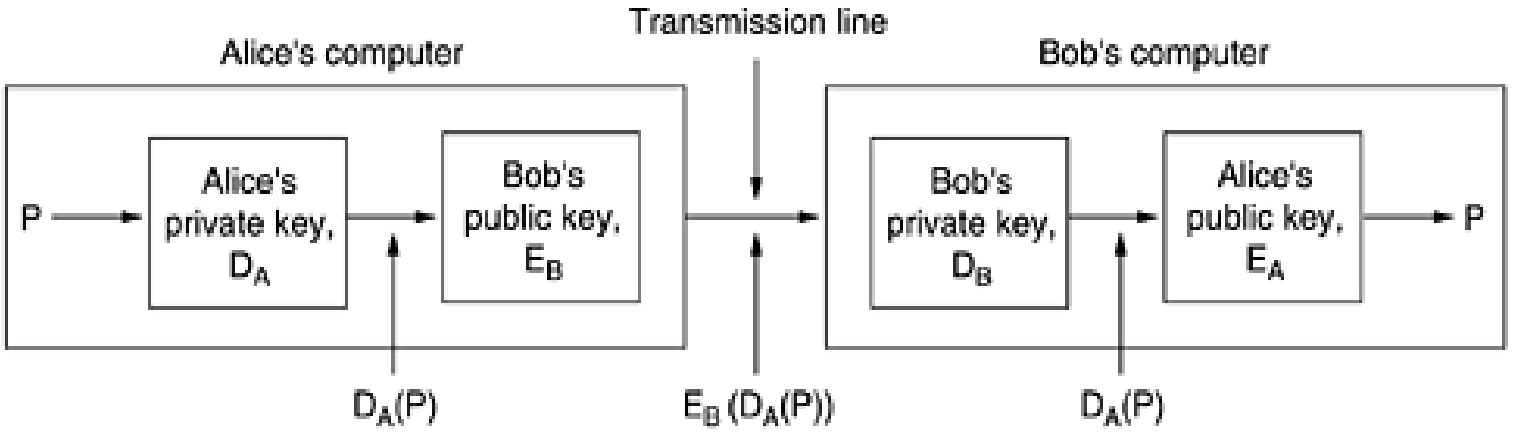
3.5.2.2 Инфраструктура на јавни клучеви

- Алгоритмите за асиметрично криптирање претставуваат основа за инфраструктурата на јавни клучеви (PKI – Public Key Infrastructure)
- Вообичаено, корисникот генерира пар клучеви (јавен/приватен) и го објавува јавниот клуч



3.5.2.2 Инфраструктура на јавни клучеви

- Но, како може да се знае дека јавниот клуч припаѓа на вистинската личност, а не на некој измамник?
- Кај PKI, доверлива трета страна (Certificate Authority) издава **сертификат** за јавниот клуч, откако корисникот ќе го потврди сопствениот идентитет

3.5.2.2 Инфраструктура на јавни клучеви

- Сертификатот претставува множество податочни елементи кои се обединети и електронски потпишани од страна на Certificate Authority

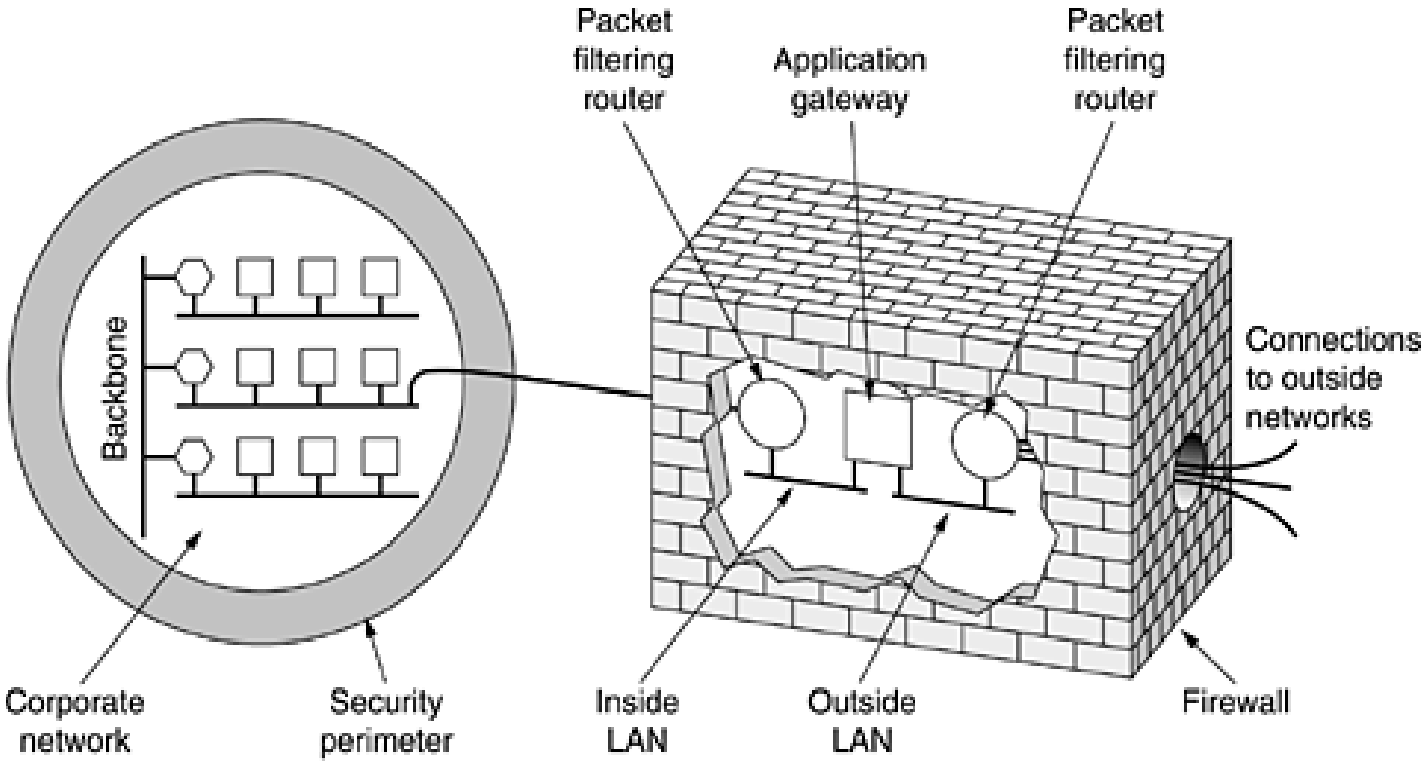
3.5.2.2 Инфраструктура на јавни клучеви

- **Class 1** сертификат – ги обединува името на корисникот, неговата e-mail адреса и јавниот клуч
  - Го користат индивидуални Интернет корисници за испраќање на безбедна електронска пошта, или за сопствена идентификација при пристап до Web сервери
- **Class 2** сертификат – обединува и дополнителни детали (на пр. број на сметка)
  - Го користат организациите (на пр. банки) за идентификација на сопствените клиенти
- **Class 3** сертификат – ги обединува името на организацијата, URL на серверот и јавниот клуч
  - Го користат web сервер операторите – овозможува размена на клучеви за криптирање и воспоставување на безбедни HTTP сесии (на пр. за електронска комерција или апликации за електронско банкарство)

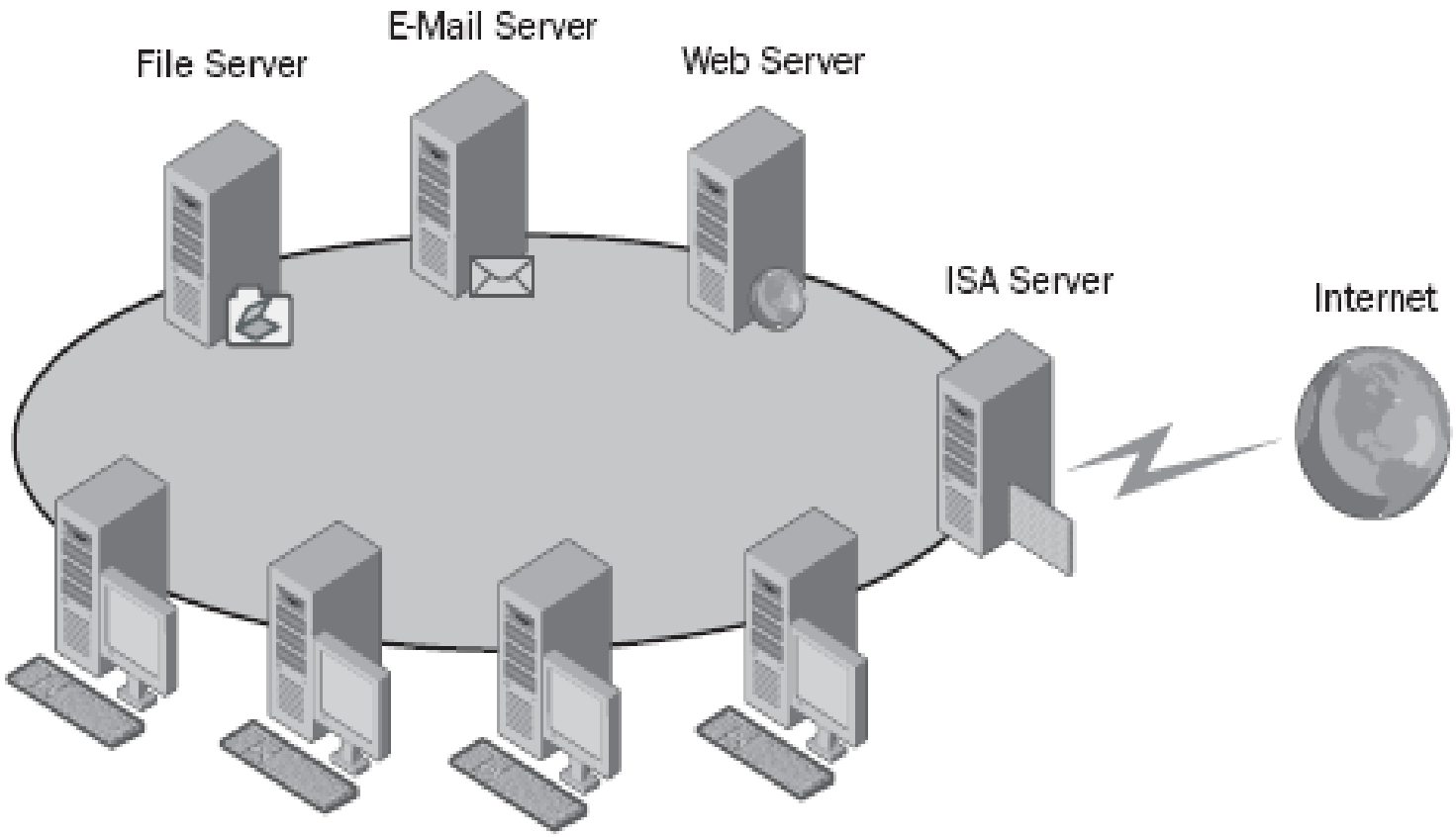
3.5.2.3 Firewall

- Примената на firewall систем е една од најефикасните и најшироко применуваните безбедносни стратегии
- Севкупната комуникација помеѓу машините внатре и надвор од претпријатието поминува низ firewall – компјутер со посебна намена
- Задача на firewall-от е да го следи и филтрира сообраќајот кој се одвива преку него и да овозможи комуникација само со добро познати сервиси или со доверливи надворешни системи
- Firewall системи овозможуваат криптирање, што се користи за креирање на безбедни тунели низ јавните мрежи (IP VPNs)

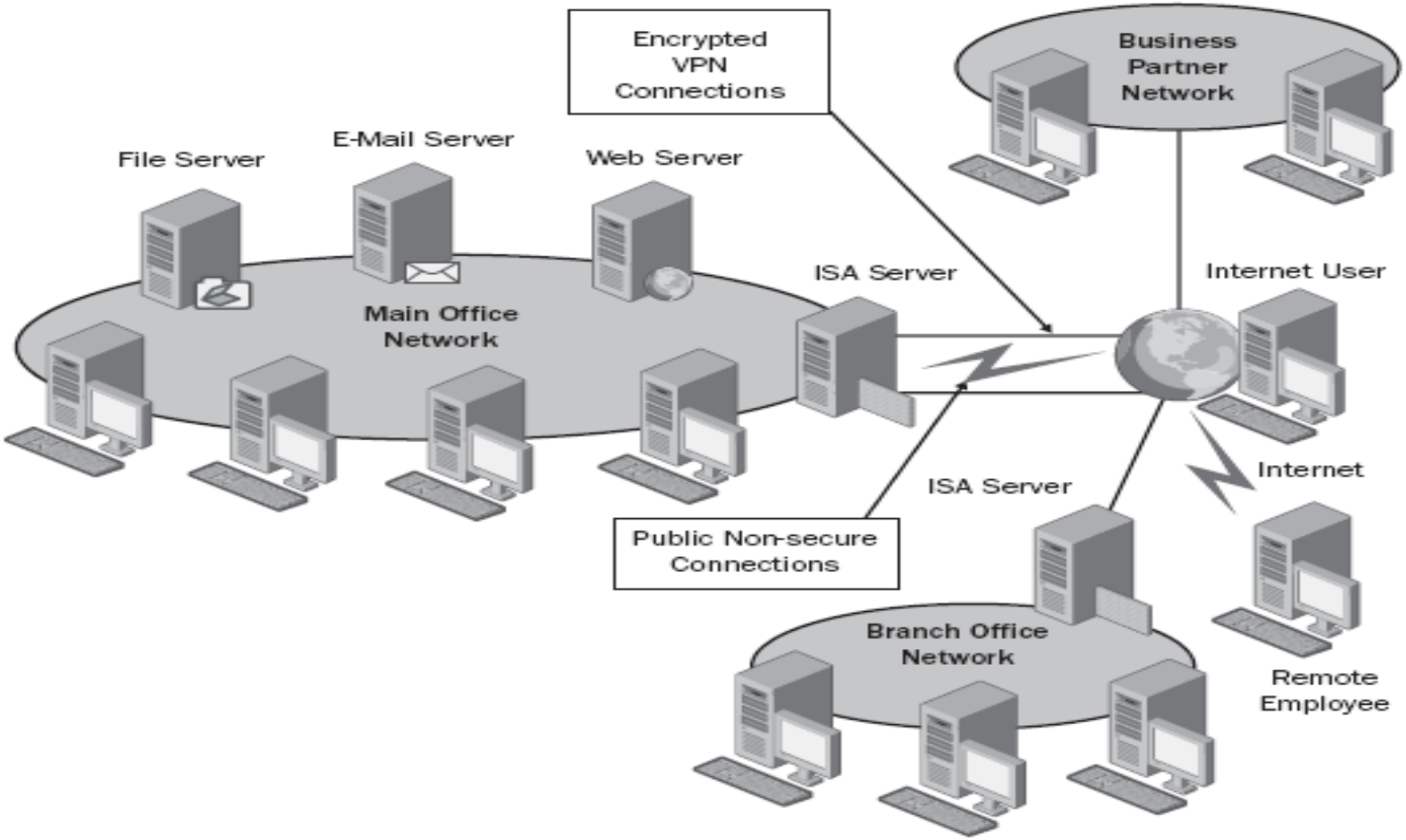
3.5.2.3 Firewall



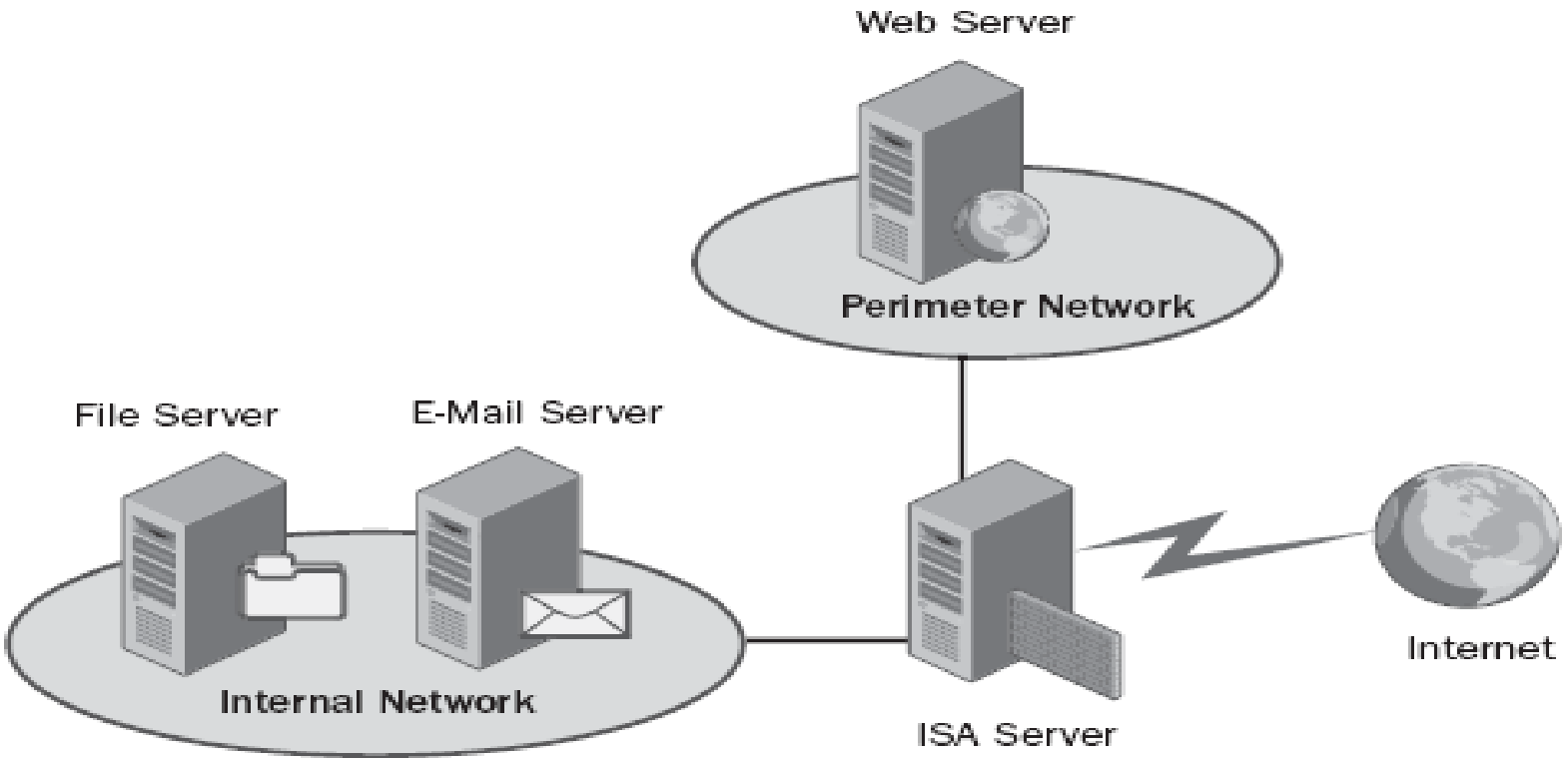
3.5.2.3 Firewall - Works as an Internet-Edge Firewall



3.5.2.3 Firewall - Works as a Branch Office Firewall



3.5.2.3 Firewall – Support for Multiple Networks



3.5.2.3 Firewall – Support for Multiple Networks