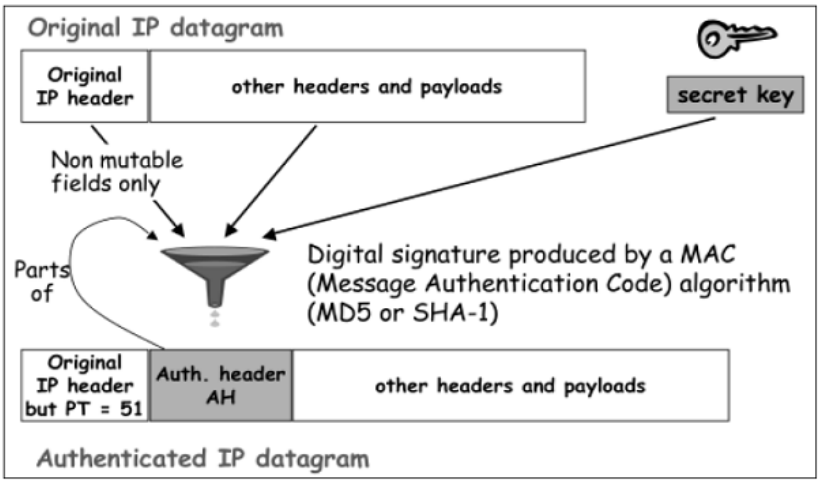
AH процесікелесікезеңдерденөтеді.

- ✓ IP пакетіпротоколдардыңжоғарғыстекіненалынғанкезде, IPsec пакеттегіқолжетімдіақпараттанқауіпсіздікқауымдастығын (SA) анықтайды; мысалы, IP мекенжайы (көзіжәнетағайындалғанорны).
- ✓ SA-дан қауіпсіздік протоколы AH екендігіанықталғаннанкейін AH тақырыбының параметрлері есептеледі. AH тақырыбы келесі параметрлерден тұрады:

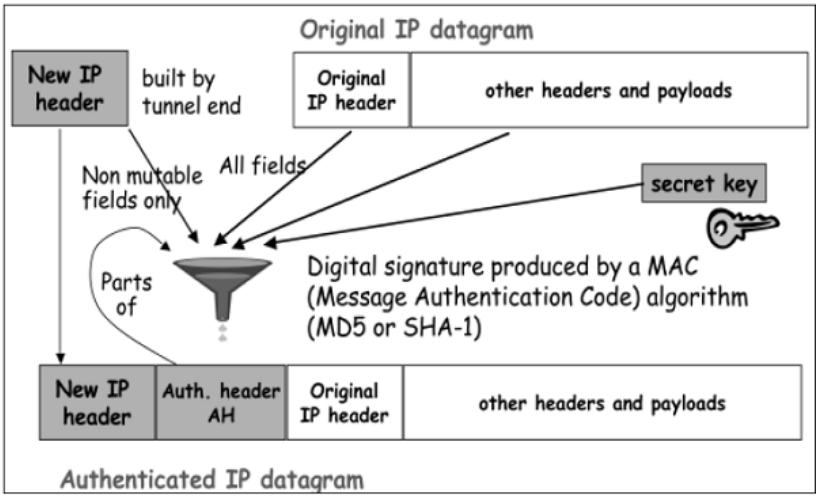


- ✓ Тақырып өрісі AH тақырыбынан кейінгі пакеттің хаттамасынкөрсетеді. Реттілікпараметрініңиндексі (SPI) байланысушытараптарарасындағы SA-даналынады.
- ✓ Реттікнөмір есептеледі және енгізіледі. Бұл сандар AH -ге шабуылға қарсы тұруғақосымша мүмкіндік береді.

- ✓ Аутентификация деректері байланыс режиміне байланысты әртүрлі есептеледі.
- ✓ Транспорттықрежимінде аутентификация деректерін есептеу және беру үшін соңғы IPпакетін құрастыру келесі диаграммада көрсетілген. Бастапқы IPтақырыбындаөзгеріс тек 51-ден көрсетілген AHқосымшасынадейінхаттаманөмірінеенгізіледі.



- ✓ Туннельрежимінде жоғарыда сипатталғанпроцесс келесі диаграммадакөрсетілгендейжүреді.



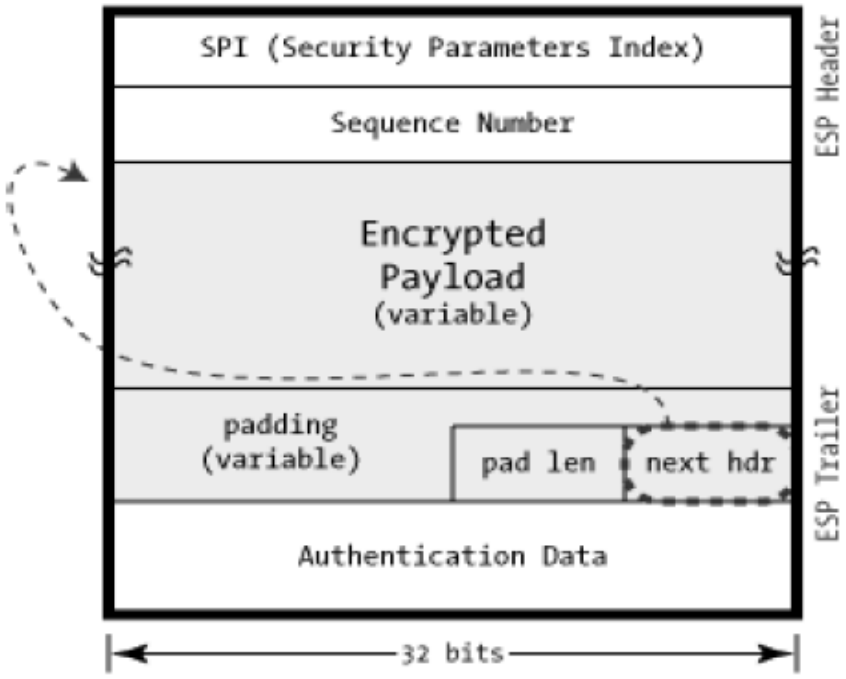
Инкапсуляцияқауіпсіздігіхаттамасы (ESP)

ESP құпиялылық, тұтастық, түпнұсқалықрастамажәнеқосымшаойнатукедергісісияқтықауіпсіздікқызметтері нұсынады. Көрсетілетінқызметтержиынтығықауіпсіздікқауымдастығын (SA) құрукезіндетаңдалғанпараметрлергебайланысты.

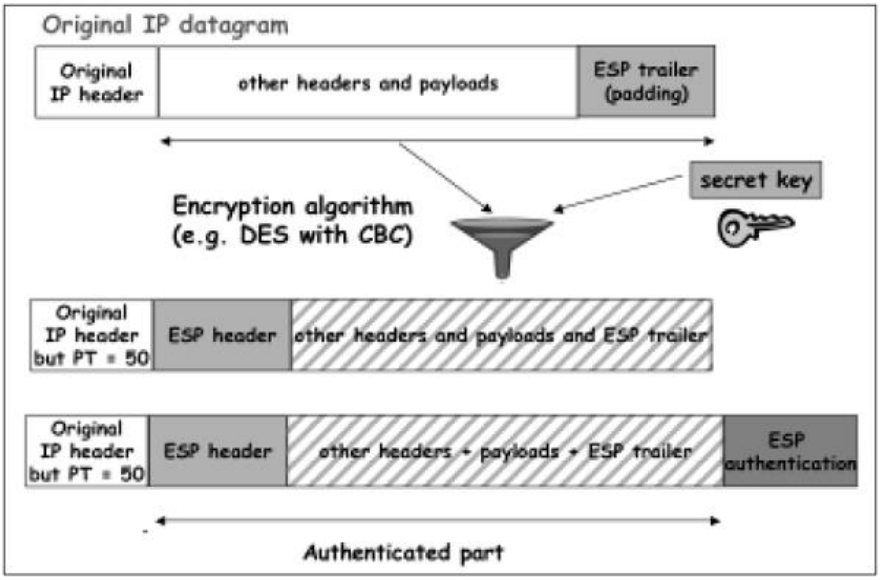
ESP-деаутентификатордышифрлаужәнеқұруүшінқолданылатыналгоритмдер SA құруүшінқолданылатынатрибуттарменанықталады.

ESP процесікелесідей. Алғашқыекіқадамжоғарыдакөрсетілгендей AH процесінеұқсас.

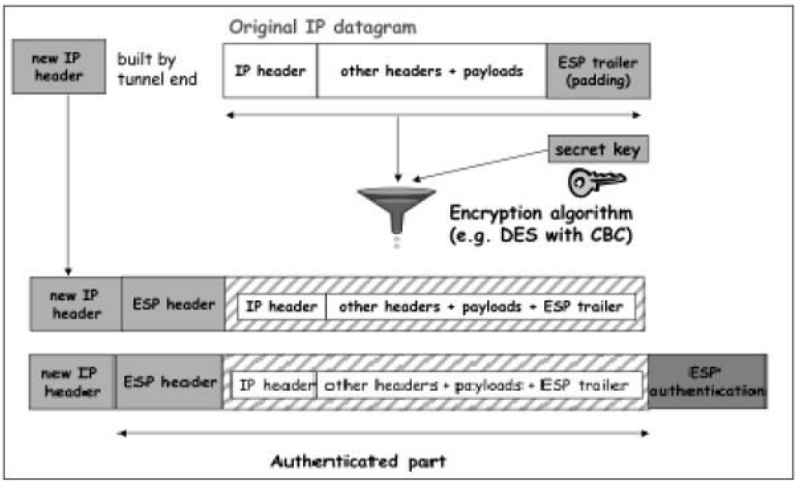
- ESP қатысқандығыанықталғаннанкейін ESP пакетініңөрістеріесептеледі. ESP өрістерініңорналасуы келесі диаграммада көрсетілген.



- Көлікрежиміндегі шифрлау және аутентификацияпроцесі келесі диаграммада көрсетілген.



- Туннель режиміжағдайында шифрлау және аутентификация процесі келесі диаграммадасипатталған.



Аутентификация және құпиялылық ESP ұсынатын негізгі қызметтерболғанымен, екеуіде міндетті емес. Техникалықтұрғыдан біз аутентификациясыз null шифрлауды қолдана аламыз. Алайда, іс жүзінде ESP тиімді пайдалану үшін екеуініңбіреуіорындалуы керек.

Негізгі тұжырымдама-аутентификация және шифрлау қажет болған кезде ESP қолдану және шифрлаусызкеңейтілгенаутентификация қажет болған кезде AH пайдалану.

IPsec қауіпсіздікқауымдастықтары

Қауіпсіздікқауымдастығы (SA) IPsec байланысыныңнегізі болып табылады. SA ерекшеліктері —

- Деректерді жібермесбұрын, жіберуші объектпенқабылдаушыобъект арасында "қауіпсіздікқауымдастығы (SA)"деп аталатынвиртуалды байланыс орнатылады.
- IPsec желілік шифрлау менаутентификацияныорындау үшін көптеген мүмкіндіктерұсынады. Әрбір IPsec қосылымышифрлауды, тұтастықты, түпнұсқалықты немесе барлық үшқызметтіқамтамасызете алады. Қауіпсіздік қызметі анықталған кезде, екі тең IPSecнысаны қандай алгоритмдердіқолданукеректігіндәланықтауы керек (мысалы, шифрлау үшін DES немесе 3DES; тұтастық үшін MD5 немесе SHA-1). Алгоритмдердітаңдағаннан кейін екі құрылғыдасеанскілттерінбөлісуі керек.
- SA-жоғарыда аталған байланыс параметрлерініңжиынтығы, ол IPsec сеансын құру үшін екі немесе одан да көп жүйелер арасындағы байланысты қамтамасыз етеді.
- SA қарапайым сипатқа ие, сондықтан екі бағытты байланыс үшін екі SA қажет.
- SA қауіпсіздікпротоколыныңтақырыбындабарқауіпсіздікпараметрініңиндекс нөмірі (SPI) бойыншаанықталады.
- Жіберу және қабылдаунысандары SA күйі туралы ақпаратты сақтайды. Бұл жағдай туралы ақпаратты қолдайтын TCP соңғы нүктелерінеұқсас. IPsec TCP сияқты қосылуға бағытталған.

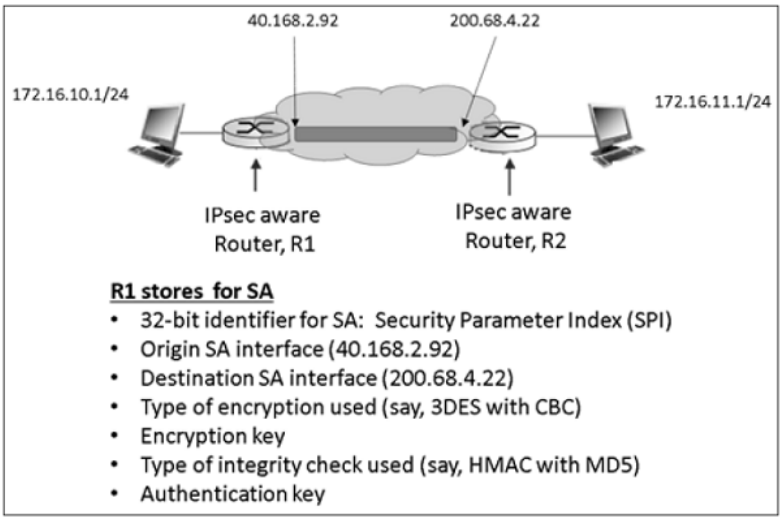
SA параметрлері

Кез-келген SA келесі үш параметрмен бірегей түрде анықталады:

- Қауісіздік параметрлерінің индексы (SPI).
    - Бұл SA тағайындаған 32 биттікмән. Ол бір бағыттааяқталатын және бірдей IPsec протоколынқолданатын әртүрлі SA-ныажырату үшін қолданылады.
    - ӘрIPSecпакетінде SPI өрісі бар тақырып бар. SPI кірісбумасы SA-менсалыстыру үшін берілген.
    - SPI-алушы үшін SA анықтау үшін жіберуші жасағанкездейсоқсан.
- Тағайындалған IP мекенжайы - Бұл соңғы маршрутизатордың IP мекенжайы болуы мүмкін.

- Қауіпсіздікпротоколыныңидентификаторы-қауымдастық AH немесе ESP SA екенінкөрсетеді.

IPsec алмасуынақатысатын екі маршрутизаторарасындағы SA мысалы келесі диаграммада көрсетілген.



Әкімшілік деректер базасыныңқауіпсіздігі

IPsec-те IPsecдатаграммасынөңдеудібасқаратын екі дерекқор бар. Біреуі - қауіпсіздікқауымдастығының мәліметтер базасы(SAD), ал екіншісі — қауіпсіздіксаясатыныңдерекқоры (SPD). IPsecқолданатынәрбірбайланыстырушы соңғы нүктеделогикалықбөлек SAD және SPD болуы керек.

Қауіпсіздікқауымдастығының мәліметтер базасы

IPsec-ке байланысты соңғы нүктедеқауіпсіздікқауымдастығының (SAD) мәліметтер базасындағы SA күйі бар. SAD дерекқорындағыәрбір SA жазбасында келесі кестедекөрсетілгендейтоғыз параметр бар:

Sr.No.	Параметрлер және олардың сипаттамасы
1	**Реттікнөмірсанауышы** Шығысхабарламаларүшін. Бұл AH немесе ESP тақырыптарындакөрсетілген 32 биттіксериялықнөмір.

2	**Реттікнөмірдітолтырусанауышы** Белгілібір SA көмегіменоданәрібайланыстыболдырмауүшінопцияжалаушасынорнатады
3	**32 биттіканти-воспроизведениетерезесі** КірісАНпакетінемесеESPвоспроизведение екенінанықтауүшінқолданылады
4	**SAөмірсүрууақыты** SA белсендіболууақыты
5	**АХАлгоритмы** АН жәнебайланыстыкілттеқолданылады
6	**ESPAuthАлгоритмы** ESP тақырыбынаутентификациялаубөлігіндеқолданылады
7	**ESP шифрлау алгоритмы** ESP жәнебайланыстыкілттуралыақпараттышифрлаукезіндеқолданылады
8	**IPsecЖұмыс тәртібі** Транспорттынеместуннельды режим
9	**PathMTU (PMTU)** Максималдыберілісбірлігініңкез-келгентраекториясы (фрагментацияныболдырмауүшін)

SAD- тағыбарлықSAжазбаларыүш SA параметріменіндекстеледі: тағайындалған IP, қауіпсіздікпротоколыныңидентификаторыжәне SPI.

Қауіпсіздіксаясатыныңмәліметтербазасы

SPD шығыспакеттерінөңдеуүшінқолданылады. Бұлқандай SAD жазбаларынпайдаланукеректігіншешугекөмектеседі. Егер SAD жазбасыболмаса, SPD жаңаларынжасауүшінқолданылады.

Кез-келген SPD жазбасындамыналарболады —

- Белсенді SA көрсеткіші SAD-даорындалады.
- Селекторөрістері-IPsec қолданудыанықтауүшінқолданылатынжоғарғыдеңгейдегікіріспакетіндегіөріс. Селекторларғадереккөзменалушыныңмекен-жайы, қажетболғанжағдайдапортнөмірлері, қолданбаидентификаторлары, хаттамаларжәнет. б. кіруімүмкін.

Шығыс IP датаграммаларыкодтаупараметрлеріналуүшін SPD жазуданбелгілібір SA-ғаөтеді. IPsec кірісдатаграммасы SPI / DEST IP / Protocol үштігінқолданаотырып, дұрыс SA-ғатүседіжәнесолжердентиісті SAD жазбасыншығарады.

SPD сонымен қатар IPsecайналыпөтуі керек трафикті көрсете алады. SPD-ді SAпроцестерінбелсендіруге байланысты әрекеттердішешетін пакет сүзгісі ретінде қарастыруға болады.

Қорытынды

IPsec-бұл желілік қосылымдардықорғауға арналған протоколдаржиынтығы. Бұл өте күрделі механизм, өйткені белгілі бір шифрлау алгоритмі мен аутентификация функциясынанықтаудыңорнына, ол екі тарапкелісетін барлық нәрсені жүзеге асыруға мүмкіндік беретін құрылымдықамтамасыз етеді.
Аутентификация тақырыбы (AH) және қауіпсіздікинкапсуляциясыныңжүктемесі (ESP) IPsecқолданатын екі негізгі байланыс протоколы болып табылады. AH тек аутентификацияланған кезде, ESP байланыс арқылы берілетін деректерді шифрлай және аутентификациялай алады.
Тасымалдаурежимі IP тақырыбынөзгертпестен екі соңғы нүкте арасында қауіпсіз байланыс орнатуға мүмкіндік береді. Туннель режимі бүкіл IP жүктемепакетінинкапсулирлейді. Жаңа IP тақырыбынқосады. Соңғысыдәстүрлі

VPN құру үшін қолданылады, өйткені ол сенімсіз Интернет арқылы виртуалдықауіпсіз туннель ұсынады.
IPsecқосылымын орнату криптографиялық таңдаудың барлық түрлерінқамтиды. Аутентификация әдетте MD5 немесе SHA-1 сияқты криптографиялық хэшкенегізделген. Шифрлау алгоритмдері-DES, 3DES, Blowfish және AES. Басқа алгоритмдерде мүмкін.
Екі өзараәрекеттесетін соңғы нүктелерхэштеу немесе шифрлау кезінде қолданылатын құпия мәндердібілуі керек. Қол кілттері екі ұшында да құпия мәндердіқолмененгізуді қажет етеді, олар кез-келген жолақтан тыс механизммен беріледі және IKE (InternetKeyExchange) бұл үшін онлайн режимінде күрделі механизм болып табылады.

Strongswan көмегімен Linux-тағы IPSec

```
dana@dana-VirtualBox:~$ sudo apt-get install strongswan
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Будут установлены следующие дополнительные пакеты:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins
  strongswan-charon strongswan-libcharon strongswan-starter
Предлагаемые пакеты:
  libstrongswan-extra-plugins libcharon-extra-plugins
Следующие НОВЫЕ пакеты будут установлены:
  libcharon-extauth-plugins libstrongswan libstrongswan-standard-plugins
  strongswan strongswan-charon strongswan-libcharon strongswan-starter
Обновлено 0 пакетов, установлено 7 новых пакетов, для удаления отмечено
в, и 166 пакетов не обновлено.
Необходимо скачать 876 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на
B.
Хотите продолжить? [Д/н]
```

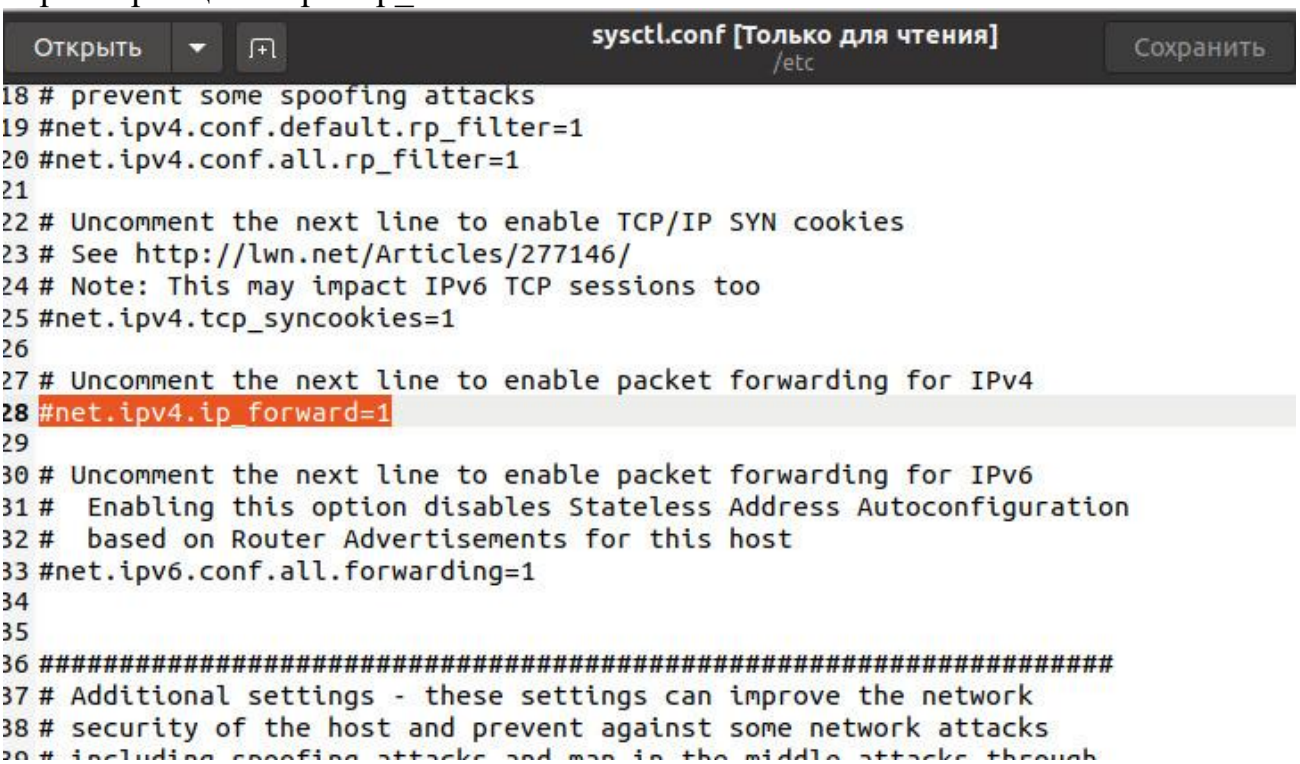
Әрі қарай, бәрі жұмыс істеуі үшін пакеттерді біздің VPN концентраторымыз арқылы бағыттауға рұқсат беру керек. Сіз мұны тексере аласыз:

```
dana@dana-VirtualBox:~$ cat /proc/sys/net/ipv4/ip_forward
0
```

Егер /proc/sys/net/ipv4/ip_forward файлында 0 болса онда маршрутизацияға тыйым салынған, бұл әдепкі әрекет. Маршруттауға рұқсат беру үшін онда 1 жазыңыз.

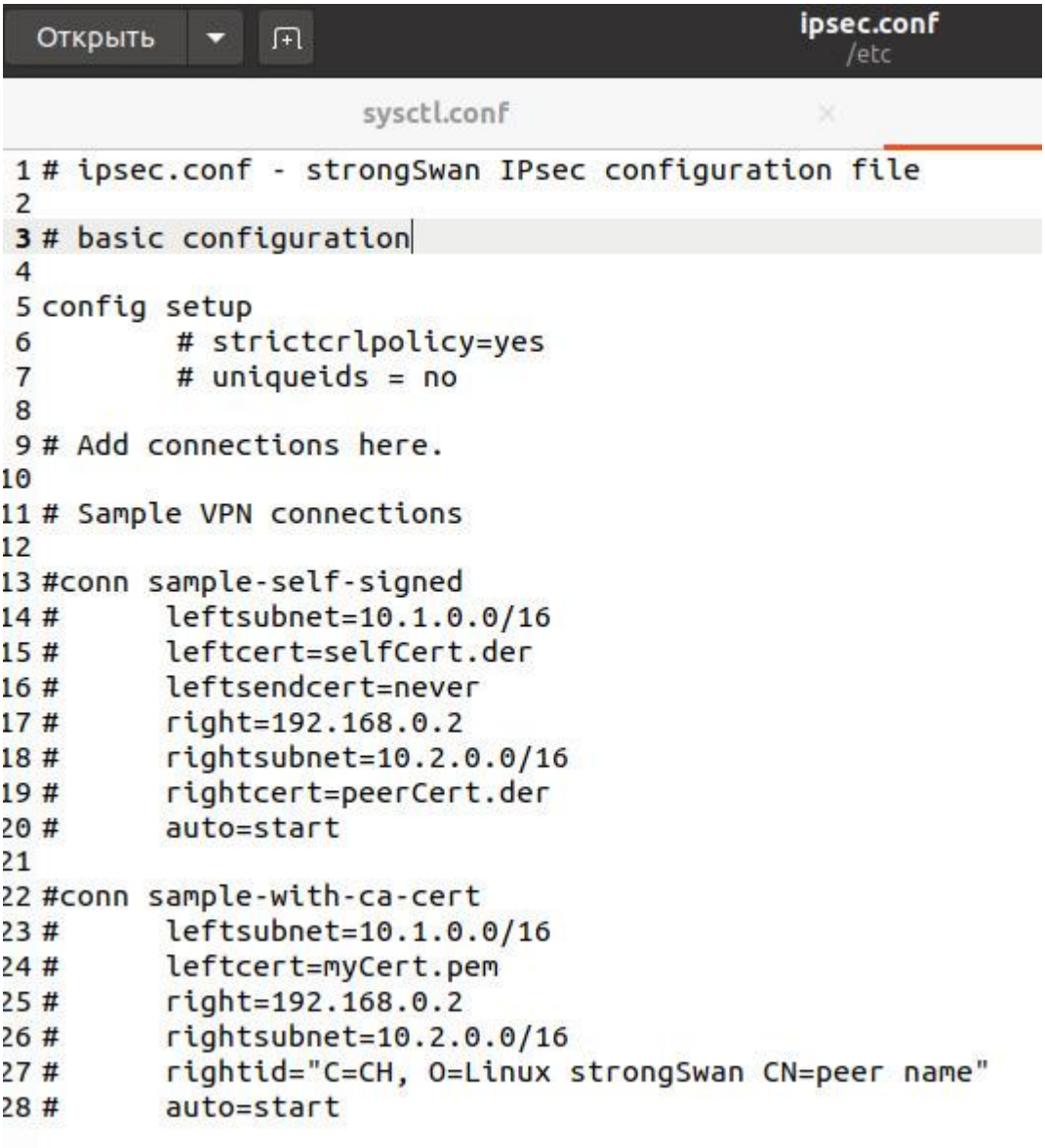
```
dana@dana-VirtualBox:~$ sudo su
[sudo] пароль для dana:
root@dana-VirtualBox:/home/dana# sudo echo 1 > /proc/sys/net/ipv4/ip_forward
root@dana-VirtualBox:/home/dana# cat /proc/sys/net/ipv4/ip_forward
1
```

Қайта жүктеуден кейін мән сақталу үшін (өйткені /proc-виртуалды файлдық жүйе), біз /etc/sysctl.conf файлына өзгерістер енгіземіз, атап айтқанда net параметрінің мәніipv4.ip_forward



Strongswan үшін негізгі конфигурация файлдары:

- /etc/ipsec.conf-барлық параметрлер
- /etc/ipsec.secrets-шифрлау кілттері мен парольдері
- /Etc/ipsec файлы.conf бөлімдерге бөлінген
- config setup-Ғаламдық параметрлер мен опциялар
- conn % default-IPSec қосылымдарының әдепкі параметрлері. Егер жеке қосылым параметрлерінде параметр көрсетілмесе, онда параметрлер осы жерден қолданылады
- conn SomeTunnel-қосылым параметрлері бар бөлім



қызметтік сөз **conn** қосылыстың атауын білдіреді. Осыдан кейін қосылысты сипаттайтын параметрлер болады.

leftжәне **right**сөздерінен кейін хост мекенжайлары жазылады. Сөздер хосттардың әр түрлі жағынан екенін білдіреді. Сіздің мекен-жайыңызды қай мекен-жайға енгізгеніңіз маңызды емес, жүйе мекен-жайлардың қайсысы оның интерфейсіне жататынын автоматты түрде анықтайды. Сондықтан әртүрлі хосттарда бірдей конфигурацияны қолдануға болады. Мекен-жайдың орнына %any кілт сөзін right=%any ретінде пайдалануға болады. Содан кейін сіз кез-келген мекен-жайдан қосыла аласыз.

leftsubnet және **rightsubnet** – трафик шифрланатын ішкі желі (суреттегі топологияға сәйкес).

type=tunnel-қосылым түрі. Tunnel, transport немесе passthrough мәндерін қабылдай алады.

authby = secret-кілт ретінде не қолданылады: PSK (пароль сөзі) немесе RSA (кілт)
auto=start-опция қосылымды қашан қосу керектігін анықтайды. Ол мәндерді қабылдай алады: start (автоматты түрде Бастау), add (басқа хосттың бастамасына жауап ретінде бастау), ignore (қосылымды елемеу), manual(қолмен бастау), route.
Айтпақшы, күрделі пароль қоюғафантазиясы жетпейтіндерге, парольдерді құрудың дұрыс (бірақ жалғыз емес) әдісі бар(генерировать пароль). Қажетті күрделіліктің 48 кездейсоқ таңбасын төмендегі команда бойынша шығарады. Мұндай парольмен сіз тыныш ұйықтай аласыз.

```
root@dana-VirtualBox:/home/dana# apt install rand
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Следующие НОВЫЕ пакеты будут установлены:
  rand
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления
в, и 170 пакетов не обновлено.
Необходимо скачать 7 548 B архивов.
После данной операции объём занятого дискового пространства воз
.
Пол:1 http://kz.archive.ubuntu.com/ubuntu focal/universe amd64
0ubuntu2 [7 548 B]
Получено 7 548 B за 1c (12,4 kB/s)
Выбор ранее не выбранного пакета rand.
(Чтение базы данных … на данный момент установлен 189181 файл и
Подготовка к распаковке …/rand 1.0.4-0ubuntu2 amd64.deb …
```

```
root@dana-VirtualBox:/home/dana# openssl rand -base64 48
OyoxObYqJJsrZ18pnqQHarq525S1Pp00UEXwQz9lIt8Y6Mj6qEuMvDuD3vqmxhMP
```

Хосттардың әрқайсысында осы екі файлды өңдегеннен кейін strongswan қайта іске қосыңыз.

```
root@dana-VirtualBox:/home/dana# ipsec start
Starting strongSwan 5.8.2 IPsec [starter]...
charon is already running (/var/run/charon.pid exists) -- skipping daemon start
```

Конфигурацияны жаңарту үшін

```
root@dana-VirtualBox:/home/dana# ipsec update
Updating strongSwan IPsec configuration...
```

ipsec status пәрменімен байланыс күйін тексеріңіз

```
dana@dana-VirtualBox:~$ sudo ipsec status
Security Associations (0 up, 0 connecting):
  none
```

Ал толығырақ ақпарат алғыңыз келсе төмендегі команданы пайдаланыңыз.