

Firewall архитектуры

Какво да защитаваме?

- нашите данни: секретност, цялостност, наличност;
- нашите ресурси: компютърните системи;
- нашата репутация.

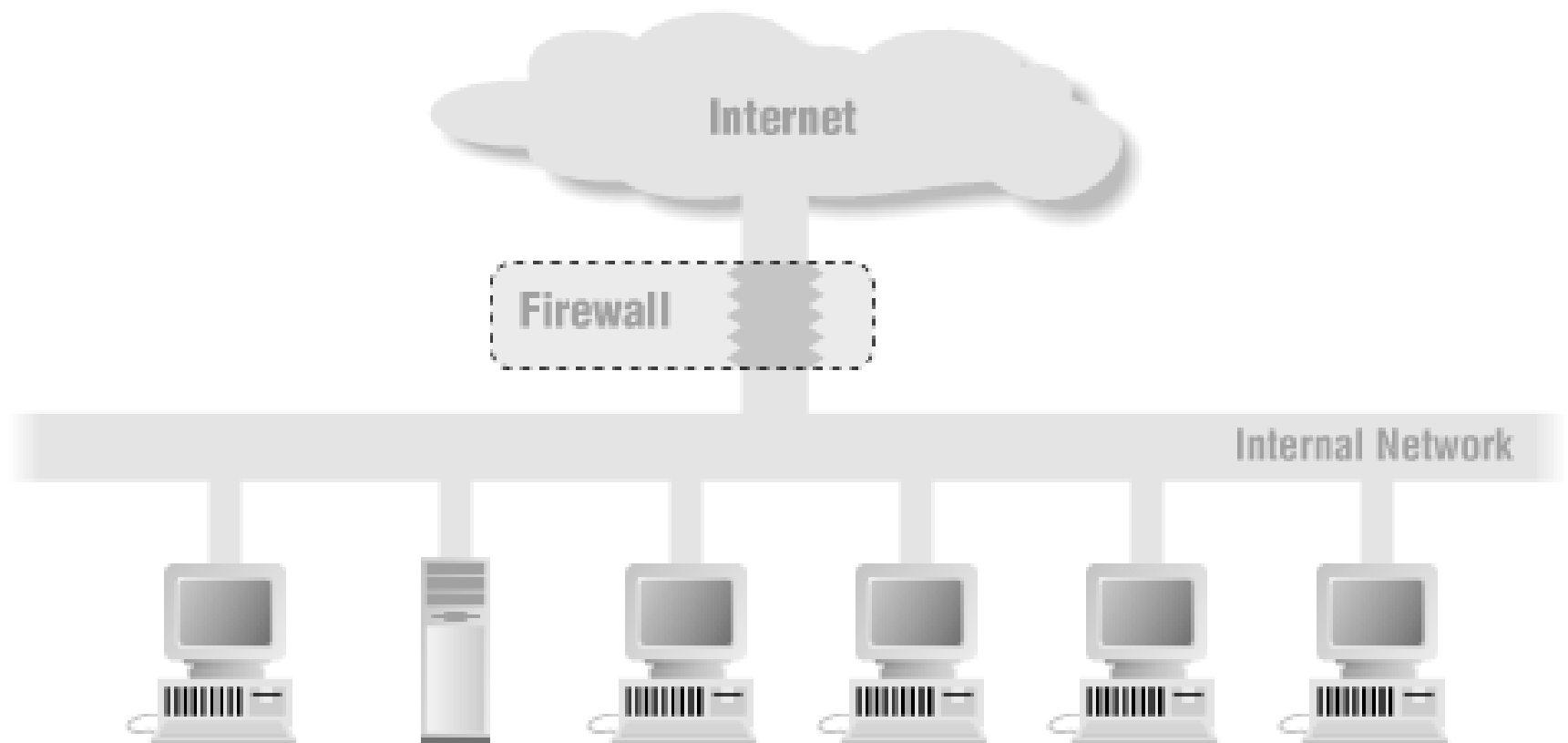
Подходи за защита

- без защита ☺;
- защита, базирана на неизвестност (Security through obscurity);
- защитаване на машината (Host security);
- мрежова защита (Network security).

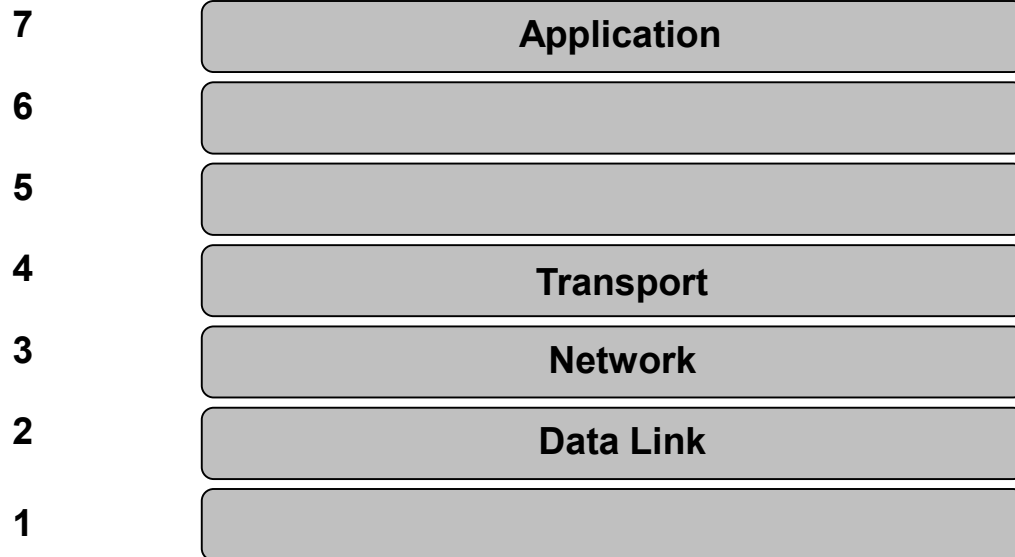
Firewall – какво е това?

Множество от компоненти, ограничаващи достъпа до Интернет или до други части на мрежите:

- ограничава входа и изхода на потребителите в контролирани точки;
- предпазва от атаки срещу защитени ресурси.



Нива на OSI за функциониране на Firewall?



Какво може Firewall?

- той е фокусираща точка за определяне на сигурността;
- подсилва политиката на сигурност;
- може да съхранява информация за Интернет трафика;
- предотвратява разпространението на вашите проблеми.

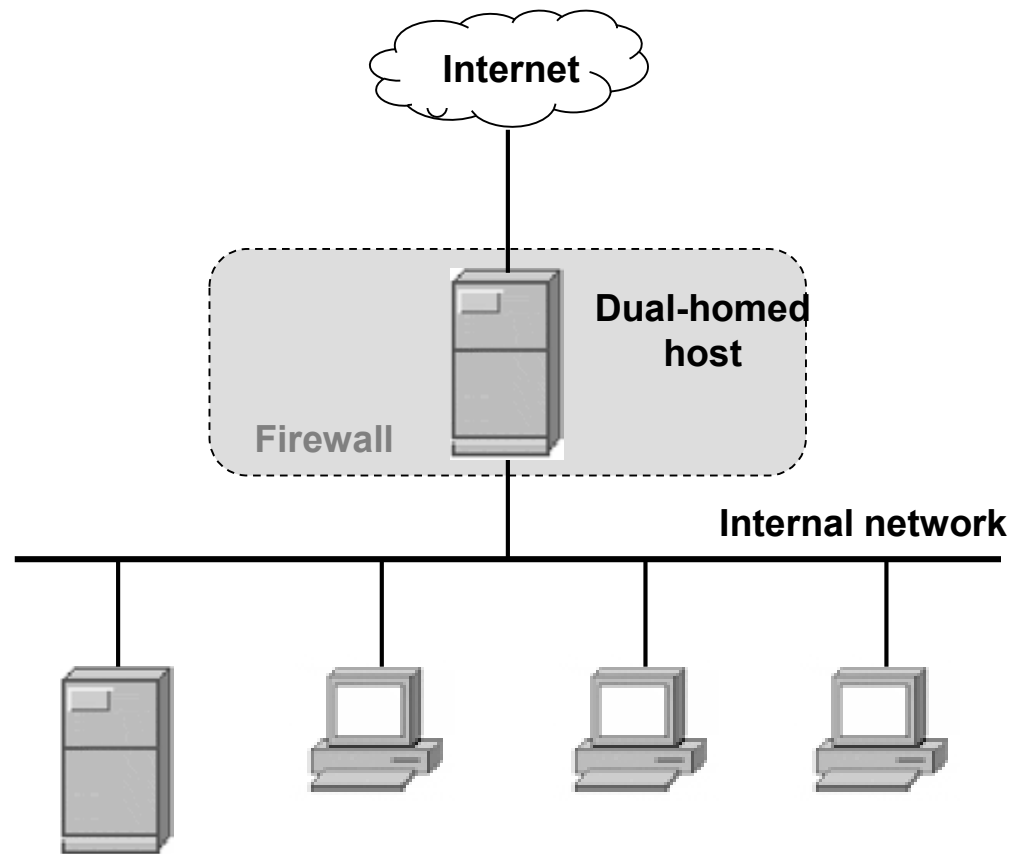
Какво не може Firewall?

- не може да предпази от вътрешни недоброжелатели;
- не може да защити от конекции, които не минават през него;
- не може да предпази от най-последните заплахи;
- не може да предпази от вируси.

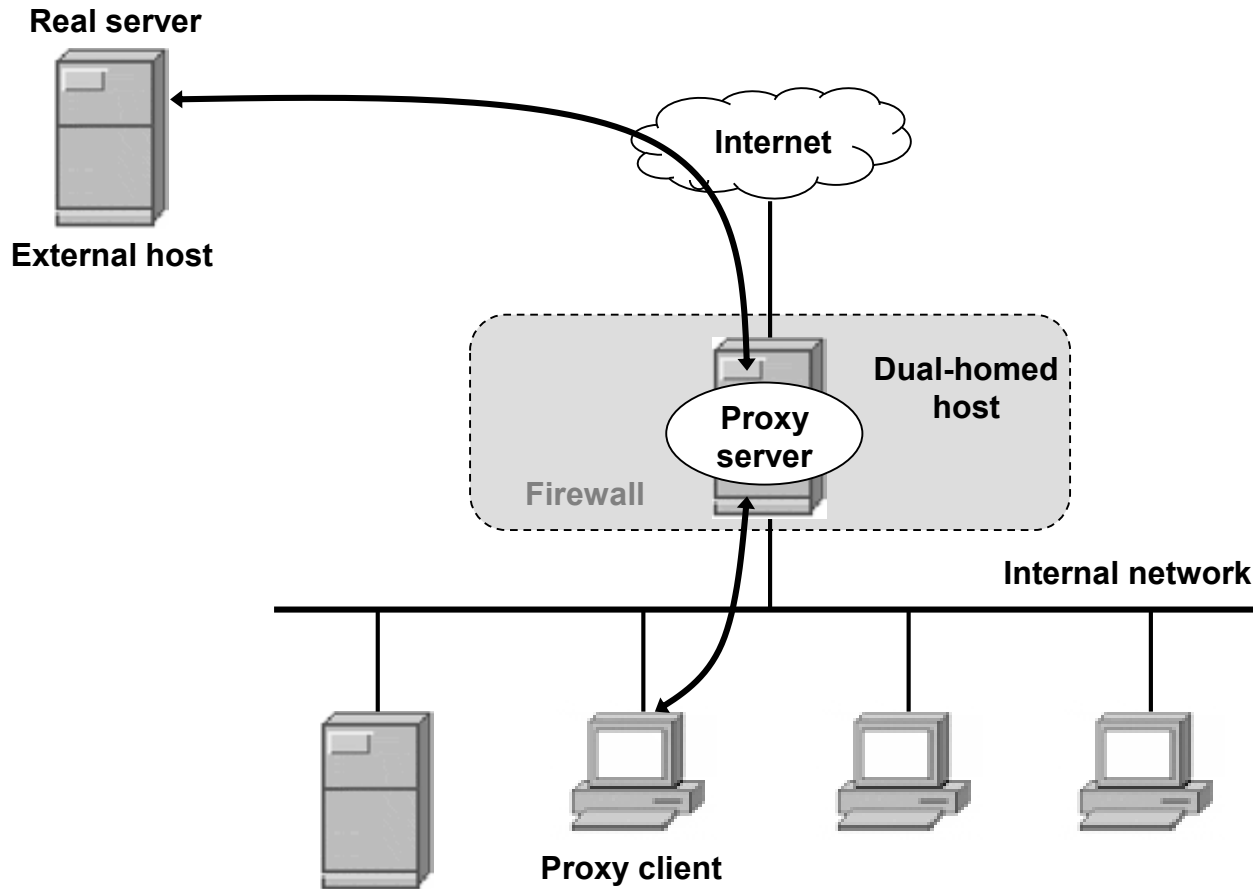
Firewall- основни понятия

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

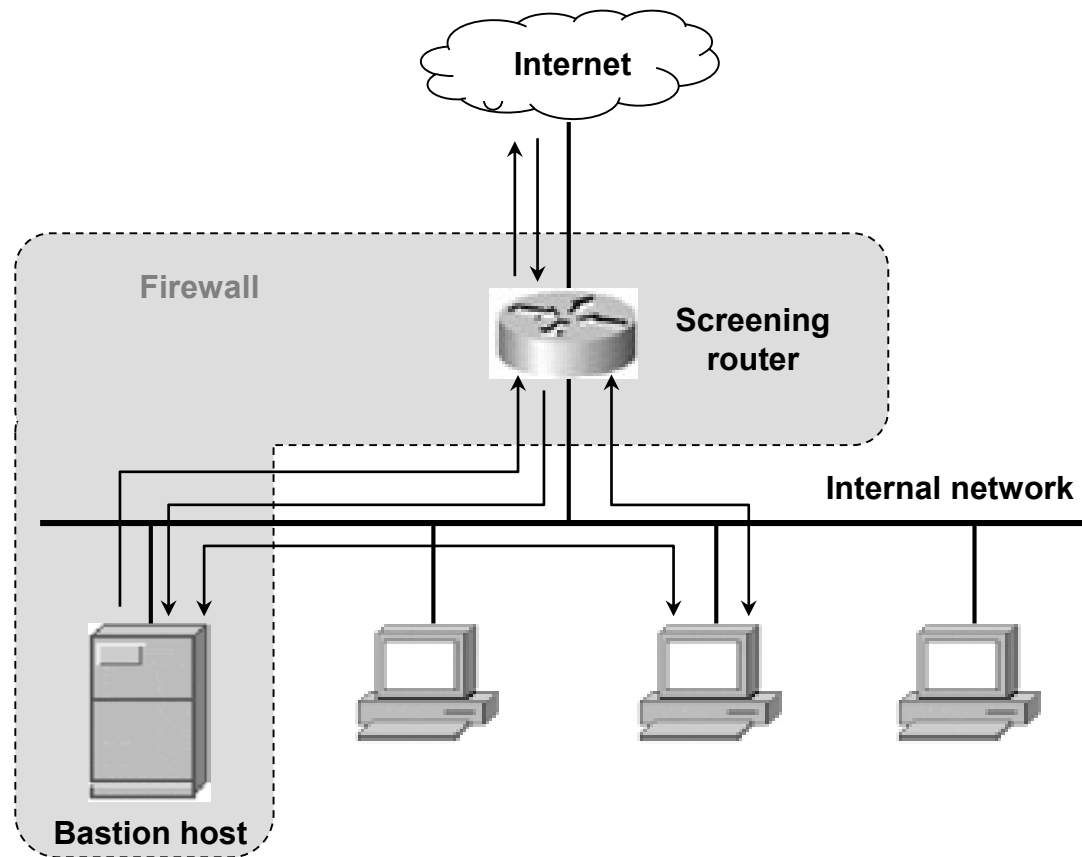
Firewall архитектуры – Dual-Homed host



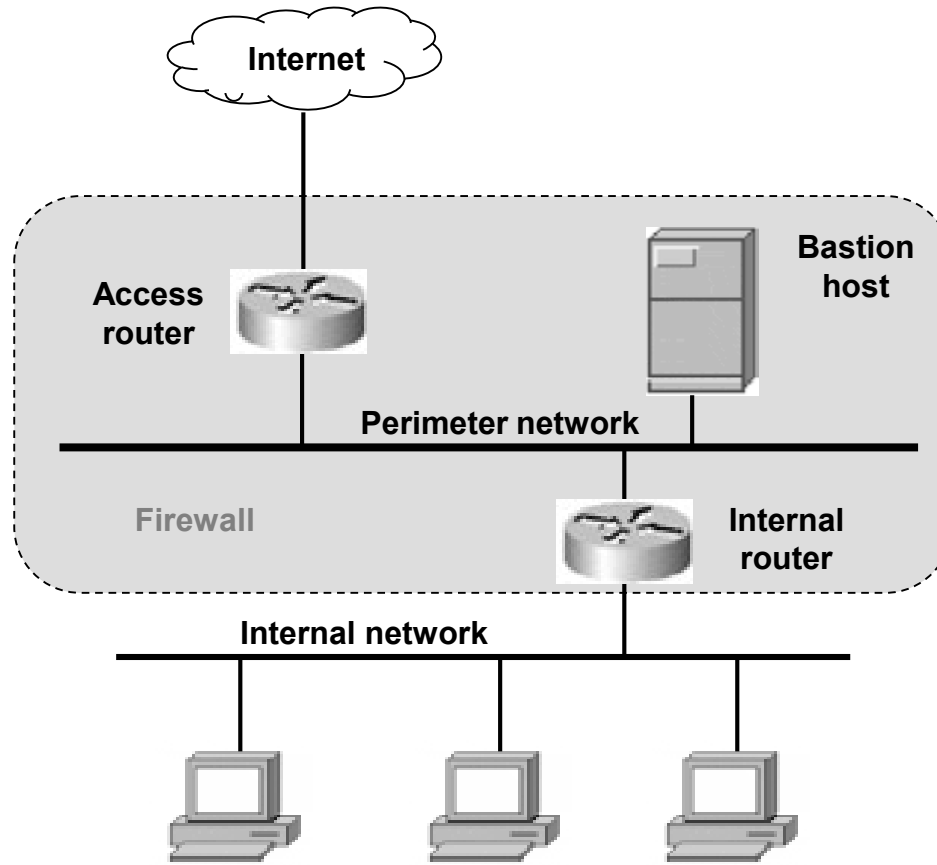
Dual-Homed Host + Proxy



Firewall архитектуры – Screened host



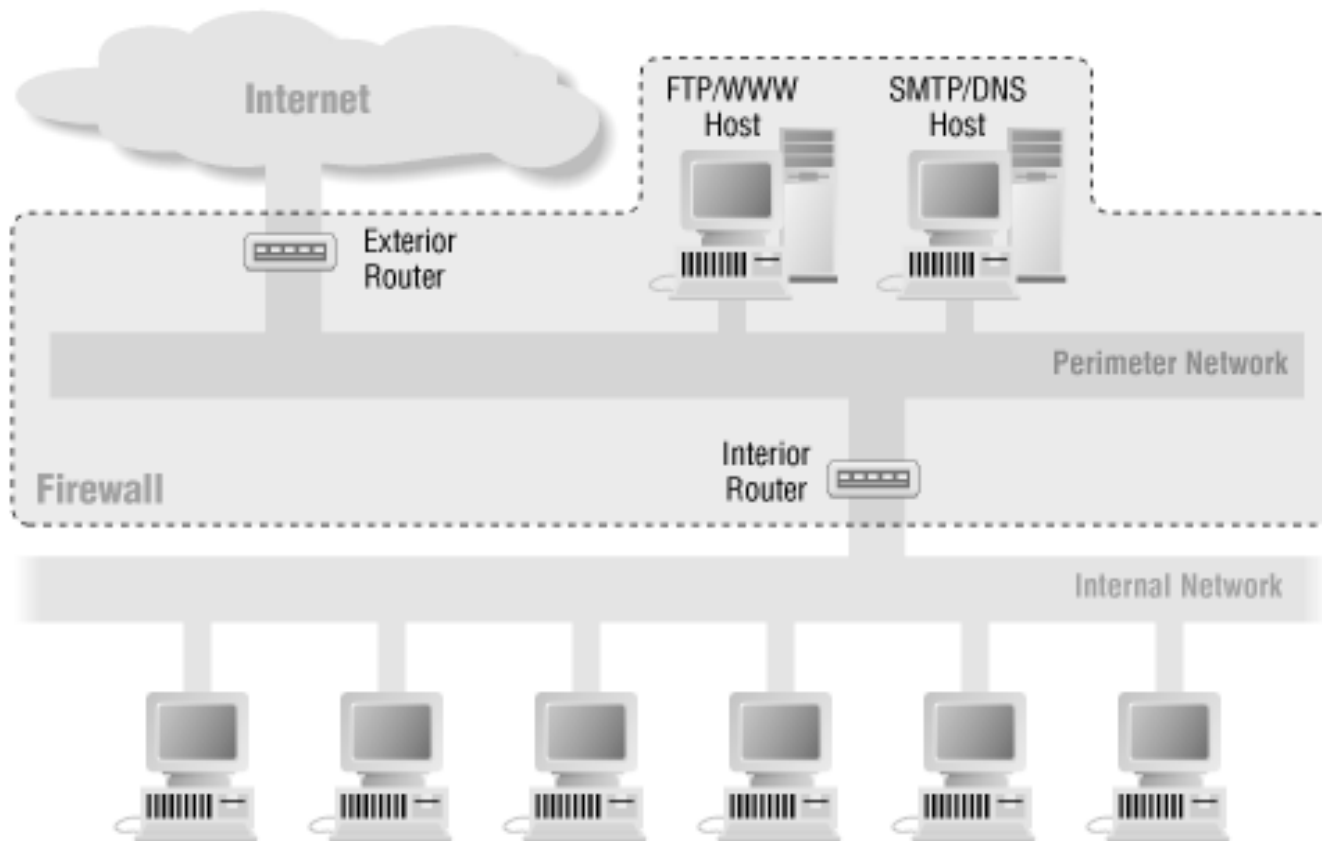
Firewall архитектуры – Screened subnet



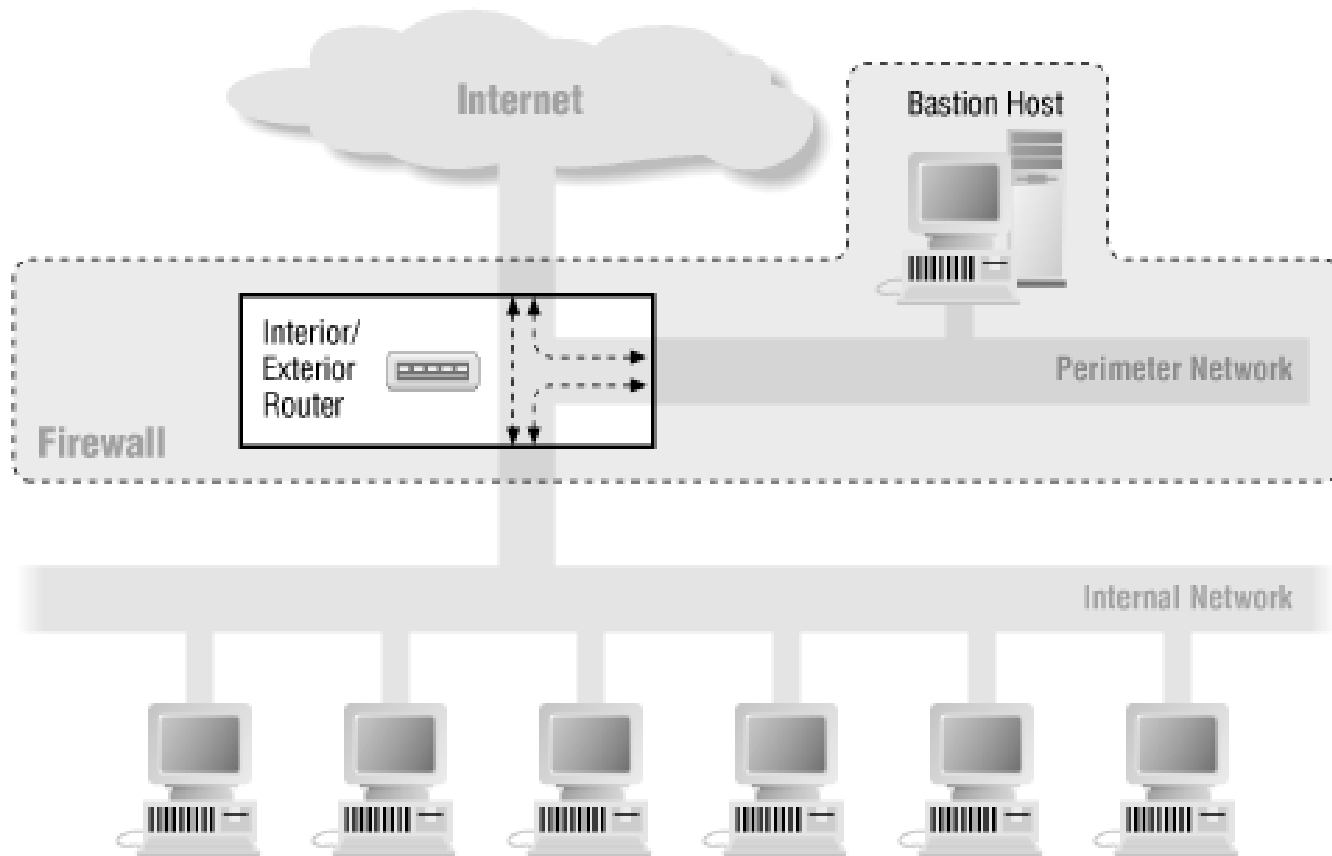
Компоненти на Screened subnet архитектура

- Perimeter network (DMZ);
- Bastion host;
- Вътрешен рутер (choke router);
- Външен рутер (access router).

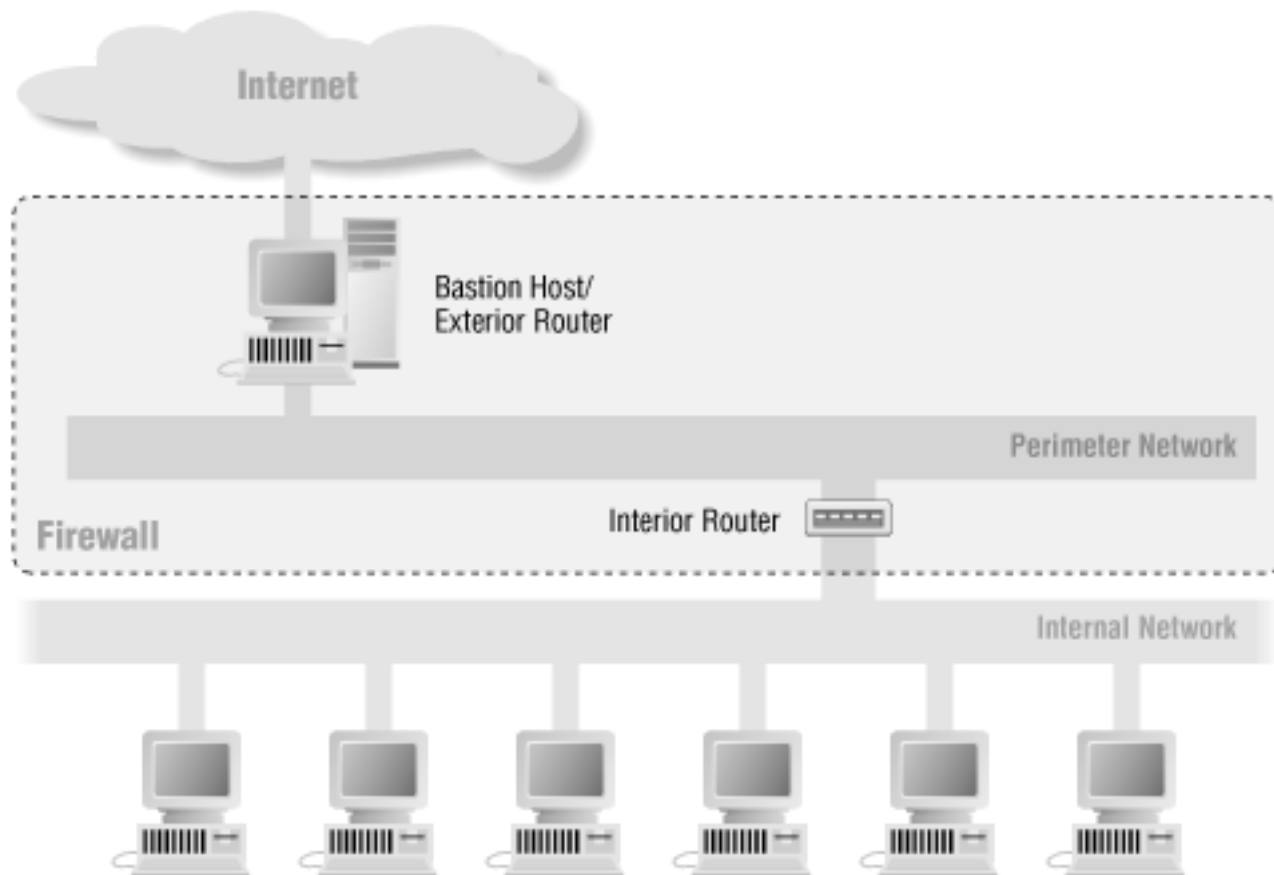
Допустими архитектурни решения – множество Bastion хостове



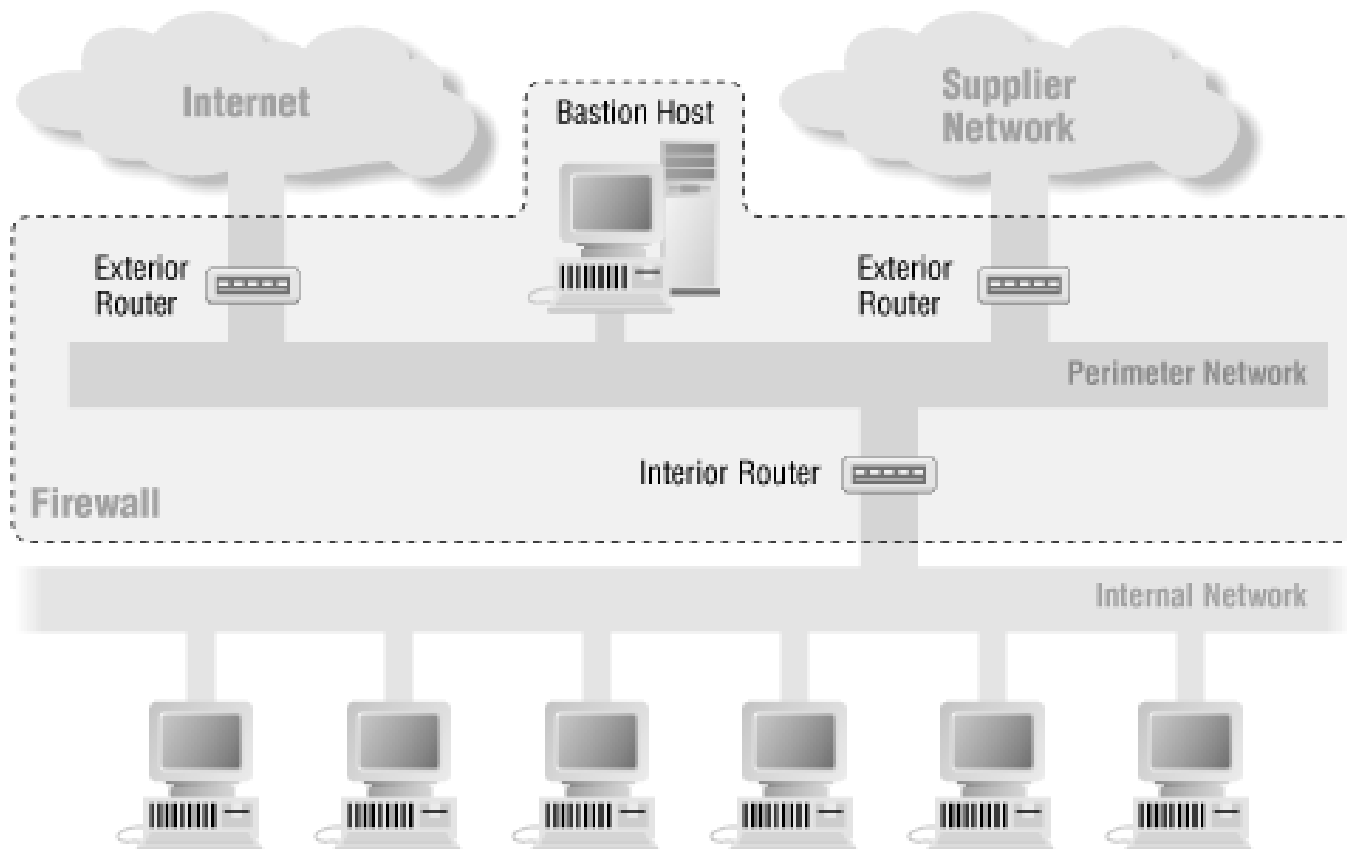
Допустими архитектурни решения –
обединяване на вътрешен и външен рутер



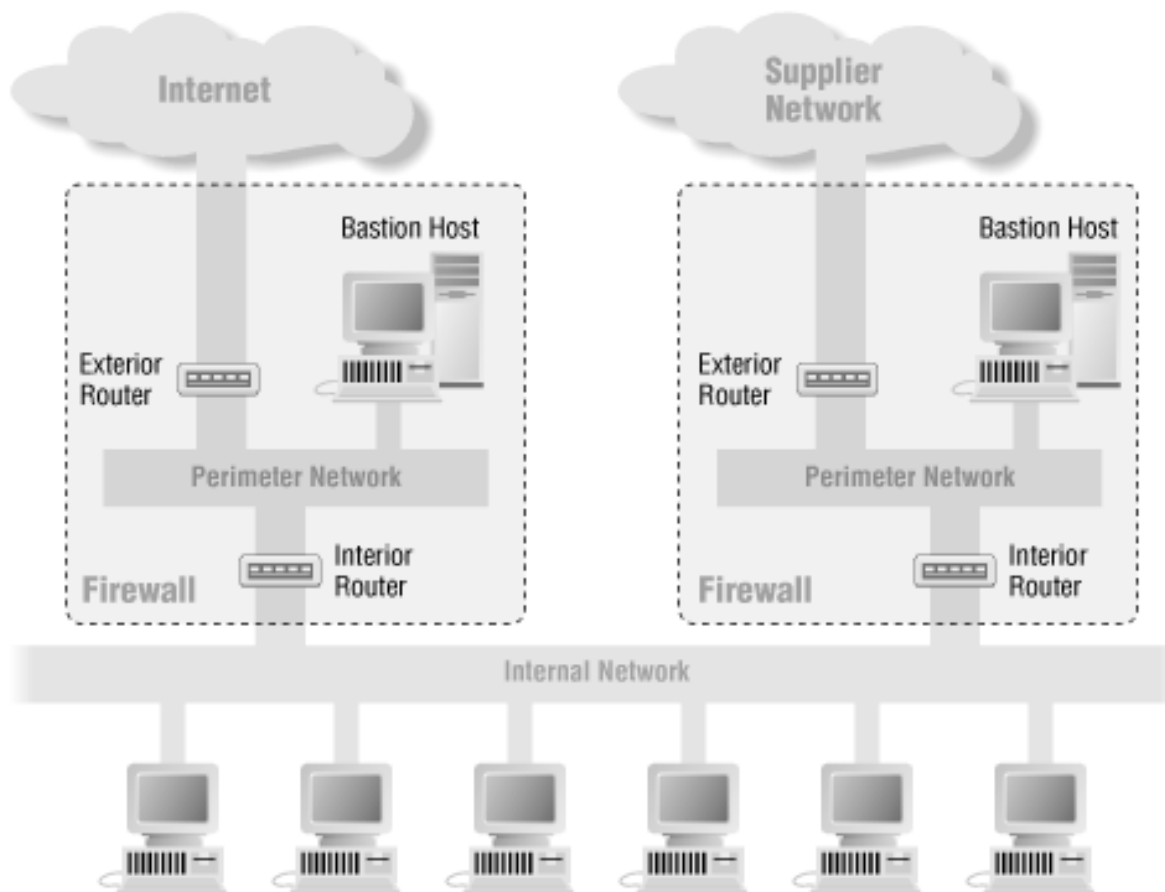
Допустими архитектурни решения –
обединяване на външен рутер и Bastion хост



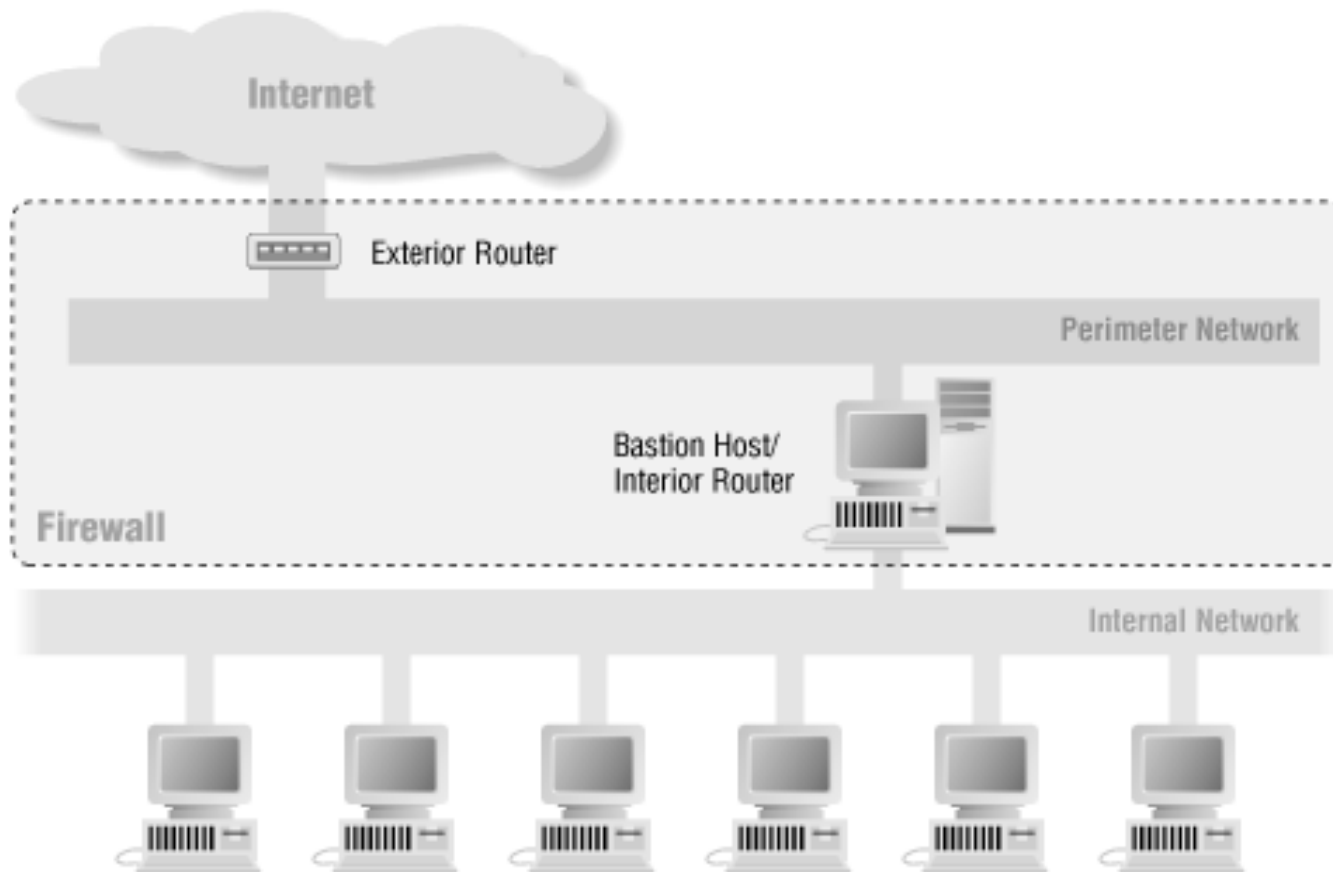
Допустими архитектурни решения – множество външни рутери



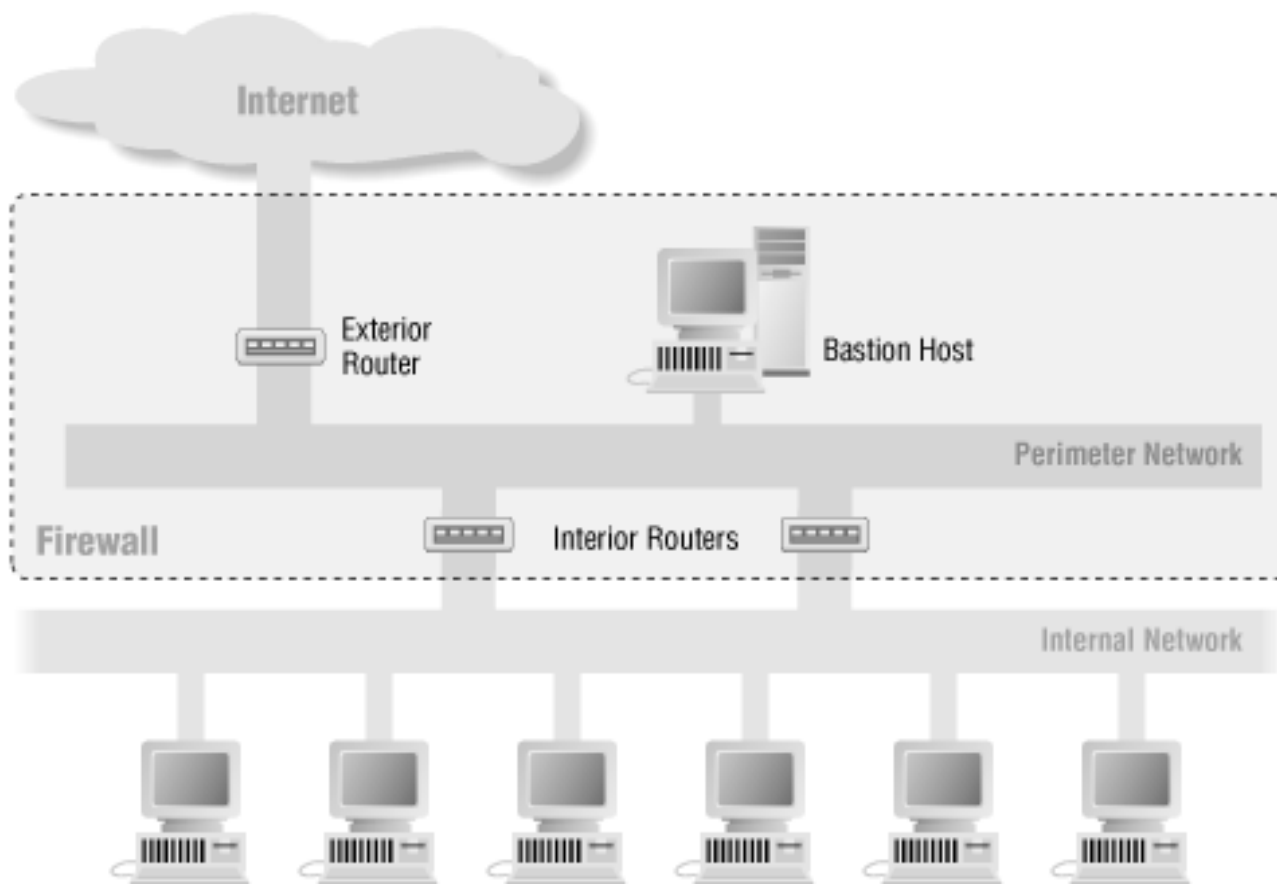
Допустими архитектурни решения – множество DMZ



Недопустими архитектурни решения – обединяване на Bastion хост и вътрешен рутер



Недопустими архитектурни решения – множество вътрешни рутери



Въпроси ?