



Jaringan Terapan

Catatan Kuliah #10

Alauddin Maulana Hirzan, M. Kom

0607069401

Firewall



Firewall

Apa itu Firewall? #1

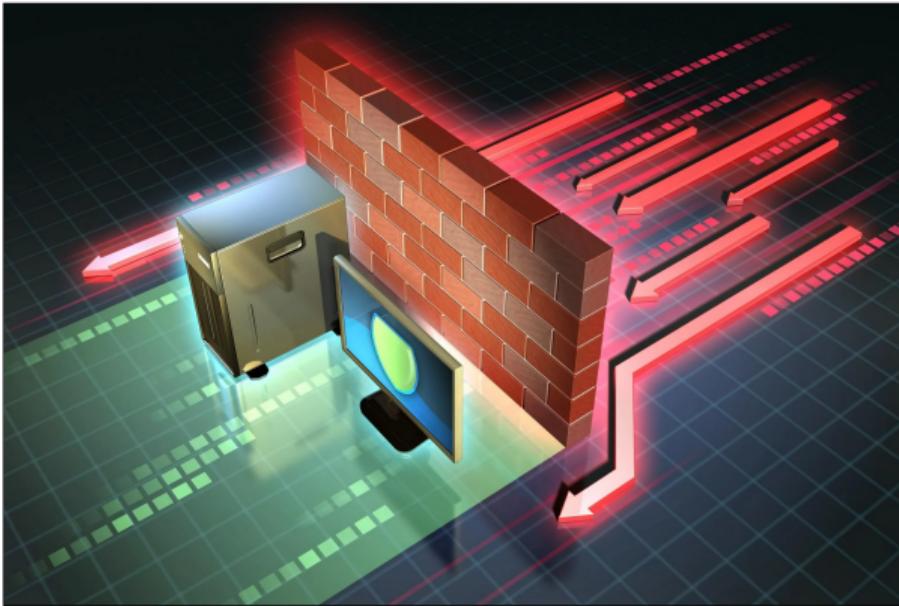
Menurut Norton:

Firewall adalah perangkat keamanan (perangkat keras atau perangkat lunak komputer) yang dapat membantu melindungi jaringan pengguna dengan menyaring lalu lintas dan memblokir orang luar untuk mendapatkan akses tidak sah ke data pribadi di komputer pengguna.

Firewall tidak hanya memblokir lalu lintas yang tidak diinginkan, tetapi juga dapat membantu memblokir perangkat lunak berbahaya agar tidak menginfeksi komputer Pengguna. Firewall dapat memberikan tingkat perlindungan yang berbeda.

Firewall

Apa itu Firewall? #2





Firewall

Cara Kerja Firewall? #1

Firewall bertindak sebagai penjaga gerbang. Dengan memonitor upaya untuk mendapatkan akses ke sistem operasi pengguna dan memblokir lalu lintas yang tidak diinginkan atau sumber yang tidak dikenal.

Firewall bertindak sebagai penghalang atau filter antara komputer pengguna dan jaringan lain seperti internet. Firewall akan memblokir lalu lintas jaringan masuk yang tidak diminta dan memvalidasi akses dengan menilai lalu lintas jaringan untuk segala sesuatu yang berbahaya seperti peretas dan malware.



Firewall

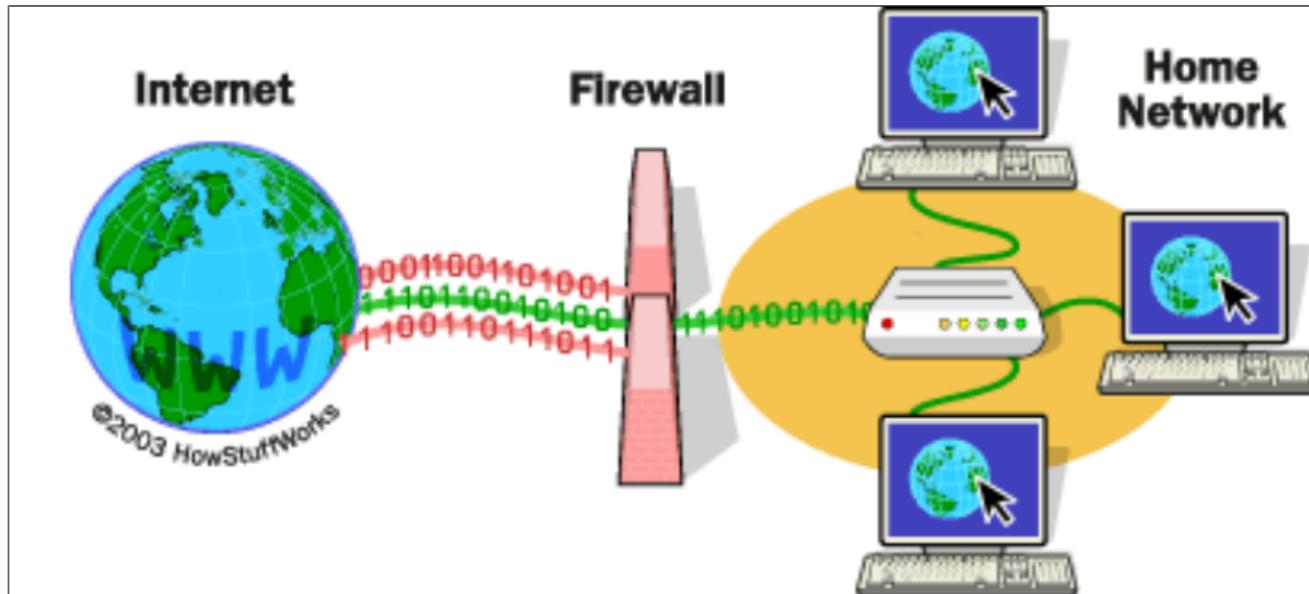
Cara Kerja Firewall? #2

Untuk memulai, sistem firewall menganalisis lalu lintas jaringan berdasarkan aturan. Firewall hanya menerima koneksi masuk yang telah dikonfigurasi untuk diterima. Ini dilakukan dengan mengizinkan atau memblokir paket data tertentu berdasarkan aturan keamanan yang telah ditetapkan sebelumnya.

Firewall bekerja seperti penjaga lalu lintas di titik masuk atau port komputer pengguna. Hanya sumber tepercaya, atau alamat IP, yang diizinkan masuk. Alamat IP penting karena mengidentifikasi komputer atau sumber.

Firewall

Cara Kerja Firewall? #3





Firewall

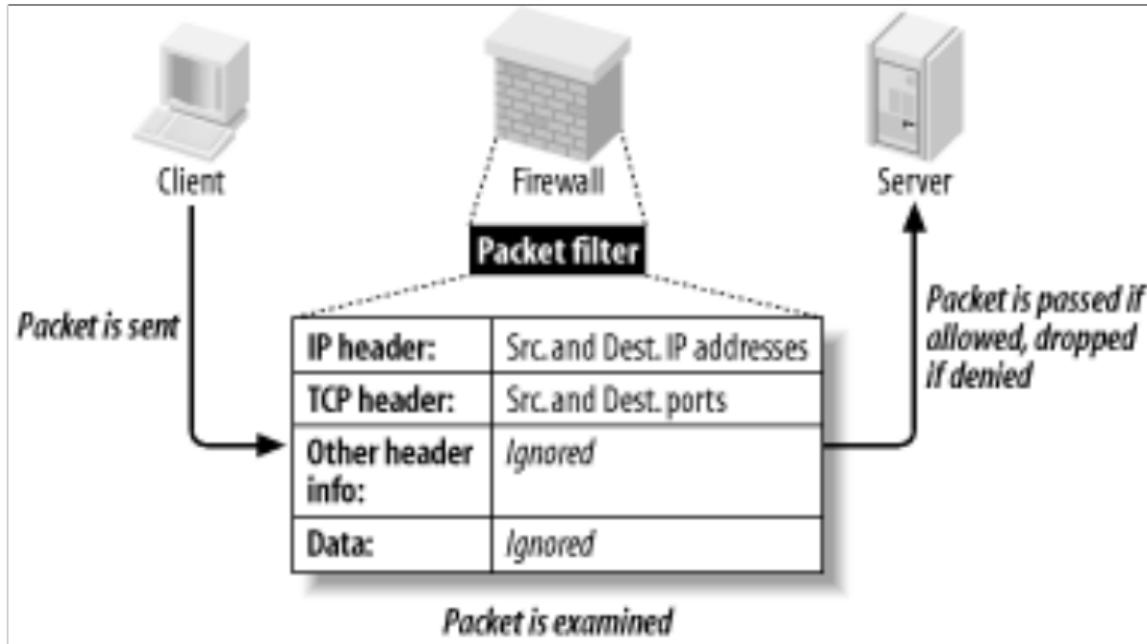
Packet-filtering firewalls #1

Firewall pemfilteran paket adalah program manajemen yang dapat memblokir protokol IP lalu lintas jaringan, alamat IP, dan nomor port. Jenis firewall ini adalah bentuk perlindungan paling dasar dan ditujukan untuk jaringan yang lebih kecil.

Tapi hati-hati. Meskipun firewall pemfilteran paket dapat membantu, mereka juga memiliki keterbatasan. Karena semua lalu lintas web diizinkan, firewall pemfilteran paket tidak memblokir serangan berbasis web. Jadi, pengguna memerlukan perlindungan tambahan untuk membedakan antara lalu lintas web yang ramah dan berbahaya.

Firewall

Packet-filtering firewalls #2





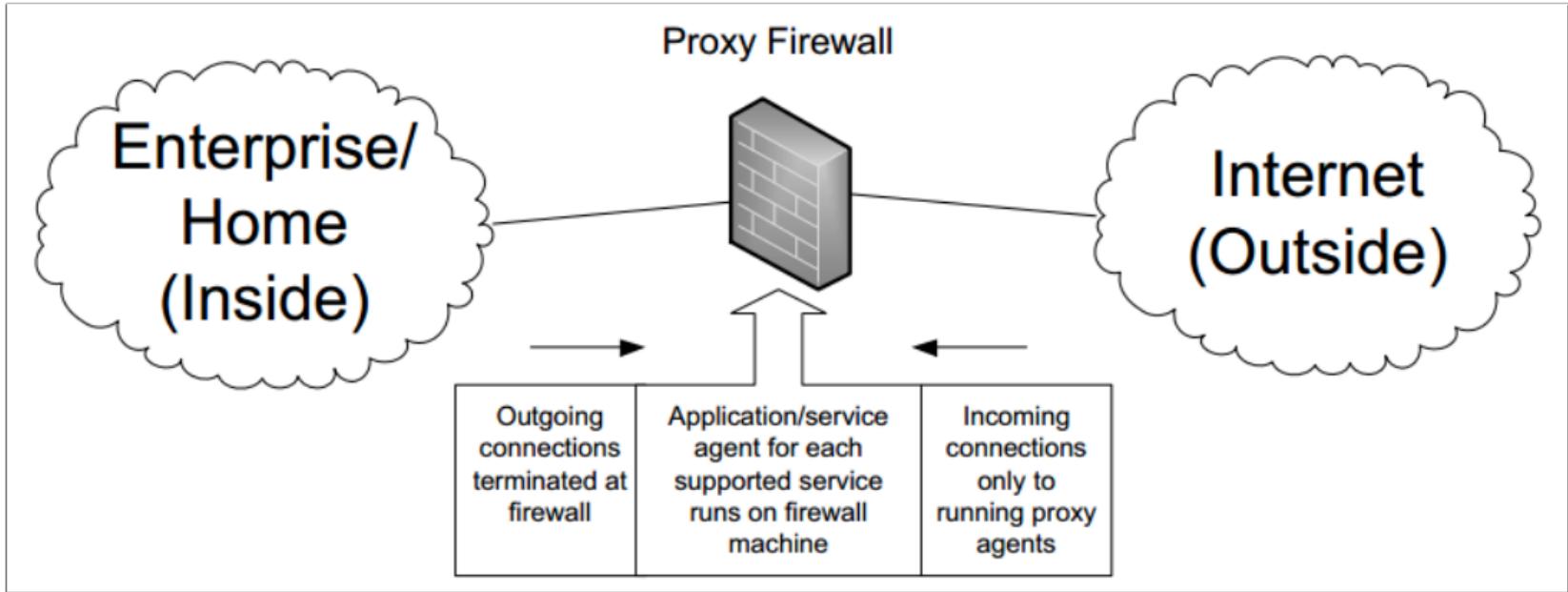
Firewall

Proxy service firewalls #1

Firewall layanan proxy adalah sistem yang dapat membantu melindungi keamanan jaringan pengguna dengan memfilter pesan pada lapisan aplikasi. Ini pada dasarnya berfungsi sebagai pintu gerbang atau perantara antara jaringan internal pengguna dan server luar di web. Juga dikenal sebagai firewall gateway, lebih aman dalam penggunaan teknologi inspeksi paket stateful dan mendalam untuk menganalisis lalu lintas masuk.

Firewall

Proxy service firewalls #2



Firewall

Stateful multi-layer inspection (SMLI) firewalls #1

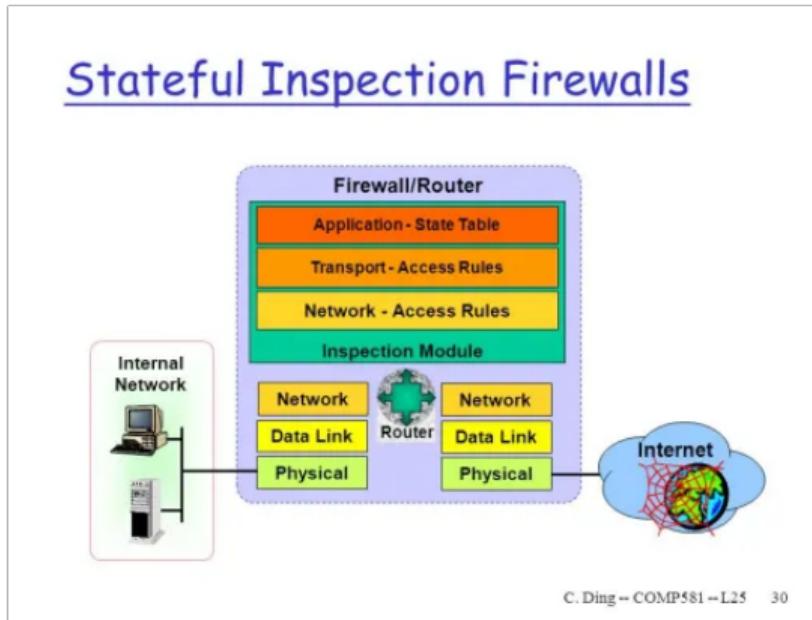
Firewall inspeksi multi-lapisan stateful memiliki kemampuan firewall standar dan melacak koneksi yang telah dibuat. Ini memfilter lalu lintas berdasarkan status, port, dan protokol, bersama dengan aturan dan konteks yang ditentukan administrator. Ini melibatkan penggunaan data dari koneksi sebelumnya dan paket dari koneksi yang sama.

Sebagian besar firewall mengandalkan inspeksi paket stateful untuk melacak semua lalu lintas internal. Firewall ini adalah langkah di atas packet-filtering dalam penggunaan pemantauan multi-layer.

Namun, masih tidak dapat membedakan antara lalu lintas web yang baik dan buruk

Firewall

Stateful multi-layer inspection (SMLI) firewalls #2





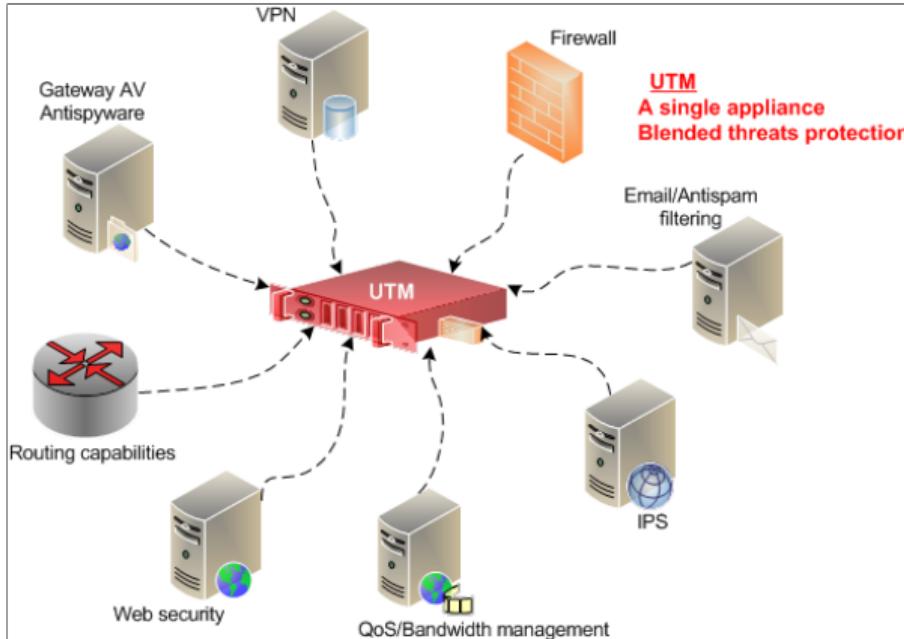
Firewall

Unified threat management (UTM) firewalls #1

Firewall manajemen ancaman terpadu adalah program yang menggabungkan fungsi firewall SMLI dengan pencegahan intrusi dan antivirus. Layanan tambahan seperti manajemen cloud dapat dimasukkan di bawah payung layanan UTM.

Firewall

Unified threat management (UTM) firewalls #2





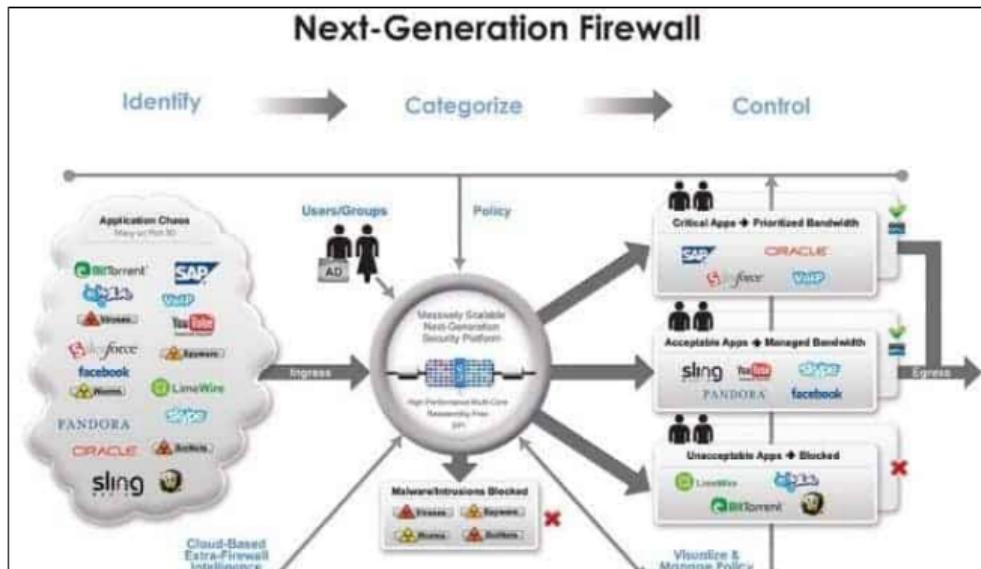
Firewall

Next-generation firewalls (NGFW) #1

Firewall generasi berikutnya lebih canggih daripada firewall packet-filtering dan stateful inspection. Mengapa? Mereka memiliki lebih banyak tingkat keamanan, melampaui penyaringan paket standar untuk memeriksa paket secara keseluruhan. Itu berarti memeriksa tidak hanya header paket, tetapi juga isi dan sumber paket. NGFW mampu memblokir ancaman keamanan yang lebih canggih dan berkembang seperti malware tingkat lanjut.

Firewall

Next-generation firewalls (NGFW) #2





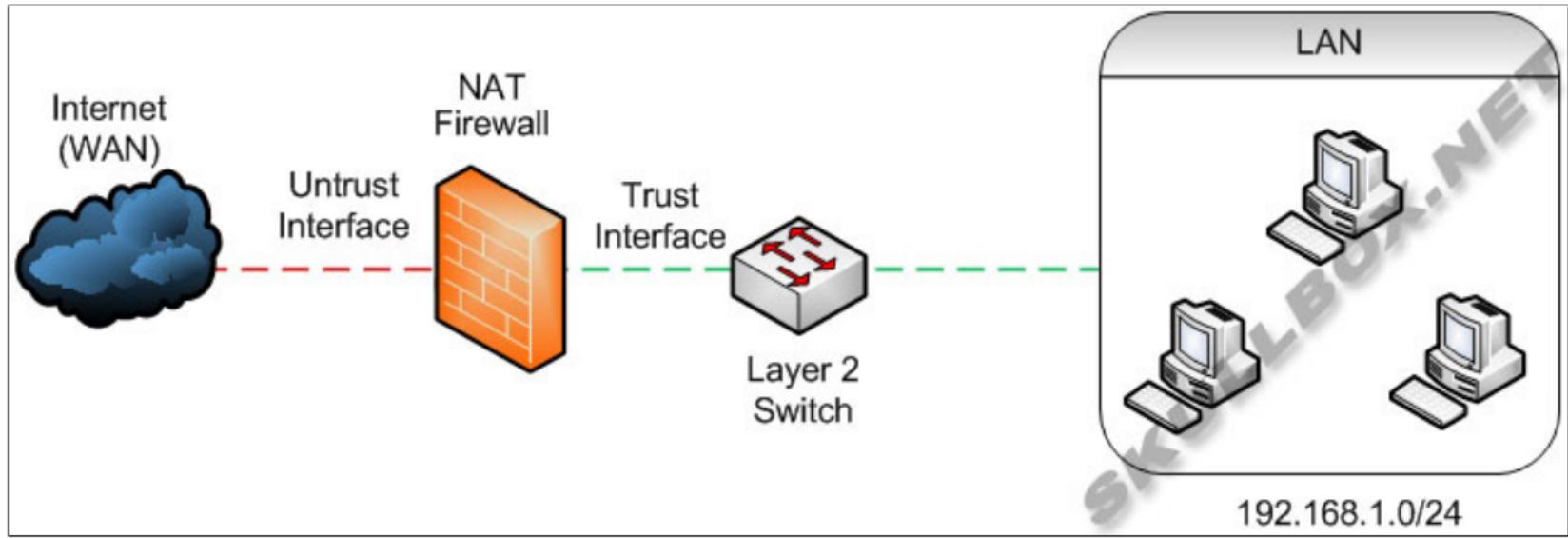
Firewall

Network address translation (NAT) firewalls #1

Firewall NAT mampu menilai lalu lintas internet dan memblokir komunikasi yang tidak diinginkan. Dengan kata lain, itu hanya menerima lalu lintas web masuk jika perangkat di jaringan pribadi pengguna memintanya.

Firewall

Network address translation (NAT) firewalls #2





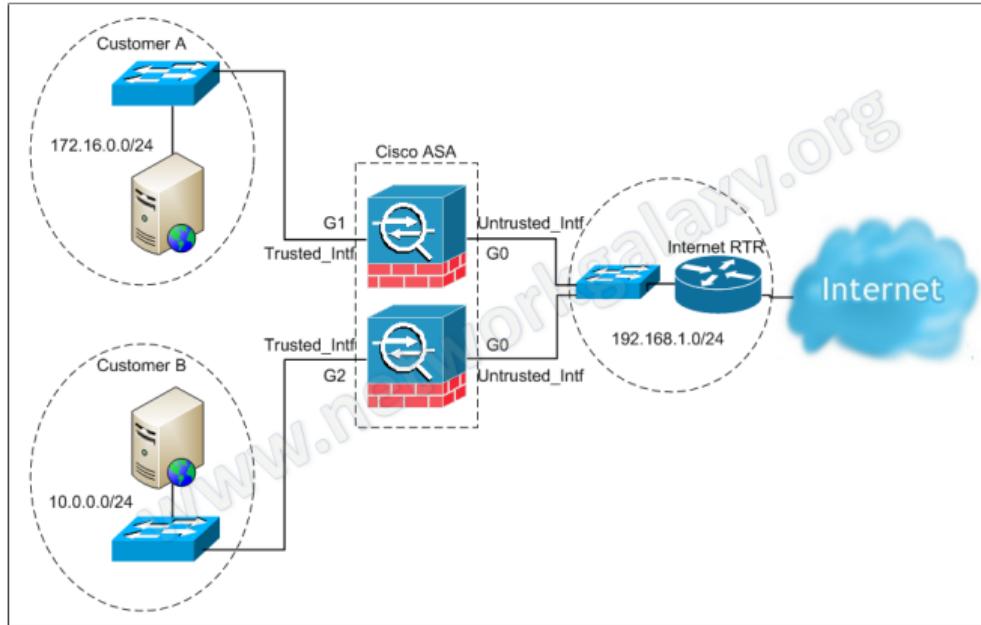
Firewall

Virtual firewalls #1

Firewall virtual adalah alat yang digunakan dalam sistem berbasis cloud, baik pribadi maupun publik. Jenis firewall ini digunakan untuk menilai dan mengelola lalu lintas internet melalui jaringan fisik dan virtual.

Firewall

Virtual firewalls #2





Firewall

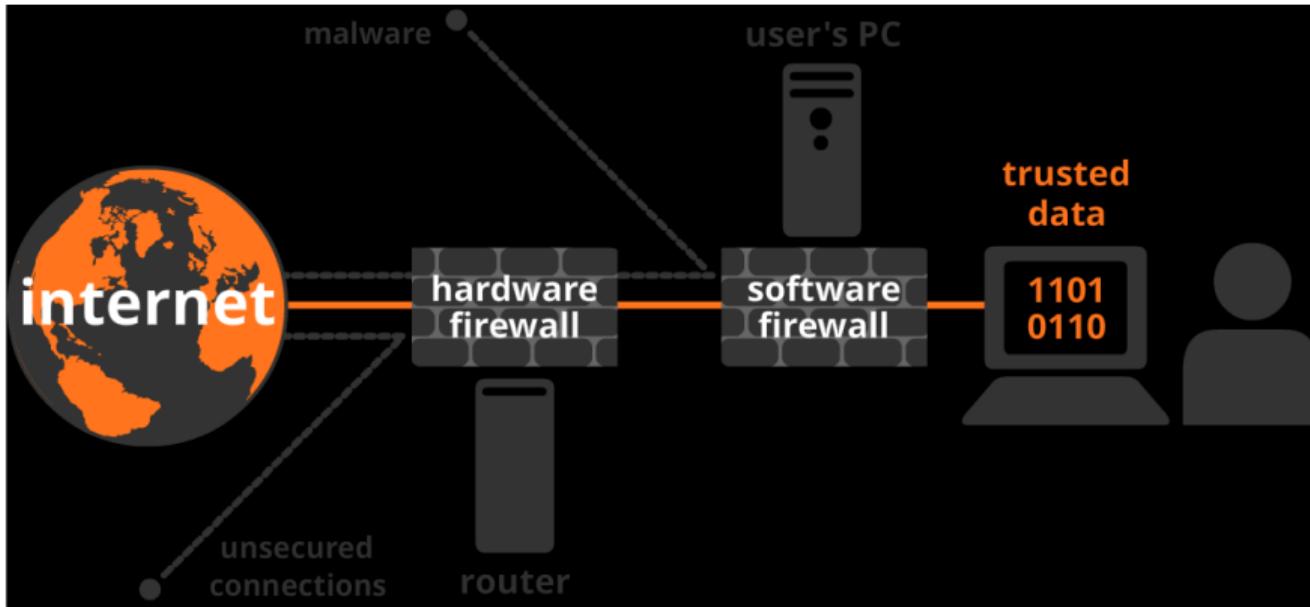
Host-based firewalls versus network-based firewalls #1

Firewall jaringan memfilter lalu lintas yang menuju dan dari internet ke jaringan area lokal (LAN) aman. Mereka biasanya digunakan oleh bisnis yang perlu melindungi jaringan besar komputer, server, dan karyawan.

Firewall berbasis host bekerja dengan cara yang sama tetapi disimpan secara lokal di satu komputer atau perangkat. Firewall berbasis host adalah aplikasi perangkat lunak atau rangkaian aplikasi yang memungkinkan lebih banyak penyesuaian.

Firewall

Host-based firewalls versus network-based firewalls #2





Firewall

Hardware vs Software Firewall

Firewall perangkat lunak adalah jenis perangkat lunak komputer khusus yang berjalan di komputer / server. Tujuan utamanya adalah untuk melindungi komputer/server Anda dari upaya luar untuk mengontrol atau mendapatkan akses dan bergantung pada pilihan firewall perangkat lunak Anda.

Firewall perangkat keras adalah peralatan fisik yang direncanakan untuk melakukan tugas firewall. Firewall perangkat keras dapat berupa komputer atau peralatan khusus yang berfungsi sebagai firewall.



Firewall

Pasaran Firewall #1

Banyak firewall yang bisa diunduh seperti

1. Hardware

- ▶ IPCop
- ▶ Cisco Firewall
- ▶ Mikrotik Router

2. Software

- ▶ Windows Firewall
- ▶ Comodo Firewall
- ▶ Uncomplicated FireWall (UFW - Linux)

Firewall

Pasaran Firewall #2





Firewall

Pasaran Firewall #3

```
root@vermillion:~# ufw allow ssh  
Rule added  
Rule added (v6)  
root@vermillion:~# ufw status  
Status: active  
  
To          Action    From  
--          -----  
22          ALLOW     Anywhere  
22 (v6)     ALLOW     Anywhere (v6)
```

THANK YOU

YOU