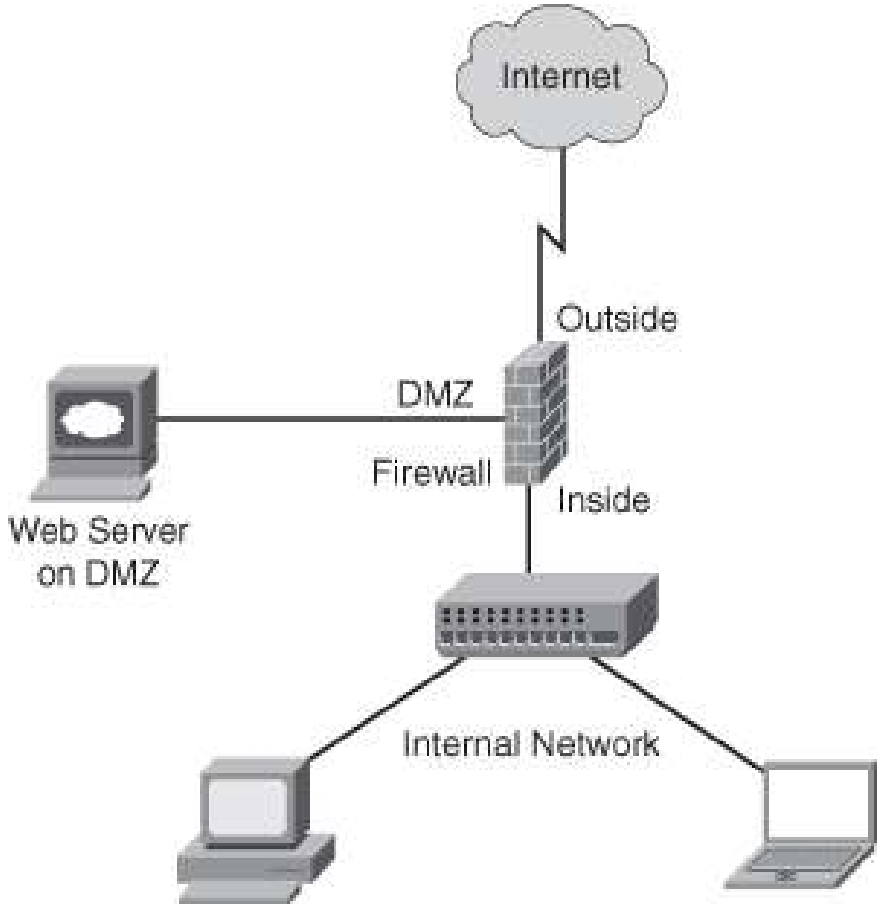
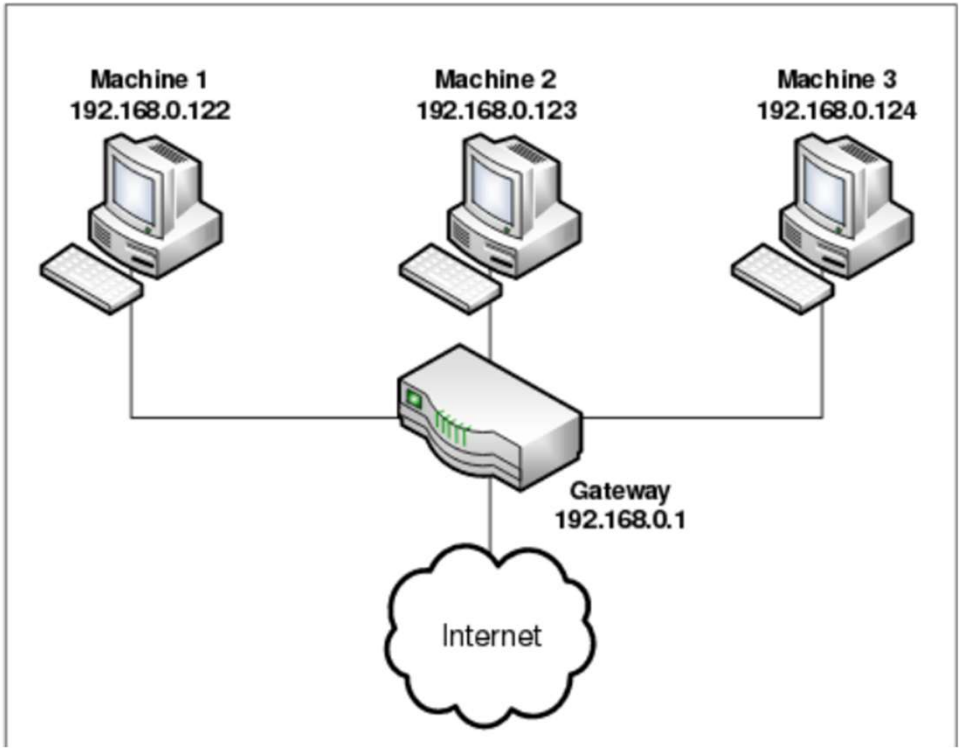
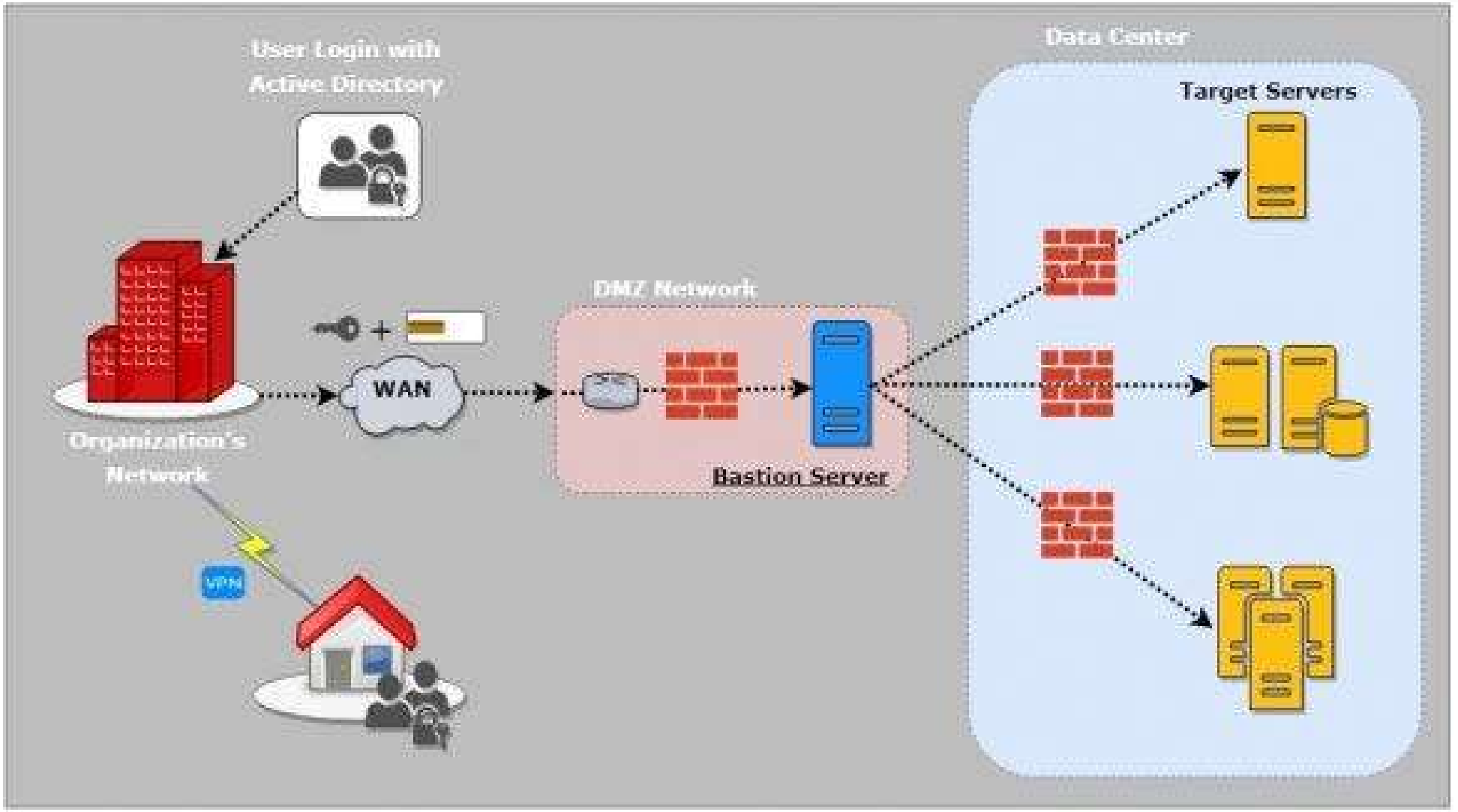
Computer Network Security


Internet
Outside
DMZ
Firewall
Inside
Web Server
on DMZ
Internal Network


Machine 1
192.168.0.122
Machine 2
192.168.0.123
Machine 3
192.168.0.124
Gateway
192.168.0.1
Internet


User Login with
Active Directory
Data Center
Target Servers
DMZ Network
WAN
Organization's
Network
Bastion Server
VPN

Daftar Istilah:

- ✓ Bastion Host : sistem/bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator.

  atau dapat di sebut bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen firewall atau bagian terluar sistem publik.

  Umumnya Bastion host akan menggunakan Sistem operasi yang dapat menangani semua kebutuhan (misal , Unix, linux, NT)

- ✓ Authentikasi : Adalah proses dalam rangka validasi user pada saat memasuki sistem. Nama dan password dari user dicek melalui proses yang mengecek langsung ke daftar mereka yang diberikan hak untuk memasuki sistem tersebut. Sifat mengetahui bahwa data yang diterima adalah sama dengan data yang dikirim dan bahwa pengirim yang mengklaim adalah benar-benar pengirim sebenarnya

Daftar Istilah:

- ✓ Proxy : Mekanisme dimana satu sistem menyediakan diri untuk sistem lain sebagai tanggapan atas permintaan untuk suatu protokol. Sistem Proxy digunakan dalam pengelolaan jaringan untuk mencegah implementasi tumpukan protokol sepenuhnya dalam perangkat yang sederhana, misalnya sebuah mode
- ✓ Router : Sistem yang digunakan untuk menghubungkan jaringan-jaringan. Perangkat yang berfungsi dalam komunikasi WAN atau menghubungkan dua network yang berbeda. Menempati layer 3 pada sistem layering OSI (network) sehingga memiliki kemampuan routing atau pengalamatan paket data baik secara static atau dinamik.

Daftar Istilah:

Sebuah komputer atau paket software yang dikhususkan untuk menangani koneksi antara dua atau lebih network yang terhubung melalui packet switching. Router bekerja dengan melihat alamat tujuan dan alamat asal dari paket data yang melewatinya dan memutuskan rute yang harus digunakan oleh paket data tersebut untuk sampai ke tujuan.

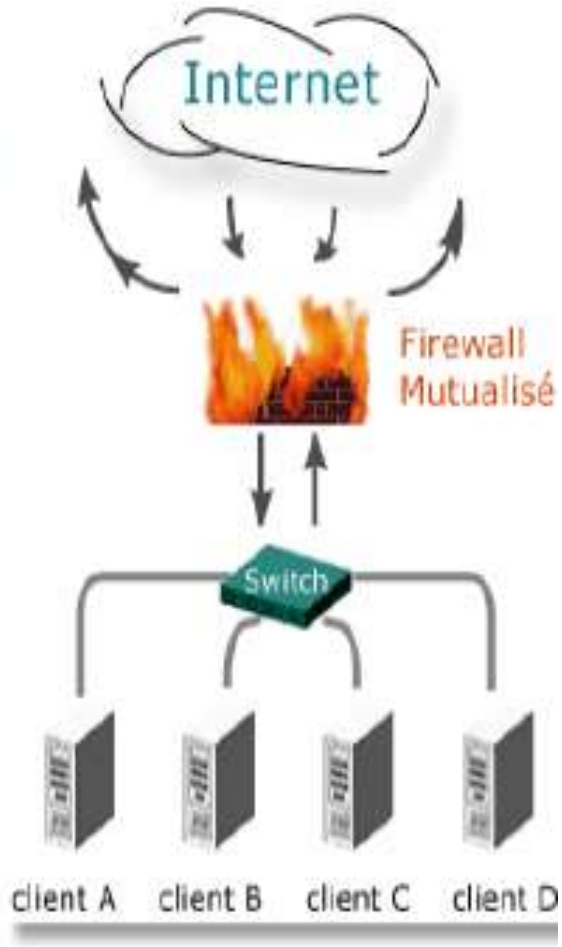
Definisi Firewall

Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini.

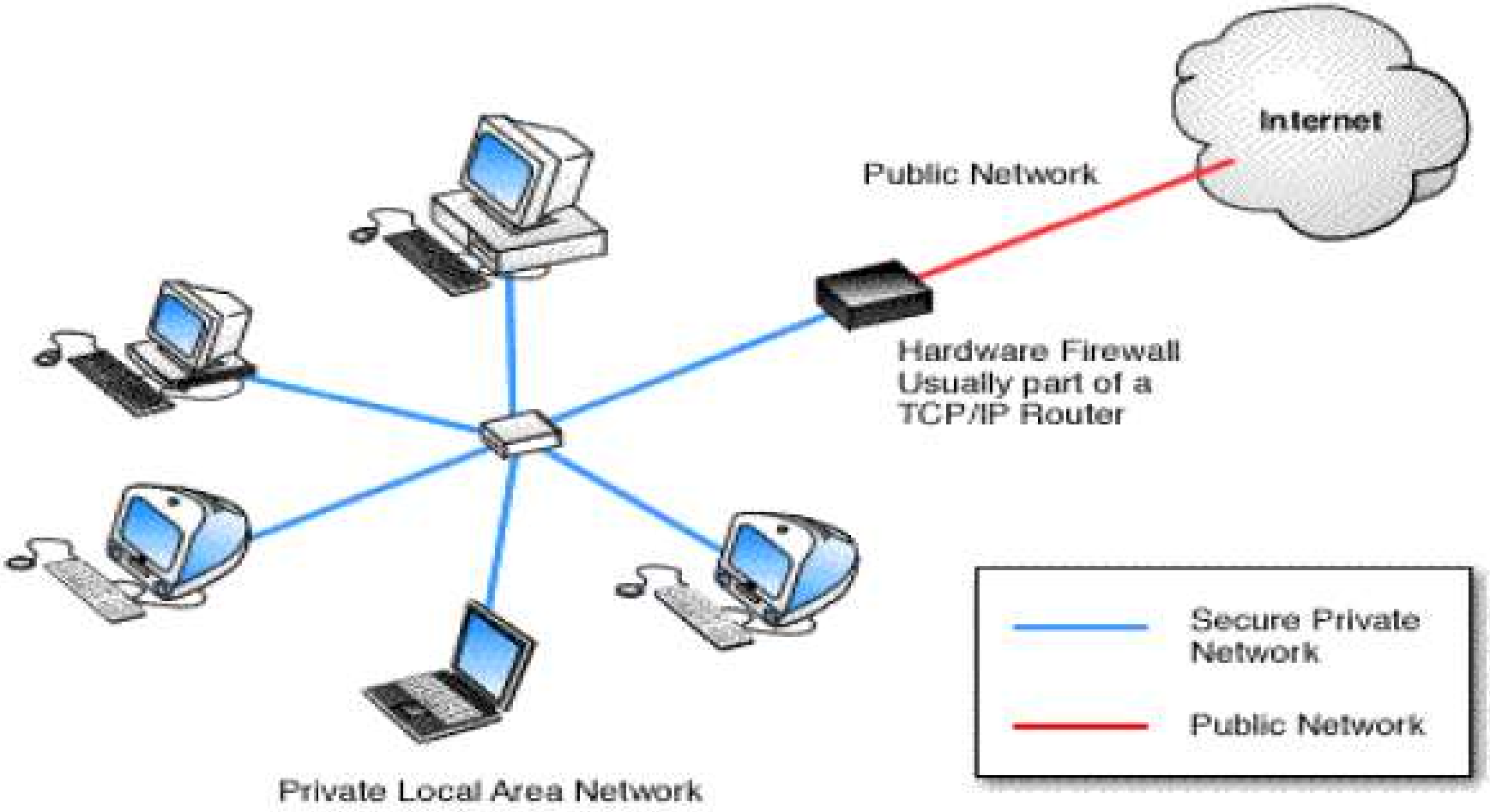
Tujuan adanya firewall adalah untuk menjaga (*prevent*) agar akses (ke dalam maupun ke luar) dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan.

Konfigurasi dari firewall bergantung kepada kebijaksanaan (*policy*) dari organisasi yang bersangkutan, yang dapat dibagi menjadi dua jenis:

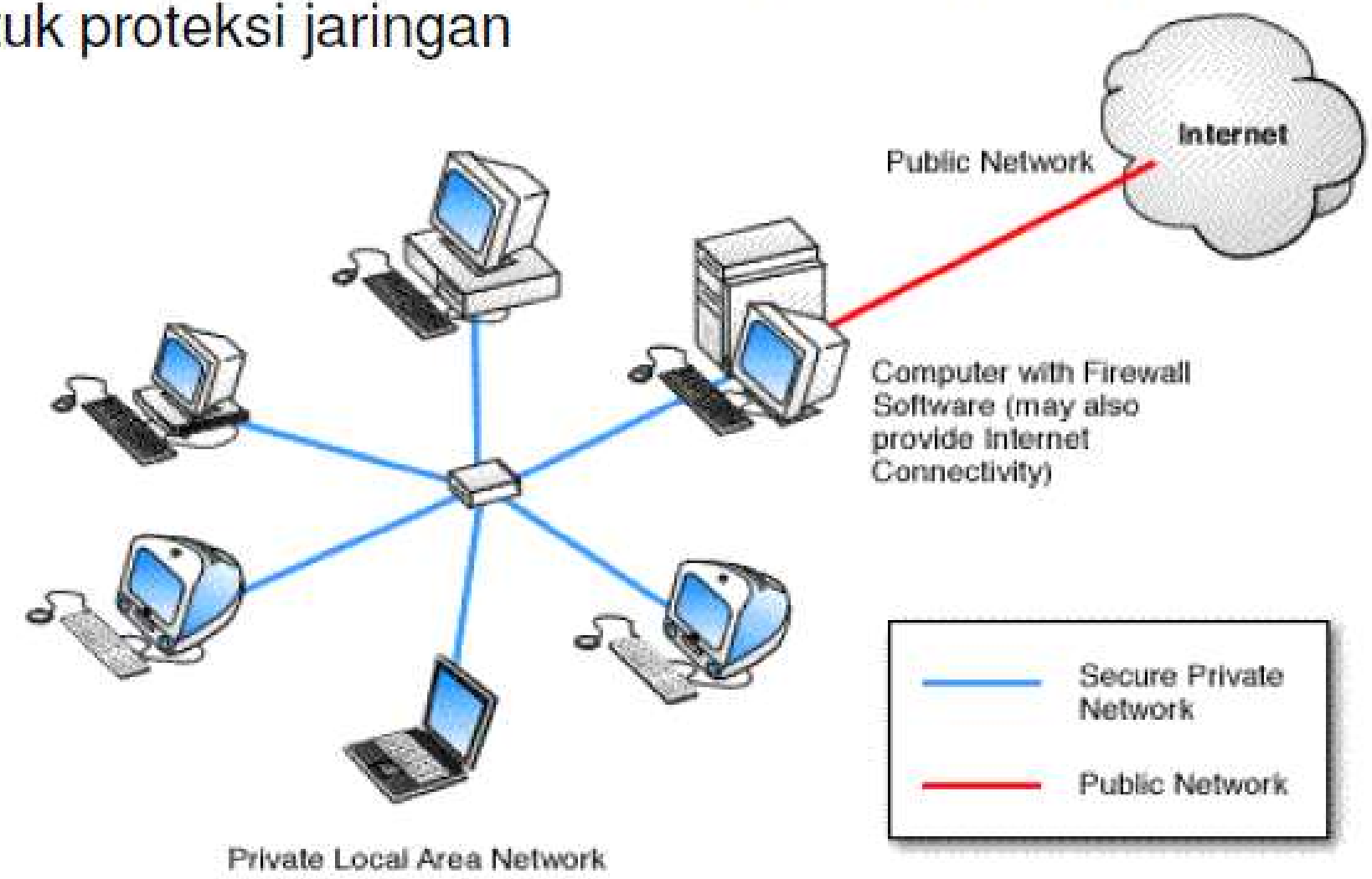
- *prohibitted*
- *permitted*



Gambar 1: Hardware Firewall: Hardware firewall menyediakan perlindungan ke Local Area Network



Gambar 2: Komputer dengan Firewall Software: Komputer yang menggunakan firewall software untuk proteksi jaringan



Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman.

Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya.

Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar.

Firewall dugunakan untuk mencegah serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, menjadi esensial."

Jadi firewall adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan.

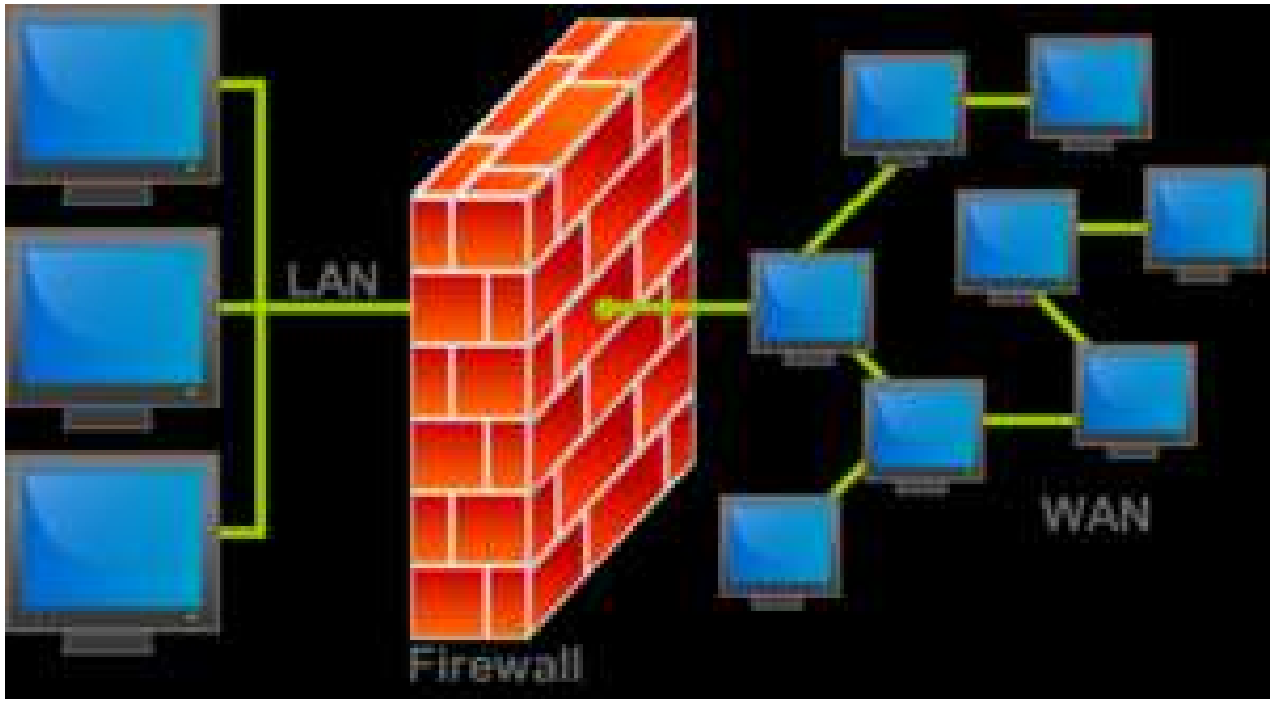
Paket data yang “baik” diperbolehkan untuk melewati jaringan dan paket data yang dianggap “jahat” tidak diperbolehkan melewati jaringan.

Firewall dapat berupa perangkat lunak atau perangkat keras yang ditanam yang dapat menfilter paket data.

Firewall dapat juga berupa suatu sikap yang ditanam dan diajarkan kepada staf IT suatu perusahaan untuk tidak membocorkan data perusahaan kepada perusahaan.

Ini untuk mencegah salah satu jenis hacking yaitu social enggeneering.

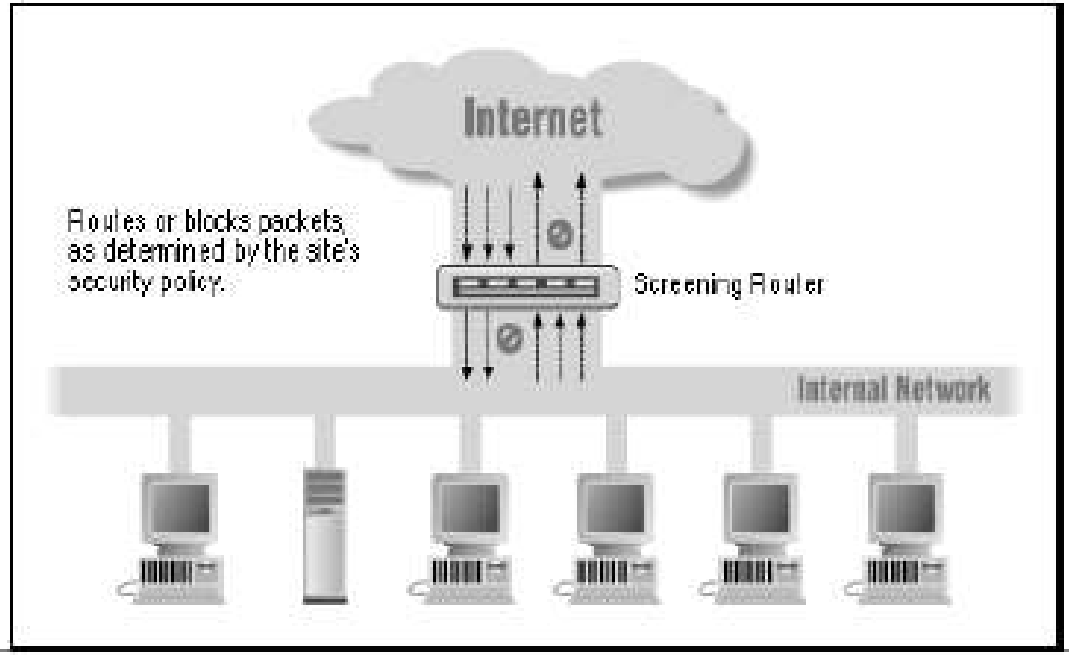
Ilustrasi Mengenai Firewall



Untuk menjaga fungsi komunikasi jaringan dalam lingkungan yang ber-firewall, dilakukan dua cara :

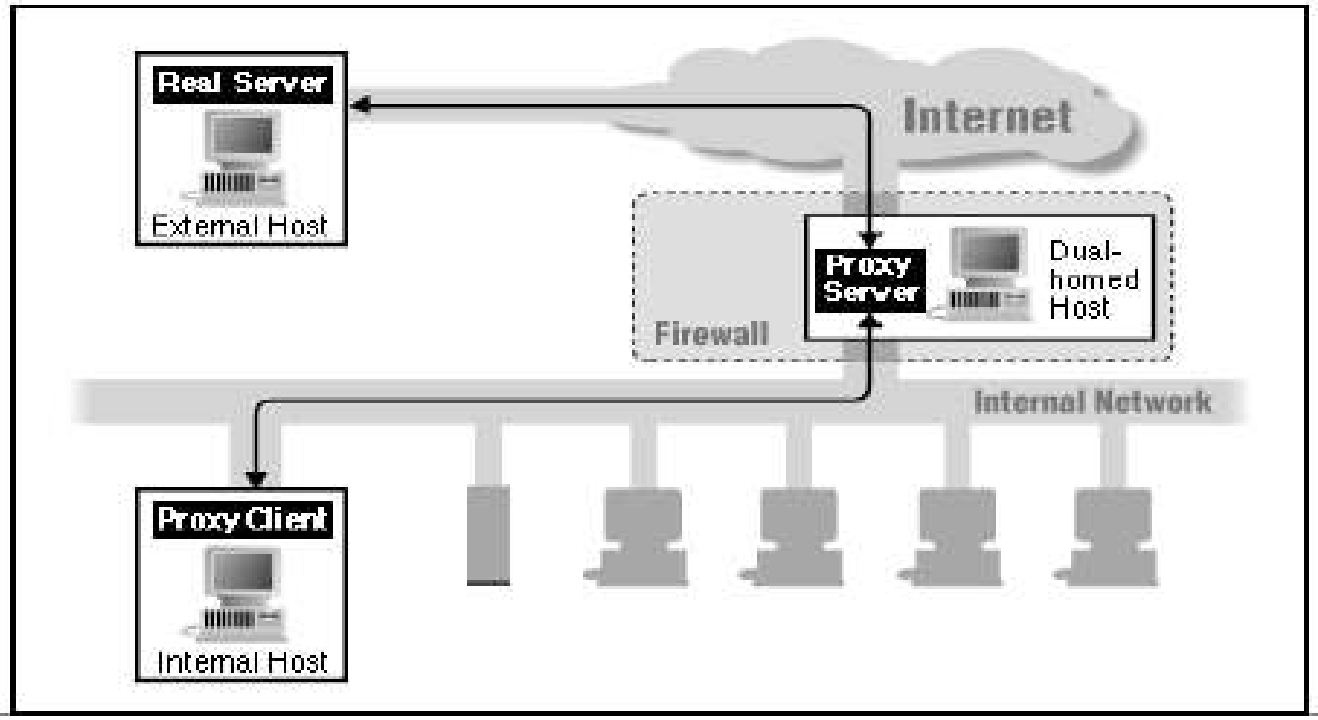
1. Packet filtering

mekanisme pengontrolan data yang diperbolehkan mengalir dari dan atau ke jaringan internal dengan menggunakan beberapa paremeter yang tercantum dalam header paket data: arah (inbound atau outbond), address asal dan tujuan, port asal dan tujuan serta jenis protokol transport. seperti telnet dan SMTP (Single Mail Transport Protocol).



2. **Menggunakan sistem proxy**, dimana setiap komunikasi yang terjadi antar kedua jaringan harus dilakukan melalui suatu operator, dalam hal ini proxy server.

Protokol FTP (File Transport Protocol) lebih efektif ditangani dengan sistem Proxy. Kebanyakan firewall menggunakan kombinasi kedua teknik ini (Packet filtering dan Proxy)



Beberapa perangkat lunak berbasis UNIX yang dapat digunakan untuk melakukan IP filtering antara lain:

- *ipfwadm*: merupakan standar dari sistem Linux yang dapat diaktifkan pada level kernel
- *ipchains*: versi baru dari Linux kernel packet filtering yang diharapkan dapat menggantikan fungsi ipfwadm

Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya.

Di sisi client sering kali dibutuhkan software tertentu agar dapat menggunakan proxy server ini, seperti misalnya dengan menggunakan SOCKS. Beberapa perangkat lunak berbasis UNIX untuk proxy antara lain:

- *Socks:* proxy server oleh NEC Network Systems Labs
- *Squid*: web proxy server

Fungsi Firewall

A. Mengontrol dan mengawasi paket data yang mengalir di jaringan.

   Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall.

   Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat.

   Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :

   1. Alamat IP dari komputer sumber
   2. Port TCP/UDP sumber dari sumber.
   3. Alamat IP dari komputer tujuan.
   4. Port TCP/UDP tujuan data pada komputer tujuan
   5. Informasi dari header yang disimpan dalam paket data.

B. Melakukan autentifikasi terhadap akses.

C. Applikasi proxy Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

D. Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini Memungkinkan membantu sebagai pendeteksian dini akan penjebolan jaringan.

KARAKTERISTIK FIREWALL

1. Seluruh hubungan/kegiatan dari dalam ke luar , harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan.
2. Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.
3. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan Operating system yang relatif aman

TEKNIK YANG DIGUNAKAN OLEH FIREWALL

1. Service control (kendali terhadap layanan) berdasarkan tipe-tipe layanan yang digunakan di Internet dan boleh diakses baik untuk kedalam ataupun keluar firewall.

   Biasanya firewall akan mencek no IP Address dan juga nomor port yang di gunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya.

   Bahkan bisa jadi software pada server itu sendiri , seperti layanan untuk web ataupun untuk mail.

2. Direction Conrol (kendali terhadap arah) berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.
3. User control (kendali terhadap pengguna) berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat menjalankan suatu servis,hal ini di karenakan user tersebut tidak di ijinkan untuk melewati firewall.

   Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap

4. Behavior Control (kendali terhadap perlakuan) berdasarkan seberapa banyak layanan itu telah digunakan. Misal, firewall dapat memfilter email untuk menanggulangi/mencegah spam.

KONFIGURASI FIREWALL

1. Screened Host FIrewall system (single-homed bastion)
   Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host*.

   Router ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang di ijinkan.

   Sedangkan untuk arus data (traffic) dari jaringan internal, hanya paket IP dari bastion host yang di ijinkan untuk keluar.

   Konfigurasi ini mendukung fleksibilitas dalam Akses internet secara langsung.

KONFIGURASI FIREWALL

Sebagai contoh apabila terdapat web server pada jaringan ini maka dapat di konfigurasikan agar web server dapat diakses langsung dari internet.

Bastion Host melakukan fungsi Authentikasi dan fungsi sebagai proxy.

Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada packet-filtering router atau application-level gateway secara terpisah.

2. Screened Host Firewall system (Dual-homed bastion)
   Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan.
   Kelebihannya adalah dengan adanya dua jalur yang meisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama,adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat diletakkan ditempat/segmenrt yang langsung berhubungan dengan internet
   Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (network interface Card) pada bastion Host.
3. Screened subnet firewall
   Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. kenapa? karena pada konfigurasi ini di gunakan 2 buah packet filtering router, 1 diantara internet dan bastion host, sedangkan 1 lagi diantara bastian host dan jaringan local konfigurasi ini membentuk subnet yang terisolasi.

Adapun kelebihannya adalah :

- Terdapat 3 lapisan/tingkat pertahanan terhadap penyusup/intruder .
- Router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible)
- Jaringan lokal tidak dapat mengkonstuksi routing langsung ke internet, atau dengan kata lain , Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).

LANGKAH-LANGKAH MEMBANGUN FIREWALL

1. Mengidenftifikasi bentuk jaringan yang dimiliki
   Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang di gunakan serta protocol jaringan, akan memudahkan dalam mendesain sebuah firewall

2. Menentukan Policy atau kebijakan
   Penentuan Kebijakan atau Policy merupakan hal yang harus di lakukan, baik atau buruknya sebuah firewall yang di bangun sangat di tentukan oleh policy/kebijakan yang di terapkan.

   Diantaranya:

   a. Menentukan apa saja yang perlu di layani. Artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat
   b. Menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut
   c. Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan

LANGKAH-LANGKAH MEMBANGUN FIREWALL

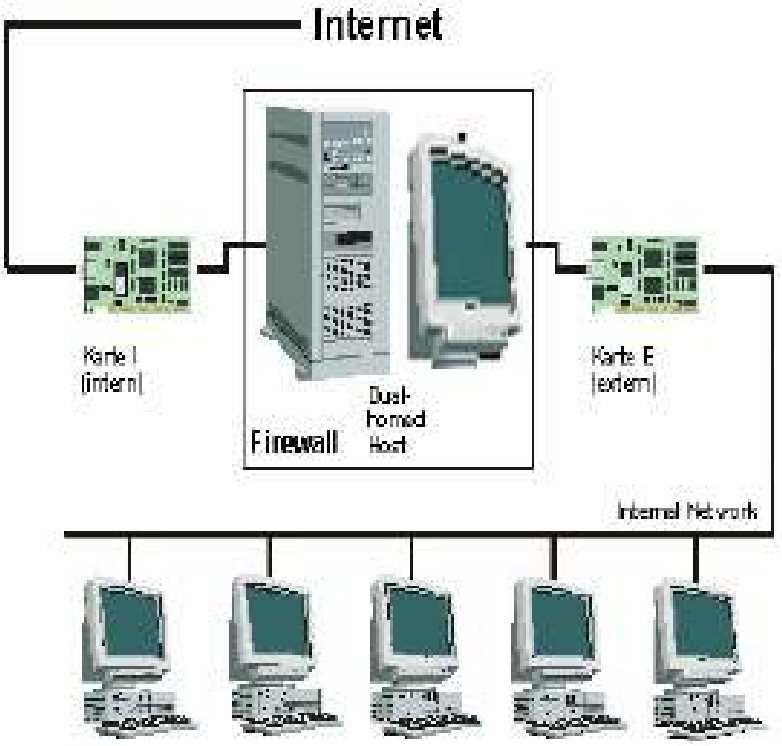
d. Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
e. Menerapkankan semua policy atau kebijakan tersebut

3. Menyiapkan Software atau Hardware yang akan digunakan Baik itu operating system yang mendukung atau software-software khusus pendukung firewall seperti ipchains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.
4. Melakukan test konfigurasi
   Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool tool yang biasa dilakukan untuk mengaudit seperti nmap.

Arsitektur dasar Firewall

Ada 3 macam arsitektur dasar firewall, yaitu :

1. **Arsitektur dengan dual-homed host (*dual homed gateway/DHG*)**

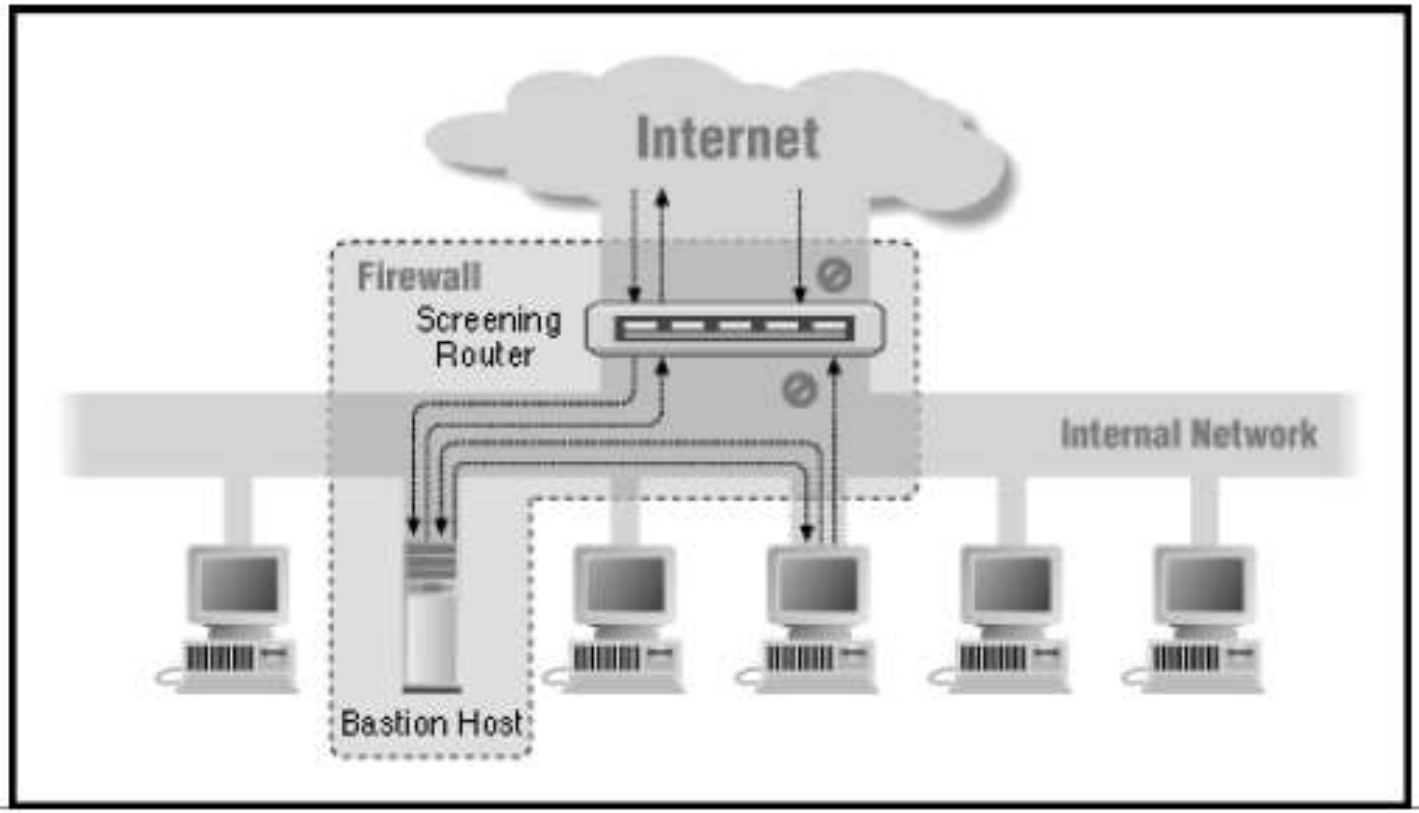


Menggunakan sebuah komputer dengan (minimal) dua NIC. Interface pertama dihubungkan ke jaringan internal dan yang lainnya dengan internet.

Dual homed host-nya sendiri berfungsi sebagai *bastion host* (Suatu sistem komputer yang harus memiliki keamanan yang tinggi, karena biasanya peka terhadap serangan jaringan, biasanya terhubung langsung ke internet dan menjadi titik utama komunikasi dengan jaringan internal.)

2. Screened-host (screened host gateway/SHG)

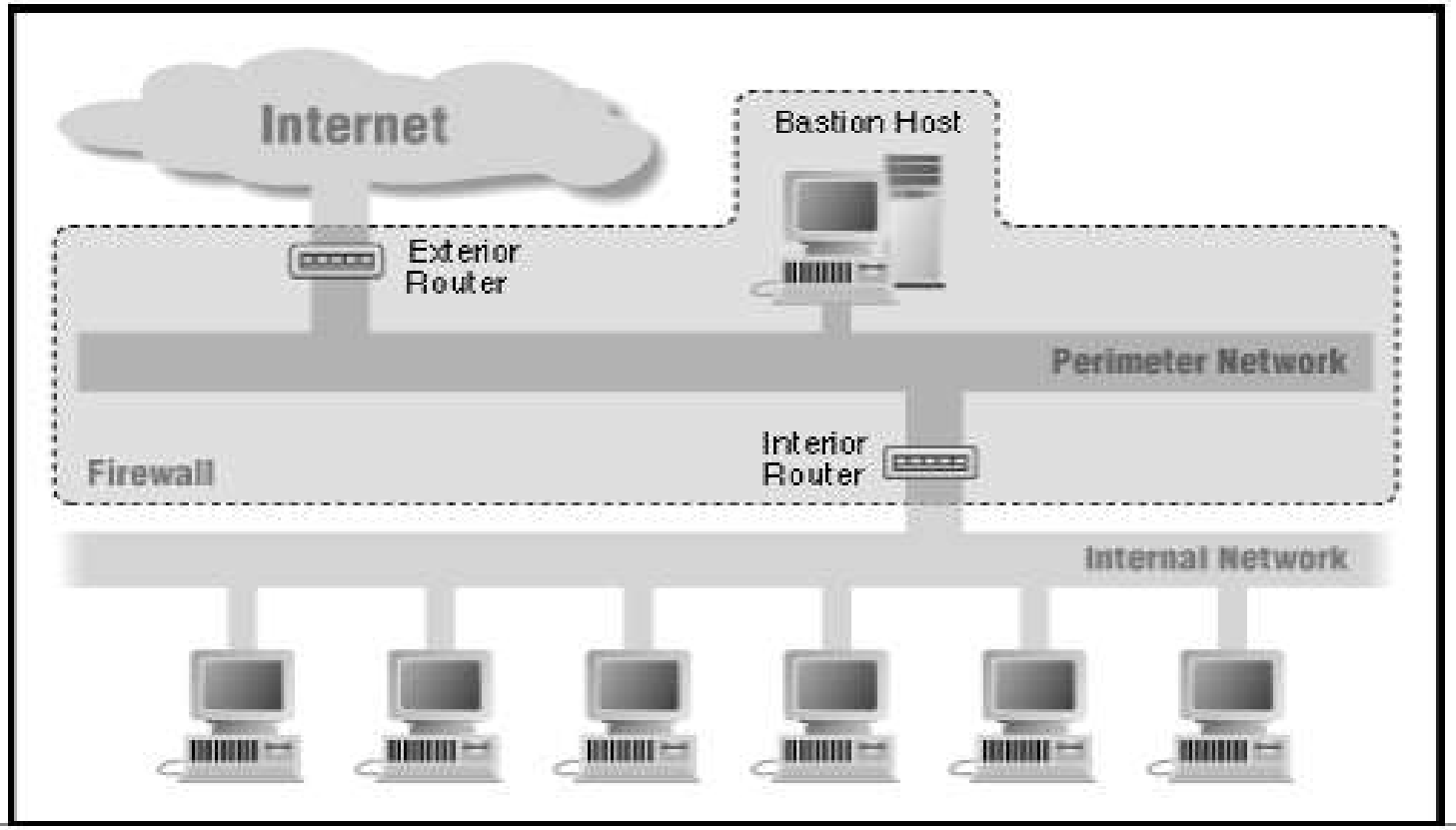
fungsi firewall dilakukan oleh sebuah screening-router dan bastian host. Router ini akan menolak semua trafik kecuali yang ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan.

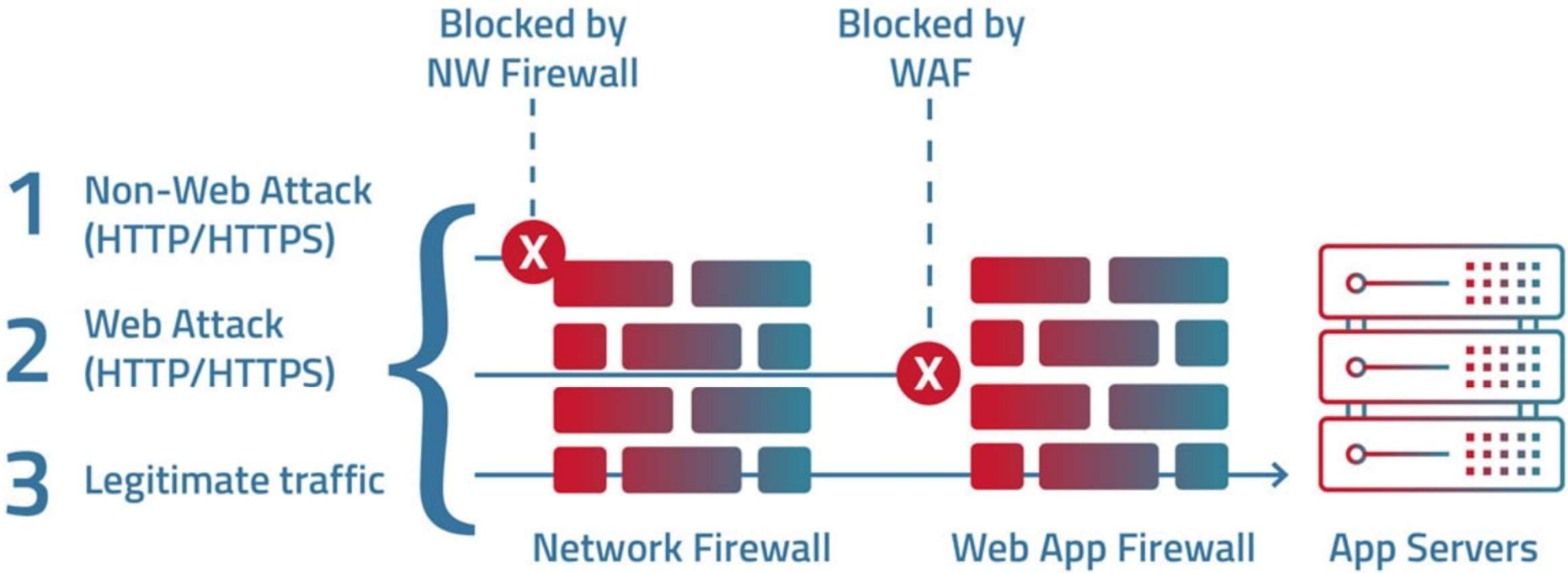


3. Screened subnet (*screened subnet gateway* (SSG)

Firewall dengan arsitektur ini menggunakan dua

Screened-router dan jaringan tengah (*perimeter network)* antara kedua router tersebut, dimana ditempatkan bastion host.





A network firewall and a web application firewall (WAF) are both security solutions that help protect against cyberattacks, although they differ in the way they work, the internet layer and protocols they monitor and the types of attacks they are designed to protect against. WAFs secure web traffic by filtering and monitoring HTTP traffic (OSI layer 7) between web applications and end-users.

They employ a different set of security policies to detect and prevent attacks such as injection, cross-site scripting, server-side request forgeries, and other web application attacks. In contrast, network firewalls monitor and control Network and Transport layers traffic (OSI Layers 3 and 4) based on pre-defined security policies to ensure unauthorized traffic is denied entry.

Types of WAF Solutions

- **Network-based WAF:** Deployed at the network perimeter. Inspects traffic before it reaches your web application.
- **Host-based WAF:** Deployed directly on the web server. Monitors traffic at the server level.
- **Cloud-based WAF:** Hosted and managed by third-party cloud security providers.

Benefits of Free WAF Solutions

Using a WAF solution can offer several advantages:

- Most of the WAFs are free or offer a free version.
- Allows customization and community-driven development.
- Preemptive attack blocking.
- Renowned for “install and forget” simplicity.

Key Features to Look For in a WAF Solution

When evaluating a WAF solution, consider the following key features:

- Ability to identify and block threats before they reach your application.
- Machine learning capabilities.
- Rules and policy customization.
- Ease of integration with your existing tech stack and development tools.
- Logging and reporting features to monitor and analyze traffic.

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

```
kb@phoenixNAP:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-05 13:45 CEST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 26.51 seconds
```

```
kb@phoenixNAP:~$ nmap -p 80 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-03 15:49 CEST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Common Ports

There are many standardized ports associated with specific services. Use the list below as a reference for these ports and their related service:

- **21** (FTP). File transfer protocol.
- **22** (SSH). Secure shell.
- **25** (SMTP). Simple mail transfer protocol.
- **53** (DNS). Domain name system.
- **67**, **68** (DHCP). Dynamic host configuration protocol.
- **80** (HTTP). Hypertext transfer protocol.
- **110** (POP3). Post office protocol version 3.
- **123** (NTP). Network time protocol.
- **143** (IMAP). Internet access message protocol.
- **443** (HTTPS). Hypertext transfer protocol secure.
- **465** (SMTPS). SMTP secure.
- **631** (CUPS). Common Unix printing system.
- **993** (IMAPS). IMAP secure.
- **995** (POP3S). POP3 secure.
- **3306** (MySQL). MySQL database server.
- **3389** (RDP). Remote desktop protocol.
- **8080** (HTTP alternate). HTTP alternate, used for proxy servers.

- To list the current configuration:

```
iptables -L -n -v --line-numbers
```

- To stop every single packet from going in/out of your system. For security reasons, make sure to do this so that no other packet that you explicitly specify, is going to be transferred.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

- To allow packets inside your loopback interface to travel without problem.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Rule Settings

Rule Name: Rate Limit Failed Login Attempts

If Traffic Matching the URL

http & https | www.example.com/login

from the same IP address exceeds 5 requests per 1 minute

Advanced Criteria

Method(s)

POST

HTTP Response Header(s)

Cf-Cache-Status | Not Equals | HIT

+ Add header response field

Also apply rate limit to cached assets

Origin Response code(s)

403

Then Block matching traffic from that visitor for 1 hour

When "Block" is set, when the threshold is exceeded, the Client will receive a "429" error page until the Block time has expired.