Keamanan Jaringan

57 . Firewall

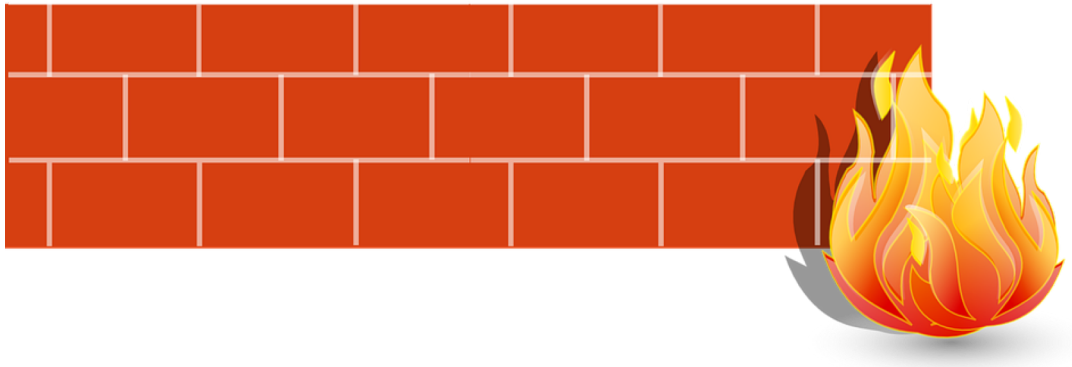
Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

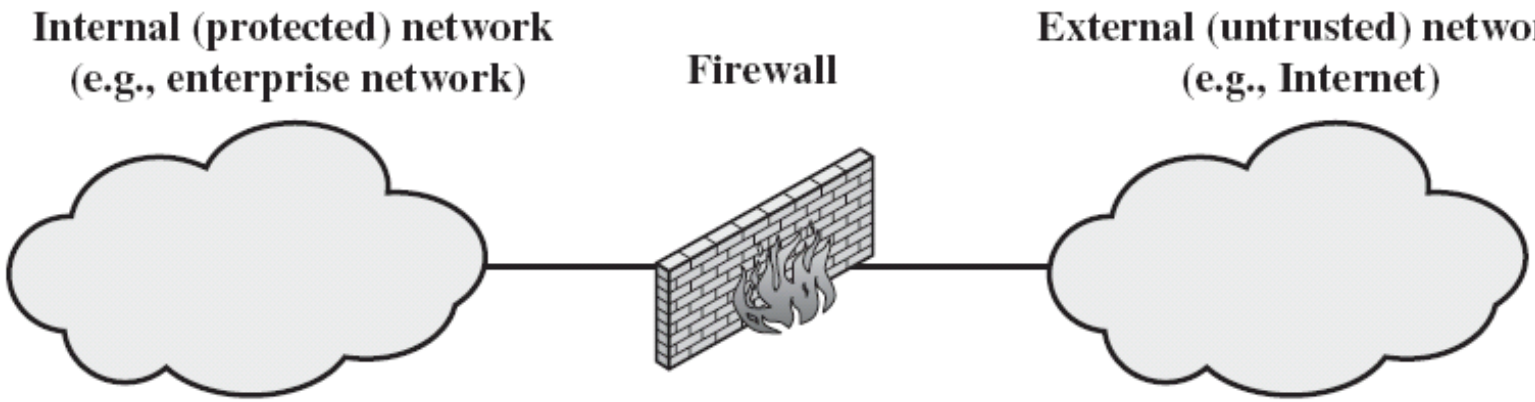
Telkom University.

Firewall

- Tembok Api



Internal Vs Eksternal



(a) General model

Tugas Firewall

- Monitoring
- Paket Masuk
- Paket Keluar

- Rules
- Mengijinkan
- Memblok paket

- Software / Hardware

Yang di monitor

- Alamat IP Pengirim
- Alamat IP Tujuan
- Port
- Jenis Paket

Rules

- Blok paket masuk dari alamat pengirim/ penerima tertentu
- Blok paket keluar dari alamat pengirim/ penerima tertentu
- Blok paket berdasarkan isi paket
- Membuka akses ke internal resource tertentu (
- Membuka koneksi ke jaringan internal
- Melaporkan semua aktifitas jaringan

Keamanan Jaringan

58. Tipe Firewall

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan
Telkom University.

Tipe Firewall

- Packet Filtering
- Circuit Level Gateway
- Application level Gateway
- Statefull Multilayer Inspection Firewall

Firewall Packet Filtering

- Network Layer (OSI)
- Router
- Setiap paket dibandingkan dengan berbagai kriteria (rules)
- Drop/ Forward
- Alamat IP Pengirim / Penerima
- Nomor port pengirim/ penerima
- Protokol

Circuit Level Gateway

- Session Layer (OSI)
- Gateway
- Monitor Request membuat session
- Data Stream

Application Level Firewall

- Proxy
- Application Layer (OSI;TCP/IP)
- Aplikasi, protokol dll
- Browser, FTP dll
- Drop FTP, Telnet dll

Statefull Multilayer Inspection Firewall

- Kombinasi 3 tipe Firewall
- Network layer
- Session
- Aplikasi

Keamanan Jaringan

59. Arsitektur Firewall

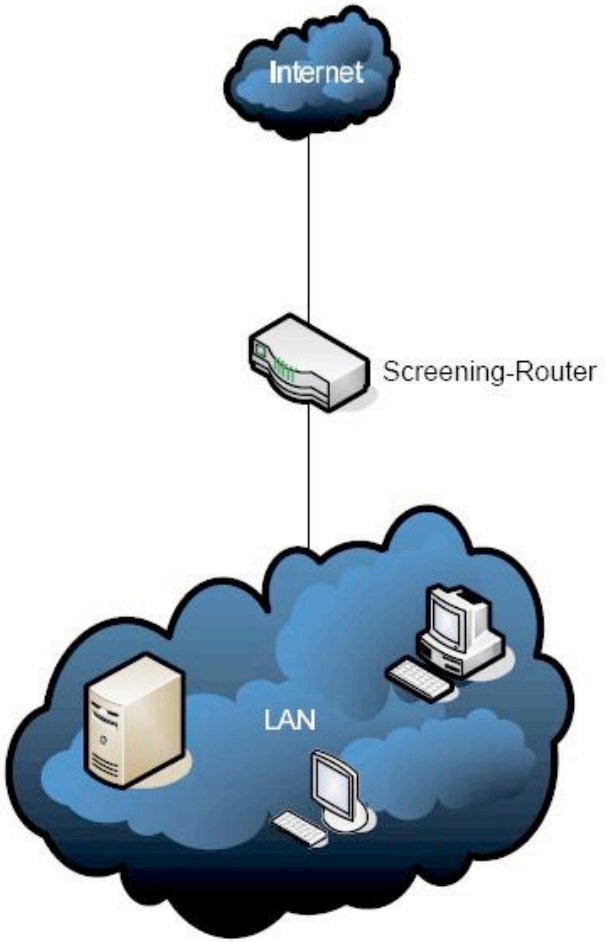
Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

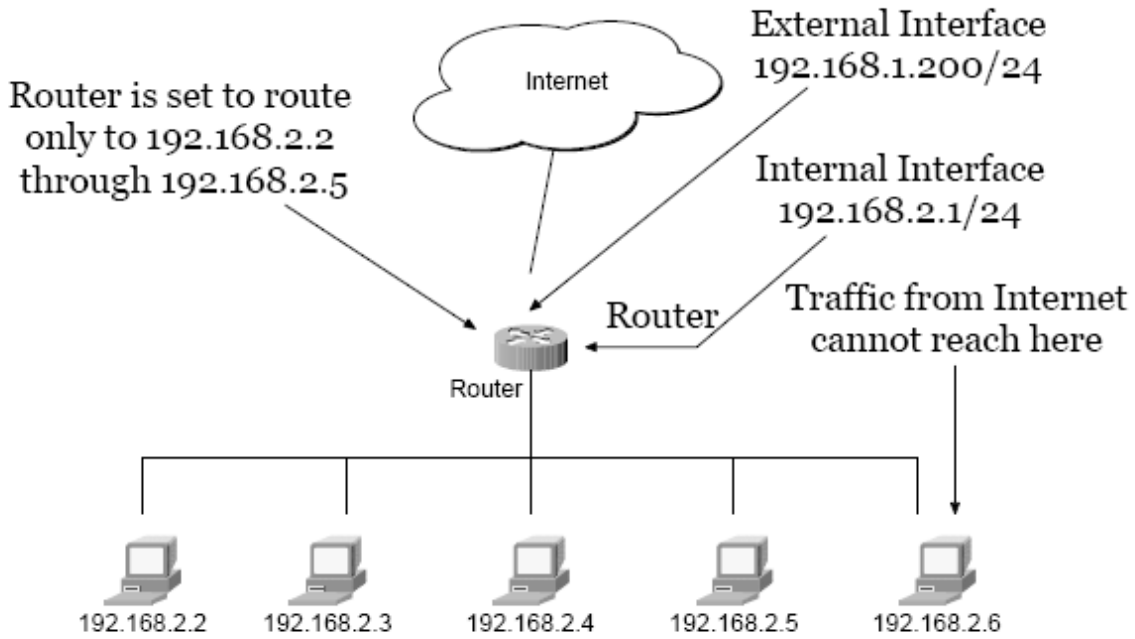
Screening Router

- Paketfilter
- Allow Outgoing
- Filter Incoming
- 2 Interface
- ACL
- Kekurangan Single Point of Error (SPoE)



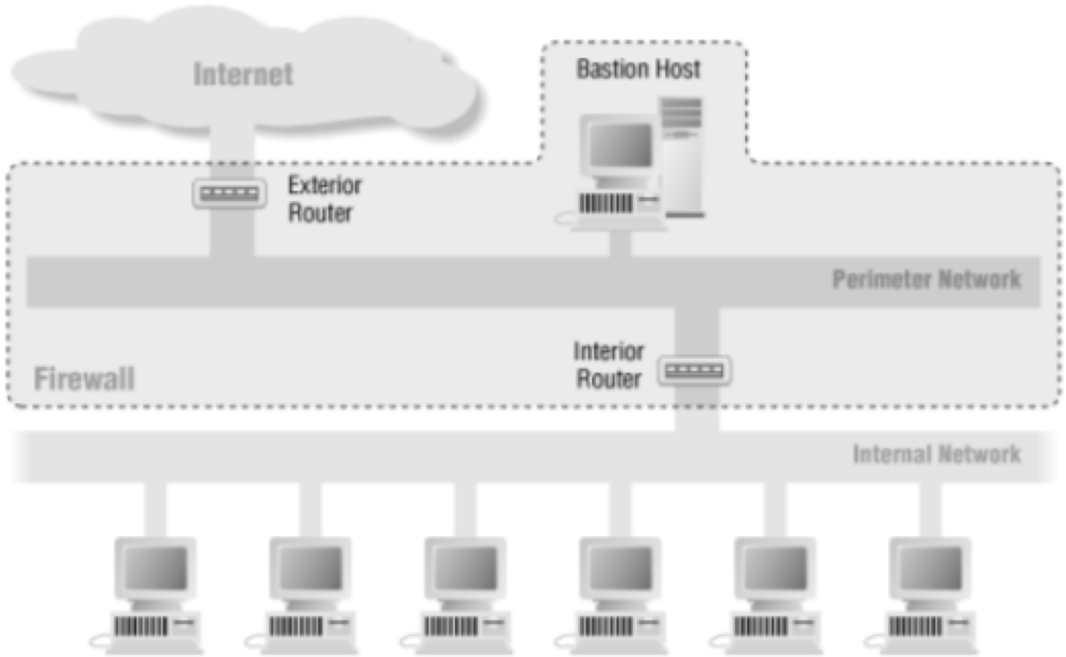
Screening Host

- Interface keluar 192.168.1.200
- Interface kedalam 192.168.2.1
- Akses dari luar ke 192.168.2.2-5
- Blok akses ke 192.168.2.8



Screening Subnet

- Melindungi 1 subnet



Contoh kebijakan Firewall

- Pembatasan akses dari jaringan eksternal
- Pembatasan akses yang tidak berhak dari jaringan internal
- Pembatasan akses ke jaringan eksternal
- Pembatasan akses pada layanan tertentu

Perlindungan Firewall Berlapis

- Aplikasi : Application level Gateway & Enkripsi data
- Session : SOCKS Proxy Server
- Transport : Packet Filtering
- Network : NAT
- Physical layer : -
- Data Link :

Keamanan Jaringan

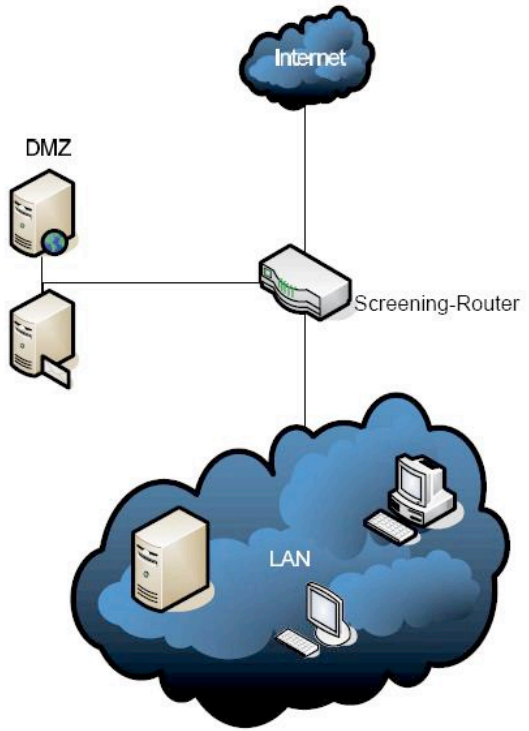
60. DMZ

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan
Telkom University.

DMZ (DeMiliterized Zone)

- Zona Khusus
- Layanan Publik (Web Server, Mail Server , DNS, FTP, VOIP)
- Melindungi Jaringan Internal
- DMZ – Internal dibatasi
- DMZ – Internet



DMZ

- Konfigurasi security ancaman Eksternal
- Ancaman Internal (Sniffing & Spoofing)

DMZ – Multi Firewall

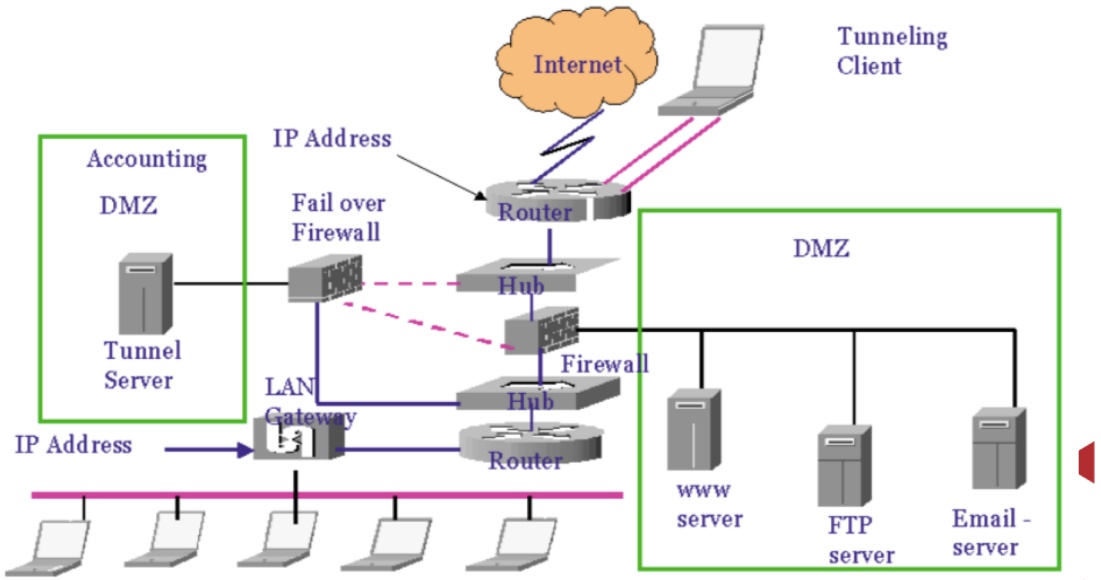
- Single Point of Error
- Firewall lebih dari satu
- 2 Firewall & 1 DMZ
- 2 Firewall & 2 DMZ

Multi Firewall

- Mahal
- Semakin Kompleks

2 DMZ – 2 Firewall

1. DMZ untuk layanan publik, Web Server, email dan DNS
2. VPN Tunnel – Data keuangan



Keamanan Jaringan

61 Contoh Firewall

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Firewall

- Windows Firewall
- ZoneAlarm
- Comodo
- Cisco Asa
- Check Point
- Untangle NG
- FortiGate
- Online Armor
- SonicWall
- Novell Border
- Jetico
- Outpost Security

Web Application Firewall (WAF)

- Monitor trafik HTTP
- ModSecurity
- Barracuda Network WAF
- Fortiweb
- Sophos XG
- Imperva Secure Sphere

Linux Firewall

- FireHOL
- Firestarter
- Firewall ID
- Netfilter
- MoBlock
- Nftables
- Privoxy
- Shorewall
- Squid
- UFW

Distro Linux

- Endian Firewall
- IPFire
- LEDE
- OpenWRT
- SmoothWall
- Untangle
- Zeroshell

- IPFilter
- IPFirewall
- NPF
- PF

BSD

- Monowall
- OPNsense
- Pfsense
- smallwall

Keamanan Jaringan

62. IPTables

Setia Juli Irzal Ismail

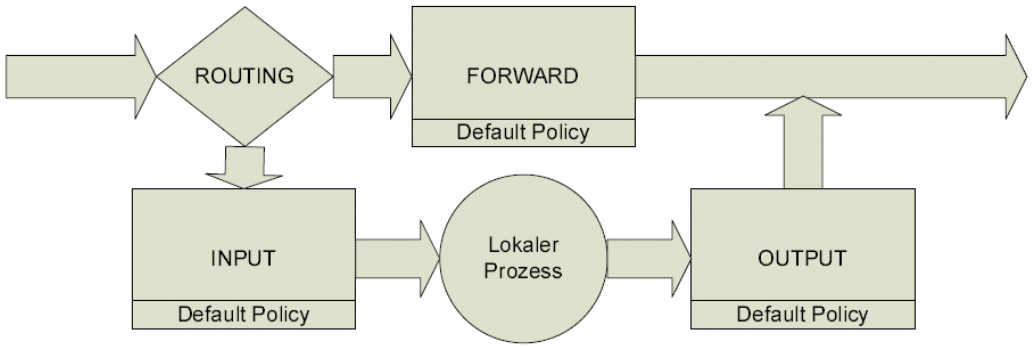
D3 Teknologi Komputer – Fakultas Ilmu Terapan

Telkom University.

Firewall Linux

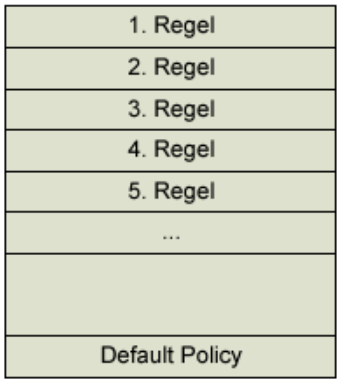
- Standar Linux
- Rules

- Input
- Forward
- Output



IPTables

- Accept
- Drop
- Return
- Queue



Contoh Rules

- Allow semua akses ke semua Website
- Allow outgoing email dari internal mail server
- Drop semua akses outgoing kecuali ke email dan website
- Drop semua incoming akses kecuali ke public web server
- Log semua akses ke website luar
- Log semua koneksi yang diblok Firewall

Contoh Rules

- Iptables –L : list
- -D :hapus
- -I : masukan rules baru
- -F : hapus semua
- -h : bantuan

Rule Set A

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

Rule Set B

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

Rule Set C

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

Rule Set D

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

Rule Set 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

Contoh rules IPtables

1. Iptables -A OUTPUT -j ACCEPT : mengijinkan semua trafik keluar
2. -A INPUT -p tcp --dport 80 -j ACCEPT : http
3. -A INPUT -p tcp -m state --state NEW --dport 22 -j ACCEPT : SSH
4. -A INPUT -j REJECT : kedalam
5. -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT : ping

Keamanan Jaringan

63. Serangan Firewall

Setia Juli Irzal Ismail

D3 Teknologi Komputer – Fakultas Ilmu Terapan
Telkom University.

Deteksi Firewall

- Port Scanning
- Firewalking (nilai TTL)
- Banner Grabbing
- Ftp, Telnet, Web server
- telnet mail.target.org 25

Evading

- IP Spoofing
- Source Routing
- Fragmen kecil

Evasion tool

- Traffic IQ Profesional
- TCP over DNS
- Snare Agent
- AckCMD
- Tomahawk
- Atelier
- Freenet
- Gtunnel
- Hotspot Shield
- Proxifier
- VPN One Click
- Your Freedom

Bypass Firewall

- Alamat IP
- Proxy Server
- ICMP Tunelling
- ACK Tunelling
- HTTP Tunelling
- SSH Tunelling

Tools tunnelling

- HTTPort; HTTHost
- Super Network Tunnel
- HTTP Tunnel
- BitVise

Defense

- Matikan port switch penyerang
- Analisa trafik
- Reset TCP Session penyerang
- Update sistem
- Hardening
- Blok paket TTL expired
- Rubah TTL → besar

REFERENSI

Engebretson, P. (2011). The Basic of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress

Stallings, W. (2010). Network Security Essentials:Applications and Standards 4th Edition. Prentice Hall.

Rash, M. (2007). Linux Firewalls: Attack Detection and Response with Iptables, psad and fwsnort. No Starch.