Защитни стени

проф. д-р инж. Венета Алексиева

Основни моменти

- Защитни стени
- Видове защитни стени
- Допустими и недопустими архитектури на защитни стени

Предмет на защита

- Данни
  - секретност
  - цялостност
  - наличност
- Ресурси
  - компютърни системи
- Репутация
  - На организацията
  - На служителите

Подходи за защита

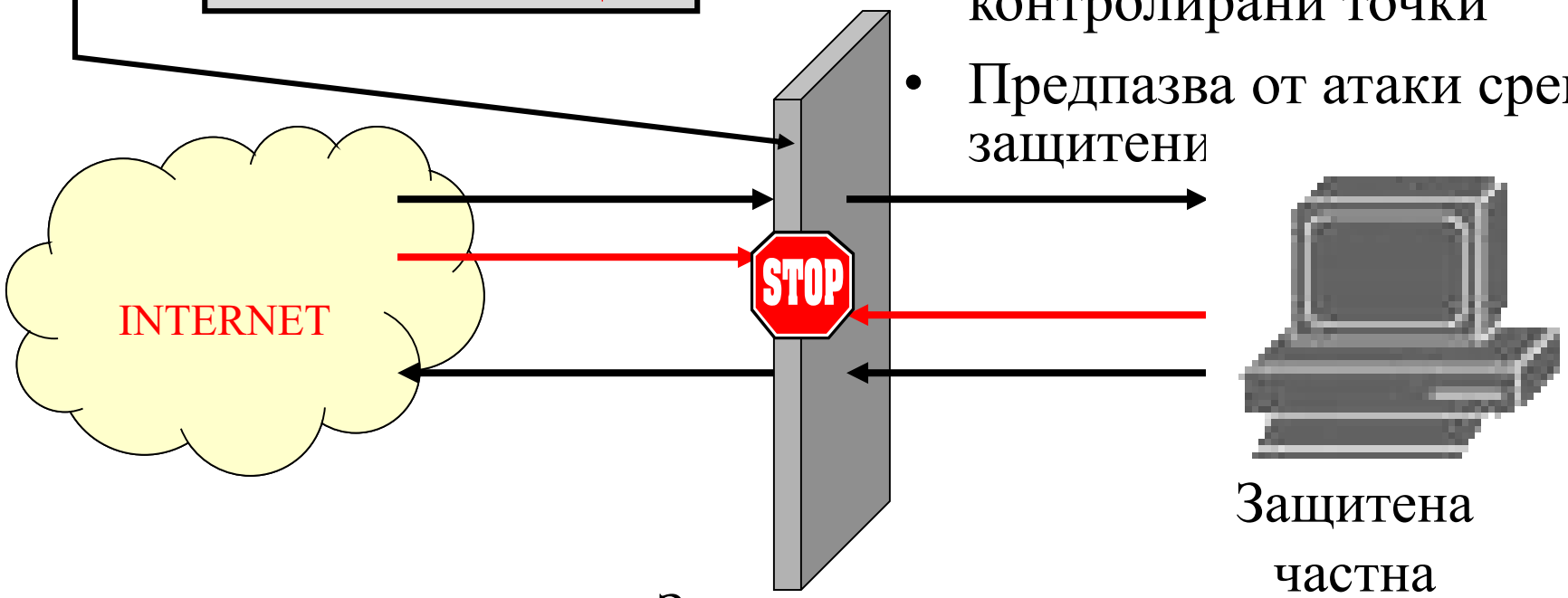
- без защита ☺
- защита, базирана на неизвестност (Security through obscurity)
- защитаване на машината
- мрежова защита

Защитна стена

Определяне на правила за достъп

Кой ? Кога ?
Как ? Защо?

- Множество от компоненти, ограничаващи достъпа до Интернет или до други части на мрежата
- Ограничава входа и изхода на трафика в контролирани точки
- Предпазва от атаки срещу защитени

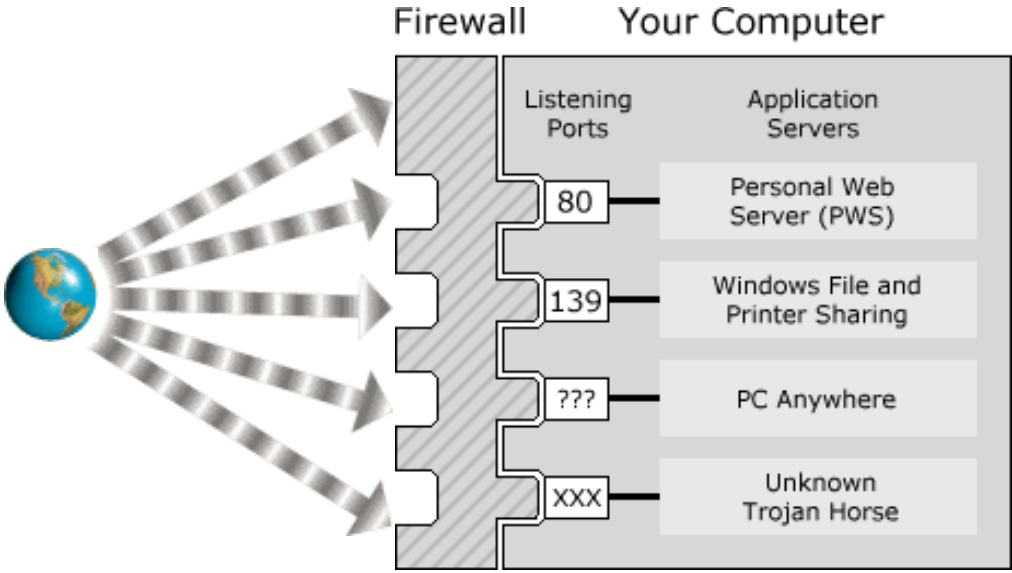


Защитена частна мрежа

Защитна стена

Нива от OSI-модела, в които работят защитните стени

- Приложно (слой 7)
- Транспортно (слой 4)
- Мрежово (слой 3)
- Канално (слой 2)



Функции на защитните стени

Защитната стена може:

- Да концентрира в една точка определянето на сигурността
- Да подсилва политиката на сигурност
- Да съхранява информация за Интернет трафика
- Да предотвратява разпространението на проблеми

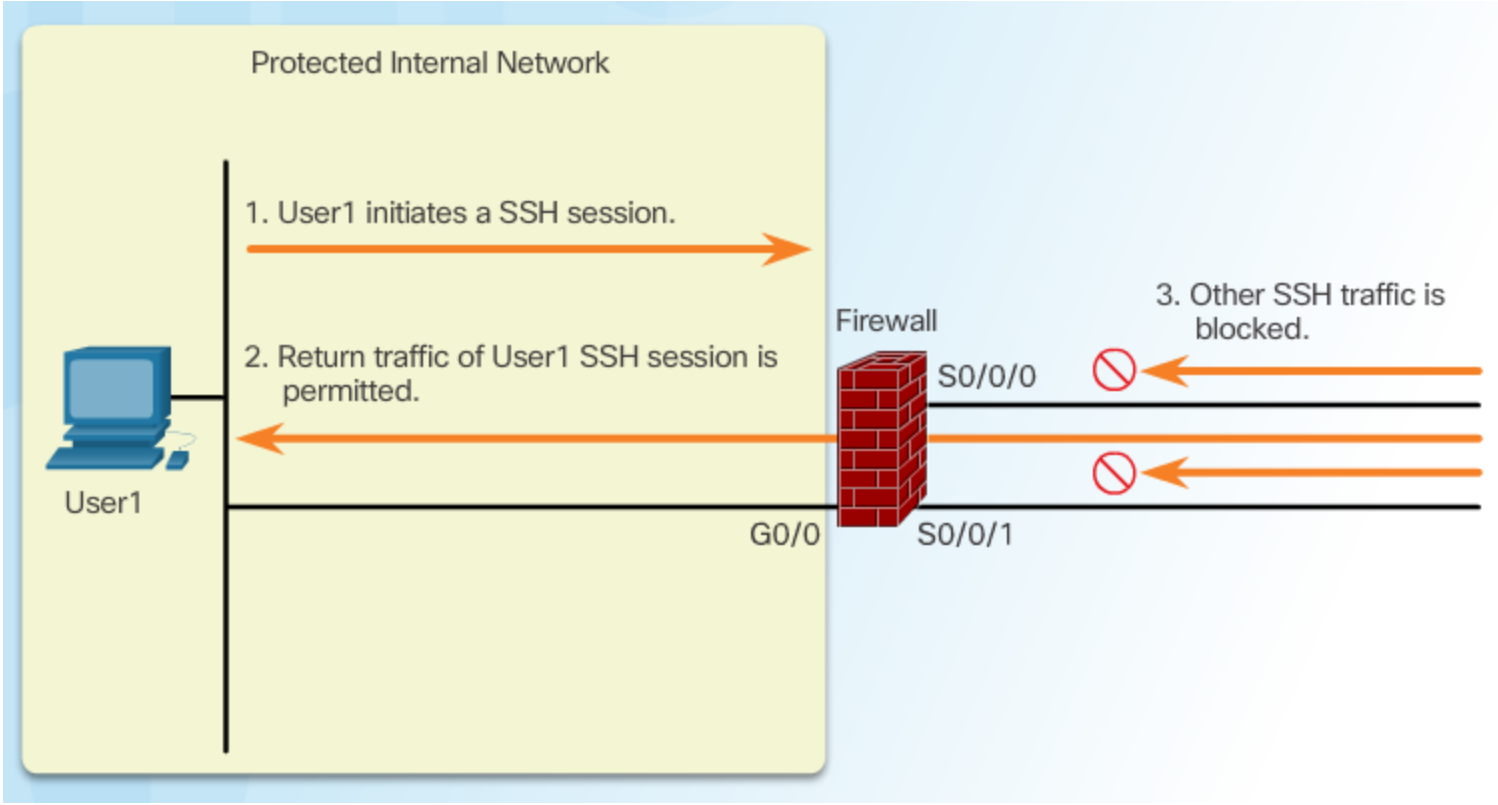
Защитната стена не може:

- Да предпази от вътрешни недоброжелатели
- Да защити от конекции, които не минават през нея
- Да предпази от най-последните заплахи
- Да предпази от вируси

Заплахи, предотвратявани от защитните стени

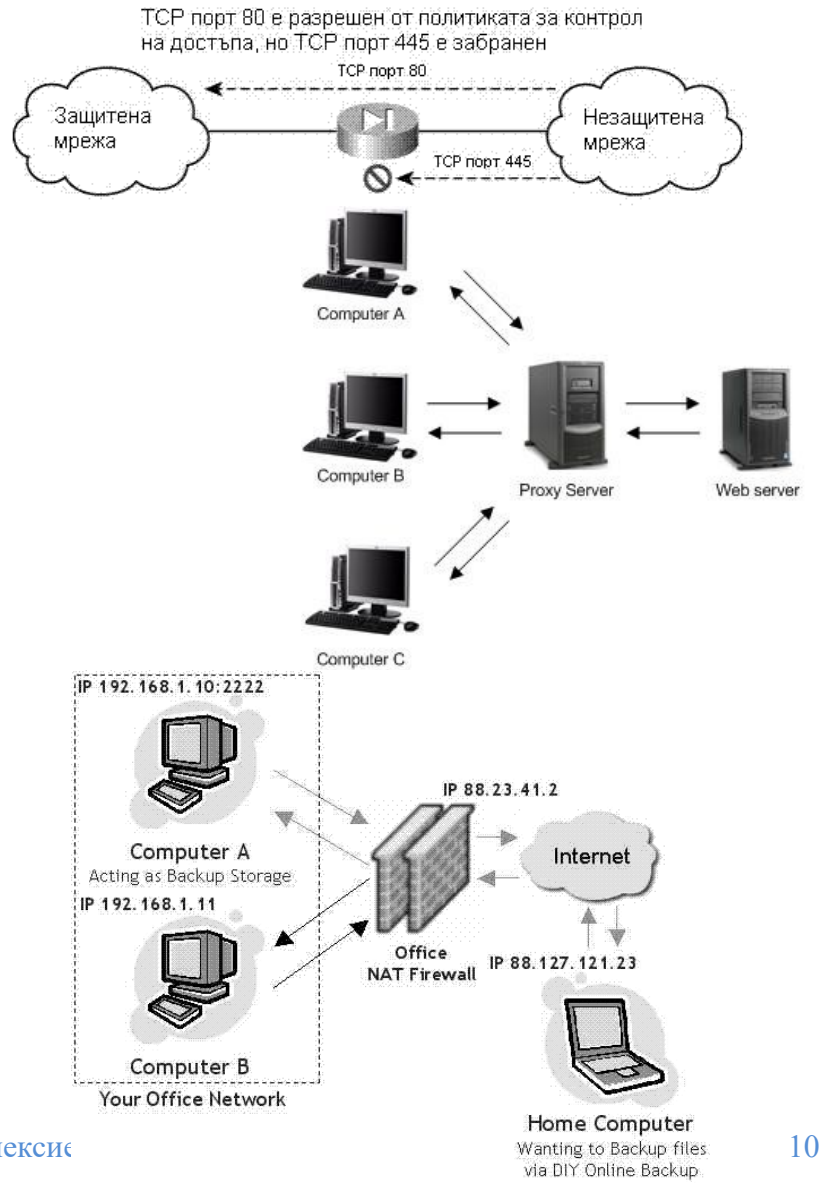
Заплаха	Цел
Remote login	отдалечено регистриране/неоторизирано
Application backdoors	слабости в кода на използваните приложения
Operating system bugs	слаби места в кода на ОС
Denial of service	отказ на достъпа до услуга от претоварване
SPAMs	спам
Trojans	троянски коне
FTP brute force	атака на грубата сила
Phishing	неправомерно присвояване на пароли

Принцип на действие на защитна стена



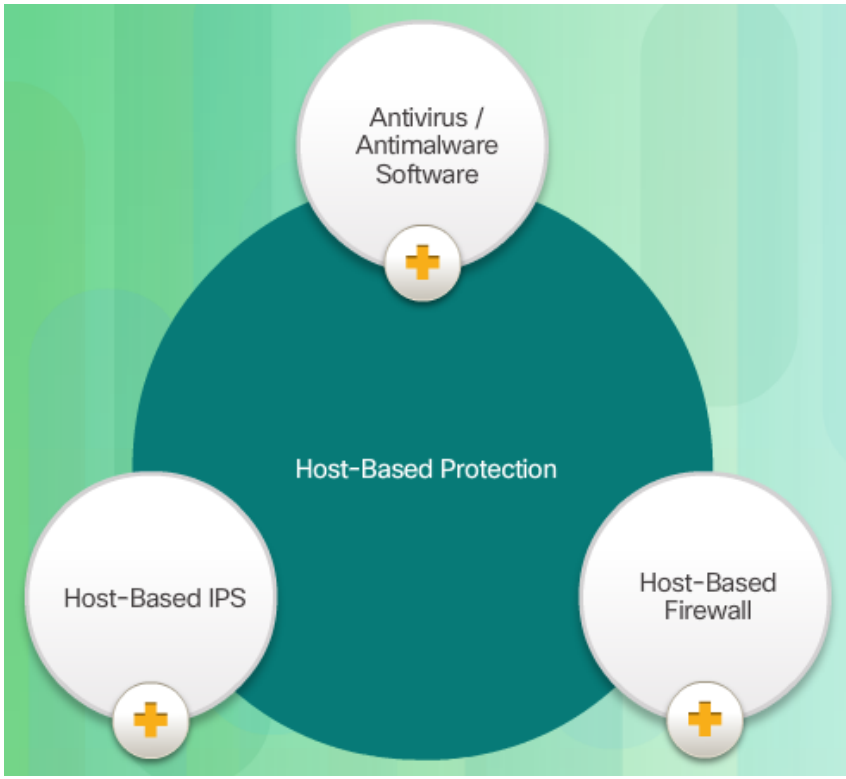
Видове защитни стени

- Хост базирани защитни стени
- Защитни стени с пакетно филтриране (появили се за пръв път към края на 80-те години на 20 век; т.нар. защитни стени от първо поколение)
- Защитни стени на приложно ниво (създадени през 1991г)
- Защитни стени от вид „proxy”
- Защитни стени с NAT (Network Address Translation)

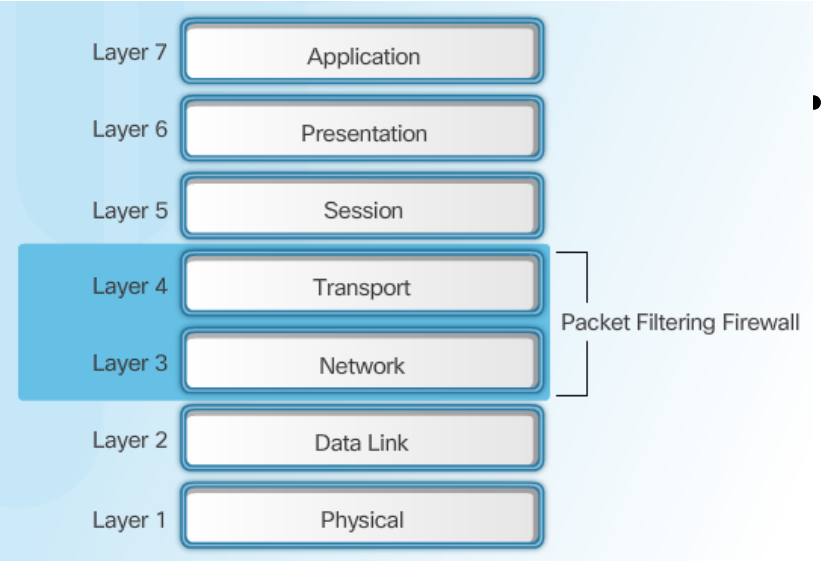


Хост базирани защитни стени

- Вътрешните сървъри могат да се защитят и не се допуска атака срещу тях, защото са зад главната защитна стена;
- Не е необходимо отделните защитни стени и подмрежи да защитават сървърите, защото за това се грижи хост-базираната защитна стена.



Защитни стени с пакетно филтриране

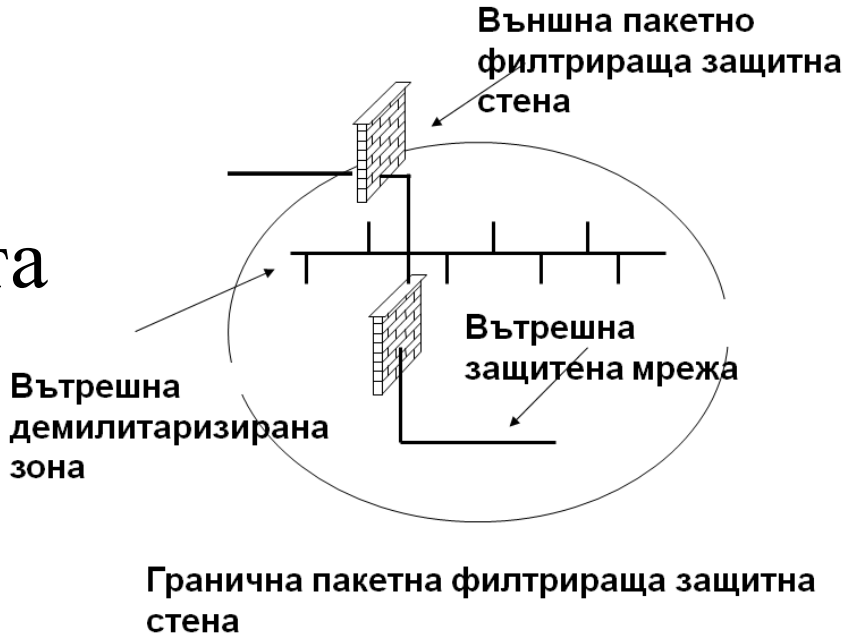


- Притежават възможности за управление и контрол на достъпа до адреси от системата и комуникационните сесии.
- Ползват информация от мрежовия и транспортния слой:
  - IP адреса на източника на пакета;
  - IP адреса на получателя на пакета;
  - типа на трафика - специфичния мрежов протокол използван за комуникация между източника и получателя;
  - характеристика от транспортния слой - порта на източника и порта на получателя.

Защитни стени с пакетно филтриране - недостатъци

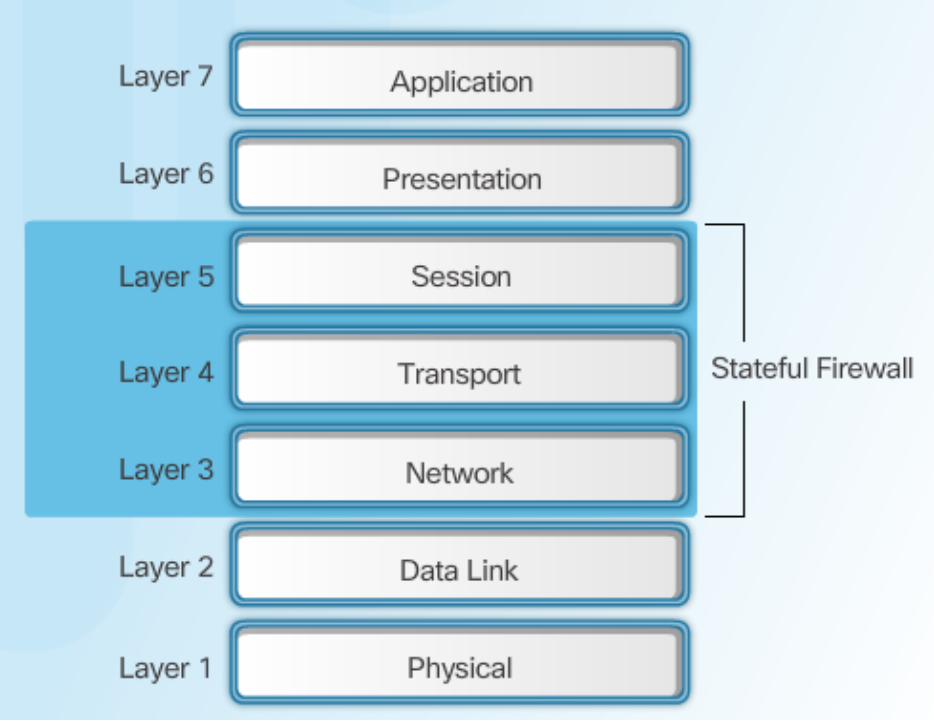
- Не се проверяват данните от по-горните слоеве на OSI модела
- Не се открива мрежов пакет, който е енкапсулиран в друг пакет от 3 слой (тунелиране).
- Податливи са към

нарушаване на сигурността поради неподходящи архитектурни решения.



Защитни стени, проверяващи състоянието

- Защитните стени с проверка на състоянието са пакетно филтриращи, към които са присъединени чувствителни данни от транспортно и сесийно ниво на OSI-модела.



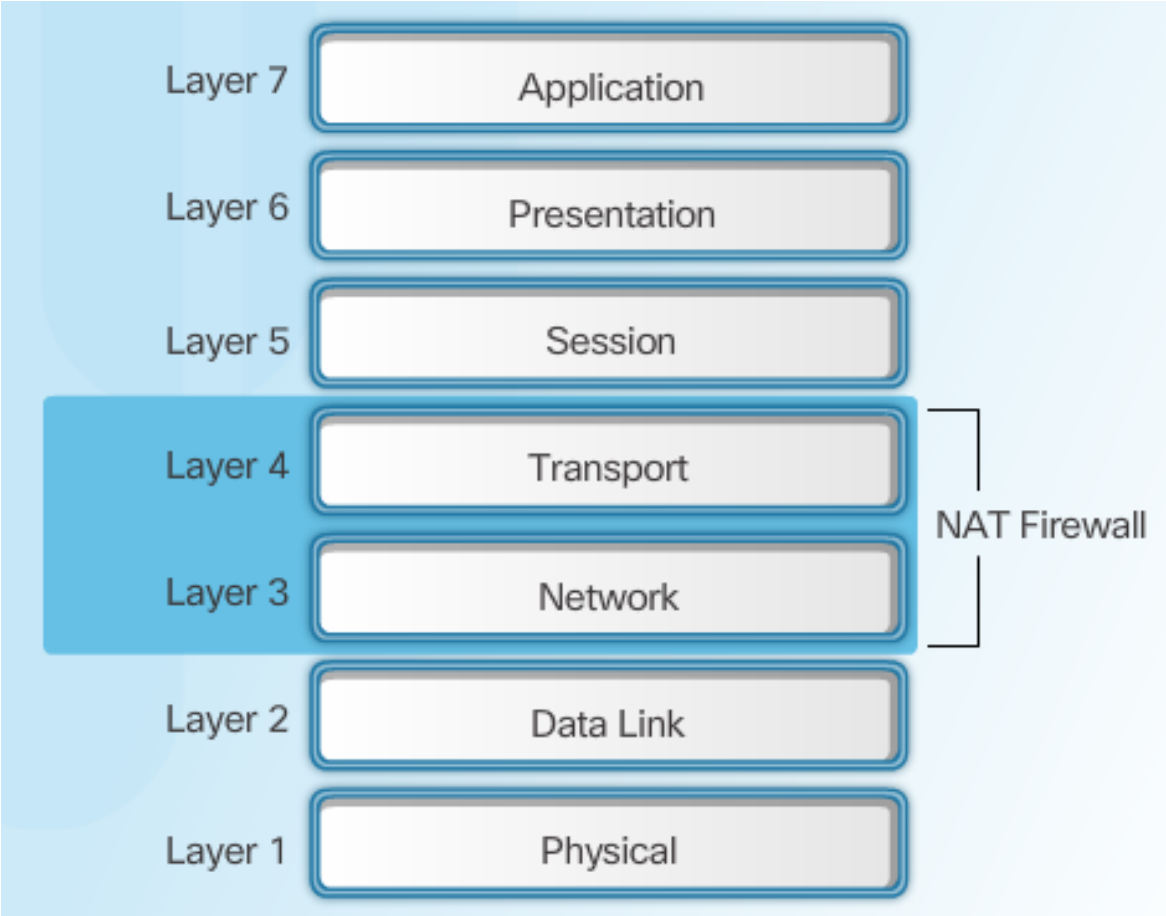
Защитни стени от вид „proxy”

- Съчетават контрола и управлението на достъпа на по-ниските нива с възможностите на приложно ниво.

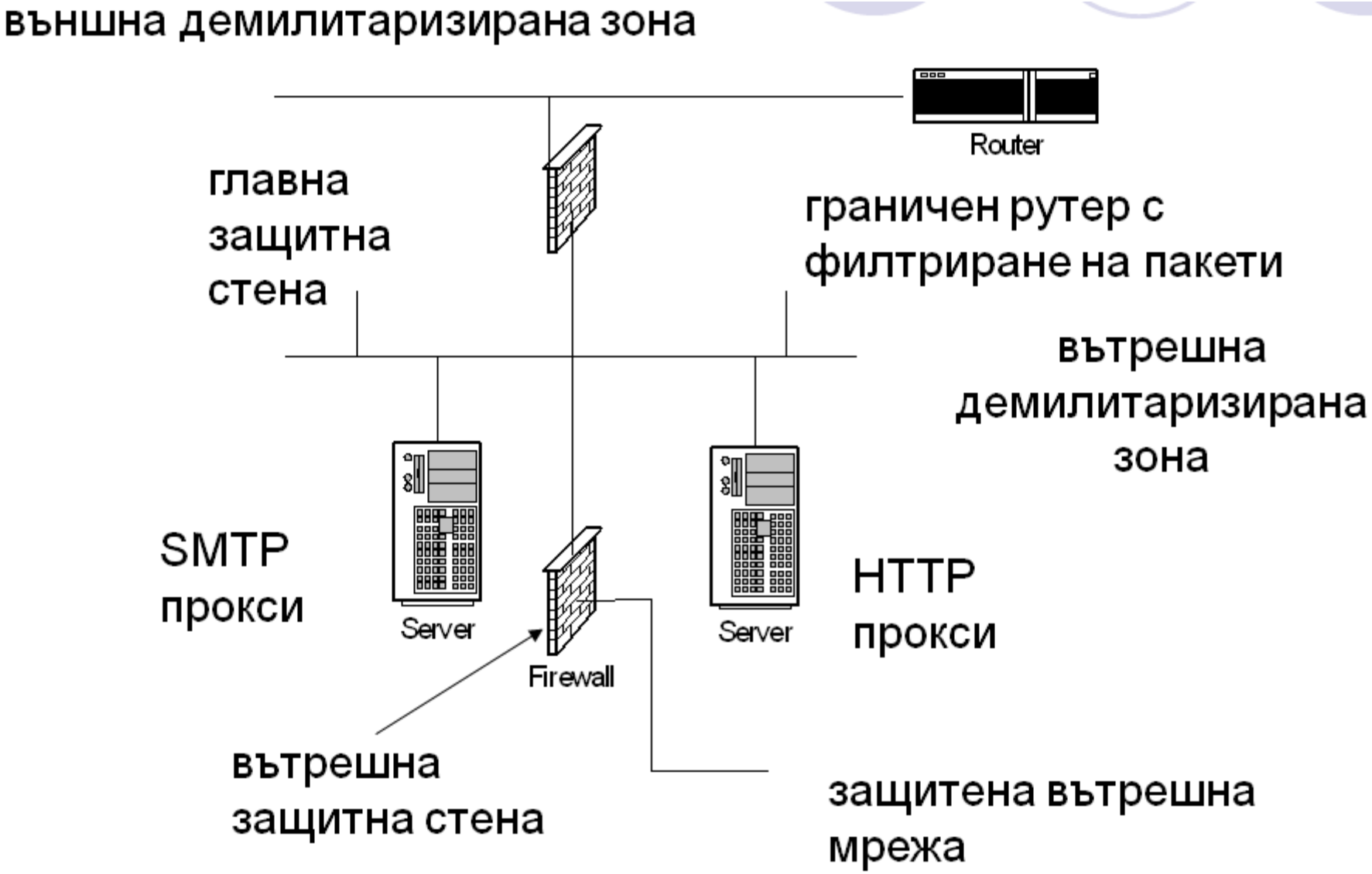
Защитни стени от вид „proxy”-предимства

- Повече възможности за външно включване през защитната стена, като се прави проверка на мрежовия адрес или порт;
- Позволява прилагане на всякакви мерки по отношение на потребителското идентифициране за оптимално използване на инфраструктурата на системата;
- Има възможност за директна автентикация на потребителите (при другите защитни стени това става чрез автентикация на мрежовия адрес на устройството, нещо което лесно може да се фалшифицира).

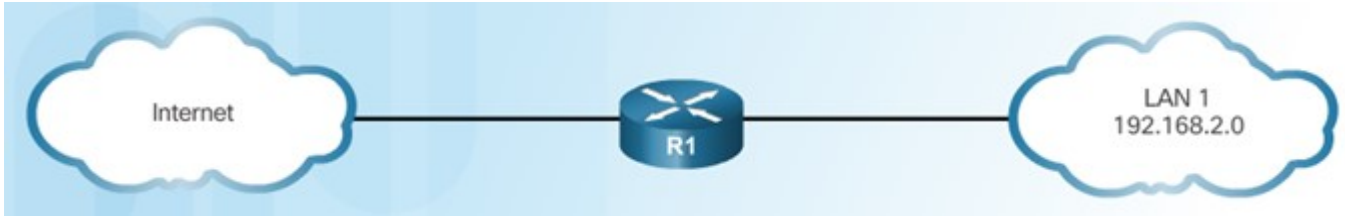
Защитни стени от тип NAT



Защитни стени за конкретни услуги

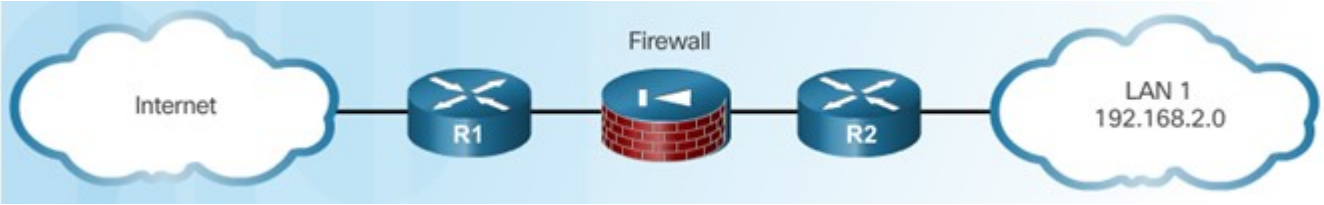


С един маршрутизатор



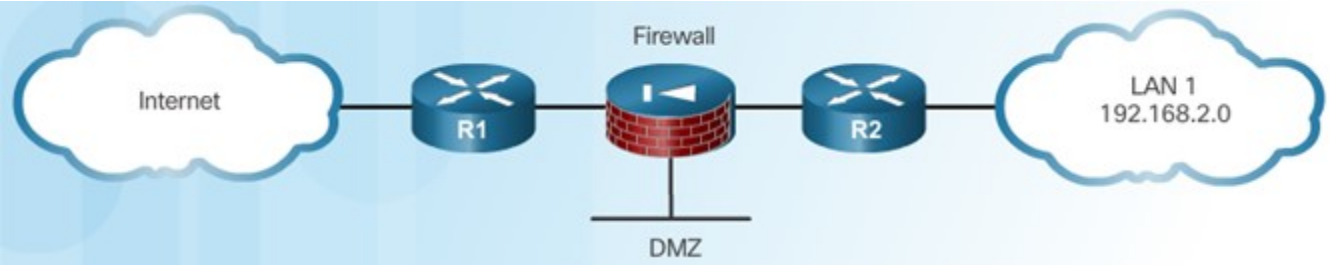
- Правила (ACLs, IPtables)
- NAT

Защита в дълбочина



- Хардуерно базирана защитна стена

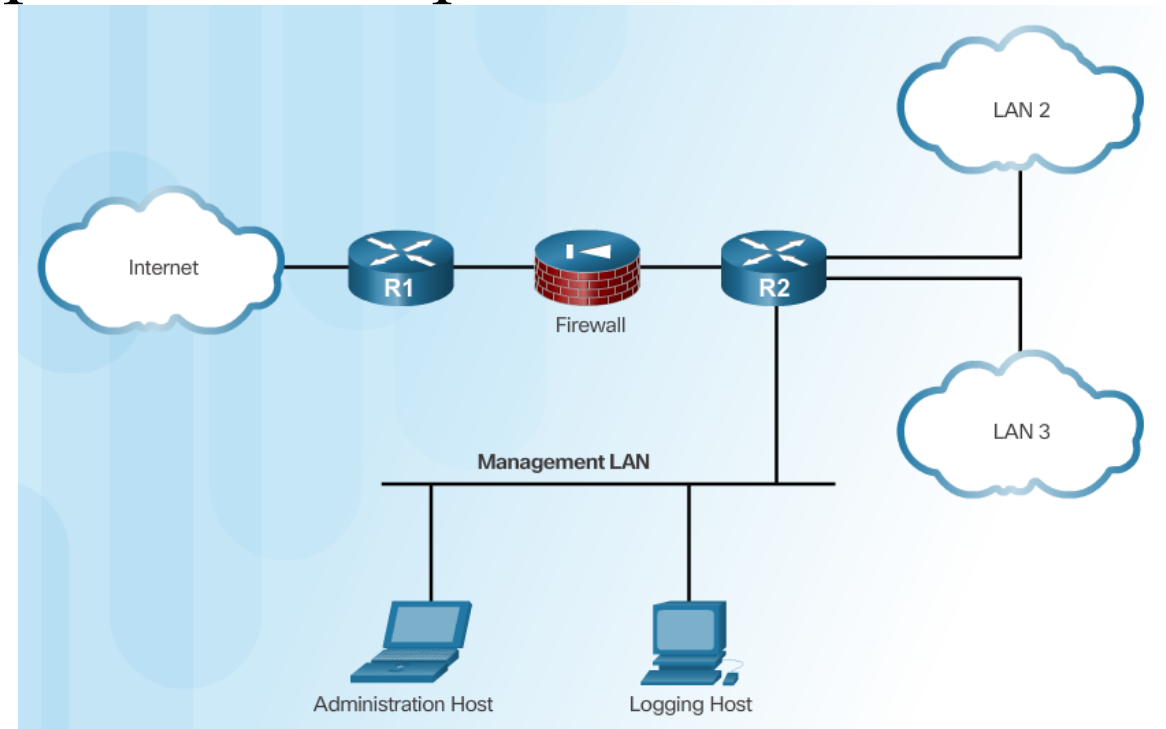
Защита с демилитаризирана зона



- DMZ- демилитаризирана зона

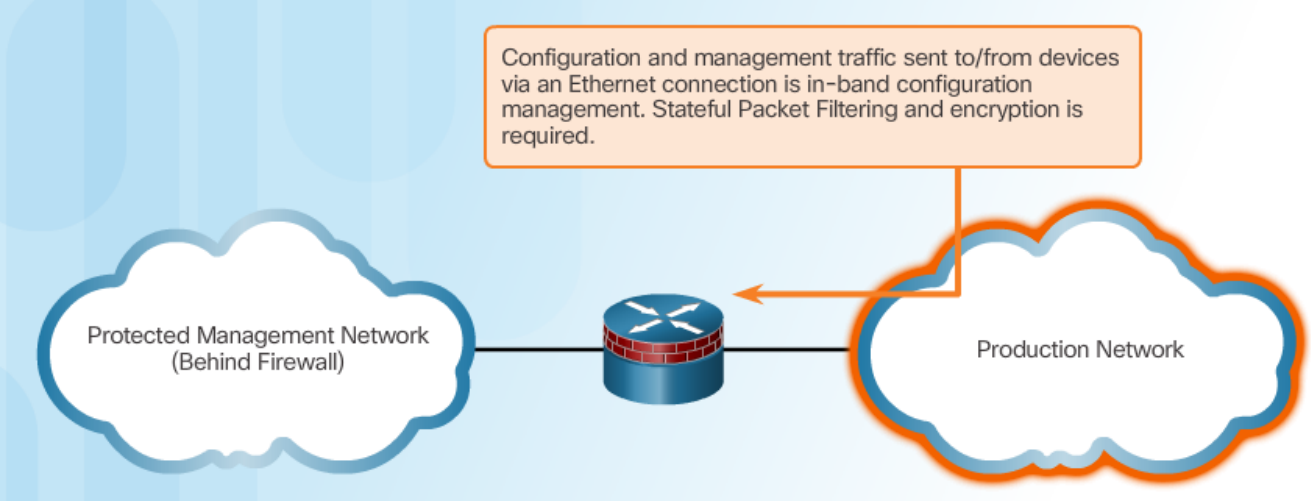
Управление от вътрешната мрежа

- Прилага се само за устройствата, които ще се управляват и наблюдават.
- Да се ползва IPsec, SSH, SSL където е възможно.
- Да се реши дали каналът за управление да е отворен цялото време.



Управление от външната мрежа

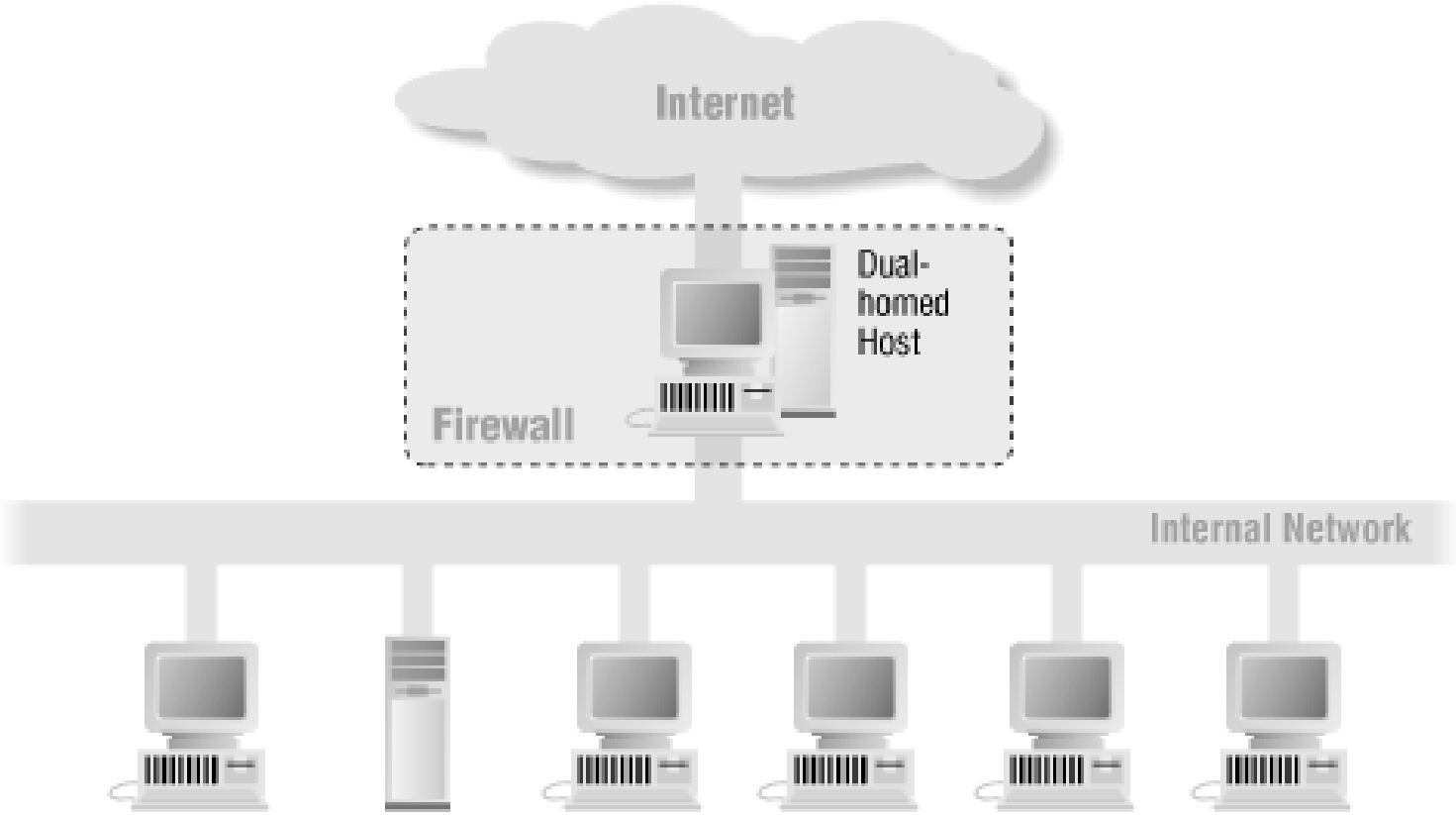
- Изисква по-високо ниво на сигурност
- Да се минимизира риска от допускане на протоколи за управление до вътрешната мрежа (production network)



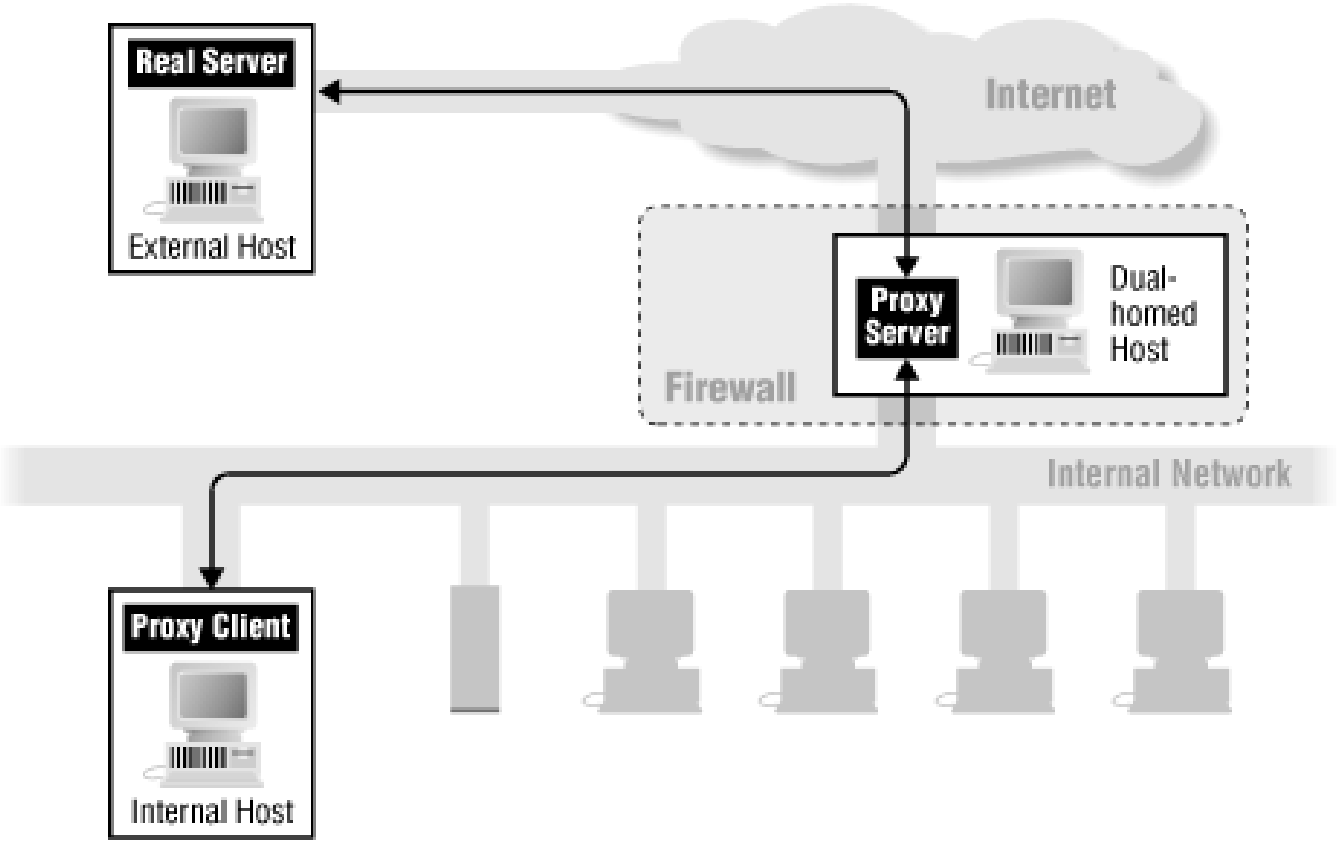
Основни понятия

- Bastion host
- Dual-homed host
- Packet filtering
- Perimeter network
- Proxy server

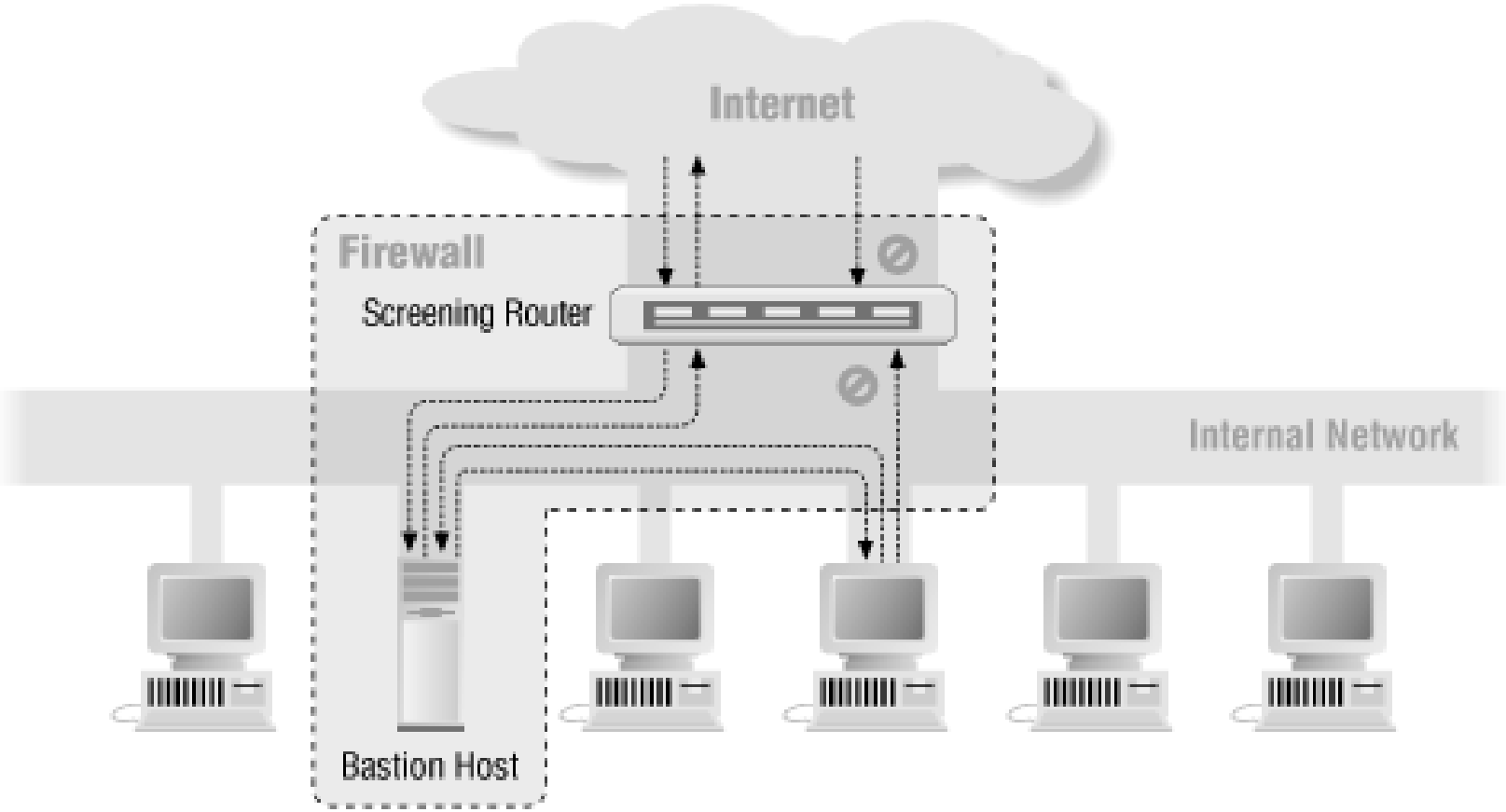
Dual-Homed host



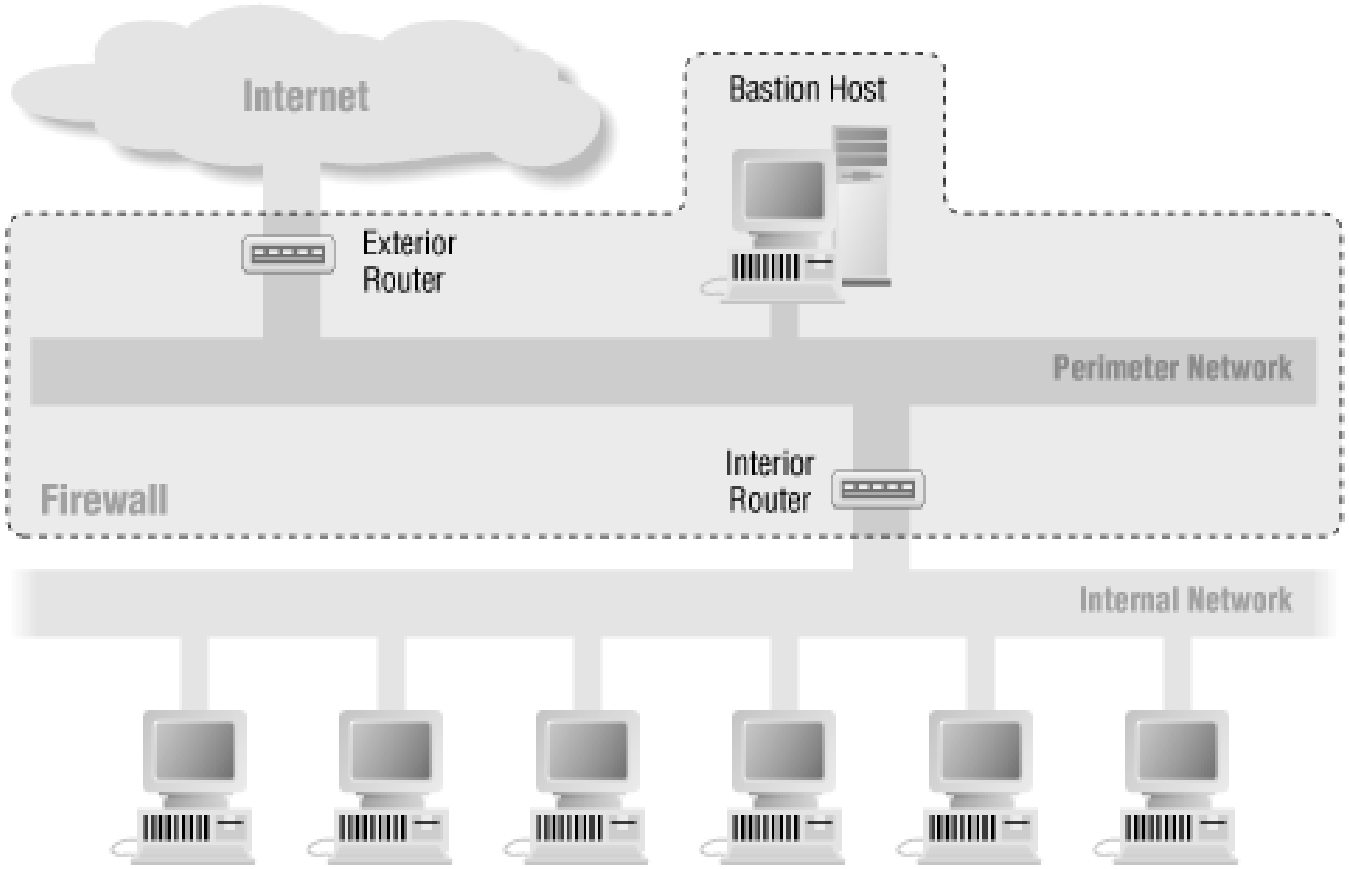
Dual-Homed Host + Proxy



Screened host

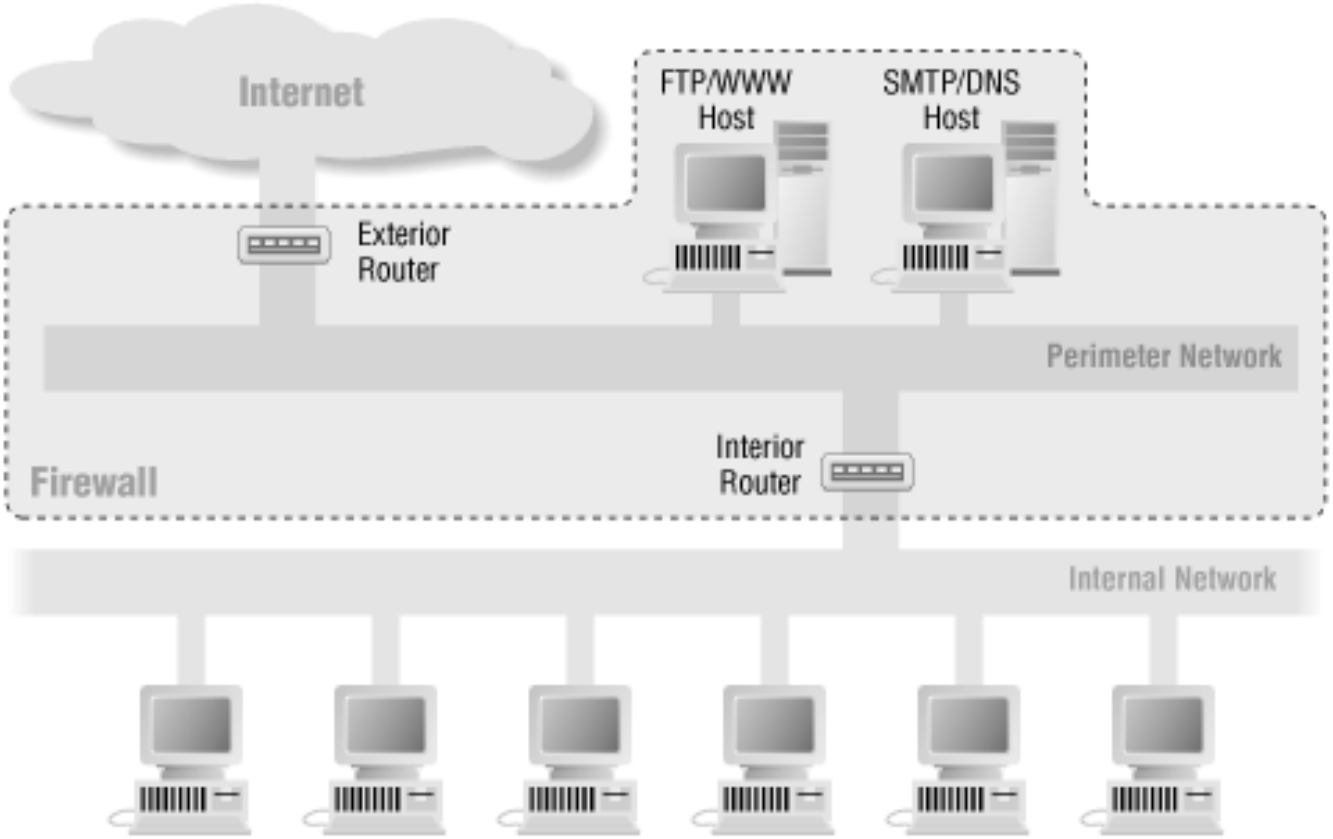


Screened subnet

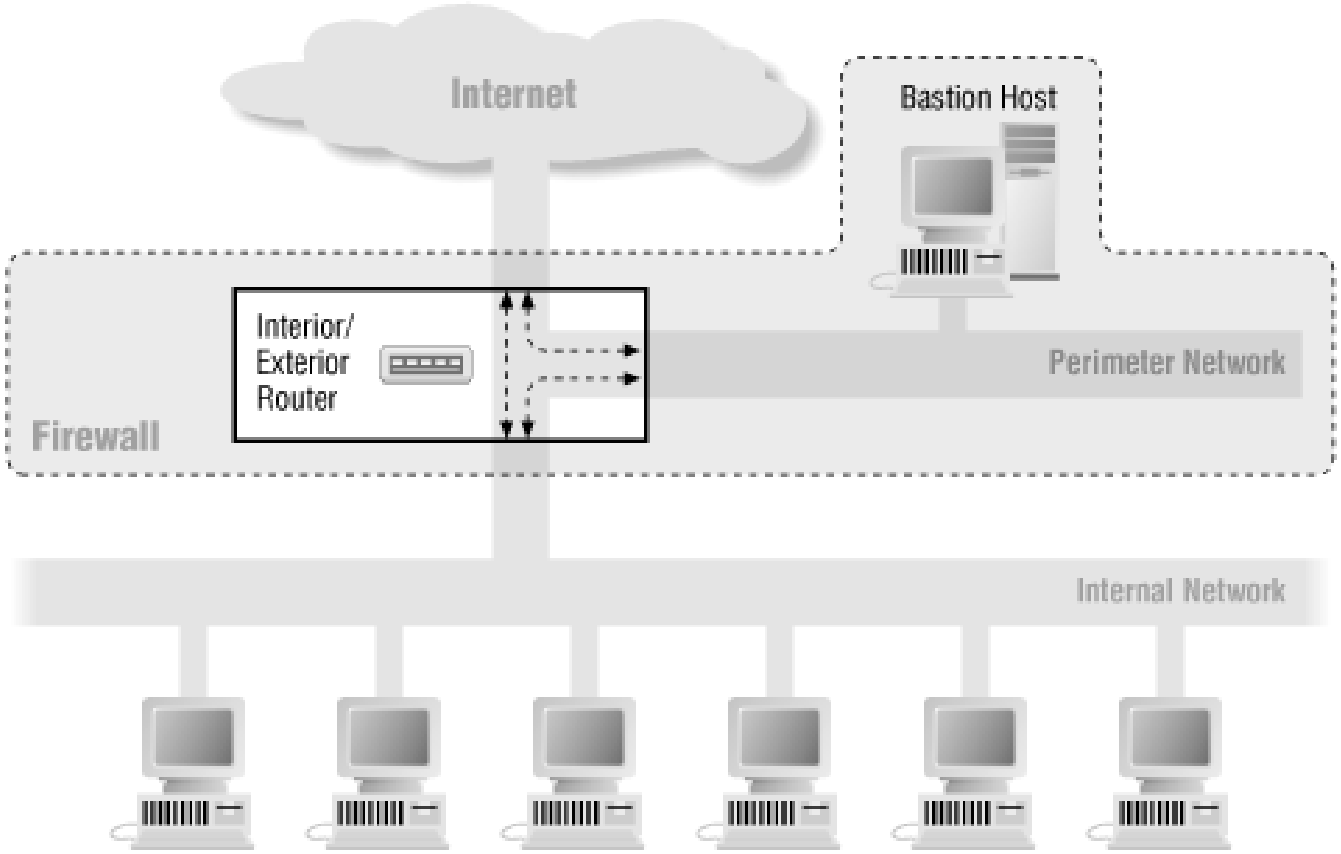


- Perimeter network (DMZ)
- Bastion host
- Вътрешен маршрутизатор
- Външен маршрутизатор

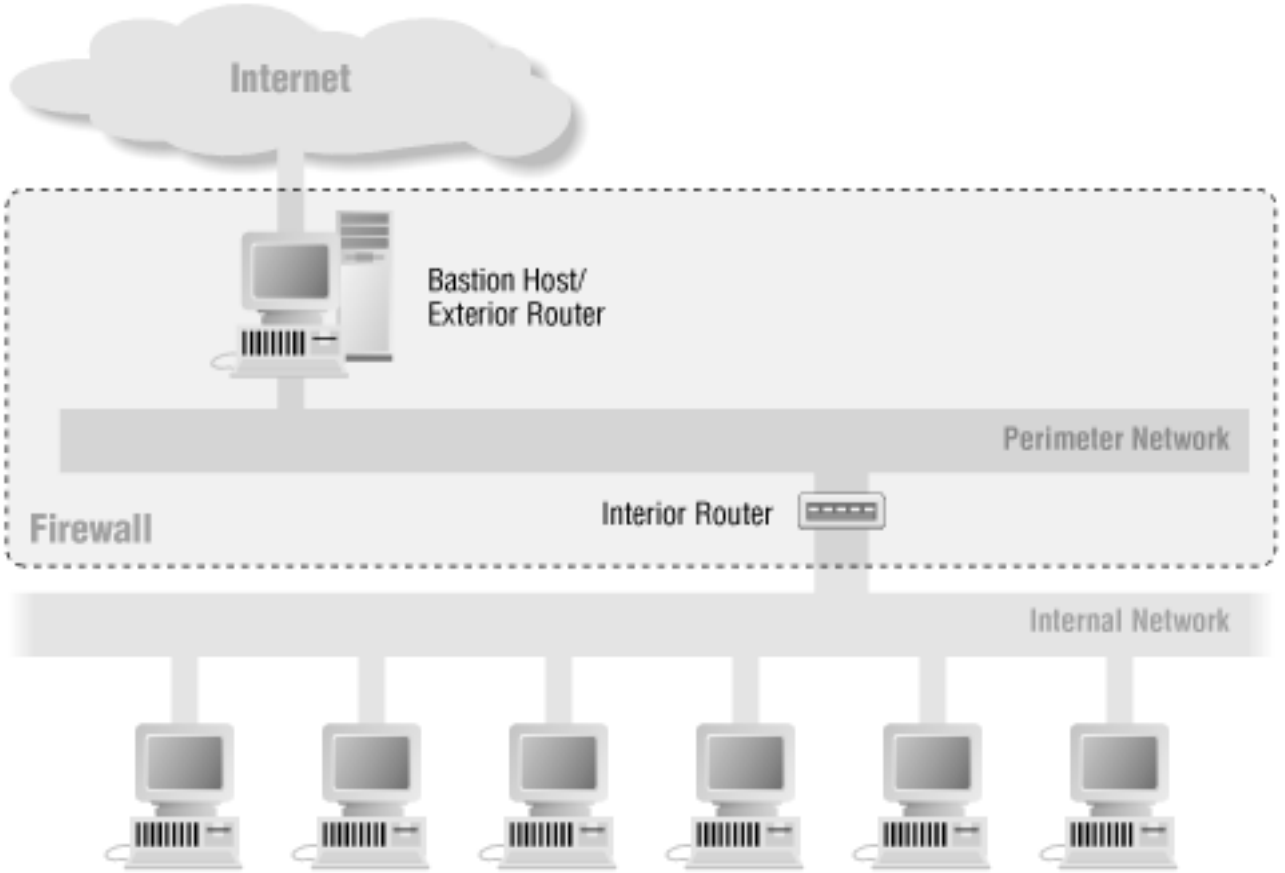
Допустими архитектурни решения – множество Bastion хостове



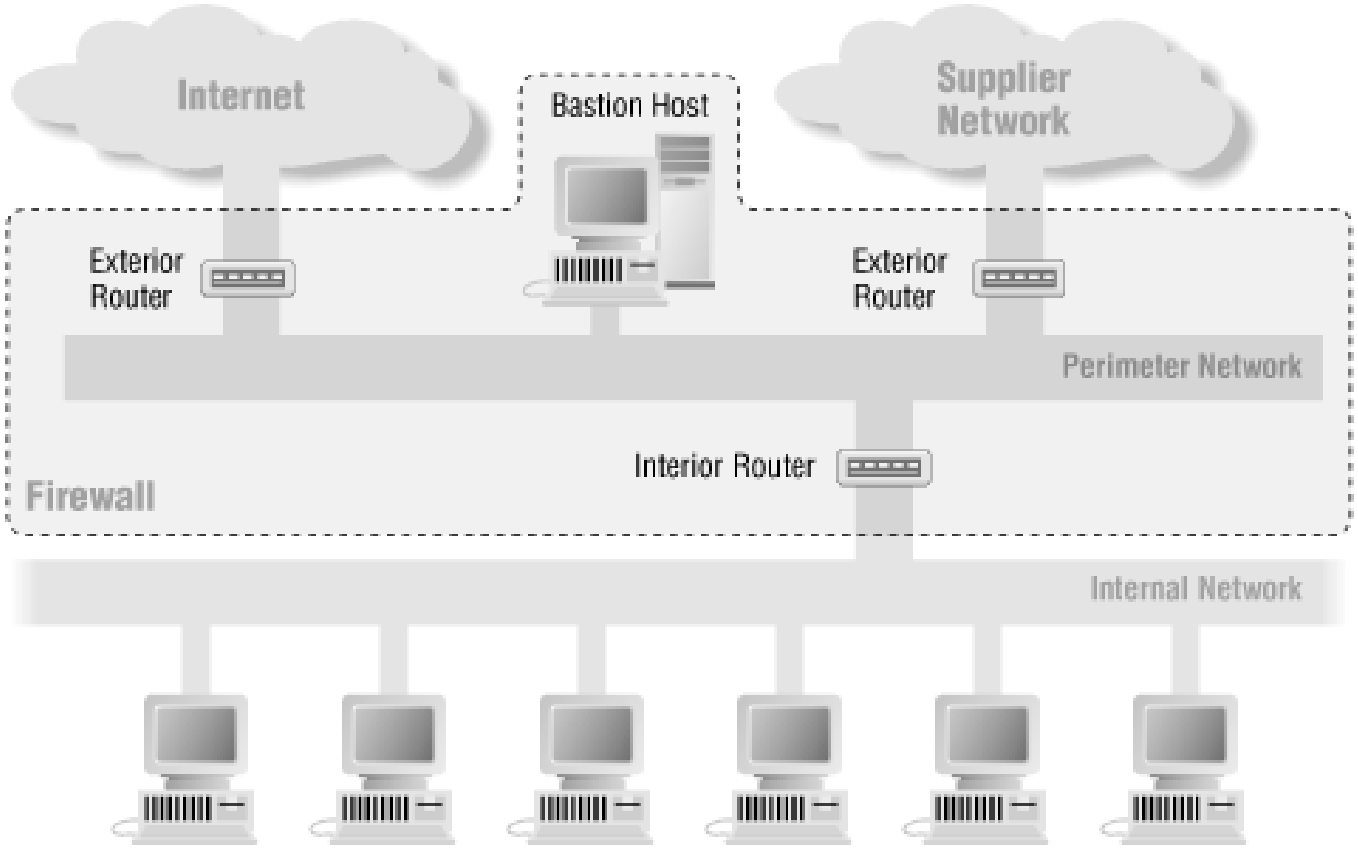
Допустими архитектурни решения – обединяване на вътрешен и външен маршрутизатор



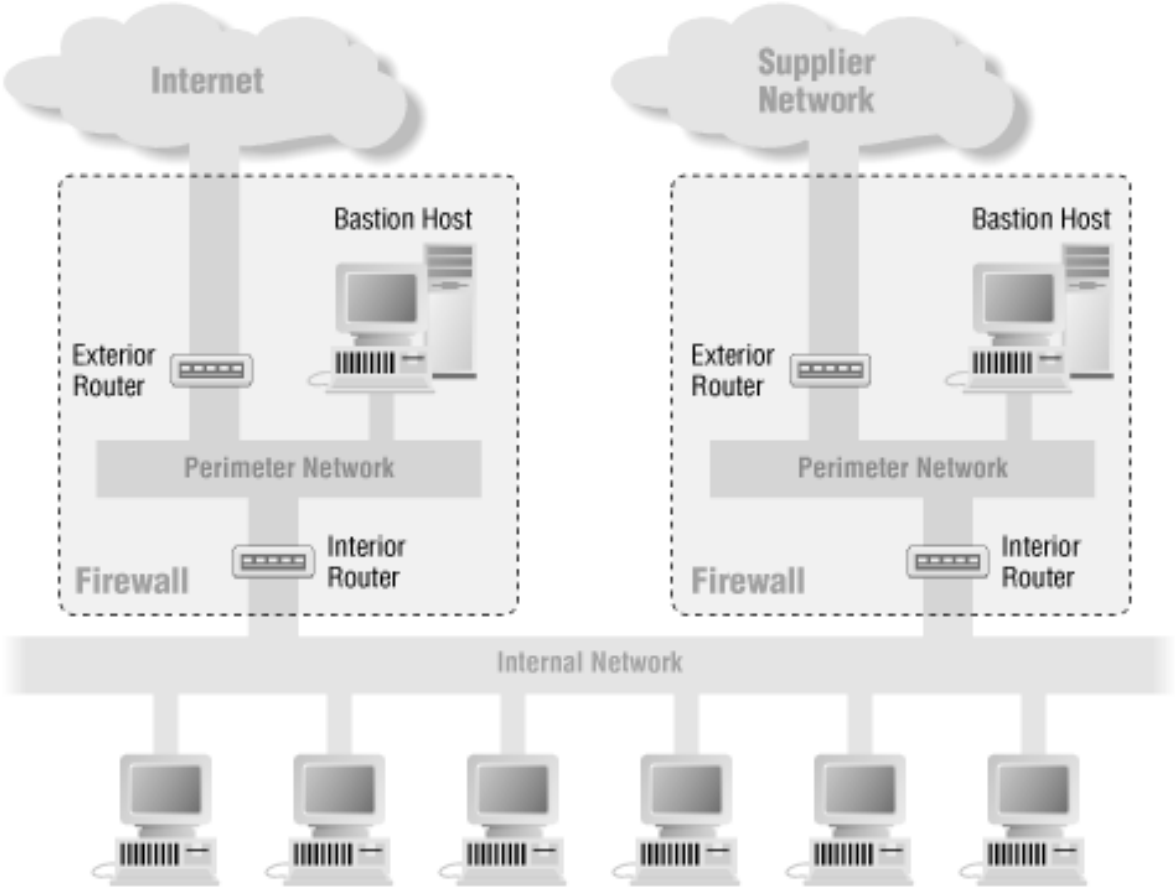
Допустими архитектурни решения – обединяване на външен маршрутизатор и Bastion хост



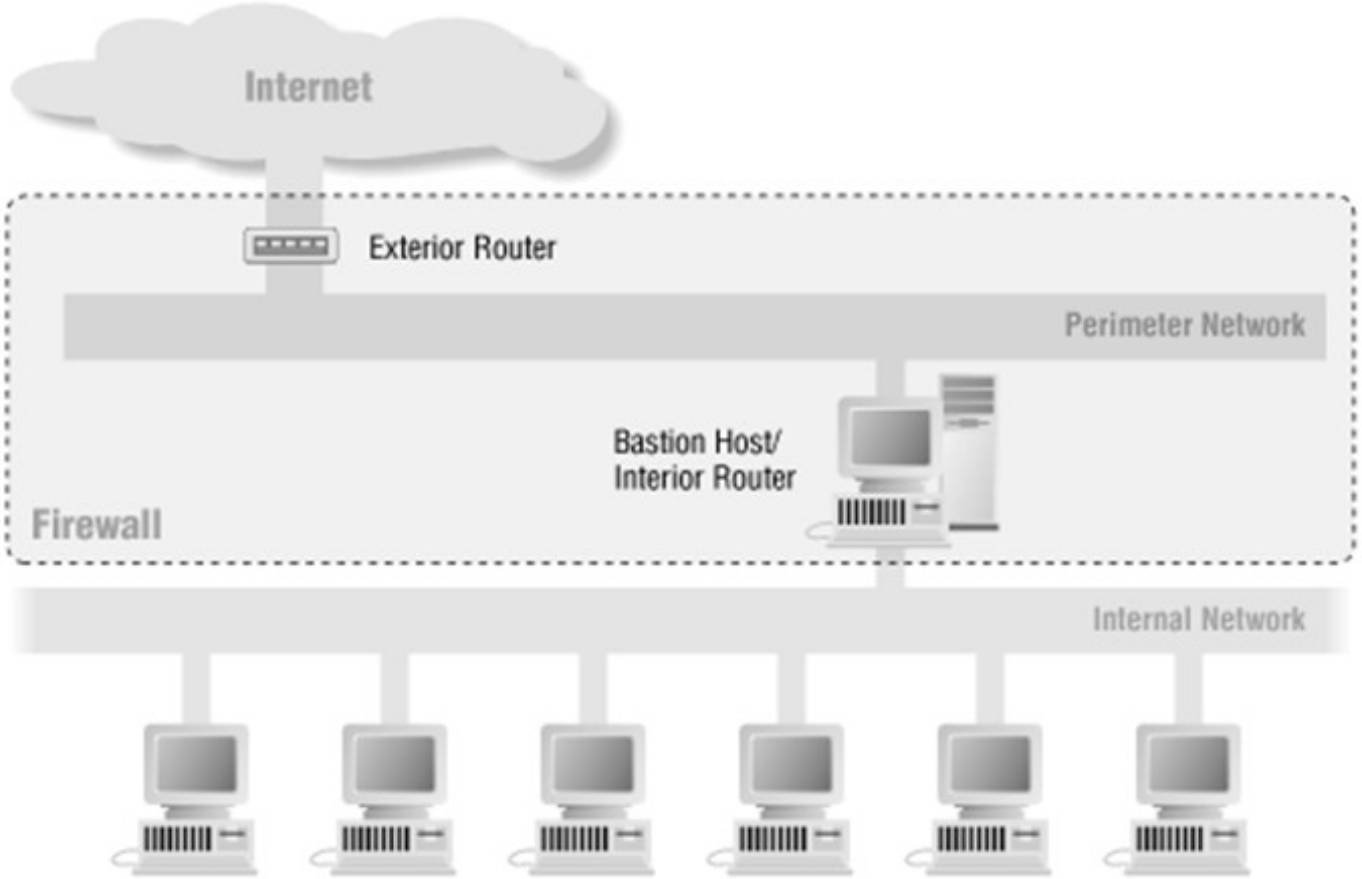
Допустими архитектурни решения – множество външни маршрутизатори



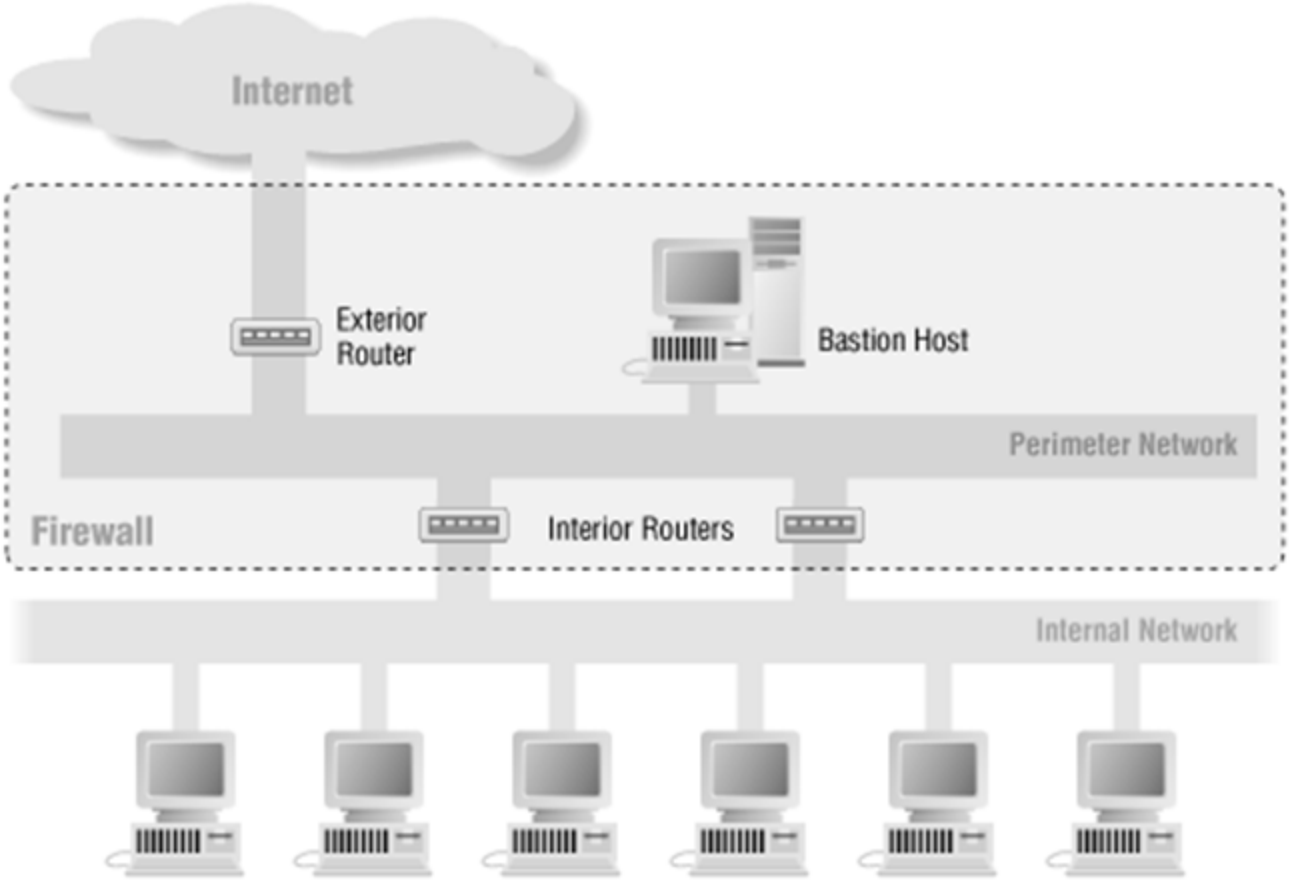
Допустими архитектурни решения – множество DMZ



Недопустими архитектурни решения – обединяване на Bastion хост и вътрешен маршрутизатор



Недопустими архитектурни решения – множество вътрешни маршрутизатори



Въпроси ?

Благодаря за вниманието !