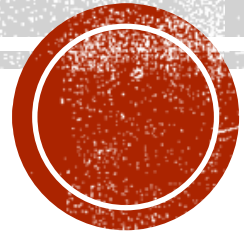
МРЕЖОВА СИГУРНОСТ

доц. д-р. Генчо Стоицов



ФОРМА НА ИЗПИТВАНЕ

проект = 3 задачи + отговори на зададените по теми въпроси (публикувани са в класната стая)

КАКВО ОЗНАЧАВА СИГУРНОСТ?

- Сигурността на системно ниво означава системата да не може да бъде пробита до такова ниво, че да се разпадне.
- Сигурността на ниво данни означава данните да не могат да бъдат подменяни.

СЪВРЕМЕННИТЕ СИСТЕМИ И МРЕЖИ

- поради сложността си са предразположени към пробиви и грешки
- съхраняват поверителна информация, която трябва да се предпази от злоупотреби
- трябва да имат добре планирана и реализирана сигурност, запазваща репутацията им

КАКВО Е ПРОБИВ В СИГУРНОСТТА НА МРЕЖАТА?

Пробивът в сигурността може да се дефинира като **нелегален достъп до информация**, който може да причини разкриване, заличаване или смяна на информацията.

Обикновено това означава:

- използване или достъп до информация или системи за незаконни цели
- или за цели, за които информацията или системите не трябва да се използват.

НЯКОИ ЧЕСТО СРЕЩАНИ ТИПОВЕ ПРОБИВИ

- Достъп до информация на абонати за изпращане на спам съобщения
- Неупълномощен достъп до поверителна информация с цел създаване на подправена самоличност
- Подслушване
- Придобиване на неупълномощен достъп до мрежа с цел достъп до фирмена информация
- Вирусни атаки
- DNS превземане

НЯКОИ ЧЕСТО СРЕЩАНИ ТИПОВЕ ПРОБИВИ

- DoS (denial of service) атаки
- DDoS атаки
- Пробив във физическите граници на организация

КОМПОНЕНТИ, КОИТО ТРЯБВА ДА БЪДАТ ЗАЩИТЕНИ

- клиент - устройството от страната на клиента е уязвимо към вирусни атаки от хакери, кракери и злонамерен код
- сървър - данните на сървърите са уязвими за неупълномощен достъп. Възможни са нарушения в сървъра, които да доведат до намаление на скоростта му на работа и в най-лошите случаи — до спирането му. Освен това ресурсите на сървъра могат да се използват с различна цел от тази, за която са предназначени
- мрежа

ОСНОВНИ НАПРАВЛЕНИЯ, ЦЕЛ НА МРЕЖОВАТА СИГУРНОСТ

- Поверителност (конфиденциалност) - степента, до която трябва да бъде поддържана поверителността, зависи от типа информация, която трябва да се защити
- Цялостност – гарантира, че данните не са променяни от неупълномощени потребители
- Достъпност - данните или информацията да бъдат налични за използване при необходимост + достъпност на системите и останалите ресурси, необходими за достъп до информацията - отказ на услуги (DoS)
- проверка за автентичност (автентикация) - да се проверява автентичността на потребителите

УРАВНЕНИЕ НА СИГУРНОСТТА

Трябва да осъществява баланс между разходите и печалбата. Да включва:

- реалната стойност на информацията – действителната стойност на информацията, която организацията иска да защити
- възприетата стойност на информацията - печалбата, която потребителят ще извлече от достигане до информацията по нечестен начин
- цената на защитата на информацията - всички финансови и нефинансови ресурси, инвестирани в осъществяване на мерки за защита на информацията
- цената на пробив в защитата - цената, която нарушителят ще трябва да плати, за да влезе в системата и да си осигури достъп до информацията

УРАВНЕНИЕ НА СИГУРНОСТТА - ФАКТОРИ

- Оценка на цената на съществуващите контроли за сигурност в сравнение с тази на нови контроли
- Цената на защитата на информацията трябва да е по-малка или равна на действителната цена на информацията
- Цената на пробиване на информацията трябва да е по-голяма от възприетата цена на информацията
- Подсигуряването да бъде такова, че цената за пробива на приложените защитни контроли да е по-висока от цената на информацията, придобита при пробива на тези контроли.

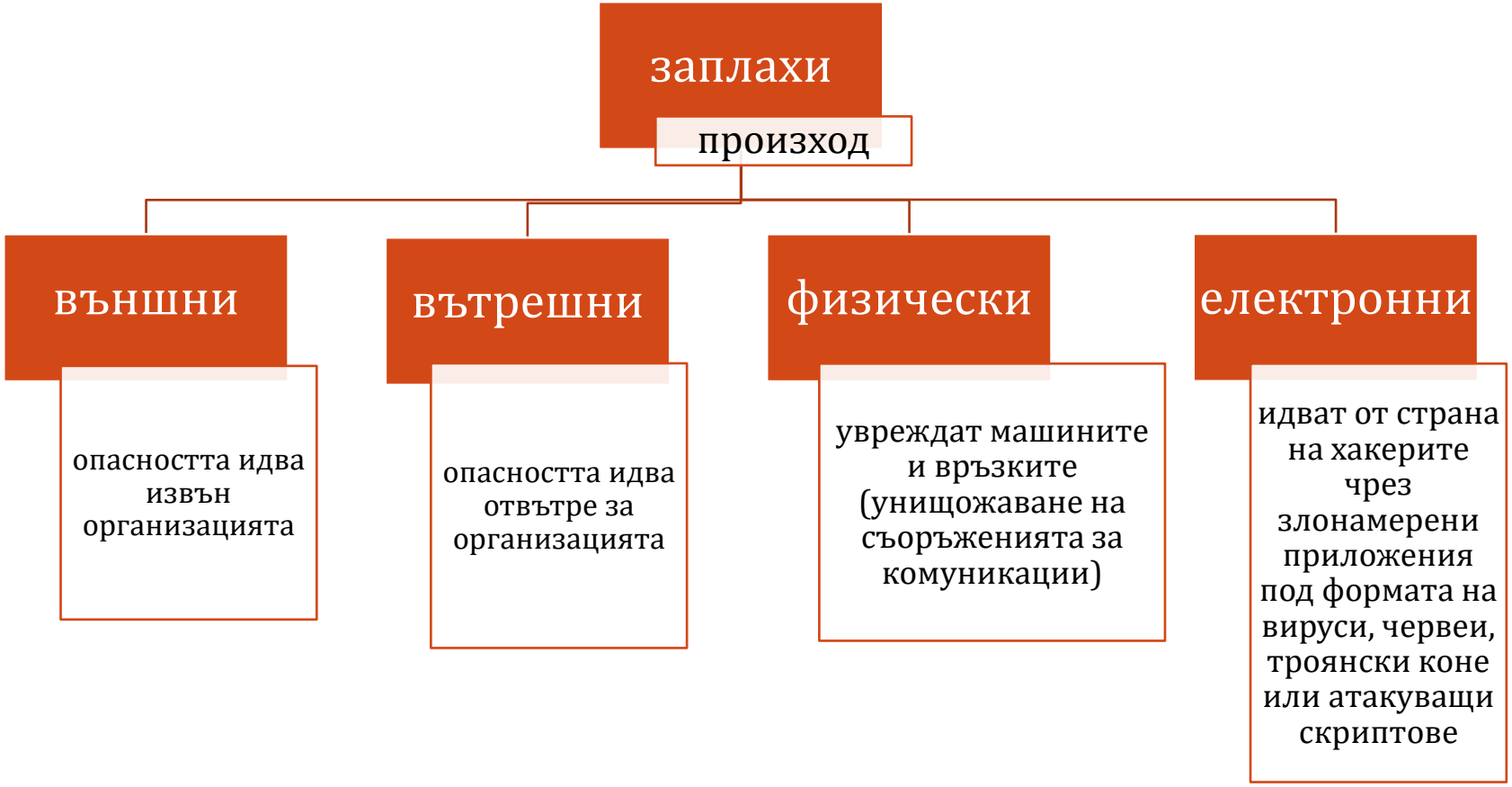
ЗАПЛАХИ И УЯЗВИМИ СТРАНИ

УЯЗВИМОСТ

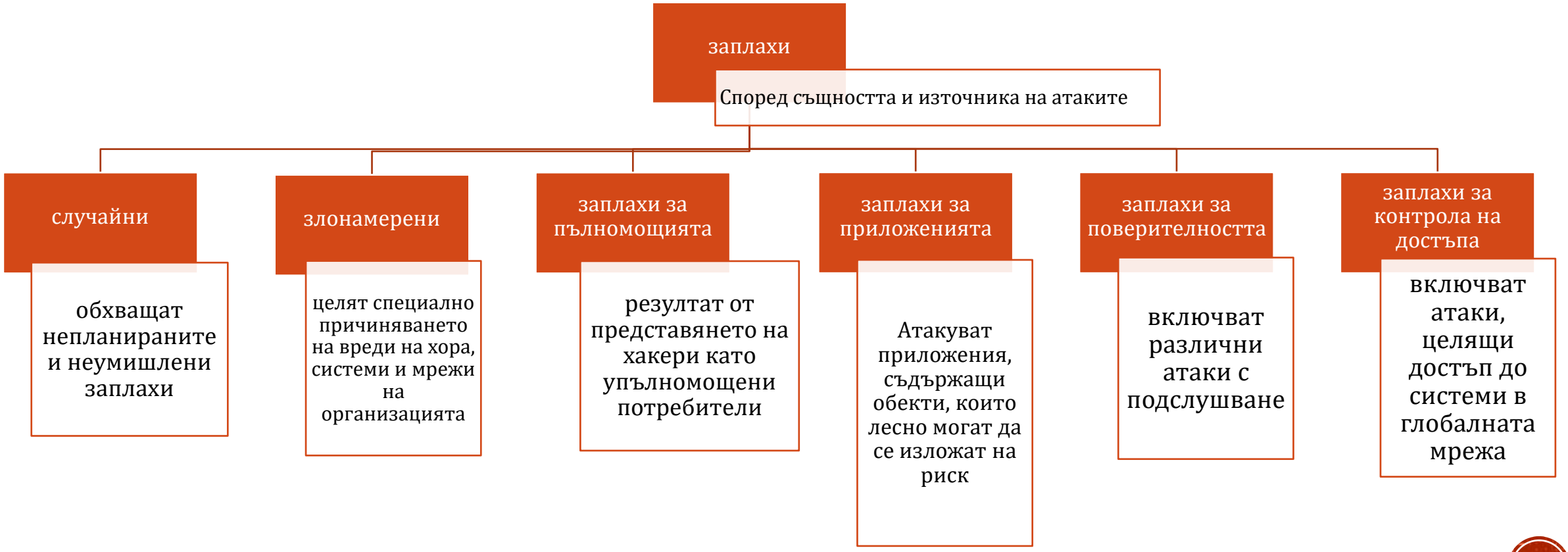
Аспект от система или мрежа, който я оставя открита за атака.

ЗАПЛАХИ

Всякакви обстоятелства или събития, които могат да навредят на система или мрежа.



ЗАПЛАХИ


заплахи
Според същността и източника на атаките
случайни
обхващат непланираните и неумишлени заплахи
злонамерени
целят специално причиняването на вреди на хора, системи и мрежи на организацията
заплахи за пълномощията
резултат от представянето на хакери като упълномощени потребители
заплахи за приложенията
Атакуват приложения, съдържащи обекти, които лесно могат да се изложат на риск
заплахи за поверителността
включват различни атаки с подслушване
заплахи за контрола на достъпа
включват атаки, целящи достъп до системи в глобалната мрежа

СЛУЧАЙНИ ЗАПЛАХИ

Обикновено са резултат от човешки грешки:

- лош избор на пароли;
- случайни или погрешни бизнес трансакции;
- случайно разкриване на информация;
- използване на неподходящ или остарял софтуер;
- недостатъчни познания в системите за сигурност;
- неправилната конфигурация на устройствата за сигурност;
- изтичане на информация поради незащитен трансфер на данните.

ЗЛОНАМЕРЕНИ ЗАПЛАХИ

- злонамерен софтуер - злонамереният софтуер е програмен код, който е целенасочено написан, за да причини вреда на система или мрежа. Вирусите, червеите и троянските коне са типични примери за злонамерени програми;
- неправомерно събиране на информация (social engineering - социално инженерство).

ВИРУСИ

Компютърният вирус е злонамерена програма, която е устроена да се прикрепя към друга програма, файл или дори сектора за зареждане на твърдия диск. Подобно на вирусите в биологията, компютърните вируси се нуждаят от приемник (хост). Обикновено такъв приемник се явява някой изпълним файл или офис документ, който бива заразен. Когато този файл бъде отворен, вирусът се изпълнява и може да порази много други файлове в системата.

ВИДОВЕ ВИРУСИ

- BOOT-секторни – вируси, заразяващи сектора за първоначално зареждане (boot record);
- BIOS вируси - заразяват входно-изходната система на компютъра;
- Файлови вируси - заразяват всички активни програмни файлове (*.COM, *.EXE, *.OVR, *.BIN, *.SYS);
- Стелт – те не променят размера на заразения файл. Секторите, които заразяват се маркират като лоши, въпреки че не са повредени;
- E-Mail вируси – особено актуална категория вируси. Разпространяват се чрез електронна поща и използват адресната книга, за да нападат нови компютри.

ТРОЯНСКИ КОНЕ

- Троянските коне са програми, отварящи вратичка в сигурността на системата;
- Атакуващият може да вижда съдържанието на екрана, да стартира и спира приложения, да изтегля и изпраща файлове, да изтрива файлове, да форматира дискове, да спира или рестартира компютъра и т.н.
- Троянският кон е изпълним файл и заразяването става винаги чрез стартирането му от потребителя;
- Троянският кон обикновено е програма от две части – клиент и сървър.

ЧЕРВЕИ

- Червеите са програми, които се самокопират от компютър на компютър, но не заразяват други програми;
- Подклас на вирусите, но за разлика от тях те могат да се пренасят от един на друг компютър без помощ от страна на човека;
- Основната вреда от тях:
  - заемано процесорно време;
  - консумирана голямо количество системна памет или мрежова лента;
  - часовете, загубени в опити да се отстранят от системата;
  - изпращат се в пространството стотици или хиляди копия на първоначално влезлия в системата червей

ЧЕРВЕИ - РАЗПРОСТРАНЕНИЕ

- Чрез електронна поща - като прикачен към съобщението файл или интегриран в самия текст на писмото. Когато потребителят отвори писмото или файла, прикачен към него, червеят прониква в системата. След това той може да започне да създава свои копия, които да изпрати до наличните контакти в адресната ви книга;
- Чрез уязвимости в операционната система, инсталирания софтуер и дори в мрежовите протоколи;
- Чрез съобщения – използва се софтуер за мигновени съобщения: всякакви **Messenger**-и, **IRC**, **iCQ**, **Skype** и т.н.

ЗАПЛАХИ ТИП СОЦИАЛНО ИНЖЕНЕРСТВО

- Социалното инженерство може да се дефинира като изкуството да използвате външни умения, за да извлечете поверителна информация. То по същество включва външно лице, което лъже персонала на организация да му осигури частна информация или нелегален достъп до ресурси.
- Социалното инженерство може да бъде разгледано като „хакване“ на хора

ЗАПЛАХИ ЗА ПЪЛНОМОЩИЯТА

Заплахите за пълномощията (правата) са резултат от представянето на хакери като упълномощени потребители. Често срещана атака над правата е когато нарушителят открие мрежовата парола на потребител и влезе в системата.

ЗАПЛАХИ ЗА ПЪЛНОМОЩИЯТА - МЕТОДИ

- Разбиване на пароли - от хакерите, и от системни администратори на организации чрез инструменти за разбиване на пароли. Обикновено се генерират хиляди пароли, които се сравняват с наличните хеш кодове, съхранявани в базата данни;
- речникова атака (dictionary attack) - намиране на паролите в определен списък и проверяване на валидността на всяка от тях (смисъл при обикновени думи):
  - Кратки атаки - малко на брой пароли се изпробват върху няколко системи
  - Атаки “Груба сила” (brute force attacks) - нарушителят първо се сдобива със списък от използвани пароли от истински източник. Хешира тези пароли, използвайки криптиращите схеми на атакуваната система. Сравнява стойностите на резултатния хеш код и хешираните пароли, съхранявани в базата данни. Сравнението е успешно, когато хеш стойността от речника съвпада с хеш стойността от базата данни.

ЗАПЛАХИ ЗА ПРИЛОЖЕНИЯТА

- Превишаване на правата - превишаването на права е налице, когато нарушителят има възможност да повиши правата и привилегиите на неговата система до ниво, по-високо от нивото, на което трябва да бъдат;
- Уязвимости на разработен от независим производител или персонализиран софтуер - доставчиците на услуги често използват софтуер, разработен от трети лица (third-party) и го преработват (персонализират) в зависимост от нуждите си. Може да има възможност за пробив.

ЗАПЛАХИ ЗА ПРИЛОЖЕНИЯТА

- Уязвимости на Web сървърите – недобре или в повече конфигурирани предлагани услуги, лошо написани **CGI** скриптове
- Превземане на сесии - HTTP е несвързан протокол. Това означава, че при приключване на първоначалния обмен на съобщения между клиента и сървъра връзката прекъсва. С други думи, HTTP протоколът не запазва състоянието на сесията. Идентификаторът на сесиите (ID) е един вид заобикаляне на проблема със запазването на състоянието на сесията. Cookies осъществяват идентичността на сесиите. При превземането на сесии нарушителят превзема идентичността на сесията чрез достъп до данни на сървъри и мрежи

ЗАПЛАХИ ЗА ПРИЛОЖЕНИЯТА

- Атаки по **e-mail:**
  - e-mail бомбардиране - нарушителят изпраща на мишената идентични писма едно след друго, като по този начин препълва кутията му;
  - изпращане на спам (нежелани) съобщения - метод, при който атакуващите изпращат e-mail на стотици или хиляди потребители;
  - e-mail подслушване и измами - при e-mail подслушването атакуващите прихващат e-mail съобщения по мрежата, преди те да са пристигнали при получателя си. При e-mail измамата атакуващият прихваща e-mail съобщение по мрежата и променя информацията в него със злонамерена цел.

ЗАПЛАХИ ЗА ПОВЕРИТЕЛНОСТТА

Включват различни атаки с подслушване. Някои от тях са:

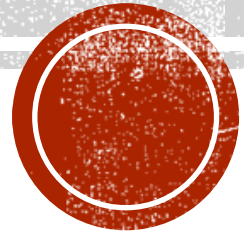
- мрежово подслушване - мрежовото подслушване включва наблюдаване на данните, които се предават по локални мрежи, и извличане на желаната информация. Заради съществуването на такива атаки се препоръчва предаването на данни в криптиран вид;
- подслушване на радио сигнал – използва се по-рядко. Скъпо оборудване.

ЗАПЛАХИ ЗА КОНТРОЛА НА ДОСТЪПА

Включват атаки, целящи достъп до системи в Интернет.

- най-често срещаният метод е разбиване на пароли.
- други атаки включват достъп до файлове с пароли или комуникационни точки като модеми;
- използване на софтуер, който дава достъп до вътрешни или външни системи през задна вратичка (backdoor), експлоатирайки този начин пробиви в мрежата.

КЛАСИФИКАЦИЯ НА ЗАПЛАХИТЕ ЗА СИГУРНОСТТА НА МРЕЖИТЕ



TCP/IP МРЕЖИ - УЯЗВИМОСТИ

Тези уязвимости могат да се класифицират в следните три категории:

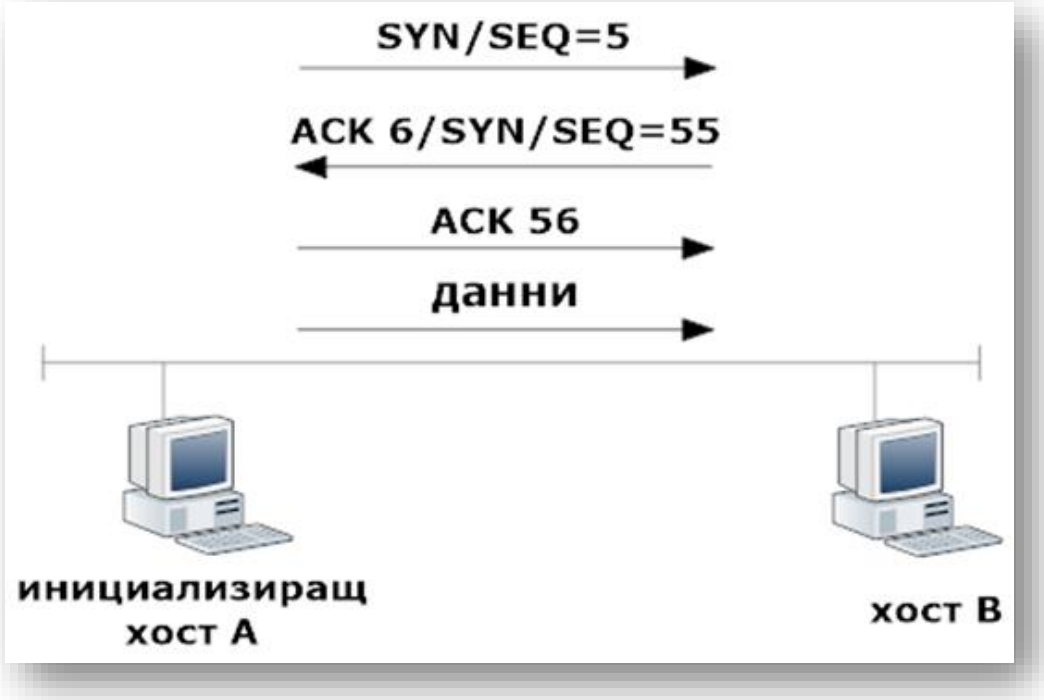
- DoS атаки (Отказ на услуги/Denial of Service) - на упълномощени потребители се отказва достъп до мрежови услуги.
- Разпределени DoS атаки (DDoS) – при атаката се използват по-голям брой компютри. DDoS атаките също целят отказа на мрежови услуги на легитимни потребители;
- Атаки с измами с данни - включват прихващане, промяна и повреждане на данни, пътуващи по мрежата или намиращи се на хостовете.

DOS АТАКИ

- Варианти на прояви:
  - Разстройване на мрежов трафик;
  - Разстройване на връзка между два компютъра в мрежата;
  - Отказ на услуги от сървъра на клиент.
- Класификация:
  - наводняващи атаки - flood атаката затрупва компютърните ресурси и мрежата с огромен брой фалшиви заявки.
  - софтуерни атаки - софтуерните атаки се възползват от присъщи на софтуера уязвимости. Могат да се предотвратят с инсталиране на “кръпки” или пачове (patches) за софтуера.

SYN НАВОДНЯВАЩИ АТАКИ

- използват процеса на трипосочно ръкостискане на TCP
- изпраща фалшива идентичност в **SYN** пакета към сървъра
- потвърждението (SYN + ACK), изпратено от сървъра, никога няма да достигне легитимния клиент
- атакуващият изпраща много фалшиви SYN заявки (с други думи, фалшиви самоличности)
- Сървърът чака по 75 секунди за потвърждение на множеството SYN + ACK



SYN НАВОДНЯВАЩИ АТАКИ

SMURF ИЛИ ICMP_ECHOREPLY НАВОДНЯВАЩИ АТАКИ

- При SMURF атака участват три компонента: компютърът на хакера, пакетен усилвател и компютър-мишена (жертва);
- Хакерът изпраща подправен *echo request* пакет с адрес на избран хост-жертва до разпределен адрес на мрежа - трето лице, която е позната още като мрежа-усилвател
- Всички хостове от мрежата-усилвател изпращат *echo reply* пакет към компютъра-жертва. Засяга се и мрежата-усилвател и атакуваната система

DOS СОФТУЕРНИ АТАКИ - PING НА СМЪРТТА ИЛИ ICMP_ECHO_REQUEST АТАКА

- изпраща верига от фрагментирани ping команди, съдържащи големи по размер ICMP пакети до компютъра-мишена (>=64 KB)
- получаването на по-голям от 65 535 байта размер пакет обикновено причинява срив в системата-жертва. С цел да отговори на ping заявките, когато хостът-мишена започне да сглобява пакетите, става ясно, че те са прекадено големи за буфера му. Следователно се получава препълване на буфера, защото компютърът-мишена е прекадено зает да сглобява толкова много пакети и да изпраща обратно отговори със същите размери

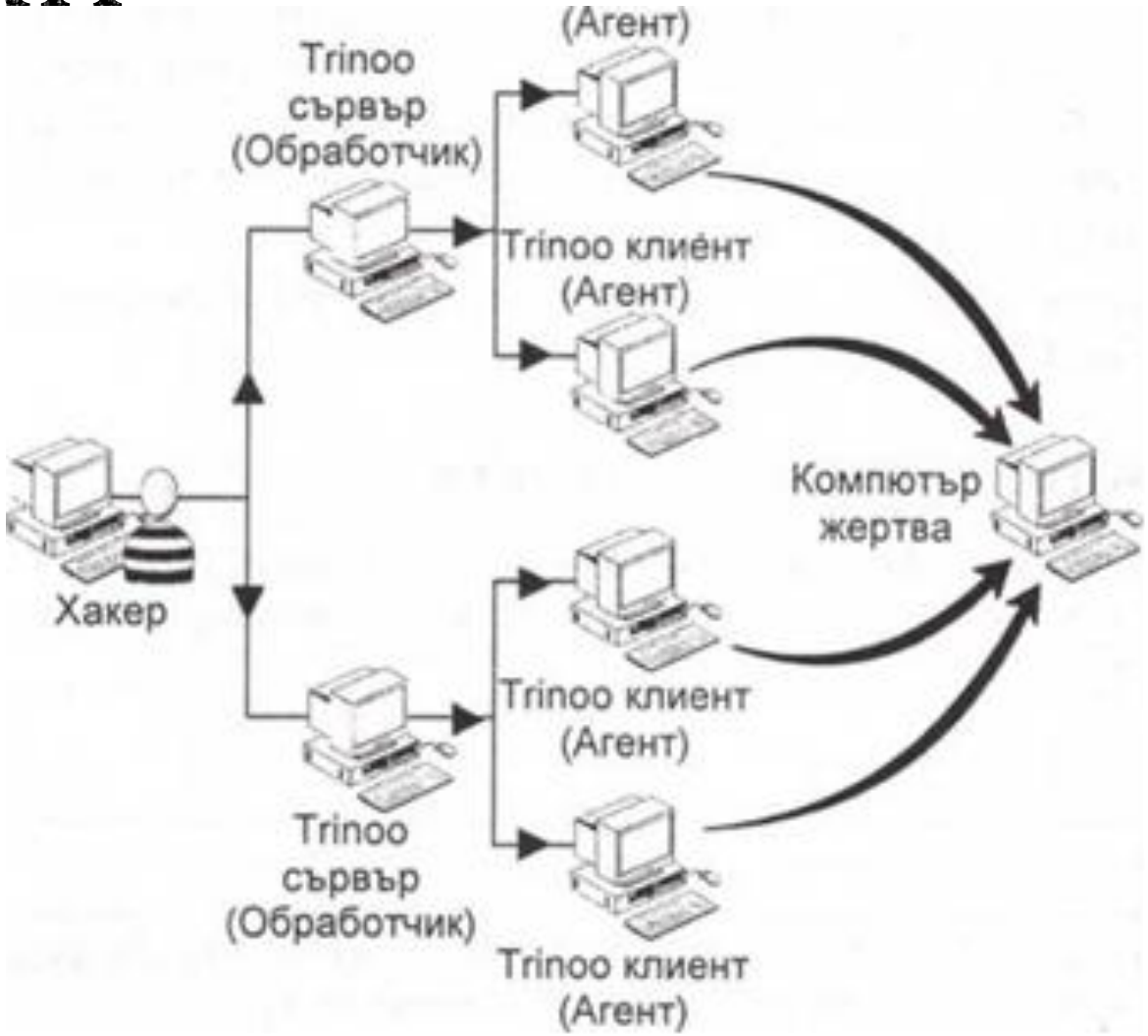
АТАКИ НА УСЛУГАТА DNS

- **DNS измами.** Тези атаки са познати и като DNS превземане. Хакерът има достъп до DNS услуги и променя информацията, която свързва домейн име и IP адрес. Заради това потребителите биват пренасочвани към различен сайт от този, който са искали.
- **DNS препълване на хост име.** В отговора на DNS за хост име има дефинирана максимална дължина на хост името. DNS препълването на хост име се получава, когато се провали проверката на разрешената дължина на името в DNS отговора. Заради това се получава препълване на буфера, когато хост името е копирано в DNS сървъра.

АТАКИ НА УСЛУГАТА DNS

- **DNS препълване на дължина.** Освен максимална дължина на хост име, DNS отговорът още съдържа и поле за дължина, което има допустим предел от 4 байта. Ако бъде определена голяма стойност, се получава препълване на буфера, което позволява на атакуващия да изпълни администраторски команди на системата-мишена.
- **DNS трансфер на зони от привилегировани портове (1-1024).** Този тип препълване се получава, когато хакерът използва DNS клиентско приложение, за да пренесе зони от вътрешен DNS сървър през привилегировани портове (1-1024). DNS зоната дефинира DNS йерархично пространство за имена, които се използват за разграничаване на различните области на действие на DNS сървъра. С други думи, те дефинират кои DNS сървъри имат право да разрешават въпроси за анализ на имена за дадена секция от DNS йерархията.

DDOS АТАКИ


(Агент)
Trinoo
сървър
(Обработчик)
Trinoo клиент
(Агент)
Компютър
жертва
Хакер
Trinoo клиент
(Агент)
Trinoo
сървър
(Обработчик)
Trinoo клиент
(Агент)

АТАКИ С ИЗМАМИ НА ДАННИ

Атаките с измами на данни включват прихващане, промяна и повреждане на данни, пътуващи по мрежата или намиращи се на хостовете. Методи:

- *измами* (spoofing) - компютърът на хакера се маскира като компютър от мрежата на компютъра-мишена
- *подслушване* или слухтене (sniffing) - улавяне на мрежова информация
- превземане на сесии
- промяна на маршрута и сканиране на портове, чрез които може да се създаде атака с измама на данни – целят се в маршрутизиращите таблици или отворени и незащитени портове.

ЗАЩИТНИТЕ СТЕНИ (FIREWALLS)

КАКВО Е ЗАЩИТНА СТЕНА В КОНТЕКСТА НА МРЕЖИТЕ?

- Система или комбинация от системи, която подсилва границата между две или повече мрежи;
- Казано просто, защитната стена реализира правила за сигурност, които отделят две мрежи от нежелана комуникация;
- Мрежовите защитни стени пазят критична информация от опасности и в същото време позволяват преминаването на информация;
- Защитните стени предпазват мрежите от хакери и атаки, като например DoS атаки или атаки “ping на смъртта”, и също позволяват преминаването на HTTP пакети и e-mail съобщения;

НА КОЙ СЛОЙ РАБОТИ ЕДНА ЗАЩИТНА СТЕНА?

- Една защитна стена може да работи на различни нива в разделена на слоеве мрежова архитектура на OSI и TCP/IP моделите;
- Най-ниското ниво, на което може да работи една защитна стена, е мрежовият слой;
- На мрежовия слой защитната стена може да определи дали един пакет идва от автентичен източник;
- Защитните стени от транспортния слой могат да потвърждават връзки, преди да решат дали да разрешат или не някой пакет;
- Защитните стени, работещи в приложния слой, могат да изпълняват по-сложни функции, като например филтриране на трафика, на базата на съдържанието на пакетите от данни или по-скоро на типовете приложения.

ФУНКЦИОНАЛНОСТ НА ЗАЩИТНИТЕ СТЕНИ

- *Филтриране на пакети*. Става въпрос за филтрирането на входящи и изходящи пакети на базата на информацията за протокола и адреса, въпреки че не се проверява съдържанието на пакета. Това е най-основната функция на една защитна стена.
- *Преобразуване на мрежов адрес*. Тази функция скрива хостове на вътрешни мрежи от хостове на външни мрежи чрез преобразуване адресите и портовете на вътрешни хостове до често срещани външни адреси на защитната стена. Защитни стени, които действат по този начин, предотвратяват наблюдението на вътрешни хостове от злонамерени хостове на публична мрежа.
- *Прокси услуги*. Те предоставят обмен на данни от страна на клиентските приложения с отдалечени системи. Така клиентският компютър се скрива зад защитната стена и за отдалечената система изглежда сякаш проксито (proxy) взаимодейства с нея.

ФУНКЦИОНАЛНОСТ НА ЗАЩИТНИТЕ СТЕНИ

- *Потребителска автентикация*. Тази функция е удобна, когато отдалечени потребители (в публична мрежа) използват динамични IP адреси, за да се свържат с частни мрежи. В този случай ограничение на базата на IP адреси не е практично, защото потребителят ще получи различен IP адрес, когато се свърже. Затова защитната стена ще поиска проверка на автентичността, преди да позволи влизане в частната мрежа.
- *Тунелиране (Tunneling)*. Чрез създаване на виртуален тунел се позволява на физически отделни мрежи да използват Интернет като среда за комуникация. Една такава реализация на защитните стени помага за създаване на виртуални частни мрежи (Virtual Pi Networking, VPN).

КЛАСИФИКАЦИЯ

- защитни стени, филтриращи пакети;
- защитни стени, преобразуващи мрежови адреси (Network Address Translation, NAT);
- circuit relay защитни стени;
- прокси защитни стени за приложения

ЗАЩИТНИ СТЕНИ, ФИЛТРИРАЩИ ПАКЕТИ

- най-основните защитни стени, които работят в мрежовия слой на OSI и TCP/IP модела;
- филтрират пакети на базата на правила, дефинирани в самите тях;
- не предоставят пълна сигурност за вътрешна мрежа;
- Стандартните филтри на пакети определят неприкосновеността на пакетите на базата на информацията, съдържаща се в заглавните части на индивидуалните пакети. Теоретично филтрите могат да бъдат конфигурирани да сортират пакети на базата на всяка част от информацията в полетата за данни в заглавието на протокола.
- Има два типа защитни стени, филтриращи пакети - stateless защитни стени stateful защитни стени.

STATELESS ЗАЩИТНИ СТЕНИ, ФИЛТРИРАЩИ ПАКЕТИ

- не могат да запазват информация за установена сесия между два хоста на частни и публични мрежи;
- не могат да определят дали между хостовете е установена обратната сокетна връзка.

Пример:

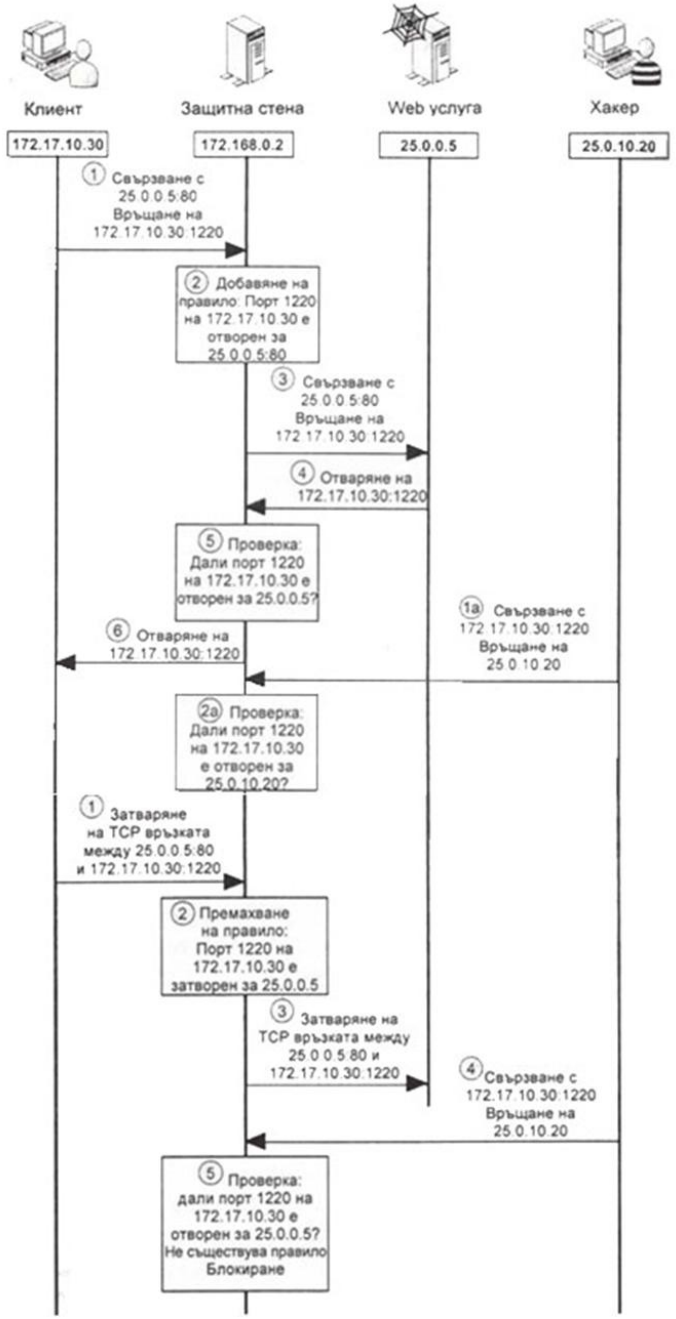
Хост в частна мрежа изпраща заявка за достъп до сайт с адрес 10.0.0.1 през порт 80.

Пакетите на заявката, доставени до хоста на публичната мрежа, съдържат още информация за обратния сокет (IP адреси и номер на порт), на който хостът на частната мрежа иска да слуша. Един stateless филтър на пакети не може да запази тази информация.

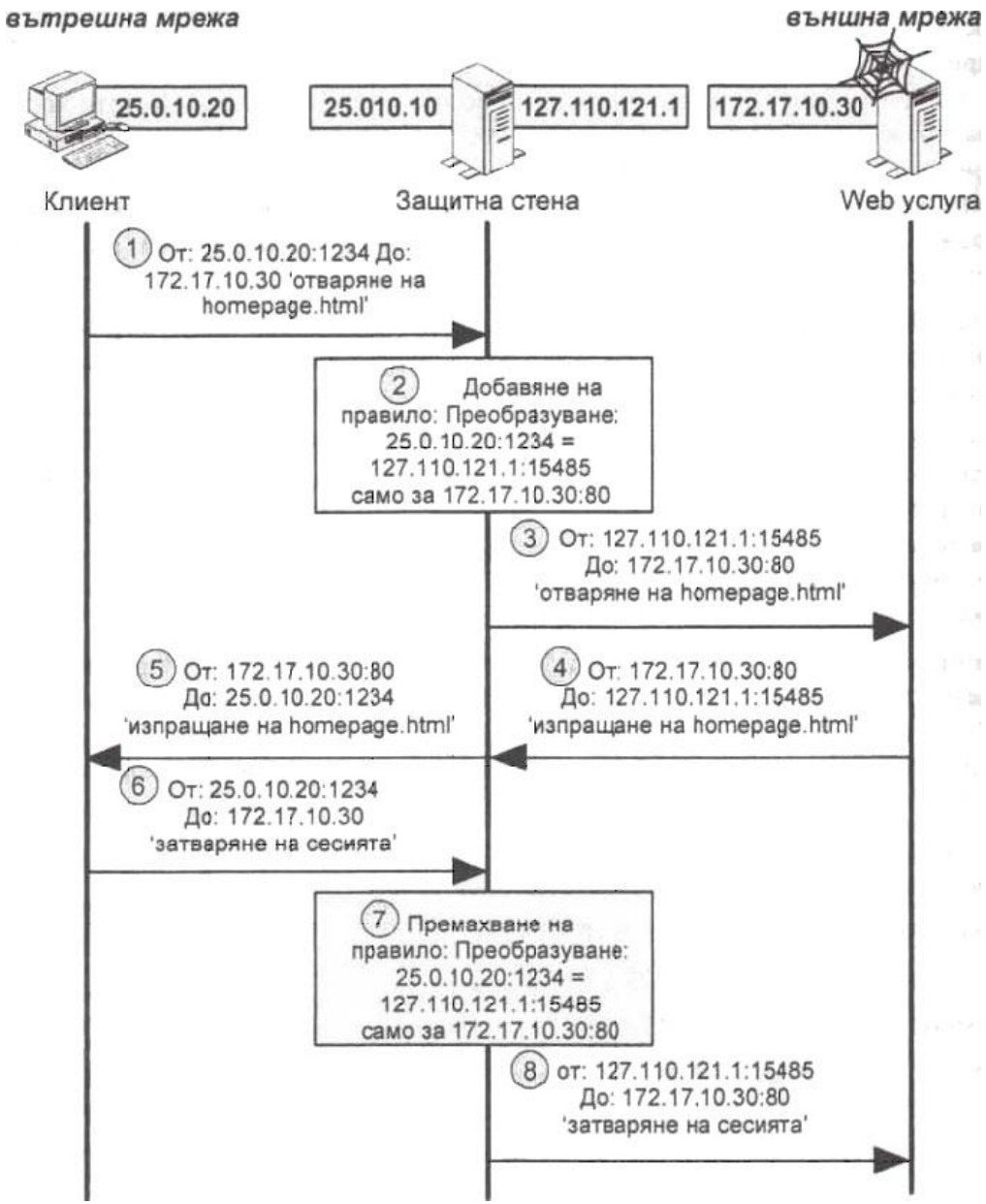
STATEFUL ЗАЩИТНИ СТЕНИ, ФИЛТРИРАЩИ ПАКЕТИ

- запазват състоянието на връзки чрез запис на информацията за установяване на сесия между два хоста по мрежите. На базата на тази информация филтрите решават дали пакетите върнати от публична мрежа са от доверени хостове.
- Полезни са, когато трябва да се филтрира безвръзков трафик като например DNS сървъри, които се базират на UDP.
- Stateful защитните стени, филтриращи пакети, не позволяват през тях да преминават никакви услуги освен тези, които са програмирани да пропускат, и връзките, които поддържат в таблицата си със състояния.
- Сесийният запис съдържа подробности, като например получаващия сокет (IP адрес и номер на порт) и сокет на източника (IP адрес и номер на порт). Когато хостът в публичната мрежа изпрати обратно отговор, филтърът проверява записа в таблицата си, за да потвърди информацията за източника на пакета и получаващия го сокет. Ако не намери запис, пакетът се игнорира.

- Stateful защитна стена, филтрираща пакети

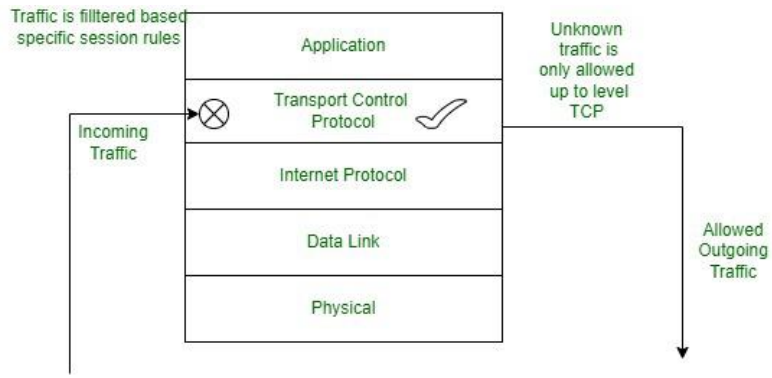


- Защитни стени, преобразуващи мрежови адреси (Network Address Translation, NAT)



CIRCUIT RELAY ЗАЩИТНИ СТЕНИ

- Circuit relay е вид circuit-level gateway методология на защитна стена, в която връзките на данните се потвърждават преди данните да се обменят в действителност. Това означава, че защитната стена не само изпълнява функцията предаване/отказване на пакети от данни, но също и определя дали връзката между двата клиента е валидна според конфигурираните правила.
- Една защитна стена може да потвърди връзка според следното:
  - Целеви IP адрес и/или порт;
  - IP адрес и/или порт на източника
  - Време от денонощието;
  - Протокол;
  - Потребител;
  - Парола и др.



- Circuit-level защитната стена работи на сесийно ниво от OSI или между слоя на приложението и транспортния слой на TCP/IP

ПРОКСИ ЗАЩИТНИ СТЕНИ ЗА ПРИЛОЖЕНИЯ

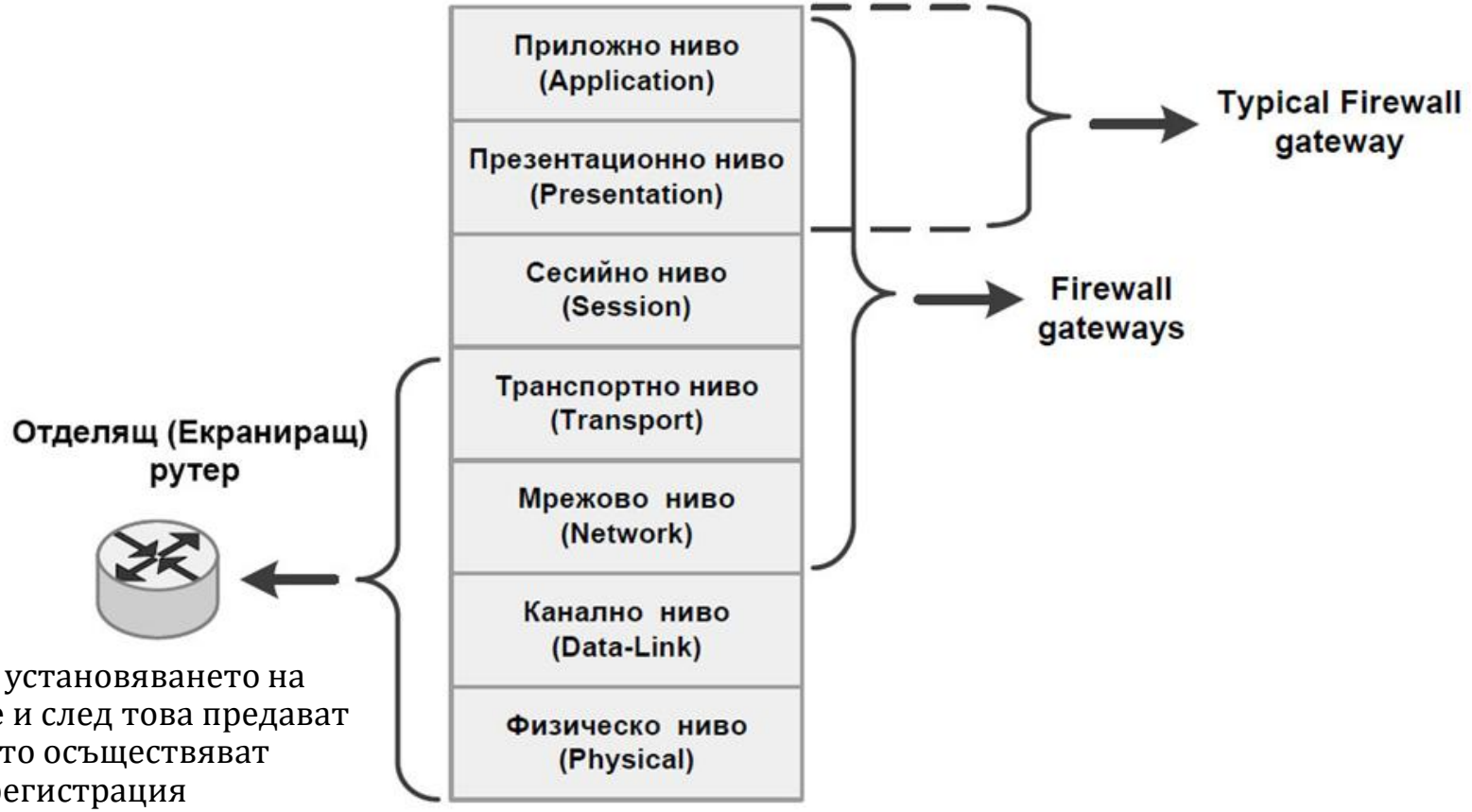
- Думата прокси (proxy) в действителност означава едно нещо, заместващо друго.
- Прокси сървърите заместват директната комуникационна връзка между клиент и сървър с техните услуги.
- Като NAT, прокси сървърите скриват клиента от сървъра, без да нарушават комуникационната връзка помежду им.
- Прокси сървърите се развиха от обикновени машини за “складиране” до защитни стени.

Някои, функции на прокси защитната стена:

- Прокси защитна стена с възможност за филтриране и скриване на IP (NAT функционалност)
- Прокси защитни стени с филтриране на ниво приложения за определено съдържание

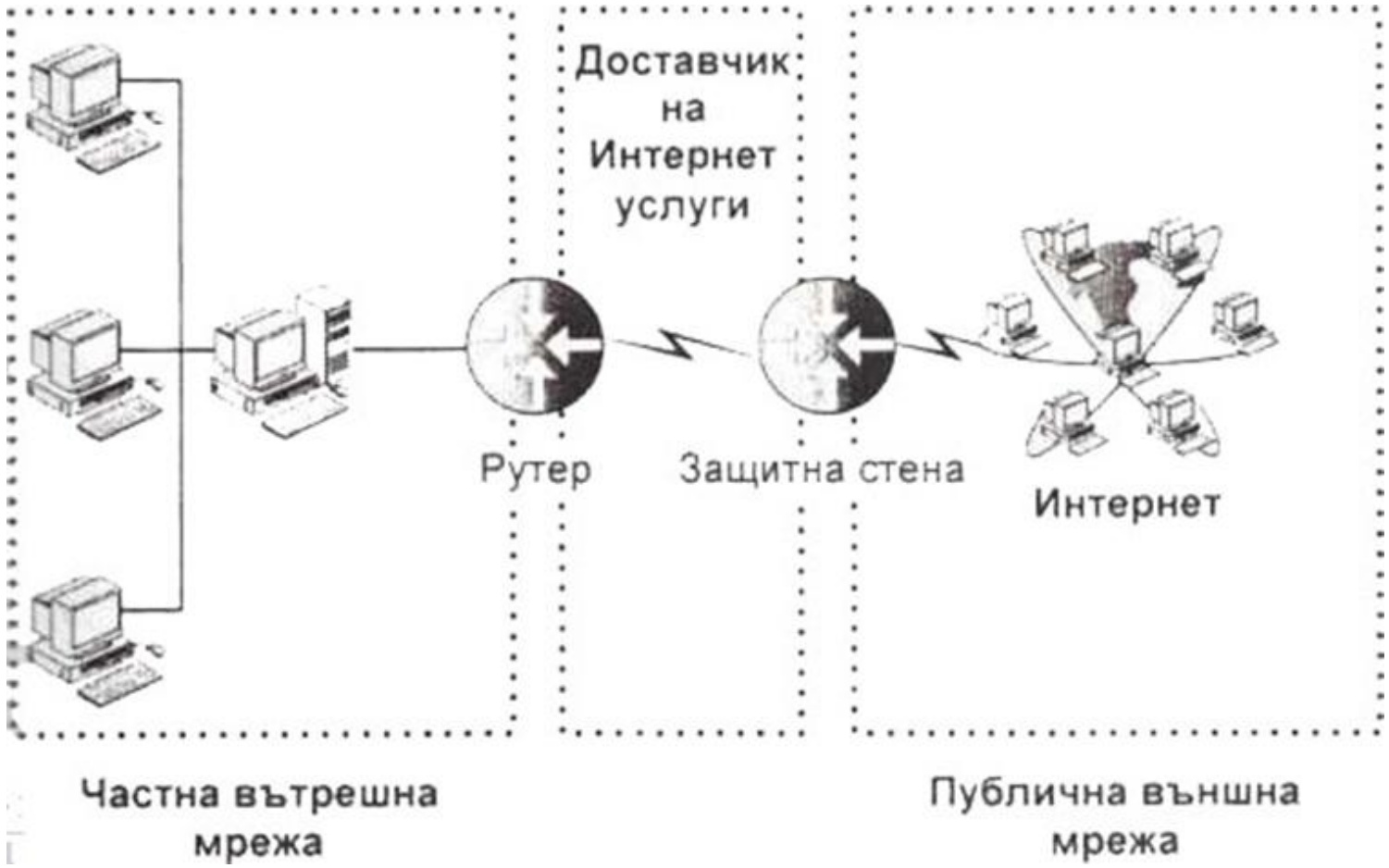
ПЛАНОВЕ НА ЗАЩИТНИ СТЕНИ

Разположението на защитните средства съгласно OSI модела

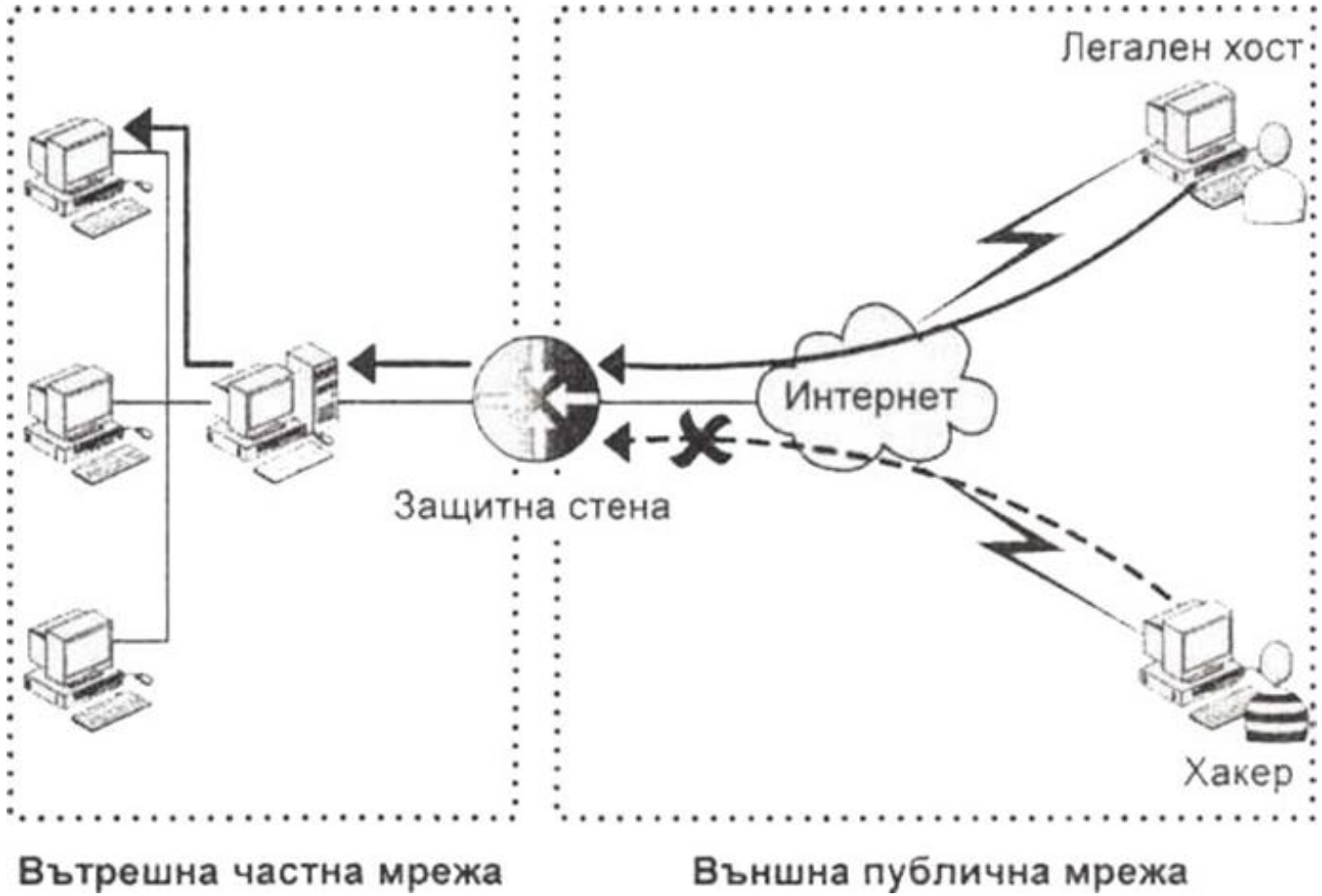


Осигуряват установяването на съединение и след това предават данните, като осъществяват контрол и регистрация

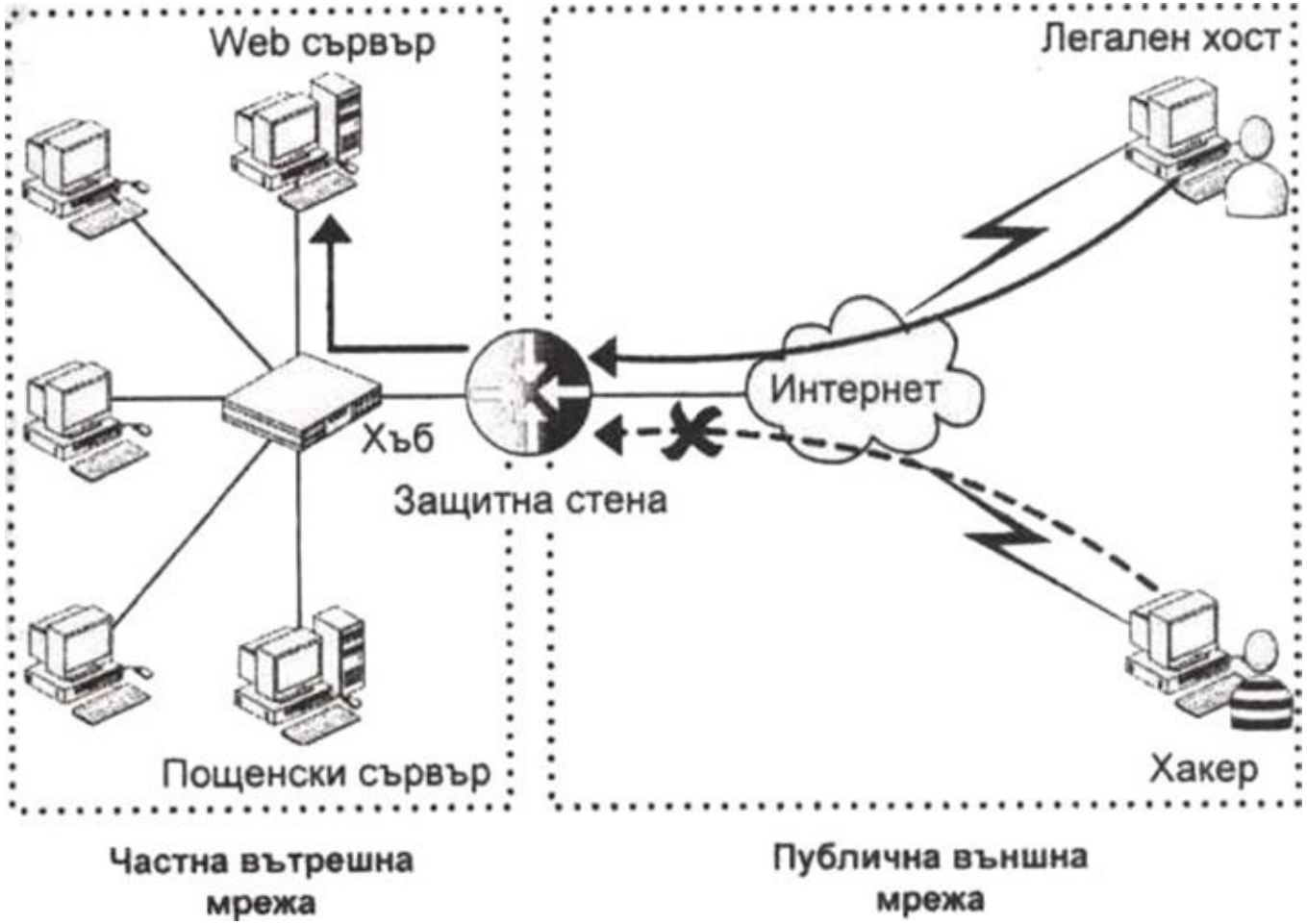
ПАКЕТНИ УСЛУГИ, ФИЛТРИРАНИ ОТ ISP



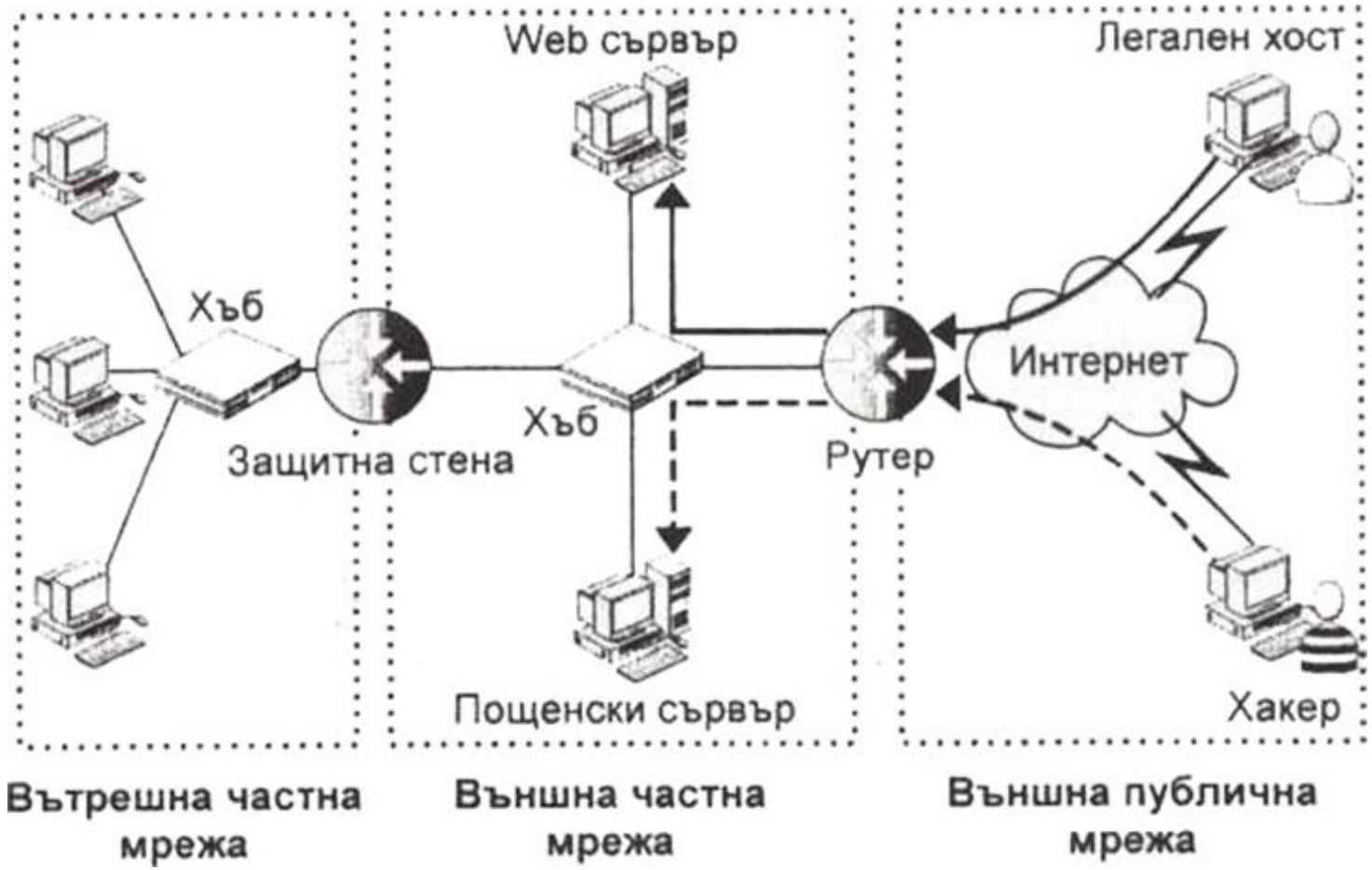
ПЛАН С ЕДИНСТВЕНА ЗАЩИТНА СТЕНА



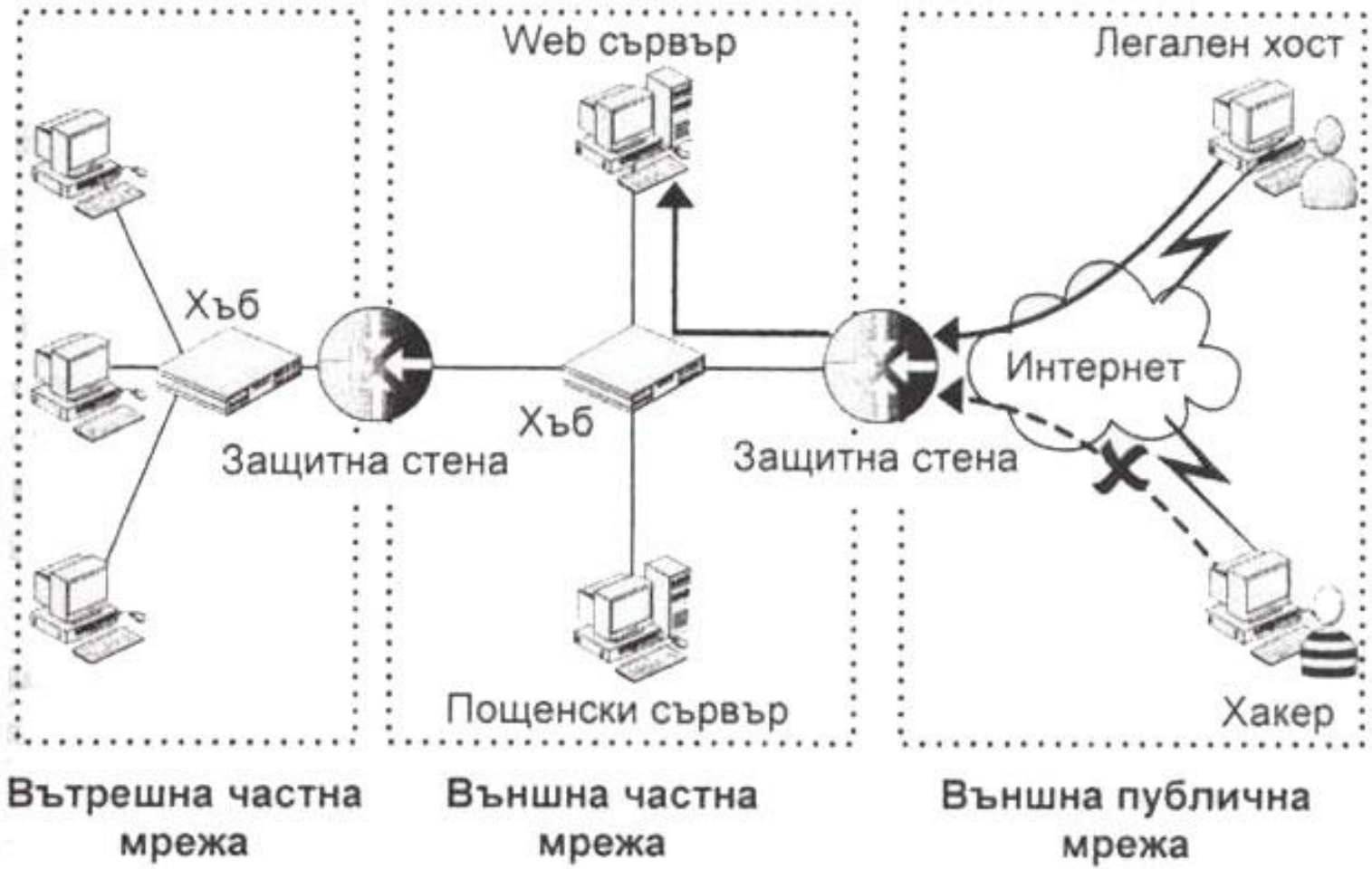
ВАРИАНТ - „ПОРТАЛНА ДВУДОМНА ЗАЩИТНА СТЕНА”



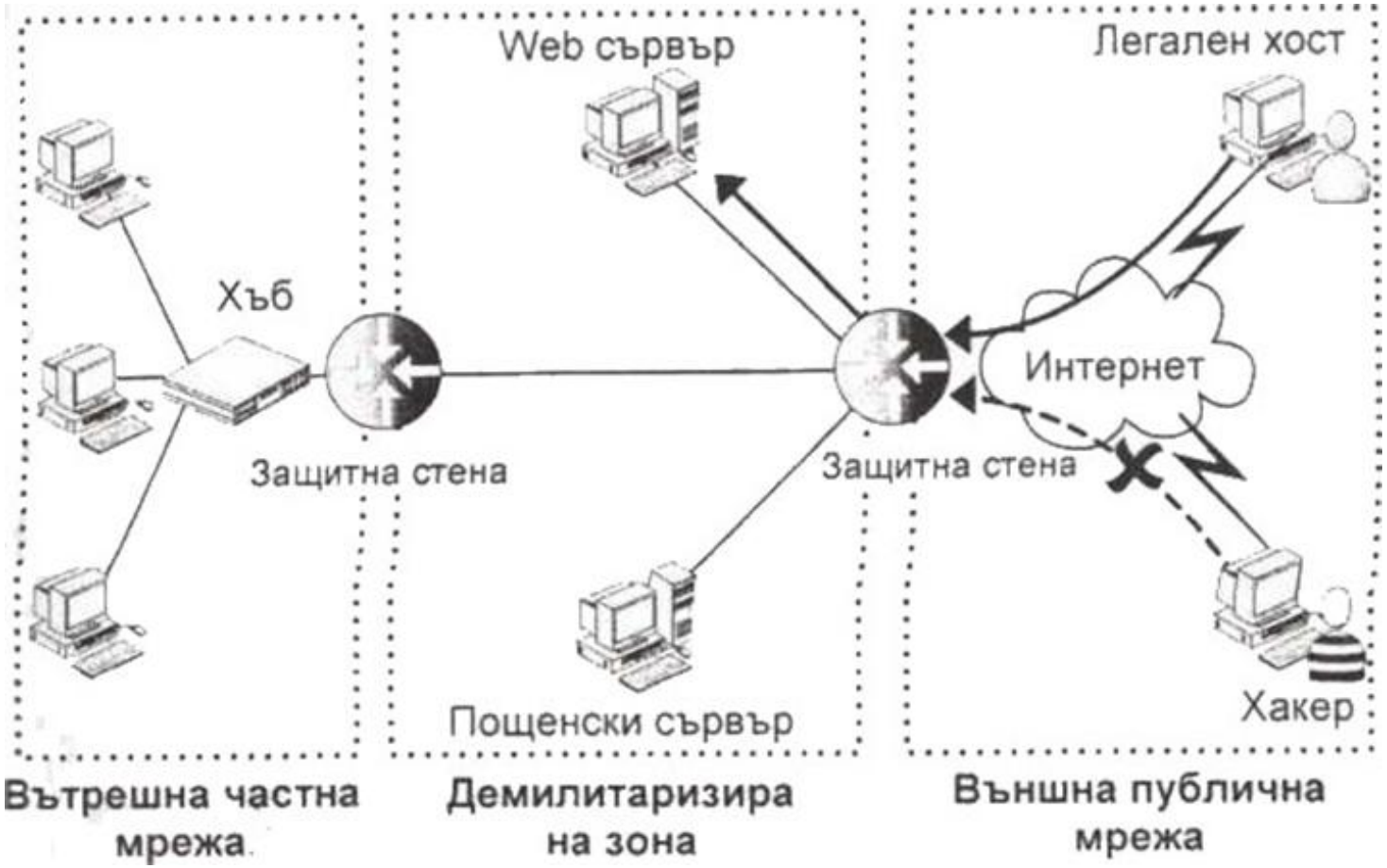
ВАРИАНТ - ЕДИНСТВЕНА ЗАЩИТНА СТЕНА С ОТКРИТИ СЪРВЪРИ



ПЛАН С ДЕМИЛИТАРИЗИРАНА ЗОНА (DEMILITARIZED ZONE, DMZ)



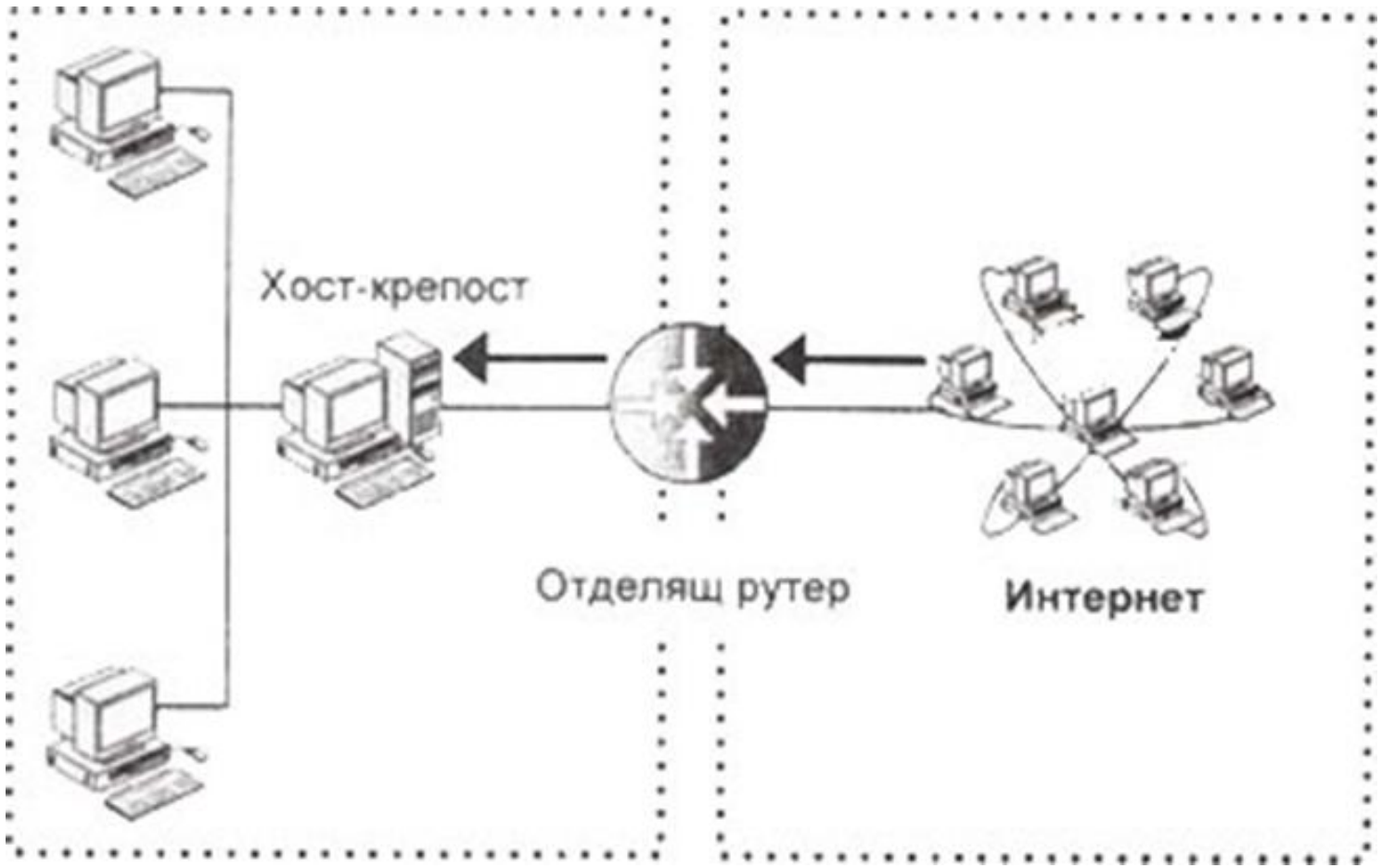
ВАРИАНТ - “ТРИДОМНА ЗАЩИТНА СТЕНА”



ЗАЩИТНА СТЕНА С ОТДЕЛЕН ХОСТ (BASTION HOST)

Бастион-хостът (хост-крепост) е компютър, управляващ входящия и изходящия трафик в дадена мрежа с възможности за филтрация на всички нива от OSI модела

ВАРИАНТ - ХОСТ-КРЕПОСТ И ОТДЕЛЯЩ РУТЕР



ПЛАН ЗА ЗАЩИТНА СТЕНА С ОТДЕЛЕНА (ЕКРАНИРАЩА) ПОДМРЕЖА

ИЗБОР НА ПОДХОДЯЩ ПЛАН НА ЗАЩИТНА СТЕНА

- План с единствена защитна стена е най-подходящ, когато организацията се нуждае да реализира икономично решение със защитна стена. Това означава, че организацията планира да използва само един рутер за осъществяване на функции на защитна стена, планът с единствена защитна стена е най-добро и най-ефективно решение относно цената.
- Ненадеждният хост план, при който публичните сървъри на организации са поставени зад защитната стена или след нея и са отворени за света, е подходящ, когато публичните сървъри на частна мрежа не изискват висока сигурност и не разстройват услугите на вътрешната мрежа.
- Планът с демилитаризирана зона е най-подходящ, когато една организация иска да защити публичните си сървъри, както и вътрешната си мрежа.

ОЦЕНКА НА ВЪЗМОЖНОСТИТЕ НА ЗАЩИТНАТА СТЕНА

- Мащабируемост - ако може да обедини други нови приложения и защитни стени.
- Сложност - не трябва да е толкова сложна, че да е трудно да се разбере, инсталира, конфигурира и поддържа. Лесни инсталационни стъпки елиминират риска от грешни конфигурационни настройки. Освен това интерфейсът на защитната стена трябва също да е прост и последователен, така че да е лесно да се администрира.
- Бързодействие - трябва да подсилва скоростта и бързодействието на цялата мрежа на организацията, вместо да я затруднява.
- Допълнителни възможности - да съдържат функционалност за тунелиране, да документират дейността на мрежата, предоставят механизми за хващане на нарушители (honeypot механизмът - примамва нарушители с показване на данни, които не са истински)

ОТКРИВАНЕ НА ПРОБИВИ

- Пробивът (intrusion) е неупълномощен достъп до и/или активност в информационна система.
- Откриването на пробиви е изкуството за откриване и реагиране на компютърни атаки и злоупотреби. Откриването на пробив (intrusion detection) е процесът на идентифициране, че е направен опит за пробив, че пробивът се случва в момента или че вече се е случил.
- Неговите функции включват предпазване, възпиране, откриване, реагиране, оценка на щетите, очакване на атаки и поддържане на информация за пробивите.
- Индикацията (indication) е информация, която предполага заплаха. Тя включва. специфични доказателства, че се е случил пробив, и включва интересите, намеренията и възможностите на заплахата.

ТЕРМИНИ

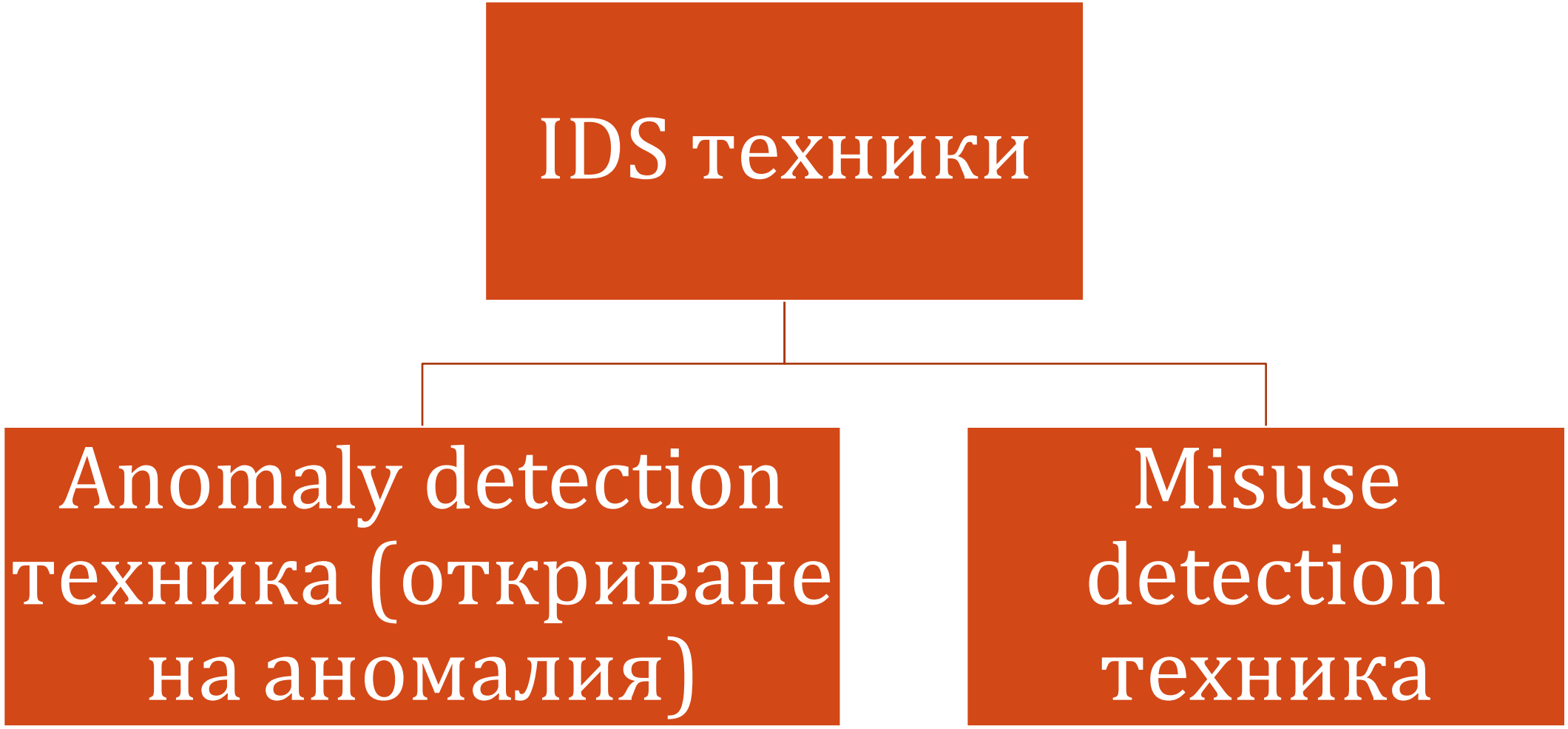
- Intrusion detection означава откриване на неупълномощен достъп до компютърна мрежа.
- Misuse detection означава откриване на активност, съвпадаща със “злоупотреба” по зададени правила.
- Anomaly detection означава откриване на нарушения от приемливия профил на поведение.
- False-positive е аларма за някои неестествени дейности, които не са злоупотреба (фалшива тревога).
- False-negative е злоупотреба, която не се открива или алармира.

СИСТЕМА ЗА ОТКРИВАНЕ НА НАРУШИТЕЛИ (IDS -INTRUSION DETECTION SYSTEM)

- Защитната стена е ключалката на врата;
- IDS е алармата срещу проникване с взлом, в случай че защитата е преодоляна;
- IDS е софтуер, който автоматизира процеса за откриване на проникванията.

СИСТЕМИТЕ ЗА ЗАЩИТА ОТ ПРОНИКВАНИЯ (INTRUSION PREVENTION SYSTEM - IPS)

- Системите за защита от прониквания (Intrusion Prevention System - IPS) е софтуер, който има всички възможности на IDS, но освен това предлага възможност да предприеме действия срещу възможните инциденти.
- Администраторът може да изключи функциите за защита от прониквания, което ще накара IPS да функционира като стандартна IDS.


IDS техники
Anomaly detection техника (откриване на аномалия)
Misuse detection техника

ANOMALY-DETECTION ТЕХНИКА

- Аномалия – поведение, което не е нормално и е неправилно. Идентифицира се като се следи за съвпадение с предварително създадени профили за мрежова активност;
- Приема всички действия, несъвпадащи с набор от зададени поведения, за аномалия;
- Създава профили за нормална работа на системата при различни операции след продължително наблюдение;
- Натрупва ги в статистическа БД – например поведение при входно-изходни операции, използване на централен процесор, памет, мрежови операции и т. н.;
- Излизането извън тези параметри – не нормално поведение;
- Недостатък – наличие на **false-positive** аларми
- Недостатък – този модел няма възможност да анализира поведение по шаблон и да идентифицира причината за ненормалното събитие.

MISUSE-DETECTION ТЕХНИКА

- Използва сигнатури (**signature-based**) – съвкупност от подпис, шаблон и поведение (образци на пакети, с които са направени опити за атака);
- Поддържа БД от сигнатури на познати атаки;
- Алармира при наличие на атака със сигнатура, съвпадаща с някоя от БД;
- Открива варианти на една и съща атака;
- Липса на **false-positive** аларми;
- Не открива нови типове атаки, ако не са открити по-рано;
- Трябва да се обновява БД. Голямата БД забавя **IDS.** Може да се използват само тези образци, които имат отношение към нашата мрежа.

КОМПОНЕНТИ НА IDS

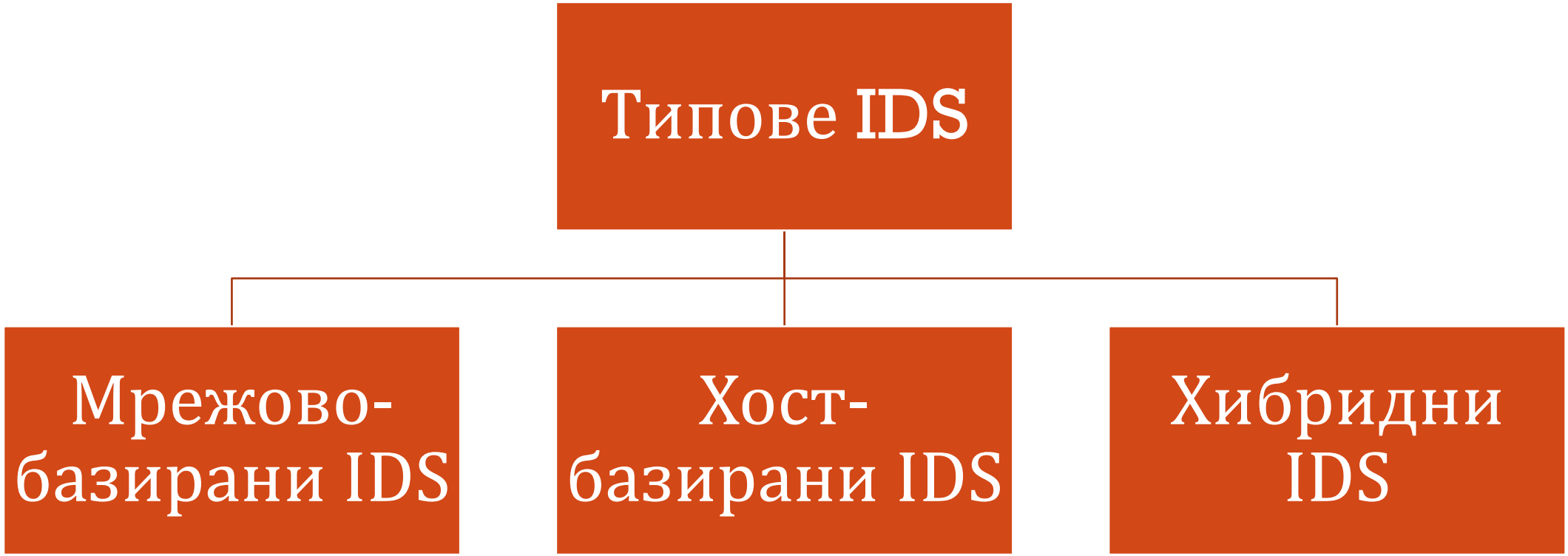
- Командна конзола - централната среда, която контролира цялата IDS. Тя обикновено е посветена машина с инструменти за указване на политики и аларми. Поддържа контакт с наблюдаваните машини и/или мрежовите сензори през кодирана връзка.
- Сензор или агент - софтуерни програми, които могат да бъдат инсталирани на посветени машини или мрежови устройства в критични сегменти на мрежата. Това са самостоятелни системи за откриване, през които минават данните по мрежата. Главната роля на сензорите е да търсят в мрежовите пакети шаблони за злоупотреба и в случай на нарушение да генерират аларми в централната конзола на мрежата.

КОМПОНЕНТИ НА IDS

- Оповестяване на проблем - този компонент в IDS е отговорен за свързването с отговорника по сигурността в случай на забелязано нарушение. Това става посредством аларми на екрана, звукови оповестявания, изпращане на съобщения до пейджър или електронна поща.
- Реагираща подсистема - както предполага името, тя е отговорна за извършването на действие, базирано на отчетените заплахи към системата-цел. Тези подсистеми могат да генерират отговори автоматично или по заявки от системния оператор. Най-честите отговори (ответни реакции), генерирани от подсистемата, включват преконфигуриране на рутер или защитна стена и изключване на системата-цел.

КОМПОНЕНТИ НА IDS

- База от данни (БД) - информационен склад за всички дейности, наблюдавани от IDS. Базата от данни включва статистика и за злоупотребите, и за поведението. Тези статистики спомагат за създаването на поведенчески шаблон за действия, които по-късно могат да се използват за оценяване на вредата и изследване.
- Мрежов кран (network tap) - устройство или софтуерна програма, която позволява събирането на информация от мрежата. Когато е устройство кранът на мрежата трябва да има (поне) три порта: порт A, порт B и порт за монитор. Освен предаването на трафика между портовете A и B в реално време копира същите тези данни на порта на монитора, което позволява на трета страна да слуша.


Типове IDS
Мрежово-базирани IDS
Хост-базирани IDS
Хибридни IDS

ОСНОВНАТА РАЗЛИКА МЕЖДУ МРЕЖОВА И ХОСТ-БАЗИРАНА IDS

Мрежово-базирана IDS

обработва TCP/IP пакети

Хост-базирана IDS

обработва журналите със събития, генерирани от операционната система и приложенията

МРЕЖОВО-БАЗИРАНА IDS

- Мрежово-базираната IDS се използва за наблюдение и анализ на пакети от данни, които минават по мрежата;
- Мрежово-базираната IDS е позиционирана така, че да открива опити за достъп и различни атаки, произхождащи извън мрежата;
- Открива кражба на данни или ресурси, изтегляне на пароли, кражба на трафик, наводнение с пакети, деформирани пакети, DoS и DDoS атаки.

Архитектура на мрежово-базираната IDS

Състои се от сензори, разгърнати из цялата мрежа и докладващи на командната конзола

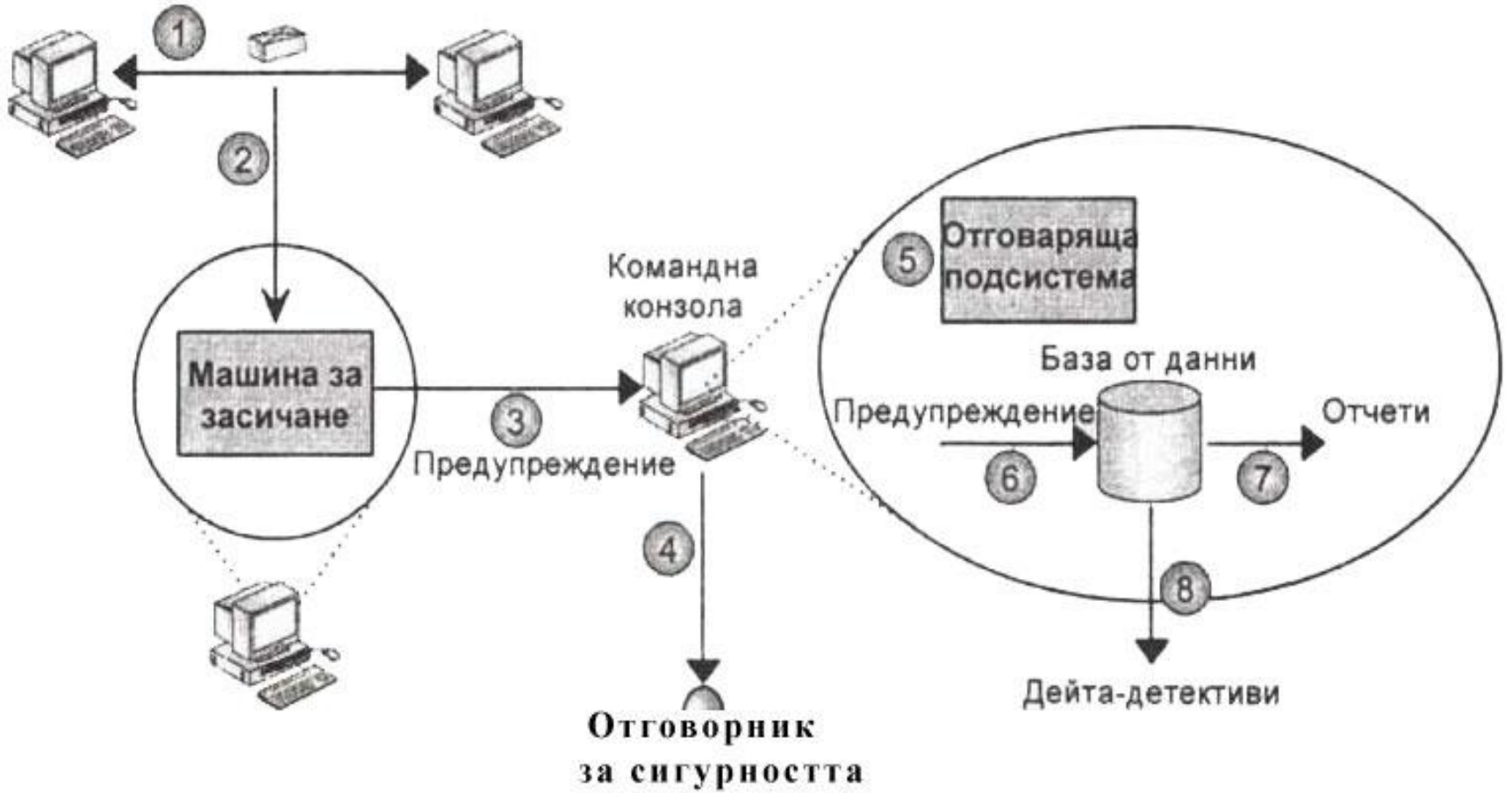
Традиционна сензорна архитектура

целя наблюдаването на всички сегменти от мрежата чрез сензори, разположени в тях

Разпределена мрежова архитектура

наблюдават пакетите насочени към един компютър чрез сензор, инсталиран на него

ТРАДИЦИОННА СЕНЗОРНА АРХИТЕКТУРА



РАЗПРЕДЕЛЕНА МРЕЖОВА АРХИТЕКТУРА

РАЗПОЛОЖЕНИЕ НА МРЕЖОВО-БАЗИРАНА IDS

Сензор, разположен във вътрешната мрежа

- голяма част от подозрителния трафик ще бъде блокиран от защитната стена
- IDS извършва и важна проверка на правилното конфигуриране и функциониране на самата защитна стена

Сензор, разположен извън защитна стена

- гарантира, че целият трафик ще бъде проверяван за атаки преди да бъде филтриран
- служи като система за ранно предупреждение, която да ни показва пред какви заплахи е изправена защитната стена
- Основният недостатък на тази конфигурация е, че тя ще генерира голям брой аларми

Може едновременно и от двете страни

Работни режима на мрежово-базираната IDS

два работни режима

с предупреждения (tip-off режим)

открива мрежов пробив по времето на случването му и предупреждава за него

наблюдение (surveillance режим)

surveillance се предприема, когато вече е имало пробив, отбелязан е или е предположен

ХОСТ-БАЗИРАНИ IDS

- Хост-базираната IDS система използва данни за анализ, произхождащи от компютри (хостове), като журнали на приложения и системни събития;
- Източниците на данни в хост включват журналите на събития в операционната система и журналите на приложения;
- Журналите на събития от тези машини осигуряват информация относно достъпа до файлове и използването на програми от упълномощени потребители;
- Цената на разгръщането на хост-базирана IDS е по-висока от традиционната мрежова IDS;
- Целеви агент - малка програма, работеща на системата (обикновено във фонов режим), която извършва дейности като: прихващане на TCP/IP пакети от мрежата, обработване на данни от журнали на събития, централизиране на необработени данни от журнали, проверка на целостта на файловете, проверка на системната конфигурация, откриване на злоупотреби, препращане на аларми (предупреждения) и изпълняване на реакции локално в целевата машина

Архитектура на хост-базираните IDS

базирани са на разпределени целеви агенти (target agent)

централизирана

Журналът на събитията се изпраща на централно място (на машина, различна от хост), преди да бъде анализиран

разпределена

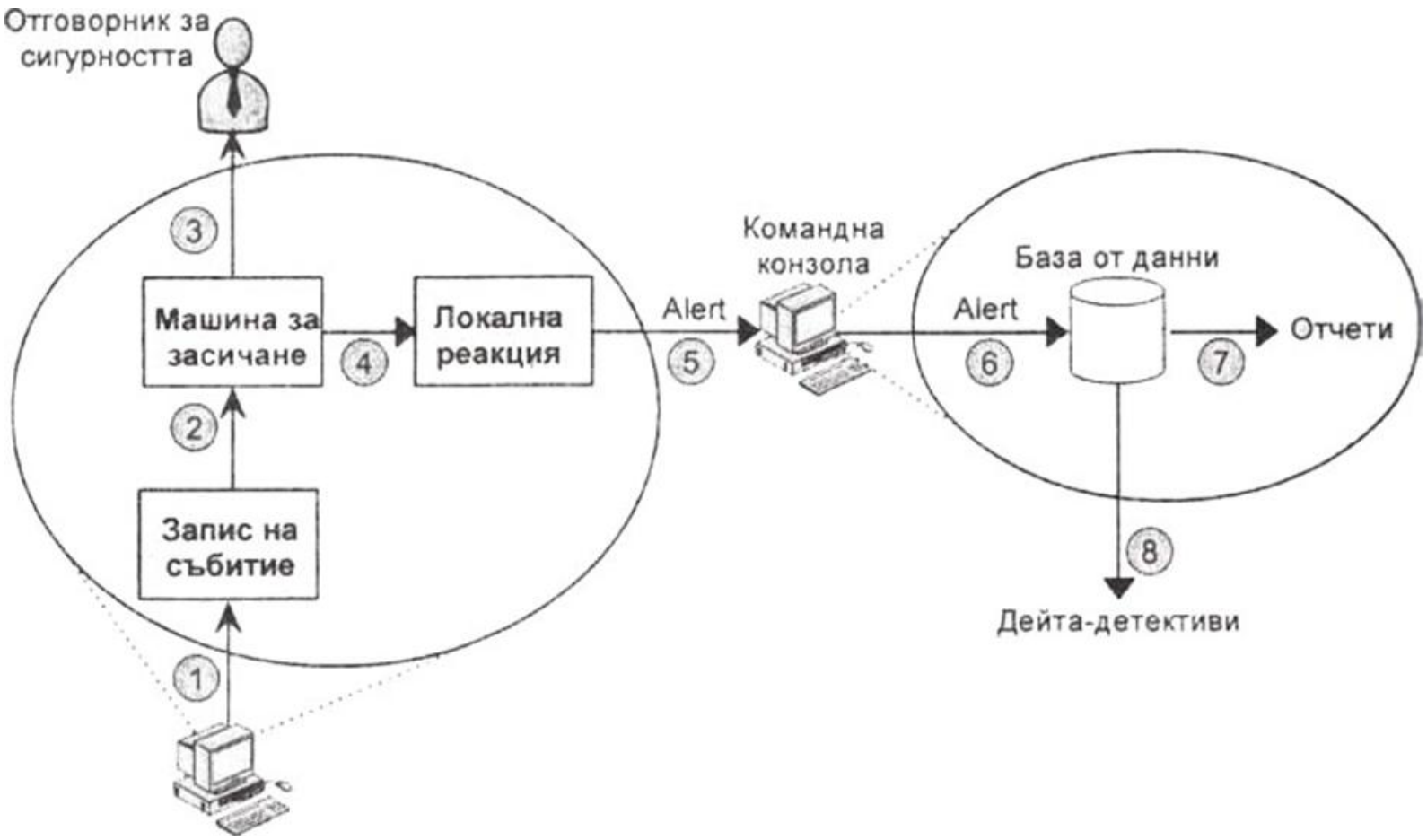
суровият журнал на събитията се анализира на машината на целевия агент

ЦЕНТРАЛИЗИРАНА ХОСТ-БАЗИРАНА АРХИТЕКТУРА

- създава малко или никакво натоварване на системата;
- Целевият агент изпраща файла на централизираната командна конзола в предварително указани времеви интервали през сигурен комуникационен канал;
- Недостатък - липса на засичания и генериране на реакции в реално време;
- Генерира се мрежов трафик, докато данните се централизират на конзолата.

РАЗПРЕДЕЛЕНА АРХИТЕКТУРА В РЕАЛНО ВРЕМЕ

- Аларми в реално време;
- Реакции в реално време;
- Може да има отражение върху производителността на системата;
- Няма статистика на поведението;
- Не е възможно сравняване на няколко сигнатури
- Няма поддръжка на архиви със сурови данни

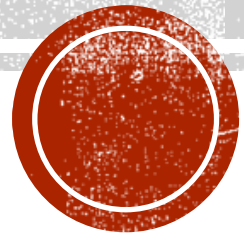


Работни режима на хост-базираните IDS

четири работни режима

- **с предупреждения (tip-off режим)**
  - открива мрежов пробив по времето на случването му и предупреждава за него
- **наблюдение (surveillance режим)**
  - surveillance се предприема, когато вече е имало пробив, отбелязан е или е предположен
- **оценка на щетите**
  - включва идентифициране на степента на вредата, причинена от злоупотребата
- **потвърждение**
  - Че потребителите следват политиките по сигурността

КРИПТОГРАФИЯ



КАКВО Е КРИПТОГРАФИЯ?

- механизъм, който защитава информацията чрез криптиране (шифриране) и декриптиране (дешифриране) на съобщения с таен код или шифър;
- Формули на криптографията:
  - за шифриране $C = E_к(P)$,
  - за дешифриране $D_k(E_k(P)) = P$, E и D са математически функции, чист текст P, шифриран текст C, ключ к

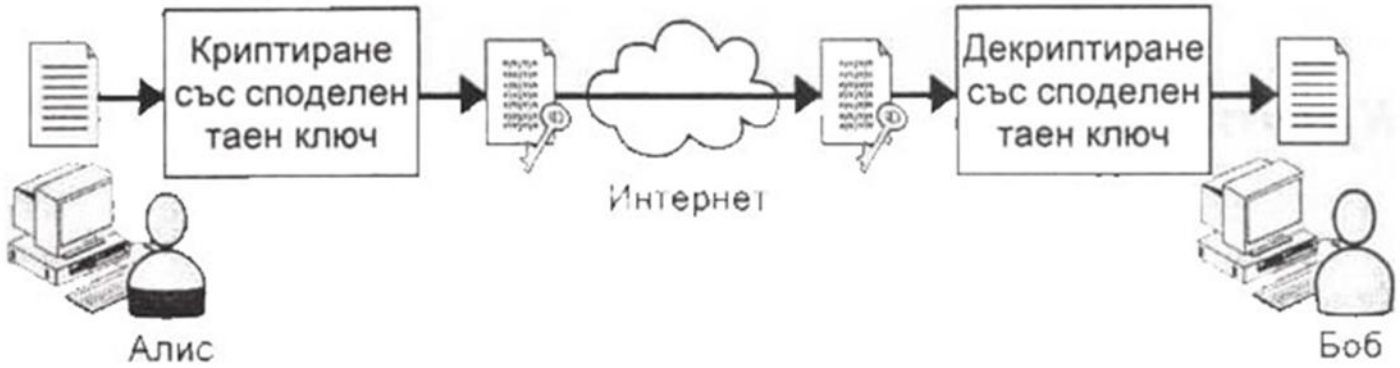
Видове криптиране

- със симетричен ключ
- с несиметричен ключ

КРИПТИРАНЕ СЪС СИМЕТРИЧЕН КЛЮЧ

- използва един и същ ключ за криптиране н декриптиране на съобщението;
- Споделянето на ключа се извършва по сигурен и таен начин, за да се поддържа поверителността;
- Наричан още механизъм за криптиране с таен ключ;
- Протоколите на сигурността използват симетрични ключове като сесийни ключове за поддържане на поверителността на съобщения в онлайн комуникация

- Например, протоколите Transport Layer Security (TLS) и Internet Protocol Security (IPSec) използват механизма на симетричния ключ, за да генерират сесийни ключове със стандартни алгоритми за криптиране и декриптиране на съобщения.
- Всяка сесия поддържа различен сесиен ключ и тези ключове се подновяват на определени интервали.

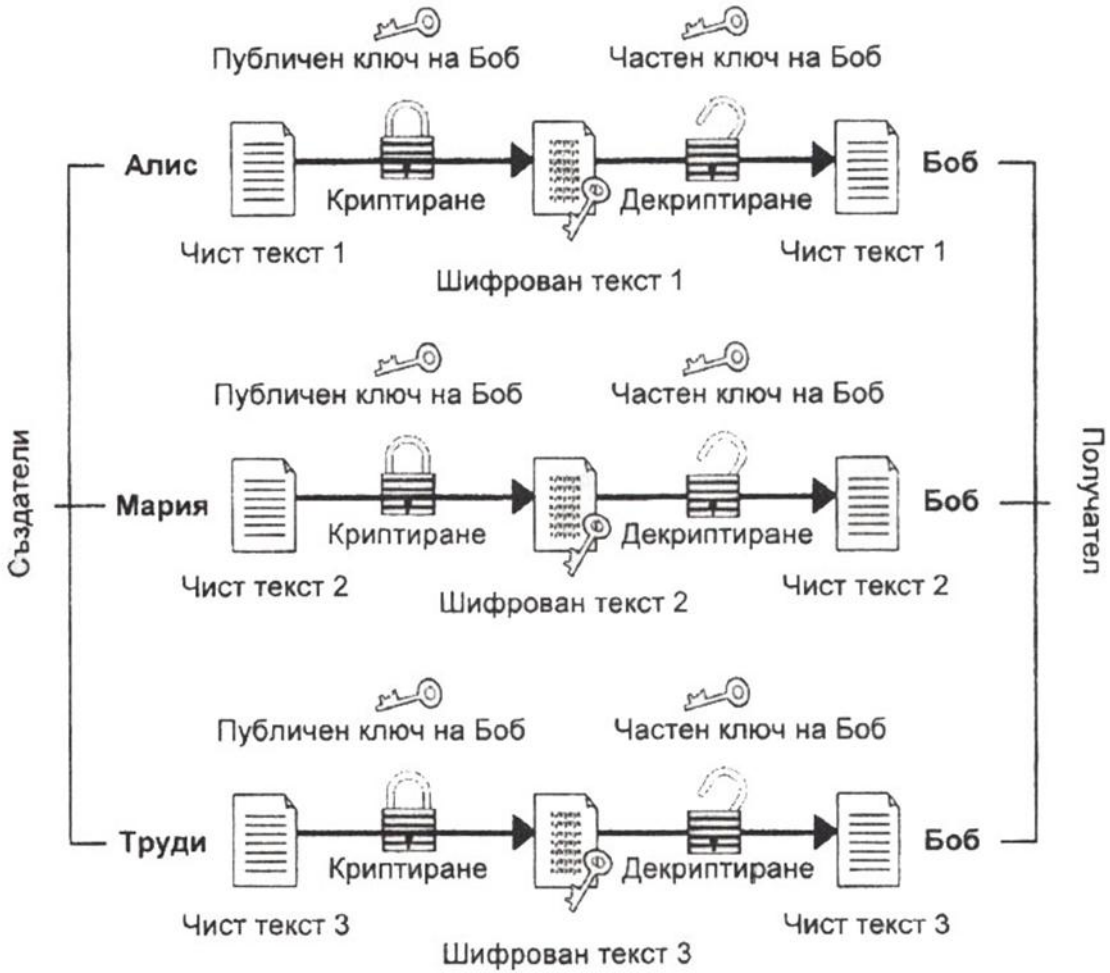


НЕДОСТАТЪЦИ НА КРИПТИРАНЕТО СЪС СИМЕТРИЧЕН КЛЮЧ

- Ключът трябва да се споделя между страните, които искат да взаимодействат. Това може да отслаби сигурността, тъй като повече от един човек знае за ключа.
- Процесът на споделяне на ключа включва риска от пресрещане на ключа по мрежата от трето лице.
- Рискът се повтаря всеки път, когато ключът се променя или между страните.

КРИПТИРАНЕ С НЕСИМЕТРИЧЕН КЛЮЧ

- криптирането с несиметричен ключ използва различни ключове за криптиране и декриптиране на съобщението;
- Изисква два ключа: публичен ключ и частен ключ;
- Наричано още криптиране с публичен ключ;
- Частният ключ е известен само на собственика.
- Публичният ключ се споделя и е достъпен за всички страни, които биха искали да взаимодействат със собственика на частния ключ.



КРИПТИРАНЕ С НЕСИМЕТРИЧЕН КЛЮЧ

- Криптиране на симетричните тайни ключове, за да ги защити по време на обмена им по мрежата или докато се използват, съхраняват или хешират в системи.
- Създаване на цифрови подписи, които предоставят автентикация и признаване за ресурси и цялостност на данни за електронни документи и съобщения.
- Пример - RSA криптирането с публичен ключ

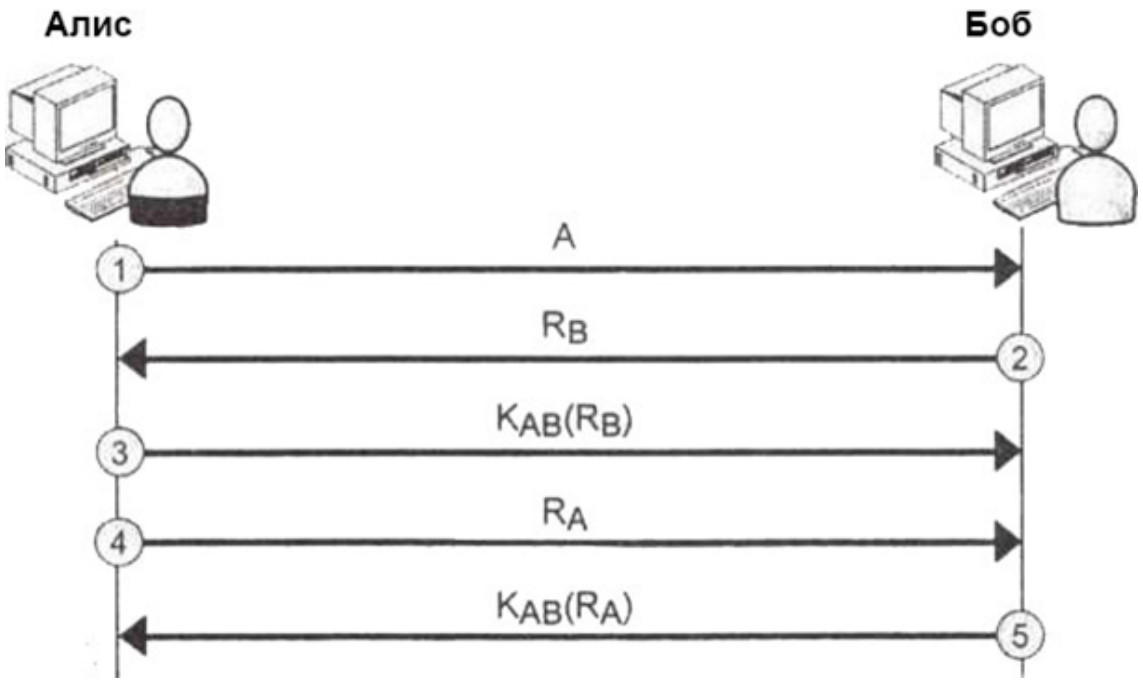
КРИПТИРАНЕ

- Криптирането със симетричен ключ е от 100 до 1000 пъти по-бързо и натоварва процесорите по-малко;
- при криптирането с несиметричен ключ се използват по-тежки алгоритми в сравнение с криптирането със симетричен ключ;
- Алгоритмите, използвани в криптирането с публичен ключ, включват сложни математически функции, които подсигуряват, че веднъж изпълнен, процесът криптиране не може да се обърне лесно;
- Съобщението, криптирано с публичен ключ, може да се декриптира само със съответния му частен ключ и обратно;
- Ключовете са генерирани по такъв начин, че не е възможно да определите единия ключ, дори и да знаете другия.


Механизми за автентикация
Challenge-response протоколи
KDC механизъм за автентикация
Kerberos
Цифрови подписи

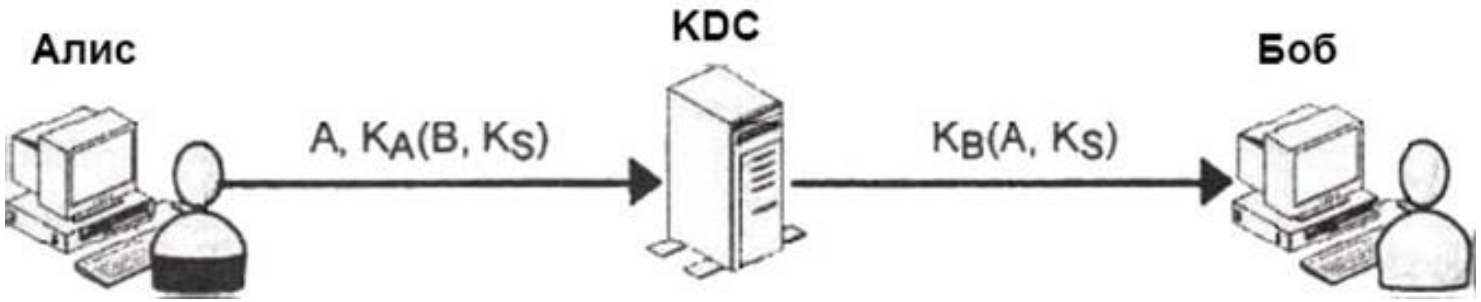
CHALLENGE-RESPONSE ПРОТОКОЛИ

Challenge-response протоколите се базират на принципа, че едната страна изпраща произволно число като предизвикателство (challenge) до другата, която го обръща в специално число и връща резултата.



KDC МЕХАНИЗЪМ ЗА АВТЕНТИКАЦИЯ

Друг възприет подход е използването на доверен център за разпределение на ключове (key distribution center, KDC). При този метод всеки потребител съхранява своя ключ в KDC. KDC е отговорен за автентикацията и управлението на сесийни ключове.



wide- mouth frog протокол

KERBEROS V5

- Kerberos е протокол за автентикация, който позволява на потребителите, взаимодействащи по мрежа, да удостоверят самоличността си.
- Системи, инсталирани с Kerberos, изискват потребителят да напише паролата си само веднъж.
- Kerberos разделя мрежата на домейни на сигурност, наречени области. Могат да се поддържат различни нива на сигурност с различни политики на сигурността за различните отдели на организацията. Една област може да приема автентикация от другите области, ако политиката на сигурността, дефинирана в нея, го позволява и обратно.
- Политиките, дефинирани в Kerberos, са йерархични. Йерархичната структура позволява дъщерните области, които нямат права за директна проверка на автентичност, да споделят информация за автентикацията с родителските области.

КОМПОНЕНТИ, ВКЛЮЧЕНИ В KERBEROS V5

- *Удостоверяващ сървър* (**Authentication server – AS**) - услуга за автентикация. Проверява автентичността на потребителите по време на регистрация.
- Използва услугите на доверена трета страна, наречена Център за дистрибуция на ключове (key distribution center -KDC) за генериране на сесиен ключ. Той споделя постоянен таен ключ за всяка основна единица (потребители и услуги в мрежата). KDC също се нарича *база от данни на Kerberos*;
- *Гарантиращ билетен сървър* (**Ticket-granting server – TGS**) - услуга за издаване на билети. Издава билети, които са доказателство за самоличност. Билетите са криптирани записи, съдържащи сесийния ключ, самоличността на потребителя и идентификатора на услугата, както и IP адреса на клиента;
- *Application Server* - сървър за приложения. Предоставя услуги на клиента.

RSA ЦИФРОВИ ПОДПИСИ