

# FIREWALL

Deris Stiawan  
FASILKOM UNSRI

# Pendahuluan

- Internet adalah jaringan publik
- Terdiri dari berbagai tipe dan sifat pengguna
- Dibutuhkan suatu cara untuk mengamankan jaringan komputer kita

# Firewall

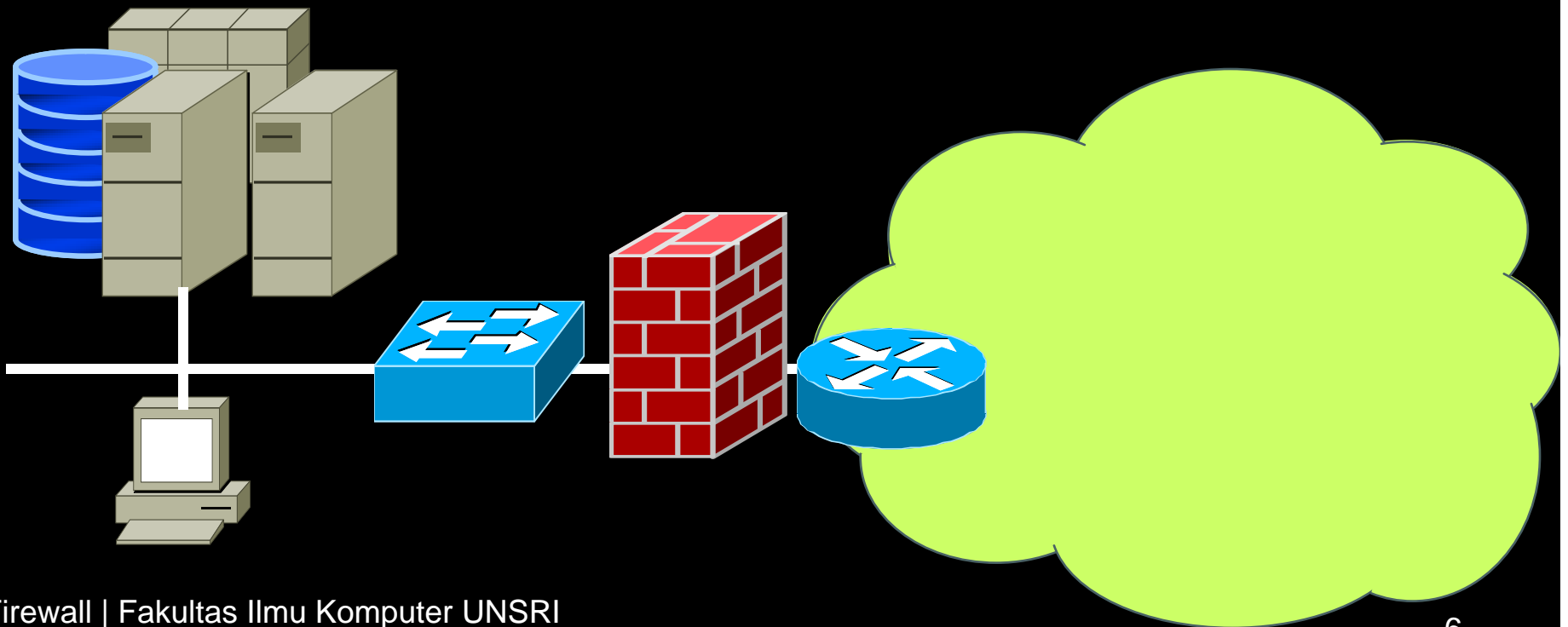
- Berupa seperangkat *hardware* atau *software*, bisa juga berupa seperangkat aturan dan prosedur yang ditetapkan oleh organisasi.
- Sistem *Security* yang menggunakan device atau sistem yang diletakkan di dua jaringan dengan fungsi utama melakukan *filtering* terhadap akses yang akan masuk
- Box h/w = PIX Firewall cisco, Passport Nortel, Checkpoint, Cyberguard,...
- H/w atau s/w yang penting “policy”

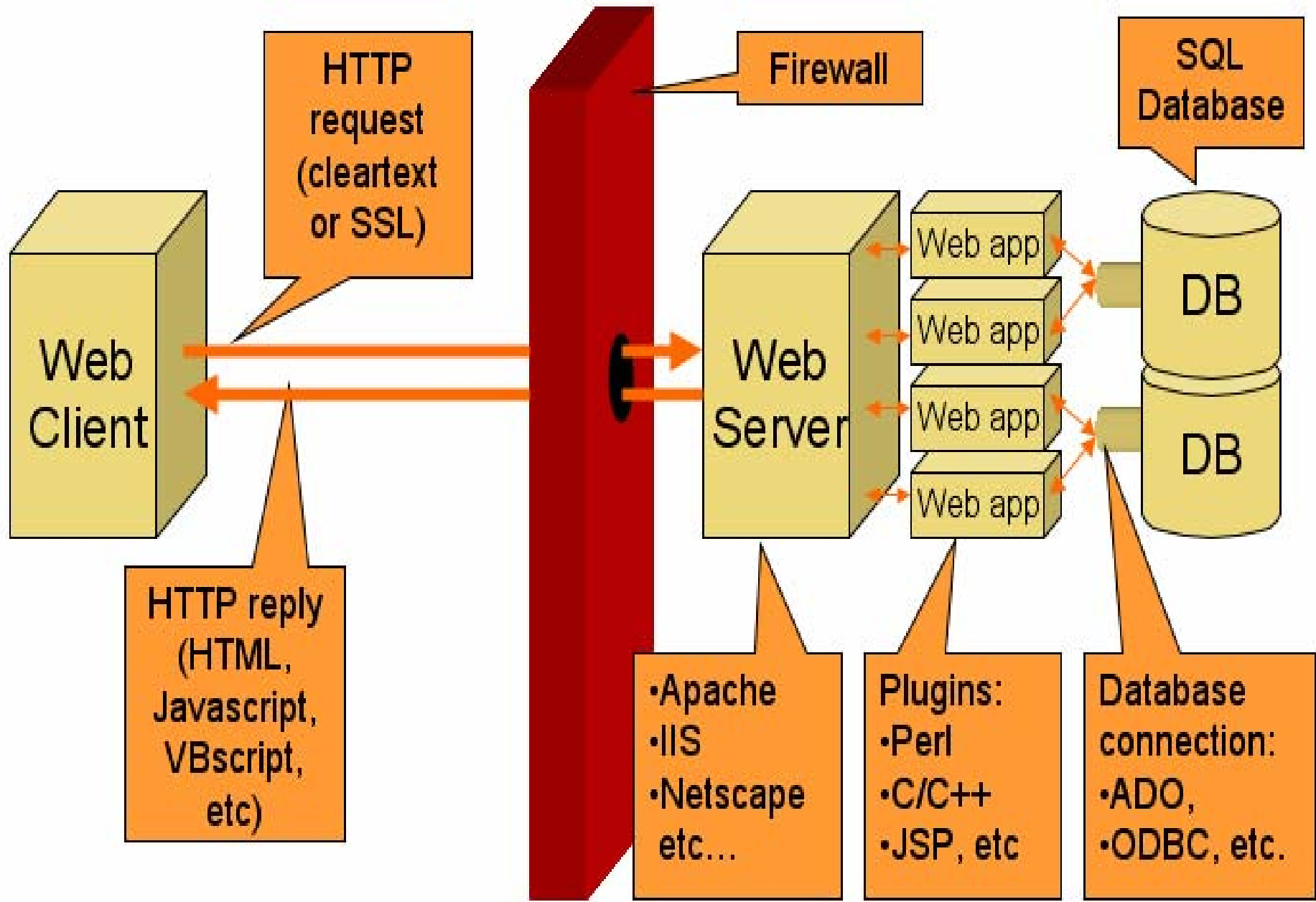
- Sebagai akses *unauthorized* yang akan keluar atau masuk ke jaringan LAN dan ke Internet.
- Seorang satpam yang akan memeriksa semua orang yang akan masuk dan keluar,
- Kebijakan direktur perusahaan tersebut, satpam hanya menjaga dan menjalankan perintah yang diterimanya

# Metode Firewall

- Packet filtering & analysis
- Protocol (TCP/UDP)
- Port address
- Keyword
- Ip address
- Application

- Pada umumnya sebuah Internet *Firewall* diinstall di antara jaringan internal yang terhubung dengan Internet





# *Funksi Firewall*

- ***Firewall sebagai focus keputusan security***, Bayangkan firewall sebagai *choke point*, semua traffic yang masuk dan keluar harus melewati “ pos pemeriksaan” ,

- ***Firewall mendukung security policy***, misalnya perusahaan menetapkan penggunaan NAT (Network Address Translation),
  - hanya user atau group
  - hanya protocol tertentu,
  - hanya beberapa aplikasi dan sumber daya
  - Waktu akses
  - Akses dari tempat tertentu

- ***Mencatat Log Aktivitas User***, oleh karena trafik melewati firewall, maka disini dapat kita buat suatu system untuk mencatat semua kegiatan system dan user yang menggunakan jaringan. Sebagai dokumentasi yang tepat untuk menentukan policy (AAA)

## *Kekurangan*

- Firewall tidak dibuat untuk penyerang “orang dalam”
- *Firewall* tidak dapat melindungi dan melawan hubungan yang tidak melewatinya (sistem *back-door*).
- *Firewall* tidak dapat melindungi dan melawan virus

# Metode-Metode FIREWALL

# Pertimbangan

- Apa yang akan diproteksi
- Membeli / membangun sendiri
  - Box atau by software
  - Fasilitas yang disediakan (log, analys,...)
  - Memperhatikan “brand” & standar dipasar
- Anggaran biaya
- User policy
- *Upgradeable* & standarisasi NCSA (National Computer Security Associates)
- Vendor dan dukungan teknis

# Proxy Server

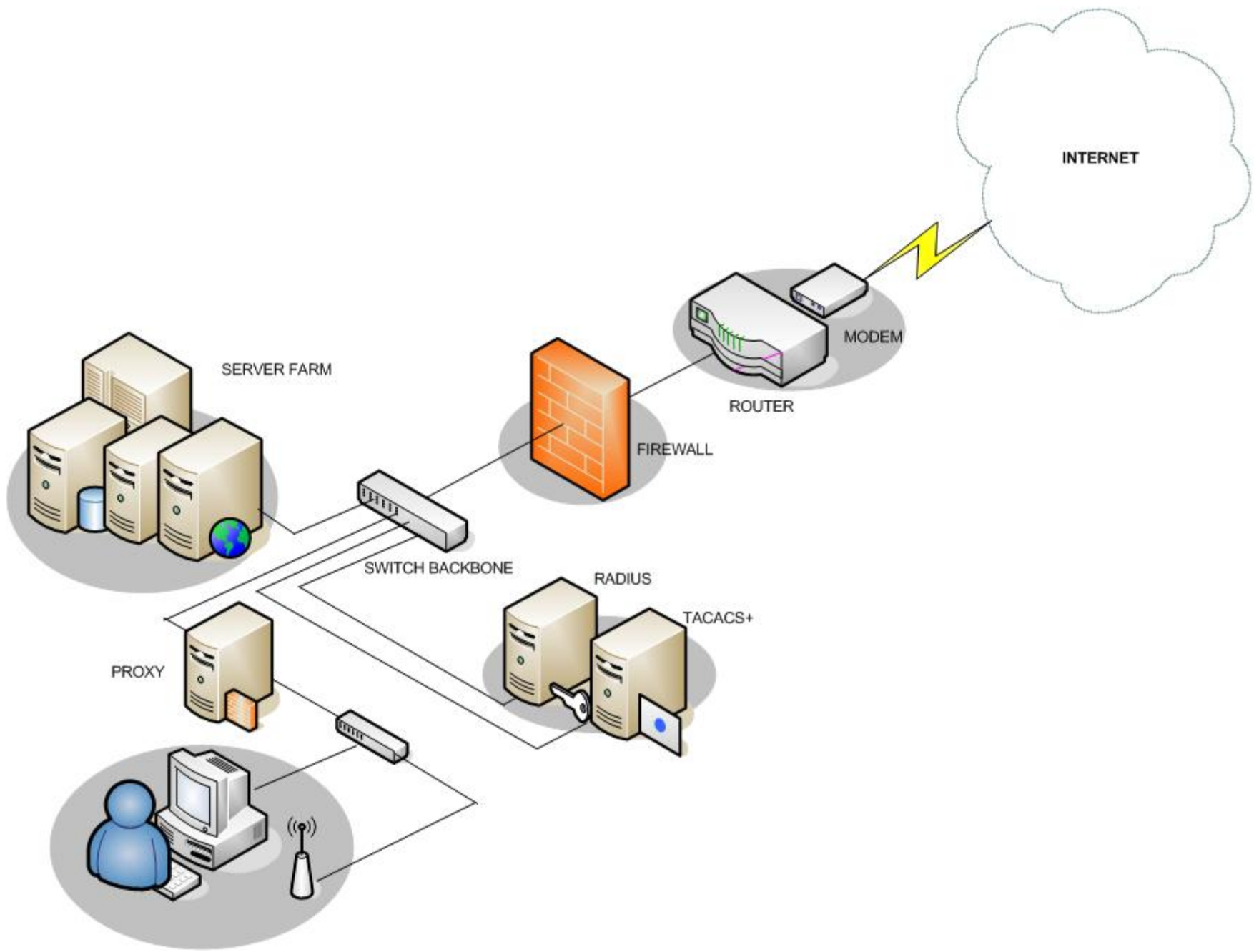
- Memenuhi permintaan *user* untuk layanan Internet (*http, FTP, Telnet*) dan mengirimkannya sesuai dengan kebijakan
- Bertindak sebagai gateway menuju layanan
- Mewakili paket data dari dalam dan dari luar
- Menangani semua komunikasi internet – eksternal

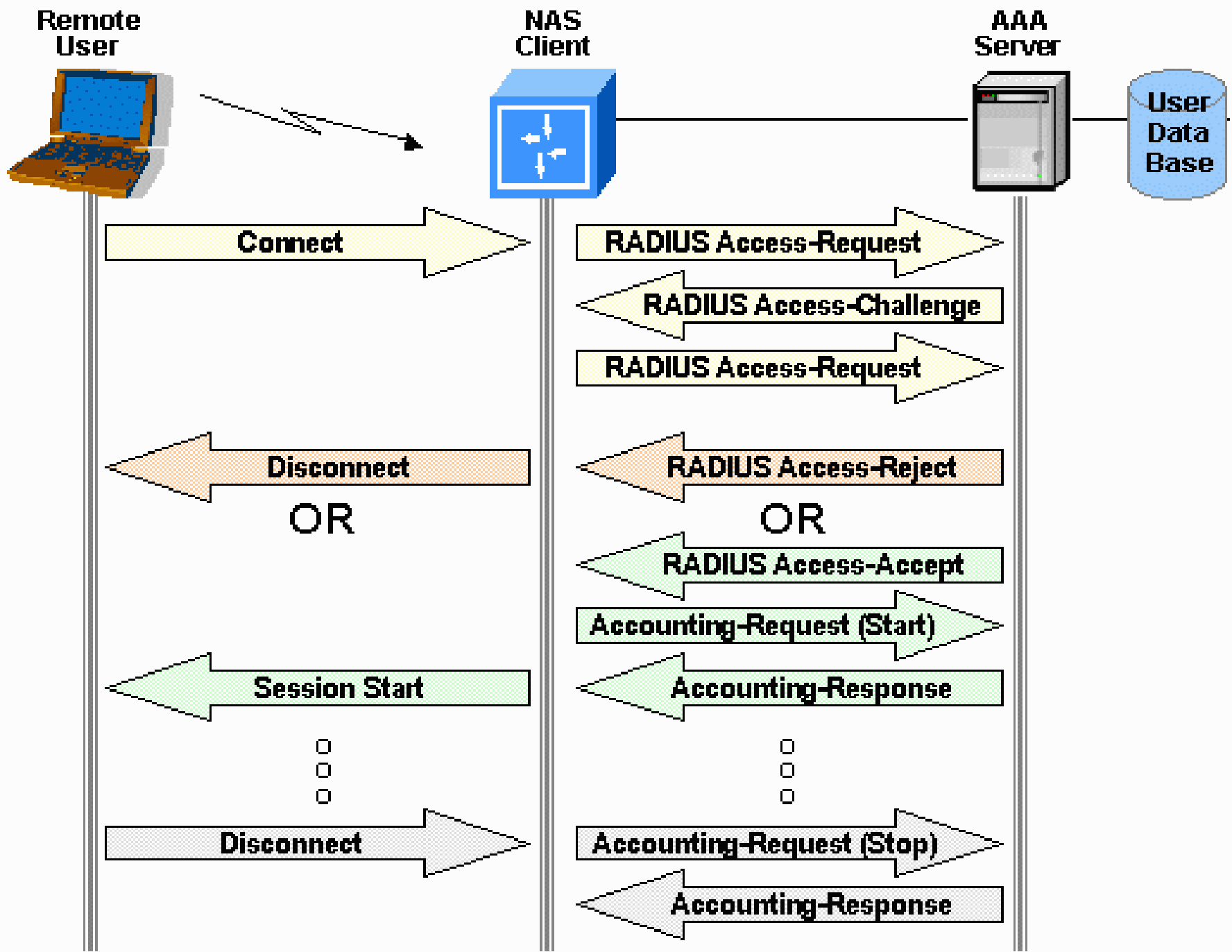
- Bertindak sebagai gateway antara mesin internal dan eksternal
- *Proxy server* mengevaluasi dan mengontrol permintaan dari *client*, jika sesuai policy dilewatkan jika tidak di deny/drop
- Menggunakan metode NAT
- Memeriksa isi paket
- *Store & forward cache*
- S/W = ISA, Squid, ...

# AAA

- ***Authentication, Authorization, Accounting System***
- Mengotentikasi keabsahan, memberi wewenang, dan mencatat semua aktivitas
- menangani proses autentikasi dari banyak user dan membandingkannya dengan database yang ada pada server

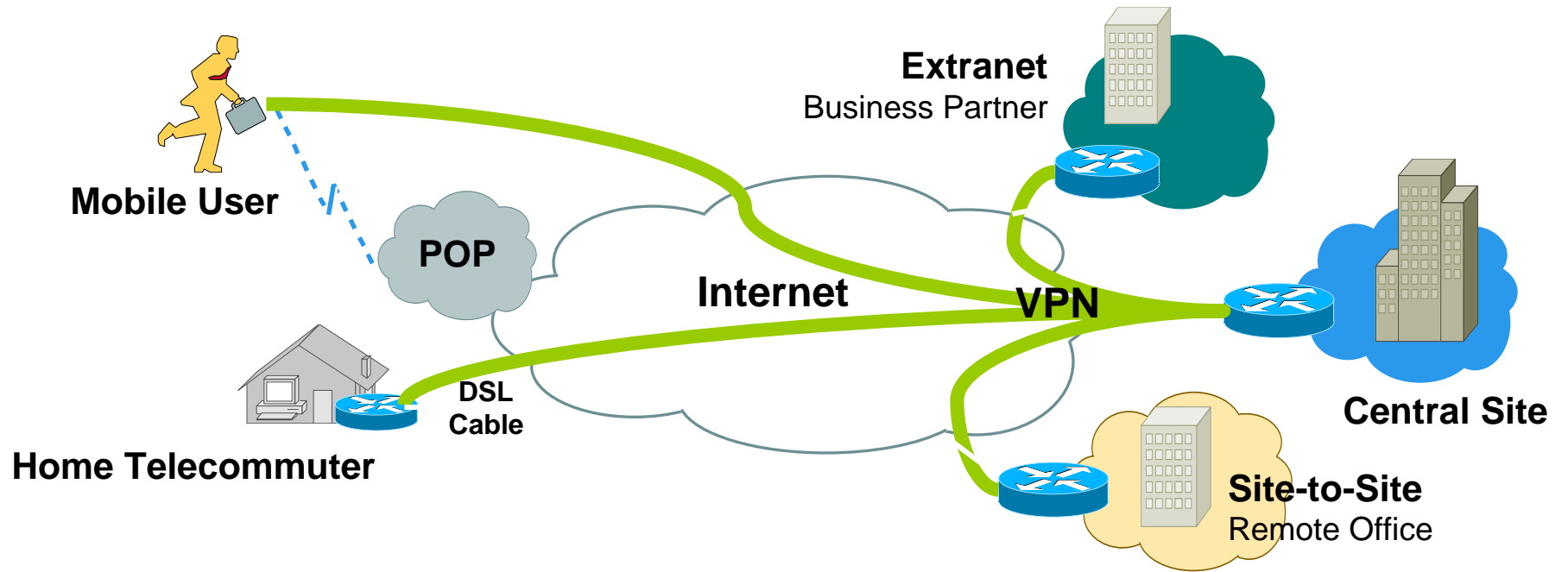
- melayani banyak user dalam waktu yang bersamaan, mensinkronisasi user yang akan login dengan Database server dan dengan server AAA lainnya
- Protocol TACACS+ (*Terminal Access Control Systems +*) dan RADIUS (*Remote Access Dial-In User Services*) dan KERBE-OS)





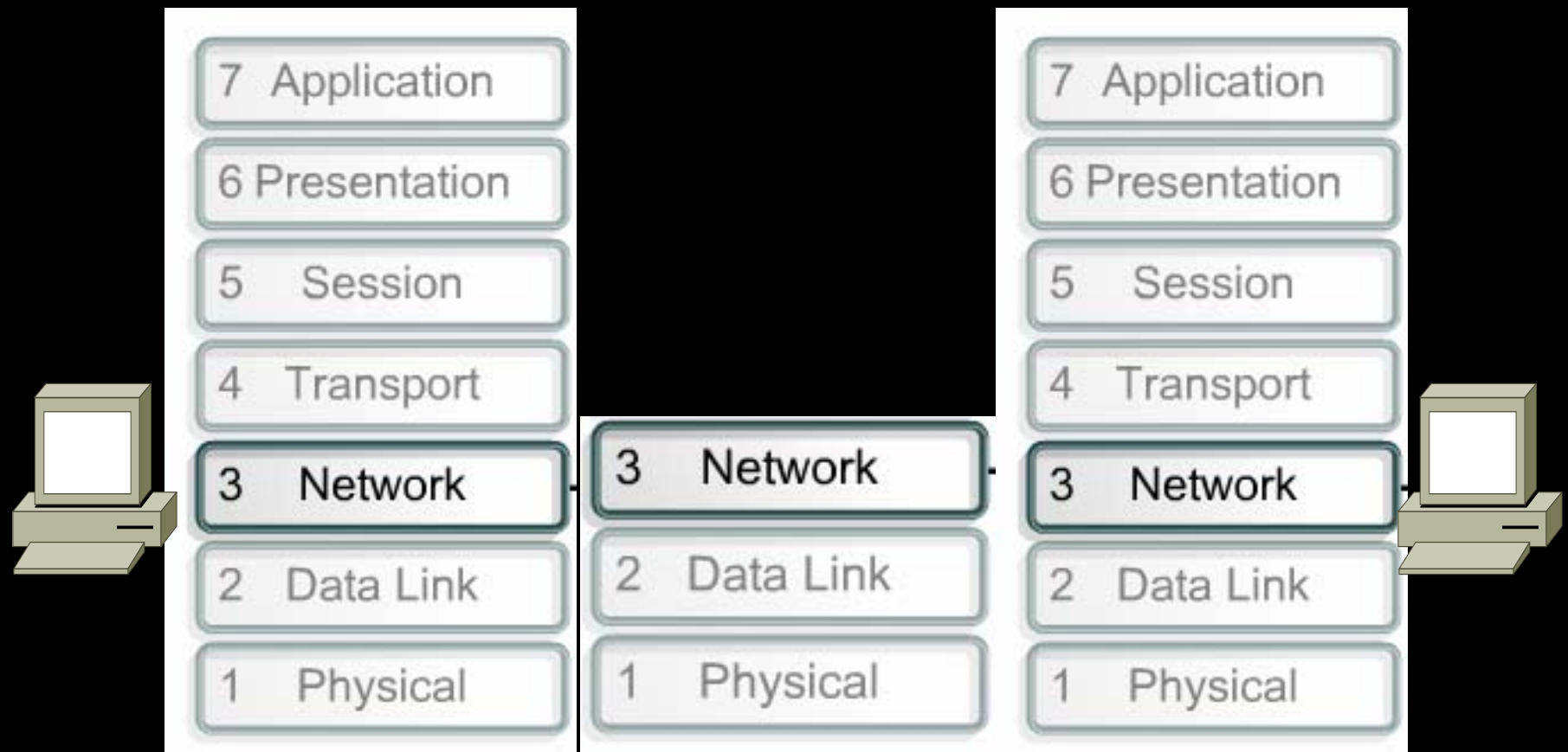
# VPN

- Encapsulation paket di jaringan publik
- Seakan-akan membuat jaringan private di atas jaringan publik
- Metode tunneling
- Protocol IPSec, PPTP, GRE
- Menghemat anggaran komdat WAN



# Packet Filter Based

- suatu aturan untuk meneruskan atau menolak akses dari dalam dan luar jaringan kita,
- variabelnya : alamat asal (source address, alamat tujuan (destination address), protocol, dan nomer port.



# Access Control Filtering

- Metode menggunakan
  - ACLs
  - IPChain
  - IPTables
  - IP filter
  - IP Fw
  - ...

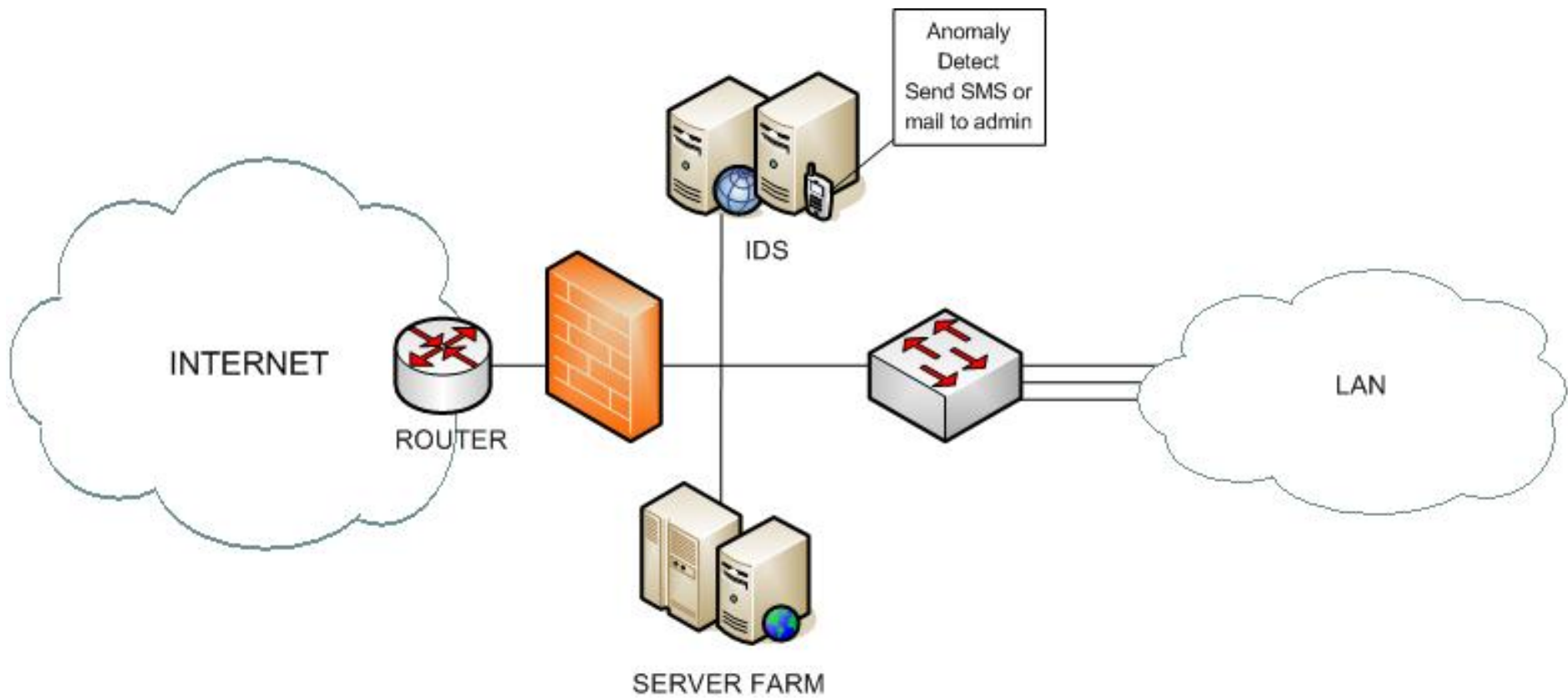
# Metode HoneySpot

- Proyek HoneyNet dengan sengaja memancing hacker. Mereka boleh bersenang-senang di sana, sementara metodenya dipelajari.
- Menyediakan server untuk “dikerjai” hacker agar menghabiskan waktu dan diawasi
- Disiapkan untuk menganalisa serangan dan metode yang dilakukannya
- By s/w : Deception Toolkit, Cybercorp, sting, snort, ...

# Intrusion Detection System (IDS)

- IDS dapat berfungsi sebagai sensor, *Director*, *Communication Service* atau peringatan dini dari percobaan kegiatan anomaly.
- memberikan peringatan secara dini jika jaringan akan ada untuk mencoba menyerang
- Sistem bisa “mixed” dengan mail/sms sebagai sistem peringatan
- Mengenali dengan metode
  - ***misuse detection***, dengan mencari “*signatures*” yang sudah dikenali
  - ***anomali detection***, dengan mengamati perilaku yang tidak wajar oleh user atau aktifitas aplikasi

- ***host-based IDS (HIDS)***
  - Memeriksa log system dan aktivitas
- ***network-based IDS (NIDS)***
  - Memeriksa tipe dan konten network packet



Enter Sensor Information - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address <https://10.1.10.98/ids-config/s511.do> Go Links >>

CISCO SYSTEMS Close | Help | About

## Management Center for IDS Sensors

User ID: **admin**

Devices
Configuration
Deployment
Reports
Admin

Sensor
Sensor Group
Progress Viewer
Statistics

You Are Here: ♦ Devices > Sensor Actions & Notifications:

**Mode: ADDING**

- 1. Select Type
- 2. Select Group
- 3. **Enter Sensor Information**
- 4. Summary

### Enter Sensor Information

Identification	
IP Address: *	<input type="text" value="10.1.10.82"/>
NAT Address:	<input type="text"/>
Sensor Name: *	<input type="text" value="nss-4255"/>
User ID: *	<input type="text" value="cisco"/>
Password: (or pass phrase if using existing SSH keys): *	<input type="password" value="XXXXXXXXXX"/>
Port:	<input type="text" value="443"/>
Enable TLS:	<input checked="" type="checkbox"/>
Version:	<input type="text" value="2.000(001)IOS"/>
Comment:	<input style="height: 40px;" type="text"/>
NAT Address to MC:	<input type="text"/>
Use Existing SSH keys:	<input type="checkbox"/>
Enable Password:	<input type="text"/>
SDEE Credentials:	
Use SSH Credentials (Applicable only for IOS IPS):	<input checked="" type="checkbox"/>

Note: \* - Required Field

- Step 3 of 4 -

< Back
Next >
Finish
Cancel

**Instructions**

Enter the sensor identification settings here.

Help...

Signature(s) in Group - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://10.1.10.98/ids-config/s1000.do>

CISCO SYSTEMS

## Management Center for IDS Sensors

Close | Help | About

User ID: admin

Devices Configuration Deployment Reports Admin

Settings Copy Pending History Updates Compare

You Are Here: Configuration > Settings > Signatures > IPS 5.x

Actions & Notifications:

### Signature(s) in Group

Scope: Global

Group by: Engine Select Group: service-rpc Filter: ID  Filter

Showing 1-10 of 75 records

	<input type="checkbox"/>	ID	Subsig	Signature	Engine	Enabled	Retired	Severity	Action	SFR	Edit Prop Src	Tune Param Src
1.	<input type="checkbox"/>	6100	0	<a href="#">RPC Port Registration</a>	service-rpc	Yes	No	high	produce-alert	100	Global	IDS 5 Defaults
2.	<input type="checkbox"/>	6100	1	<a href="#">RPC Port Registration</a>	service-rpc	Yes	No	high	produce-alert	100	Global	IDS 5 Defaults
3.	<input type="checkbox"/>	6101	0	<a href="#">RPC Port Unregistration</a>	service-rpc	Yes	No	high	produce-alert	100	Global	IDS 5 Defaults
4.	<input type="checkbox"/>	6101	1	<a href="#">RPC Port Unregistration</a>	service-rpc	Yes	No	high	produce-alert	100	Global	IDS 5 Defaults
5.	<input type="checkbox"/>	6102	0	<a href="#">RPC Dump</a>	service-rpc	Yes	No	medium	produce-alert	100	Global	IDS 5 Defaults
6.	<input type="checkbox"/>	6102	1	<a href="#">RPC Dump</a>	service-rpc	Yes	No	medium	produce-alert	100	Global	IDS 5 Defaults
7.	<input type="checkbox"/>	6103	0	<a href="#">Proxied RPC Request</a>	service-rpc	Yes	Yes	informational	produce-alert	100	Global	IDS 5 Defaults
8.	<input type="checkbox"/>	6103	1	<a href="#">Proxied RPC Request</a>	service-rpc	Yes	Yes	informational	produce-alert	100	Global	IDS 5 Defaults
9.	<input type="checkbox"/>	6104	0	<a href="#">RPC Port Reg Spoof</a>	service-rpc	Yes	No	high	produce-alert	100	Global	IDS 5 Defaults
10.	<input type="checkbox"/>	6104	1	<a href="#">RPC Port Reg Spoof</a>	service-rpc	Yes	No	high	produce-alert	100	Global	IDS 5 Defaults

Rows per page: 10 Go to page: 1 of 8 Pages Go

Edit Tune Enable Disable Retire Activate

**Instructions**

This screen contains a list of attack signatures recognized by the sensor.

To view the NSDB information regarding a specific signature, click on the signature ID link; to edit a specific signature, click on the Signature link; to tune a signature micro-engine, click on the Engine link.

[Help...](#)

**TOC**

- > Signatures
  - .. Signature Variables
  - .. IDS 4.x
  - .. **IPS 5.x**
  - .. IOS IPS
  - .. Miscellaneous (IPS 5.x)
- > Signature Wizard
  - .. IDS 4.x
  - .. IPS 5.x
  - .. IOS IPS
- > Event Actions (IPS 5.x)
  - .. Event Variables
  - .. Target Value Rating
  - .. Action Overrides
  - .. General Settings
- > Interfaces (IPS 5.x)
  - .. Bypass
  - .. Traffic Flow
  - .. Notifications
- > Analysis Engine (IPS 5.x)
  - .. Global Parameters
- > SNMP (IPS 5.x)
  - .. General Configuration
  - .. Traps Configuration
  - .. Traps Destination
- .. Port Mapping (IDS 4.x)
- .. Internal Networks (IDS 4.x)
- .. NTP Server
- > Blocking
  - .. 4.x Blocking Properties
  - .. 5.x Blocking Properties
  - .. Never Block Addresses
- > Logging (IDS 4.x)
  - .. Automatic IP Logging
- > Communications
  - .. IOS IPS SDEE Properties
  - .. Allowed Hosts
  - .. IOS IPS General Properties

Applet objectselector started

Internet

Rows Columns Events Graph Actions Networking Tools

Count	Attacker Address	Sig Name	Attacker Port	Victim Address	Victim Port	Severity	Sensor Name	Alert Details	Local Time	Local Date
1	10.1.1.223	BO2K-TCP-nonStealth	5150	10.10.101.104	1581	High	ips-4255	<n/a>	09:12:04 AM	Fri, Jul 01, 2005
3		Back Door Response (TCP 3127)	3127	+						
1		Deep Throat Response	2140	10.10.101.101	60000	High	ips-4255	<n/a>	09:12:02 AM	Fri, Jul 01, 2005
3		DsRolerUpgradeDownlevelServer Request	3946	10.10.110.111	445	Info	ips-4255	<n/a>	+	
2		ICMP Redirect	<n/a>	10.10.108.100	<n/a>	Info	ips-4255	<n/a>	09:17:30 AM	Fri, Jul 01, 2005
2		IE Object Tag Overflow Exploit	80	10.10.107.135	2328	High	ips-4255	<n/a>	+	
1		Impossible IP Packet	135	10.1.1.223	135	High	ips-4255	<n/a>	09:12:41 AM	Fri, Jul 01, 2005
2		Microsoft ActiveX Help Control	80	10.10.107.108	3120	High	ips-4255	<n/a>	+	
3		SMB Remote Lsarpvc Service Access Attempt	3946	10.10.110.111	445	Info	ips-4255	<n/a>	+	
3		Windows LSASS RPC Overflow	3946	10.10.110.111	445	High	ips-4255	<n/a>	+	
1	10.3.1.104	NSS Back Orifice Ping	53	10.1.1.15	31337	Medium	ips-4255	<n/a>	10:01:56 AM	Fri, Jul 01, 2005
1	10.3.17.14	Half-open SYN Attack	60577	10.4.18.1	80	High	ips-4255	<n/a>	08:02:22 AM	Fri, Jul 01, 2005
1	10.3.17.25	Half-open SYN Attack	24903	10.4.18.1	80	High	ips-4255	<n/a>	07:02:21 AM	Fri, Jul 01, 2005
2	10.10.101.100	Back Orifice Activity (UDP)	1034	10.1.1.223	31337	Medium	ips-4255	+		
1	10.10.101.103	NetBus Pro Traffic	1026	10.1.1.223	20034	Medium	ips-4255	<n/a>	09:12:03 AM	Fri, Jul 01, 2005
2	10.10.101.108	ISS PAM.dll ICQ Parser Buffer Overflow	4000	10.1.1.223	50212	High	ips-4255	+		
1	10.10.102.101	DNS Inverse Query Buffer Overflow	57788	10.1.1.223	53	High	ips-4255	<n/a>	09:12:30 AM	Fri, Jul 01, 2005
2	10.10.102.102	Invalid Netbios Name	+							
1	10.10.103.101	SMB Suspicious Password Usage	51559	10.1.1.223	139	Low	ips-4255	<n/a>	09:12:42 AM	Fri, Jul 01, 2005
1	10.10.103.104	Netbios Enum Share DoS	4247	10.1.1.223	139	High	ips-4255	<n/a>	09:12:45 AM	Fri, Jul 01, 2005
3	10.10.103.105	NETBIOS Stat	33082	10.1.1.223	137	Low	ips-4255	<n/a>	+	
1	10.10.103.106	LPR Format String Overflow	1214	10.1.1.223	515	High	ips-4255	<n/a>	09:12:47 AM	Fri, Jul 01, 2005
2	10.10.103.108	SMB: RFPoison Attack	1469	10.1.1.223	139	High	ips-4255	+		
1	10.10.104.100	HTTP 1.1 Chunked Encoding Transfer	59603	10.1.1.223	80	Medium	ips-4255	<n/a>	09:13:23 AM	Fri, Jul 01, 2005
1	10.10.104.101	HTTP 1.1 Chunked Encoding Transfer	59431	10.1.1.223	80	Medium	ips-4255	<n/a>	09:13:25 AM	Fri, Jul 01, 2005
1	10.10.104.102	WWWIS Internet Printing Overflow	32800	10.1.1.223	80	High	ips-4255	<n/a>	09:13:26 AM	Fri, Jul 01, 2005
2	10.10.104.104	MSSQL Resolution Service Stack Overflow	+							
2	10.10.104.105	MSSQL Resolution Service Stack Overflow	+							
2	10.10.104.110	SysV /bin/login Overflow	+							
1	10.10.104.111	HTTP 1.1 Chunked Encoding Transfer	45908	10.1.1.223	80	Medium	ips-4255	<n/a>	09:14:30 AM	Fri, Jul 01, 2005
1	10.10.104.112	Long WebDAV Request	46071	10.1.1.223	80	High	ips-4255	<n/a>	09:14:34 AM	Fri, Jul 01, 2005
1	10.10.104.113	Long HTTP Request	3246	10.1.1.223	80	Medium	ips-4255	<n/a>	09:14:34 AM	Fri, Jul 01, 2005
1	10.10.104.114	Long HTTP Request	3247	10.1.1.223	80	Medium	ips-4255	<n/a>	09:14:35 AM	Fri, Jul 01, 2005
1	10.10.104.115	Long HTTP Request	3248	10.1.1.223	80	Medium	ips-4255	<n/a>	09:14:36 AM	Fri, Jul 01, 2005
1	10.10.104.116	Long HTTP Request	3249	10.1.1.223	80	Medium	ips-4255	<n/a>	09:14:37 AM	Fri, Jul 01, 2005
1	10.10.104.117	Apache/mod_ssl Worm Buffer Overflow	33025	10.1.1.223	443	High	ips-4255	<n/a>	09:14:43 AM	Fri, Jul 01, 2005
1	10.10.104.118	RPC WinNuke	1244	10.1.1.223	135	High	ips-4255	<n/a>	09:14:43 AM	Fri, Jul 01, 2005
1	10.10.104.119	RPC WinNuke	33103	10.1.1.223	135	High	ips-4255	<n/a>	09:14:44 AM	Fri, Jul 01, 2005
2	10.10.105.100	Finger root	32777	10.1.1.223	79	Medium	ips-4255	<n/a>	+	
2	10.10.105.101	Finger root shell	32777	10.1.1.223	79	High	ips-4255	<n/a>	+	
2	10.10.105.101	File access in finger	32773	10.1.1.223	79	Medium	ips-4255	<n/a>	+	
2	10.10.105.102	Perl fingerd Command Exec	32778	10.1.1.223	79	High	ips-4255	<n/a>	+	
2	10.10.105.103	Finger Redirect	1026	10.1.1.223	79	Medium	ips-4255	<n/a>	+	
4	10.10.106.100	Solaris in.fingerd Information Leak	1026	10.1.1.223	79	Low	ips-4255	+		
3	10.10.106.101	FTP PASS Suspicious Length	39182	10.1.1.223	21	High	ips-4255	<n/a>	+	
6	10.10.106.101	FTP realpath Buffer Overflow	39189	10.1.1.223	21	High	ips-4255	+		
3	10.10.106.102	FTP Improper Address Specified	32806	10.1.1.223	21	Medium	ips-4255	<n/a>	+	
3	10.10.106.103	FTP Improper Port Specified	32806	10.1.1.223	21	Medium	ips-4255	<n/a>	+	
3	10.10.106.104	Ftp Privileged Login	3497	10.1.1.223	21	Low	ips-4255	<n/a>	+	
3	10.10.106.104	FTP SYST Command Attempt	36553	10.1.1.223	21	Info	ips-4255	<n/a>	+	
6	10.10.107.100	WUJ-FTPD Heap Corruption	36553	10.1.1.223	21	High	ips-4255	+		
4	10.10.107.101	HTTP cgi HylaFAX Faxsurvey	3334	10.1.1.223	80	High	ips-4255	<n/a>	+	
4	10.10.107.101	Unix Password File Access Attempt	3334	10.1.1.223	80	Medium	ips-4255	<n/a>	+	
3	10.10.107.101	Dot Dot Slash in HTTP Arguments	4948	10.1.1.223	80	Low	ips-4255	<n/a>	+	
4	10.10.107.101	WWW TEST-CGI Attack	4948	10.1.1.223	80	Low	ips-4255	<n/a>	+	

Event 1 of 2

Details

Sig Name: MSSQL Resolution Service Stack Overflow  
 Sig ID: 4703  
 Severity: High  
 Risk Rating: 85  
 Sig Version: S161  
 Attack Type: <n/a>  
 OS Family: <n/a>  
 OS: <n/a>  
 Protocol: udp  
 Protocol Details: <n/a>  
 Service: <n/a>

Attacker Address: 10.10.104.104  
 Attacker Port: <n/a>  
 Attacker Loc: OUT  
 Attacker Unreliable: False  
 Victim Address: 10.1.1.223  
 Victim Port: <n/a>  
 Victim Loc: OUT

Local Date: Fri, Jul 01, 2005  
 Local Time: 09:14:33 AM  
 Time Offset: 60  
 Time Zone: GMT+01:00

Response

IP Logs: False  
 Trig Pkt Created: False  
 Connection Block Requested: False  
 Host Block Requested: False  
 Deny Packet: False  
 Deny Flow: False  
 Deny Attacker: False  
 Would've Denied Packet: False  
 Would've Denied Flow: False  
 Would've Denied Attacker: False  
 TCP Reset: False  
 Resolved: False

Reporting Chain

Sensor Name: ips-4255  
 Orig App Name: sensorApp  
 Orig App Addr: 10.1.10.81  
 Orig SecMon Addr: <n/a>  
 Original SecMon ID: 0  
 Downstream SecMon ID: 0

Prev Next



# Life Cycle Security

- Business Requirement
- Design Arsitektur
- Analisa resiko dan kebutuhan
- Pengembangan Policy
- Prosedur dan perencanaan
- Testing dan implementasi

# POLICY FIREWALL

# Policy FIREWALL

- *Computer Physical*, membuat aturan baku tentang akses computer dan jaringan secara langsung misalnya kabel, server yang diletakkan diruangan khusus, hub, router, dan lain-lain
- Koneksi kabel yang dilindungi, kabel UTP, STP atau coax dari gangguan sabotase langsung.
- Membuat *password* BIOS, LILO boots, Screen saver

- *Automatic Lock*, aturan yang memungkinkan penguncian sistem secara otomatis, jika terjadi misalkan penulisan password yang salah sebanyak tiga kali.
- *Check Log administrasi* secara priodik melakukan checking semua aktivitas sistem computer
- *Closed Port / Services / Daemon*, menutup port-port atau layanan-layanan yang tidak penting atau tidak digunakan
- Ganti password secara berkala (admin & user) dan dokumentasikan

- *New accounts*, membatasi user baru dengan quota, memory dan akses beserta hak yang dimilikinya
- *Checking Files*, melakukan pemeriksaan secara intersif file atau software yang didapatkan dari luar sistem atau dari download di Internet
- *Remote account*, melakukan checking misalnya remote account yang telah kadaluarsa
- *User id dan Group id*, menerapkan kelompok-kelompok berdasarkan user dan kelompok agar mudah dimaintenance
- *Account*, apakah sebuah account dapat digunakan bersama, disaat accountnya ditolak apa yang harus dilakukan oleh user.

- *Root Security*, sistem administrasi dengan menggunakan remote sistem harus melalui jaringan yang aman, misalnya VPN, SSL, atau SSH.
- *Remote User*, disaat akan terkoneksi ke jaringan apa yang mesti dilakukan oleh user, bagaimana jika user akan terkoneksi ke jaringan local dari jaringan public.
- *Backup*, membuat aturan dengan menerapkan kegiatan backup secara berkala atau menggunakan sistem cadangan.

- *Patch terbaru*, melakukan updating patch yang disediakan vendor perangkat lunaknya untuk menutupi lubang-lubang keamanan
- Sosialisasi dan kemudahan prosedur
- *Team hotline*, membuat sebuah tim penanganan jika terjadi serangan dan kerusakan dan menyiapkan nomer khusus online setiap saat.

- Jika memungkinkan, alihkan atau gandakan log dari suatu server ke mesin lainnya. Tujuannya, agar menyulitkan hacker menghapus log setelah melancarkan aksinya, ataupun jika berhasil, kita masih mempunyai backup log-nya.
- Jangan lupa buat check list terhadap apa-apa yang perlu dilakukan dan juga buat catatan tentang apa-apa yang telah dilakukan terutama dilakukan jika terjadi anomaly sistem.

# Mengenal Jenis Serangan

- DOS & DDOS
- Spoofing
- TCP SYN attack
- Brute Force & Dictionary attack password

# Ancaman Internet

- E-mail
- HTTP
- FTP
- File Sharing
- Instance Messaging

# Password

- Jangan pernah menggunakan kata-kata umum yang ada dikamus
- Gunakan kombinasi huruf dan angka (besar dan kecil)
- Min 5 karakter
- Ganti secara berkala
- Jangan gunakan password tentang pribadi :  
TTL, nama pacar, nama ortu, alamat, dll
- Harus mudah diingat
- Don't trust any one...!! (paranoid)