Firewall

Budi Rahardjo
(@rahard)

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)

- A firewall is a network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules
  [source: Fortinet]
- Firewall dapat berbentuk hardware dan/atau software

Definisi Firewall [3]

- 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 sharing via SMB di Windows NT dan Windows 95/98
- Rentan berbagai serangan DoS
- Solusi
  - akses terbatas SMB di lingkup lokal, dibatasi dengan firewall

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 (firewall) daripada banyak host
- Host lain yang tidak aman (unsecure) disembunyikan / dilindungi di belakang firewall
- Tidak semua OS bisa/mudah/murah diamankan tanpa bantuan sistem lain (firewall). Misal sistem yang sudah jadul

Peningkatan Privasi

- Pembatasan terhadap aplikasi untuk mencari informasi pengguna, misal *finger*
- Melindungi dari penyadapan (snoop/sniff)
- Membatasi 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 dapat mengandalkan sepenuhnya kerjasama pengguna lokal dan remote
- Firewall = policy enforcement

Bagaimana caranya?

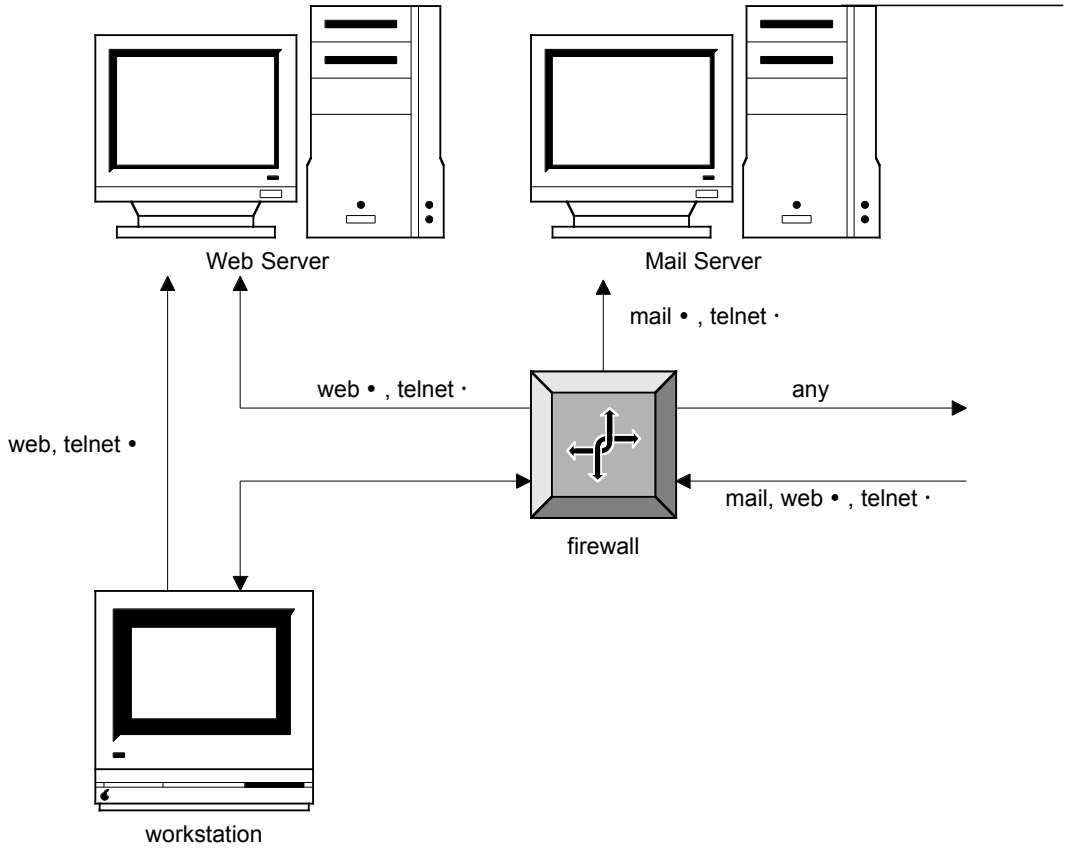
- Packet filter
- Application layer gateway (proxy)
- (Stateful inspection)
- Next-Generation Firewall (NGFW)

Packet Filter: Filter di level paket

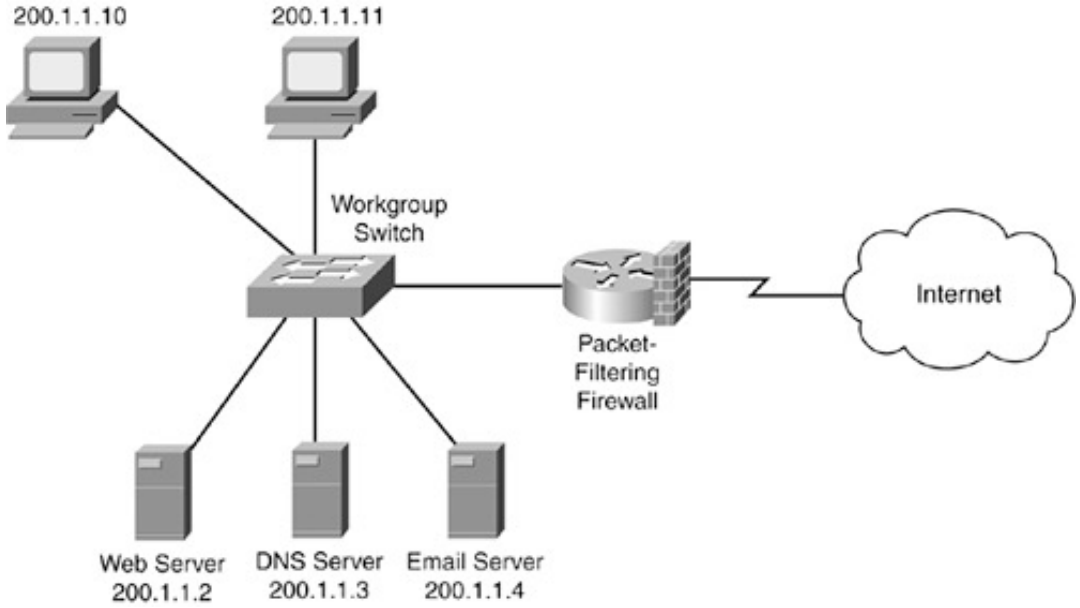
- Independen terhadap aplikasi
- kinerja tinggi
- skalabilitas
- security rendah
- tidak kenal konteks

Packet Filter

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



Packet Filter



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

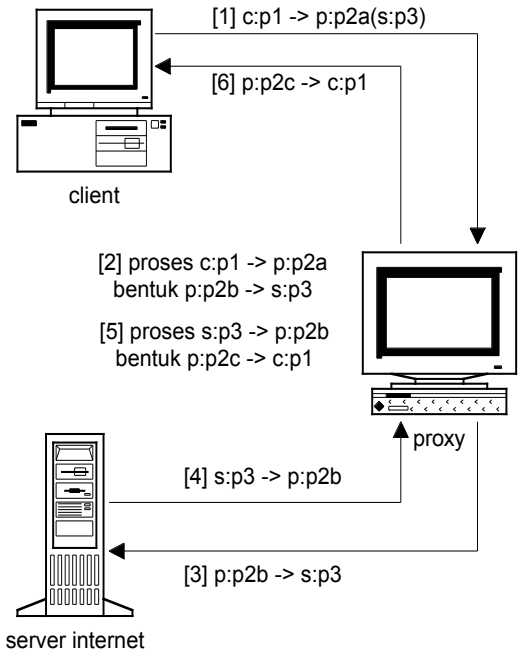
from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

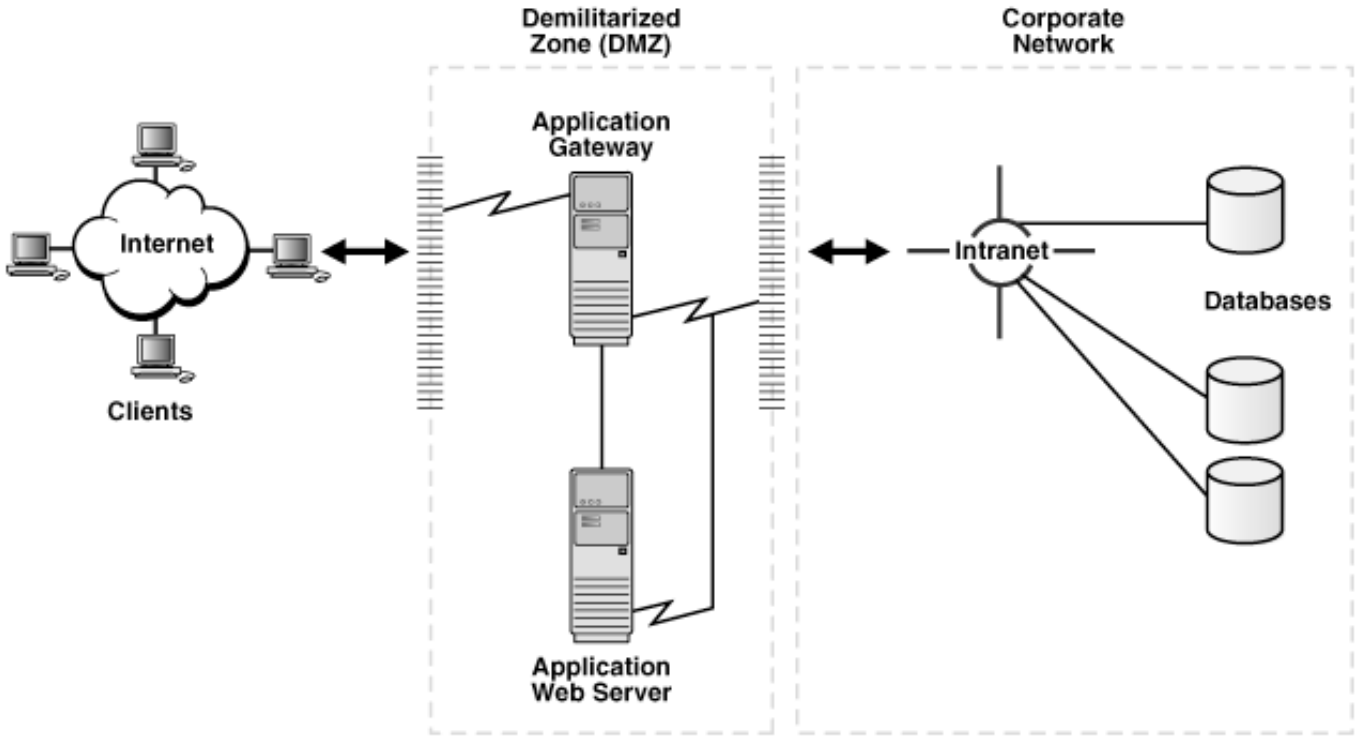
Application Layer Gateway/Proxy

- 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



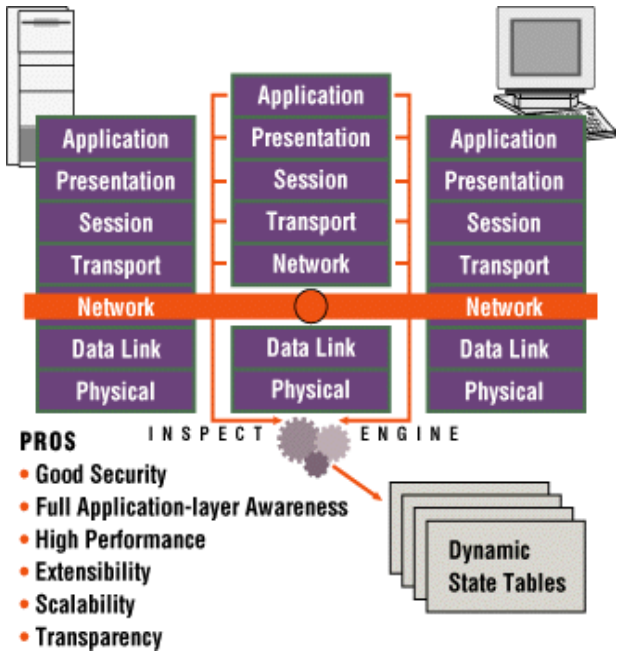

Demilitarized
Zone (DMZ)
Corporate
Network
Application
Gateway
Internet
Intranet
Databases
Clients
Application
Web Server

Stateful Inspection

- security bagus
- pemahaman konteks lengkap
- kinerja tinggi

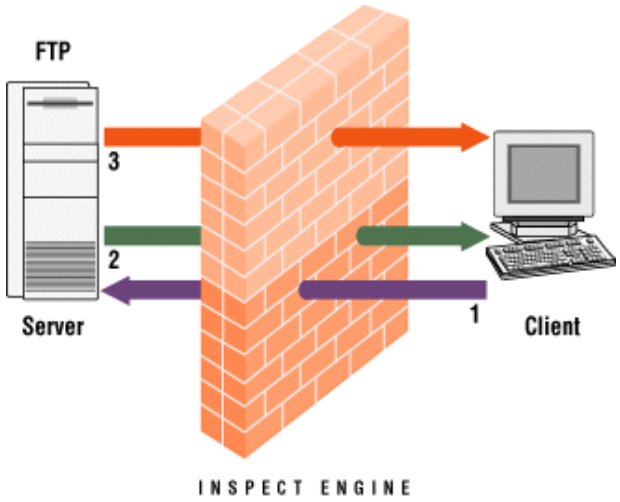
- algoritma inspeksi state!
  - spesifik vendor
  - harus di-update untuk protokol baru

Stateful Inspection

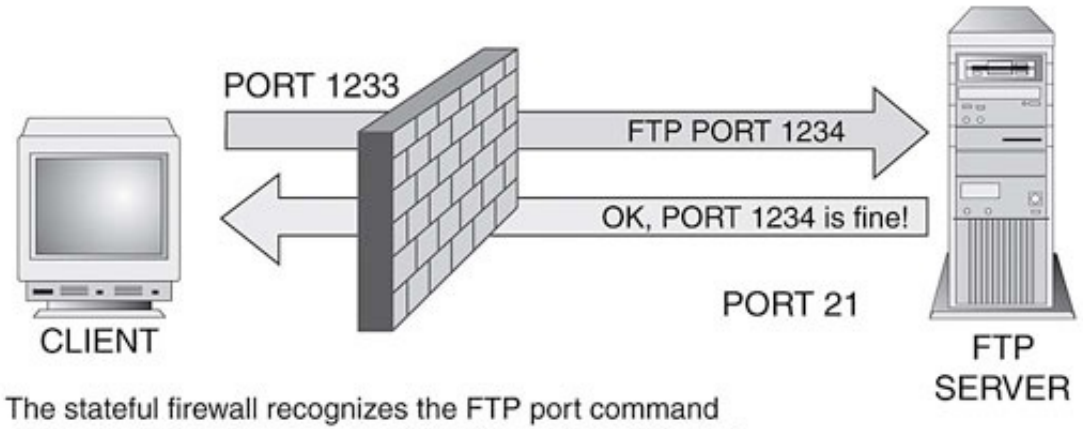


- intersepsi packet di layer network
- inspeksi state
  - ekstraksi informasi state
  - tabel dinamik state
- filtering di layer network
  - packet rule
  - state rule

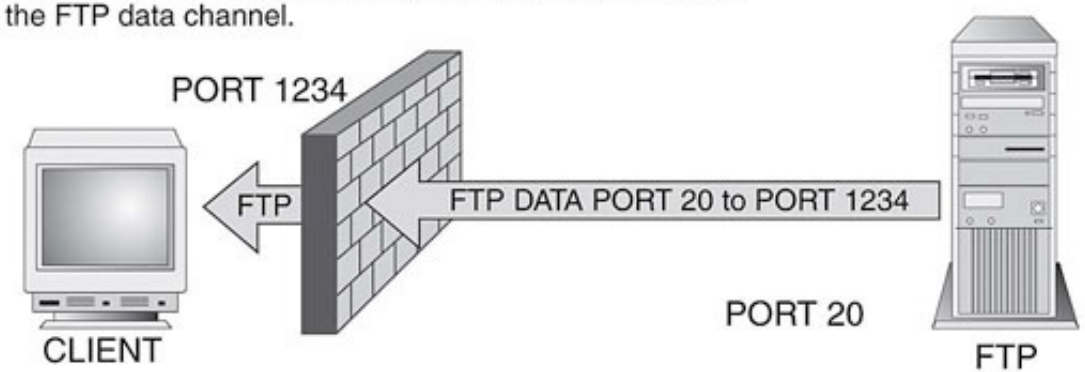
Stateful Inspection



- 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



The stateful firewall recognizes the FTP port command and records its value to securely facilitate the creation of the FTP data channel.



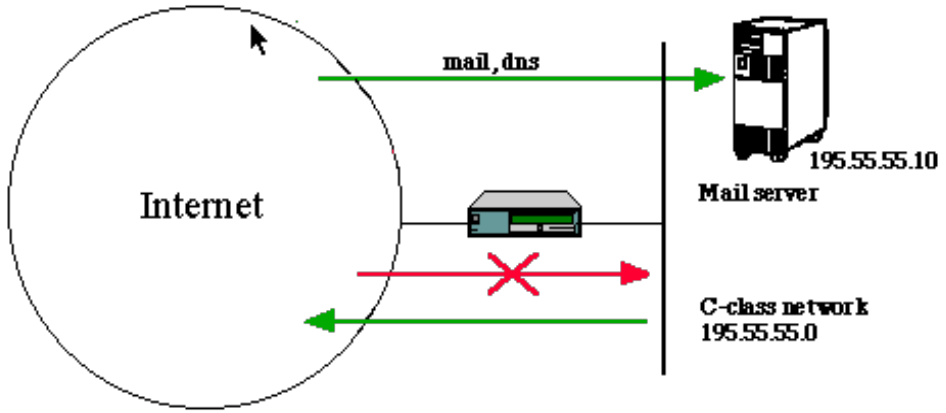
When the FTP data connection is initialized by the server, the firewall recognizes the IP address and port combination used and allows the inbound connection to pass.

Kombinasi

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

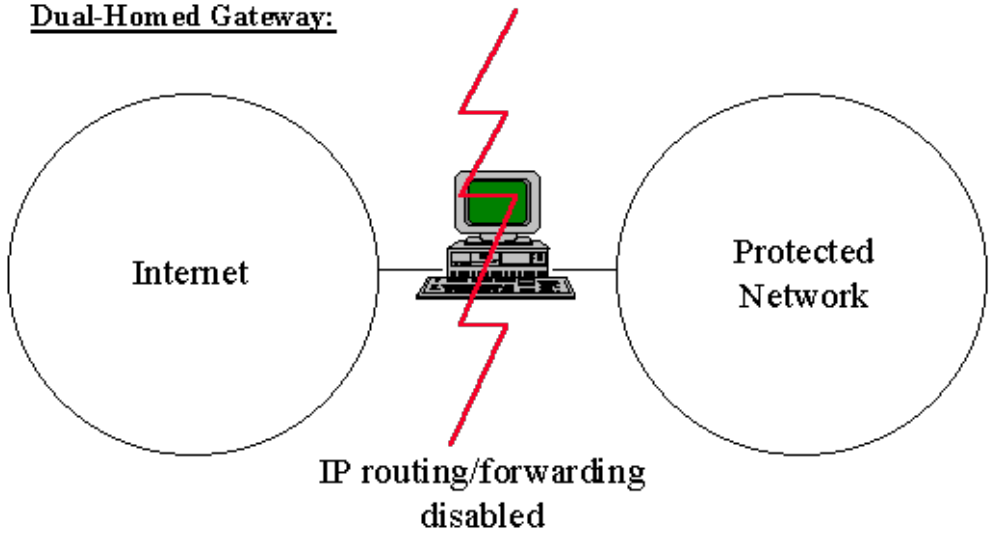
Packet Filtering

- full routing, tetapi
- packet filter diaktifkan



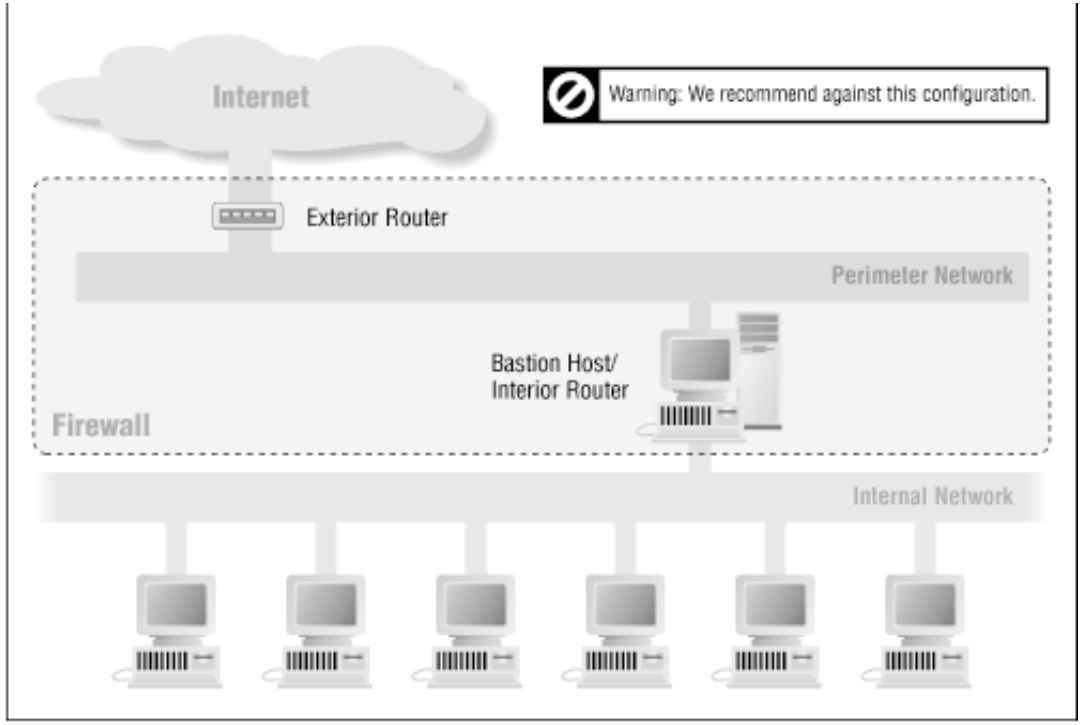
Dual Homed Gateway

- no routing
- proxy



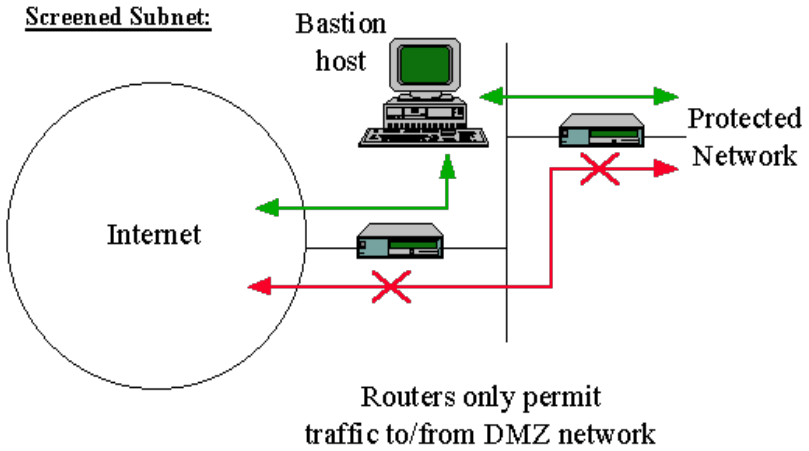
Screened Host

- packet filtering router
- single bastion host



Screened Subnet

- packet filtering router
- several servers
- DMZ



Next-Generation Firewall

- IPS: menggabungkan IDS
- Deep Packet Inspection (DPI)
  - Mengevaluasi content dari paket, bukan saja header
- Application awareness
  - ”Memahami” aplikasi (zoom, dropbox, dll.) tidak hanya berbasis pada port yang digunakan saja
- Threat intelligence integration
- Additional: SSL/TLS, sandbox

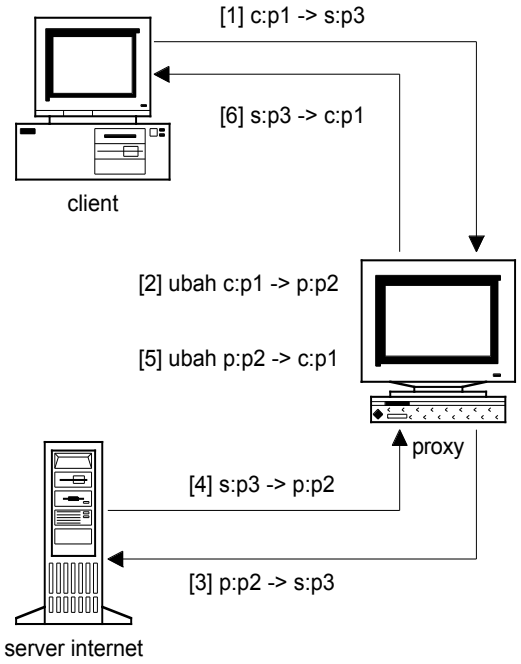
Masalah Pada Firewall

- 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)

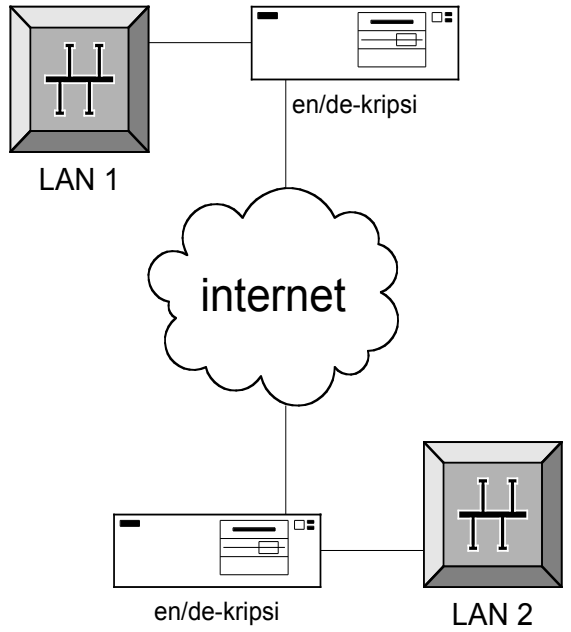
NAT



- 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



Hardware vs Software

Hardware

- High performance

Software

- Easy configuration and update
- Sekarang kinerjanya (performance) mendekati hardware

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

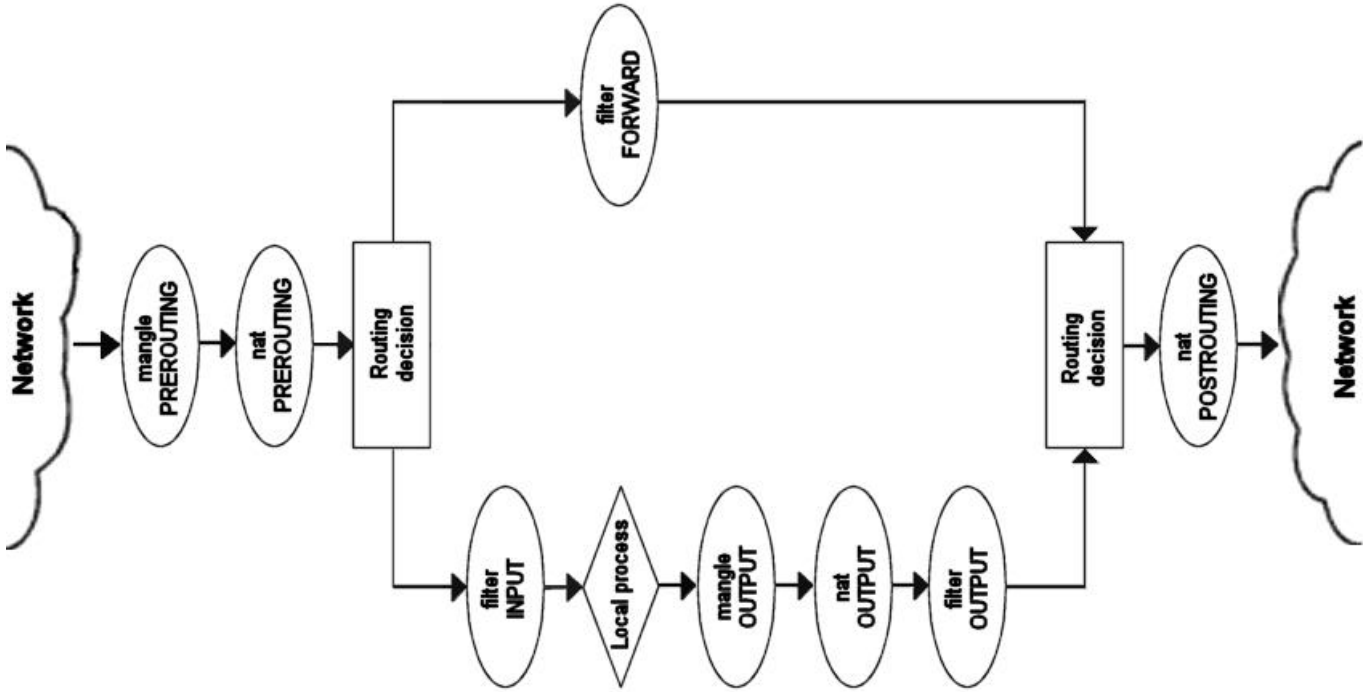
INDOCISC Linux Firewall

- 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 akses dari satu segmen (misal 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
```

Catatan: untuk menghapus filter itu gunakan "-D"

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
  - Menggunakan aplikasi firewall
- Pada dasarnya memberikan perintah iptables
- Mengurangi kesalahan (jika rules sangat kompleks)

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

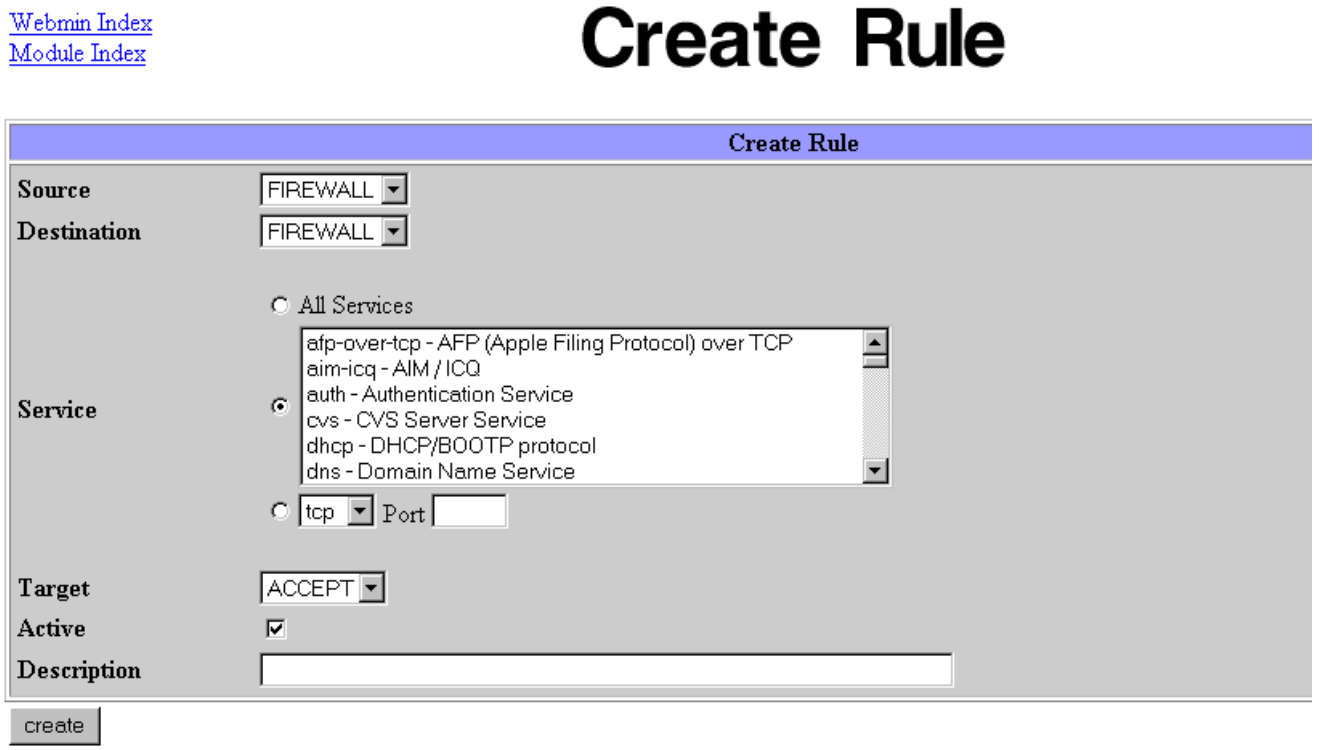
Webmin Index
Module Index

Firewall Rules

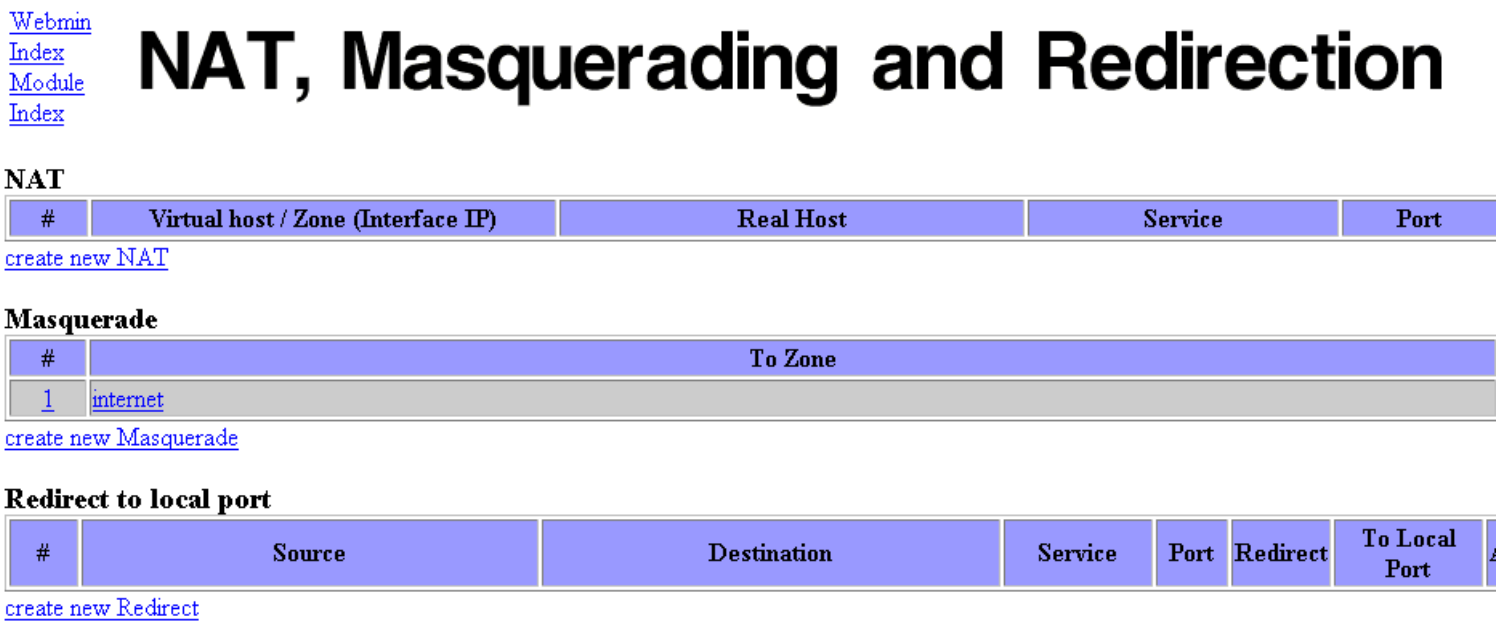
#	Source	Destination	Service	Port	Target	Active
1	dmz	internet	cvs, dns, ftp, http, https, icmp_acc, ping		ACCEPT	YES
2	internet	dmz	dns, http		ACCEPT	YES

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

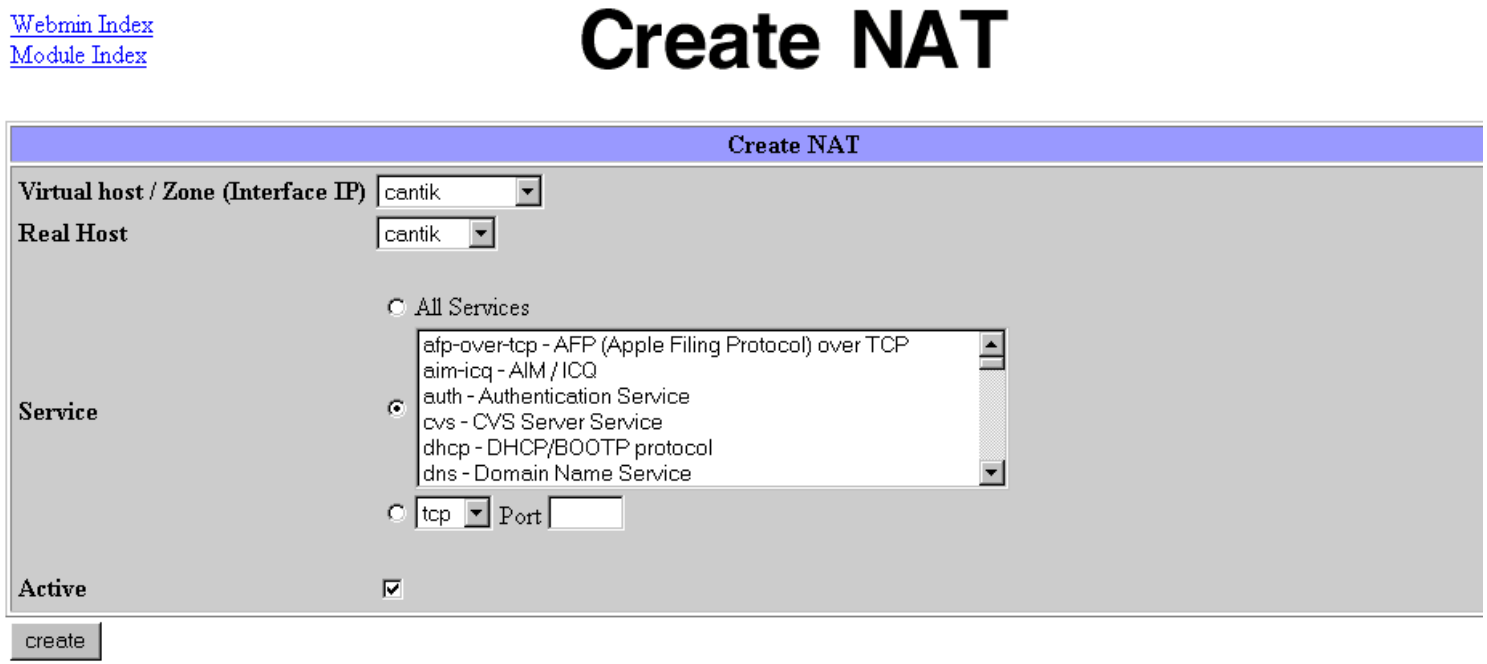
create new Masquerade

Redirect to local port

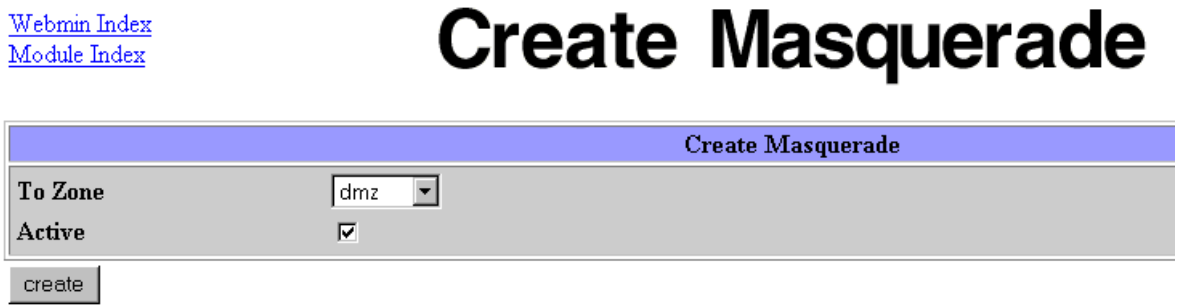
#	Source	Destination	Service	Port	Redirect	To Local Port

create new Redirect

Membuat NAT baru



Membuat Masquerade baru



Berbagai Firewall

- Iptables
- IPCop: www.ipcop.org
- Shorewall: shorewall.net
- ClearOS: https://www.clearos.com/
- Monowall: http://m0n0.ch/wall/index.php
- UFW (Uncomplicated Firewall), GUFW (GUI version)
- ...

Application Firewall

- Melakukan fungsi firewalling tetapi pada lapisan (layer) aplikasi (biasanya aplikasi web/HTTP)
  - Melakukan pembatasan aplikasi yang melakukan SQL injection
  - Membatasi akses dari paket yang dikenal sebagai serangan (attack)

Penutup

- Firewall merupakan salah satu bagian dari *perimeter security*, yaitu yang melindungi sistem dengan mengamankan sekeliling (perimeter) sistem

Referensi

- Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet Security: Repelling the Wily Hacker (2nd ed.). Addison-Wesley.
- Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.
- IST Special Publication 800-41 Rev. 1 (2009). Guidelines on Firewalls and Firewall Policy. National Institute of Standards and Technology.