FIREWALL & IDS

Tools untuk pengamanan

Definisi Firewall [1]

- *A firewall is a system or group of systems that enforces an access control policy between two networks*
  http://www.clark.net/pub/mjr/pubs/fwfaq/
- *The main purpose of a firewall system is to control access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated*
  http://csrc.ncsl.nist.gov/nistpubs/800-10/node31.html

Definisi Firewall [2]

- sistem yang mengatur layanan jaringan
  - dari mana
  - ke mana
  - melakukan apa
  - siapa
  - kapan
  - seberapa besar/banyak
- dan membuat catatan layanan

Mengapa perlu Firewall?

- Melindungi servis yang rentan
- Akses terkendali ke sistem di suatu situs lokal
- Security terkonsentrasi
- Peningkatan privasi
- Statistik dan logging penggunaan dan penyalahgunaan jaringan
- Policy enforcement

Servis yang Rentan

- Kebutuhan internal: file server via SMB di Windows NT dan Windows 95/98
- Rentan berbagai DoS
- Solusi: akses terbatas SMB di lingkup lokal

Akses Terkendali ke Situs Lokal

- Hanya host tertentu yang dapat dicapai
- Hanya layanan tertentu yang dapat dimintai layanannya

Security Terkonsentrasi

- Lebih mudah & murah mengamankan satu host daripada banyak host
- Host lain yang tidak secure disembunyikan/ dilindungi
- Tidak semua OS bisa/mudah/murah diamankan tanpa bantuan sistem lain

Peningkatan Privasi

- finger
- snoop/sniff
- dns zone transfer
- lokalisasi *unlogged public access data*

Logging dan Statistik

- pemanfaatan saluran dan trend
  - layanan
  - dari mana
  - ke mana
  - berapa besar/lama
- alarm
- status keamanan dan kecenderungan serangan

Policy Enforcement

- tidak mengandalkan sepenuhnya kerjasama user lokal dan remote

Bagaimana caranya?

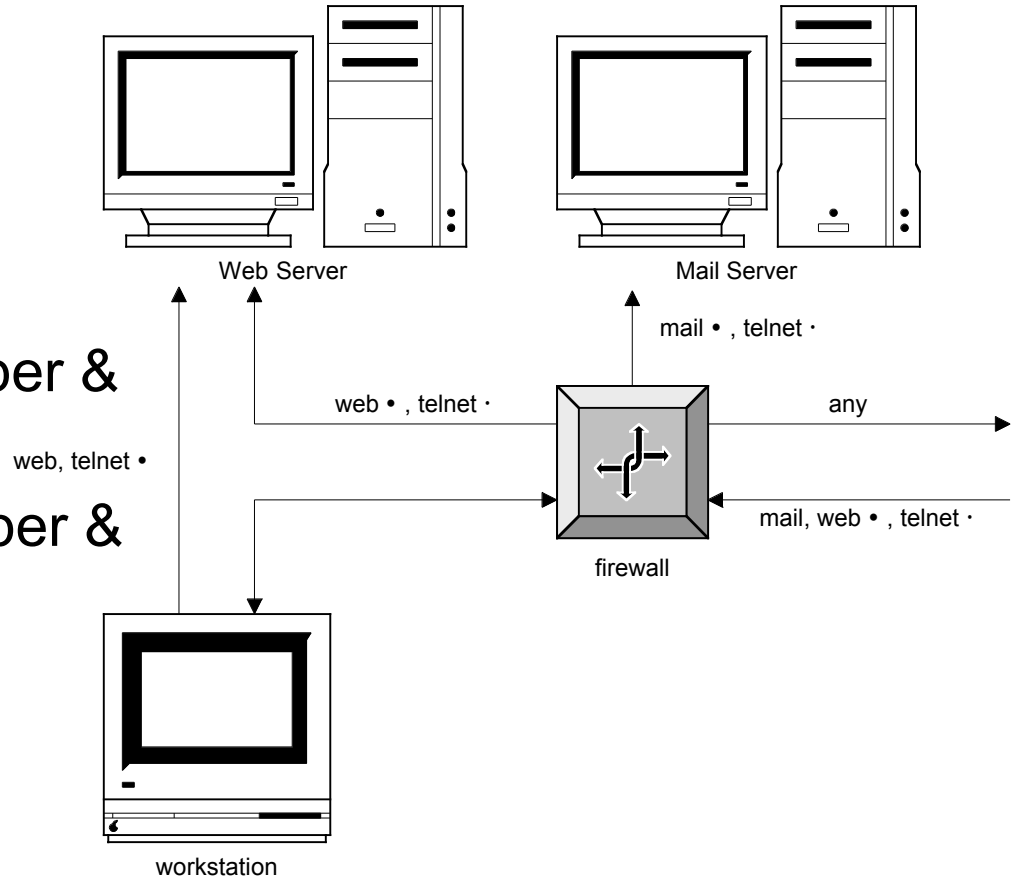
- Packet filter
- Application layer gateway
- Stateful inspection

Packet Filter

- Independen aplikasi
- kinerja tinggi
- skalabilitas
- security rendah
- tidak kenal konteks

Packet Filter

- Pemilahan berdasarkan
  - IP address sumber & tujuan
  - nomor port sumber & tujuan



Packet Filter

- Protokol ‘berbahaya’
  - tftp(69), Xwindows(2000, 6000+), rpc(111), rsh(514), rlogin(513), rexec(512), netbios(137 - 139), ...
- Protokol ‘exploitable’
  - telnet(23), ftp(20, 21), smtp(25), dns(53), uucp(540), pop3(110), finger(79), ...

Contoh Rule Packet Filter

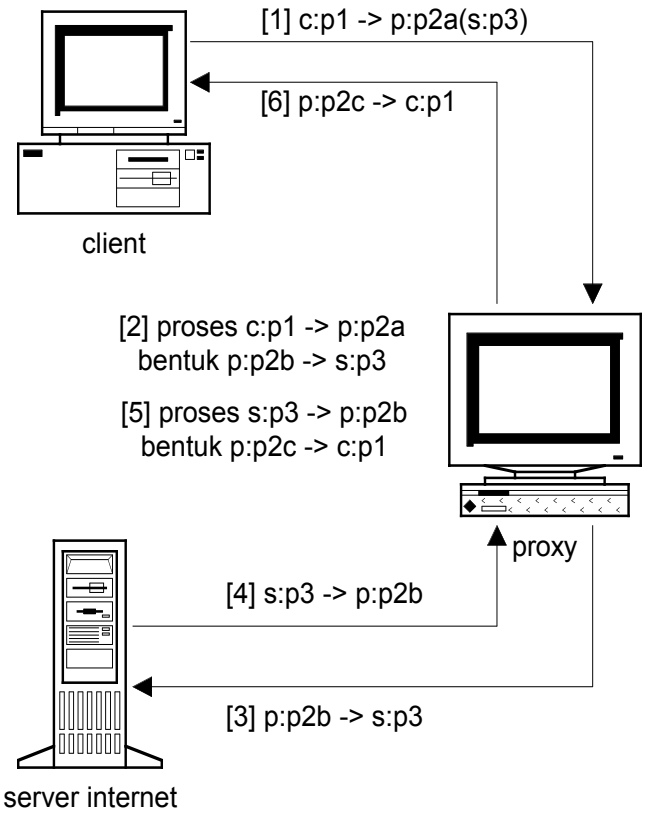
from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

Application Layer Gateway/Proxy

- security tinggi
- sangat paham konteks
- potensi meningkatkan kinerja (dengan cache)
- potensi mengurangi kinerja (tanpa cache)
- proxy spesifik per aplikasi
- skalabilitas rendah, memecah model client-server

Proxy

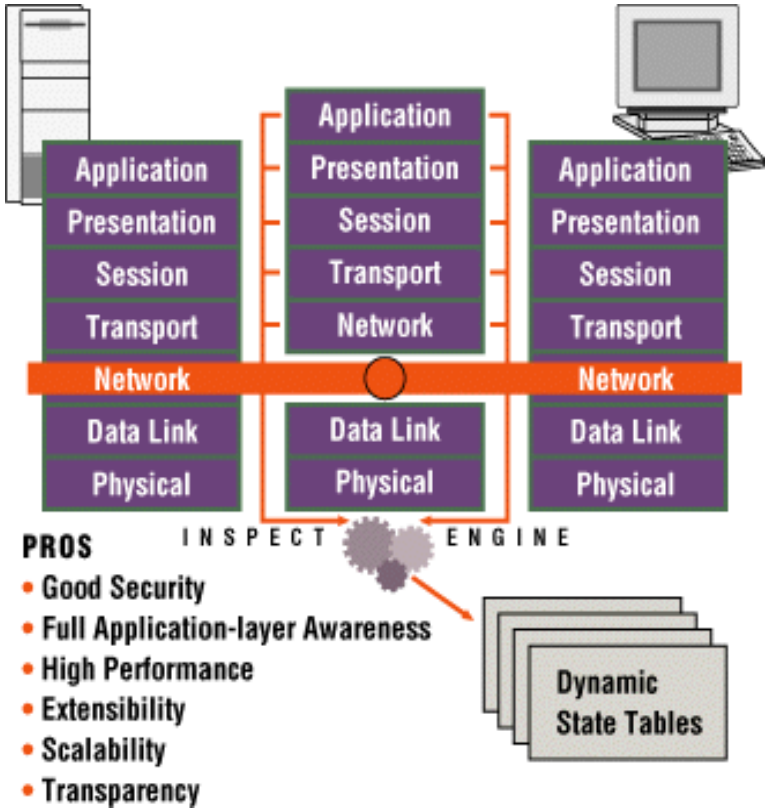
- bisa tanpa routing
- host lokal hanya boleh/perlu menghubungi proxy
- proxy meneruskan request ke tujuan sebenarnya
- kombinasi dengan packet filtering



Stateful Inspection

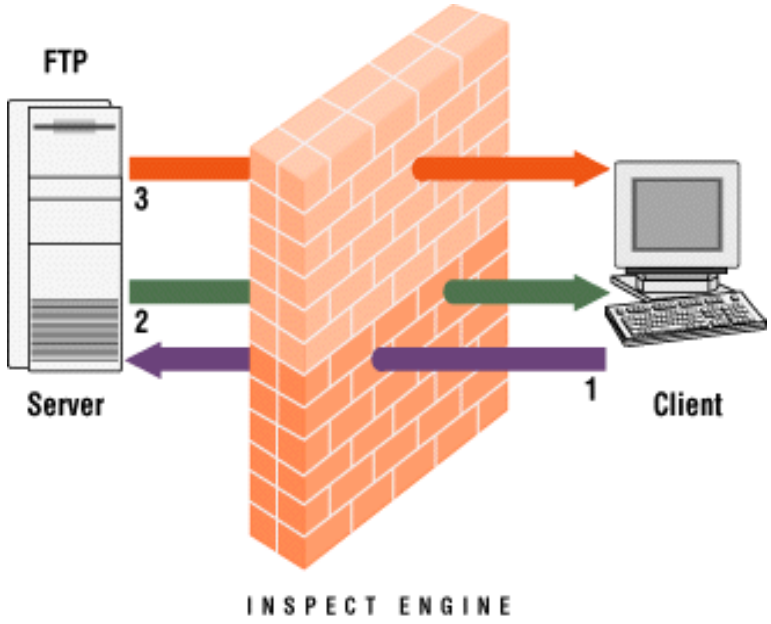
- security bagus
- pemahaman konteks lengkap
- kinerja tinggi
- algoritma inspeksi state!
  - spesifik vendor
  - harus di-update untuk protokol baru

Stateful Inspection



- intersepsi packet di layer network
- inspeksi state
  - ekstraksi informasi state
  - tabel dinamik state
- filtering di layer network
  - packet rule
  - state rule

Stateful Inspection



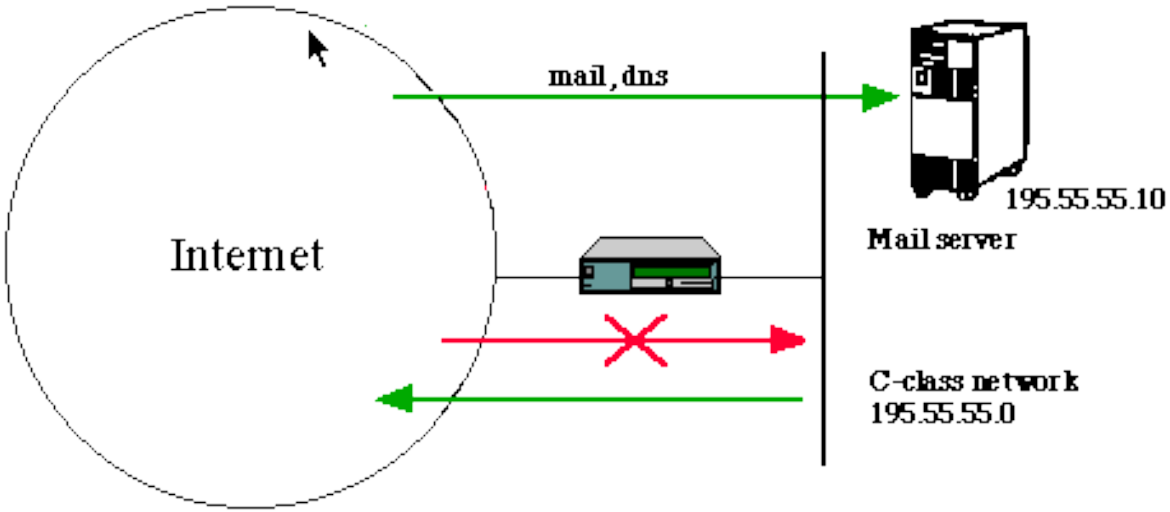
- client membuka sesi, meminta penyambungan ke port x
- *ip address sumber dan tujuan, beserta nomor port yang diminta dicatat*
- server memberi konfirmasi ke client bahwa port x akan dipakai
- *konfirmasi dicatat*
- server membuka saluran balik ke client, di port x

Kombinasi

- packet filtering firewall
- dual-homed gateway firewall
- screened host firewall
- screened subnet firewall

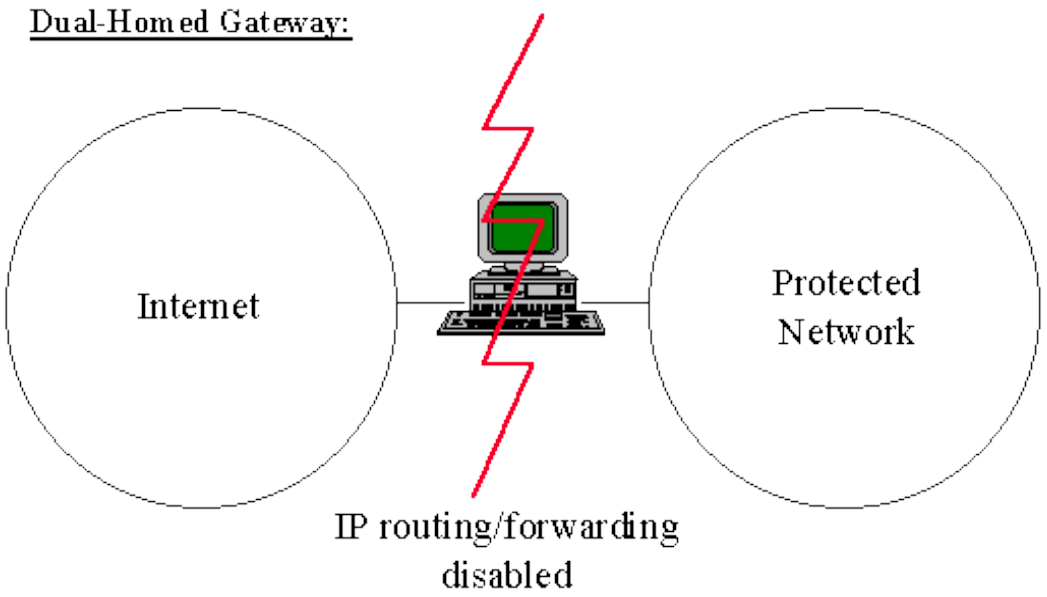
Packet Filtering

- full routing, tetapi
- packet filter diaktifkan



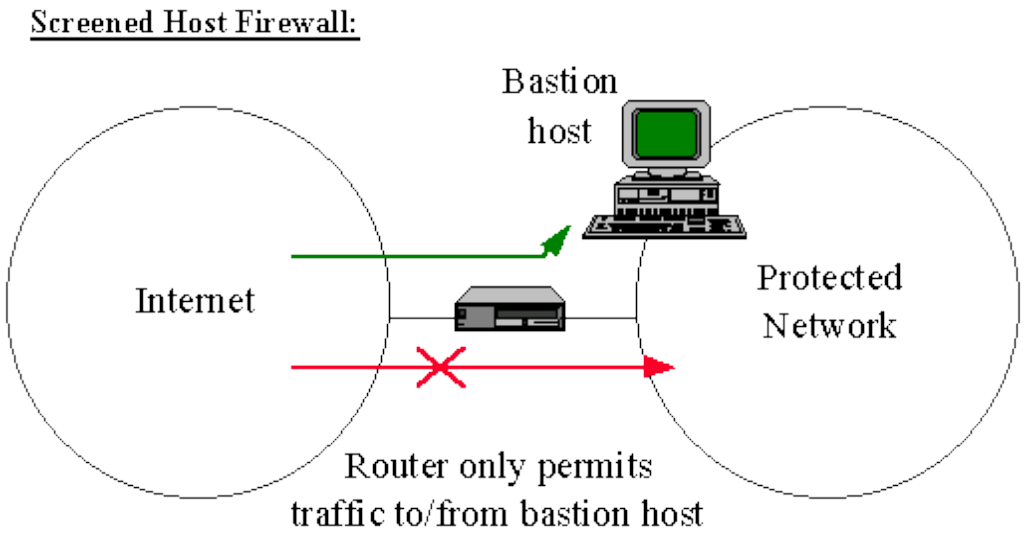
Dual Homed Gateway

- no routing
- proxy



Screened Host

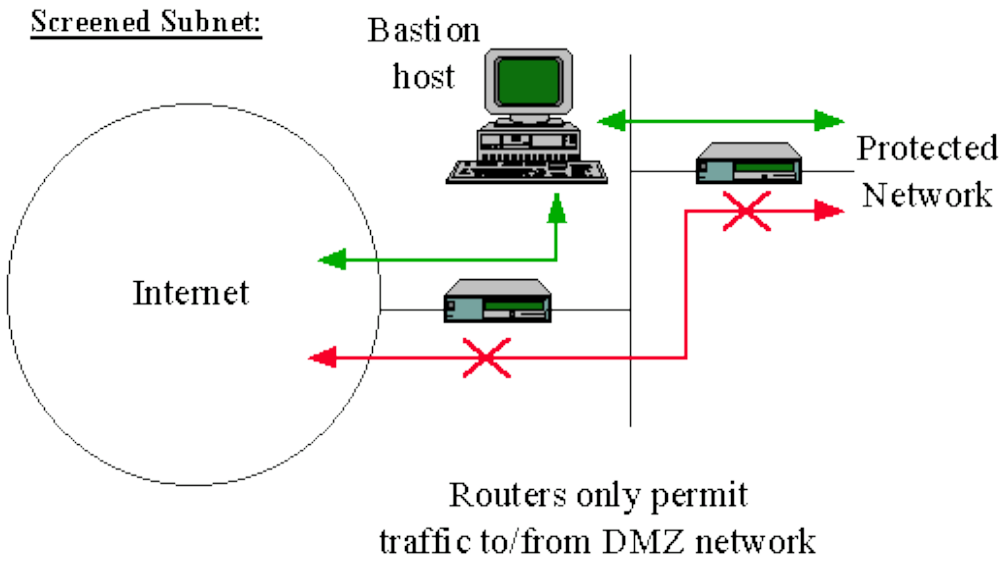
- packet filtering router
- single bastion host



Screened Subnet

- packet filtering router
- several servers

- DMZ



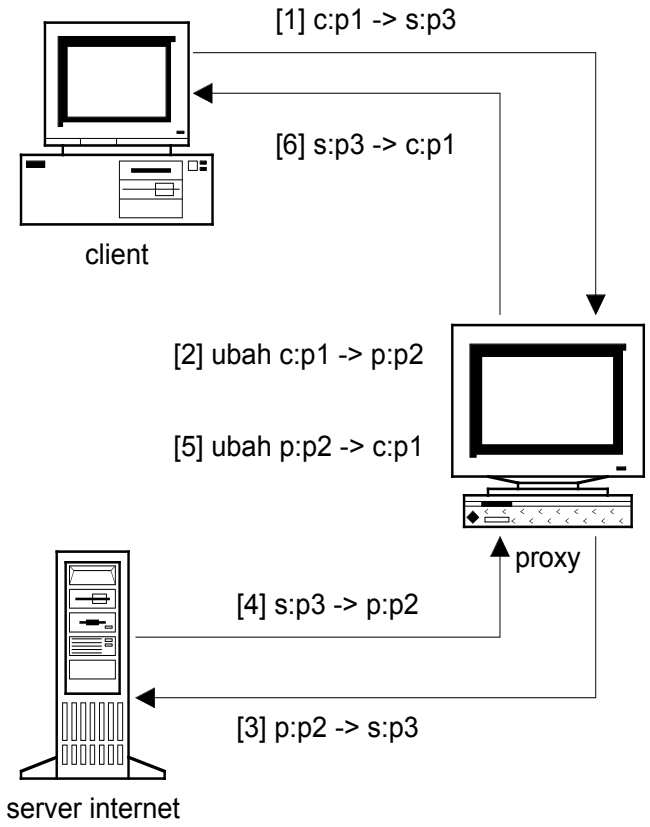
Masalah Pada Firewall

- Membatasi akses layanan yang dibutuhkan
- Potensi backdoor
- Proteksi terbatas atas serangan dari dalam
- Lain-lain
  - multicast
  - virus
  - throughput

Teknologi Yang Relevan

- NAT (network address translation), IP masquerading
- Bandwidth limiter
- VPN (virtual private network)

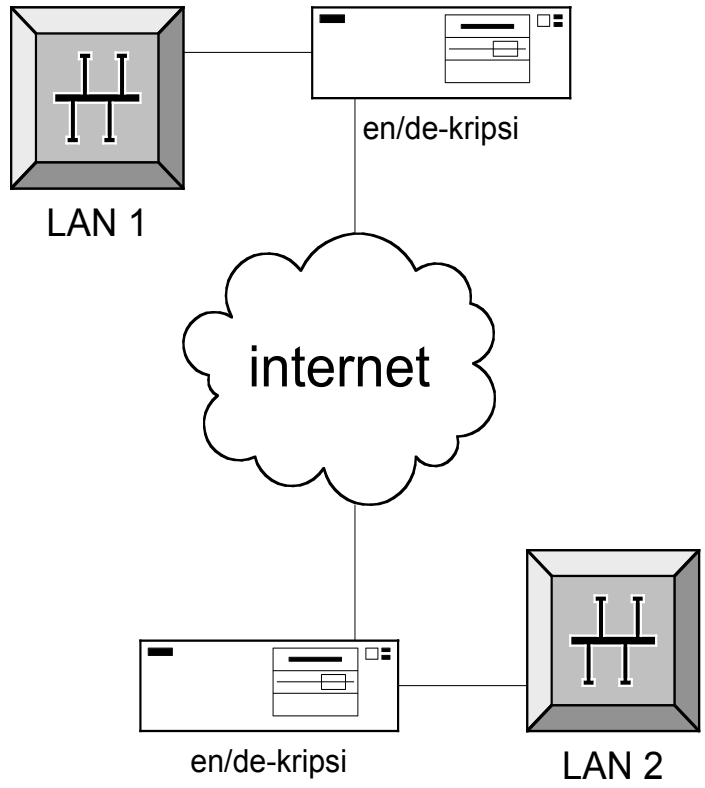
NAT



- proses transparan terhadap client
- sangat sering digunakan untuk mengatasi keterbatasan IP address global

VPN

- menyambung LAN ke LAN via media akses publik
- perlu penterjemahan pengalamatan
- sangat perlu enkripsi/dekripsi



Non-teknis

- implementasi kebijakan security dari suatu organisasi
- titik awal policy
  - yang tidak eksplisit diperbolehkan berarti dilarang, atau
  - yang tidak eksplisit dilarang berarti boleh

LINUX FIREWALL

indocisc

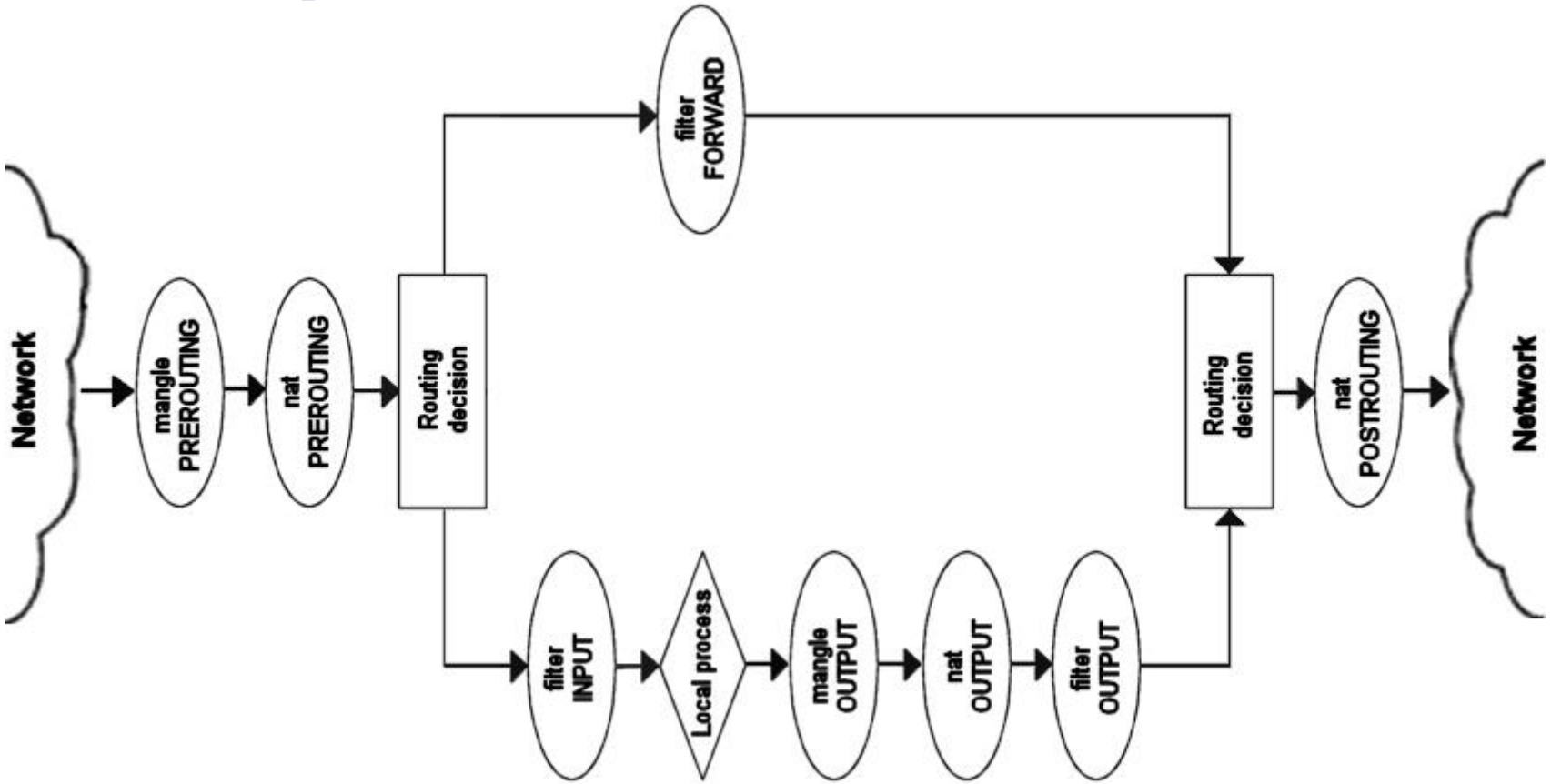
INDOCISC Linux Firewall

- Linux sudah memiliki fasilitas firewall
  - Kernel versi baru (2.4 dan 2.6): iptables
  - Kernel versi lama: ipchains
  - Kemampuan bergantung kepada hardware yang digunakan

Konsep Chain

- INPUT
  - Semua paket yang masuk ke komputer melalui chain ini
- OUTPUT
  - Semua paket yang keluar dari komputer
- FORWARD
  - Paket yang diterima dari satu network dan diteruskan ke network lainnya

Konsep Chain



Tutorial 0: Reset firewall

- `unix#` **`iptables -F INPUT`**
- `unix#` **`iptables -F OUTPUT`**
- `unix#` **`iptables -F FORWARD`**

Periksa status

- `unix#` **`iptables -nvL`**

Tutorial 1: Batasi Akses

- Membatasi akses dari sebuah nomor IP, misal dari 192.168.1.53

```
iptables -s 192.168.1.53
```

- "-s" menunjukkan source host
- Apa yang akan dilakukan terhadap paket tersebut?
  - ACCEPT, DENY, DROP

```
iptables -s 192.168.1.53 -j DROP
```

Batasi Akses (lanjutan)

- Terhadap chain mana rule berlaku? INPUT
  - Tambahkan (append) pada chain INPUT dengan "-A"
  - Perintah menjadi

```
iptables -A INPUT -s 192.168.1.53 -j DROP
```

Contoh perintah lainnya

- Untuk membatasi satu segmen
  - 192.168.1.0/24
- Untuk membatasi port tertentu
  - Protokol (-p): TCP, UDP, ICMP?
  - Servis / nomor port: misal 21 (FTP), dengan "--destination-port"

```
iptables -A INPUT -s 192.168.1.0/24
  -p tcp --destination-port 21 -j DROP
```

Tutorial 1b: Batasi Semua Akses

- Membatasi semua kecuali yang diperbolehkan
  (Jangan dilakukan dari remote!)

  ```
  unix# iptables -P INPUT DROP
  ```

- Periksa fungsi
  - *ping* firewall sebelum perintah dieksekusi
  - *ping* firewal kembali setelah perintah dilakukan
  - apa yang terjadi?

Tutorial 2: Membuka Akses

- Membuka akses DNS, yaitu UDP port 53

```
# iptables -A INPUT -p UDP -s 0/0 --dport 53 -j ACCEPT
# dig course.indocisc.com @$SERVER
```

- Membuka akses ke web server: TCP port 80

```
# iptables -A INPUT -P TCP -s 0/0 -dport 80 -j ACCEPT
```

Tutorial 3: Membatasi Akses

- Membatasi akses dari sebuah alamat

```
# iptables -I INPUT -s $BAD_IP/32 -j DROP
```

- Membatasi akses dari sejumlah alamat

```
# iptables -I INPUT -s $BAD_NET/25 -j LOG
# iptables -I INPUT -s $BAD_NET/25 -j DROP
```

Contoh lebih kompleks

```
iptables -A goodtcp -p TCP --syn -j ACCEPT
iptables -A goodtcp -p TCP -m state --state \
  ESTABLISHED, RELATED, -j ACCEPTED
iptables -A goodtcp -p TCP -j DROP


iptables -A tcpsrv -p TCP -s 0/0 --dport 80 -j goodtcp
iptables -A tcpsrv -p TCP -s 0/0 --dport 21 -j goodtcp


# drop paket tcp yang NEW tapi tidak membuat SYN flag
iptables -A INPUT -p TCP ! --syn -m state --state NEW \
  -j DROP
iptables -A INPUT -p TCP -j tcpsrv
```

GUI-based interface

- Pengelolaan firewall dapat dilakukan melalui web dengan menggunakan webmin dan paket turtle

Tampilan Firewall Items

Webmin Index
Module Index

Firewall Items

Zone	Interface	Description
FIREWALL		
dmz	eth1	Ruang Server
internet	eth0	Trafic Out

create new zone

Net	Net address	Netmask	Zone	Description
dev	192.168.1.0	255.255.255.0	internet	Segment Develop
internal_net	192.168.2.0	255.255.255.0	dmz	Network Dalam

create new net

Host	IP address	MAC address	Zone	Description
cantik	192.168.1.55		internet	cantika
indocisc	192.168.1.30		internet	Virtual web
nomad	192.168.2.10		dmz	Web Server

create new host

Tampilan Firewall Rules

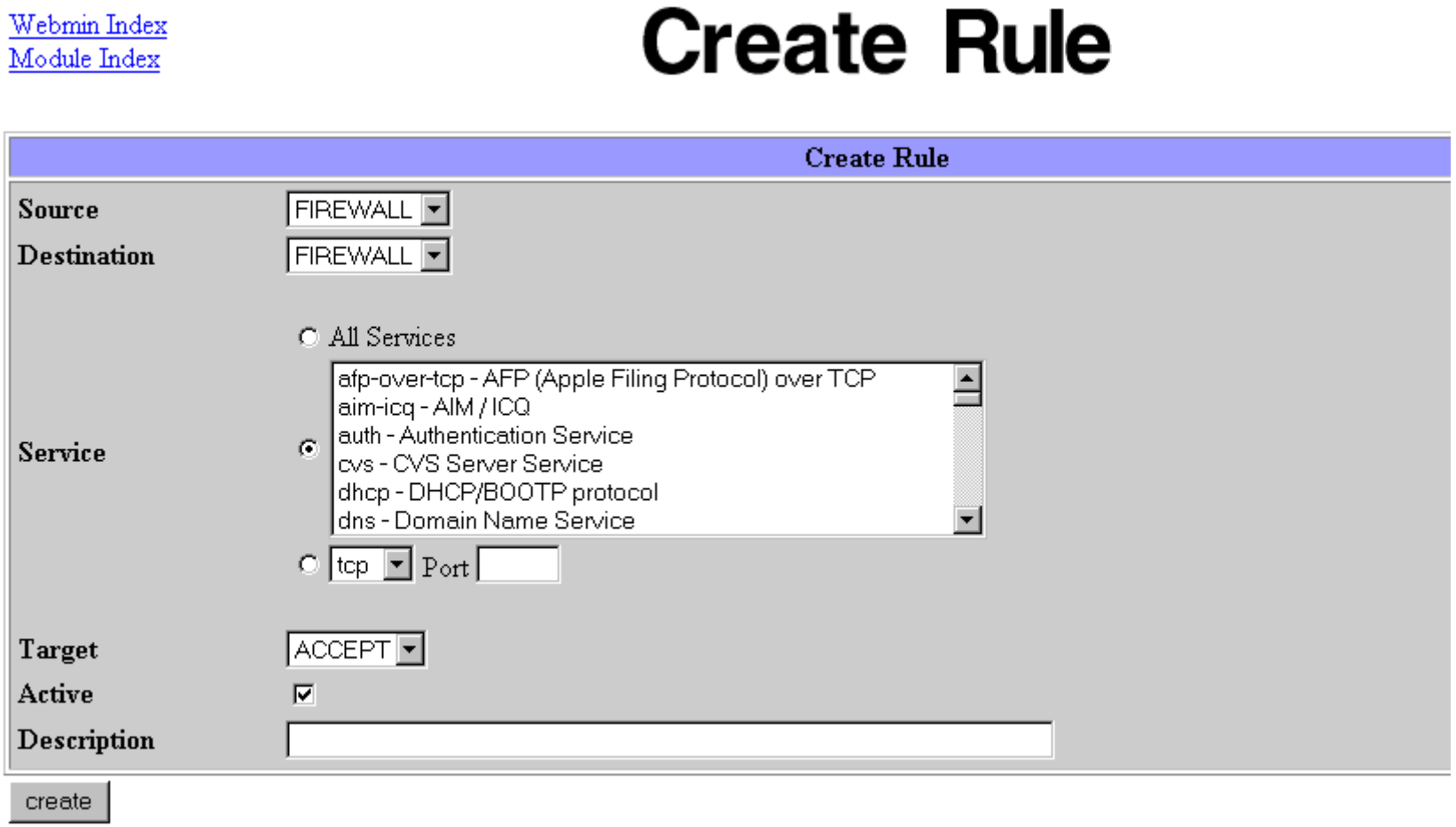
Webmin Index
Module Index

Firewall Rules

#	Source	Destination	Service	Port	Target	Active
1	dmz	internet	cvs, dns, ftp, http, https, icmp_acc, ping	_	ACCEPT	YES
2	internet	dmz	dns, http	_	ACCEPT	YES

create new rule

Membuat Rule Baru



NAT

Webmin Index
Module Index

NAT, Masquerading and Redirection

NAT

#	Virtual host / Zone (Interface IP)	Real Host	Service	Port

create new NAT

Masquerade

#	To Zone
1	internet

create new Masquerade

Redirect to local port

#	Source	Destination	Service	Port	Redirect	To Local Port

create new Redirect

Membuat NAT baru

Webmin Index
Module Index

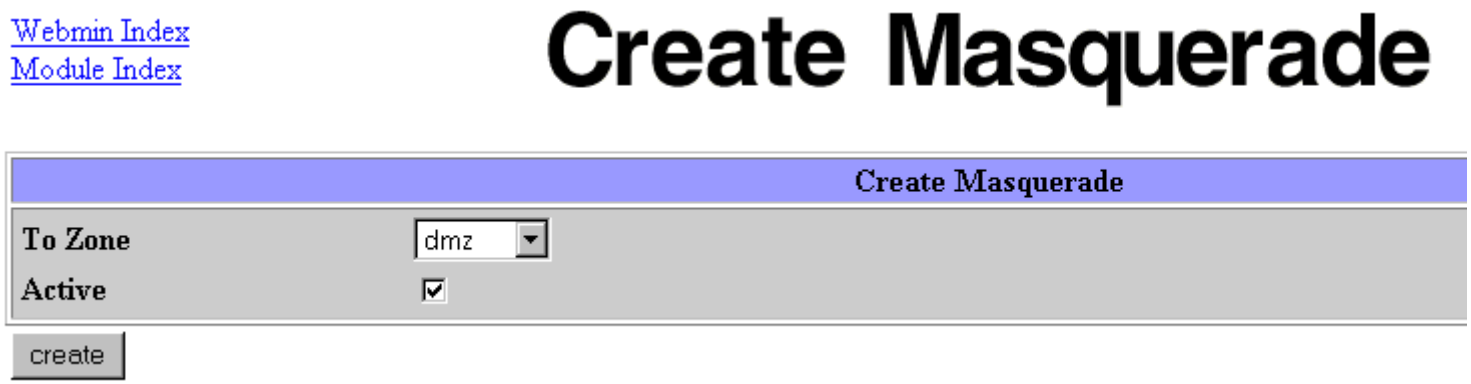
Create NAT

Create NAT

Virtual host / Zone (Interface IP)	cantik
Real Host	cantik
Service	○ All Services ● afp-over-tcp - AFP (Apple Filing Protocol) over TCP aim-icq - AIM / ICQ auth - Authentication Service cvs - CVS Server Service dhcp - DHCP/BOOTP protocol dns - Domain Name Service ○ tcp Port
Active	☑

create

Membuat Masquerade baru



INTRUSION DETECTION SYSTEM (IDS)

Snort-based
Network Intrusion Detection System (NIDS)

Apa itu IDS?

- Sistem untuk mendeteksi adanya "*intrusion*" yang dilakukan oleh "*intruder*"
- Mirip seperti alarm/camera
- Kejadian (intrusion) sudah terjadi
- Bekerjasama dengan (komplemen dari) firewall untuk mengatasi intrusion

Definisi Intrusion

- Didefinisikan sebagai kegiatan yang bersifat *anomaly*, *incorrect*, *inappropriate* yang terjadi di jaringan atau di host
- Apa yang didefinisikan sebagai intrusion kemudian dikodekan menjadi “rules” dalam IDS
  Contoh rules:
  - Mendeteksi port scanning

Jenis IDS

- Network-based
  memantau anomali di jaringan,
  misal melihat adanya network scanning
  Contoh: snort
- Host-based
  memantau anomali di host,
  misal memonitor logfile, process, file owenership, mode
  Contoh: portsentry

Contoh anomali

- *Traffic* / aktivitas yang tidak sesuai dgn policy:
  - akses dari/ke host yang terlarang
  - memiliki content terlarang (virus)
  - menjalankan program terlarang (web directory traversal:
    `GET ../..;`
    `cmd.exe`)

Snort NIDS

- Open source IDS
  host-based
  network-based
  packet sniffer
  implementasi di UNIX & Windows
- Beroperasi berdasarkan “rules”
- Informasi lebih lengkap
  http://www.snort.org

Snort Rules

- Terbagi menjadi dua (2) bagian:
  - Rule header
  - Rule option
- Contoh snort rules

```
alert tcp any any -> 202.138.228.0/24 111
(content:"|00 01 86 a5|";\ msg: "mountd
access";)
```

Tulisan yang diberi garis bawah adalah “rule header”, sedangkan selebihnya adalah “rule option”

Menangkap sesi FTP

- Buat rule snort di dalam berkas "`ftp.conf`", dengan isi:

```
log tcp any any -> 192.168.1.0/24 21
```

- Perhatikan: rule header saja
- Buat direktori bernama "`coba`", kemudian jalankan perintah berikut:

```
unix# snort -d -l coba -c ftp.conf
```

Lanjutan sesi FTP

- Jalankan sesi FTP yang menuju ke sebuah host di jaringan 192.168.1.0

```
unix$ ftp 192.168.1.101
Connected to 192.168.1.101.
220 FTP server ready.
Name: anonymous
331 Guest login ok, send your complete e-mail
  address as password.
Password: guest@hotmail.com
ftp> quit
```

Lanjutan …

- Hentikan sesi snort dengan ^c (ctrl c), kemudian pindah ke direktori “coba”
- Perhatikan bahwa ada direktori yang namanya merupakan nomor IP dari komputer yang menyerang (dalam hal ini yang melakukan FTP); misalnya 192.168.1.5
- Pindah ke direktori ini. Akan ditemukan sebuah berkas yang namanya kira-kira sebagai berikut:

  ```
  TCP:35724-21
  ```

- Kemudian amatilah isi berkas ini.

Mengamati sesi TELNET

- Buat rule snort di dalam berkas telnet.conf, dengan isi:

```
var HOME_NET [192.168.1.0/24]
log tcp any any <> $HOME_NET 23
  (session: printable;)
```

[Baris kedua ini harus ditulis dalam satu baris panjang. Perhatikan sudah ada rule option]

- Kemudian jalankan perintah berikut:

```
snort -d -l coba -c telnet.conf
```

Sesi TELNET [lanjutan]

- Jalankan sesi telnet yang menuju ke sebuah host di jaringan 192.168.1.0

```
unix$ telnet 192.168.1.101
Trying 192.168.1.101...
Connected to 192.168.1.101.
Escape character is '^]'.
Debian GNU/Linux 3.0 hurd
hurd login: user01
Password: user01
Unix% ls
Unix% exit
```

Sesi TELNET [lanjutan]

- Tahap selanjutnya sama seperti pada bagian Pengamatan Sesi FTP.
- Berkas yang dihasilkan oleh program snort kira-kira bernama

```
SESSION:35733-23
```

- Amatilah berkas ini. Anda akan dapatkan isi sesi telnet anda

Rules yang lebih kompleks

- Rules yang lebih kompleks dapat dilihat pada distribusi snort di direktori /etc/snort
  - Mendeteksi virus
  - Mendeteksi akses daerah (file) terlarang di web server
  - Paket yang memiliki isi aneh
  - Paket yang memiliki sifat aneh (flag tidak lazim)
  - Adanya portscanning
  - dan lain-lain

ACID

- Analysis Console for Intrusion Databases (ACID)
- Program yang dirancang untuk mengelolah data-data security event seperti; IDS, Firewall, dan Network Monitoring Tools
- Data-data disimpan dalam database (MySQL)

Manfaat ACID

- Log-log yang tadinya susah dibaca menjadi mudah di baca
- Data-data dapat dicari (search) dan difilter sesuai dengan kriteria tertentu
- Managing Large Alert Databases (Deleting and Archiving)
- Untuk kasus-kasus tertentu dapat merujuk alert pada situs database security seperti Securityfocus, CVE, arachNIDS

Tampilan halaman muka ACID

Analysis Console for Intrusion Databases

Added 24 alert(s) to the Alert cache

Queried on : Fri November 15, 2002 16:15:21

Database: snort_log@localhost (**schema version:** 105)

Time window: [2002-07-30 11:57:57] - [2002-11-15 16:15:03]

Sensors: 1
Unique Alerts: 133 (16 categories)
Total Number of Alerts: 629348
Source IP addresses: 9019
Dest. IP addresses: 427
Unique IP links 13996

Source Ports: 4591
TCP (4533) UDP (69)
Dest. Ports: 30065
TCP (30045) UDP (35)

Traffic Profile by ProtocolTCP (13%)

UDP (< 1%)

ICMP (87%)

Portscan Traffic (0%)

Daftar Jenis Attack

ACID Alert Listing

Added 13 alert(s) to the Alert cache

Queried DB on : Fri November 15, 2002 16:32:23

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

< Signature > < Classification > < Total > Sensor # < Src. Addr. > < Dest. Addr. > < First > < Last >

[arachNIDS] MISC Large ICMP Packet bad-unknown 17686 (3%) 1 403 5 2002-07-30 11:57:57 2002-11-15 16:31:4

ICMP Destination Unreachable misc-activity 75 (0%) 1 5 2 2002-07-30 11:59:08 2002-07-30 13:31:33

[CVE] DDOS mstream client to handler attempted-dos 1293 (0%) 1 128 2 2002-08-02 14:53:17 2002-11-15 15:00:59

PORN free XXX kickass-porn 24925 (4%) 1 1996 3 2002-08-02 10:28:40 2002-11-15 16:29:38

Tampilan Individual Attack

ACID Query Results

Meta Criteria	Signature "[CVE] DDOS mstream client to handler"
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

ID < Signature > < Timestamp > < Source Address > < Dest. Address > < Layer 4 Proto >

#0-(1-19879) [CVE] DDOS mstream client to handler 2002-08-02 14:53:17
202.53.224.41:80 202.152.6.196:12754 TCP

#1-(1-20267) [CVE] DDOS mstream client to handler 2002-08-02 15:48:59
81.27.33.7:80 202.152.6.197:12754 TCP

...