Firewalls I

By Prof. Hesham Abusaimeh

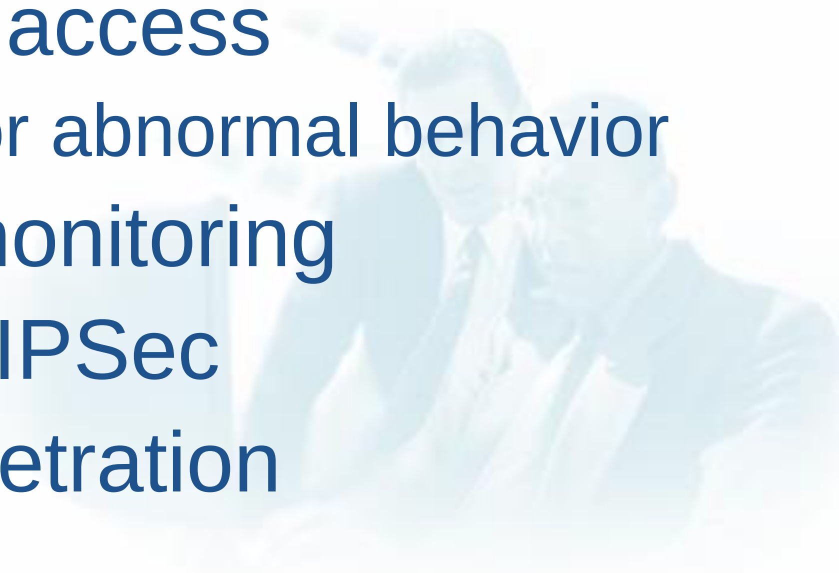
MEU

Introduction

- seen evolution of information systems
- now everyone want to be on the Internet
- and to interconnect networks
- has persistent security concerns
  - can’t easily secure every system in org
- typically use a **Firewall**
- to provide **perimeter defence**
- as part of comprehensive security strategy

What is a Firewall?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
  - only authorized traffic is allowed
- auditing and controlling access
  - can implement alarms for abnormal behavior
- provide NAT & usage monitoring
- implement VPNs using IPSec
- must be immune to penetration



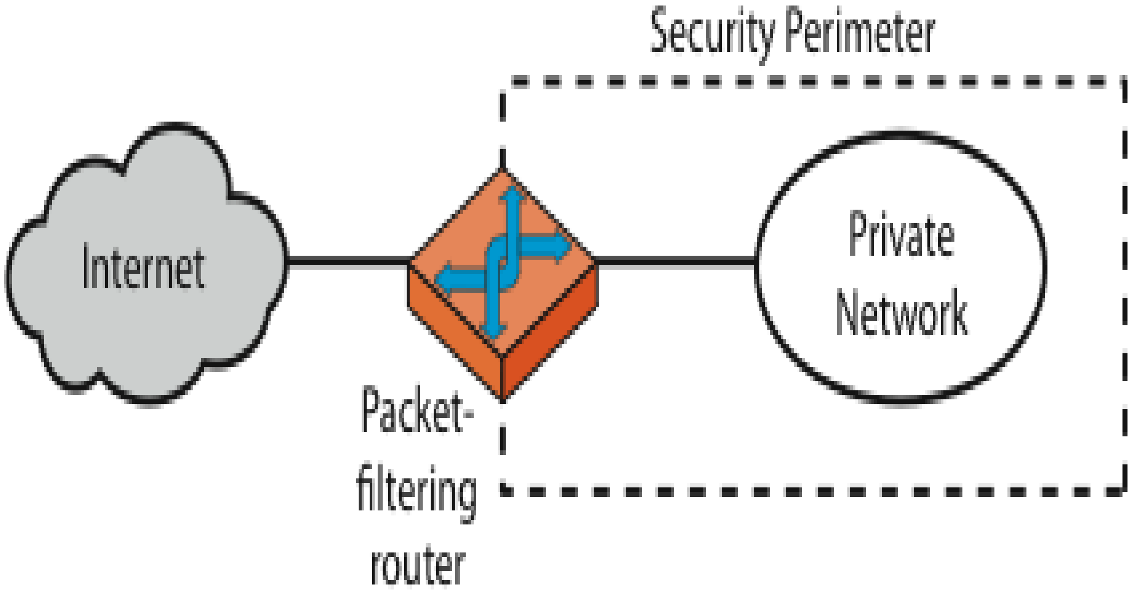
Firewall Limitations

- cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - eg disgruntled or colluding employees
- cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

Firewalls – Packet Filters

- simplest, fastest firewall component
- foundation of any firewall system
- examine each IP packet (no context) and permit or deny according to rules
- hence restrict access to services (ports)
- possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

Firewalls – Packet Filters



(a) Packet-filtering router

Firewalls – Packet Filters

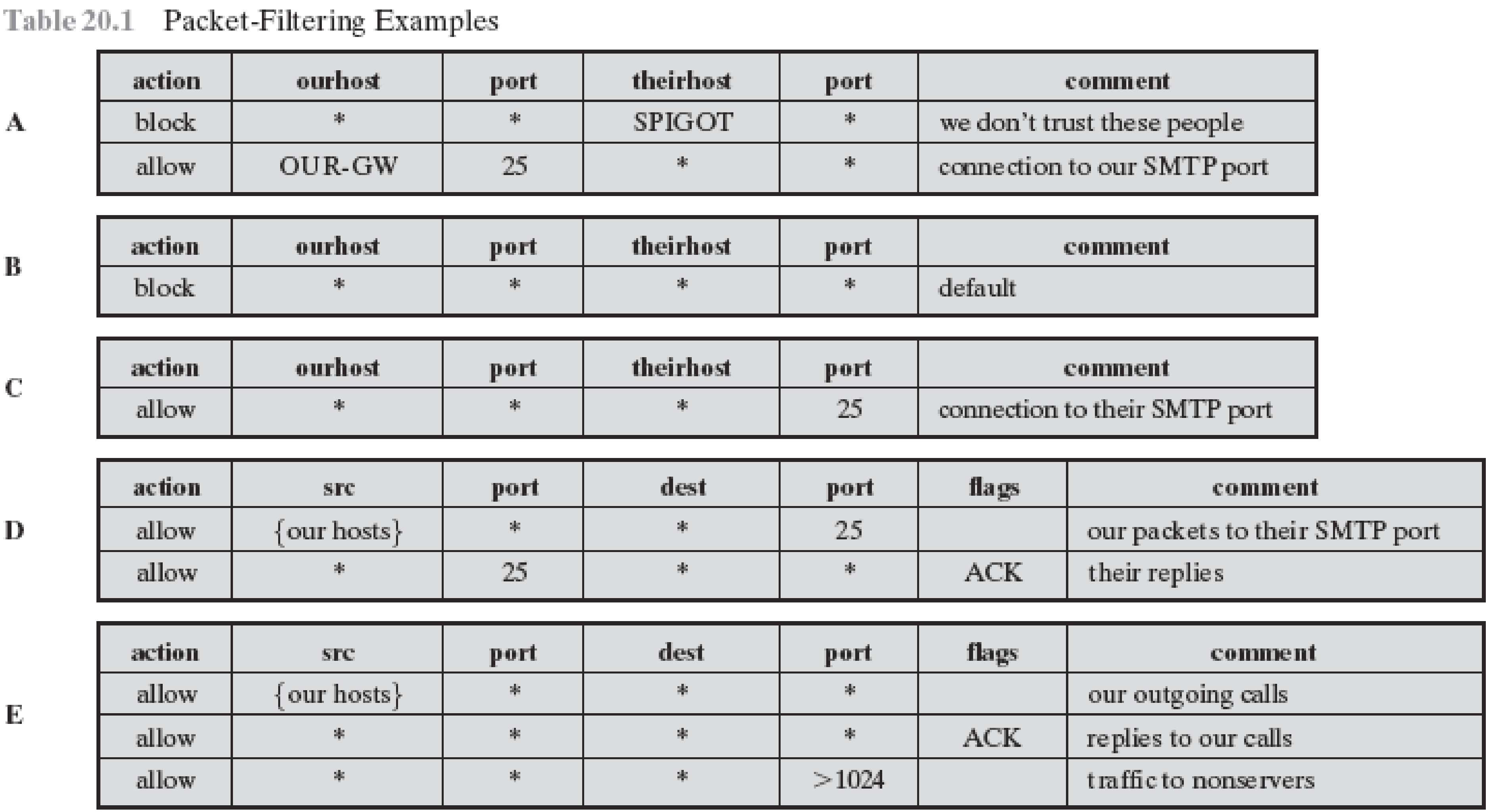


Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don’t trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

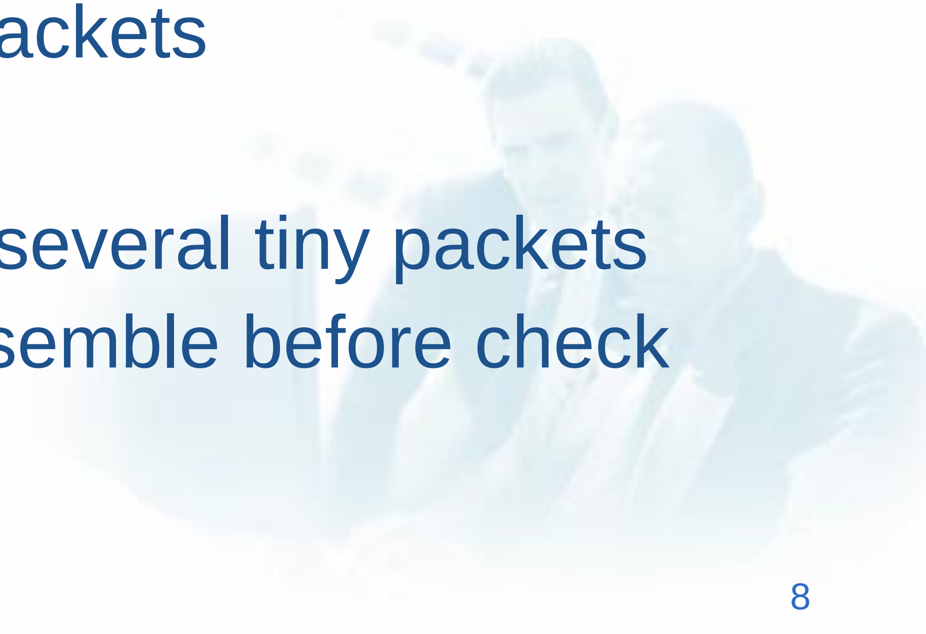
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Attacks on Packet Filters

- IP address spoofing
  - fake source address to be trusted
  - add filters on router to block
- source routing attacks
  - attacker sets a route other than default
  - block source routed packets
- tiny fragment attacks
  - split header info over several tiny packets
  - either discard or reassemble before check



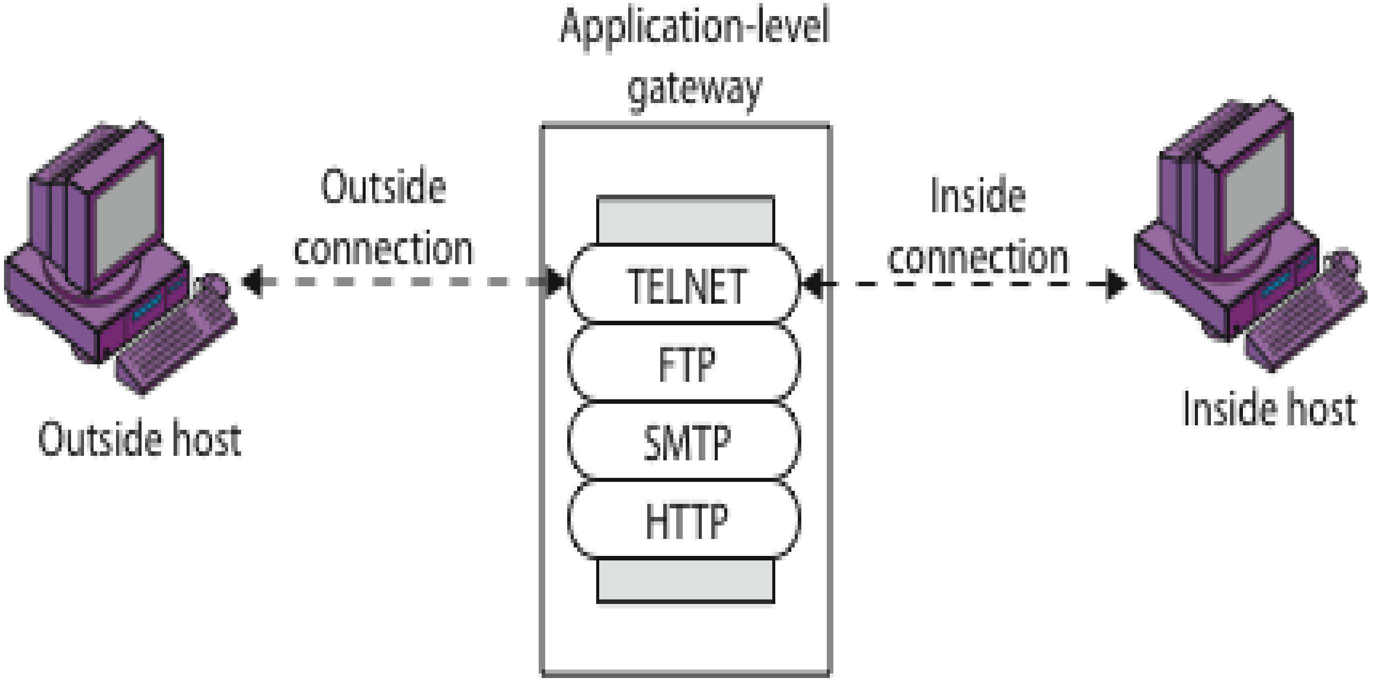
Firewalls – Stateful Packet Filters

- traditional packet filters do not examine higher layer context
  - ie matching return packets with outgoing flow
- stateful packet filters address this need
- they examine each IP packet in context
  - keep track of client-server sessions
  - check each packet validly belongs to one
- hence are better able to detect bogus packets out of context

Firewalls - Application Level Gateway (or Proxy)

- have application specific gateway / proxy
- has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
  - can log / audit traffic at application level
- need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic

Firewalls - Application Level Gateway (or Proxy)

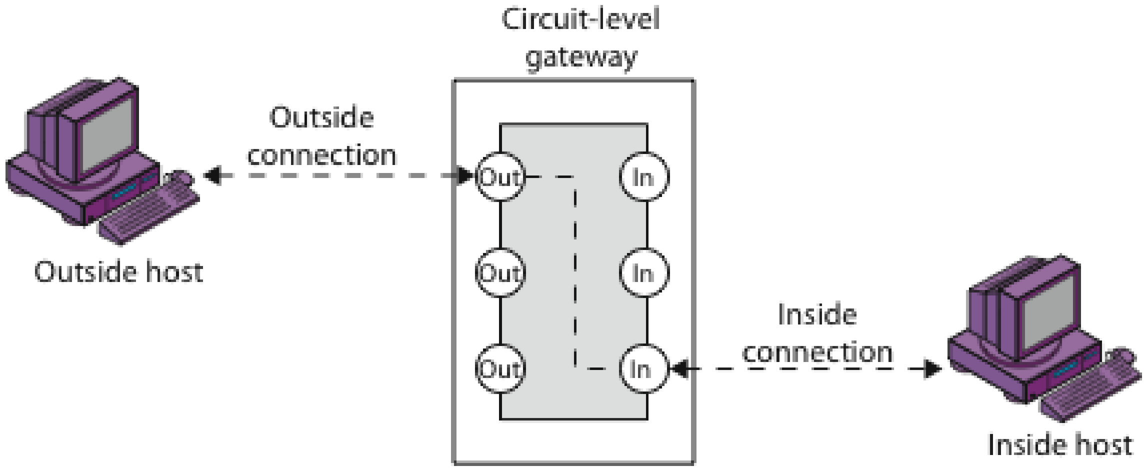


(b) Application-level gateway

Firewalls - Circuit Level Gateway

- relays two TCP connections
- imposes security by limiting which such connections are allowed
- once created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections
- SOCKS is commonly used

Firewalls - Circuit Level Gateway

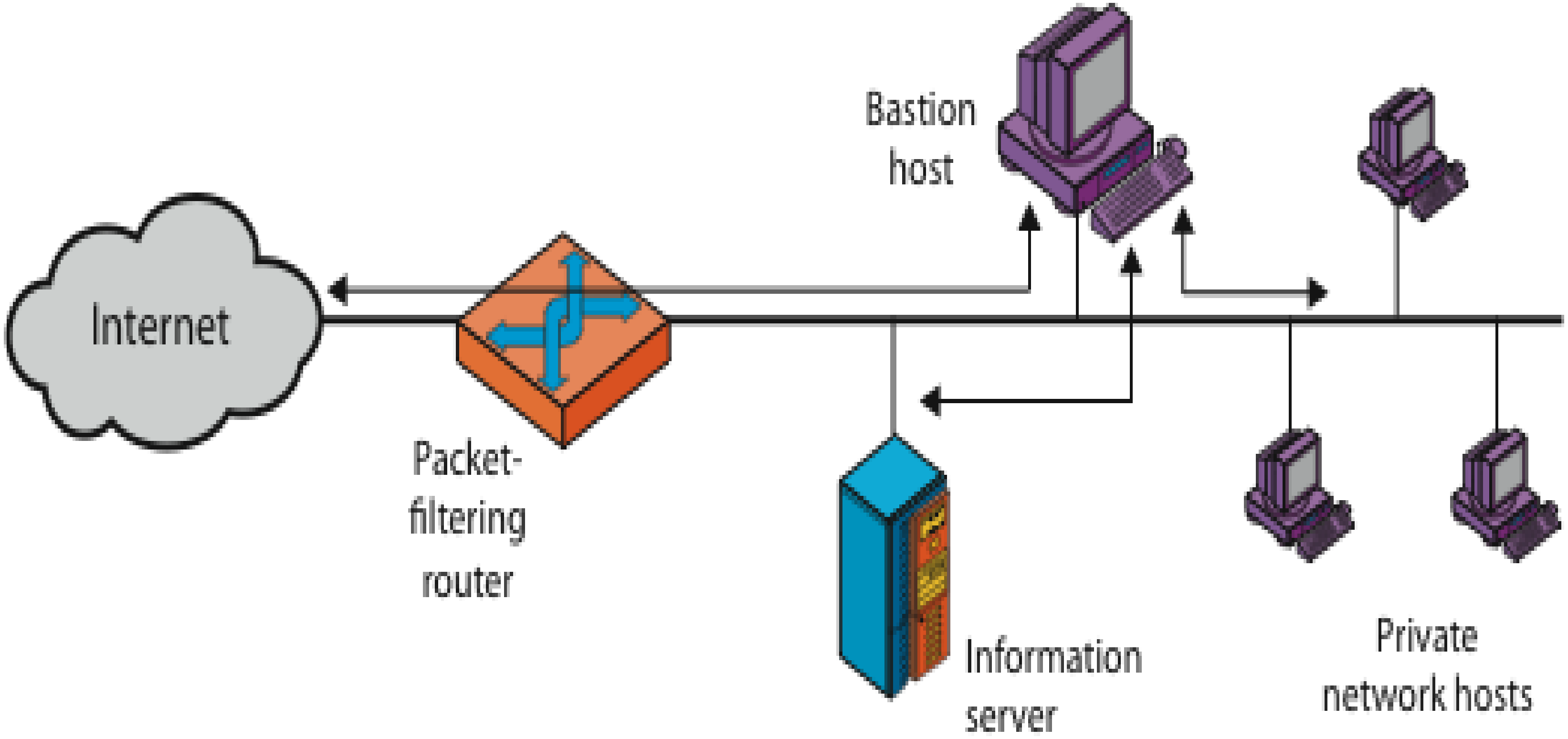


(c) Circuit-level gateway

Bastion Host

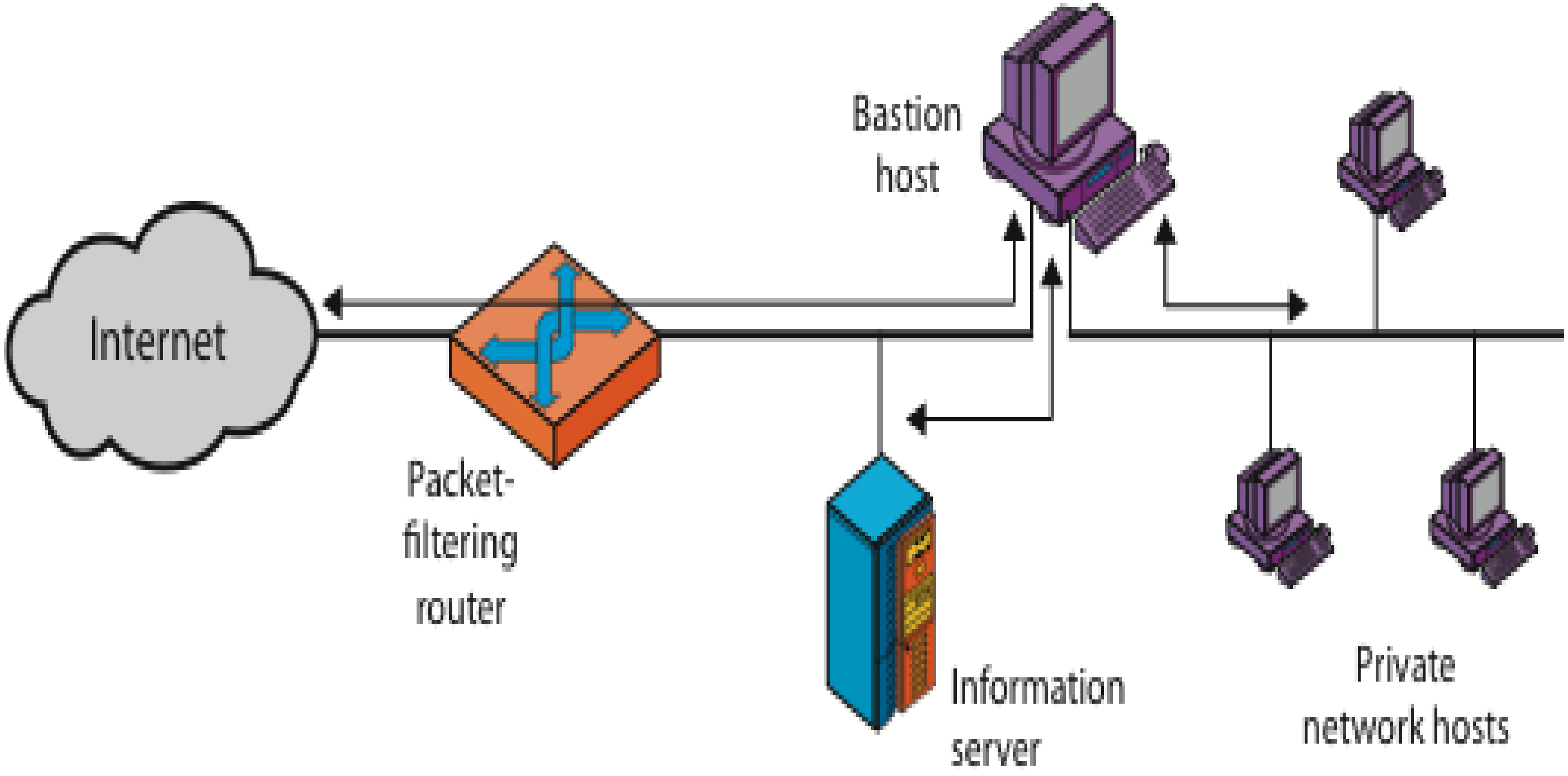
- highly secure host system
- runs circuit / application level gateways
- or provides externally accessible services
- potentially exposed to "hostile" elements
- hence is secured to withstand this
  - hardened O/S, essential services, extra auth
  - proxies small, secure, independent, non-privileged
- may support 2 or more net connections
- may be trusted to enforce policy of trusted separation between these net connections

Firewall Configurations



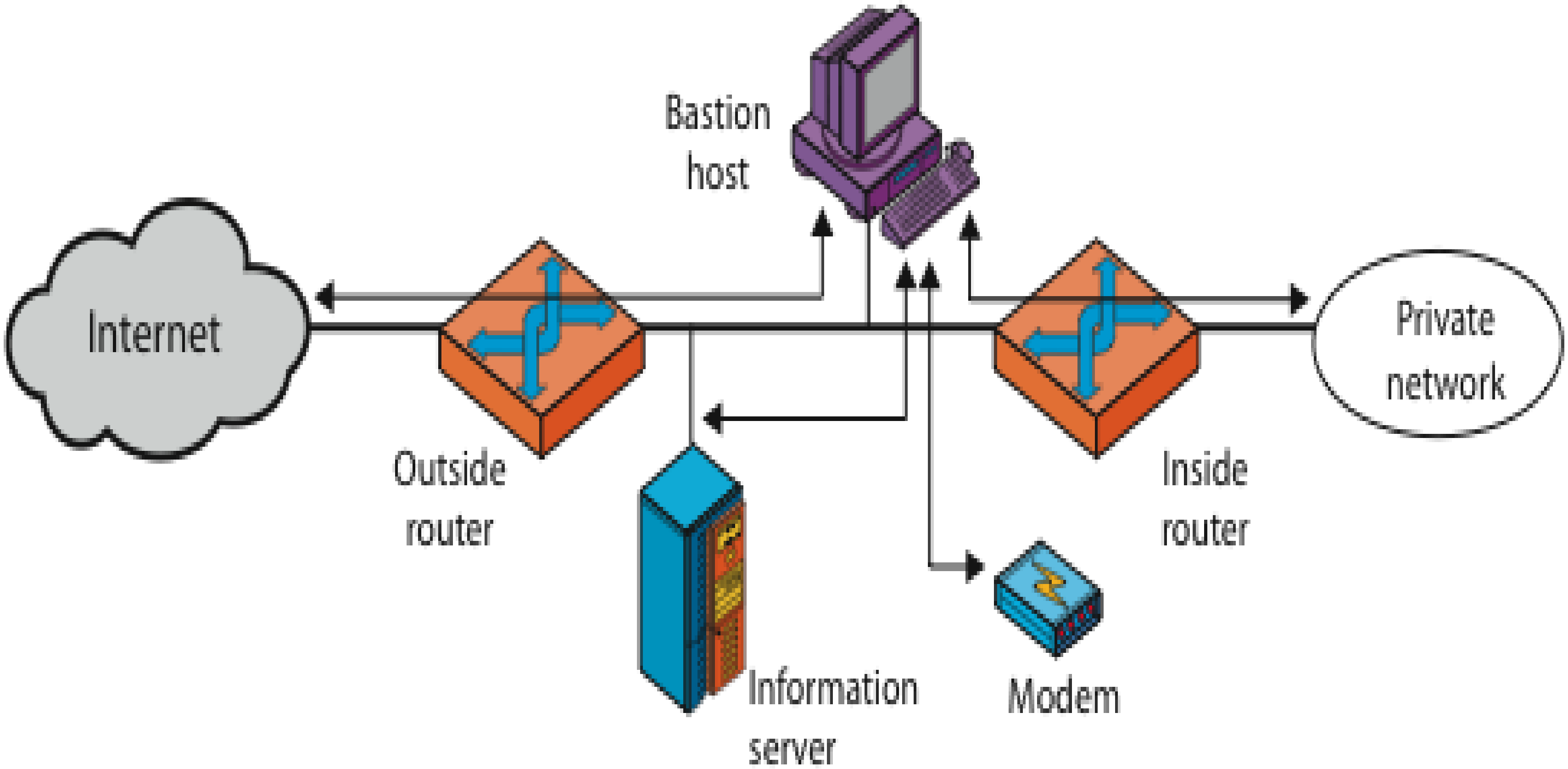
(a) Screened host firewall system (single-homed bastion host)

Firewall Configurations



(b) Screened host firewall system (dual-homed bastion host)

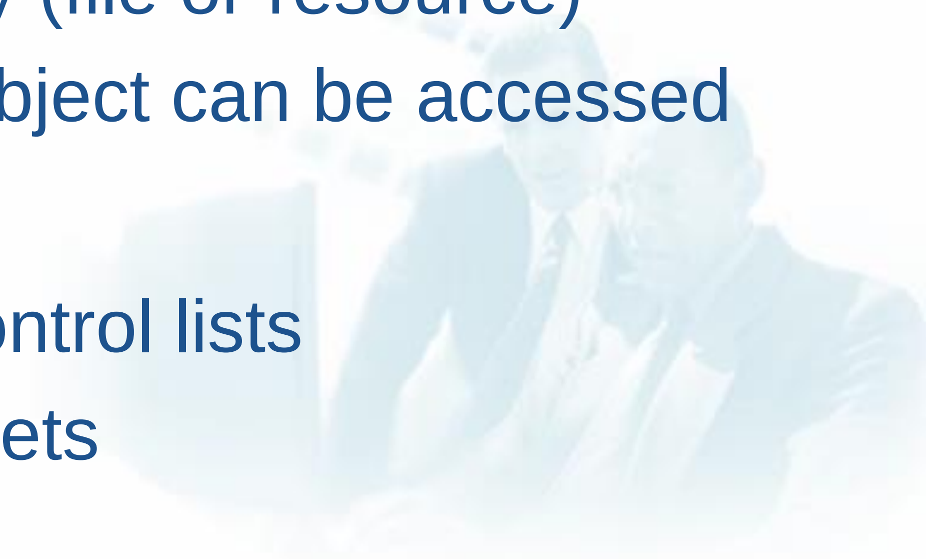
Firewall Configurations



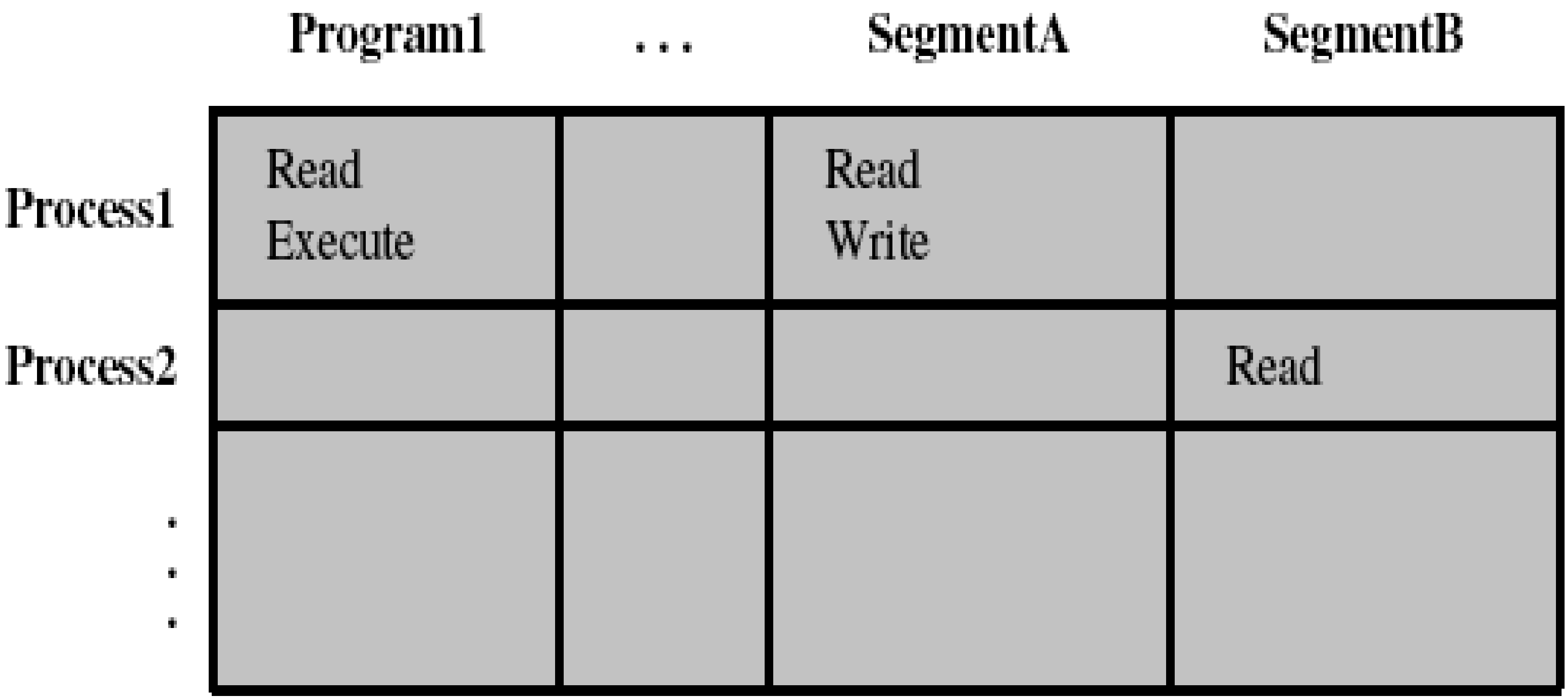
(c) Screened-subnet firewall system

Access Control

- given system has identified a user
- determine what resources they can access
- general model is that of access matrix with
  - **subject** - active entity (user, process)
  - **object** - passive entity (file or resource)
  - **access right** – way object can be accessed
- can decompose by
  - columns as access control lists
  - rows as capability tickets



Access Control Matrix



	Program1	. . .	SegmentA	SegmentB
Process1	Read Execute		Read Write	
Process2				Read
⋮				

(a) Access matrix

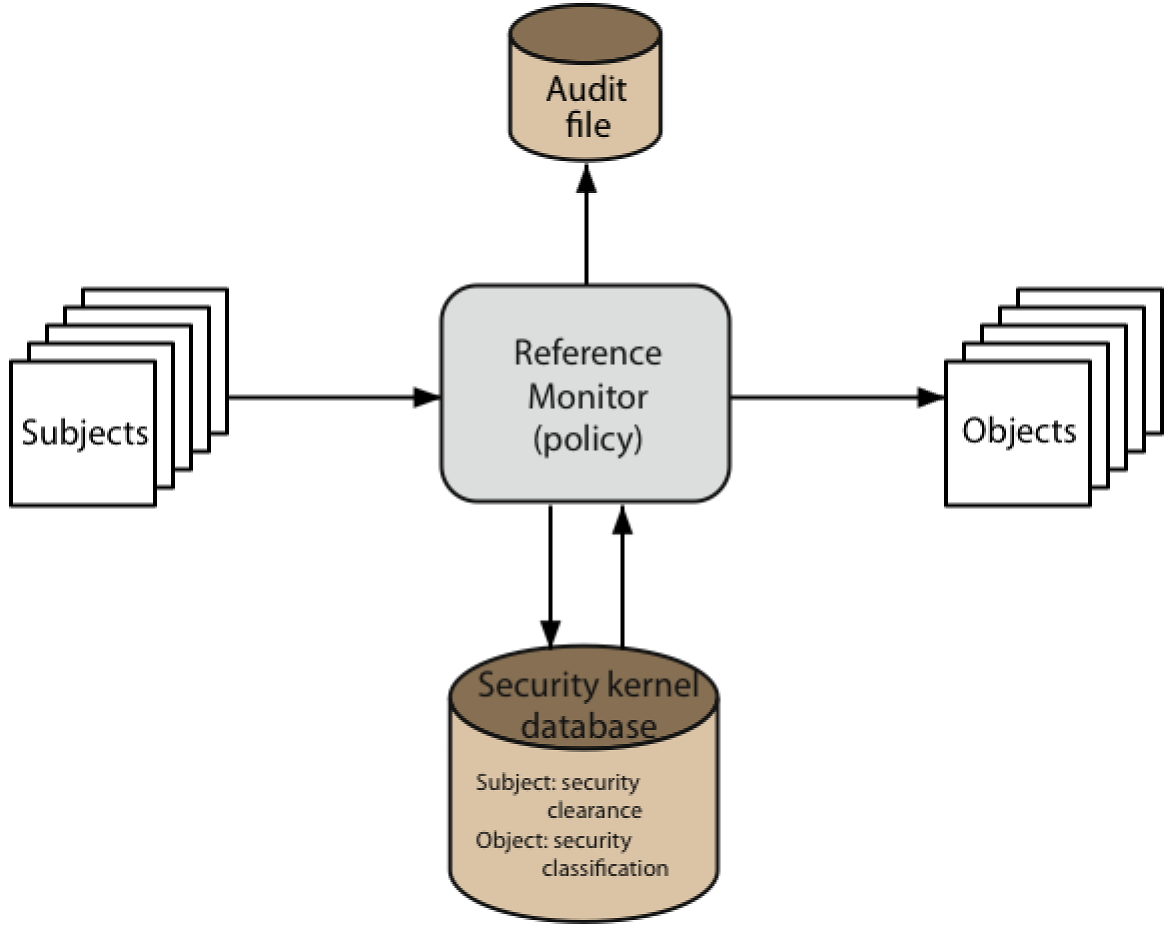
Trusted Computer Systems

- information security is increasingly important
- have varying degrees of sensitivity of information
  - cf military info classifications: confidential, secret etc
- subjects (people or programs) have varying rights of access to objects (information)
- known as multilevel security
  - subjects have **maximum** & **current** security level
  - objects have a fixed security level **classification**
- want to consider ways of increasing confidence in systems to enforce these rights

Bell LaPadula (BLP) Model

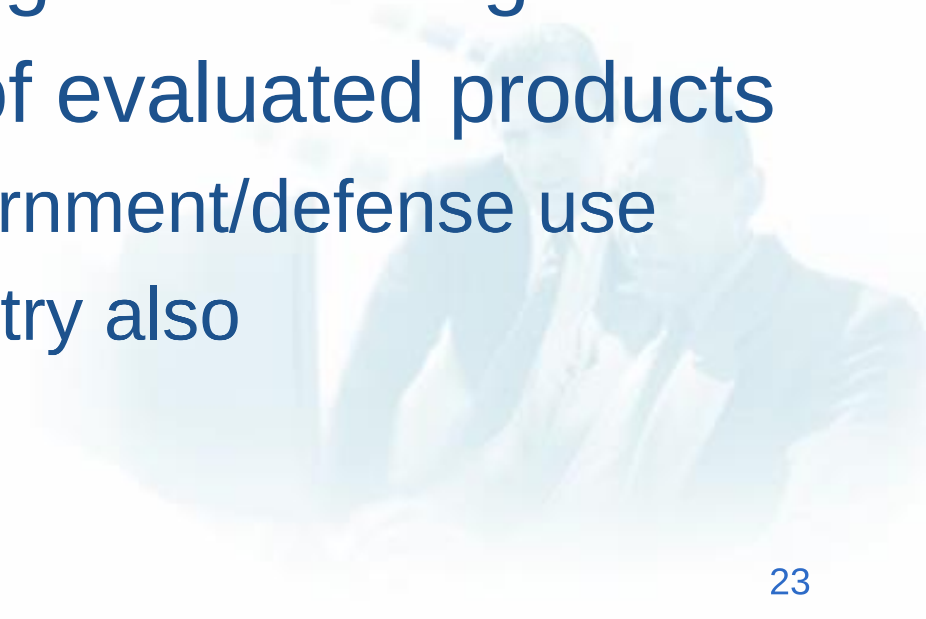
- one of the most famous security models
- implemented as mandatory policies on system
- has two key policies:
- **no read up** (simple security property)
  - a subject can only read/write an object if the current security level of the subject dominates (>=) the classification of the object
- **no write down** (*-property)
  - a subject can only append/write to an object if the current security level of the subject is dominated by (<=) the classification of the object

Reference Monitor


Audit file
Subjects
Reference Monitor (policy)
Objects
Security kernel database
Subject: security clearance
Object: security classification

Evaluated Computer Systems

- governments can evaluate IT systems
- against a range of standards:
  - TCSEC, IPSEC and now Common Criteria
- define a number of “levels” of evaluation with increasingly stringent checking
- have published lists of evaluated products
  - though aimed at government/defense use
  - can be useful in industry also



Common Criteria

- international initiative specifying security requirements & defining evaluation criteria
- incorporates earlier standards
  - eg CSEC, ITSEC, CTCPEC (Canadian), Federal (US)
- specifies standards for
  - evaluation criteria
  - methodology for application of criteria
  - administrative procedures for evaluation, certification and accreditation schemes

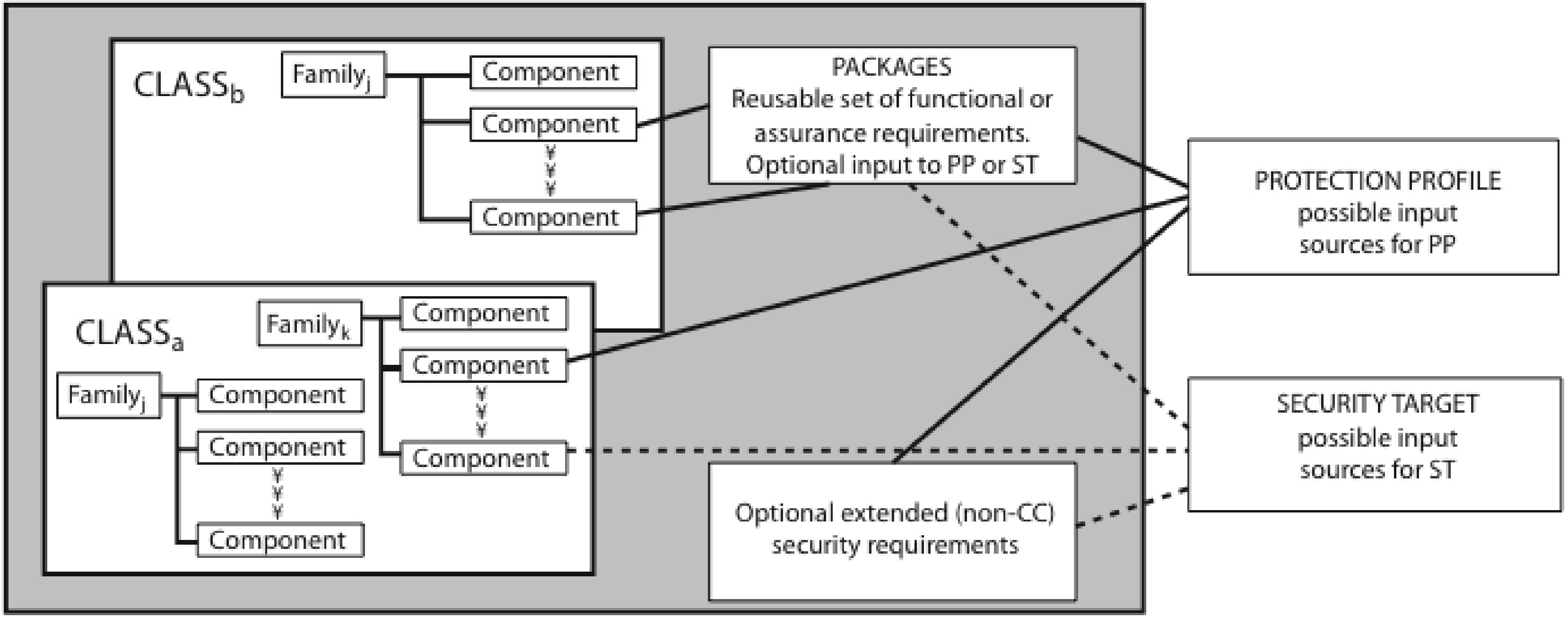
Common Criteria

- defines set of security requirements
- have a Target Of Evaluation (TOE)
- requirements fall in two categories
  - functional
  - assurance
- both organised in classes of families & components

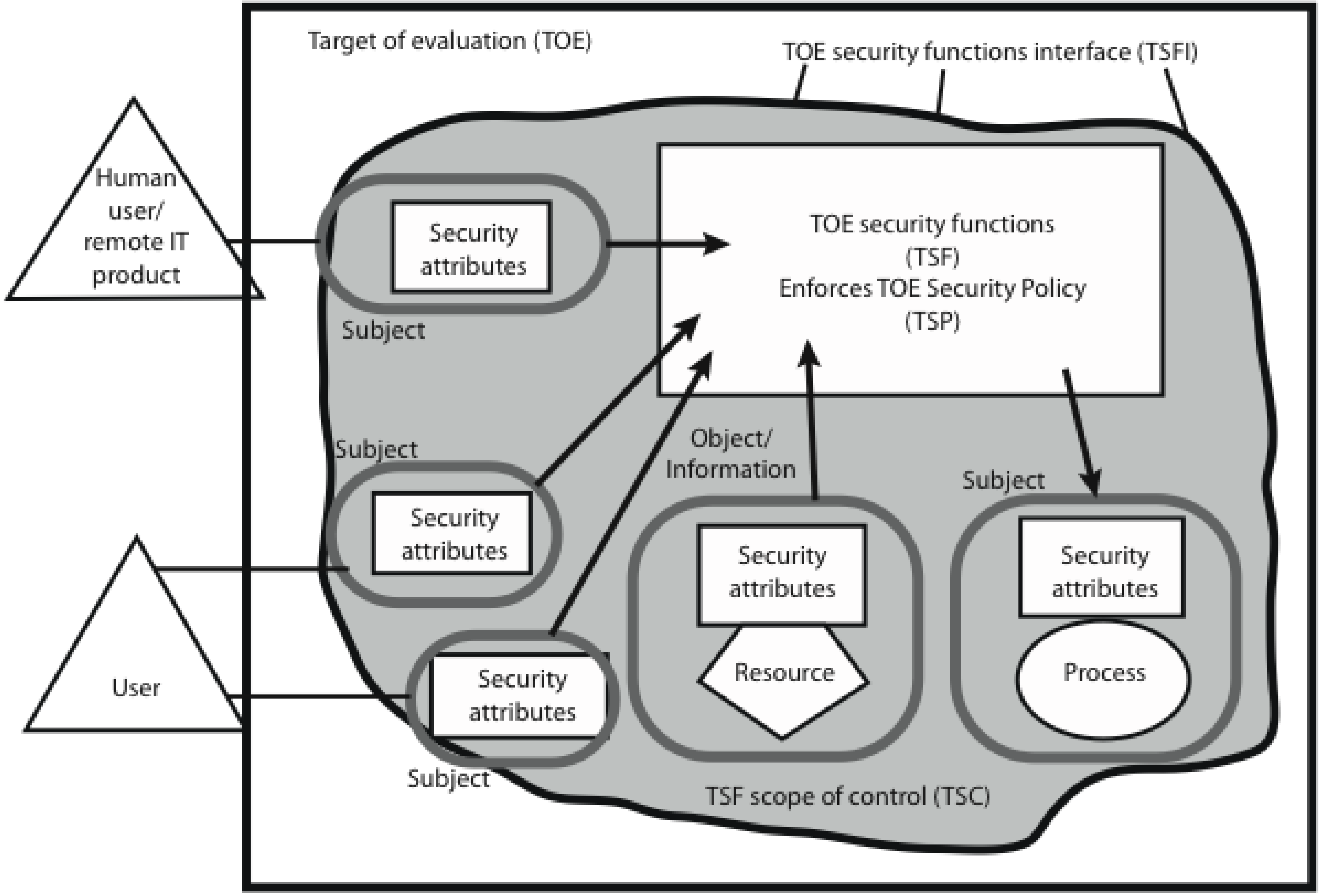
Common Criteria Requirements

- Functional Requirements
  - security audit, crypto support, communications, user data protection, identification & authentication, security management, privacy, protection of trusted security functions, resource utilization, TOE access, trusted path
- Assurance Requirements
  - configuration management, delivery & operation, development, guidance documents, life cycle support, tests, vulnerability assessment, assurance maintenance

Common Criteria



Common Criteria


Target of evaluation (TOE)
TOE security functions interface (TSFI)
Human user/ remote IT product
Security attributes
Subject
TOE security functions (TSF)
Enforces TOE Security Policy (TSP)
Subject
Security attributes
Object/ Information
Subject
User
Security attributes
Resource
Security attributes
Process
Security attributes
Subject
TSF scope of control (TSC)

Summary

- have considered:
  - firewalls
  - types of firewalls
  - configurations
  - access control
  - trusted systems
  - common criteria