Firewall

Vulnerability

- Wiretapping
- Modification
- Impersonation
- Interruption
- Illegal (repetitive) access trial
- Packet spoofing
- Source routing
- Modification of security policy-related data
- Defects in firewall system
- Insider or user's attack

Req't of Firewall

- Efficient implementation of security policy over network
- Easy implementation of security policy
- Cost saving of security labor
- Concentrated control
- Basic function
  - Access Control
  - Identification & Authentication
  - Logging & Audit Trail
  - Encryption (Optional) and VPN

Function(I)

Access Control

- Applying rule to packet filtering
  - IP Address
  - Service port number
  - Protocol etc.
- Access control to external network and inner network
- Feasible at router or host

Function(II)

User Authentication

- Problem of existing solutions
  - Transfer of plain password
  - Reuse of password
  - No solution against password compromised password
- New solution
  - Smart card, OTP
  - Authentication server, use biometric information
- Use strong authentication S/W or H/W

Function(III)

Audit Trail

- Need to maintain all log informations
  - All traffic must pass into firewall
  - Connection and network usage information
- Record keeping all connection informations
- Warning message to administrator
- Reuse of log information
  - Statistics of control, checking vulnerabilities
  - Setup security-enforced policy
  - Provide tracing capability

Function(IV)

Encryption & VPN

- Firewall-to-firewall connections over the internet
- Encryption of all traffics
- Provide confidentiality of information
- Provide VPN of enterprise over open network
- widespread
- Using IPSEC(IP Security)
  - Authentication Header
  - Encapsulation Security Payload Header

Function(V)

Auxiliary function

- Content screening
  - Virus screening
  - URL screening

Properties

- Keep Privacy
- Protect vulnerabilities of service
  - Access control to inside services
- Concentration of security functions
  - Embedding other security S/W into firewall
  - Authentication system, etc

Classification(I)

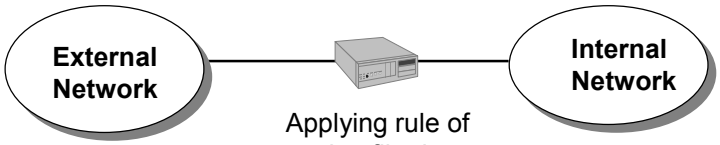
Packet Filtering

- IP Packet filtering
  - IP address of source and destination
  - TCP/UDP port address of source of destination

- Protocol filtering
  - Control of highly vulnerable services
    - tftp, RPC, rlogin, rsh, rexec, etc
  - Control on demand
    - telnet, ftp, SMTP, RIP, DNS, etc

Packet filtering

- Exist between network segments
- Check all transferring traffic
- The increasing number of segment causes complex and performance degradation.

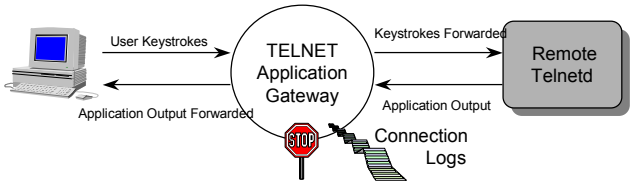


Applying rule of packet filtering.

Classification(II)

Application Gateway

- Use store-and-forward for sending traffic
- Some types of interactive traffic



Application Gateway

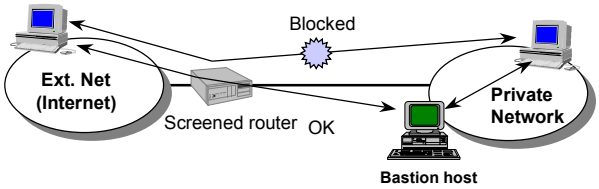
- Control traffic at application layer
- Fully understanding of protocol in application program
- Loging and auditing of all traffic
- Application Gateways can have extra security or authorization built into them as needed
- Examples
  - Telnet Gateway
  - FTP Gateway

Hybrid

- Combing application gateway and packet filtering types

Configuration

- Screened host
  - Single-homed bastion host
  - Dual-homed bastion host
- Screened subnet



Screened Host Gateway

- Most popular firewall configuration
- Consists of screening router and one bastion host
- Outgoing access granted by only Bastion Host
- Packet filtering on screening router
  - Allows incoming and outgoing traffics only to Bastion host
- Easy implementing security policy to external network
  - Direct access to external network
  - Access thru bastion host