

Keamanan Sistem dan Jaringan

Pertemuan ke-6



Pesantren Teknologi Informasi dan Komunikasi

Jln. Mandor Basar No. 54 RT 01/RW 01 Rangkapanjaya,
Pancoran Mas, Depok 16435 | Telp. (021) 77 88 66 91

Koordinat (-6.386680 S, 106.777305 E)

www.petik.or.id





Jalan Mandor Basar Nomor 54, RT.
01/001, Rangkapanjaya, Pancoran
Mas, Kota Depok 16435



www.petik.or.id



021 7788 6691



info@petik.or.id

Firewall (ufw)

ufw

- Singkatan dari uncomplicated firewall
- Merupakan antarmuka untuk iptables yang sederhana dan mudah digunakan
- Tool default untuk melakukan konfigurasi firewall di Ubuntu
- Pada Ubuntu server 20.04, ufw secara default akan diinstall ketika proses instalasi tetapi dalam status disable

ufw

- Nama paket: ufw
- Nama service: ufw
- Konfigurasi: - File /etc/default/ufw
- Direktori /etc/ufw/
- File log: /var/log/ufw.log

Sintaks Perintah ufw

- `ufw [--dry-run] enable|disable|reload`
- `ufw [--dry-run] default allow|deny|reject [incoming|outgoing|routed]`
- `ufw [--dry-run] logging on|off|LEVEL`
- `ufw [--dry-run] reset`
- `ufw [--dry-run] status [verbose|numbered]`
- `ufw [--dry-run] show REPORT`

Sintaks Perintah ufw

- **ufw** [**--dry-run**] [**delete**] [**insert** NUM] [**prepend**] **allow|deny|reject|limit** [**in|out**] [**log|log-all**] [**PORT[/PROTOCOL]** | **APPNAME**] [**comment** COMMENT]
- **ufw** [**--dry-run**] [**rule**] [**delete**] [**insert** NUM] [**prepend**] **allow|deny|reject|limit** [**in|out** [**on** INTERFACE]] [**log|log-all**] [**proto** PROTOCOL] [**from** ADDRESS [**port** PORT | **app** APPNAME]] [**to** ADDRESS [**port** PORT | **app** APPNAME]] [**comment** COMMENT]

Sintaks Perintah ufw

- **ufw [--dry-run] route [delete] [insert NUM] [prepend] allow|deny|reject|limit [in|out on INTERFACE] [log|log-all] [proto PROTOCOL] [from ADDRESS [port PORT | app APPNAME]] [to ADDRESS [port PORT | app APPNAME]] [comment COMMENT]**
- **ufw [--dry-run] delete NUM**
- **ufw [--dry-run] app list|info|default|update**

Sintaks Perintah ufw

OPTIONS	
- -version	menampilkan versi program
-h, - -help	menampilkan bantuan
- -dry-run	tidak menyimpan perubahan tapi hanya menampilkan perubahannya saja.
enable	memuat ulang firewall dan mengaktifkan firewall saat boot.
disable	tidak memuat firewall dan menonaktifkan firewall saat boot.
reload	memuat ulang firewall.

Sintaks Perintah ufw

default allow|deny|reject DIRECTION

mengubah default policy untuk lalulintas yang menuju DIRECTION, dimana DIRECTION salah satu dari incoming, outgoing atau routed.

logging on|off|LEVEL

mengubah logging. Menentukan LEVEL akan mengaktifkan logging untuk LEVEL tertentu. Level log default adalah 'low'. LEVEL bisa berupa 'off', 'low', 'medium', 'high' dan 'full'.

Sintaks Perintah ufw

reset	menonaktifkan dan me-reset firewall ke default instalasi. Bisa juga memberikan opsi --force untuk melakukan reset tanpa konfirmasi.
status	menampilkan status firewall dan aturan yang dikelola ufw. Gunakan status verbose untuk menampilkan informasi tambahan. Gunakan status numbered untuk menampilkan nomor aturan.
show REPORT	
	menampilkan informasi tentang firewall yang berjalan.

Sintaks Perintah ufw

allow ARGS	menambahkan aturan allow.
deny ARGS	menambahkan aturan deny.
reject ARGS	menambahkan aturan reject.
limit ARGS	menambahkan aturan limit.
delete RULE NUM	
	menghapus aturan.
insert NUM RULE	
	menyisipkan RULE sebagai aturan nomor NUM
prepend RULE	
	memindahkan RULE ke aturan paling atas.

Contoh Penggunaan ufw

- Melihat status ufw
`$ sudo ufw status`
- Melihat status ufw lebih rinci
`$ sudo ufw status verbose`
- Melihat status dengan nomor aturan
`$ sudo ufw status numbered`


Contoh Penggunaan ufw

- Mengaktifkan ufw
`$ sudo ufw enable`
- Menonaktifkan ufw
`$ sudo ufw disable`
- Memuat ulang ufw
`$ sudo ufw reload`

Contoh Penggunaan ufw

- Mengubah default policy untuk incoming traffic
`$ sudo ufw default allow incoming`
`$ sudo ufw default deny incoming`
- Mengubah default policy untuk outgoing traffic
`$ sudo ufw default allow outgoing`
`$ sudo ufw default deny outgoing`
- Mengubah default policy untuk routed traffic
`$ sudo ufw default allow routed`
`$ sudo ufw default deny routed`

Contoh Penggunaan ufw

- Menolak seluruh akses ke port 53
\$ sudo ufw deny 53
- Menolak seluruh akses ke tcp port 80 
\$ sudo ufw deny 80/tcp
- Membolehkan seluruh akses ke port 22
\$ sudo ufw allow 22
- Membolehkan seluruh akses ke udp port 514
\$ sudo ufw allow 514/udp

Contoh Penggunaan ufw

- Membolehkan seluruh akses dari jaringan RFC1918 ke komputer ini

```
$ sudo ufw allow from 10.0.0.0/8
```

```
$ sudo ufw allow from 172.16.0.0/12
```

```
$ sudo ufw allow from 192.168.0.0/16
```

- Menolak akses ke udp port 514 dari 192.168.100.10

```
$ sudo ufw deny proto udp from 192.168.100.10 to  
any port 514
```

Contoh Penggunaan ufw

- Menyisipkan rule

```
$ sudo ufw status numbered  
$ sudo ufw insert 2 allow 80
```

- Menghapus rule

```
$ sudo ufw status numbered  
$ sudo ufw delete allow 80  
atau  
$ sudo ufw delete 2
```

Contoh Penggunaan ufw

ufw mendukung integrasi aplikasi dengan membaca profil yang terletak di `/etc/ufw/applications.d`.

- Menampilkan daftar aplikasi yang dikenal oleh ufw

```
$ sudo ufw app list
```

- Menampilkan profile rinci suatu aplikasi

```
$ sudo ufw app info apache2
```

- Membolehkan akses ke web server apache

```
$ sudo ufw allow apache2
```



Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya,
Pancoran Mas, Kota Depok 16435



www.petik.or.id



021 7788 6691



info@petik.or.id