Mastering TCP/IP

Chapter 9: Security

JIE B3

9.1 Overview

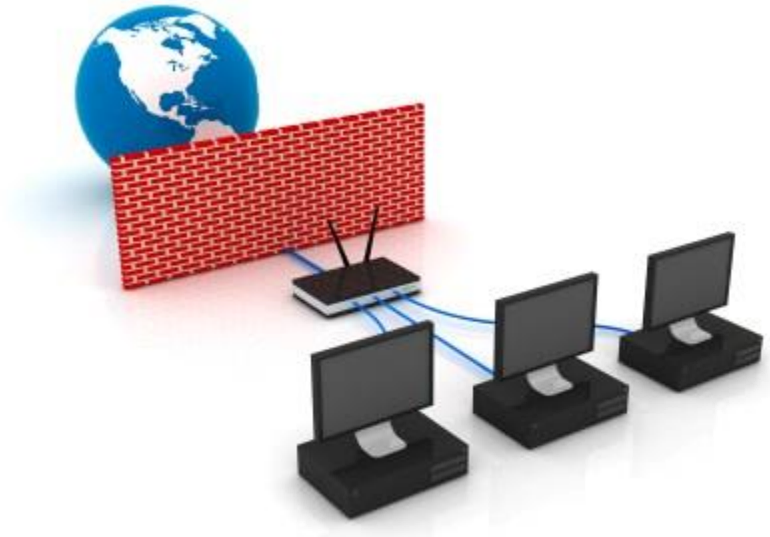
- TCP/IP was originally designed for information communication and sharing in a certain range (for limited users).
- Security’s importance grows with the diffusion of Internet.
- Conflict between convenience and security.
- Policy and technology are essential.

9.2 Security Components

- Firewall
- IDS(Intrusion Detection System)
- Anti-Virus/ Personal Firewall

9.2.1 Firewall

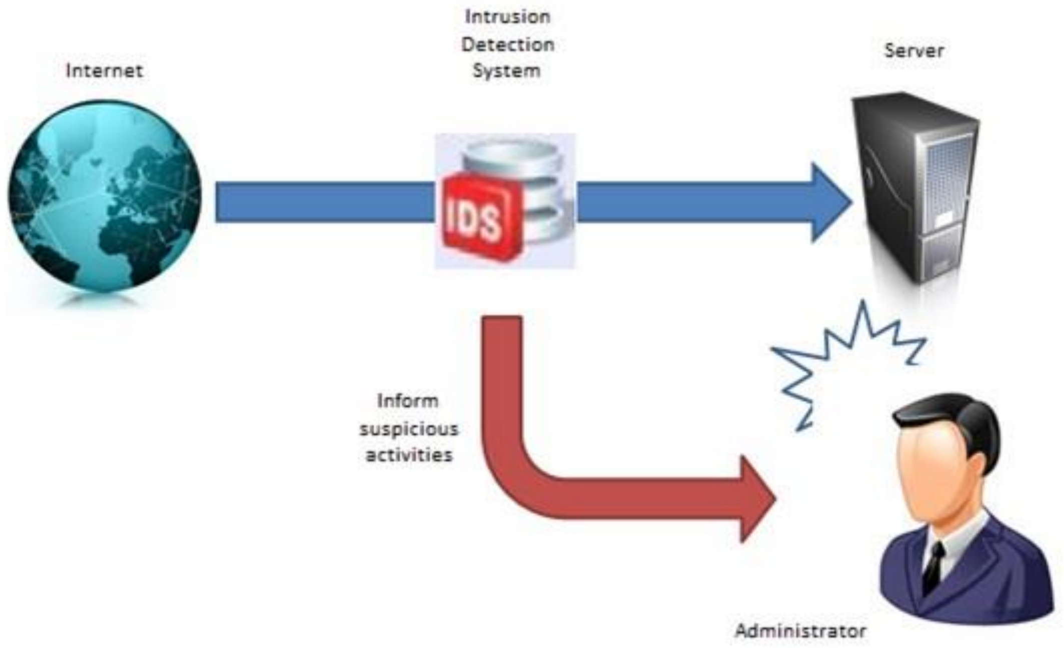
- Basic function: divide the network to different areas and make policies to filter the traffic between different networks.
- Example: Internet vs. Working Network , Mail servers , web servers
- Use case: Office, School.



https://i0.wp.com/www.ebrahma.com/wp-content/uploads/2015/04/Firewall-%E2%80%93-Basic-concepts.jpg

9.2.2 IDS

- Basic function: Real-time surveillance inside current networking.
- Advantage: Cover the mistake for firewall/ Notify users about risks.



http://www.pkfavantedge.com/wp-content/uploads/2012/12/IDS.jpg

9.2.3 Anti-virus/ Personal firewall

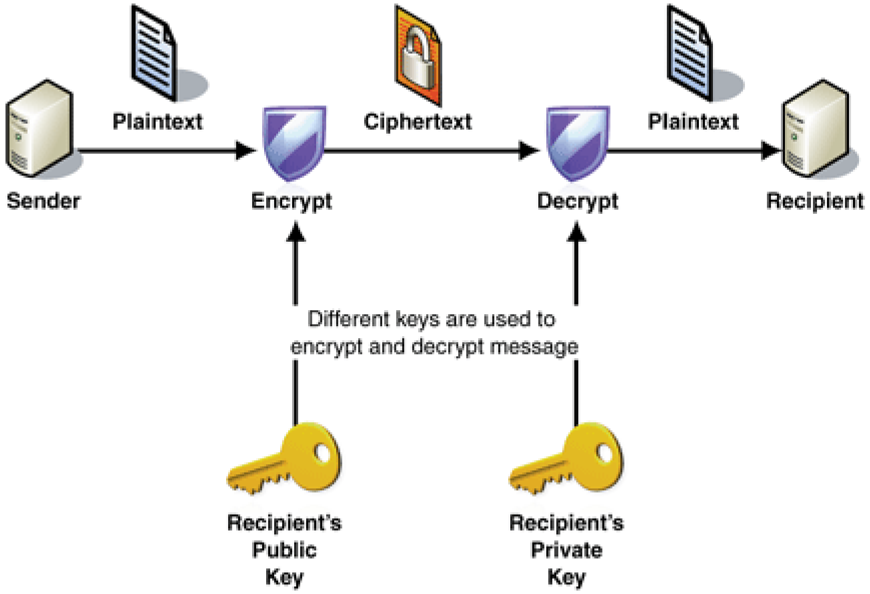
- User-side firewall
- Firewall and IDS for personal computer
- Adblock, URL filtering etc.

9.3 Encryption Technology

- Different Technology in different Internet layer and communicating with each other.
- Public Key and Common Key
- Authenticate technology

9.3.1 Public Key and Common Key

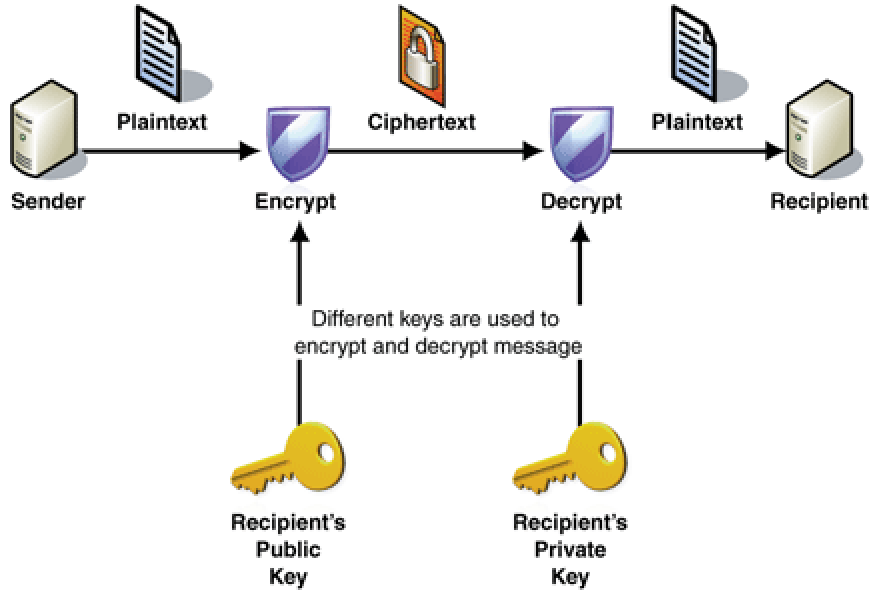
- Key – algorism for cipher and decipher
- Theory: Use key to cipher data and use key to decipher data.



https://i-msdn.sec.s-msft.com/dynimg/IC155063.gif

9.3.1 Public Key

- Key pairs: public key and private key
- Public key for ciphering and private key for deciphering



https://i-msdn.sec.s-msft.com/dynimg/IC155063.gif

9.3.1 Common Key

- One key for everything (cipher and decipher)

9.3.2 Authentication Technology

1. Knowledge factor
2. Ownership factor
3. Inherence factor

http://www.redorbit.com/media/uploads/2013/03/fingerprint-137201864.jpg

http://www.qrcodepress.com/qr-codes-provide-one-swipe-authentication-securenvoy/8528399/

9.4 Protocols for security

1. IPsec & VPN
2. TLS/SSL & HTTPS
3. IEEE802.1X

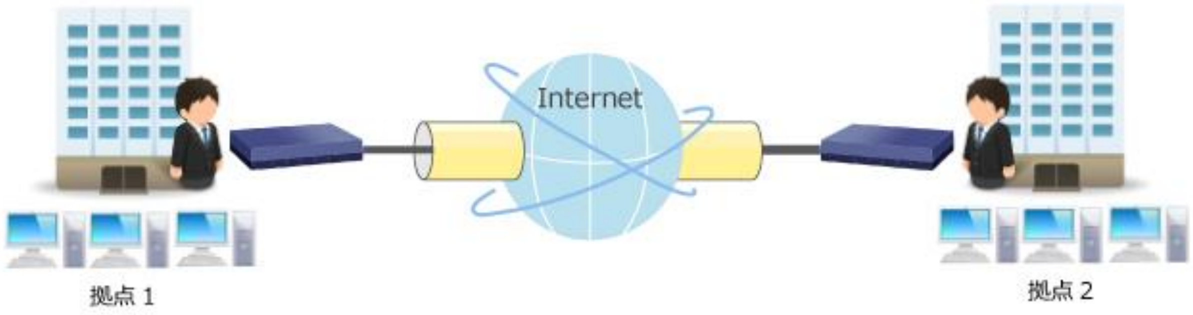
9.4.1 IPsec & VPN

VPN : a virtual private network inside public network/internet.

Private network: exclusive network for data transfer but expensive.

VPN authentication: IPsec

IPsec: data package after a certain IP header will be encrypted with ESP header and AH header and decrypted when received.



http://jp.yamaha.com/products/network/solution/wp-content/uploads/2016/05/lan_vpn.jpg

9.4.2 TLS/SSL & HTTPS

TSL/SSL: Transport Layer Security / Secure Sockets Layer

HTTPS: HTTP transport with TLS/SSL

Using Common key for data encryption

Using Public key to cipher the common key.

CA (Certificate Authority)'s certification checks the correctness of the public key.

9.4.3 IEEE802.1X

- Only allows certified device to access.
- Use case: School Wireless Network/ Home WIFI
- Authentication: MAC Address, Certification, User name and password etc.