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..
❖ Insya allah menjadi amal ibadah , Manjadda Wajadda !!

AGENDA

- Introduction/Defense in Depth
- Using Perimeter Defenses
- Using ISA Server to Protect Perimeters
- Using ICF to Protect Clients
- Protecting Wireless Networks
- Protecting Communications by Using IPSec

❖ Agenda Pembahasan ke-6 dari 6 agenda Network and Internet Defense

GOALS OF NETWORK SECURITY

	Perimeter Defense	Client Defense	Intrusion Detection	Network Access Control	Confi-dentiality	Secure Remote Access
ISA Server	X		X	X		X
ICF		X				
802.1x / WPA				X	X	
IPSec		X			X	X

Komponen IP Sec yang akan dibahas dalam Goal of Network Security

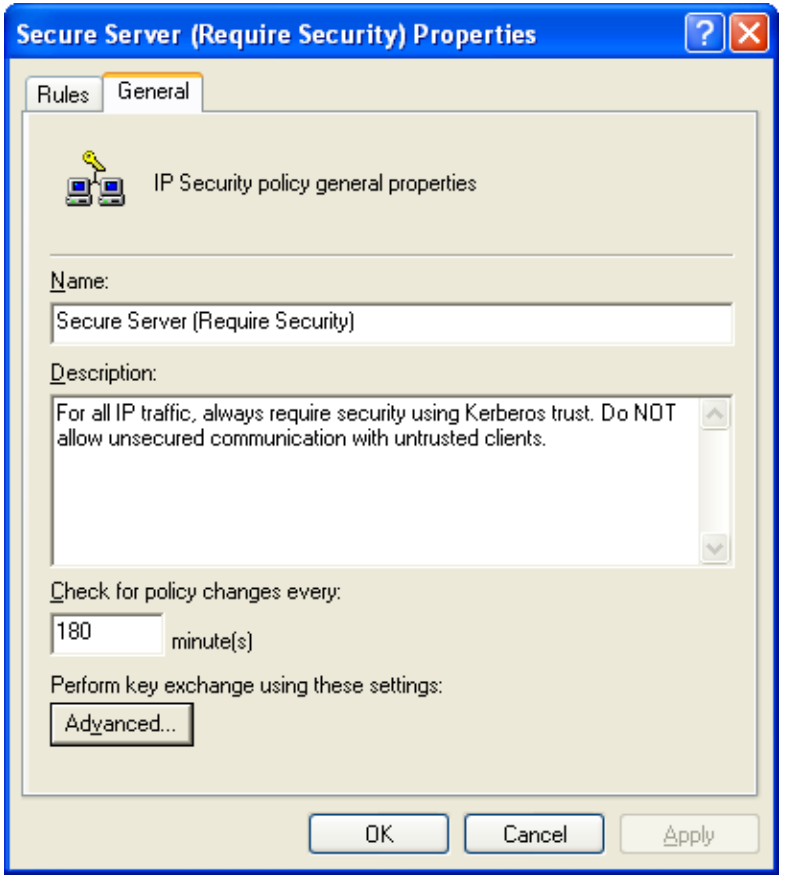
OVERVIEW OF IPSEC

- **What is IP Security (IPSec)?**
  - **A method to secure IP traffic**
  - **Framework of open standards developed by the Internet Engineering Task Force (IETF)**
- **Why use IPSec?**
  - **To ensure encrypted and authenticated communications at the IP layer**
  - **To provide transport security that is independent of applications or application-layer protocols**

❖ Apa dan mengapa IPSec diperlukan dalam Network and Internet Defense

IPSEC SCENARIOS

- **Basic permit/block packet filtering**
- **Secure internal LAN communications**
- **Domain replication through firewalls**
- **VPN across untrusted media**



❖ Skenario IP Sec dalam Protecting Communications by Using IPSec

IMPLEMENTING IPSEC PACKET FILTERING

- Filters for allowed and blocked traffic
- No actual negotiation of IPSec security associations
- Overlapping filters—most specific match determines action
- Does not provide stateful filtering
- Must set "NoDefaultExempt = 1" to be secure

From IP	To IP	Protocol	Src Port	Dest Port	Action
Any	My Internet IP	Any	N/A	N/A	Block
Any	My Internet IP	TCP	Any	80	Permit

❖ Skenario IP Sec dalam implementasi IPSec Filtering

PACKET FILTERING IS NOT SUFFICIENT TO PROTECT SERVER

- **Spoofed IP packets containing queries or malicious content can still reach open ports through firewalls**
- **IPSec does not provide stateful inspection**
- **Many hacker tools use source ports 80, 88, 135, and so on, to connect to any destination port**

❖ Info terkait Protecting Communications by Using IPSec, bahwa Packet Filtering is not sufficient

TRAFFIC NOT FILTERED BY IPSEC

- IP broadcast addresses
  - Cannot secure to multiple receivers
- Multicast addresses
  - From 224.0.0.0 through 239.255.255.255
- Kerberos—UDP source or destination port 88
  - Kerberos is a secure protocol, which the Internet Key Exchange (IKE) negotiation service may use for authentication of other computers in a domain
- IKE—UDP destination port 500
  - Required to allow IKE to negotiate parameters for IPSec security
- Windows Server 2003 configures only IKE default exemption

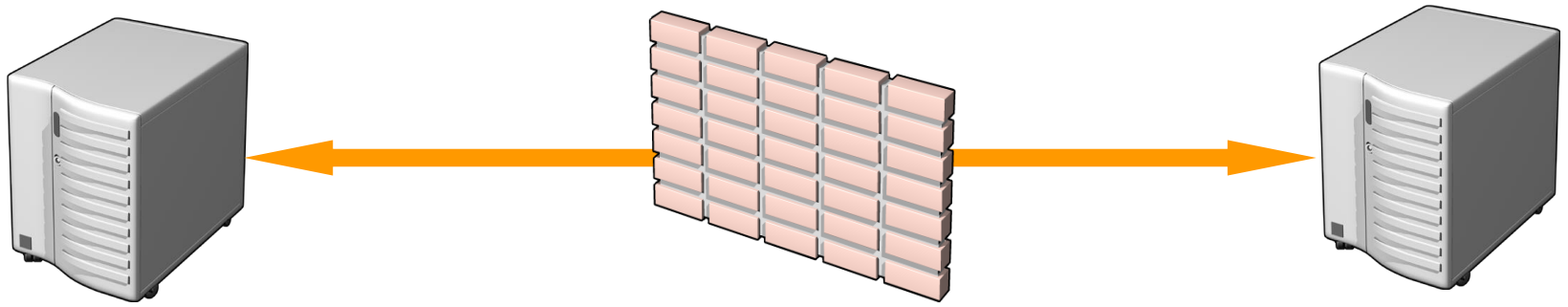
SECURE INTERNAL COMMUNICATIONS

- **Use IPSec to provide mutual device authentication**
  - **Use certificates or Kerberos**
  - **Preshared key suitable for testing only**
- **Use Authentication Header (AH) to ensure packet integrity**
  - **AH provides packet integrity**
  - **AH does not encrypt, allowing for network intrusion detection**
- **Use Encapsulation Security Payload (ESP) to encrypt sensitive traffic**
  - **ESP provides packet integrity and confidentiality**
  - **Encryption prevents packet inspection**
- **Carefully plan which traffic should be secured**

❖ Info terkait tentang Protecting Communications by Using IPSec, Secure Internal Communication

IPSEC FOR DOMAIN REPLICATION

- **Use IPSec for replication through firewalls**
  - **On each domain controller, create an IPSec policy to secure all traffic to the other domain controller's IP address**
- **Use ESP 3DES for encryption**
- **Allow traffic through the firewall:**
  - **UDP Port 500 (IKE)**
  - **IP protocol 50 (ESP)**



❖ Info terkait Protecting Communications by Using IP Sec For Domain Replication

VPN Across Untrusted Media

- Client VPN
  - Use L2TP/IPSec
- Branch Office VPN
  - Between Windows 2000 or Windows Server, running RRAS: Use L2TP/IPSec tunnel (easy to configure, appears as routable interface)
  - To third-party gateway: Use L2TP/ISec or pure IPSec tunnel mode
  - To Microsoft Windows NT® 4 RRAS Gateway: Use PPTP (IPSec not available)

IPSEC PERFORMANCE

- IPSec processing has some performance impact
  - IKE negotiation time—about 2–5 seconds initially
    - 5 round trips
    - Authentication—Kerberos or certificates
    - Cryptographic key generation and encrypted messages
    - Done once per 8 hours by default, settable
  - Session rekey is fast—<1–2 seconds, 2 round trips, once per hour, settable
  - Encryption of packets
- How to improve?
  - Offloading NICs do IPSec almost at wire speed
  - Using faster CPUs

❖ IP Sec Performance dalam Protecting Communications by Using IPSec

BEST PRACTICES

- Plan your IPSec implementation carefully
- Choose between AH and ESP
- Use Group Policy to implement IPSec Policies
- Consider the use of IPSec NICs
- Never use Shared Key authentication outside your test lab
- Choose between certificates and Kerberos authentication
- Use care when requiring IPSec for communications with domain controllers and other infrastructure servers

PERIMETER AND INTERNAL DEFENSES

- Commonly deployed defenses
  - Perimeter defenses – Firewall, IDS
    - Protect local area network and hosts
    - Keep external threats from internal network
  - Internal defenses – Virus scanning
    - Protect hosts from threats that get through the perimeter defenses
  - Extend the "perimeter" – VPN
- Common practices, but could be improved
  - Internal threats are significant
    - Unhappy employees
    - Compromised hosts

❖ Hal hal lain terkait dengan Perimeter and Internal Defense

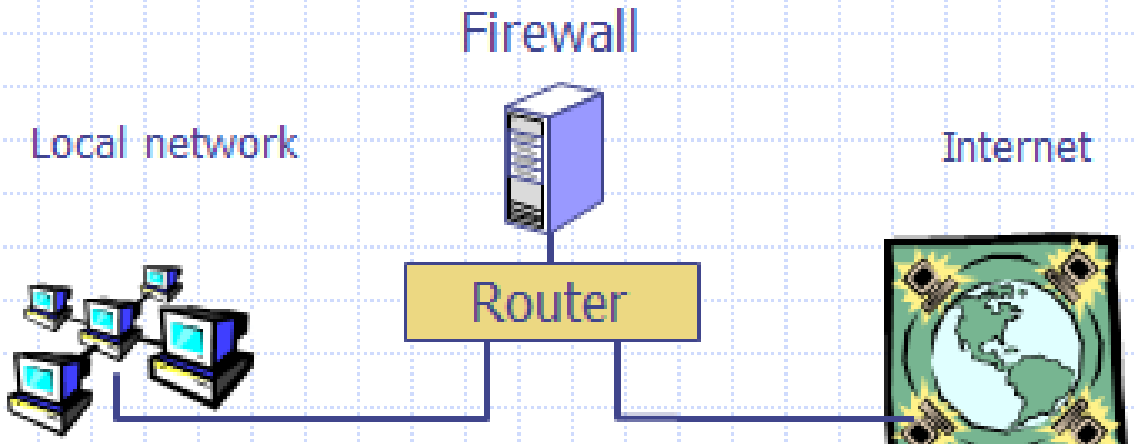
FOKUS

- Standard perimeter defense mechanisms
  - Firewall
    - Packet filter (stateless, stateful)
    - Application layer proxies
  - Traffic shaping
  - Intrusion detection
    - Anomaly and misuse detection
    - Methods applicable to network or host
- Future lectures
  - Virus and malware
  - Worm propagation and detection

❖ Fakus dalam Perimeter Network and Internet Defense

BASIC FIREWALL CONCEPT

- Separate local area net from internet



All packets between LAN and internet routed through firewall

- Basic Firewall Concept dalam Network and Internet Defense

FIREWALL GOALS

- Prevent malicious attacks on hosts
  - Port sweeps, ICMP echo to broadcast addr, syn flooding, …
  - Worm propagation
    - Exploit buffer overflow in program listening on network
- Prevent general disruption of internal network
  - External SMNP packets
- Provide defense in depth
  - Programs contain bugs and are vulnerable to attack
  - Network protocols may contain;
    - Design weaknesses (SSH CRC)
    - Implementation flaws (SSL, NTP, FTP, SMTP…)
- Control traffic between "zones of trusts"
  - Can control traffic between separate local networks, etc

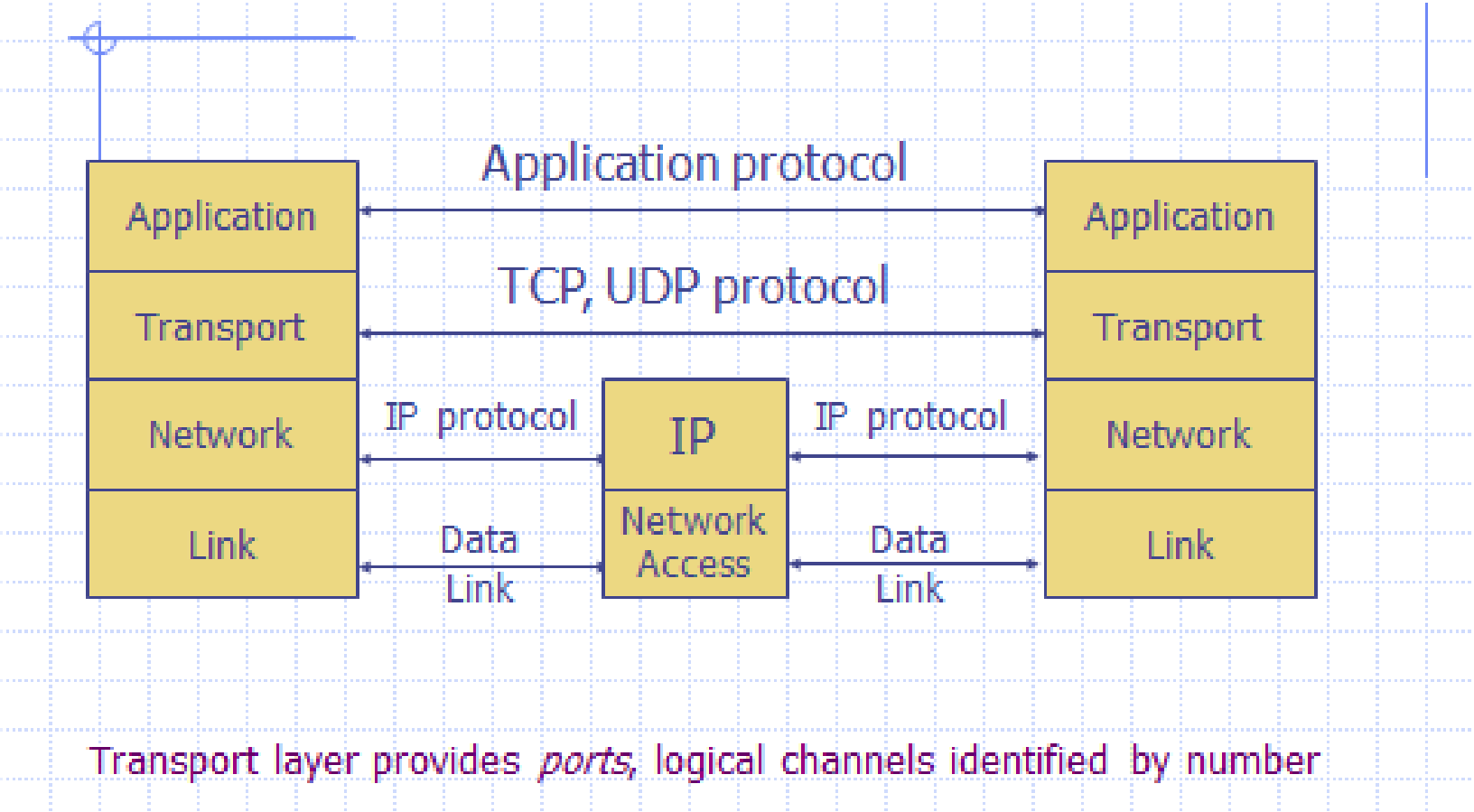
❖ Penerapan Firewall dalam Network and Internet Defense

TWO SEPARABLE TOPIC

- Arrangement of firewall and routers
  - Several different network configurations
    - Separate internal LAN from external Internet
    - Wall off subnetwork within an organization
    - Intermediate zone for web server, etc.
  - Personal firewall on end-user machine
- How the firewall processes data
  - Packet filtering router
  - Application-level gateway
    - Proxy for protocols such as ftp, smtp, http, etc.
  - Personal firewall
    - E.g., disallow telnet connection from email client

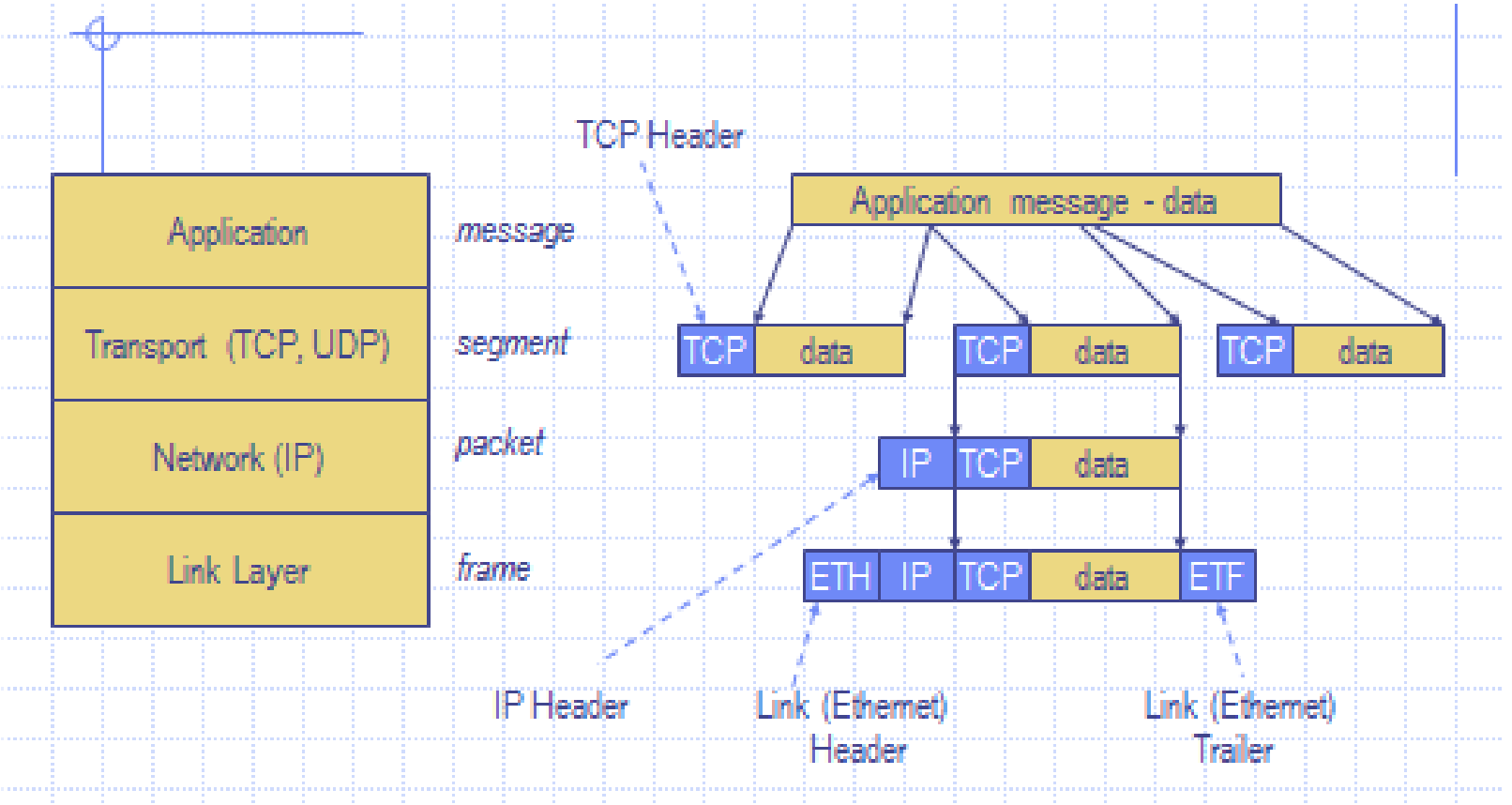
❖ Bentuk Two Separable dalam lingkup Network and Internet Defense

REVIEW : TCP PROTOCOL STACK



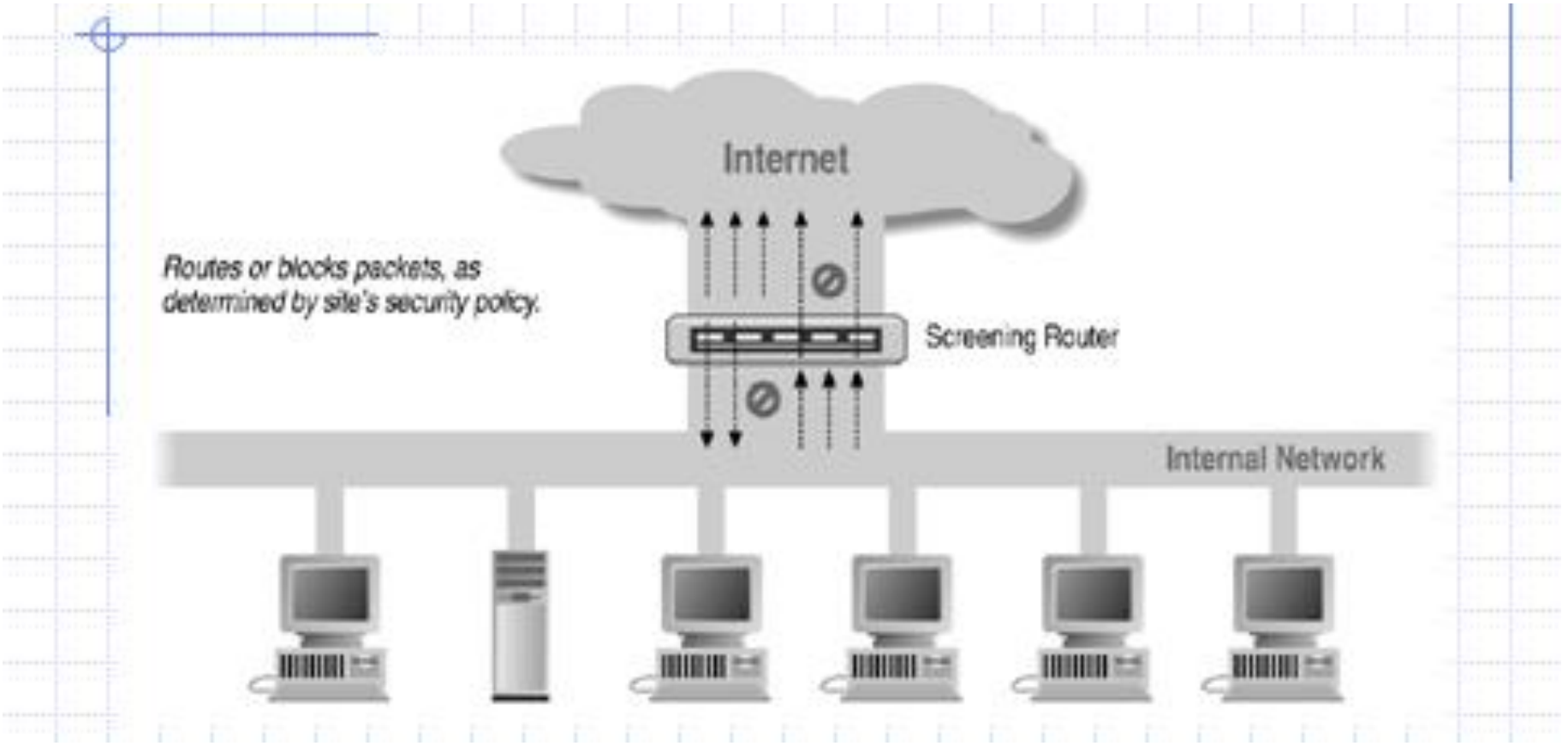
- TCP Protocol Stack, dasar kemampuan yang harus diketahui

REVIEW : DATA FORMATS



- Data Format dari TCP / IP

SCREENING ROUTER FOR PACKET FILTERING



- Bagan Router untuk Packet Filtering dalam Network and Internet Defense

PACKET FILTERING

- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Examples
  - DNS uses port 53
    - Block incoming port 53 packets except known trusted servers
- Issues
  - Stateful filtering
  - Encapsulation: address translation, other complications
  - Fragmentation

❖ Point penting dalam Packet Filtering

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

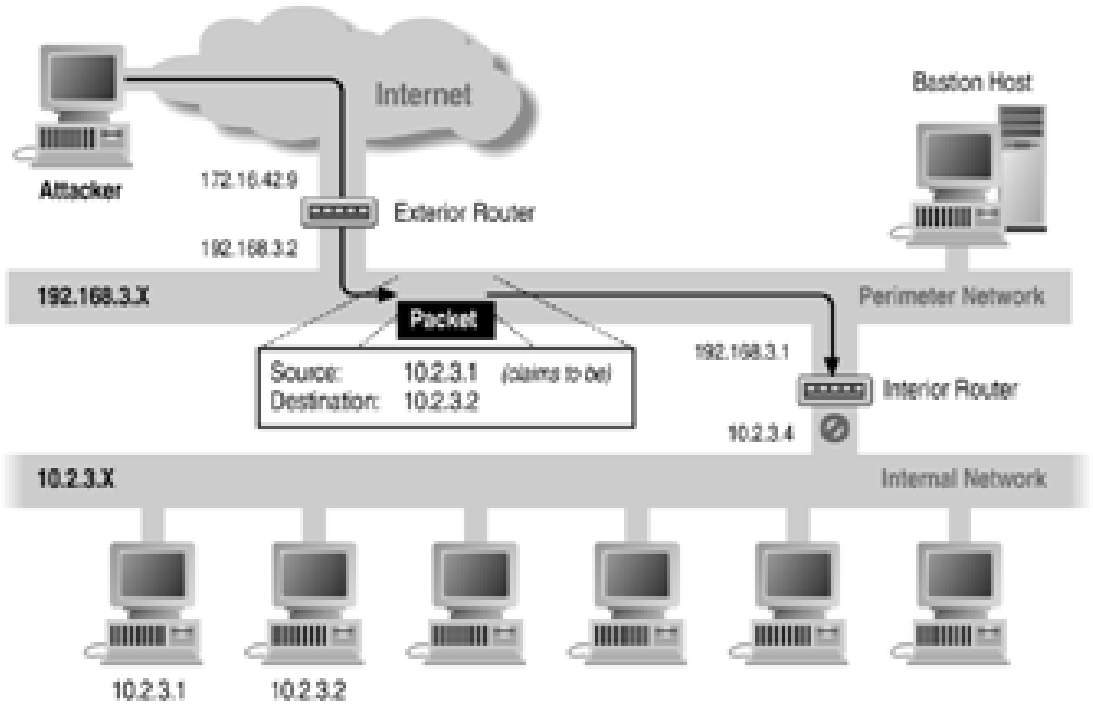
E

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

Compare: Tiny Personal Firewall, ZoneAlarm

- Contoh Packet Filtering dalam Network and Internet Defense

DESTINATION ADDRESS FORGERY



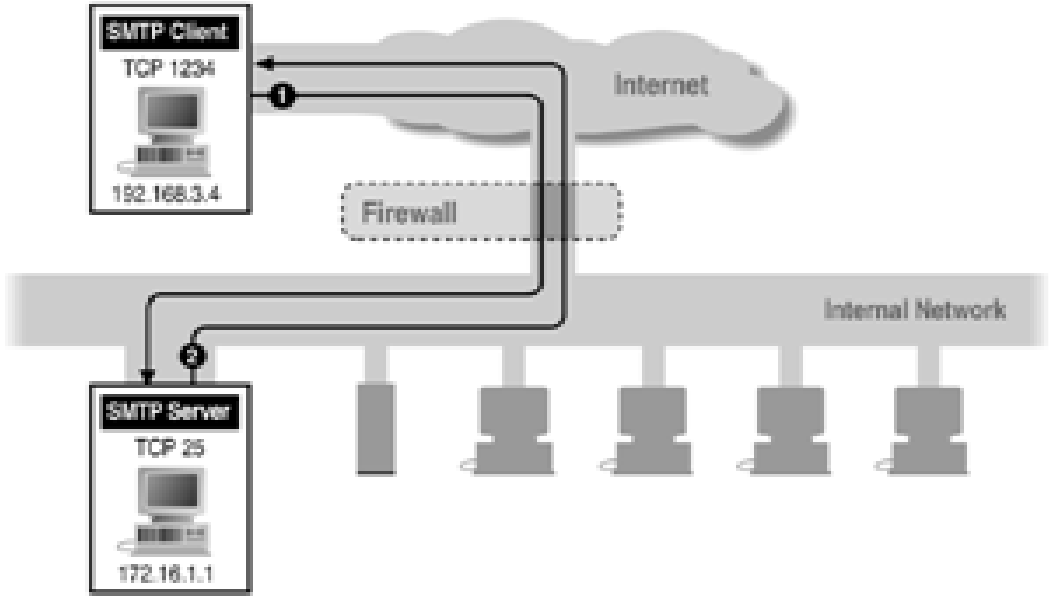
- Destination Address Forgery dalam Network and Internet Defense

PORT NUMBERING

- TCP connection
  - Server port uses number less than 1024
  - Client port uses number between 1024 and 16383
- Permanent assignment
  - Ports <1024 assigned permanently
    - 20,21 for FTP 23 for Telnet
    - 25 for server SMTP 80 for HTTP
- Variable use
  - Ports >1024 must be available for client to make connection
  - Limitation for stateless packet filtering
    - If client wants port 2048, firewall must allow incoming traffic
  - Better: stateful filtering knows outgoing requests
    - Only allow incoming traffic on high port to a machine that has initiated an outgoing request on low port

❖ Info tentang Port Numbering

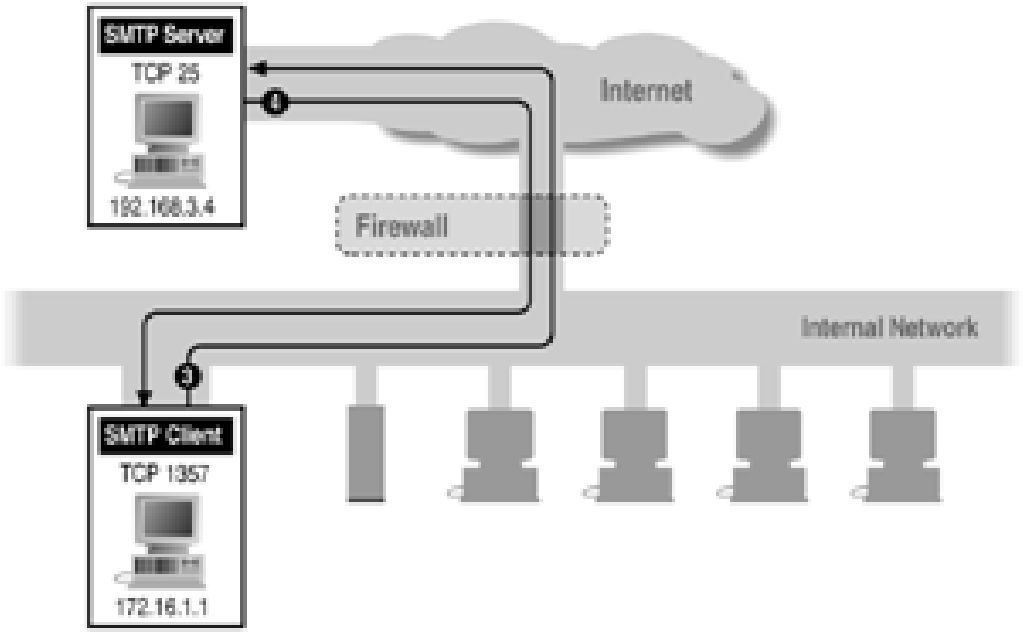
INBOUND SMTP



Can block external request to internal server based on port number

- Bentuk dan bagan dari Inbound SMTP

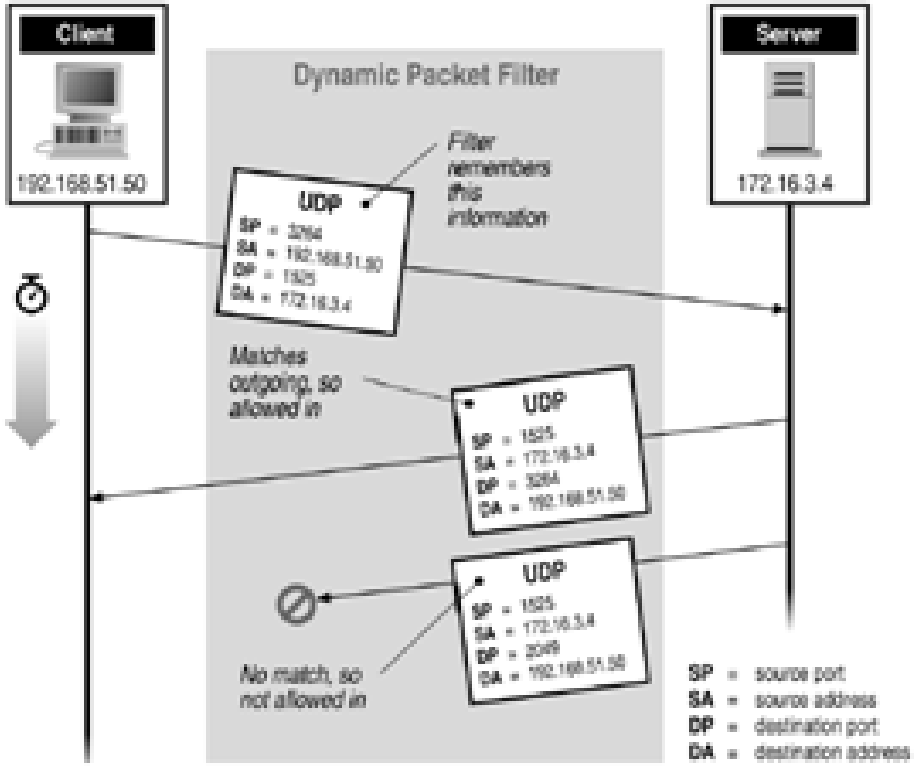
OUTBOUND SMTP



Known low port out, arbitrary high port in
If firewall blocks incoming port 1357 traffic then connection fails

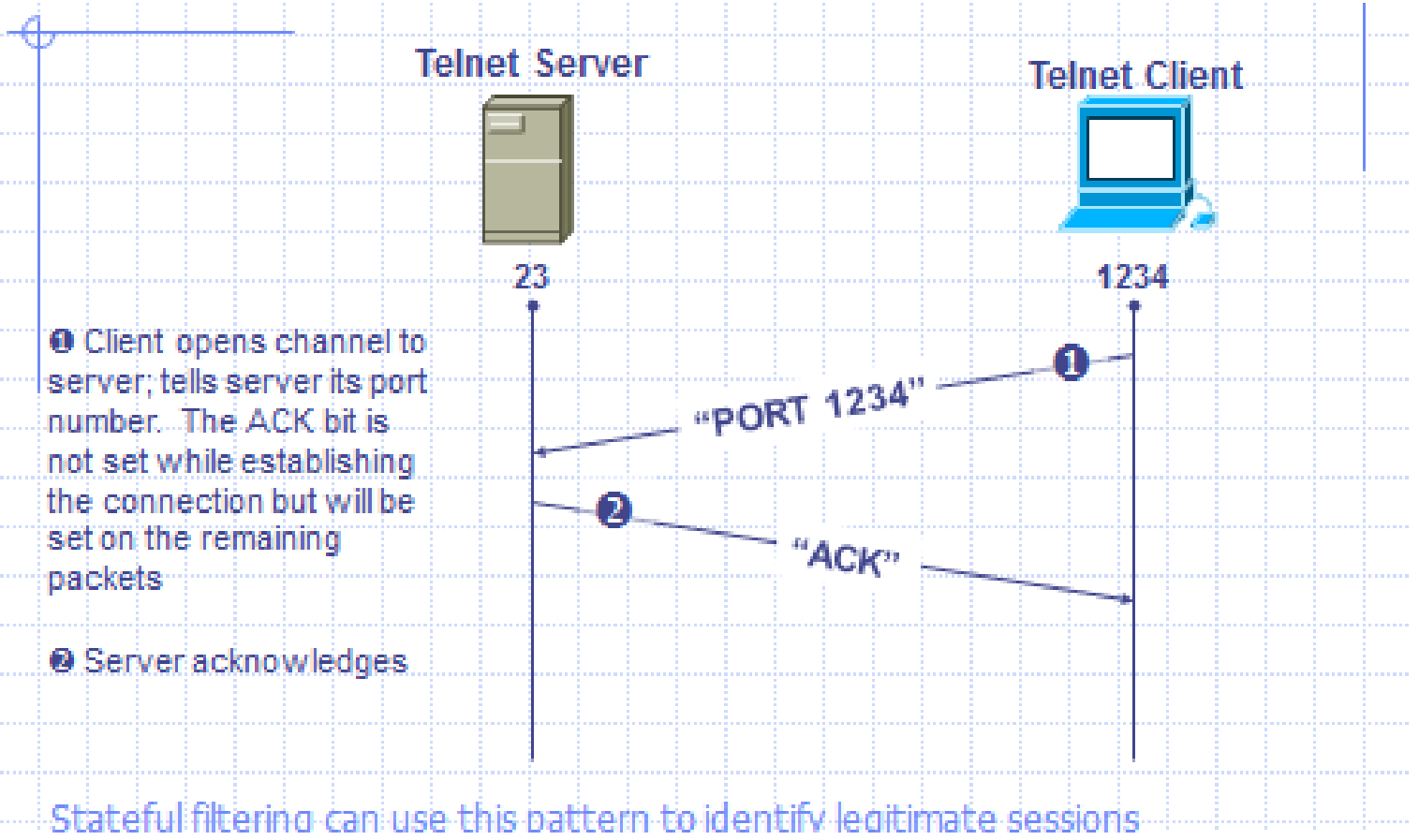
- Bentuk dan Bagan Outbound SMTP dalam Network and Internet Defense

PACKET FILTERING



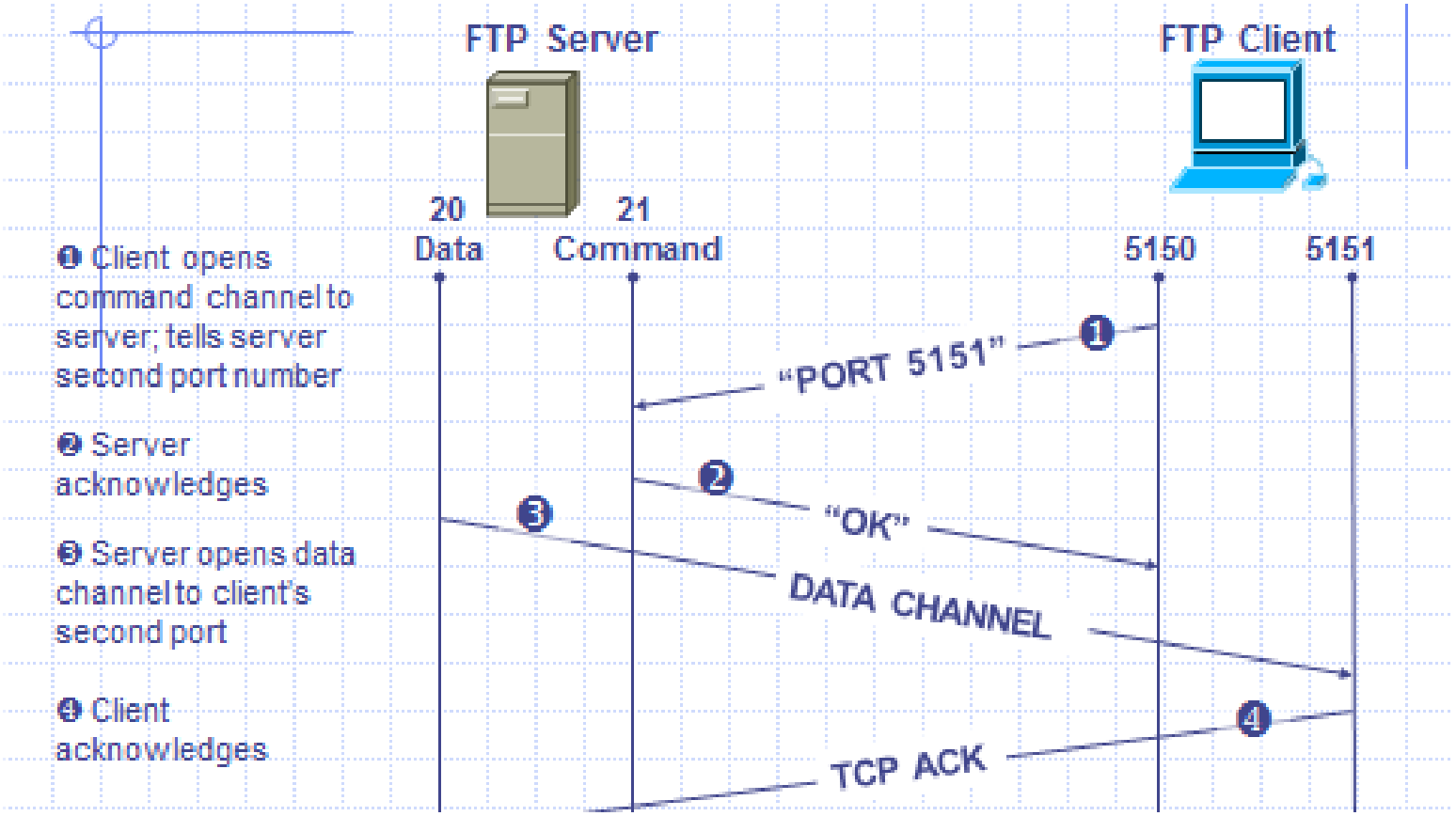
- Gambar dan pola Packet Filtering dalam Network and Internet Defense

TELNET



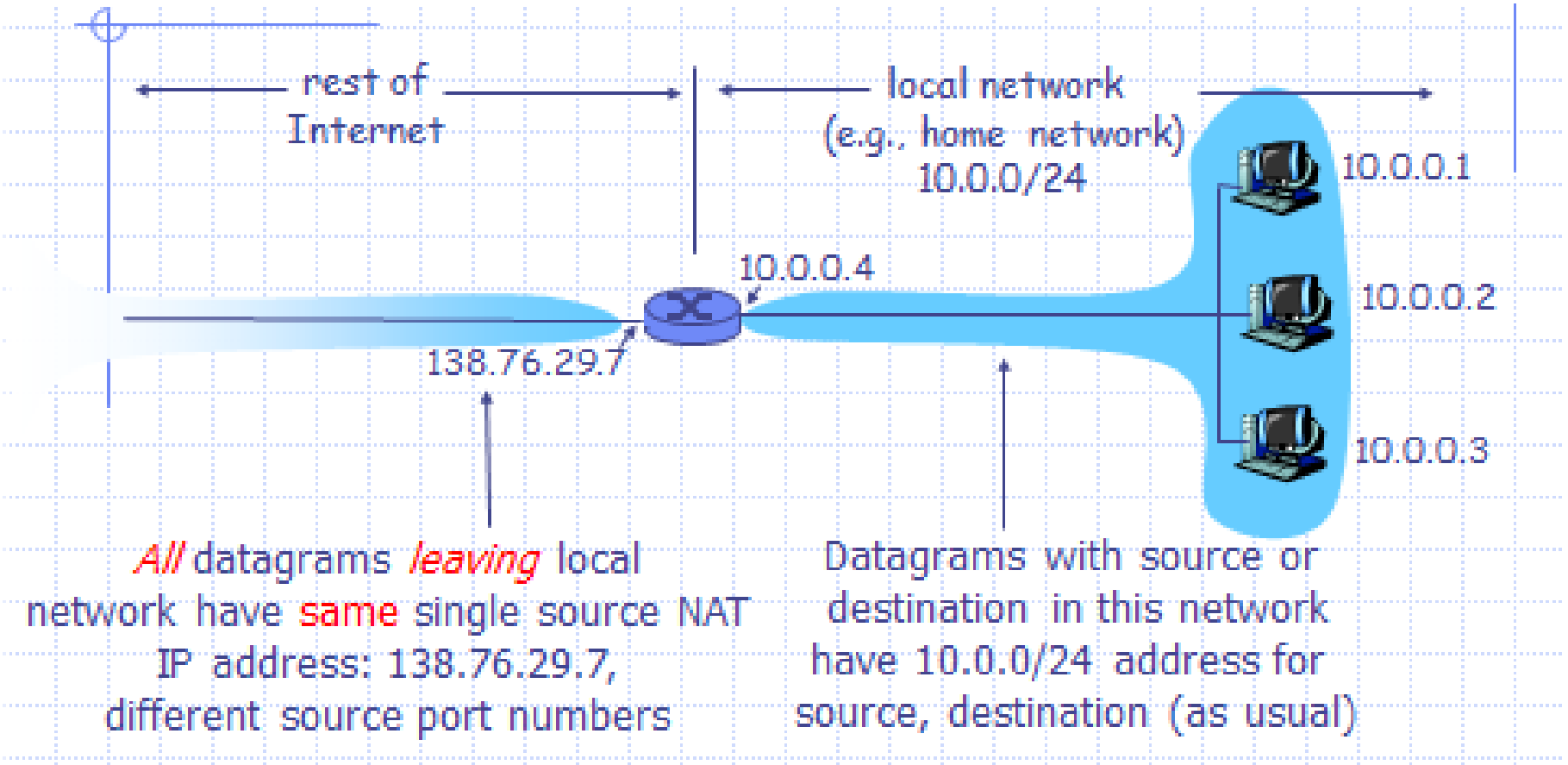
- Gambar dan pola Telnet dalam implementasi secara menyeluruh Network and Internet Defense

FTP



- Gambar dan pola Telnet dalam implementasi secara menyeluruh Network and Internet Defense

NETWORK ADDRESS TRANSLATION



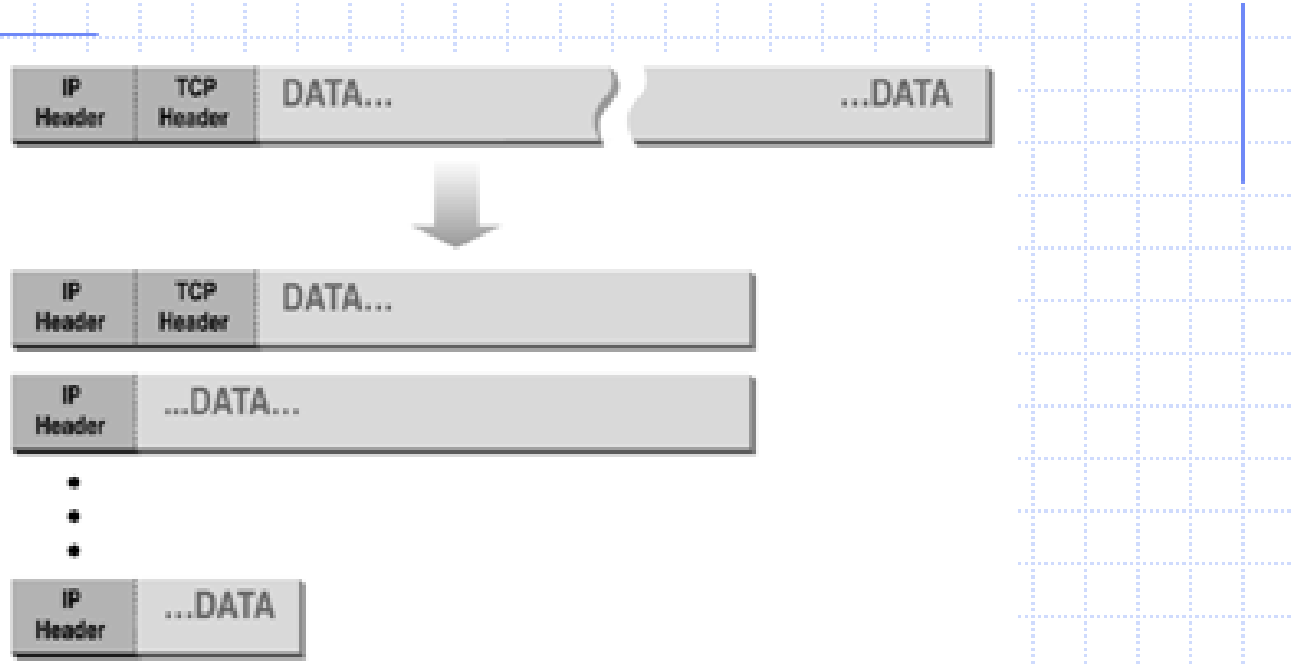
- Gambar dan pola Neteork Address Translation dalam Network and Internet Defense

ADVANTAGES OF NAT

- Motivations for NAT
  - Limited address space
  - Prevent unsolicited inbound requests
    - Port numbering: host behind NAT not reachable as server
  - Avoid renumbering if provider changes
    - Small/mid-sized LANs inherit address space from ISP
- Addresses hidden by NAT
  - Normal routing
    - Outgoing msg from 171.64.78.90 contains sending address
    - Recipient or observer can access 171.64.78.90
  - Addressing with NAT
    - NAT rewrites outgoing packet so recipient sees public addr only
    - An outside computer cannot see 171.64.78.90

❖ NAT : dalam Advantages NAT

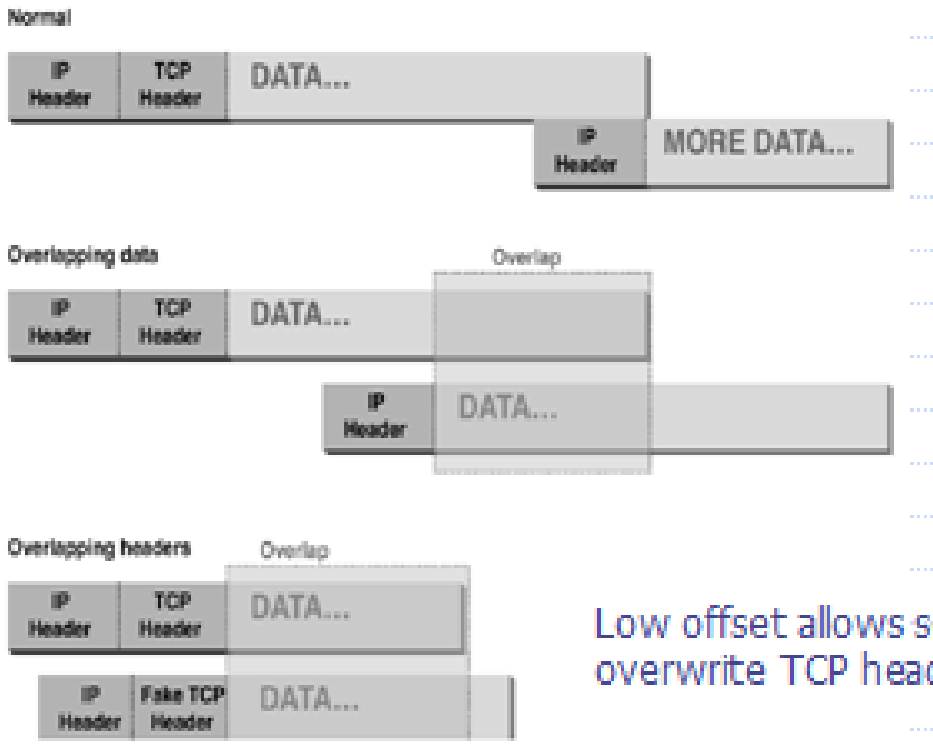
NORMAL IP FRAGMENTATION



Flags and offset inside IP header indicate packet fragmentation

- Normal IP Fragmentation, IP – TCP dan DATA

ABNORMAL FRAGMENTATION



Low offset allows second packet to overwrite TCP header at receiving host

- Abnormal Fragmentation – TCP – IP Data

FRAGMENTATION ATTACK

- Firewall configuration
  - TCP port 23 is blocked but SMTP port 25 is allowed
- First packet
  - Fragmentation Offset = 0.
  - DF bit = 0 : "May Fragment"
  - MF bit = 1 : "More Fragments"
  - Destination Port = 25. TCP port 25 is allowed, so firewall allows packet
- Second packet
  - Fragmentation Offset = 1: second packet overwrites all but first 8 bits of the first packet
  - DF bit = 0 : "May Fragment"
  - MF bit = 0 : "Last Fragment."
  - Destination Port = 23. Normally be blocked, but sneaks by!
- What happens
  - Firewall ignores second packet "TCP header" because it is fragment of first
  - At host, packet reassembled and received at port 23

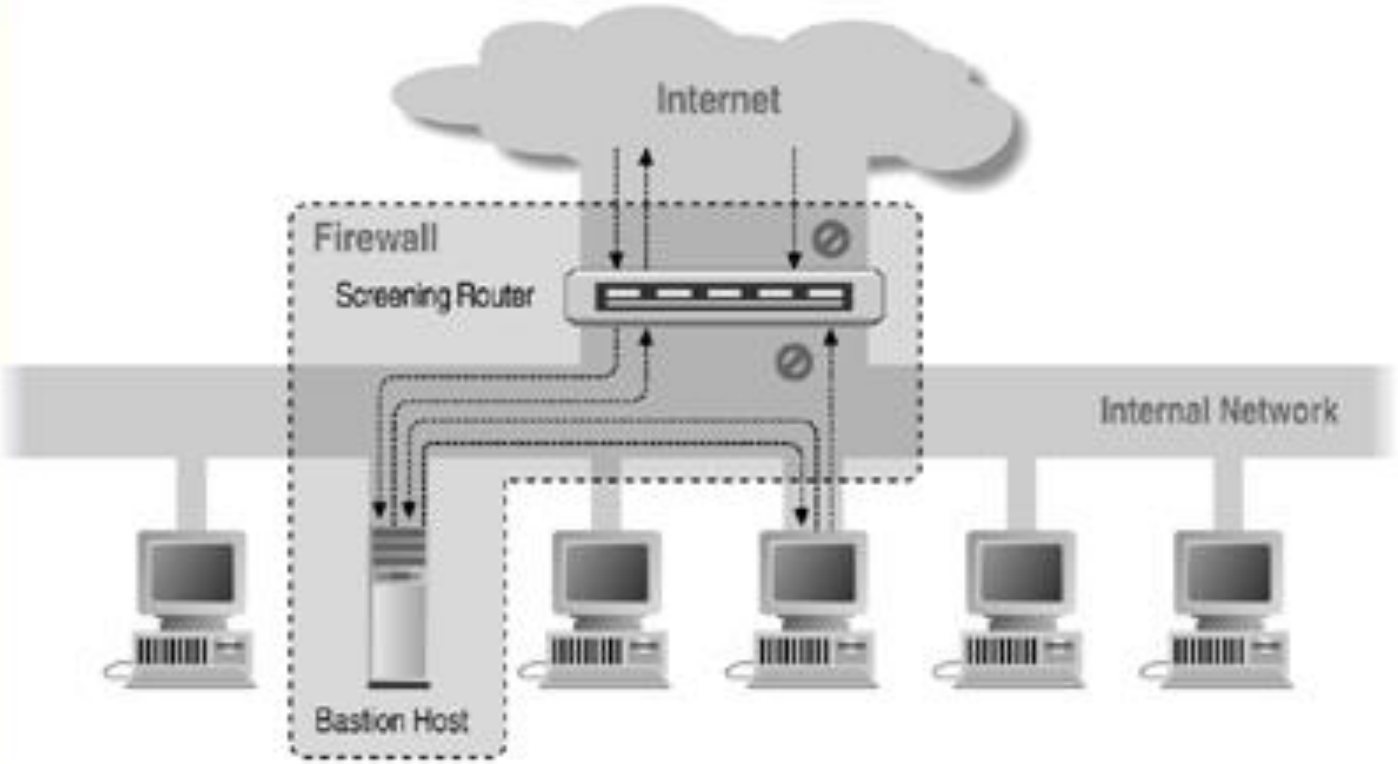
❖ Fragmentation Attack dalam lingkup Network and Internet Defense

PROXYING FIREWALL

- Several network locations – see next slides
- Two kinds of proxies
  - Circuit-level proxies
    - Works at session layer (which I omitted from OSI diagram)
  - Application-level proxies
    - Tailored to http, ftp, smtp, etc.
    - Some protocols easier to proxy than others
- Policy embedded in proxy programs
  - Proxies filter incoming, outgoing packets
  - Reconstruct application-layer messages
  - Can filter specific application-layer commands, etc.
    - Example: only allow specific ftp commands
    - Other examples: ?

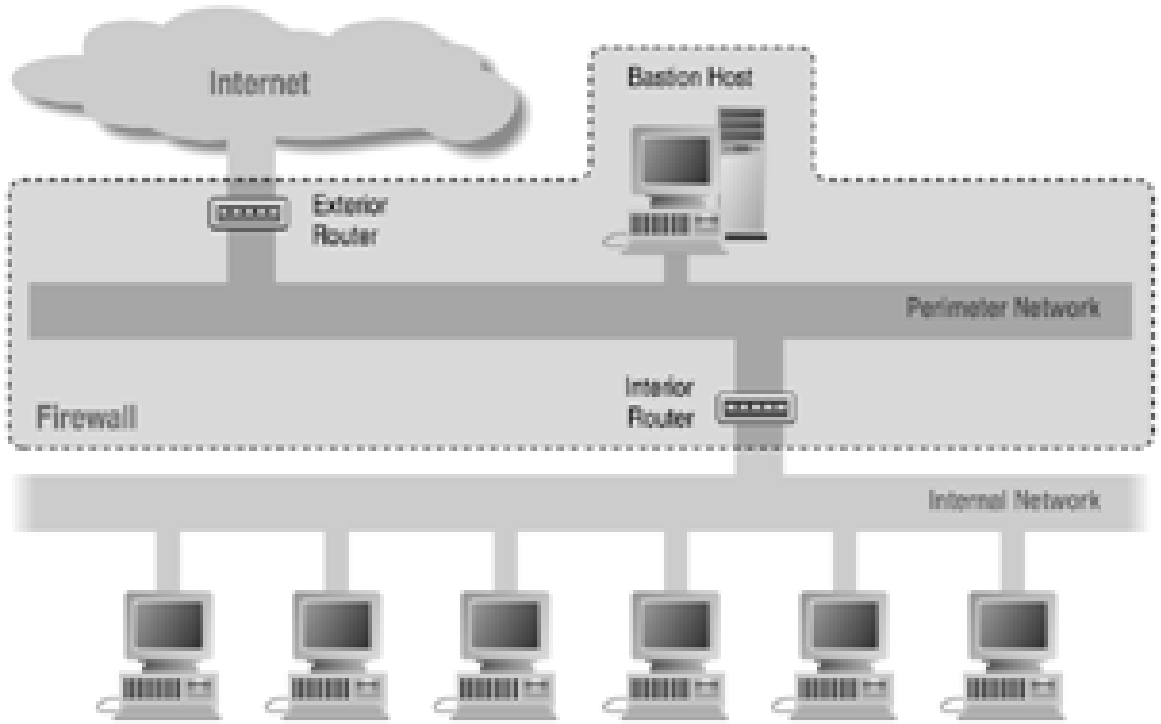
❖ Proxing Firewall dalam lingkup Network and Internet Defense

SCREENED HOST ARCHITECTURE



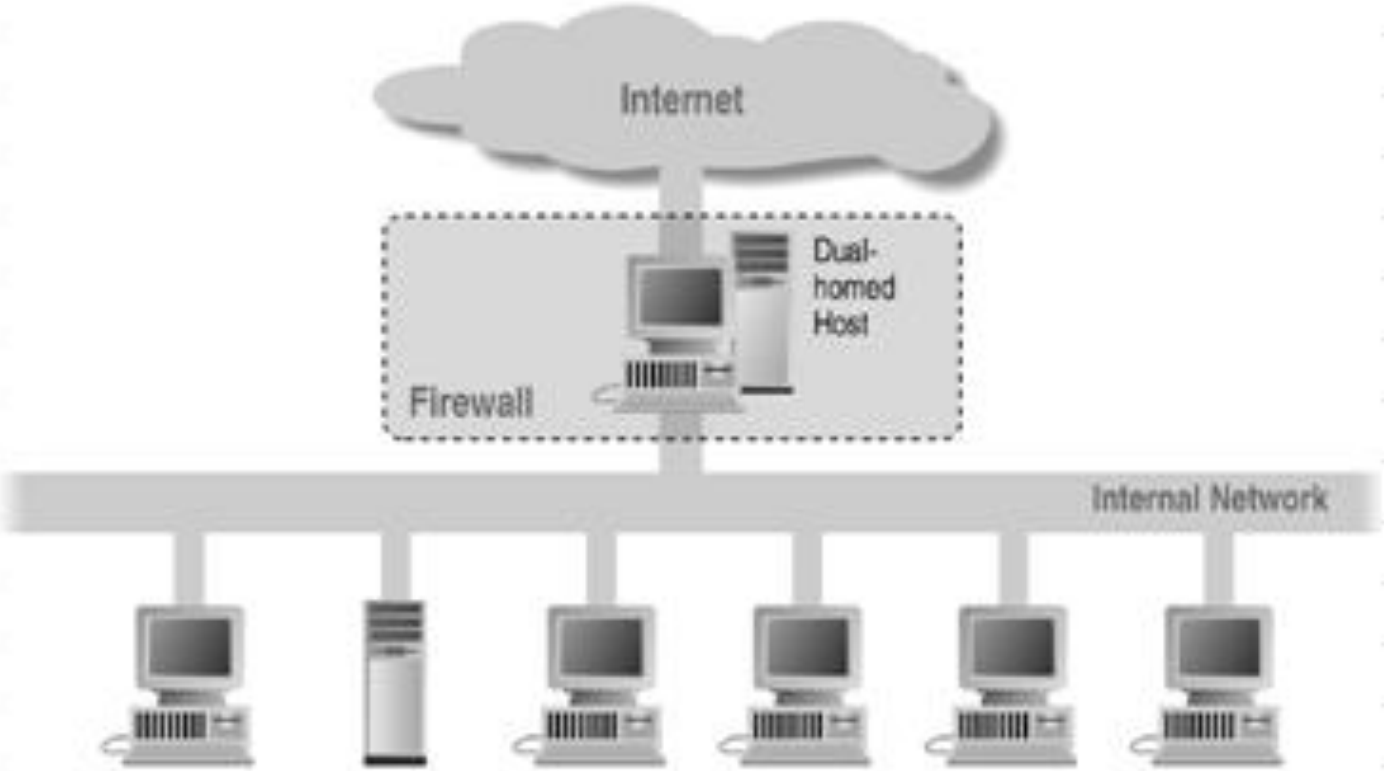
Host Arsitektur (Internet – Firewall – Host) dalam lingkup Network and Internet Defense

SCREENED SUBNET USING TWO ROUTERS



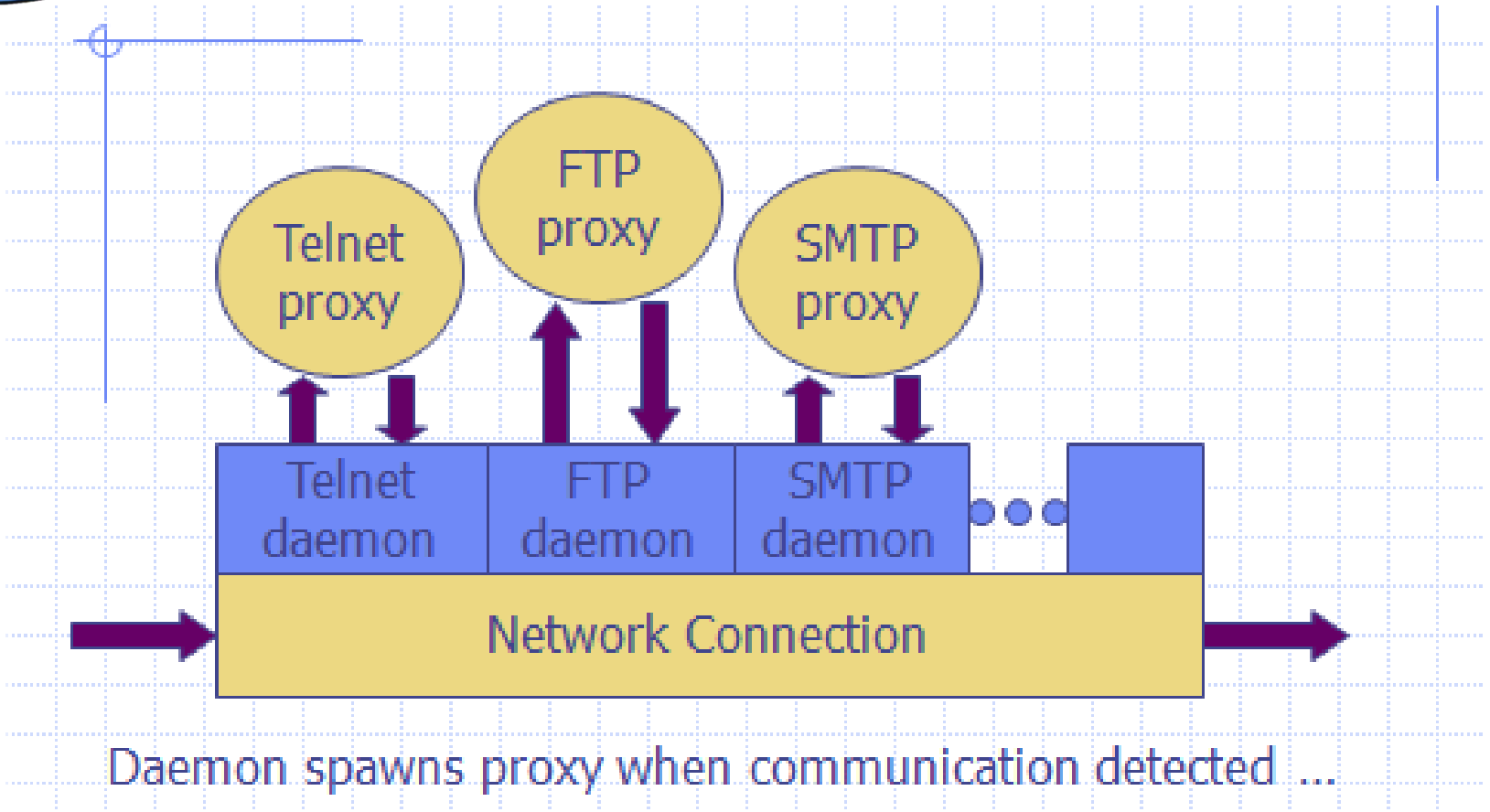
- Subnet Using Two Routers – Network And Internet Defense

DUAL HOMED HOST ARCHITECTURE



- Gambar sebuah Dual Homed Host Arsitektir – Network and Internet Defense

FIREWALL WITH APPLICATION PROXIES

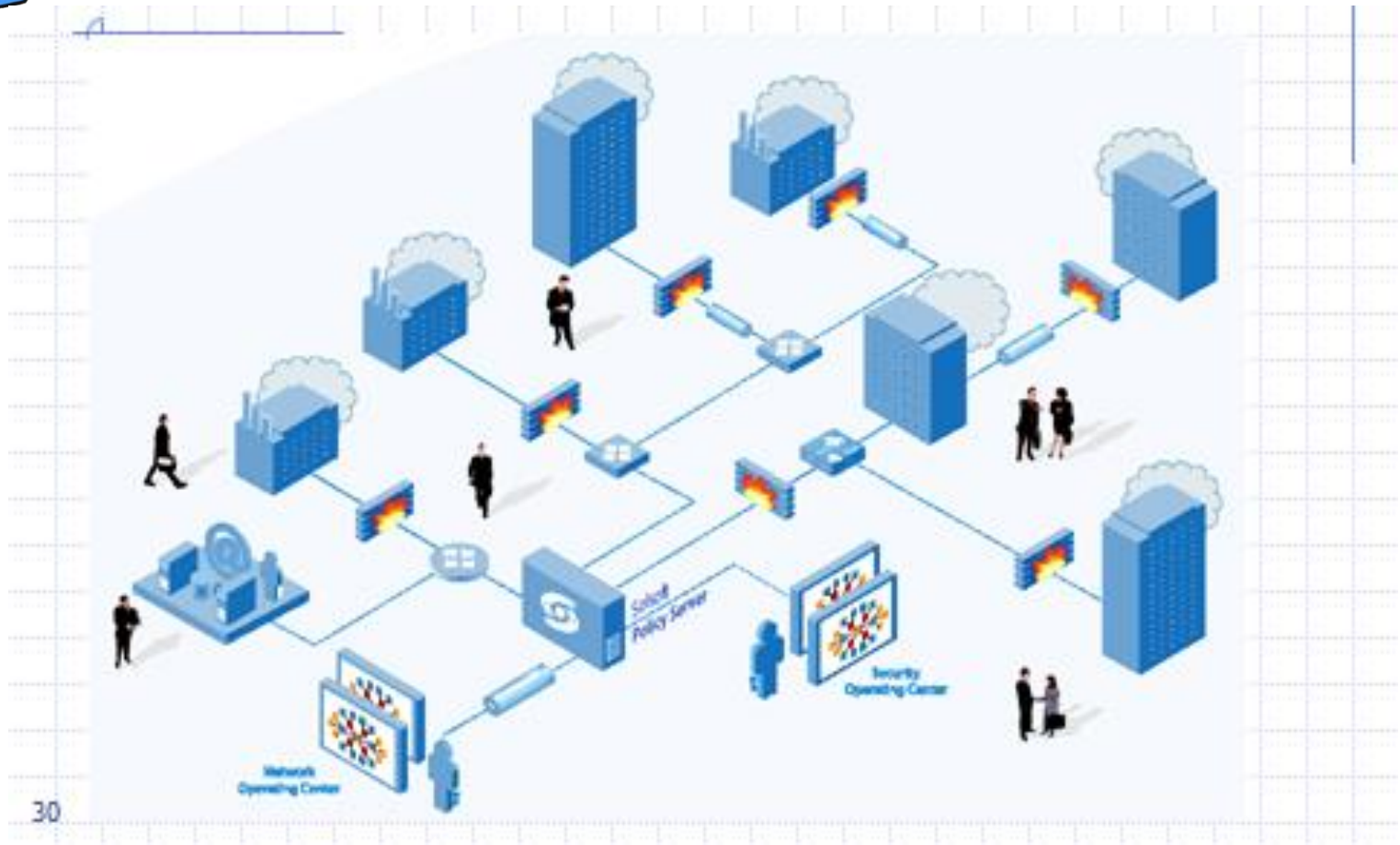


- Firewall with Apllication Proxies - Network and Internet Defense

APPLICATION LEVEL PROXIES

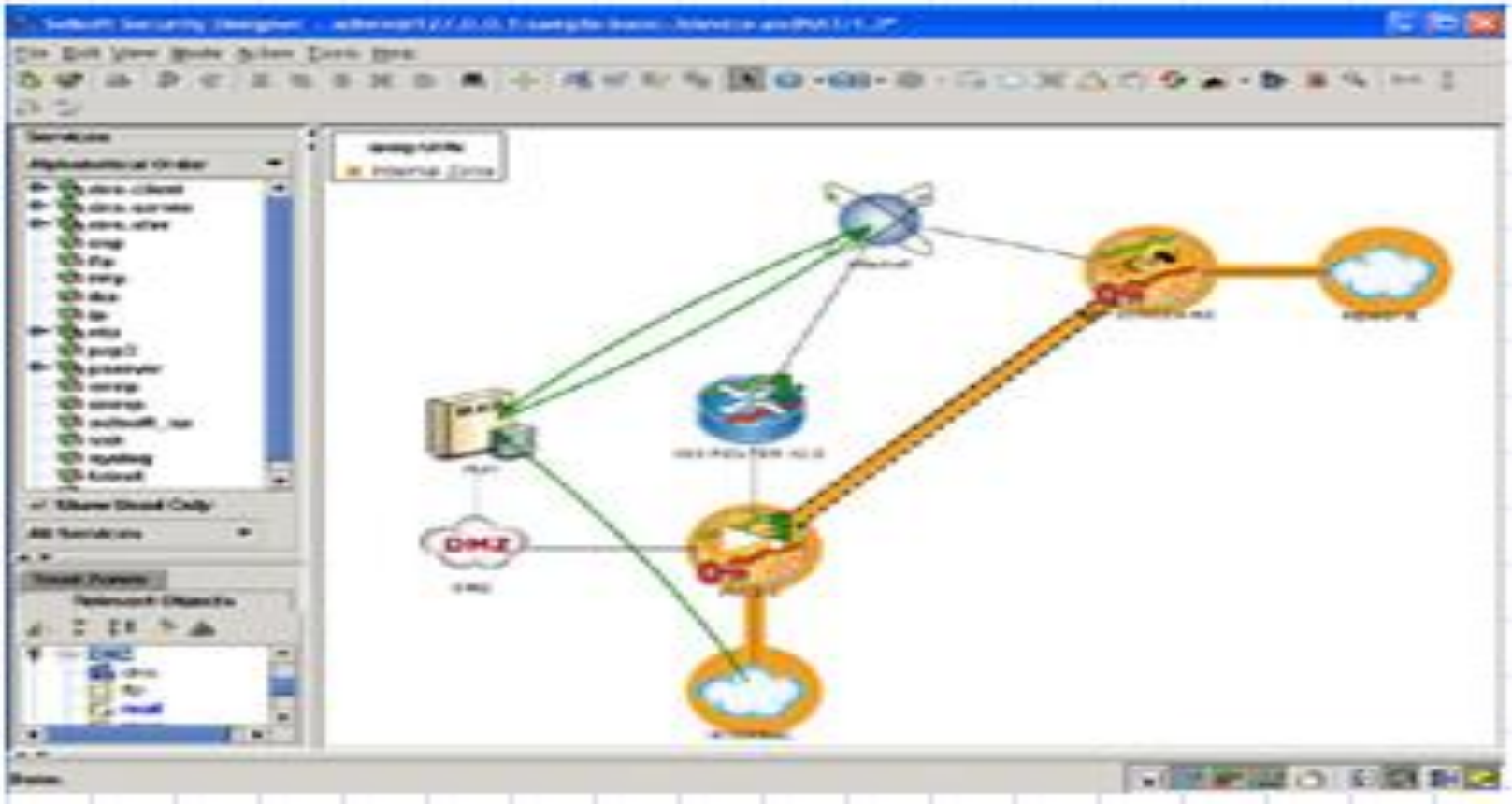
- Enforce policy for specific protocols
  - E.g., Virus scanning for SMTP
    - Need to understand MIME, encoding, Zip archives
  - Flexible approach, but may introduce network delays
- "Batch" protocols are natural to proxy
  - SMTP (E-Mail) NNTP (Net news)
  - DNS (Domain Name System) NTP (Network Time Protocol
- Must protect host running protocol stack
  - Disable all non-required services; keep it simple
  - Install/modify services you want
  - Run security audit to establish baseline
  - Be prepared for the system to be compromised

CONFIGURATION ISSUES



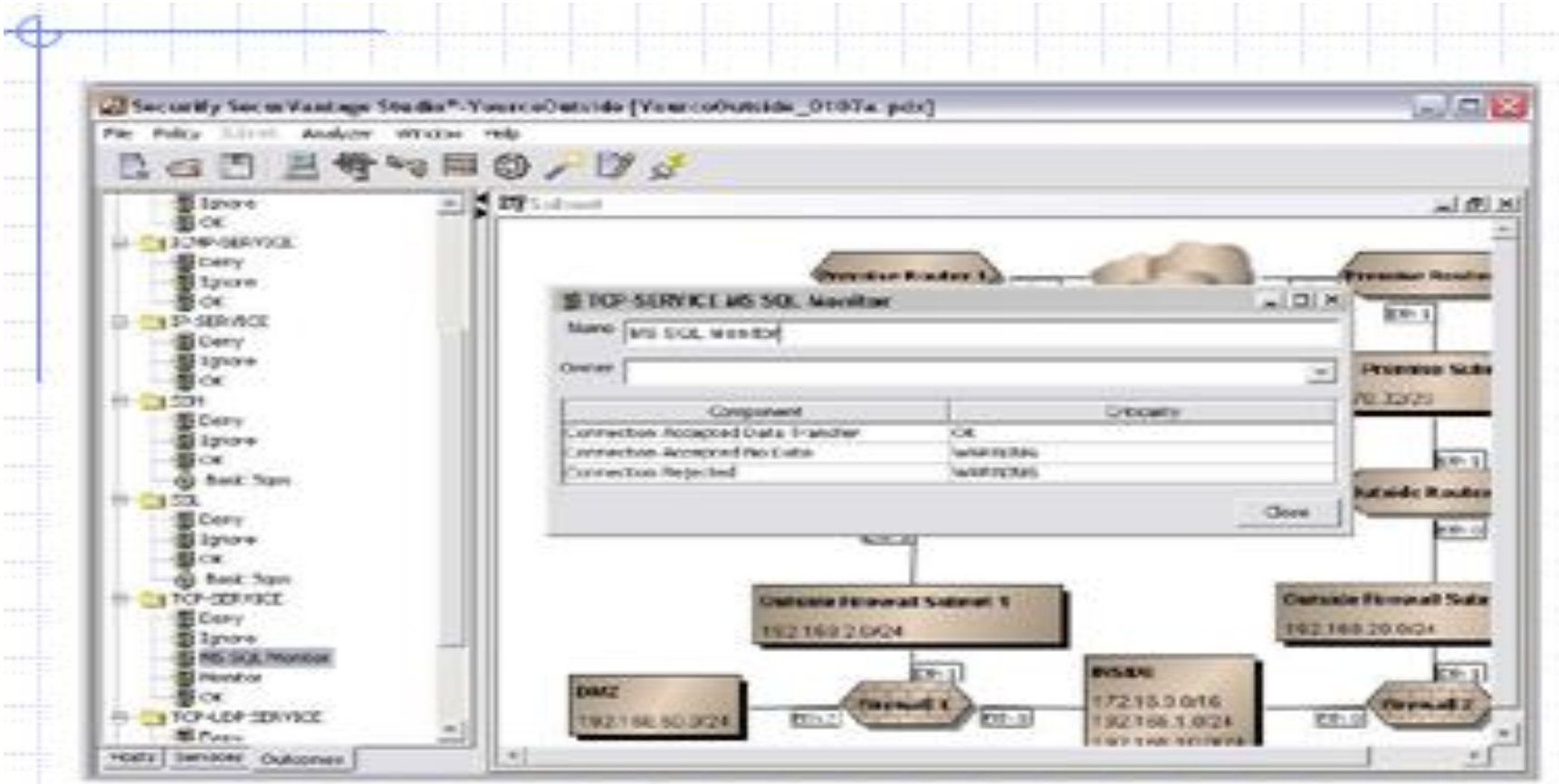
- Konfigurasi dalam lingkup Network and Internet Defense

SOLSOFT



- Desain yang dihasilkan dengan menggunakan apliasi SOLSOF

SECURITY



- Bidang Security dalam penerapan Perimeter Solusi

PROBLEMS WITH FIREWALLS

- Performance
  - Firewalls may interfere with network use
- Limitations
  - They don't solve deeper problems
    - Buggy software
    - Bad protocols
  - Generally cannot prevent Denial of Service
  - Ineffective against insider attacks
- Administration
  - Many commercial firewalls permit very complex configurations

❖ Masalah yang harus siap diantisipasi

TRAFFIC SHAPING

- Traditional firewall
  - Allow traffic or not
- Traffic shaping
  - Limit certain kinds of traffic
  - Can differentiate by host addr, protocol, etc
  - Multi-Protocol Label Switching (MPLS)
    - Label traffic flows at the edge of the network and let core routers identify the required class of service
- The real issue here on Campus:
  - P2P file sharing takes a lot of bandwidth
  - 1/3 of network bandwidth consumed by BitTorrent
    - Students: what are BitTorrent, Gnutella, Kazaa, … used for?

❖ Traffic Shaping dalam lingkup Network and Internet Defense

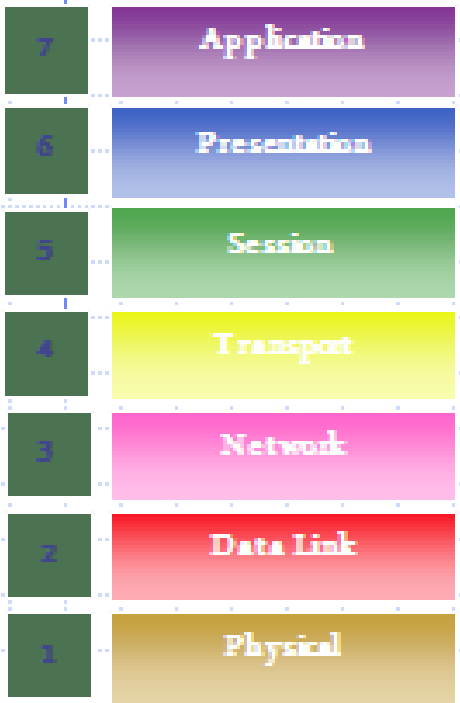
TRAFFIC SHAPING FUNCTIONS

Traffic shaping functions

- Classify and analyze traffic
  - Classify by IP address and port number
  - Use application-specific information (layer 7)
- Control traffic
  - Selectively slow certain classes of traffic
- Monitor network performance
  - Collect performance data, used to improve policies
- Network resilience
  - Active traffic management can provide resilience to DoS attacks, at least within the enterprise network

❖ Fragmentation Attack dalam lingkup Network and Internet Defense

PACKET SHAPER CLASSIFICATION



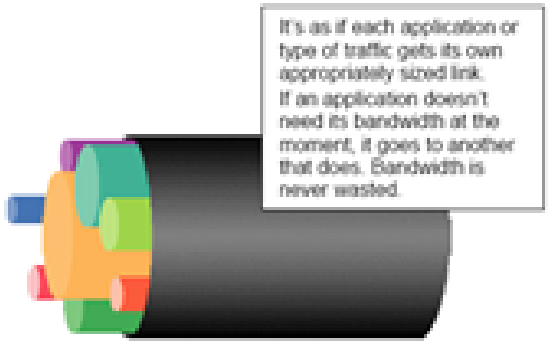
Classify 400+ Apps at OSI Layers 2-7

Peer-to-Peer Apps:
- Aimster
- AudioGalaxy
- CuteMX
- DirectConnect
- Gnutella
- Hotline
- iMesh
- KaZaA/Morpheus
- Napster
- ScourExchange
- Tripnosis....

Some Other Apps:
- H.323
- RTP-I/RTCP-I
- PASV FTP
- HTTP
- Real
- WinMedia
- Shoutcast
- MPEG
- Quicktime
- RTSP
- Chatting Apps
- Games

❖ Packet Shaper Clasification dalam lingkup Network and Internet Defense

PACKET SHAPPER CONTROL

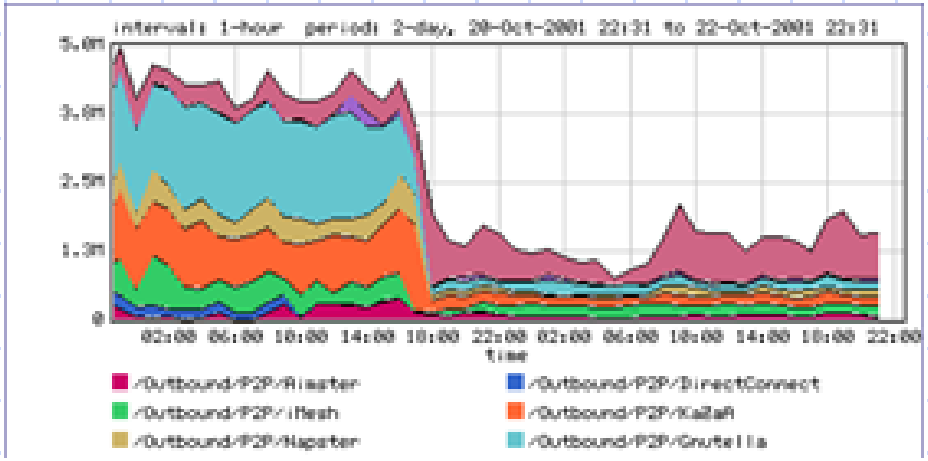


A partition:

- Creates a virtual pipe within a link for each traffic class
- Provides a min, max bandwidth
- Enables efficient bandwidth use

Rate shaped P2P capped at 300kbps

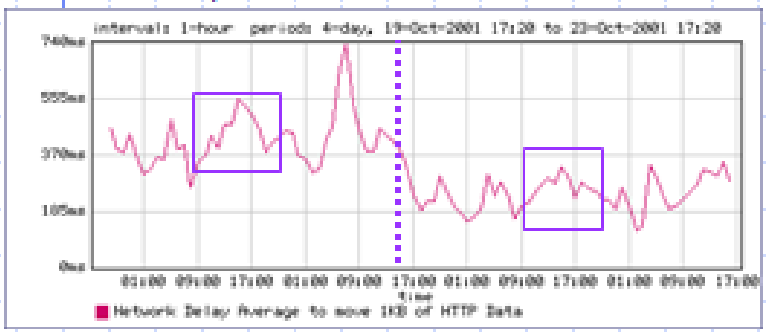
Rate shaped HTTP/SSL to give better performance



❖ Contoh Packet Shapper Control dalam lingkup Network and Internet Defense

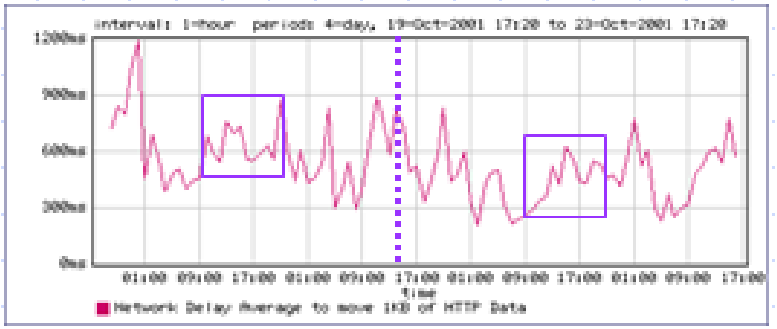
PACKET SHAPER REPORT : HTTP

Outside Web Server Normalized
Network Response Times



No Shaping Shaping

Inside Web Server Normalized
Network Response Times



No Shaping Shaping

- Contoh Packet Shapper Report dalam lingkup Network and Internet Defense

HOST AND IDS

- Intrusion prevention
  - Network firewall
    - Restrict flow of packets
  - System security
    - Find buffer overflow vulnerabilities and remove them!
- Intrusion detection
  - Discover system modifications
    - Tripwire
  - Look for attack in progress
    - Network traffic patterns
    - System calls, other system events

❖ Info tentang Host dan IDS dalam lingkup Network and Internet Defense

TRIPWIRE

- Outline of standard attack
  - Gain user access to system
  - Gain root access
  - Replace system binaries to set up backdoor
  - Use backdoor for future activities
- Tripwire detection point: system binaries
  - Compute hash of key system binaries
  - Compare current hash to hash stored earlier
  - Report problem if hash is different
  - Store reference hash codes on read-only medium

❖ Informasi dan Penggunaan Tripware dalam lingkup Network and Internet Defense

IS TRIPWIRE TOO LATE

- Typical attack on server
  - Gain access
  - Install backdoor
    - This can be in memory, not on disk!!
  - Use it
- Tripwire
  - Is a good idea
  - Wont catch attacks that don't change system files
  - Detects a compromise that *has happened*

Remember: Defense in depth

❖ Type Attack on server Network and Internet Defense

DETECT MODIFIED BINARY IN MEMORY

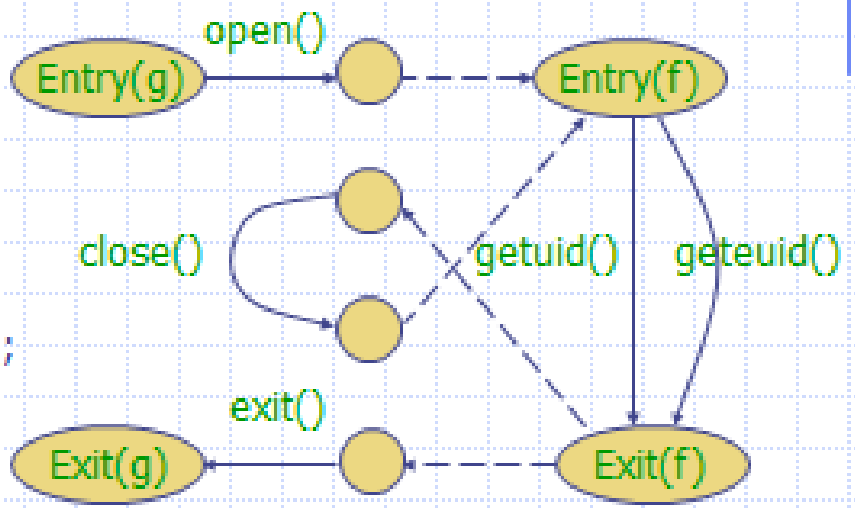
- Can use system-call monitoring techniques
- For example [Wagner, Dean IEEE S&P '01]
  - Build automaton of expected system calls
    - Can be done automatically from source code
  - Monitor system calls from each program
  - Catch violation

Results so far: lots better than not using source code!

❖ Pendetksian dan Momidif Binary In Memorial dalam lingkup Network and Internet Defense

EXAMPLE CODE AND AUTOMATION

```
f(int x) {
    x ? getuid() : geteuid();
    x++
}
g() {
    fd = open("foo", O_RDONLY);
    f(0); close(fd); f(1);
    exit(0);
}
```



If code behavior is inconsistent with automaton, something is wrong

- Penggunan “ Example Code dan Autimation dalam lingkup Network and Internet Defense

GENERAL IDS

- Many intrusion detection systems
  - Close to 100 systems with current web pages
  - Network-based, host-based, or combination
- Two basic models
  - Misuse detection model
    - Maintain data on known attacks
    - Look for activity with corresponding signatures
  - Anomaly detection model
    - Try to figure out what is "normal"
    - Report anomalous behavior
- Fundamental problem: too many false alarms

❖ Pengetahuan General tentang IDS : Intrusion Detection System

ROOTKIT

- Rootkit sniffs network for passwords
  - Collection of programs that allow attacker to install and operate a packet sniffer (on Unix machines)
  - Emerged in 1994, has evolved since then
  - 1994 estimate: 100,000 systems compromised
- Rootkit attack
  - Use stolen password or dictionary attack to get user access
  - Get root access using vulnerabilities in rdist, sendmail, /bin/mail, loadmodule, rpc.ypupdated, lpr, or passwd
  - Ftp Rootkit to the host, unpack, compile, and install it
  - Collect more username/password pairs and move on

❖ Contoh Rootkit, dalam lingkup Network and Internet Defense

ROOTKIT COVERS ITS TRACKS

- Modifies netstat, ps, ls, du, ifconfig, login
  - Modified binaries hide new files used by rootkit
  - Modified login allows attacker to return for passwords
- Rootkit fools simple Tripwire checksum
  - Modified binaries have same checksum
  - But a better hash would be able to detect rootkit

❖ Contoh Rootkit cover Its Tracks

DETECTING ROOTKIT ON SYSTEM

- Sad way to find out
  - Disk is full of sniffer logs
- Manual confirmation
  - Reinstall clean ps and see what processes are running
- Automatic detection
  - Rootkit does not alter the data structures normally used by netstat, ps, ls, du, ifconfig
  - Host-based intrusion detection can find rootkit files
    - As long as an update version of Rootkit does not disable your intrusion detection system ...

❖ Deteksi rootkit on system dalam Network and Internet

DETECTING NETWORK

- Symantec honeypot running Red Hat Linux 9
- Attack
  - Samba 'call_trans2open' Remote Buffer Overflow (BID 7294)
  - Attacker installed a copy of the SHV4 Rootkit
- Snort NIDS generated alerts, from this signature

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 \
(msg:"NETBIOS SMB trans2open buffer overflow attempt"; \
flow:to_server,established; \
content:"|00|"; offset:0; depth:1; \
content:"|ff|SMB|32|"; offset:4; depth:5;
content:"|00 14|"; offset:60; depth:2; \
...
```

- Pendetksian jaringan dalam lingkup Network and Internet Defense

ANOMALY DETECTION

- Basic idea
  - Monitor network traffic, system calls
  - Compute statistical properties
  - Report errors if statistics outside established range
- Example – IDES (Denning, SRI)
  - For each user, store daily count of certain activities
    - E.g., Fraction of hours spent reading email
  - Maintain list of counts for several days
  - Report anomaly if count is outside weighted norm

Big problem: most unpredictable user is the most important

❖ Contoh Anomaty Detection dalam lingkup Network and Internet Defense

ANOMALY – SYS CALL SEQUENCES

- Build traces during normal run of program
  - Example program behavior (sys calls)

    open read write open mmap write fchmod close
  - Sample traces stored in file (4-call sequences)

    open read write open

    read write open mmap

    write open mmap write

    open mmap write fchmod

    mmap write fchmod close
  - Report anomaly if following sequence observed

    open read read open mmap write fchmod close

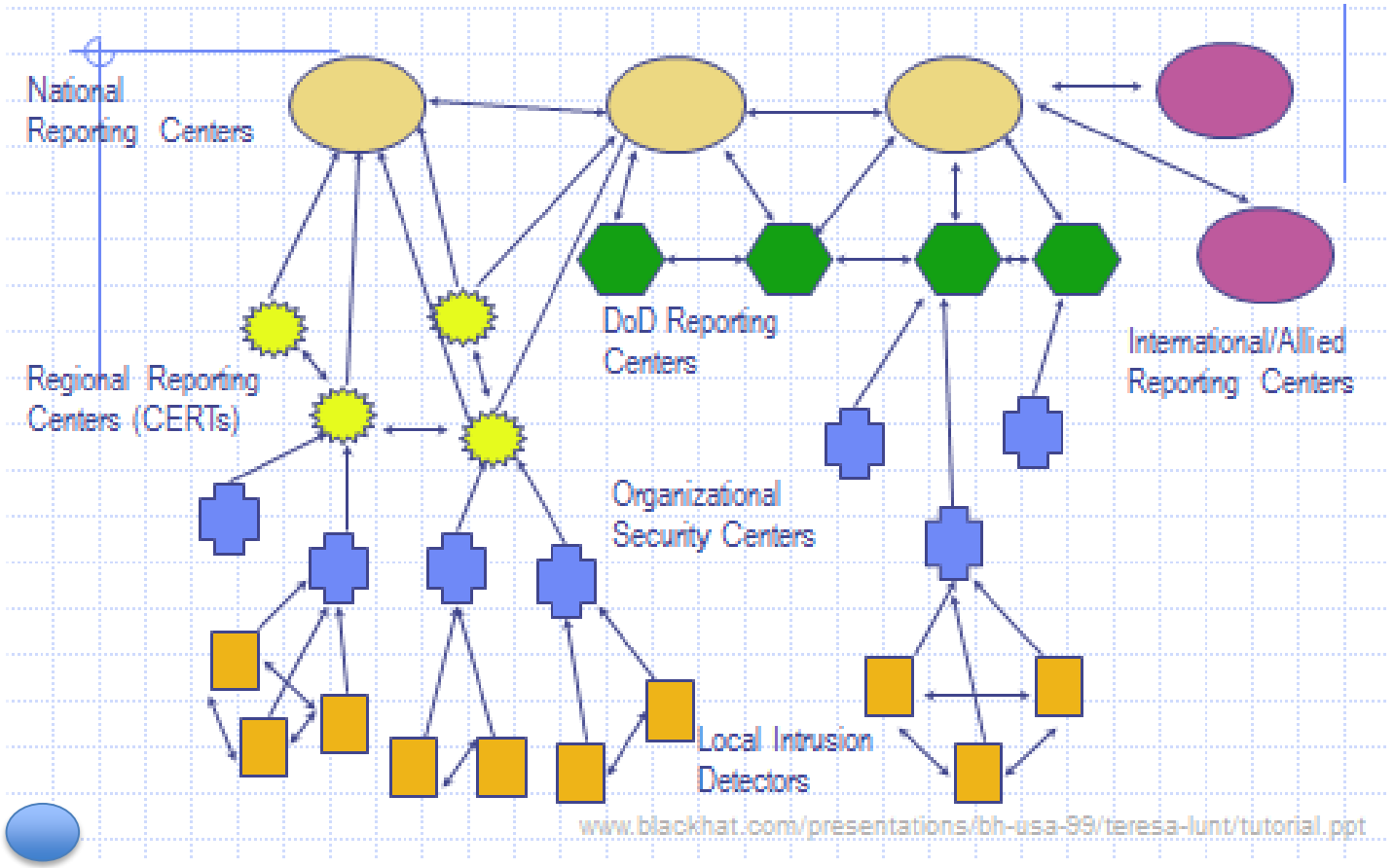
❖ Anomaly – Sys Call Sequensces dalam Network and Intenet

DIFICULTIES IN INTRUSION DETECTION

- Lack of training data
  - Lots of "normal" network, system call data
  - Little data containing realistic attacks, anomalies
- Data drift
  - Statistical methods detect changes in behavior
  - Attacker can attack gradually and incrementally
- Main characteristics not well understood
  - By many measures, attack may be within bounds of "normal" range of activities
- False identifications are very costly
  - Sys Admin spend many hours examining evidence

❖ Dificutlties in Intrusion Detection am lingkup Network and Internet Defense

STRATEGIC INTRUSION ASSESMENT

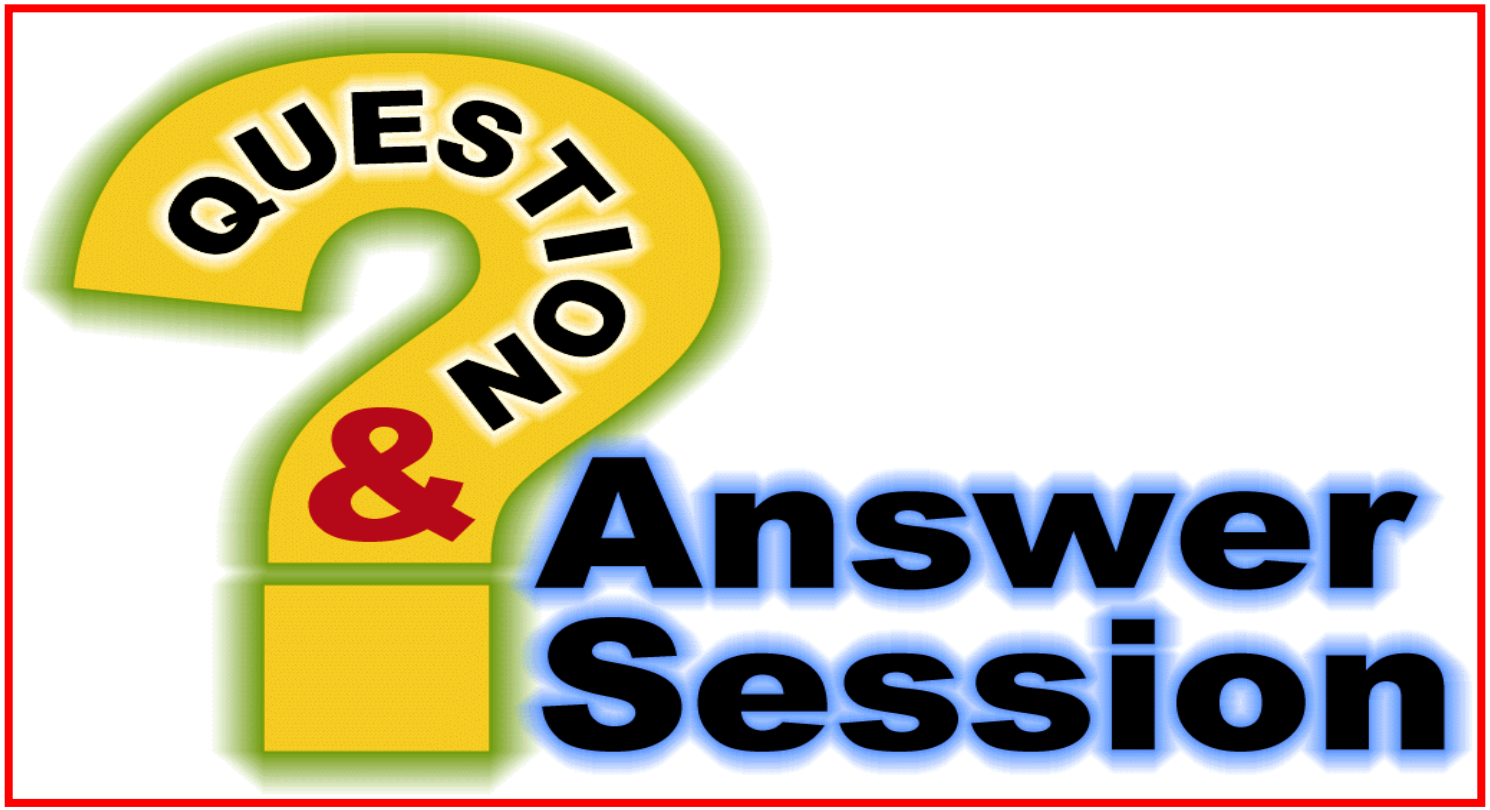


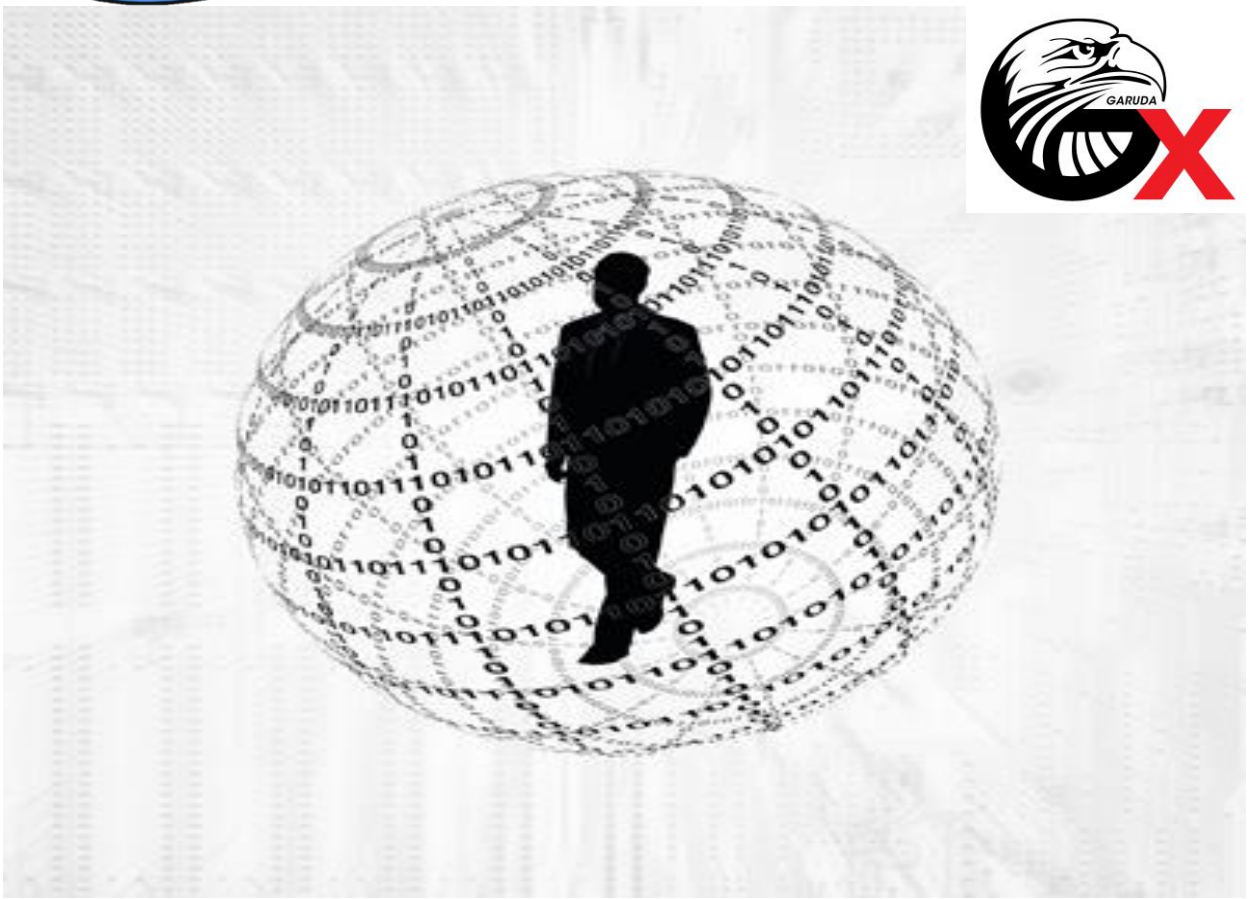
- Strategic Intrusions Assessment dalam lingkup Network and Internet Defense

STRATEGIC INTRUSION ASSESMENT

- Test over two-week period
  - AFIWC's intrusion detectors at 100 AFBs alarmed on 2 million sessions
  - Manual review identified 12,000 suspicious events
  - Further manual review => four actual incidents
- Conclusion
  - Most alarms are false positives
  - Most true positives are trivial incidents
  - Of the significant incidents, most are isolated attacks to be dealt with locally

❖ Strategic Intrusions Assessment dalam lingkup Network and Internet Defense


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