# 3.5 Безбедност

- Секоја мрежа е потенцијална цел на напад од страна на злонамерни, или љубопитни „хакери“
- Кој се’ може да ја нападне мрежата и зошто?
  - Вработените во претпријатието
  - Традиционални „хакери“
  - Конкуренти или незадоволни клиенти
  - Криминалци
  - Индиректен напад – компјутерски вирус преку e-mail порака
- Кои компоненти можат да бидат цел на напади?
  - Мрежни елементи – router, switch, access point …
  - Оперативни системи – Unix, Windows
  - Web, E-mail, SQL и др. сервери, како и апликации кои се инсталирани на нив

# 3.5.1 Безбедносни решенија

- На кое ниво од OSI моделот треба да бидат имплементирани безбедносните техники?
  - Апликациски слој
    - Тајност (confidentiality) – криптирање на податоците
    - Интегритет (integrity) – електронски потписи на пораките
    - Идентификација (authentication) – корисничко име и шифра
    - Расположливост (availability) – апликацијата е ставена на располагање од повеќе сервери на различни сајтови
    - Инспекција, следење (audit) – записи за корисниците кои се поврзуваат на даден host и за нивните активности

# 3.5.1 Безбедносни решенија

- Мрежен слој
  - Виртуелни приватни мрежи (VPN)
  - Перманентни виртуелни кола (PVC)
  - Затворени кориснички групи (Closed User Groups)
  - Идентификација на повикувачот
  - Firewall
    - Во наједноставна форма, станува збор за рутер кој е конфигуриран со **листа за пристап (access list)** која овозможува низ него да поминува само сообраќајот од претходно дефинирани локации
    - Во пософистицирана форма (во повисоките слоеви од OSI моделот) firewall-от може да обезбеди повеќе функции:
      - Криптирање
      - Менаџмент на сесии со верификација на кориснички шифри
      - Преведување на адреси (NAT)
      - Proxy агент

# 3.5.1 Безбедносни решенија

- Слој на податочна врска
  - PPP протоколот вклучува и безбедносни механизми кои се користат при dial-up поврзување
    - Во рамки на процесот на воспоставување на врска, повикувачката страна испраќа шифра која, потоа, се проверува на приемната страна
      - CHAP (Challenge Handshake Authentication Protocol)
      - PAP (Password Authentication Protocol)

# 3.5.2 Безбедносни технологии

- Криптирање (Encryption)
- Инфраструктура на јавни клучеви (Public Key Infrastructure)
- Firewall

# 3.5.2.1 Криптирање

- Основна улога на криптирањето – да обезбеди приватност на податоците кога поминуваат преку јавни мрежи
  - Идеален случај – податоците треба да се криптираат уште во end-системите
  - Компромисно решение – податоците се криптираат кога поминуваат низ рутери за таа намена или низ друг независен хардвер за криптирање (пр. Firewall)
    - Повеќето независни системи за криптирање се дизајнирани за работа на point-to-point синхрони податочни врски
    - Се' поголем е бројот на системи за пакетно-ориентирани мрежи
      - 'Payload' encryptors – ги криптираат само корисничките податоци, оставајќи ги заглавијата неизменети, така што пакетите можат непречено да бидат упатувани низ мрежата

# 3.5.2.1 Криптирање

- Типови на криптирање
  - **Симетрично** криптирање – безбедноста на криптирањето зависи од некоја заедничка тајна (shared secret) која ја знаат само двете страни инволвирани во комуникацијата
    - Бидејќи истиот клуч се користи и за криптирање и за декриптирање, ваквите системи оперираат над блокови од податоци, применувајќи бит-пермутации и други логички операции кои зависат од клучната вредност – благодаредние на големата брзина, можат да бидат и чисто хардверски имплементирани
  - **Асиметрично** криптирање – корисникот поседува пар од клучеви – еден приватен (private) и еден јавен (public)
    - Порака која е криптирана со јавниот клуч, може да биде декриптирана само со приватниот (и обратно)
    - На овој начин, можат да се примаат пораки од секој што го знае јавниот клуч (таквите пораки ќе се декриптираат со приватниот клуч), а можат и да се испраќаат криптирани пораки на секого чиј јавен клуч е познат

# 3.5.2.1 Криптирање

- **IPsec** (IP Security) – стандард чија цел е да обезбеди безбедно, криптирано тунелирање преку Интернет и/или безбедно комуницирање во LAN
- Основна задача на IPSec е да обезбеди:
  - Заштита на податоците во IP пакетите
  - Заштита од мрежни напади преку филтрирање на пакетите и обезбедување на доверлива комуникација.

Целите се постигнуваат преку користење на безбедносни сервиси базирани на криптографија, безбедносни протоколи, и динамичко менаџирање на клучеви.

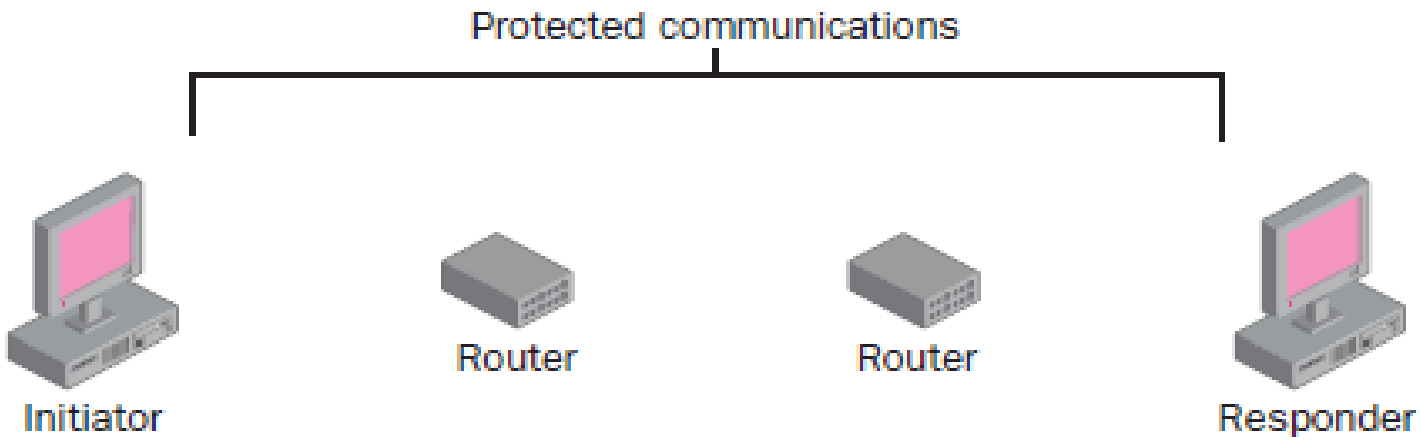
# IPSec

IPSec успешно се имплементира во следниве сценарија:

- **Local area network (LAN)** Client/server и peer-to-peer LANs
- **Wide area network (WAN)** Router-to-router и gateway-to-gateway WANs
- **Далечински пристап**(**Remote access)** Internet пристап до приватни мрежи

# IPSec mode(метод) на работа

- **Транспортен** (**Transport mode) –** се користи кога е потребна безбедност помеѓу крајните системи кои **не** смеат да комуницираат преку NAT.



# IPSec mode

**Тунелирање (Tunnel mode) –** се користи за site-to-site комуникација која се одвива преку Интернет (или други јавни мрежи).