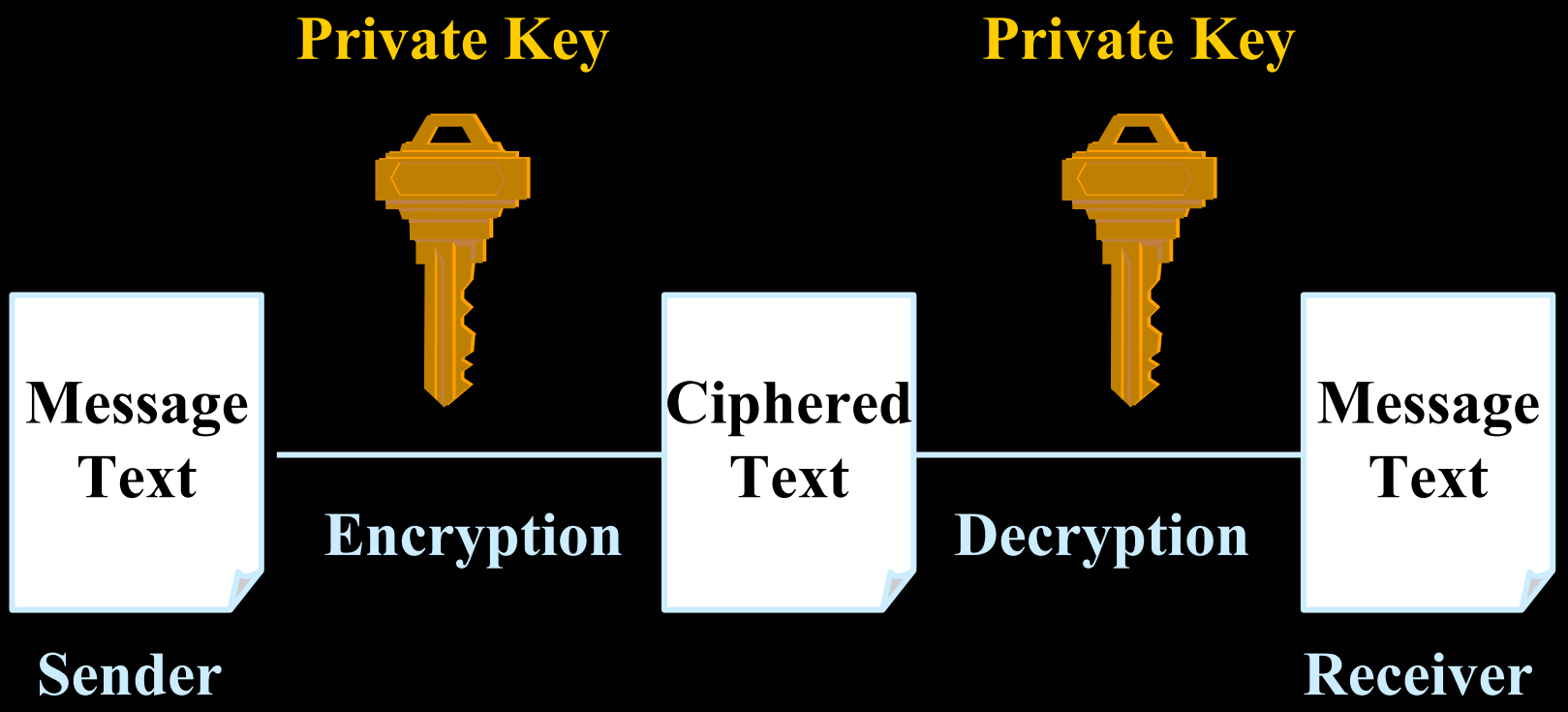
Internet Security

Cornerstones of Security

- Authenticity
  - the sender (either client or server) of a message is who he, she or it claims to be
- Privacy
  - the contents of a message are secret and only known to the sender and receiver
- Integrity
  - the contents of a message are not modified (intentionally or accidentally) during transmission
- Non-repudiation
  - the sender of a message cannot deny that he, she or it actually sent the message

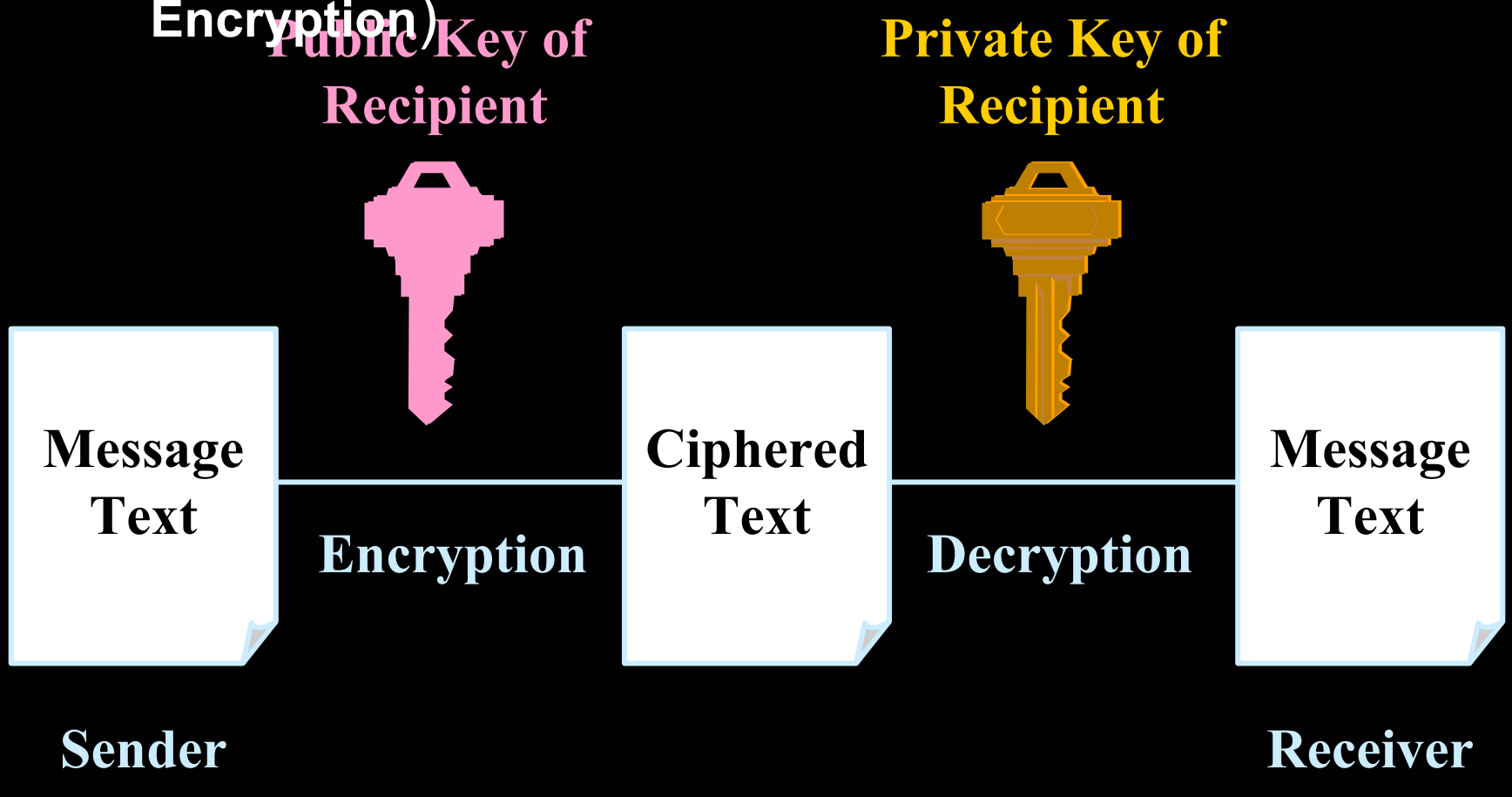
Encryption

- Private Key Encryption (**Symmetrical Key Encryption**)
  - **Data Encryption Standard (DES)** is the most widely used symmetrical encryption algorithm



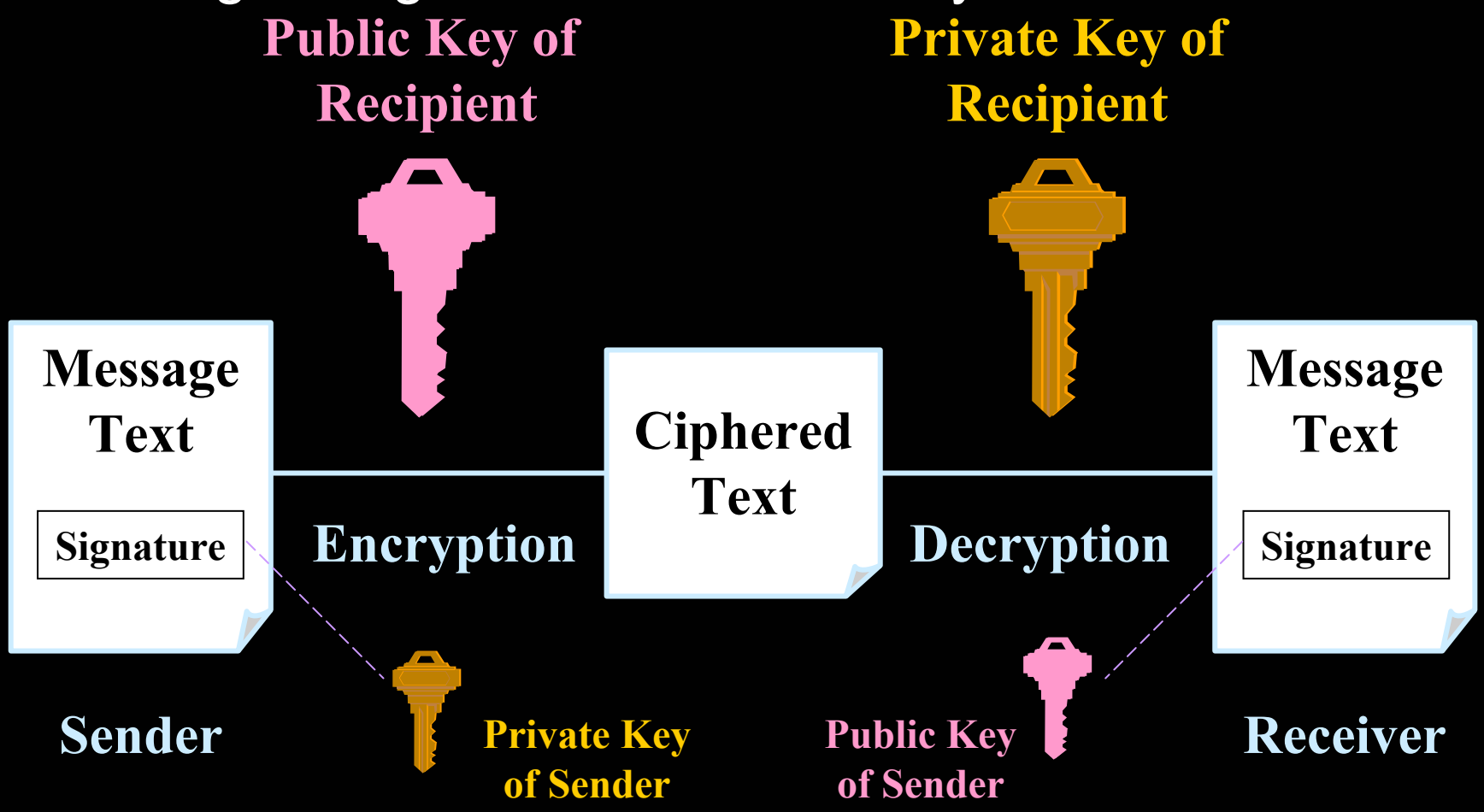
Encryption *(cont.)*

- Public Key Encryption (Asymmetrical Key Encryption)



Encryption *(cont.)*

- Digital Signatures : Authenticity and Non-Denial



Digital Certificates and Certifying Authorities

- Digital Certificates
  - Verify the holder of a public and private key is who he, she or it claims to be
- Certifying Authorities (CA)
  - Issue digital certificates
  - Verify the information and creates a certificate that contains the applicant's public key along with identifying information
  - Uses their private key to encrypt the certificate and sends the signed certificate to the applicant

Secure Socket Layer (SSL)

- Is a secure socket connection protocol that operates at the TCP/IP layer
- Authenticates and encrypts communications between browsers and servers
- Supports a variety of encryption algorithms and authentication methods
- Verifies that the content of the message hasn't been altered
- HTTP servers that implement SSL must run on socket port 443 instead of 80. It has become a common practice for firewall vendors to leave this port open.

The SSL protocol provides

- Private client/server interactions using encryption
- Server authentication
- Message integrity checks that detect tampering
- When a client and server first start communicating:
  - They agree on an SSL protocol version
  - Select the cryptographic algorithm
  - Optionally authenticate each other
  - Use public-key encryption technology for message sending
- SSL is now called TLS (Transport Layer Security) protocol

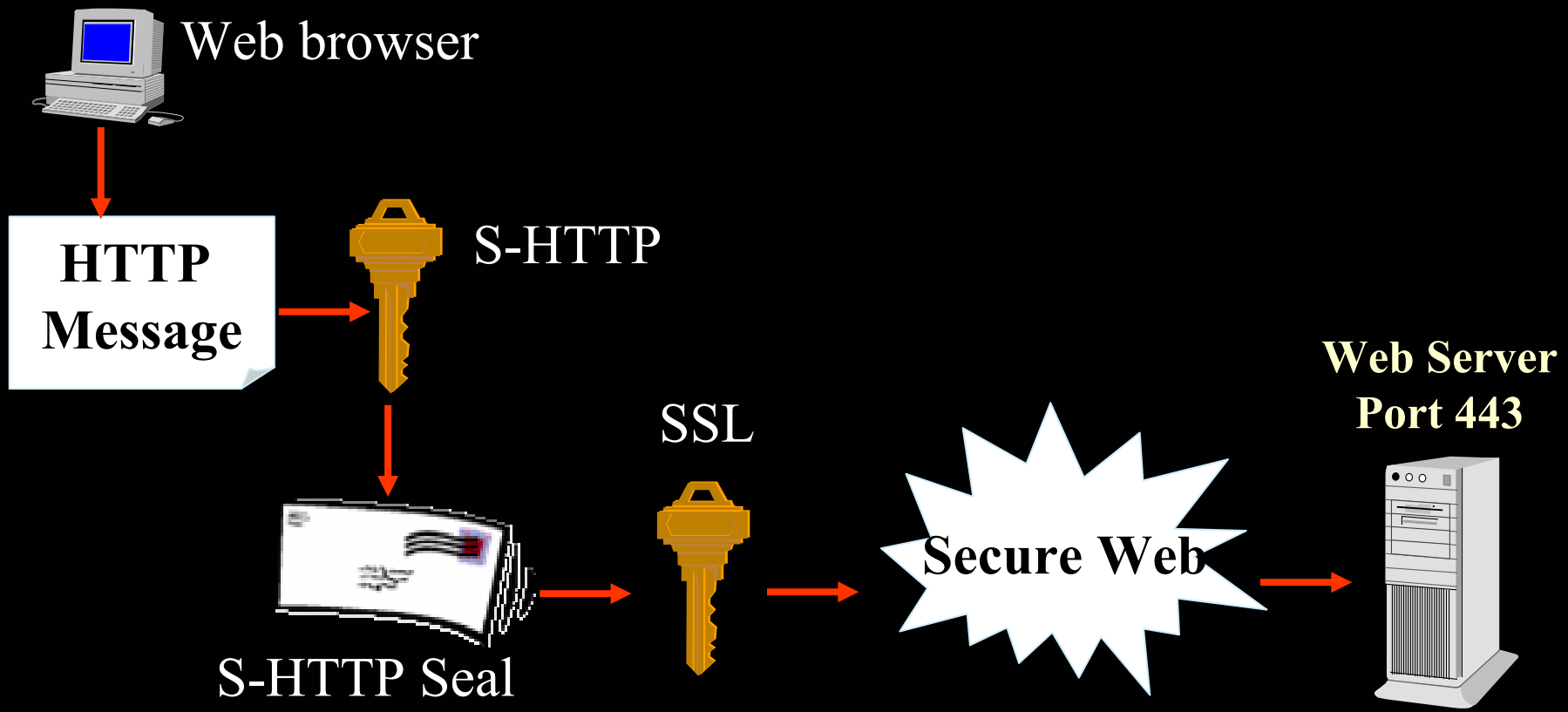
S-HTTP

- S-HTTP is a security-enhanced variant of the HTTP protocol
- Adds application-level encryption and security on top of ordinary sockets-based communications
- The browser and server communicate over an ordinary HTTP session and then negotiate their security requirements
- Like SSL, S-HTTP incorporates public-key cryptography from RSA.
- It also supports password- and Kerberos-based security systems.

S-HTTP (cont.)

- It provides the following security checks:
  - It authenticates both clients and servers
  - It checks for server certificate revocations
  - It supports certificate chaining and hierarchies
  - It supports digital signatures that attest to a message's authenticity
  - It allows an application to negotiate the security levels it needs
  - It provides secured communications through existing corporate firewalls

S-HTTP on top of SSL

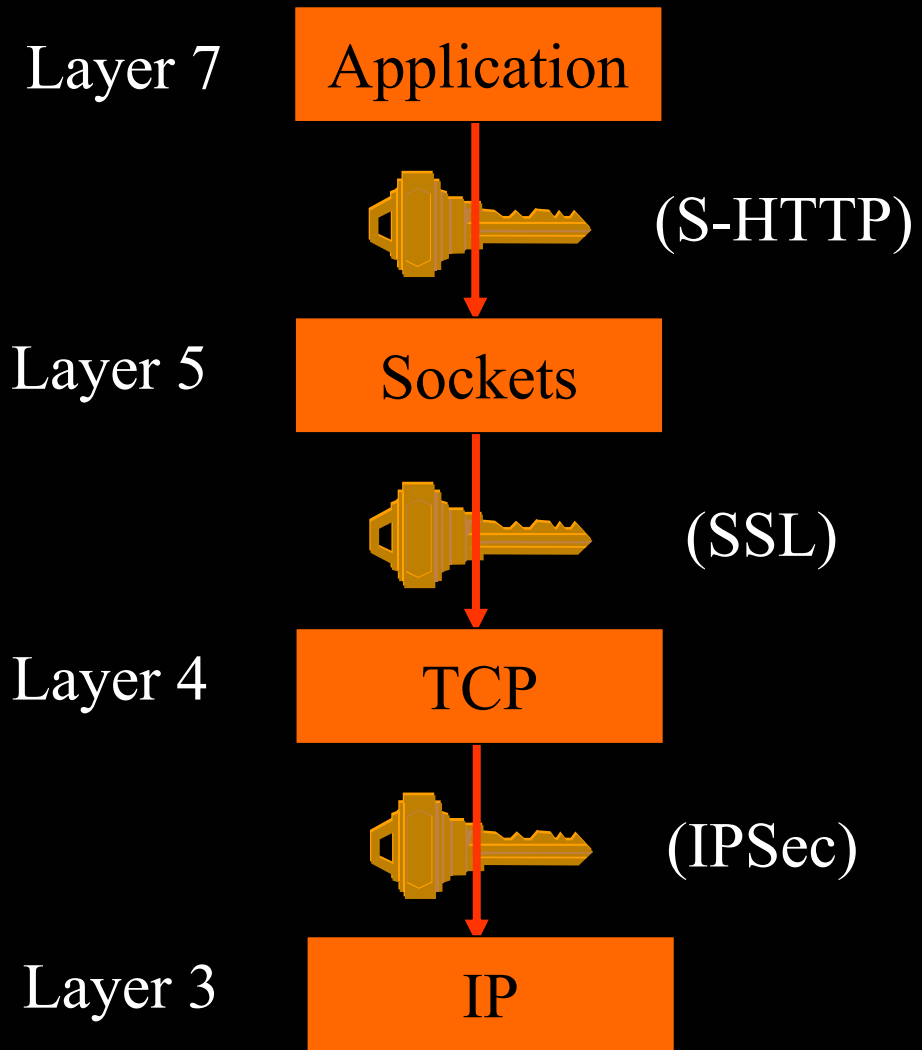


IPSec

- It provides authentication and encryption at the IP layer (Layer 3)
- SSL operates at the TCP layer (Layer 4)

- IPSec is less visible than SSL
- IPSec is faster since IP switches and routers can implement the protocol in their hardware

TCP/IP encryption: the choices



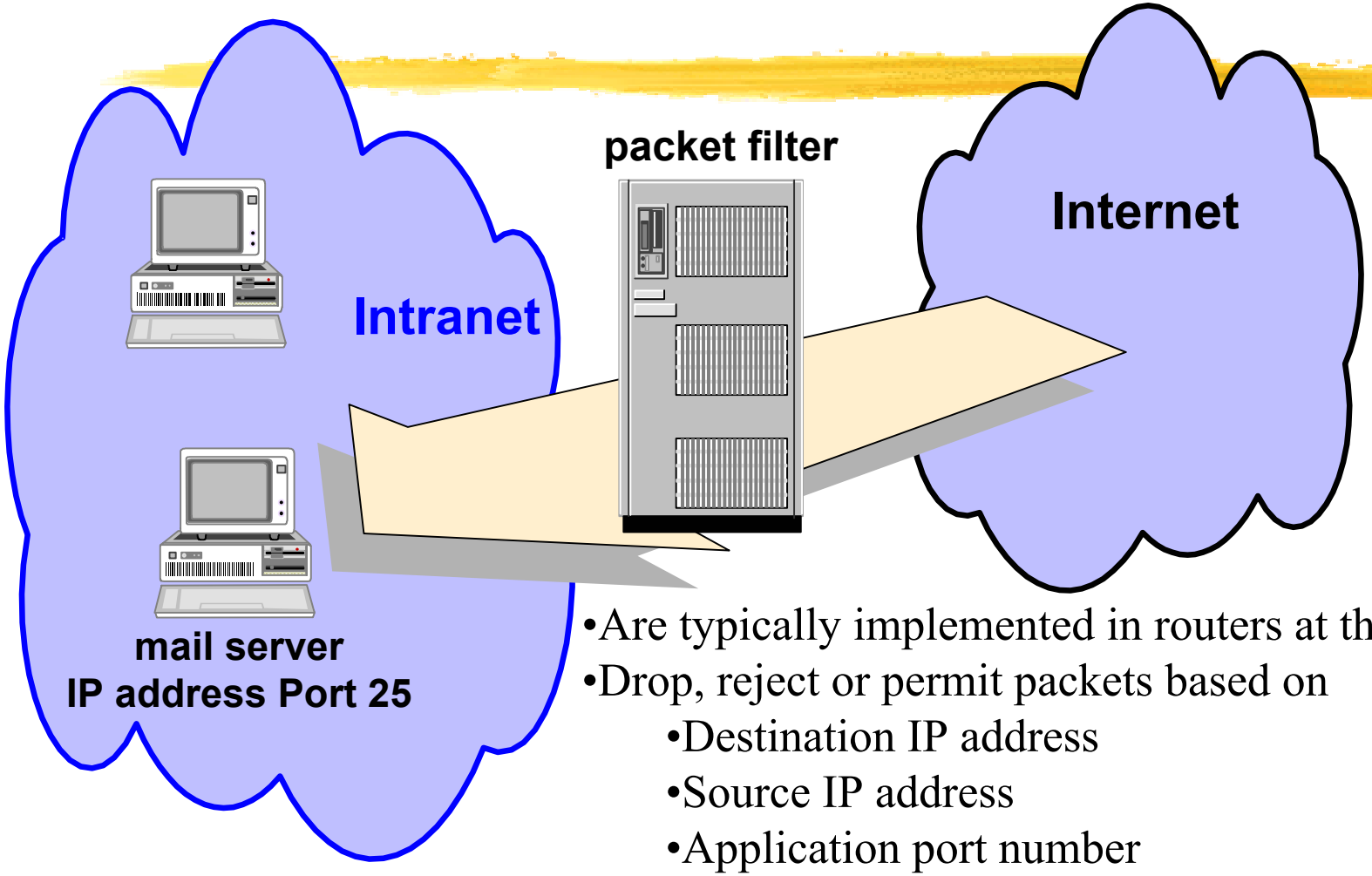
Access Control

- Password Protection
  - Passwords are notoriously susceptible to compromise
    - **Users have a habit of sharing their passwords with others, writing them down where others can see them, and choosin passwords that are easily guessed.**
    - **Browser transmits the passwords in a form that is easily intercepted and decoded.**
  - **One of the roles of a firewall: making sure that even if the passwords are compromised the intruder only has restricted access to the rest of the network.**

Firewalls

- A network node consisting of both hardware and software that isolates a private network from a public network
- Make sure that even if the passwords are compromised the intruder only has restricted access to the rest of the network
- Three types
  - **Packet-filtering firewalls**
  - **Application level firewalls (Dual-homed gateway)**
    - **bastion gateway connects a private internal network to outside Internet**
    - **proxies (software programs) run on the gateway server and pass repackaged packets from one network to the other**
  - **Screen-host gateway**
    - **screened subnet gateway in which the bastion gateway offers access to a small segment of the internal network**
    - **demilitarized zone (DMZ) is the open subnet**

Packet-filtering firewalls

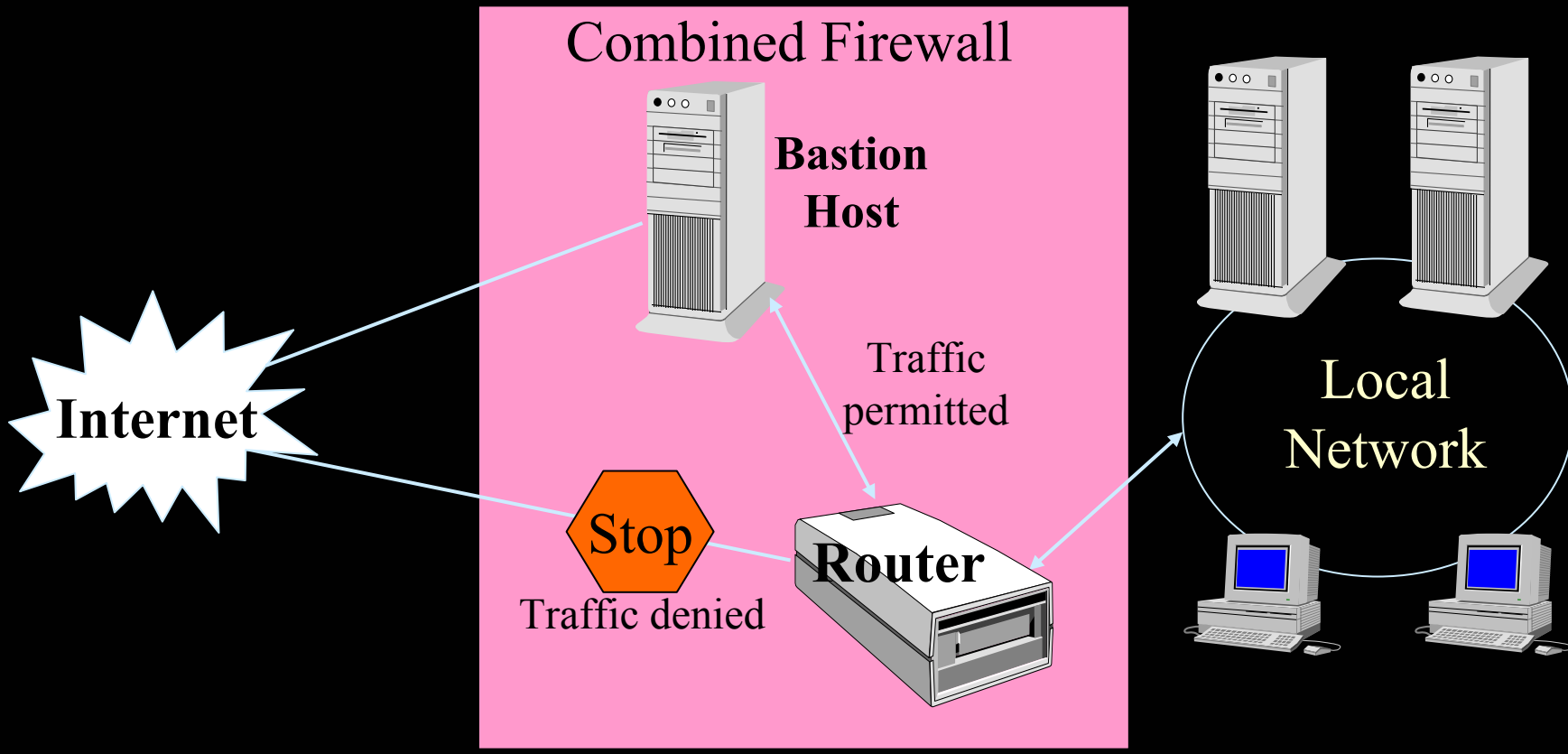


- Are typically implemented in routers at the **IP level**
- Drop, reject or permit packets based on
  - Destination IP address
  - Source IP address
  - Application port number
- Drawback: easy to mimic the IP addresses of trusted machines

Proxy (application) firewalls

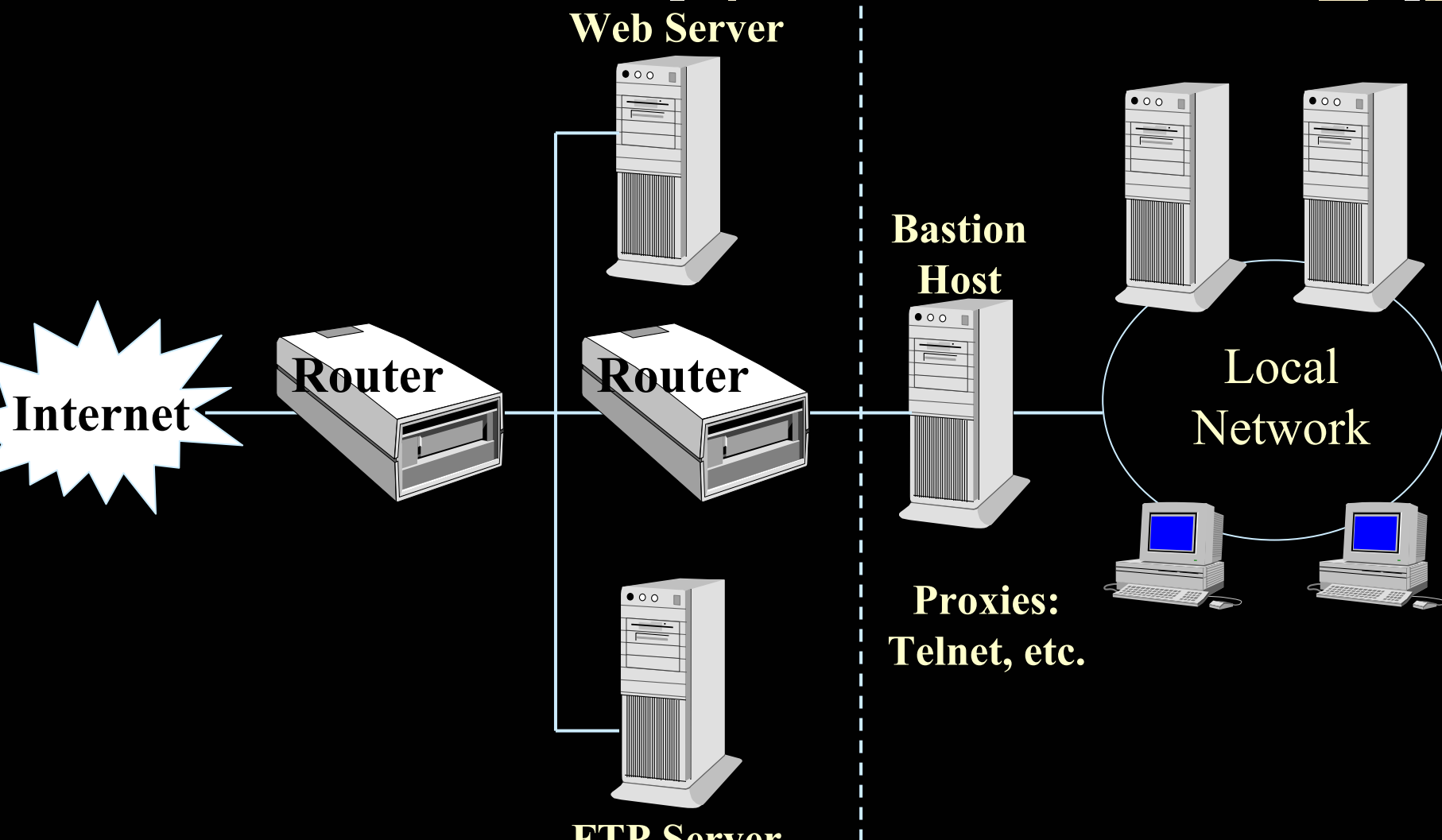
- The **most secure form** of firewalls.
- They run a small number of proxies that can be secured and trusted.
- **All incoming Internet traffic** is passed to the appropriate proxy gateway (for mail, HTTP, FTP, etc.).
- The proxies transfer the incoming information to the internal network, **based on access rights** of individual users.
- The proxy makes its decision **based on authentication**, **authorization rules** instead of IP addresses.
- The proxy's firewall address is the only one **visible** to the outside world.
- The IP addresses of your internal network are totally **invisible** to the outside world.

Combined Firewall

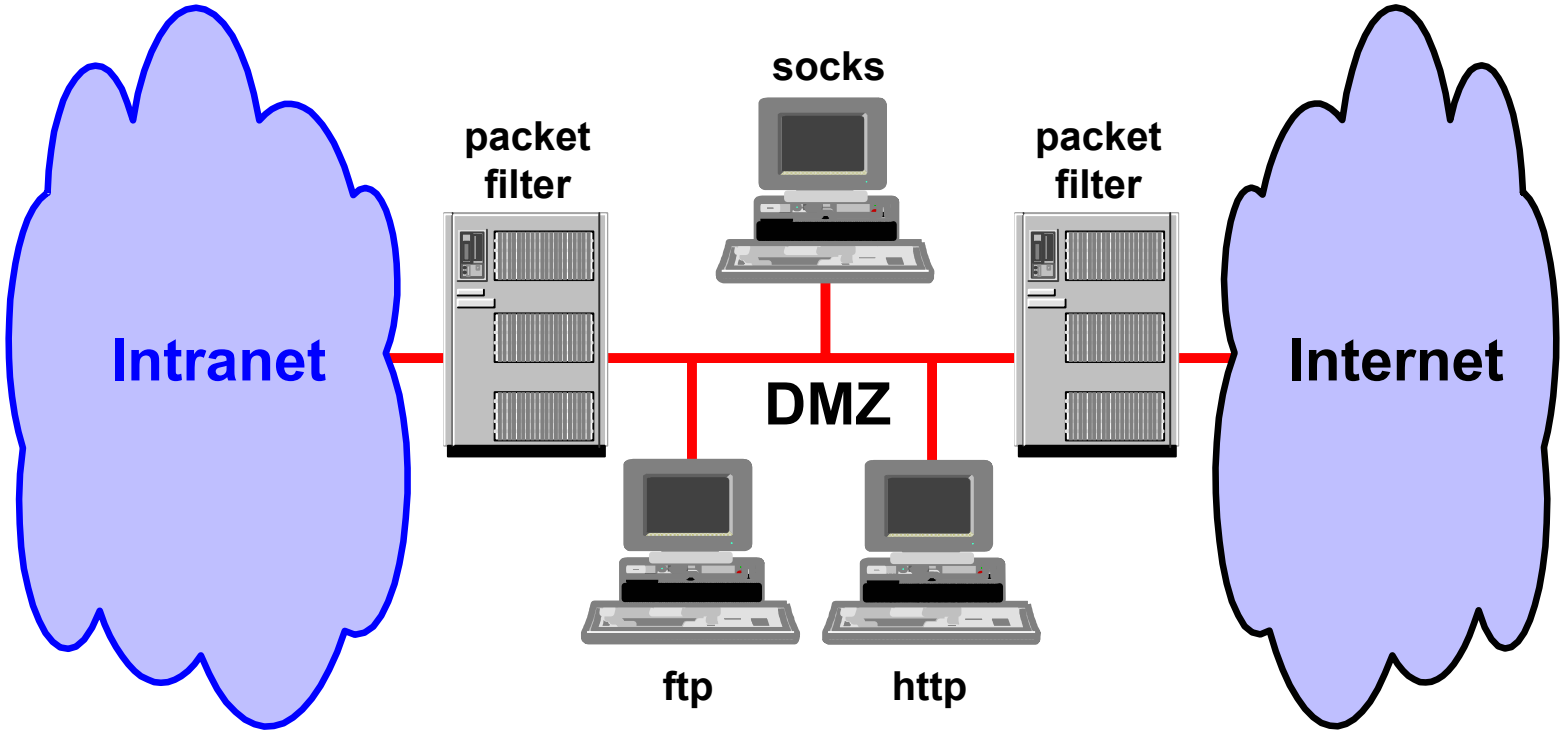


- Router is configured to only allow traffic through the bastion's IP address
- Computers on both sides of the firewall can only communicate via the bastion

Screened Subnet Firewall



Demilitarized zone (DMZ) firewall



Firewall Design Guidelines

- **Anything not explicitly permitted is denied**
- **Keep it simple: complexity is a risk**
  - No unneeded services on firewall
  - No other applications
  - No users
- **Watch those logs**
  - Integration with systems management

Virtual Private Networks (VPN)

A VPN lets organizations connect their geographically dispersed LANs via the Internet.

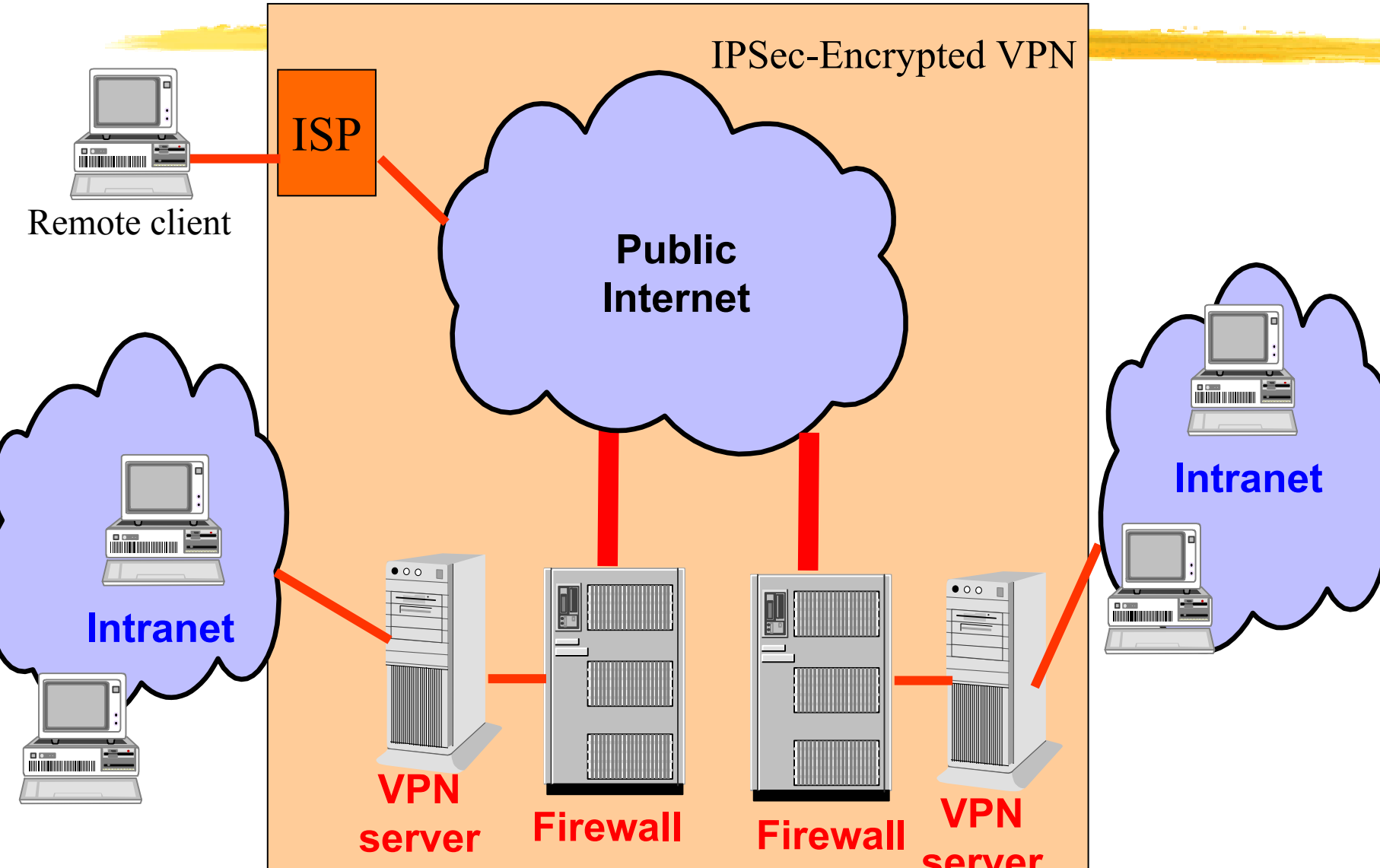
A VPN combines encryption, authentication, and protocol tunneling to provide secure transport of private communications over the public Internet.

It's as if the Internet becomes part of a larger enterprise wide area network (WAN).

A VPN user can access enterprise data by making a local call into an ISP (Internet Service Provider) rather than using a long distance phone call.

In this way, transmission costs are drastically reduced.

Structure of a VPN



Köszönöm a figyelmüket

További információ: www.lpds.sztaki.hu