Firewall Management

Rangga Firdaus, M.Kom

Identitas Diri

Nama : Rangga Firdaus, M.Kom
NIP : 197410102008011015

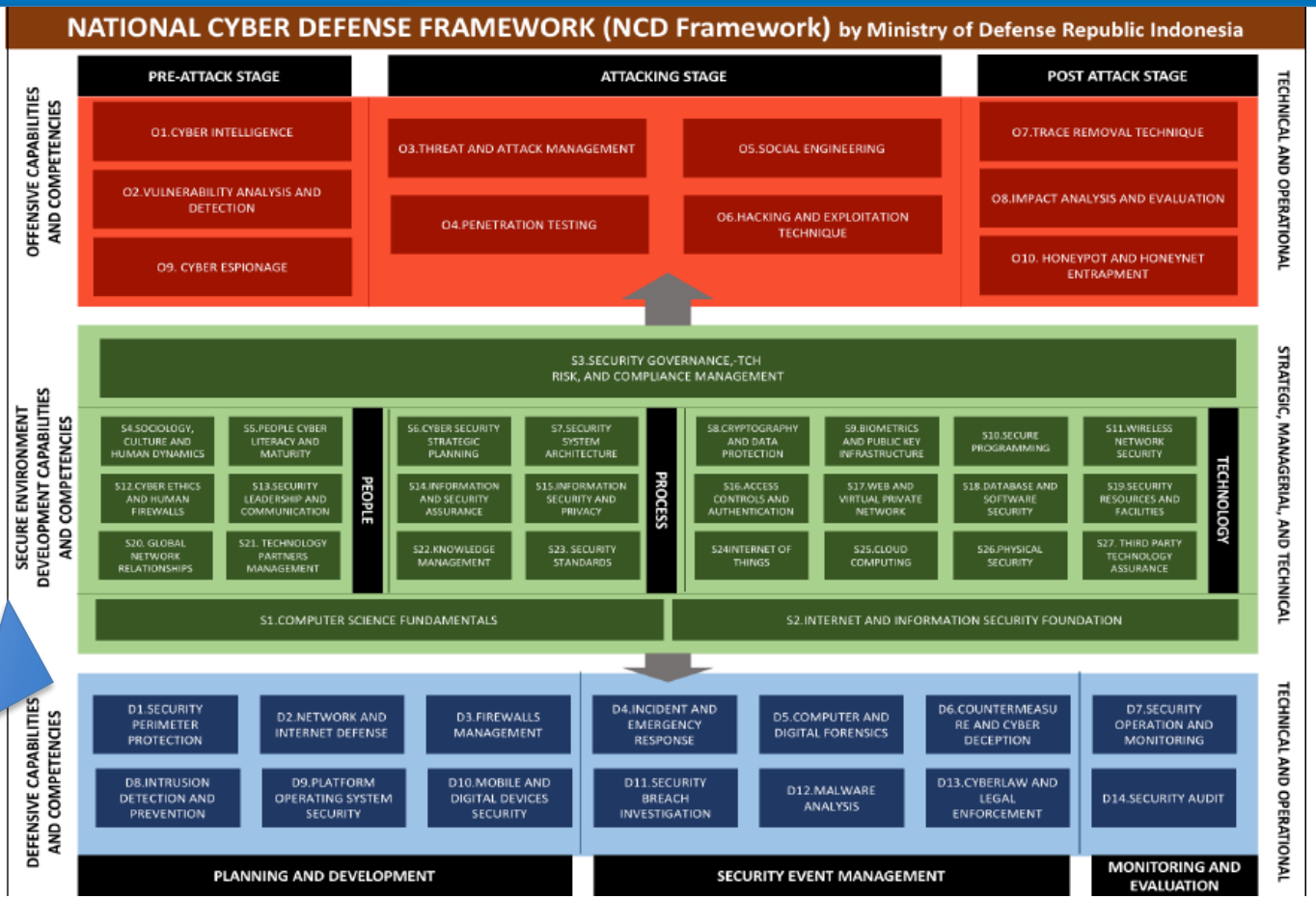
Pendidikan
S1 Teknik Komputer Univ Gunadarma Jakarta
S2 Ilmu Komputer Univ Gadjah Mada Yogykarta
S3 Teknologi Pendidikan Univ Negeri Jakarta (Progress)

Aktivitas :

- Dosen Ilmu Komputer FMIPA **Universitas Lampung**
- Tim Pembelajaran Daring Indonesi Terbuka dan Terpadu – **Kemenristek Dikti**, Belmawa
- Direktur Pengembangan Wilayah dan Sertifikasi Ikatan Ahli Informatika Indonesia (**IAII**)
- Direktur Konferensi Seminar Asosiasi Pendidikan Tinggi Informatik dan Komputer (**APTIKOM**)
- Koordinator Ikatan Alumni TOT **LEMHANNAS** RI Wilayah Sumatera Bagian Selatan
- Asesor Kompetensi Bidang Informatika , **Lembaga Sertifikasi Profesi Informatika** - BNSP

❖ Pemahaman yang baik, akan menimbulkan aktivitas yang baik, niatkan karena Allah.. Menjadi amal ibadah , Manjada Wajadda !

NCD Framework



- **3 KOMPETENSI 1.Security Perimeter Protection**
  2. Network and Internet Defense
  3. Firewall Management

POINT PENTING

WHAT(T)

WHY (Y)

WHERE (E)

WHEN (N)

WHO (O)

HOW (W)

5.1 (D1) Security Perimeter Protection (D2) Network And Internet Defense (D3) Firewall Management

5.1.1 WHAT(T)

- (D1T-1) Menjelaskan apa yang dimaksud dengan **D1 D2 D3**
- (D1T-2) Mengidentifikasi komponen-komponen pada **D1 D2 D3**

5.1.2 WHY (Y)

- (D1Y-1) Mengemukakan alasan diperlukannya **D1 D2 D3**
- (D1Y-2) Memberikan contoh keuntungan yang diperoleh dari keberadaan **D1 D2 D3**
- (D1Y-3) Memberikan contoh kerugian yang diperoleh jika tidak memiliki **D1 D2 D3**

5.1.3 WHERE (E)

• (D1E-1) Menjelaskan unit organisasi yang bertanggung jawab dalam mengembangkan Security Perimeter Protection

• (D1E-2)Menjelaskan batasan teritori organisasi yang terikat atau harus patuh terhadap Security Perimeter Protection

5.1.4 WHEN (N)

• (D1N-1) Menjelaskan waktu yang tepat bagi sebuah organisasi untuk menyusun Security Perimeter Protection

• (D1N-2) Menyusun jadwal proses penyusunan Security Perimeter Protection

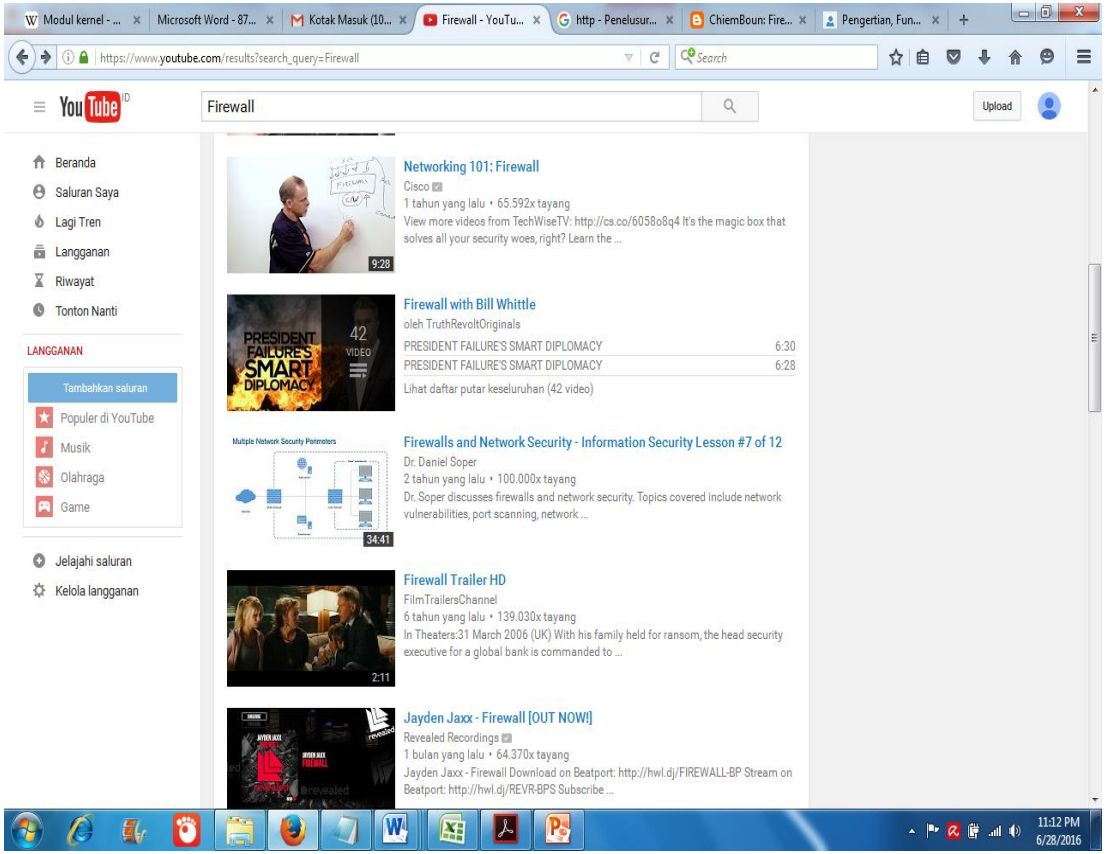
5.1.5 WHO (O)

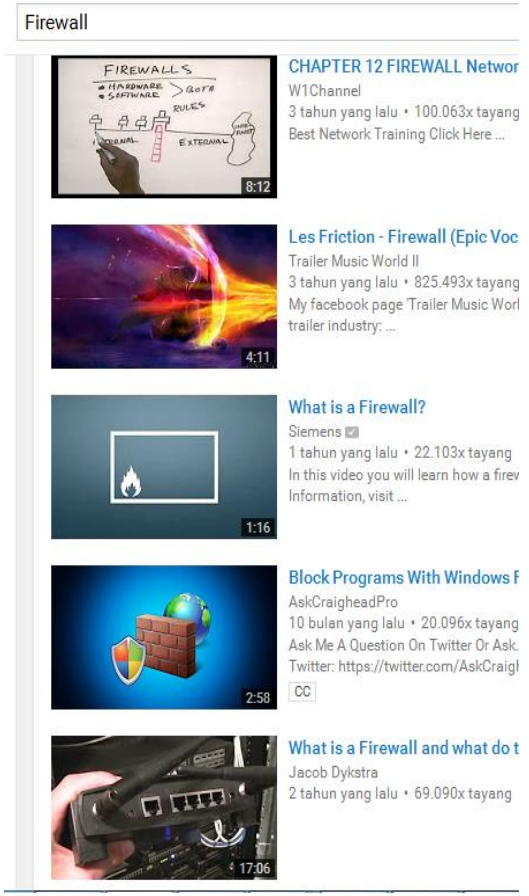
- (D1O-1) Mengidentifikasi individu atau pihak yang bertanggung jawab dalam menyusun **D1 D2 D3**
- (D1O-2) Menetapkan peranan, tugas, dan tanggung jawab individu dan pihak-pihak yang harus terlibat dalam penyusunan **D1 D2 D3** dalam sebuah organisasi

5.1.6 HOW (W)

- (D1W-1) Menggambarkan metodologi pengembangan **D1 D2 D3**
- (D1W-2) Menjelaskan langkah-langkah yang harus dilakukan dalam menyusun **D1 D2 D3**
- (D1W-3) Menjelaskan rangkaian aktivitas yang harus dilakukan pada setiap langkah pada metodologi penyusunan **D1 D2 D3**

CONTOH IMPLEMENTASI D1 D2 D3





(D1) Security Perimeter Protection
(D2) Network And Internet Defense
(D3) Firewall Management

Overview

- Why Computers Need to Protect?
- What is a Firewall?
- Need of Firewall
- Firewall Design Principles
- Firewall Characteristics
- Software Vs. Hardware Firewall
- Where Can You Place a Firewall
- How Does a Firewall Work?
- Firewall Rules
- Methods to Attack or View Computer Data
- Architecture of Firewall
- Packet Filtering Router
- Stateful Packet Inspections
- Application Level Firewalls
  - Common Proxy Services
- Content Filtering
- Virtual Private Networks
- Firewall Configurations
  - Dual Homed Gateway
  - Screen Host Gateway
  - Double Proxying and DMZ
- Distributed Firewall
  - KeyNote
- Making the Firewall Fit
- What it Protect you From
- Security Strategies Implemented
- Testing Firewall Configuration
- Implementations of Firewall
- Firewall Deployment
- Firewall Security Operations
- Defining Audit Scope
- Firewall Auditing Methodology
- What a Firewall Can Do?
- What a Firewall Can't Do?
- Future of Firewalls
- Conclusions

Firewall Management

Why Computers Need to Protect?

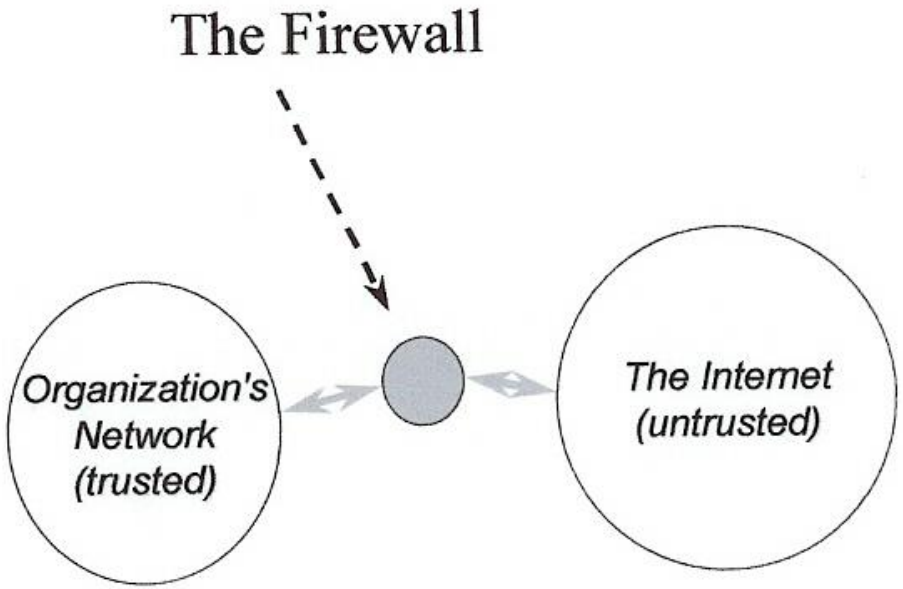
- If a home or business computer owner bounds to a network or an internet connection, their personal datas open to reach unauthorized person who have a connection a network or an internet.

- This situation will become harder to protect data security than to provide local area network or internet data security. Because, a system of computer how much having strong external relations, it will become more undefend system.

- Also,it is exposed to spies, thieves, hackers, thrill seekers, or various.So that, users need to be increasingly vigilant of security issues.

❖ “AMAN dari segala hal !

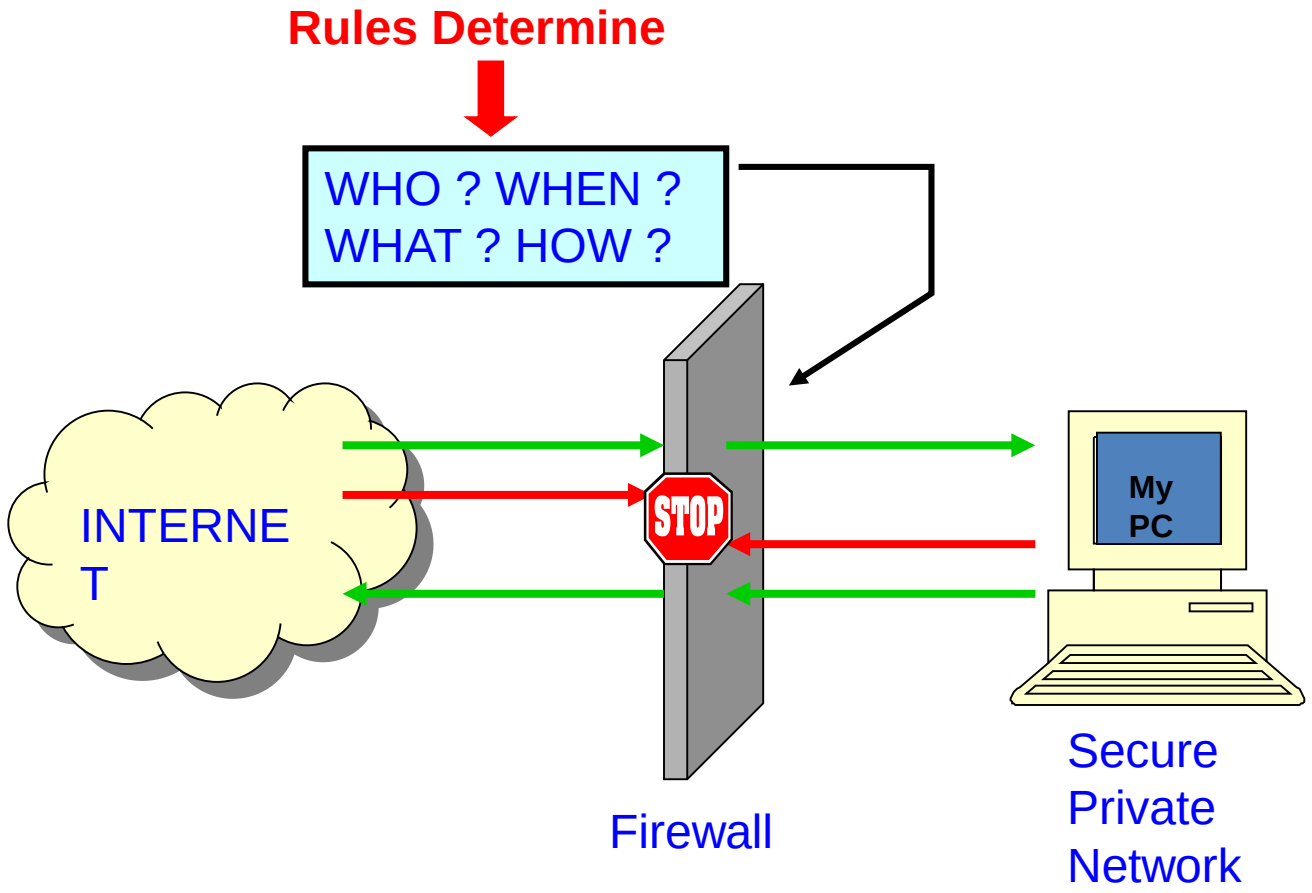
What is a Firewall?



- A secure Internet gateway that is used to interconnect a private network to the Internet.

❖Fungsi utama Firewall

What is a Firewall?



- **Firewall** adalah perangkat yang digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar

Firewalls History

- **First generation - packet filters**
  - The first paper published on firewall technology was in 1988, when Jeff Mogul from Digital Equipment Corporation (DEC) developed filter systems known as packet filter firewalls.
- **Second generation - circuit level**
  - From 1980-1990 two colleagues from AT&T Company, developed the second generation of firewalls known as circuit level firewalls.
- **Third generation - application layer**
  - Publications by Gene Spafford of Purdue University, Bill Cheswick at AT&T Laboratories described a third generation firewall. also known as proxy based firewalls.
- **Subsequent generations**
  - In 1992, Bob Braden and Annette DeSchon at the University of Southern California (USC) were developing their own fourth generation packet filter firewall system.
  - In 1994 an Israeli company called Check Point Software Technologies built this into readily available software known as FireWall-1.
  - Cisco, one of the largest internet security companies in the world released their PIX ” Private Internet Exchange ” product to the public in 1997.

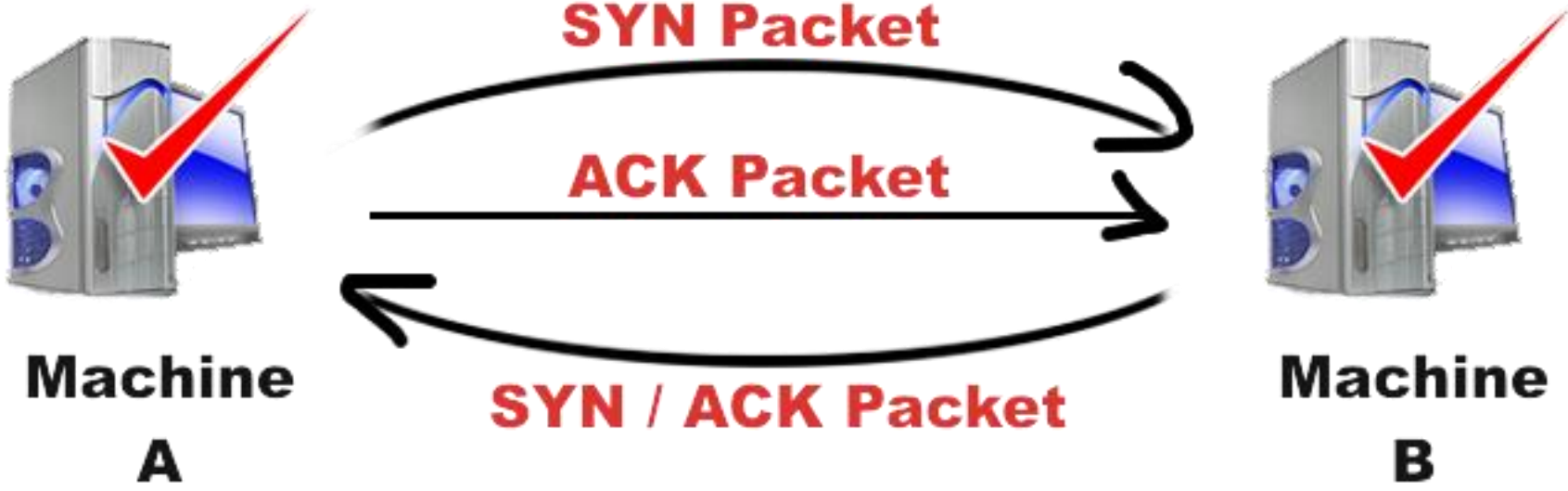
❖ Beberapa tahapan – perubahan Firewall

Need of Firewall

- Theft or disclosure of internal data
- Unauthorized access to internal hosts
- Interception or alteration of data
- Vandalism & denial of service
- Wasted employee time
- Bad publicity, public embarassment, and law suits

❖ Pencurian atau pengungkapan data internal, akses tidak sah ke host internal
Intersepsi atau perubahan data, Vandalisme & penolakan layanan
waktu karyawan yang terbuang, publisitas buruk, malu publik, dan tuntutan hukum

How can 2 Computers Connect?



We can see it in Windows Operating System, “netstat -n “ command to cmd. In this cmd we can see “ established “ word. Established connections are correctly connecting with A machine to our machine.

- Proses sebuah sistem Firewall

The Nature of Today's Attackers

- Who are these "hackers" who are trying to break into your computer?

Most people imagine someone at a keyboard late at night, guessing passwords to steal confidential data from a computer system.
This type of attack does happen, but it makes up a very small portion of the total network attacks that occur.

Today, worms and viruses initiate the vast majority of attacks. Worms and viruses generally find their targets randomly.

As a result, even organizations with little or no confidential information need firewalls to protect their networks from these automated attackers.

❖ Pola dan sifat penyerangan hari ini , terpola dalam sebuah aktivitas

Firewall Design Principles

1. Information systems undergo a steady evolution (from small LAN`s to Internet connectivity)
2. Strong security features for all workstations and servers not established
3. The firewall is inserted between the premises network and the Internet
4. Aims:
    1. Establish a controlled link
    2. Protect the premises network from Internet-based attacks
    3. Provide a single choke point

❖ Firewall : Membangun , Melindungi, Menyediakan

Firewall Characteristics

Design goals:

1. All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
2. Only authorized traffic (defined by the local security police) will be allowed to pass
3. The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Firewall Characteristics

Four general techniques:

1. Service control
   - Determines the types of Internet services that can be accessed, inbound or outbound

2. Direction control
   - Determines the direction in which particular service requests are allowed to flow

3. User control
   - Controls access to a service according to which user is attempting to access it

4. Behavior control
   - Controls how particular services are used (e.g. filter e-mail)

❖ Mengontrol : Layananan, arah, pengguna dan perilaku

Software vs. Hardware Firewalls

Software Firewall	*Hardware Firewall*
-Protect a single computer -Usually less expensive, easier to configure	-Protect an entire network. -Usually more expensive, harder to configure
Norton Internet Security	Cisco PIX
Mcafee Internet Security	NetScreen
Outpost	WatchGuard
Ms. ISA Server	Check Point

❖ Perbedaan antara Software dan Hardware Firewall

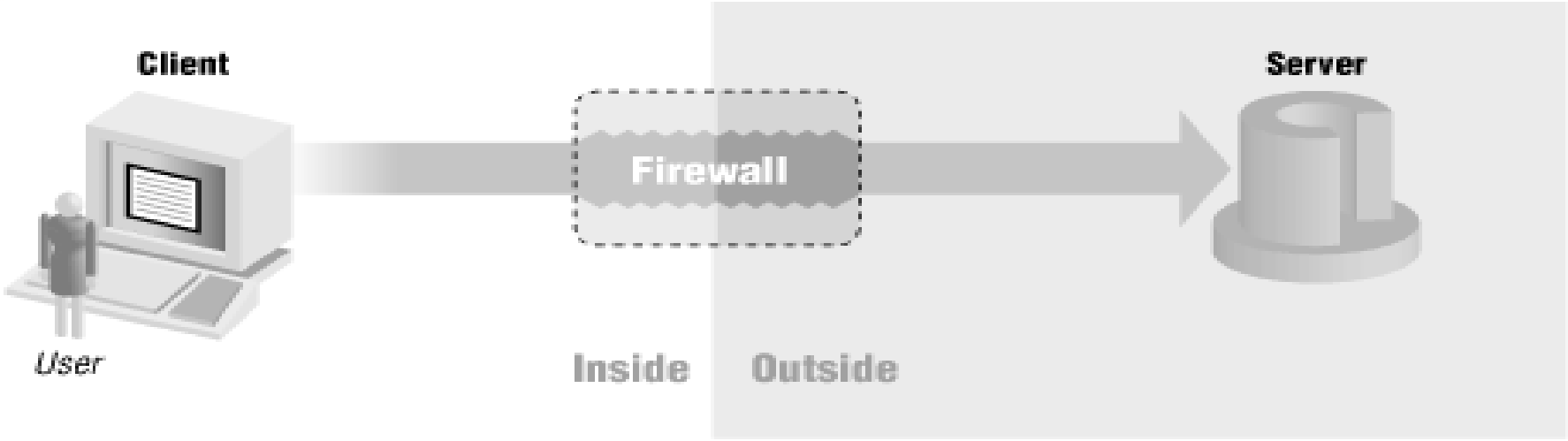
Where Can You Place a Firewall?

Firewalls, Layers and Models

ISO 7 Layer Model	Internet 5 Layer Model	Firewalls
Application (7)	Application (5)	Proxy Service
Transport (4)	TCP/UDP (4)	Packet Filtering Router/Packet Screening Router
Network (3)	IP/ICMP (3)	Stateful Inspection
Link (2)	Link (2)	none
Physical (1)	System Interface (1)	

- Posisi Firewall dalam sebuah 7 Layer / 7 Lapisan

How does a Firewall Work?



- **Inbound** to or **outbound** from your computer.
- **Inspects** each "**packet**" of data that arrives at either side of the firewall.
- Determines whether it should be allowed to **pass** through or if it should be **blocked**.

❖ Gambaran secara umum bagaimana Firewall bekerja

How does a Firewall Work?

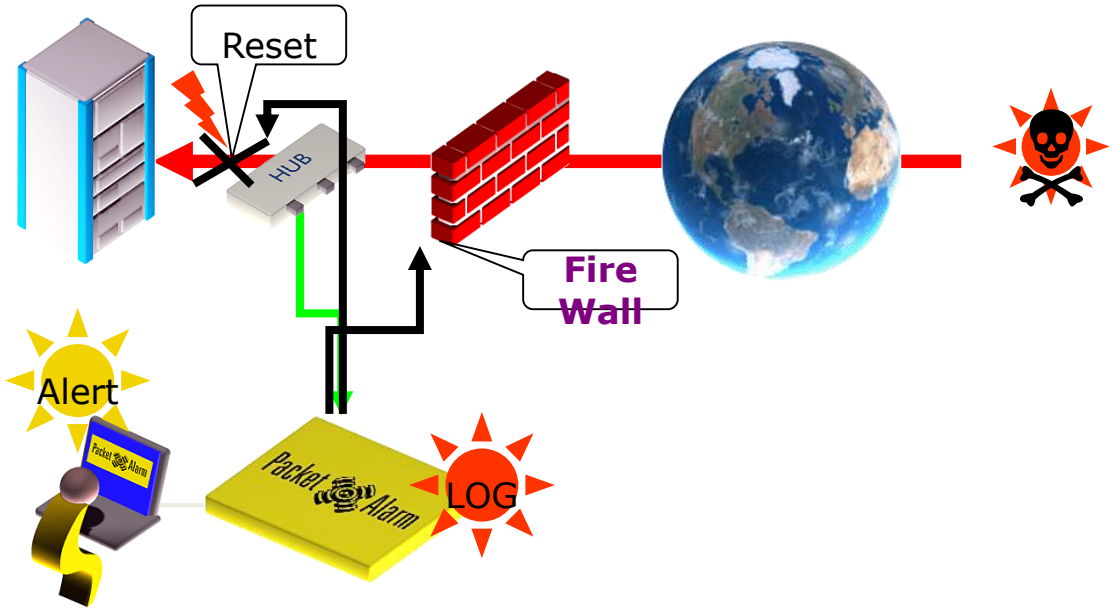
Sniffing Mode

1) An attacker tries to compromise a service on the protected network.

2) The Firewall identifies the attempt.

The FIREWALL can now:

- **Alert the admin**
- **Harden the firewall**
- **Or reset a TCP/IP connection**



❖ Antisipasi Firewall pada Modus Sniffing

Firewall Rules

- **Allow** – traffic that flows automatically because it has been deemed
- **Block** – traffic that is blocked because it has been deemed dangerous to your computer
- **Ask** – asks the user whether or not the traffic is allowed to pass through

❖ Aturan dasar dari sebuah Firewall : Allow – Block – Ask

Methods to Attack or View Computer Data

Some of the most common methods to attack or view computer data include:

- IP Spoofing
- Network Packet Sniffers
- Man-in-the-Middle Attacks
- Distribution of Sensitive Internal Information to External Sources
- Password Attacks

❖ Beberapa metode yang paling umum untuk menyerang ditampilan komputer

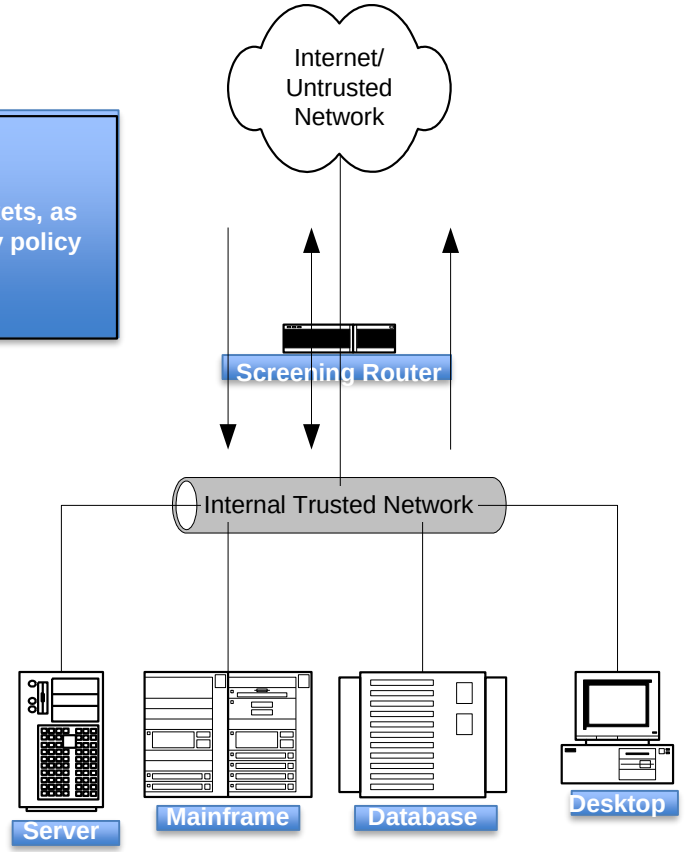
Firewall Architectures

- Screening Router
- Simple Firewall
- Multi-Legged firewall
- Firewall Sandwich
- Layered Security Architecture

❖ Arsitektur Firewall, beberapa arsitektur Firewall yang ada
❖ Kemampuan dari arsitektur yang berbeda beda

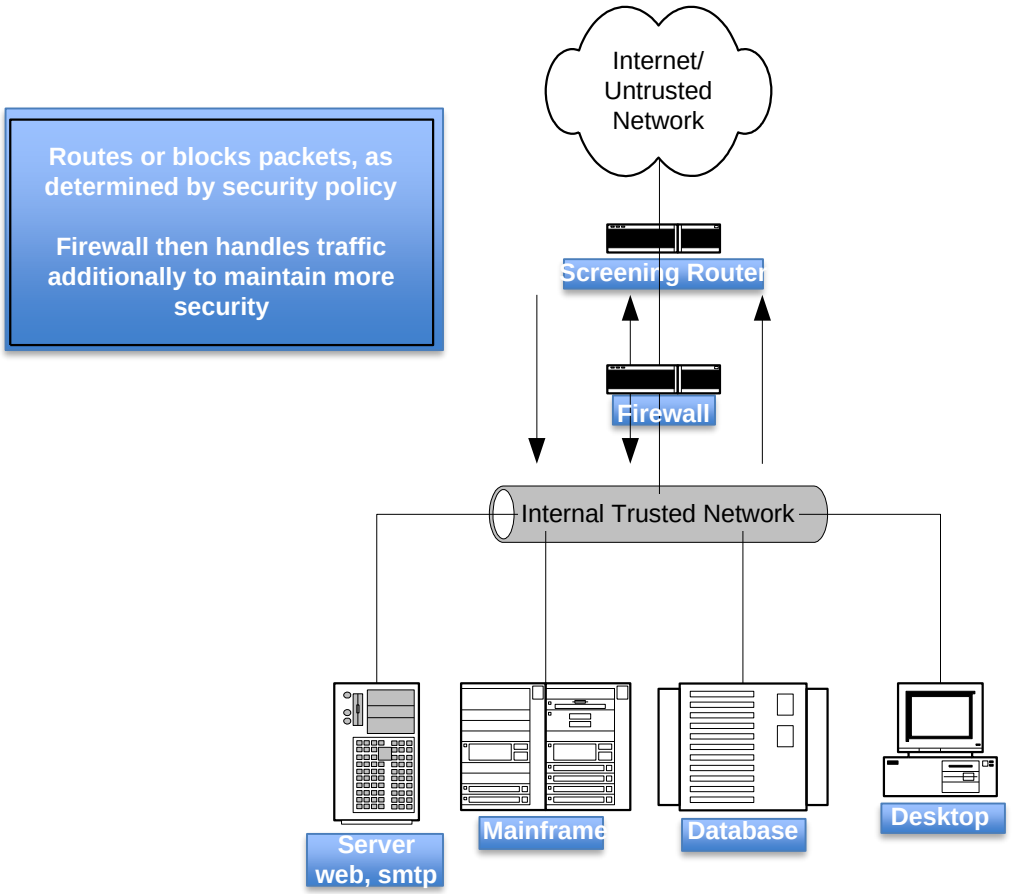
Screening Router

Routes or blocks packets, as determined by security policy



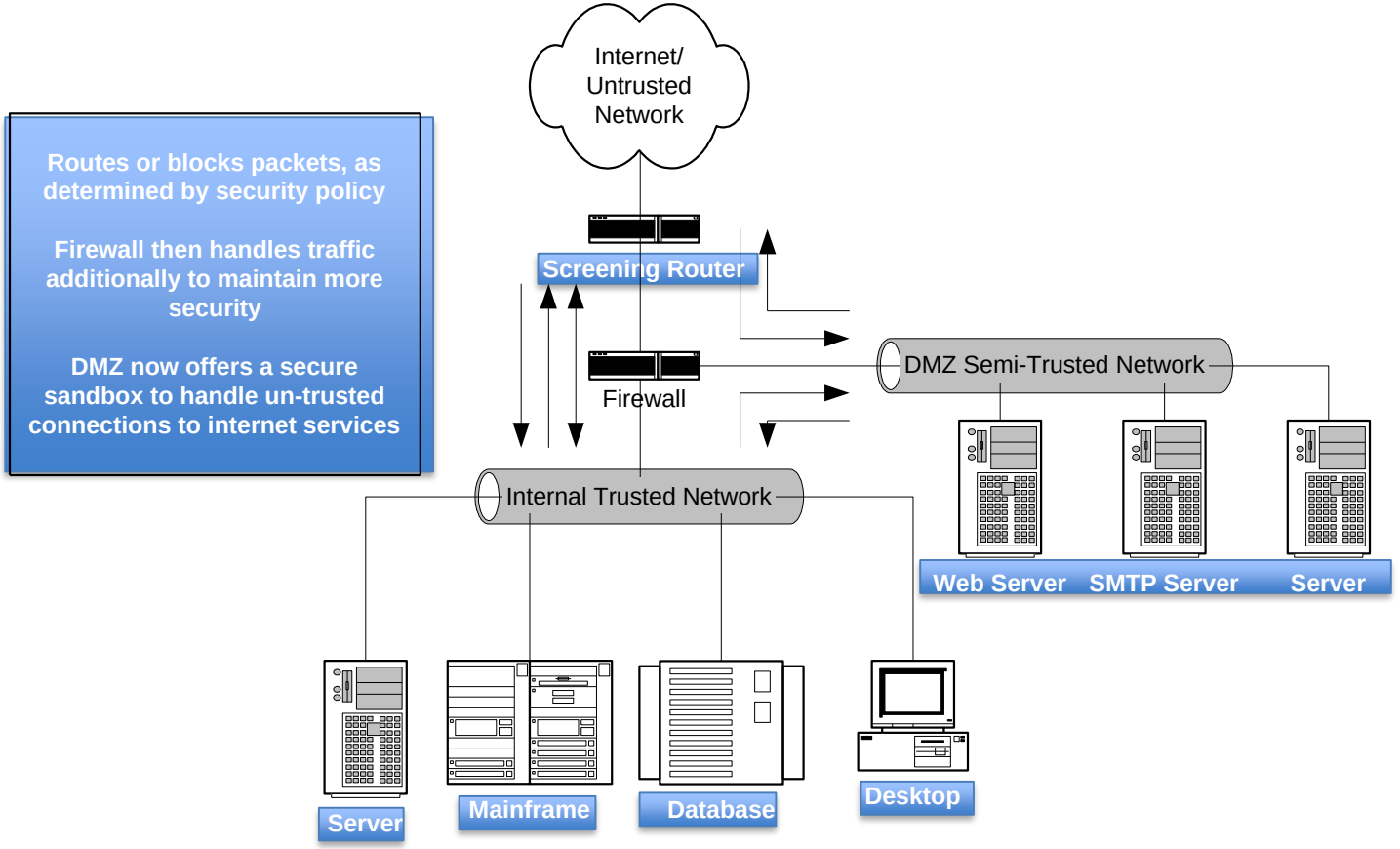
- Pola kerja dari Firewall – Screening Router : memastikan “internal Trusted Network

Simple Firewall



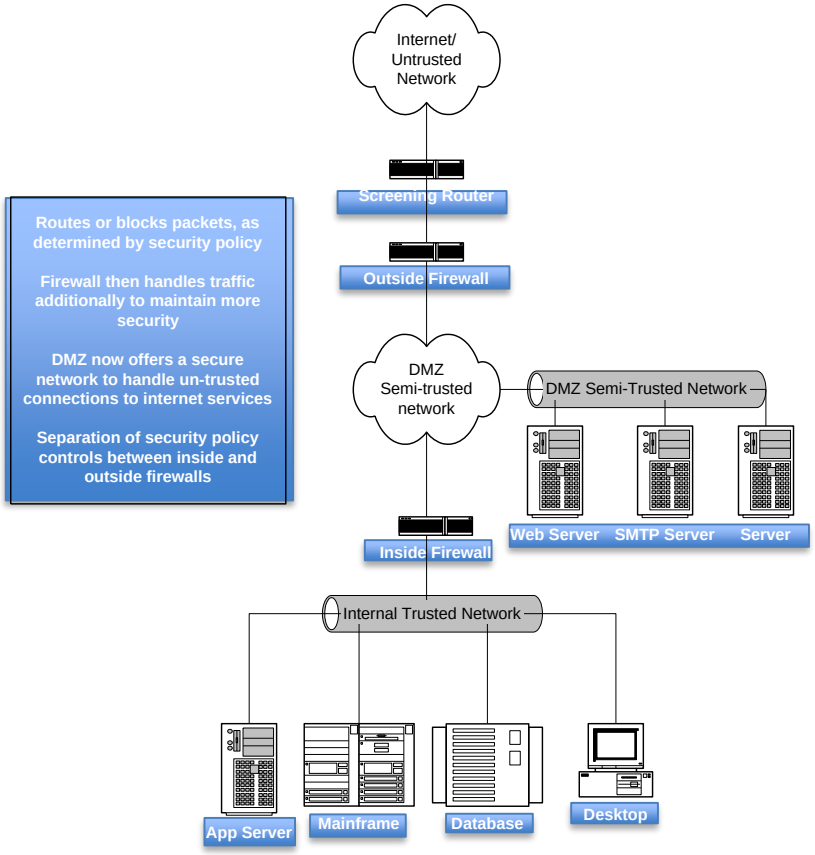
- Pola kerja dari Firewall – Simple Firewall

Multi-Legged Firewall



- Pola kerja dari Firewall – Multi Legged Firewall

Firewall Sandwich



- Pola kerja dari Firewall, “Firewall Sandwich

Layered Firewall

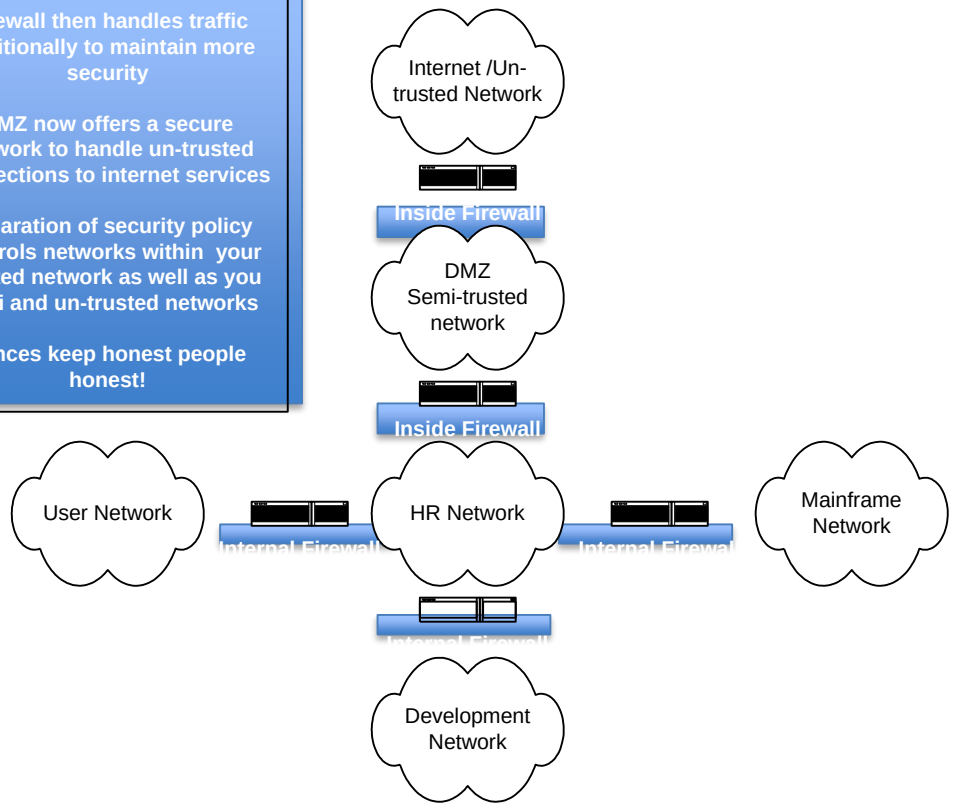
Routes or blocks packets, as determined by security policy

Firewall then handles traffic additionally to maintain more security

DMZ now offers a secure network to handle un-trusted connections to internet services

Separation of security policy controls networks within your trusted network as well as you semi and un-trusted networks

Fences keep honest people honest!



- Pola kerja dari Firewall - Layered Firewall

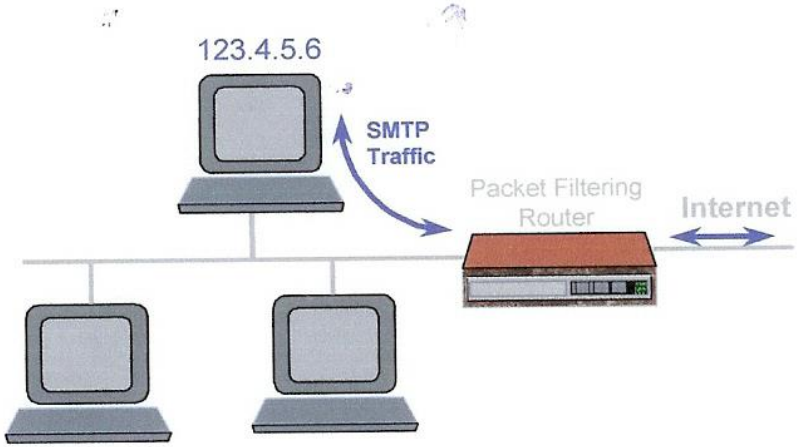
Packet Filtering Router

- Router placed between the Internet and an internal network
- Filters IP packet based on four fields
  - Source IP address
  - Destination IP address
  - TCP/UDP source port
  - TCP/UDP destination port
- Filtering techniques
  - Block connections to/from specific hosts or networks
  - Block connection to/from specific ports

❖ Fokus kerja dari Firewall : Filtering Router

Packet Filtering Router

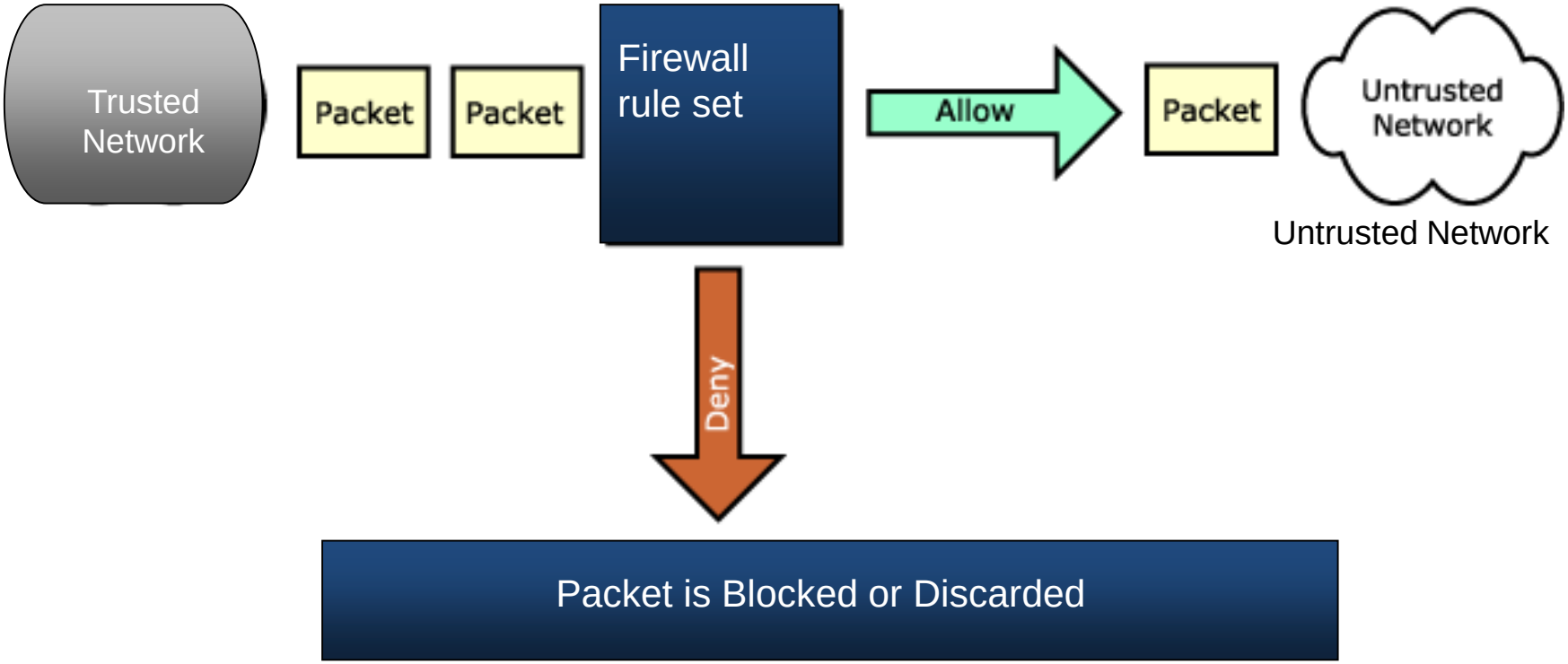
Packet Filtering Firewall



Type	S. Add.	D. Add.	S. Port	D. Port	Action
TCP	*	123.4.5.6	>1023	25	Permit
TCP	123.4.5.6	*	>1025	25	Permit
*	*	*	*	*	Deny

- Setting – Packet Filtering pada sebuah Firewall

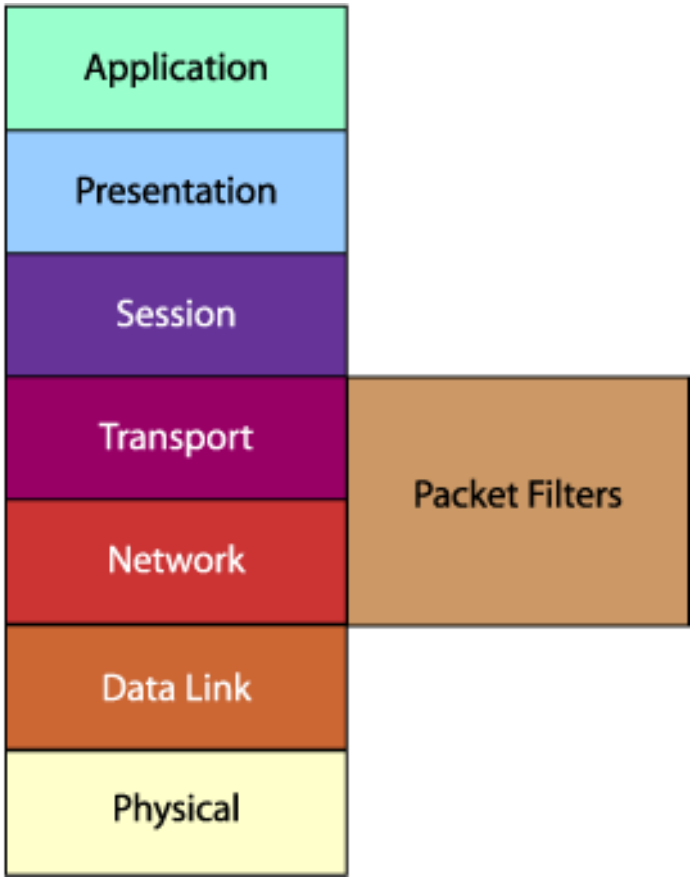
Packet Filtering Firewall



❖ Paket Filter Firewall, pada saat memblok Paket data yang masuk dalam rule set Firewall

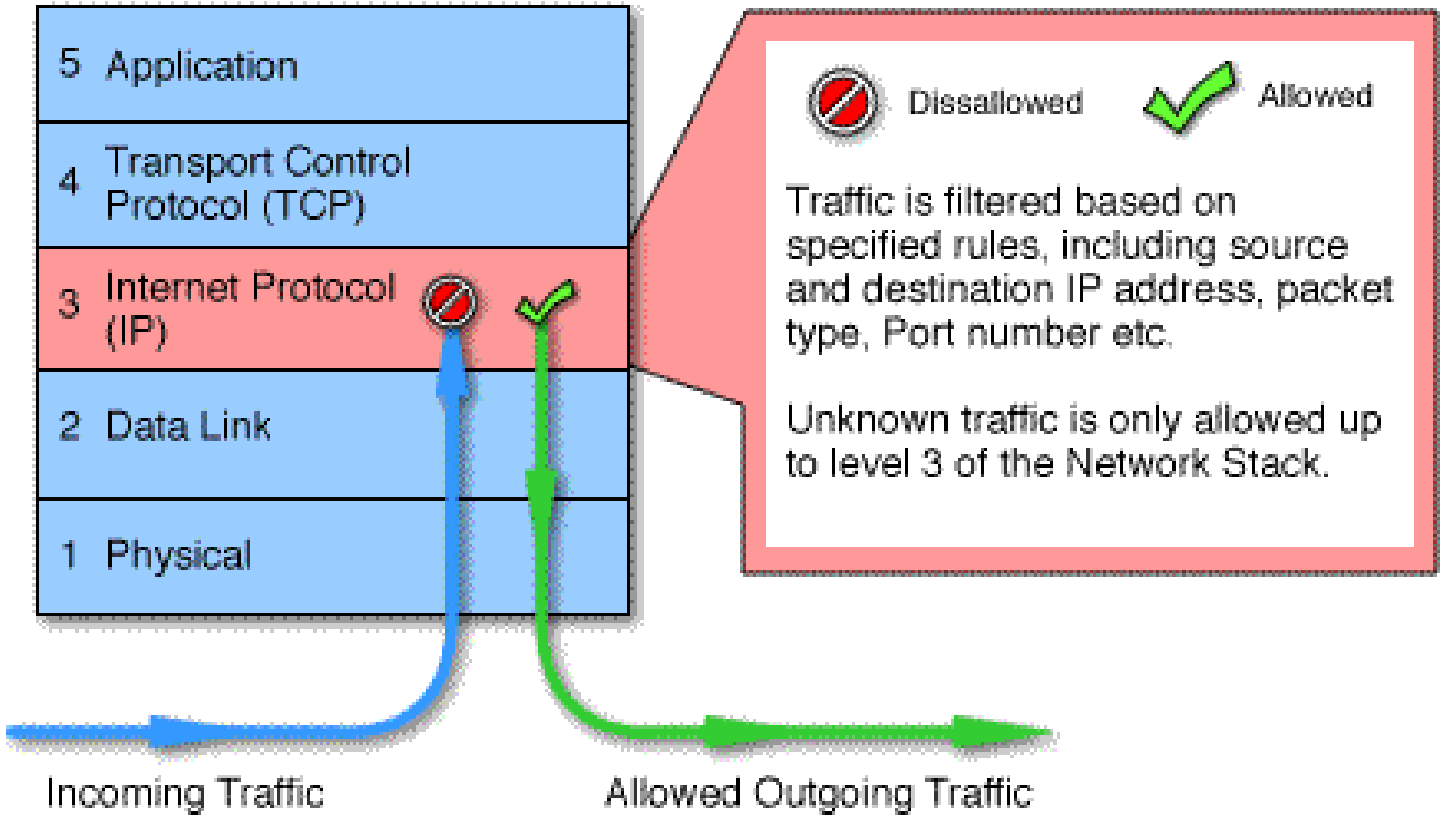
Packet Filtering Firewall

A packet filtering firewall is often called a network layer firewall because the filtering is primarily done at the network layer (layer three) or the transport layer (layer four) of the OSI reference model.



- Penyaringan terutama dilakukan pada lapisan jaringan (lapisan ketiga) atau lapisan transport (lapisan keempat)

Packet Filtering Firewall



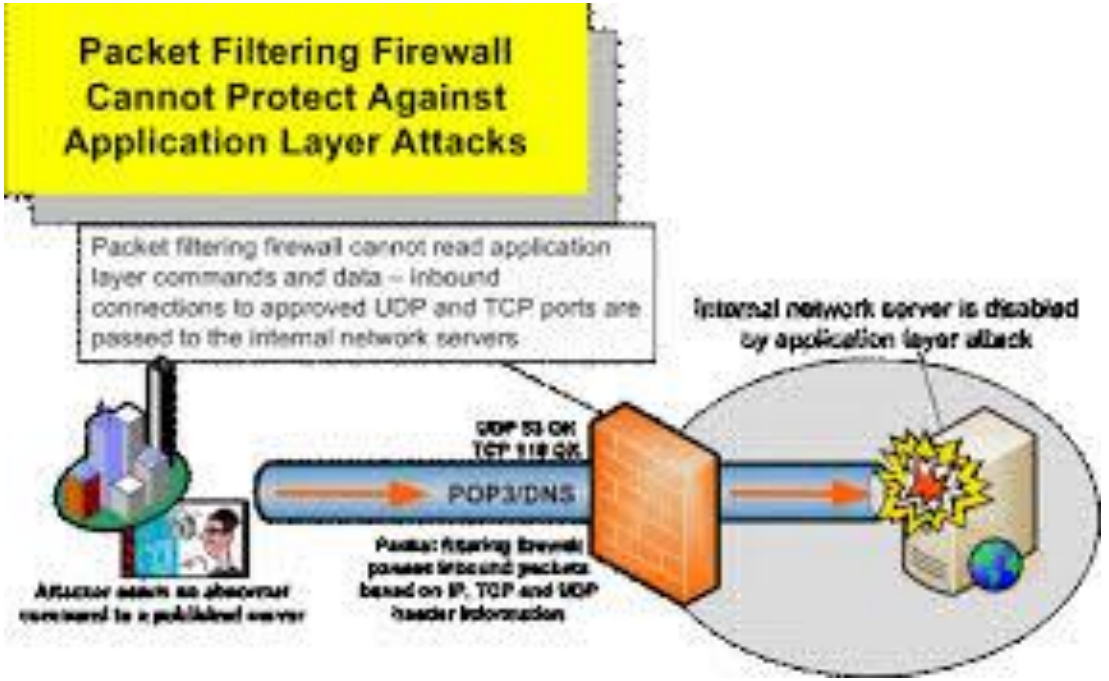
Penyaringan terutama dilakukan pada lapisan jaringan (lapisan ketiga) atau lapisan transport (lapisan keempat)

Packet Filtering Router

- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

❖ Keuntungan: Kesederhanaan, Transparansi kepada pengguna - Kecepatan tinggi
❖ kekurangan: Kesulitan menyiapkan aturan packet filter - Kurangnya Authentication

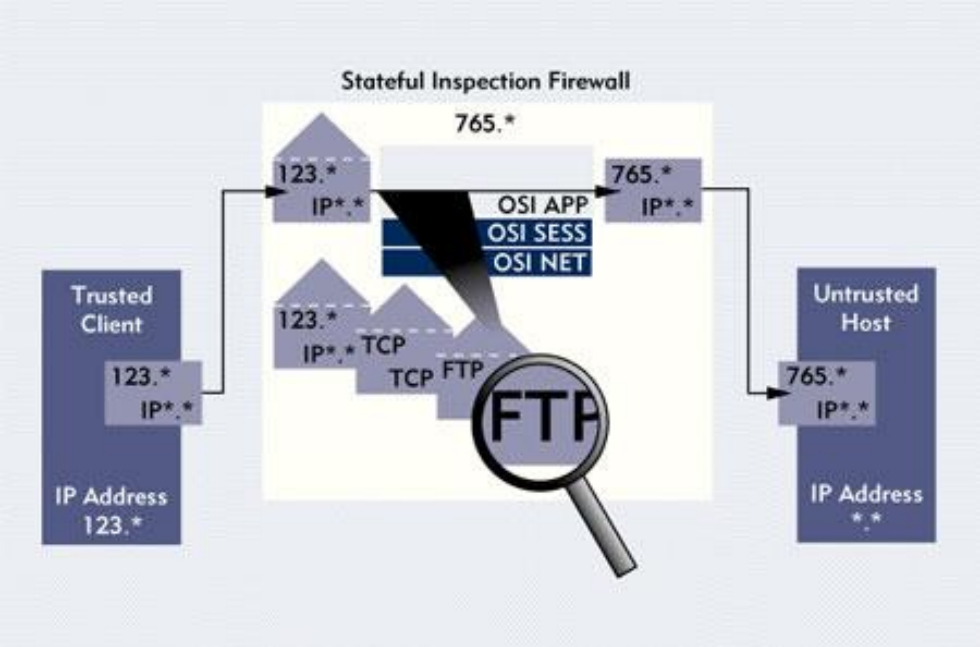
Packet Filtering Problem



- **Rule set is LARGE**
- **Special rules complicate the rule set**
- **Data inside a packet is not checked**
- **Senders of the packets are not authenticated.**

❖ Kendala teknis dalam Paket Filtering

Stateful Packet Inspections



- Module that processes in the operation system of a Windows or Unix PC firewall
- Inspects the packets as they arrive
- Headers from the different layers are inspected
- Information from the headers are fed into a dynamic state table
- Table is used to examine subsequent packets and connections.

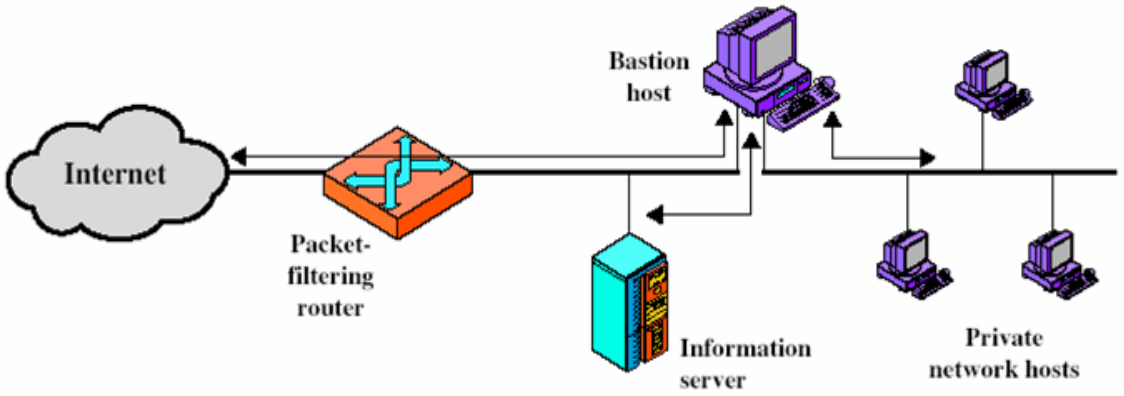
❖ Teknis kerja dari Proses Firewall

Stateful Packet Inspections

- Advantages
  - More secure than simple packet filtering routers
  - Performs faster than application proxies
- Disadvantages
  - Not as secure as application gateways
  - Application layer data is not inspected

- Beberapa keuntungan dan kekurangan dari Stateful Packet Inspections

Application Level Firewalls

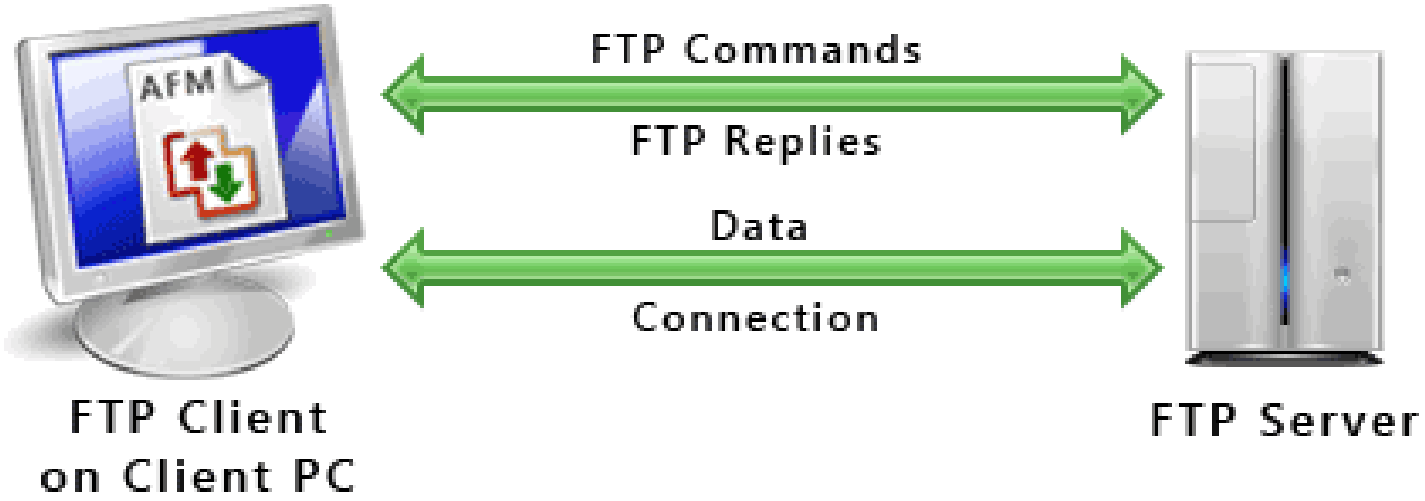


(b) Screened host firewall system (dual-homed bastion host)

- Bastion Computer
  - Placed between the packet filtering router and the internal network
  - Slimmed down proxy services
    - Allows messages through
    - Denies messages
    - Modifies messages
  - Proxy Services not running on the Bastion are not provided within the network.

- Application Level Firewall, Bastion Komputer ditempatkan antara router
- Packet filtering dan jaringan internal

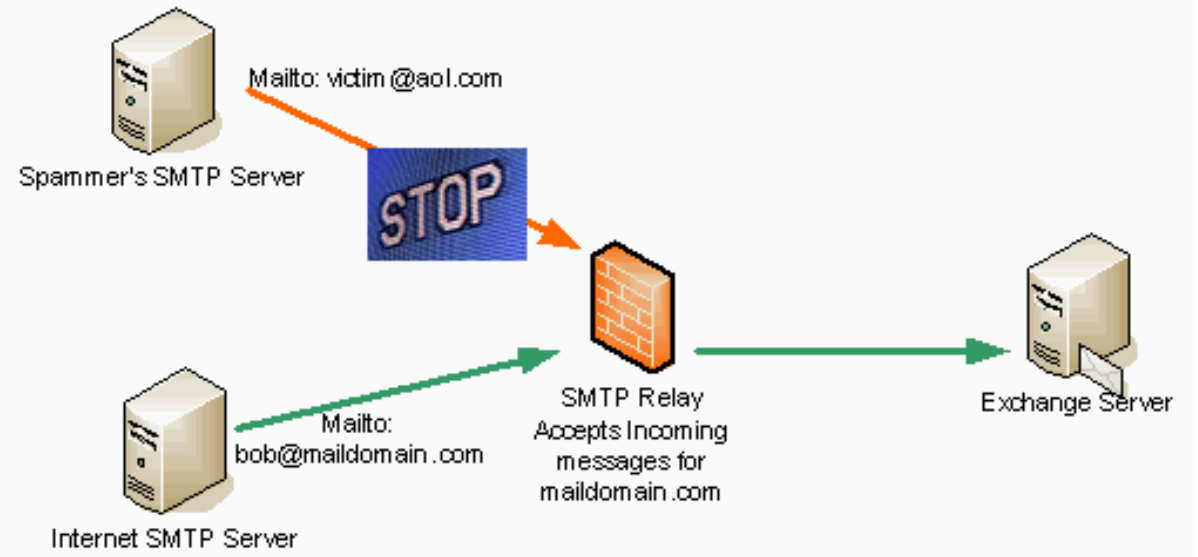
Common Proxy Services



- **FTP**
  - Threat – confidential information may be exported or bogus information may be deposited within an organization's file
  - FTP commands are selectively blocked according to the source and destination addresses.

❖ Layanan Umum Proxy - FTP Client - FTP Server

Common Proxy Services



- **SMTP**
  - Threat – Mail servers run with system level permission to deliver mail to mailboxes.
  - Isolates the internal Email system from incoming Internet mail.
  - Incoming mail is spooled on the Bastion host without system privileges.
  - Remote sender is disconnected.
  - Mail is forwarded to internal Email system.

❖ Layanan Umum Proxy : SMTP Simple Mail Transport Protocol

Common Proxy Services

- **TELNET**
  - Threat – remote users are allowed to login to a network with standard username and passwords
  - Configuration
    - Specific systems allowed to connect to the network
    - Specific systems from the network allowed to connect
    - Typical setting: allow internal users to connect to the Internet only

Telnet (**Tel**ecommunication **net**work) sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal

Common Proxy Services

- **http://**
  - Filter http:// commands
    - POST
    - PUT
    - DELETE
- Filter URLs

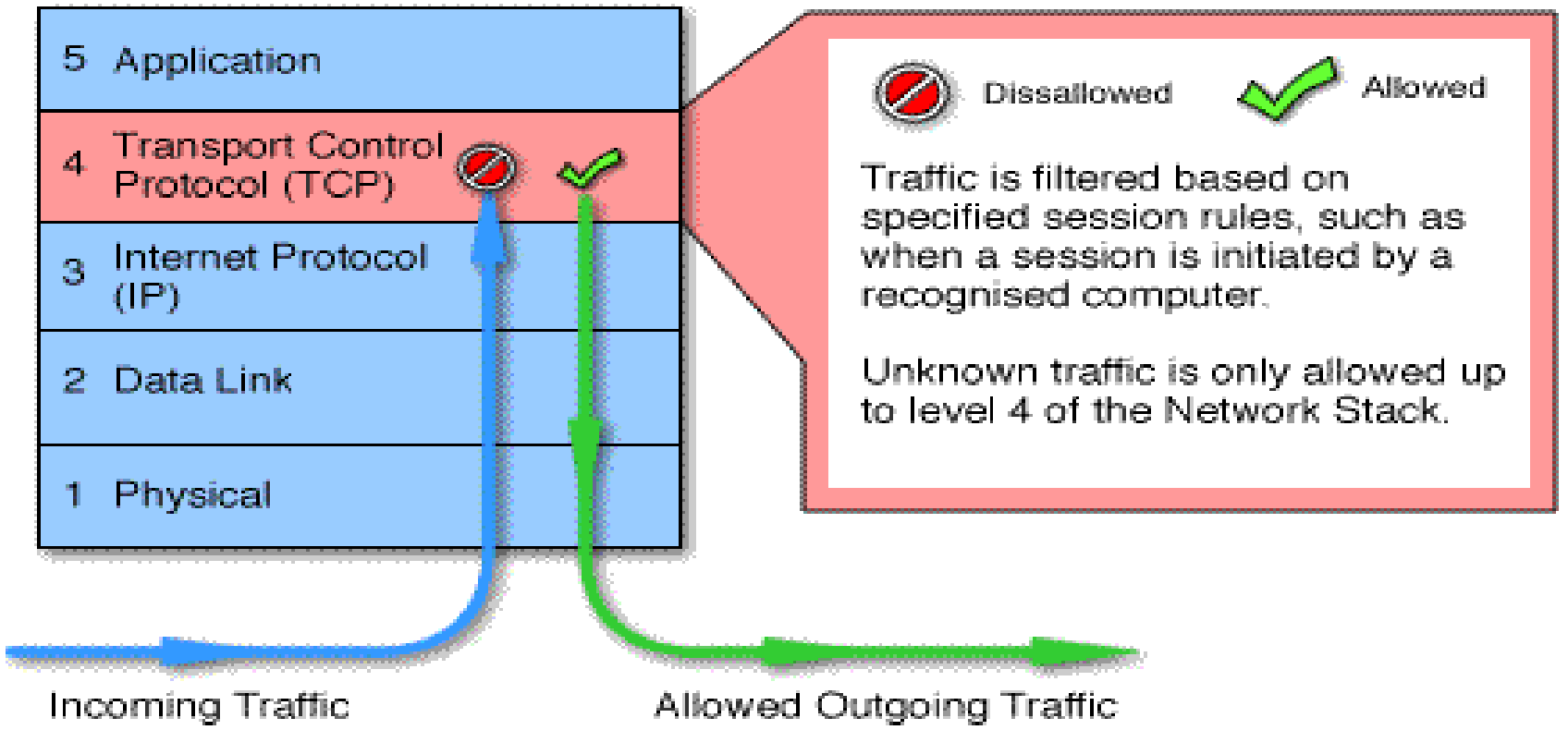
Layanan Hypertext Transfer Protocol (**HTTP**) sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan hipermedia.

Circuit-level Gateway

1. Stand-alone system
2. Specialized function performed by an Application-level Gateway
3. Sets up two TCP connections
4. The gateway typically relays TCP segments from one connection to the other without examining the contents
5. The security function consists of determining which connections will be allowed
6. Typically use is a situation in which the system administrator trusts the internal users
7. An example is the SOCKS package

❖ Beberapa point dalam Circuit Level Gateway yang harus diperhatikan

Circuit-level Gateway



- Pola Kerja Firewall pada layer 4 – Circuit Level Gateway

Content Filtering

- Application data is unpacked and examined
- Harmful content is disposed of
- Executables can be removed based on a security policy
- Authors of Digitally Signed Code are checked against a trusted list
- Text files can be scanned for a list of undesirable words
- Java applets can be removed

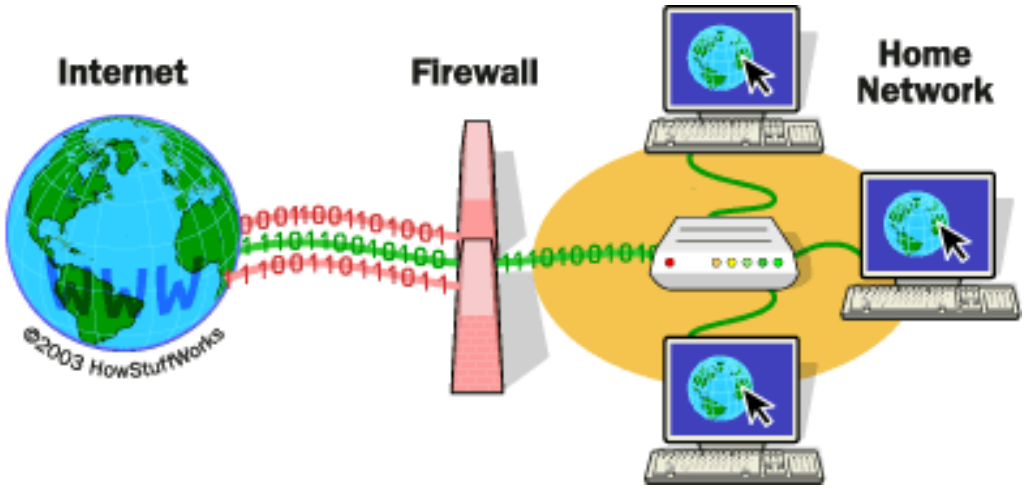
❖ Pemfilteran berdasarakan Content

Virtual Private Networks

- Connects two private networks via a secure link
- A secure tunnel is established
- Provides confidentiality, integrity, authentication, anti-replay

VPN singkatan dari **Virtual Private Network**, yaitu jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar remote-site secara aman : !

Firewall Configuration



- Dual Homed Gateway
- Screen Host Gateway
- Screened Subnet Gateway
- Double Proxying and a DMZ

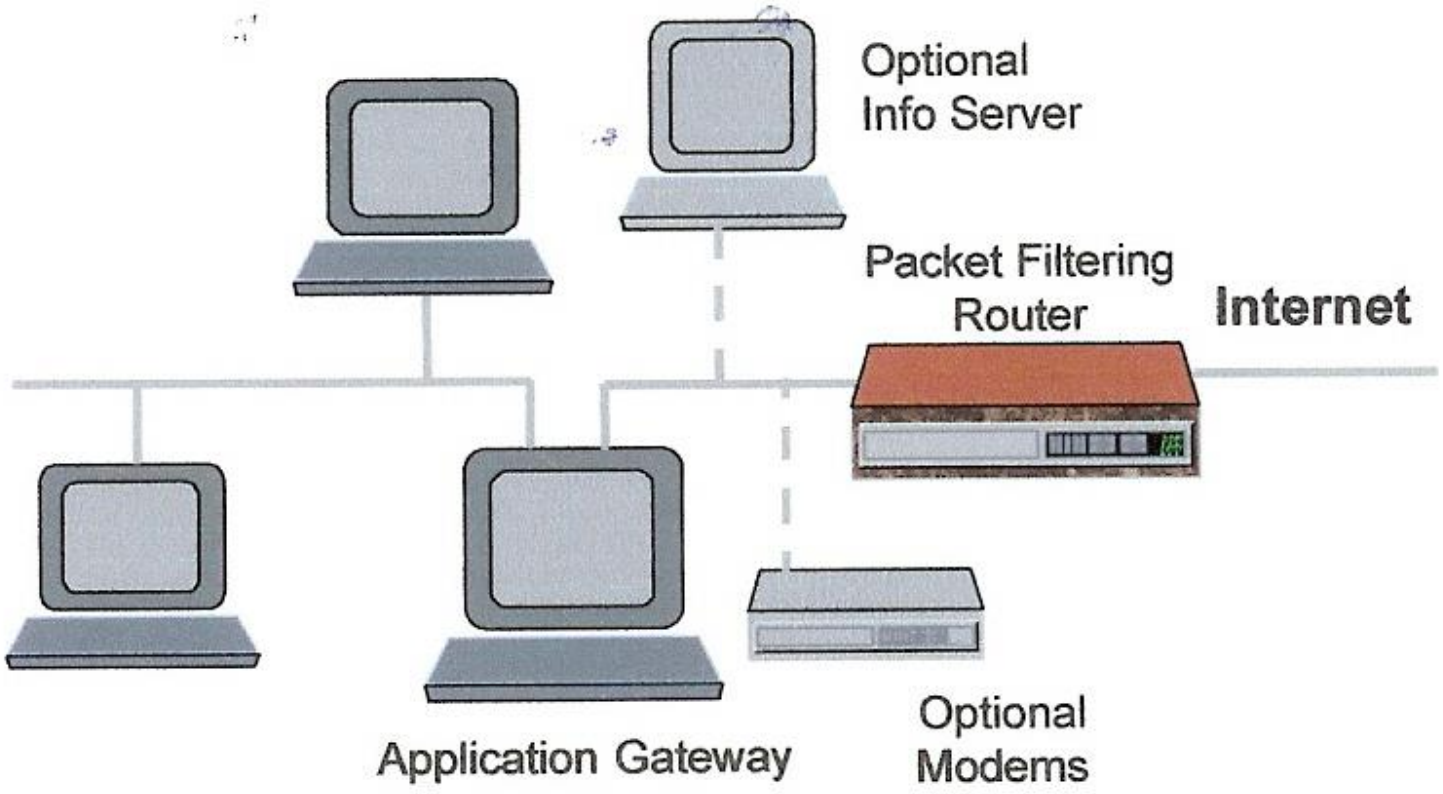
❖ Konfirgurasi penerapan Firewall yang ada

Dual Homed Gateway

- Gateway has two network interfaces
- Only applications with proxy services on the application gateway are able to operate
- IP forwarding is disabled
- IP packets must be directed to one of the proxy servers

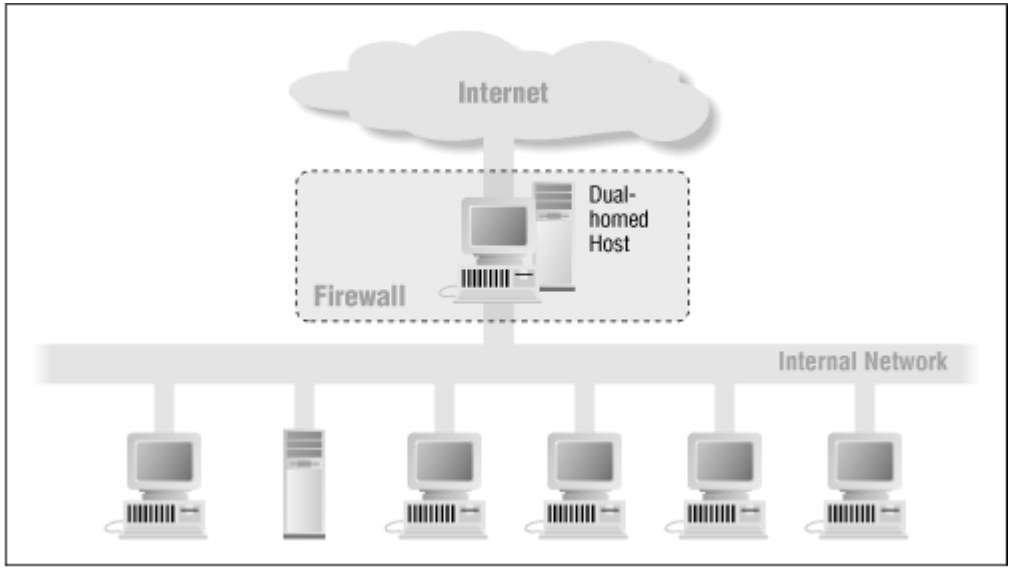
❖ Ciri ciri dari Dual Homed Gateway

Dual Homed Gateway



❖ Ilustrasi Dual Homed Gateway

Dual Homed Gateway



- **Disadvantages**
  - Bottleneck to performance
  - Too secure for some sites

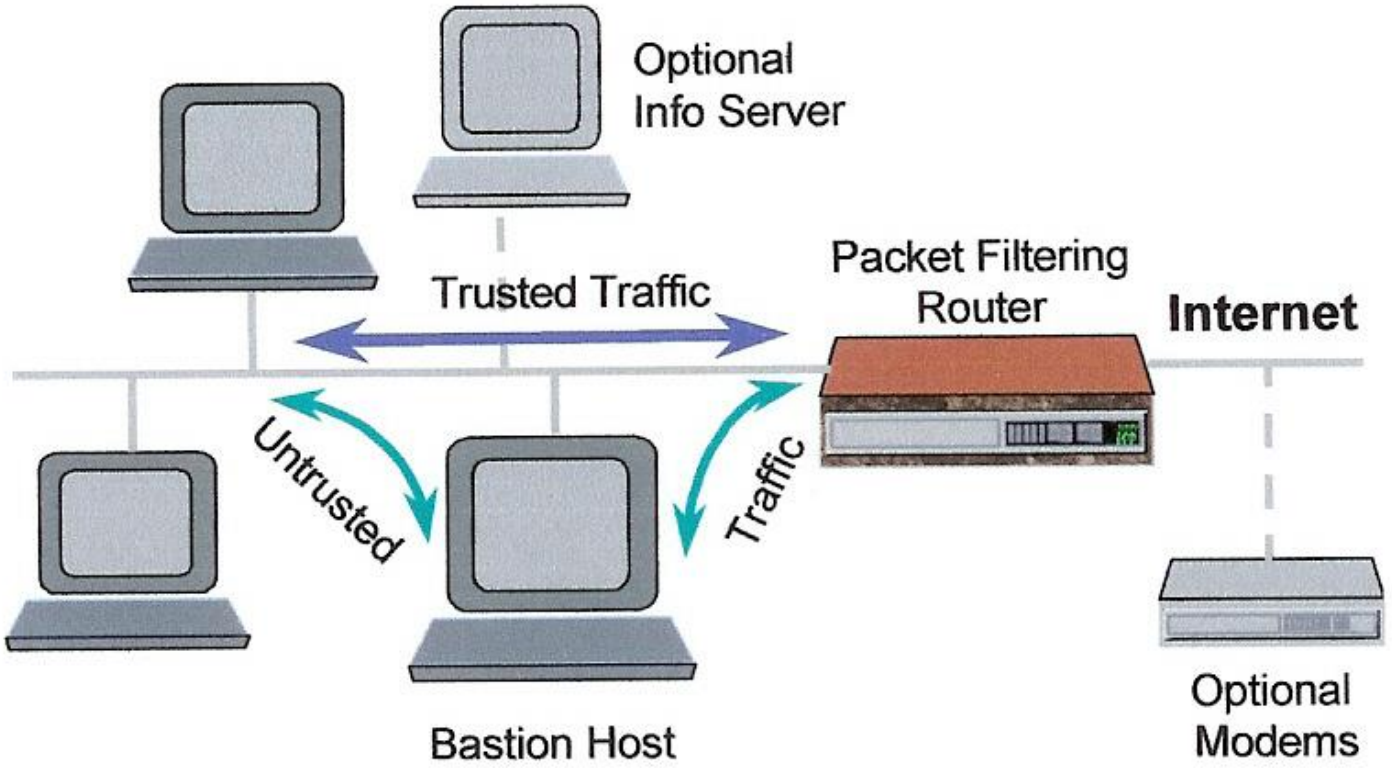
❖ Kekurangan Bottleneck untuk kinerja, Terlalu aman untuk beberapa situs!

Screen Host Gateway

- More flexible and less secure then Dual Homed Gateway
- Packet Filtering Router separates the internet from the internal network
- All incoming traffic is forced through the bastion

❖ Lebih fleksibel dan kurang aman dari dual homed Gateway – Screen Host Gateway

Screen Host Gateway



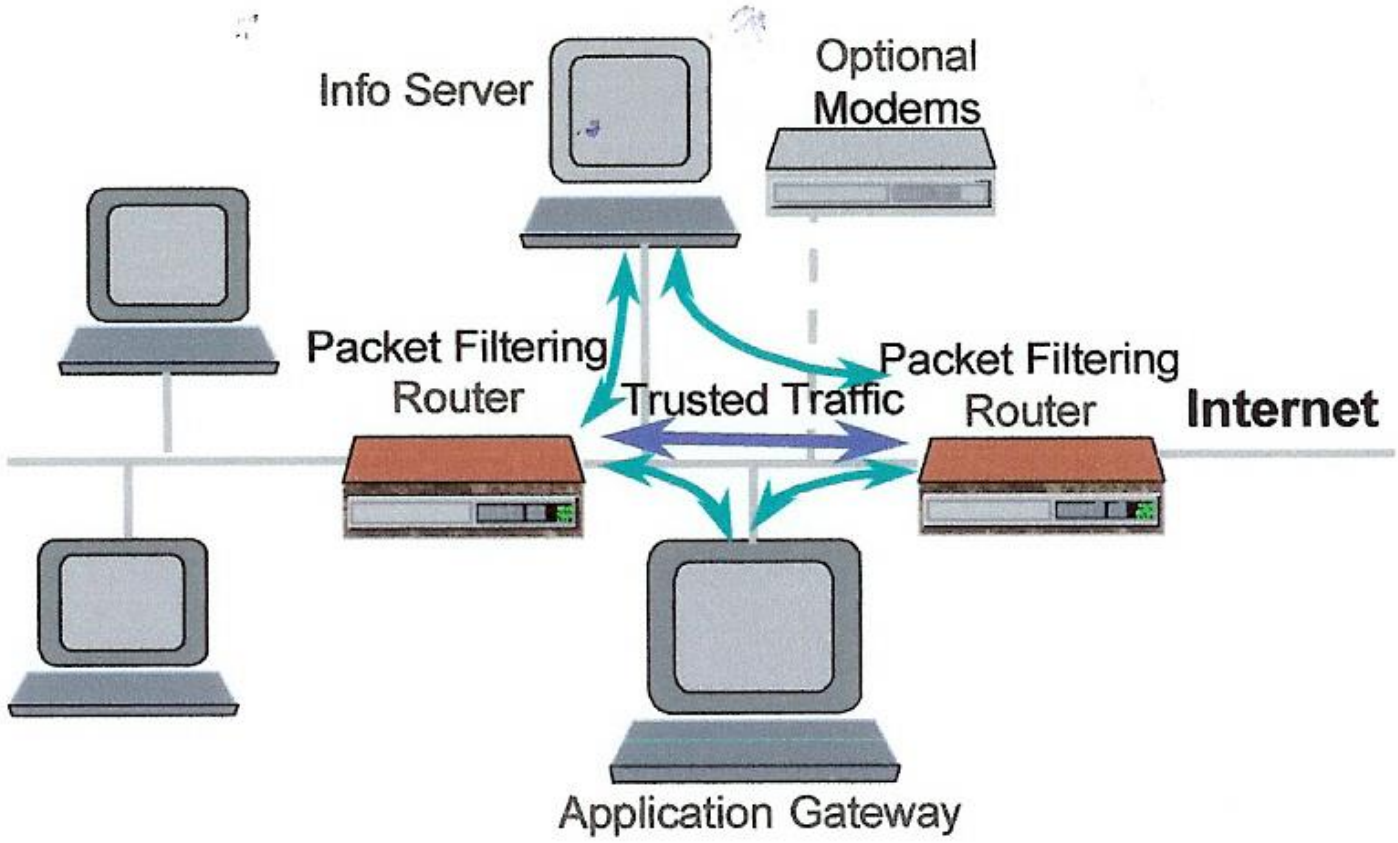
❖ Gambaran Screen Host Gateway

Screened Subnet Gateway

- Creates a small network between the Internet and the internal network also known as a demilitarized zone (DMZ)
- Multiple hosts and gateways could be added to handle more traffic at a time
- Two packet filtering routers are placed on each side of the DMZ
- Very secure

Menciptakan jaringan kecil antara internet dan jaringan internal “ zona demiliterisasi (DMZ)”

Screened Subnet Gateway

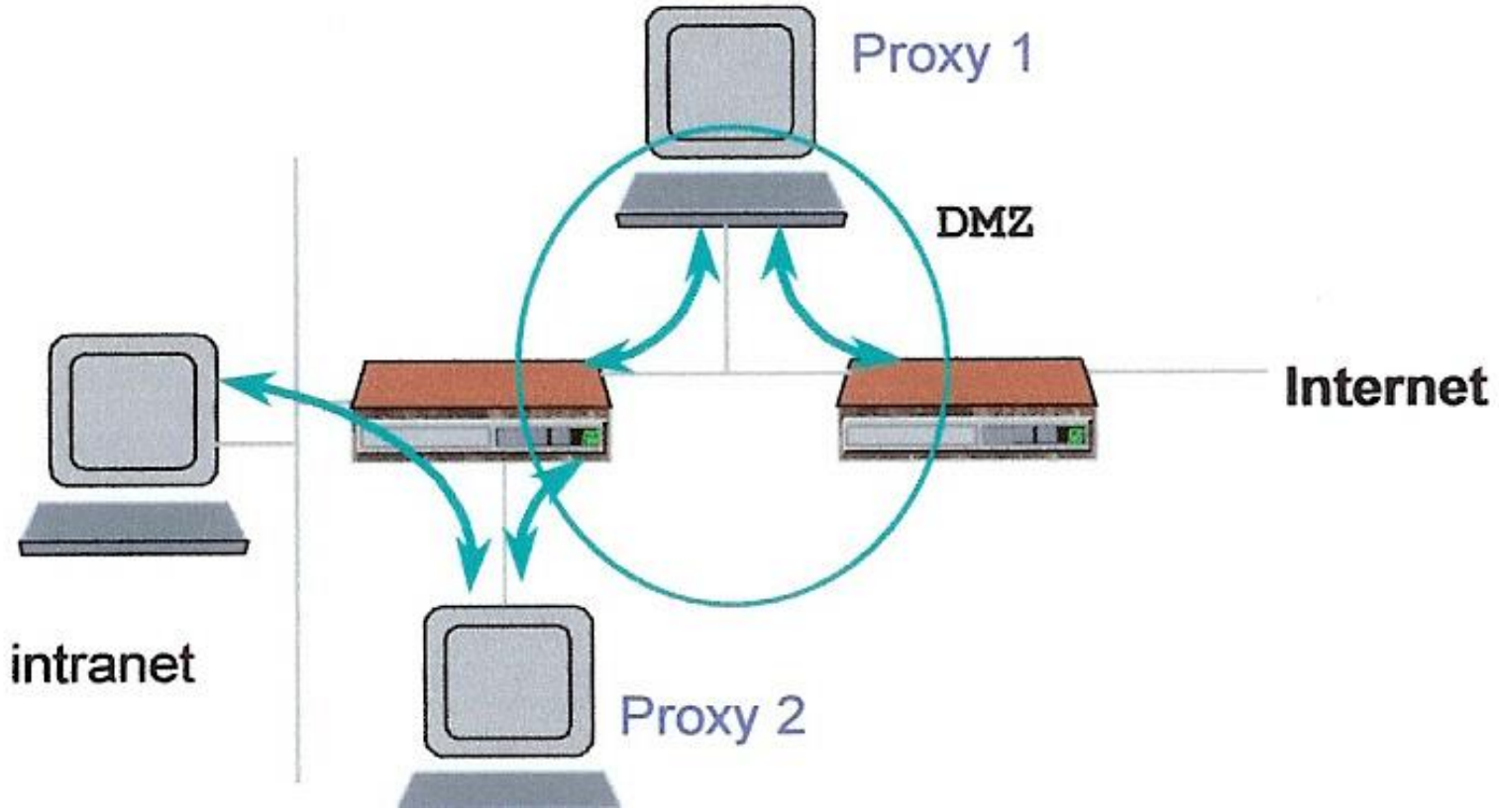


❖ Ilustrasi Firewall - Screened Subnet Gateway

Double Proxying and a DMZ

- Very secure
- Users from the Internet must pass through two application proxies before they can access the internal network
- Application Proxies check incoming data for known vulnerabilities

Double Proxying and a DMZ



❖ Ilustrasi Double Proxying and Demilitarized Zone

Distributed Firewall

- Definition
  - A mechanism that uses a centralized policy, but pushes enforcement to the end points
- Topology is different than traditional firewalls
- End points are identified by their IPsec identity
- Assigns specific rights to specific machines on the network
- Invalid users are not able to access the network since they do not have credentials

❖ Distribusi Firewall !,: Topology is different than traditional firewalls

Distributed Firewall

- Need for a security policy language
  - KeyNote
- Need for an authentication mechanism
  - IPsec
- Need for a distribution mechanism
- Usually avoids application level security mechanisms
  - Requires extensive modifications of all applications to make them aware of all security mechanisms
  - It is impossible to secure legacy applications with inadequate provisioning for security

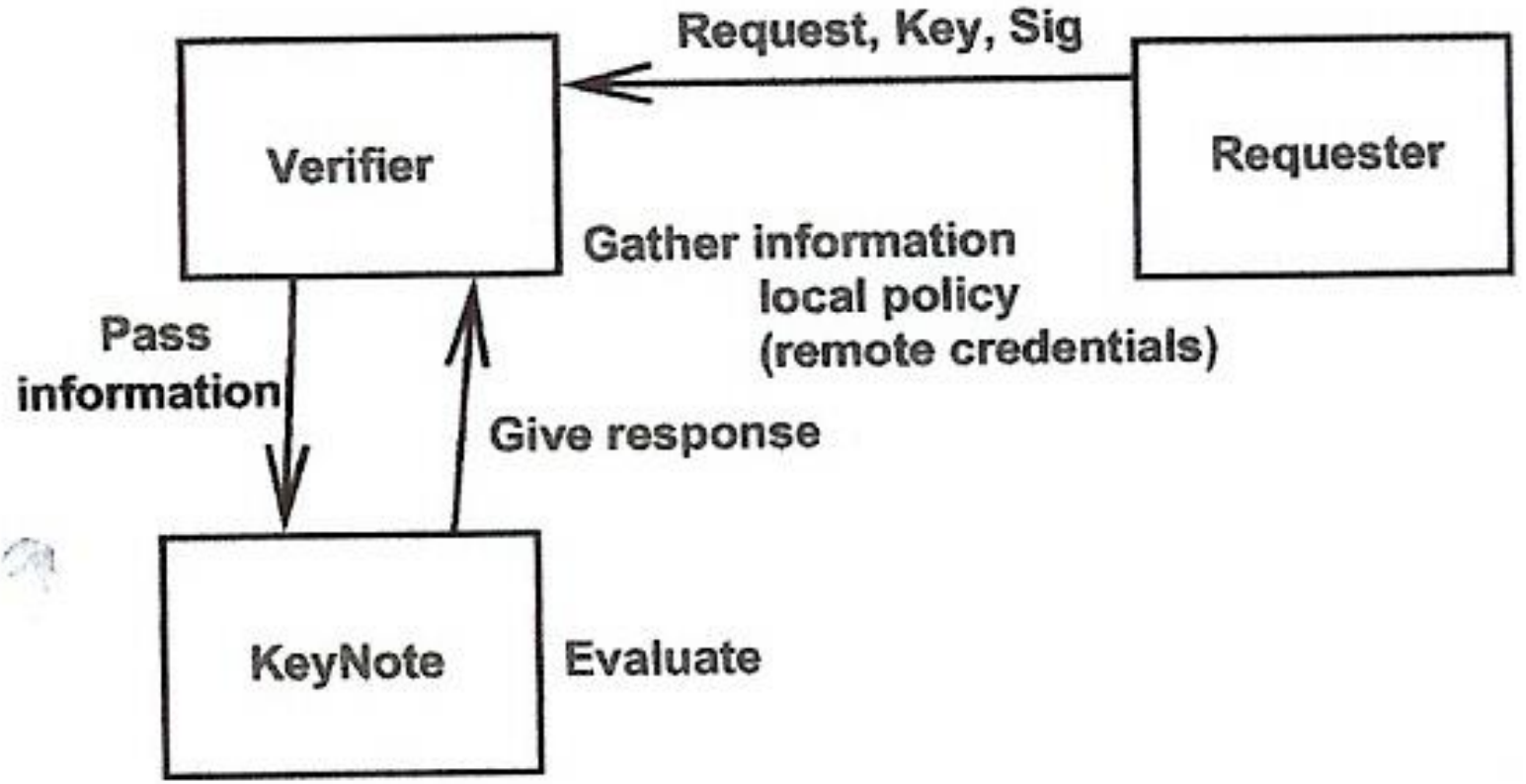
❖ Standar baku Distributes Firewall," Need for a security policy language "

Key Note

- Provides local security policies and credentials over an un-trusted network
- Policy and credentials contain predicates that describe the trusted actions permitted by the holders of specific public keys
- Evaluator determines if proposed actions comply with the local policy
- Supports application-specific credentials

❖ Key Note “Supports application-specific credentials

KeyNote



❖ Diagaram Alur – Proses Firewall KeyNote

KeyNote

- **Concept**
  - Monotonicity – given a set of credentials associated with a request, if there is any subset that would cause the request to be approved, then the complete set will cause the request to be approved.
    - Simplifies request resolution and credential management

❖ Adanya Proses yang monoton dalam KeyNotes

KeyNote

- Uses cryptographic keys to identify users
  - Multiple user computers
    - Operation system or trusted application must secure the user identifications
    - KeyNote is not responsible

KeyNote

```
KeyNote-Version: 2
Authorizer: "POLICY"
Licensees: "rsa-hex:1023abcd"
Comment: Allow Licensee to connect to local port 23 (telnet) from
         internal addresses only, or to port 22 (ssh) from anywhere.
         Since this is a policy, no signature field is required.
Conditions: (local_port == "23" && protocol == "tcp" &&
             remote_address > "158.130.006.000" &&
             remote_address < "158.130.007.255") -> "true";
            local_port == "22" && protocol == "tcp" -> "true";

KeyNote-Version: 2
Authorizer: "rsa-hex:1023abcd"
Licensees: "dsa-hex:986512a1" || "x509-base64:19abcd02=="
Comment: Authorizer delegates SSH connection access to either
         of the Licensees, if coming from a specific address.
Conditions: (remote_address == "139.091.001.001" &&
             local_port == "22") -> "true";
Signature: "rsa-md5-hex:f00f5673"
```

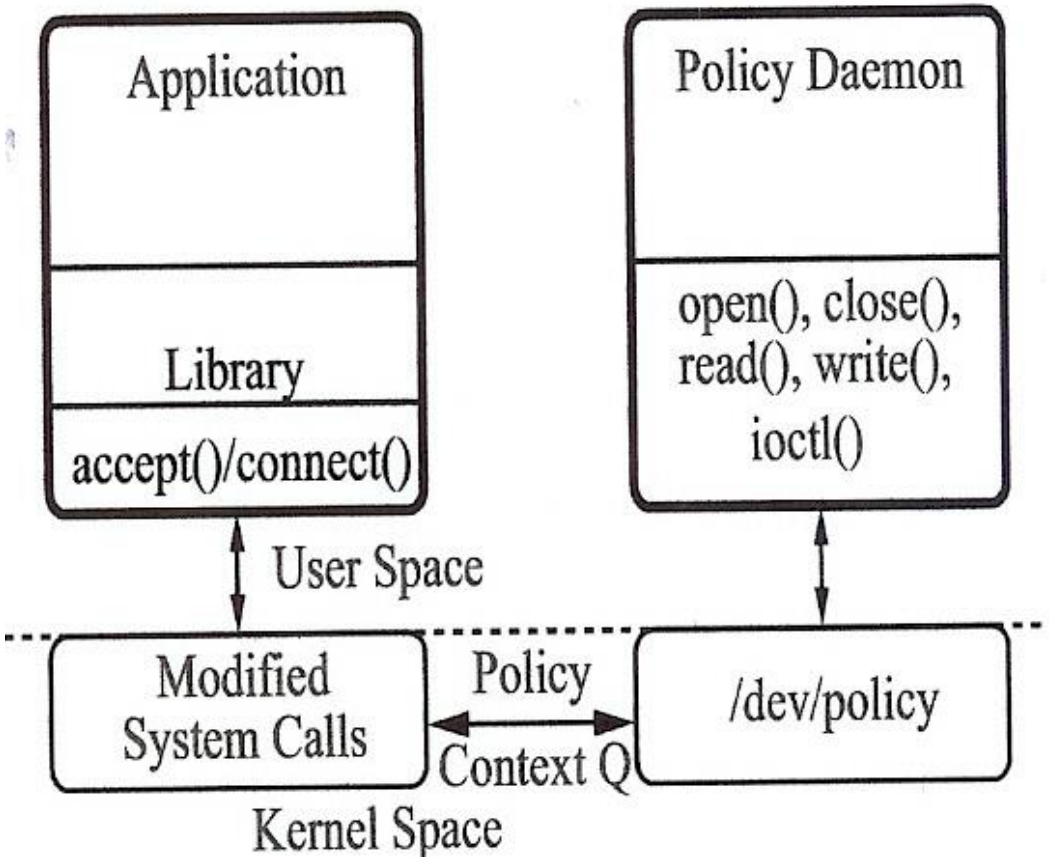
- Secara sotftwre : Dapat dilakuan dan disesuaikan sesuai keinginan

Implementation of KeyNote

- OpenBSD platform
- Three components
  - Kernel Extensions
  - User level daemon process
  - Device driver
- Approx. 1150 lines of C code

❖ Beberapa contoh penerapan KeyNote,

KeyNote System



- Alur KeyNote Sytem dalam Firewall

Kernel Extensions

- User Space
  - Applications are linked to libraries with security mechanisms
  - Operating System independent
  - Hard to enforce
- Kernel Space
  - Security mechanisms are enforced transparently to the application
  - Filters two systems calls
    - Connect(2)
    - Accept(2)

❖ Kernel Extension Pemanfaatan ruang bagi user dan kernel dalam sebuah Firewall :

Kernel Extensions

- Kernel Space
  - Policy context is created for each connection
    - Container for relevant information for the policy daemon
    - Sequence Number
  - Commit Context
    - Adds the context to the list of contexts the policy daemon needs to handle
  - Application is blocked

❖ Kernel Extensions, Kernel Space : adanya kebijkaan,commit context & blokir aplikasi

Policy Device

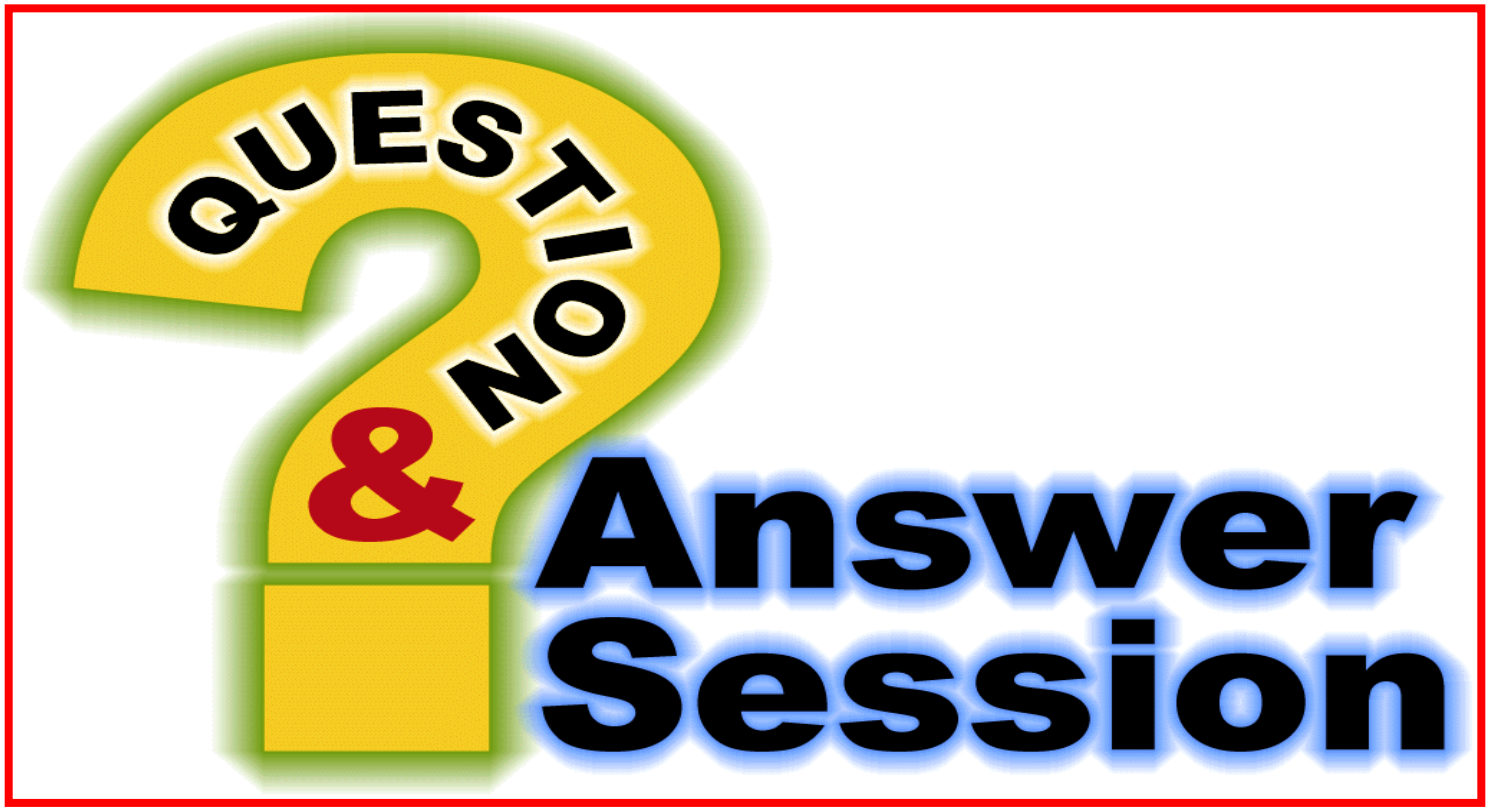
- Serves as a communication path between the user space policy daemon and the modified system calls in the kernel
- Implemented as a pseudo device driver
  - /dev/policy
  - Loadable module
  - Supports close(2), open(2), read(2), write(2), and ioctl(2)
  - If device is not loaded, then no connection filtering will be processed

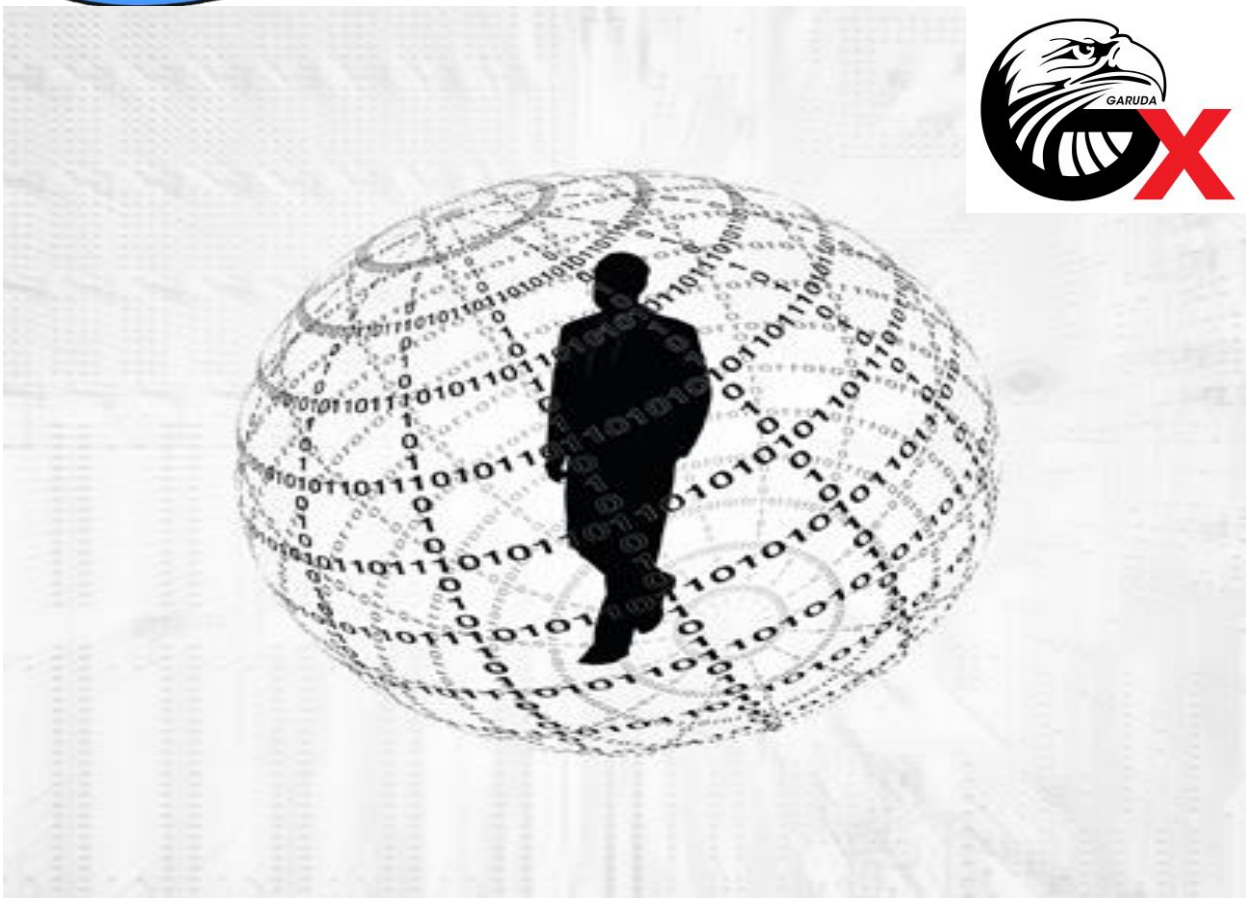
❖ Kebijakan Perangkat “ruang pengguna dan panggilan sistem dimodifikasi di kernel”

Policy Device

- User level process
- Application independent
- Responsible for making decisions based on the policies and credentials
- Receives a request from Policy Device
- Processes the request using the KeyNote library
- Writes back a reply (Deny, Approve) to the kernel via Policy Daemon
- The pending application is unblock and service is denied or approved.

❖ Berbagai kebijakan penggunaan perangkat


QUESTION
&
Answer
Session



- **Hatur Nuhun**
- Matur Nuwun
  Terima Kasih
- **Syukron**
  Merci bien
  ありがとう
  Obrigado
- **Dank**
- **Thanks**
- **Matur se Kelangkong**
- **Kheili Mamnun**
- ευχαριστίες
  Danke
- **Grazias**
- 谢谢