PENGAMANAN
JARINGAN KOMPUTER

KONSEP DASAR

KEAMANAN JARINGAN KOMPUTER

- **Keamanan jaringan komputer adalah** proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer.
- **Tujuan dari keamanan jaringan komputer adalah** untuk mengantisipasi risiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung yang mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

TIDAK ADA jaringan yang **ANTI SADAP**
atau tidak ada jaringan komputer
YANG BENAR-BENAR AMAN.

ELEMEN UTAMA

PEMBENTUK KEAMANAN JARINGAN

1. **TEMBOK PENGAMANAN**, baik secara fisik maupun maya, yang ditaruh diantara piranti dan layanan jaringan yang digunakan serta orang-orang yang akan berbuat jahat.
2. **RENCANA PENGAMANAN**, yang akan diimplementasikan bersama dengan user lainnya untuk menjaga agar sistem tidak bisa ditembus dari luar.

BENTUK ANCAMAN

KEAMANAN JARINGAN KOMPUTER

- FISIK
  - Pencurian Hardware Komputer / Perangkat Jaringan
  - Kerusakan pada Komputer dan Perangkat Komunikasi Jaringan
  - Wiretapping
  - Bencana Alam
- LOGIK
  - Kerusakan pada Sistem Operasi atau Aplikasi
  - Virus
  - Sniffing

BENTUK ANCAMAN

KEAMANAN JARINGAN KOMPUTER

- Beberapa bentuk ancaman jaringan komputer:
  - **SNIFFER**, Peralatan yang dapat memonitor proses yang sedang berlangsung.
  - **SPOOFING**, Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP).
  - **REMOTE ATTACK**, Segala bentuk serangan terhadap suatu mesin dimana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jaruh di luar sistem jaringan atau media transmisi.

BENTUK ANCAMAN

KEAMANAN JARINGAN KOMPUTER

- **HOLE**, Kondisi dari software atau hardware yang bisa diakses oleh pemakai yang tidak memiliki otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi.
- **PHREAKING**, Perilaku menjadikan sistem pengamanan telepon melemah.
- **HACKER**,
  - Orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-share hasil ujicoba yang dilakukannya.
  - Hacker tidak merusak sistem.

BENTUK ANCAMAN

KEAMANAN JARINGAN KOMPUTER

- **CRACKER**,
  - Orang yang secara diam-diam mempelajari sistem dengan maksud jahat.
  - Muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak).

BAGAIMANA CIRI-CIRI SEORANG CRACKER

BENTUK ANCAMAN

KEAMANAN JARINGAN KOMPUTER

- **CRACKER**, Ciri-cirinya adalah:
  - Bisa membuat program C, C++, atau Pearl dan memiliki pengetahuan TCP/IP.
  - Menggunakan internet lebih dari 50 jam per bulan.
  - Menguasai sistem operasi UNIX atau VMS.
  - Suka mengoleksi software atau hardware lama.
  - Terhubung ke internet untuk menjalankan aksinya.
  - Melakukan aksinya pada malam hari dengan alasan waktu yang memungkinkan, jalur komunikasi tidak padat, dan tidak mudah diketahui orang lain.

BENTUK ANCAMAN

KEAMANAN JARINGAN KOMPUTER

- **CRACKER**, Faktor melakukan serangan karena:
  - SPITE, kecewa / balas dendam.
  - SPORT, petualangan.
  - PROFIT, mencari keuntungan dari imbalan orang lain.
  - CRURIOUSITY, mencari perhatian.
  - POLITICS, alasan politis.

FAKTOR PENYEBAB RISIKO
KEAMANAN JARINGAN KOMPUTER

- Kelemahan manusia (human error)
- Kelemahan perangkat keras komputer
- Kelemahan sistem operasi jaringan
- Kelemahan sistem jaringan komunikasi

METODE PENYERANGAN

KEAMANAN JARINGAN KOMPUTER

- **EAVESDROPPING**, Mendapatkan duplikasi pesan tanpa izin.
- **MASQUERADING**, Mengirim atau menerima pesan menggunakan identitas lain tanpa izin.
- **MESSAGE TAMPERING**, Mencegat atau menangkap pesan dan mengubah isinya sebelum dilanjutkan ke penerima sebenarnya.
- **REPLAYING**, Menyimpan pesan yang ditangkap untuk pemakaian berikutnya.
- **DENIAL OF SERVICE**, Membanjiri saluran atau sesumber lain dengan pesan yang bertujuan untuk menggagalkan pengaksesan pemakai lain.

KATEGORI SERANGAN

KEAMANAN JARINGAN KOMPUTER

1. **INTERRUPTION**
   - Suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang.
   - Contoh: Perusakan / modifikasi terhadap piranti keras atau saluran jaringan.

2. **INTERCEPTION**
   - User yang tidak berhak (anauthorized) mendapatkan akses file.
   - Contoh: Penyadapan terhadap data dalam suatu jaringan.

SERANGAN-SERANGAN
KEAMANAN JARINGAN KOMPUTER

3. **MODIFICATION**
   - User yang tidak berhak tidak hanya mendapatkan akses, tetapi juga dapat mengubahnya.
   - Contoh: Perubahan nilai pada file data, Modifikasi program sehingga berjalan dengan tidak semestinya, dan Modifikasi pesan yang sedang ditransmisikan dalam jaringan.

4. **FABRICATION**
   - User yang tidak berwenang menyisipkan objek palsu ke dalam sistem.
   - Contoh: Pengiriman pesan palsu kepada orang lain.

PENGENDALIAN I:

MEMBATASI AKSES KE JARINGAN

1. **MEMBUAT TINGKATAN AKSES**
   - Melakukan pembatasan-pembatasan, sehingga memperkecil peluang penembusan oleh pemakai yang tak diotorisasi.
   - Misalnya:
     - Pembatasan Login
     - Pembatasan Jumlah Usaha Login
     - Tingkat Akses yang Diizinkan (Read/Write/Execute)

PENGENDALIAN I:
MEMBATASI AKSES KE JARINGAN

2. MEKANISME KENDALI AKSES

- Melakukan user authentication (autentikasi pemakai), yaitu masalah identifikasi pemakai ketika login.
- Metode autentikasi didasarkan pada tiga cara:
  - Sesuatu yang diketahui pemakai. Misalnya: Password, Kombinasi Kunci, Nama Kecil Ibu Mertua, dsb.
  - Sesuatu yang dimiliki pemakai. Misalnya: Badge, Kartu Identitas, Kunci, dsb.
  - Sesuatu mengenai (ciri) pemakai. Misalnya: Sidik Jari, Sidik Suara, Foto, Tanda Tangan.

PENGENDALIAN I:

MEMBATASI AKSES KE JARINGAN

3. **WASPADA TERHADAP REKAYASA SOSIAL**
   - **Mengaku sebagi eksekutif** yang tidak berhasil mengakses dengan menghubungi administrator via telepon/fax.
   - **Mengaku sebagai administrator** yang perlu mendiagnosa masalah network dengan menghubungi end user via email/fax/surat.
   - **Mengaku sebagai petugas keamanan e-commerce** dengan menghubungi customer yang telah bertransaksi untuk mengulang kembali transaksinya di form yang disediakan olehnya.
   - **Pencurian** surat atau password, **penyuapan**, dan **kekerasan**.

PENGENDALIAN I:

MEMBATASI AKSES KE JARINGAN

4. **MEMBEDAKAN SUMBER DAYA INTERNAL & EKSTERNAL**
   - Memanfaatkan teknologi firewall yang memisahkan network internal dengan network eksternal dengan rule tertentu.

5. **SISTEM AUTENTIKASI USER**
   - Sistem Autentikasi User adalah proses penentuan identitas dari seseorang yang sebenarnya.
   - Diperlukan untuk menjaga keutuhan (integrity) dan keamanan (security) data.

UPAYA PENGAMANAN PROTEKSI PASSWORD

Upaya untuk lebih mengamankan proteksi password, antara lain:

- **SALTING**, Menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu.
- **ON TIME PASSWORD (OTP)**, User harus mengganti password secara teratur. User mendapat satu buku berisi daftar password. Setiap kali melakukan login, user menggunakan password berikutnya yang terdapat di daftar password.
- **TANTANGAN TANGGAPAN (CHALLENGE RESPONSE)**, User diberi kebebasan memilih suatu algoritma, misalnya x^3. Ketika user login, komputer menuliskan di layar angka 3. Dalam kasus ini, user mengetik angka 27 agar login berhasil. Algoritma dapat berbeda di pagi, sore, dan hari berbeda, dari terminal berbeda, dan seterusnya.

UPAYA PENGAMANAN PROTEKSI PASSWORD

- **SATU DAFTAR PANJANG PERTANYAAN DAN JAWABAN**, Variasi terhadap password adalah mengharuskan pemakai memberi satu daftar pertanyaan panjang dan jawabannya.

  Pertanyaan berikut dapat dipakai, misalnya :

  - Siapa mertua abang ipar Agus?
  - Apa yang diajarkan Bu Astri waktu SD ?
  - Film animasi apa yang disukai oleh Anda dan pasangan hidup Anda?

  Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke user, dan memeriksa jawaban yang diberikan.

CONTOH-CONTOH

PRODUK AUTENTIKASI USER

- Secured Ace (Access Control Encryption)
- S/Key (Bellcore)
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Remote Authentication Dial-in User Servis (RADIUS)
- Terminal Access Controller Access Control System (TACACS)

PENGENDALIAN II:
MELINDUNGI ASET ORGANISASI

Ada dua cara dalam melindungi aset organisasi dalam jaringan komputer, yaitu:

- **SECARA ADMINISTRATIF / FISIK**, dengan membuat rencana kemungkinan terhadap bencana, program penyaringan calon pegawai sistem informasi, program pelatihan user, dan kebijakan akses network.
- **SECARA TEKNIS**, dengan menerapkan Firewall dan membentuk VPN.

KONSEP FIREWALL

KEAMANAN JARINGAN KOMPUTER

- **Firewall adalah** sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan.
- **Secara prinsip**, Firewall dapat dianggap **sebagai sepasang mekanisme**:
  1. Memblok lalu lintas
  2. Mengizinkan lalu lintas jaringan
- **Firewall digunakan untuk** melindungi jaringan Anda dari serangan jaringan pihak luar.
- **Firewall tidak dapat melindungi** dari serangan yang tidak melalui firewall, serangan dari seseorang yang berada di dalam jaringan Anda, serta dari program-program aplikasi yang ditulis dengan buruk.

KONSEP FIREWALL

KEAMANAN JARINGAN KOMPUTER

- **Secara konseptual**, terdapat **dua macam Firewall**, yaitu Network Level dan Application Level.
- **Network Level** didasarkan pada keputusan mereka pada alamat sumber, alamat tujuan, dan port yang terdapat dalam setiap paket IP.
- **Application Level** biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengizinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya.

ISTILAH FIREWALL

KEAMANAN JARINGAN KOMPUTER

- **HOST**

  Suatu sistem komputer yang terhubung pada suatu network.

- **BASTION HOST**

  Sistem komputer yang harus memiliki tingkat sekuritas yang tinggi.

  MENGAPA? Karena sistem ini rawan sekali terhadap serangan hacker dan cracker, karena biasanya mesin ini diekspos ke network luar (internet) dan merupakan titik kontak utama para user dari internal network.

ISTILAH FIREWALL

KEAMANAN JARINGAN KOMPUTER

- **PACKET FILTERING**
  - Aksi dari suatu alat / device untuk mengatur secara selektif alur data yang melintasi suatu network.
  - Dapat memblok / memperbolehkan suatu paket data yang melintasi network tsb sesuai dengan kebijaksanaan alur data yang digunakan (security policy).
- **PERIMETER NETWORK / DMZ (De-Millitarized Zone)**
  - Suatu network tambahan yang terdapat di antara network yang dilindungi dengan network eksternal untuk menyediakan layer tambahan dari suatu sistem keamanan.

KEUNTUNGAN FIREWALL

KEAMANAN JARINGAN KOMPUTER

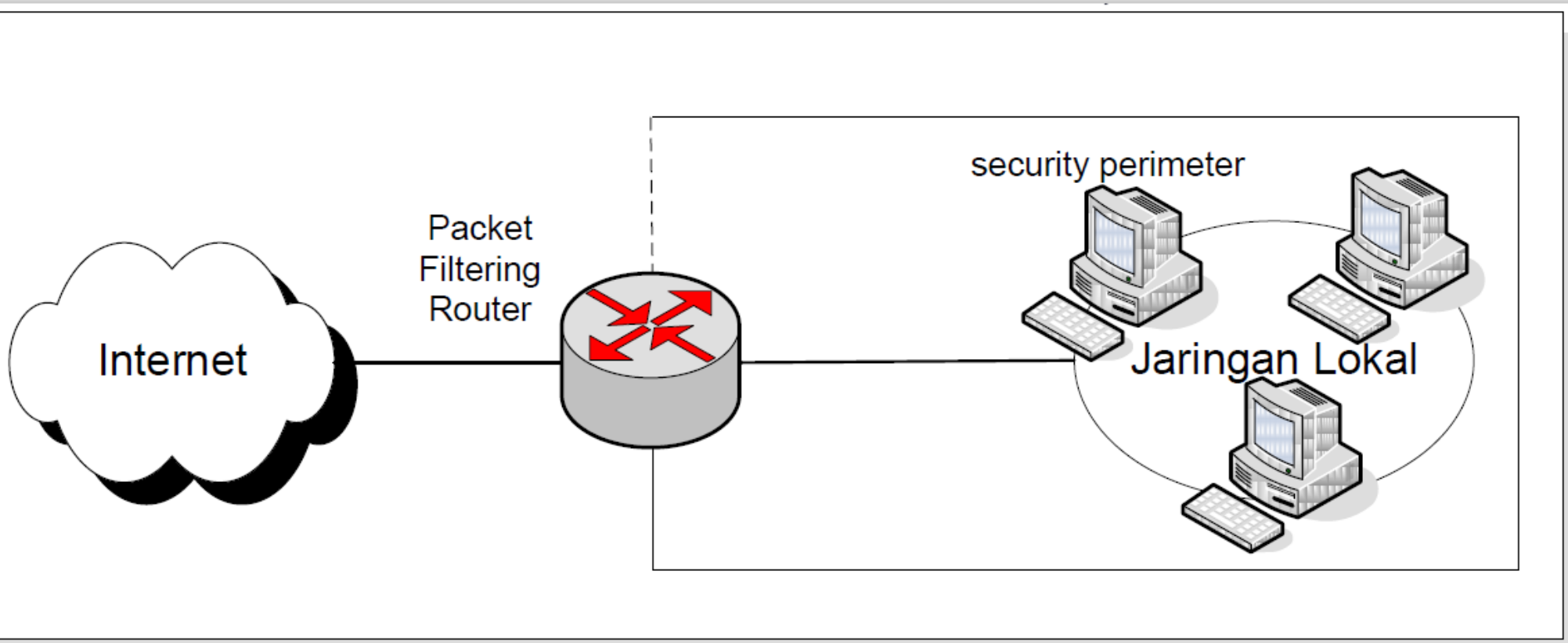
- Fokus dari segala keputusan sekuritas karena merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.
- Dapat menerapkan suatu kebijaksanaan sekuritas. Tidak semua service di internet aman digunakan, sehingga Firewall berfungsi sebagai penjaga untuk mengawasi service-service mana yang dapat digunakan untuk menuju dan meninggalkan suatu network.
- Dapat mencatat segala aktivitas yang berkaitan dengan alur data secara efisien.
- Dapat digunakan untuk membatasi pengunaan sumberdaya informasi.

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER

1. PACKET FILTERING

- Sistem Packet Filtering / Screening Router adalah router yang melakukan routing paket antara internal dan eksternal network secara selektif sesuai dengan security policy yang digunakan pada network tersebut.
- Informasi yang digunakan untuk menyeleksi paket-paket tersebut adalah:
  - IP address asal
  - IP address tujuan
  - Protocol (TCP, UDP, atau ICMP)
  - Port TCP atau UDP asal
  - Port TCP atau UDP tujuan

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER



Gambar 1. Packet Filtering Router

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER

- Contoh routing paket selektif yang dilakukan oleh Screening Router:
  - Semua koneksi dari luar sistem yang menuju internal network diblokade, kecuali untuk koneksi SMTP.
  - Memperbolehkan service email dan FTP, tetapi memblok service-service berbahaya, seperti TFTP, X Window, RPC, dan ‘r’ service (rlogin, rsh, rcp, dan lain-lain).

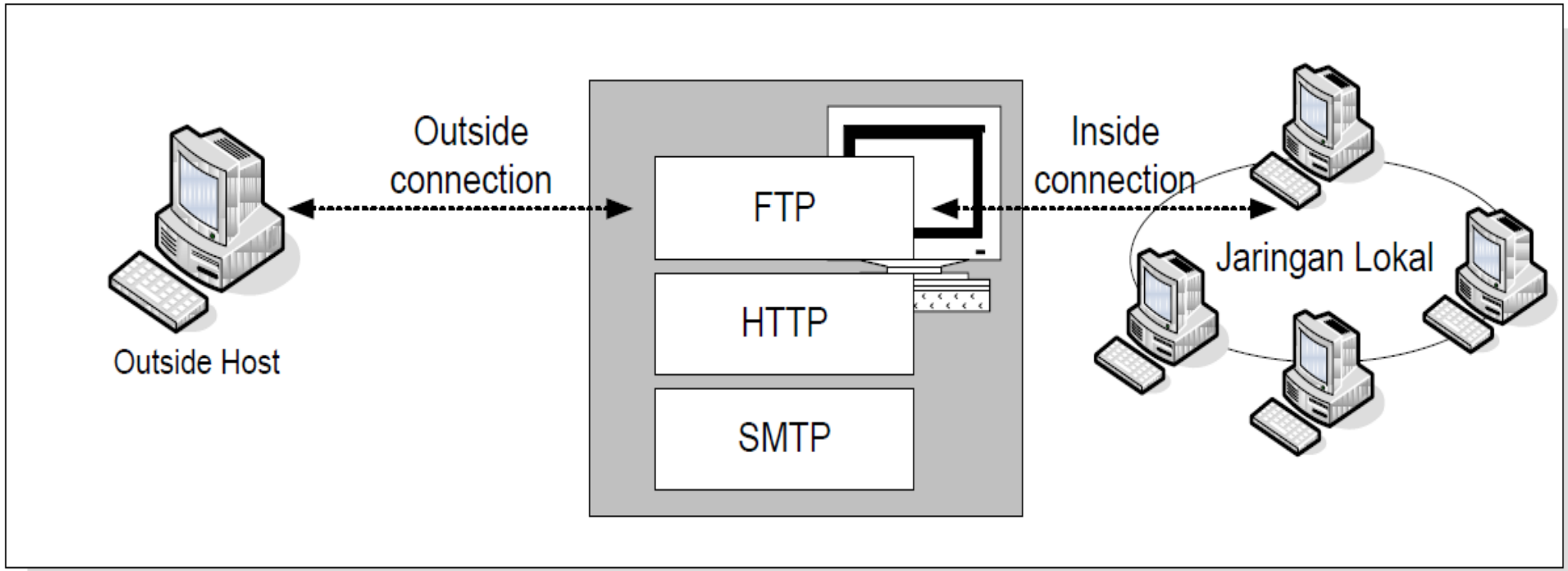
KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER

- **Keuntungan** dari Packet Filtering / Screening Router:
  - Bersifat transparan dan implementasinya relatif lebih murah dibandingkan metode Firewall yang lain.
- **Kekurangan** dari Packet Filtering / Screening Router:
  - Tingkat keamanannya masih rendah.
  - Masih memungkinkan adanya IP Spoofing.
  - Tidak ada screening pada layer-layer di atas network layer.

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER

2. **APPLICATION LEVEL GATEWAY (PROXY SERVICE)**
   - **Proxy merupakan** perantara antara internal network dengan eksternal network (internet).
   - **Proxy Service merupakan** aplikasi spesifik atau program server yang dijalankan pada mesin Firewall.
   - Program ini mengambil user request untuk internet service (seperti FTP, telnet, HTTP) dan meneruskannya (bergantung pada security policy) ke host yang dituju.

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER



Gambar 2. Application-Level Gateway

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER

- **Keuntungan** dari Sistem Proxy:
  - Tingkat keamanannya lebih baik daripada Screening Router.
  - Deteksi paket yang dilakukan sampai pada layer aplikasi.

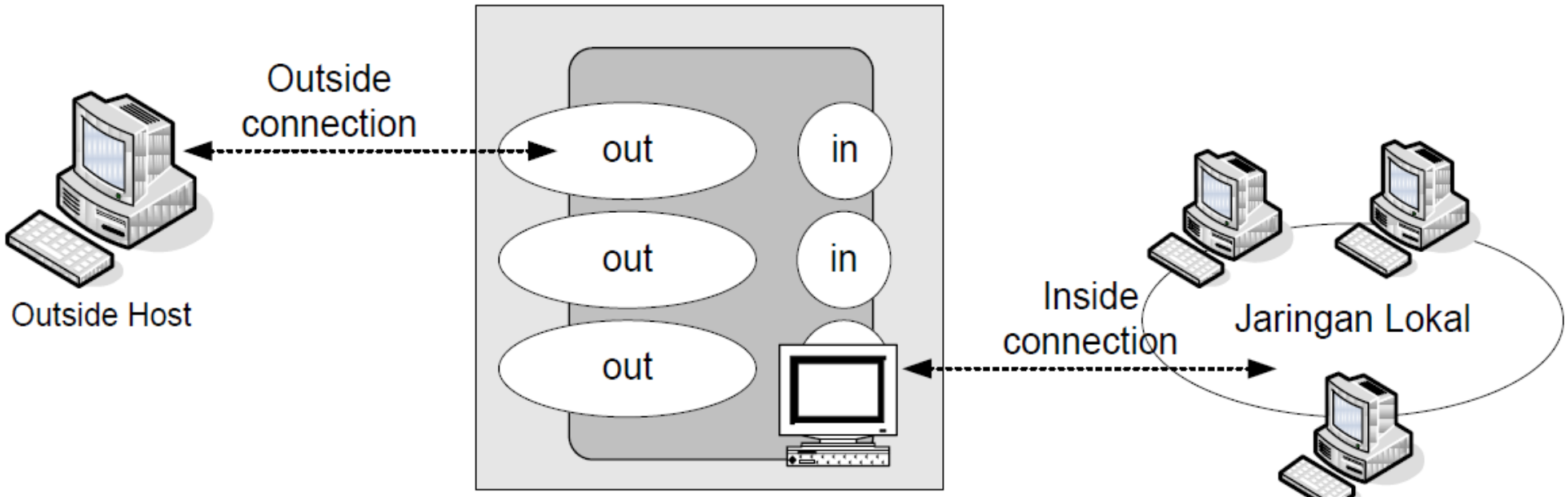
- **Kekurangan** dari Sistem Proxy :
  - Perfomansinya lebih rendah daripada Screening Router karena terjadi penambahan header pada paket yang dikirim.
  - Aplikasi yang di-support oleh Proxy ini terbatas.
  - Sistem ini kurang transparan.

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER

3. CIRCUIT-LEVEL GATEWAY

- Circuit-Level Gateway merupakan sistem yang berdiri sendiri atau fungsi khusus yang terbentuk dari tipe application-level gateway.
- Tipe ini tidak mengizinkan koneksi TCP end to end (langsung).

KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER



Gambar 3. Circuit-level Gateway

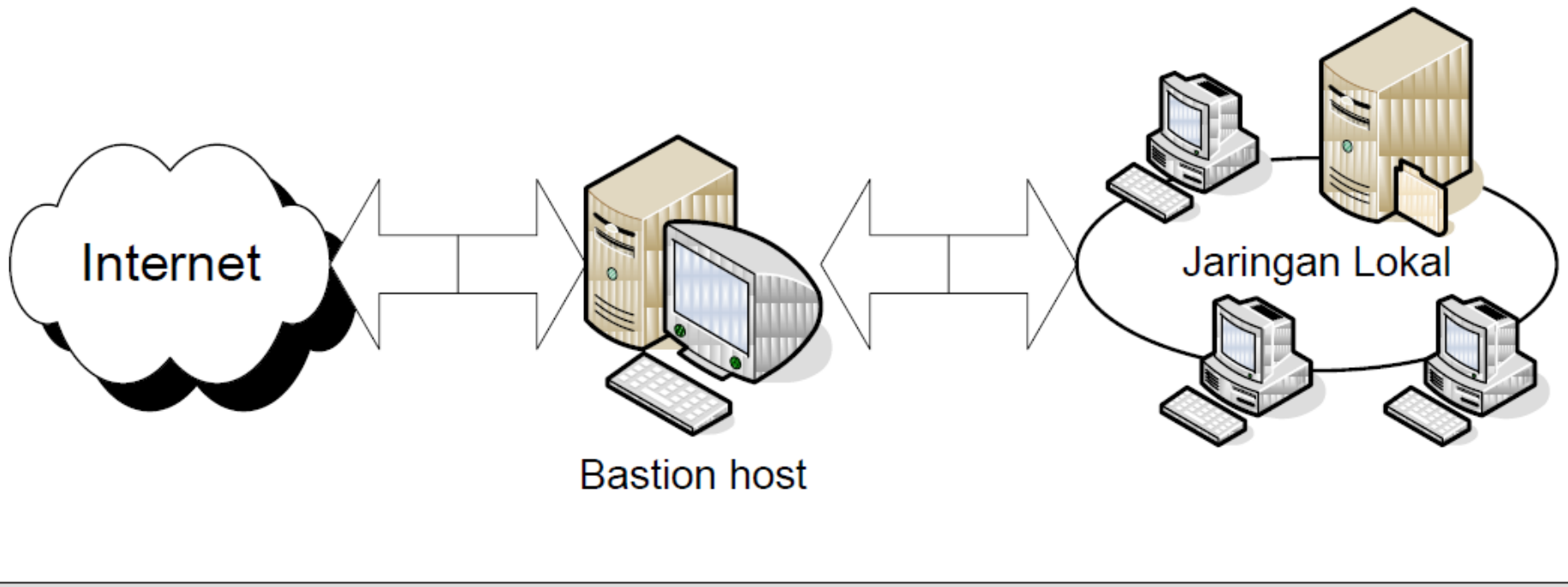
KLASIFIKASI DESAIN FIREWALL
KEAMANAN JARINGAN KOMPUTER

- Cara kerja **CIRCUIT-LEVEL GATEWAY** adalah:
  - Gateway akan mengatur kedua hubungan TCP tersebut.
  - 1 antara dirinya (gw) dengan TCP pada pengguna lokal (inner host) serta 1 lagi antara dirinya (gw) dengan TCP pengguna luar (outside host).
  - Saat dua buah hubungan terlaksana, gateway akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya.
  - Fungsi pengamanannya terletak pada penentuan hubungan mana yang diizinkan.

ARSITEKTUR DASAR FIREWALL
KEAMANAN JARINGAN KOMPUTER

1. **ARSITEKTUR DUAL-HOMED HOST (DUAL-HOMED GATEWAY / DHG)**
   - Sistem DHG menggunakan sebuah komputer dengan (paling sedikit) dua network-interface.
   - Interface pertama dihubungkan dengan jaringan internal dan yang lainnya dengan internet.
   - Dual-Homed Host berfungsi sebagai **Bastion Host** (front terdepan, bagian terpenting dalam Firewall).

ARSITEKTUR DASAR FIREWALL
KEAMANAN JARINGAN KOMPUTER

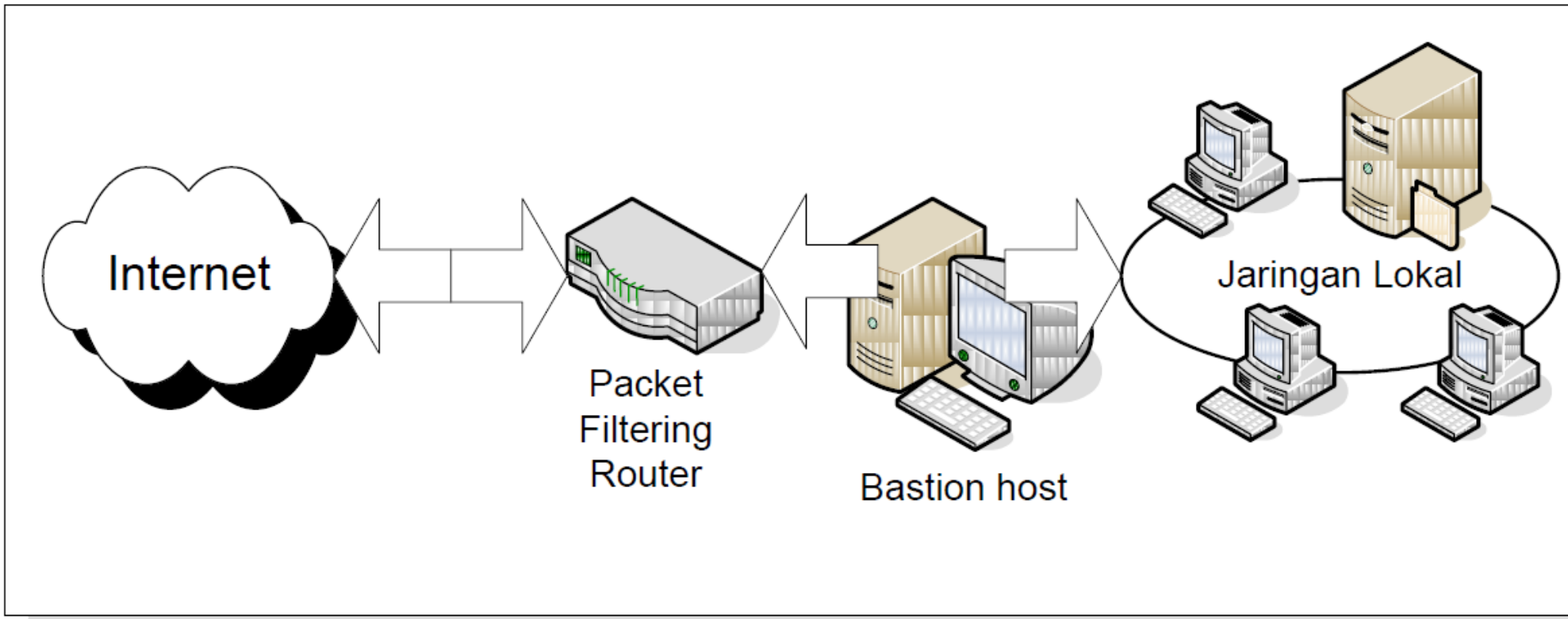


Gambar 4. Screened Host Firewall system (Dual-homed bastion)

ARSITEKTUR DASAR FIREWALL
KEAMANAN JARINGAN KOMPUTER

2. **SCREENED-HOST (SCREENED-HOST GATEWAY / SHG)**
   - Pada topologi SHG, fungsi Firewall dilakukan oleh sebuah Screening Router dan Bastion Host.
   - Router ini dikonfigurasi sedemikian, sehingga akan menolak semua trafik, kecuali yang ditujukan ke Bastion Host, sedangkan pada trafik internal tidak dilakukan pembatasan.
   - Dengan cara ini, setiap client service pada jaringan internal dapat menggunakan fasilitas komunikasi standard dengan internet tanpa harus melalui Proxy.

ARSITEKTUR DASAR FIREWALL
KEAMANAN JARINGAN KOMPUTER

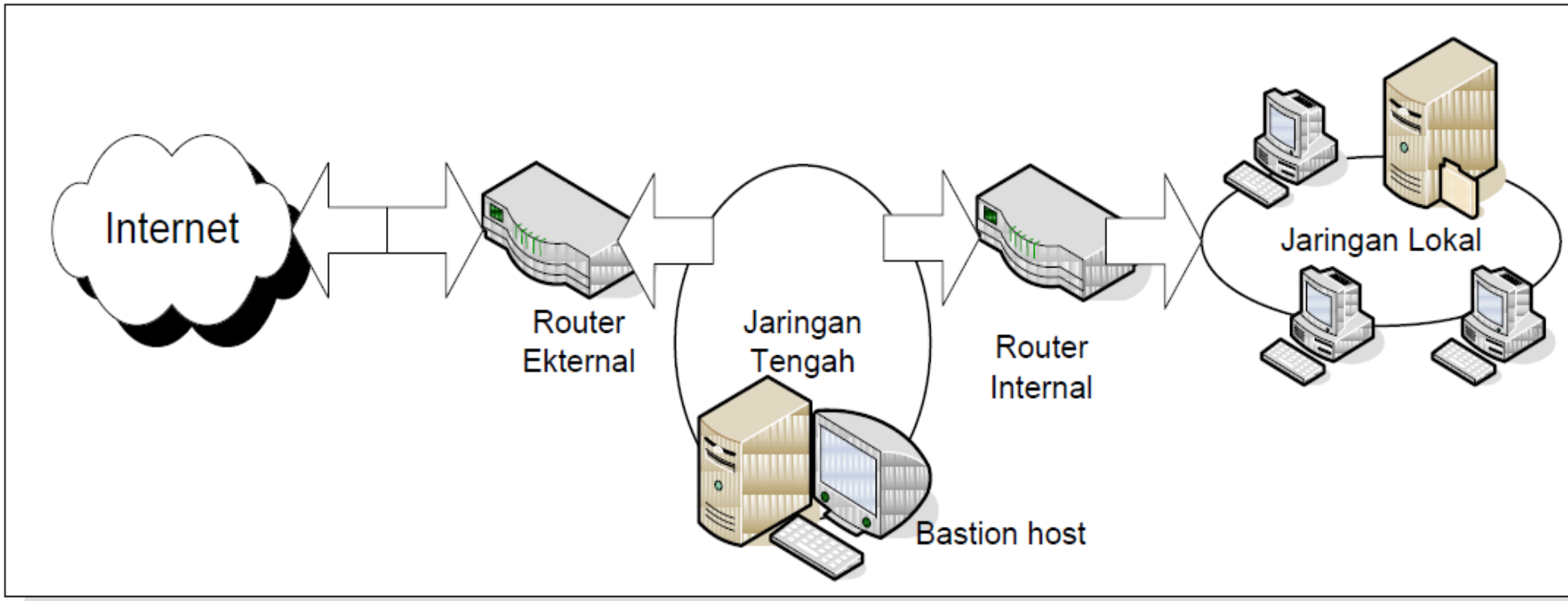


Gambar 5. Screened Host Firewall system

ARSITEKTUR DASAR FIREWALL
KEAMANAN JARINGAN KOMPUTER

3. **SCREENED SUBNET (SCREENED SUBNET GATEWAY / SSG)**
   - Firewall dengan arsitektur Screened Subnet menggunakan dua Screening Router dan jaringan tengah (Perimeter Network) antara kedua router tersebut, dimana ditempatkan Bastion Host.
   - Kelebihan susunan ini akan terlihat pada waktu optimasi penempatan server.

ARSITEKTUR DASAR FIREWALL
KEAMANAN JARINGAN KOMPUTER



Gambar 6. Screened subnet firewall

KONSEP VPN

KEAMANAN JARINGAN KOMPUTER

- **Virtual Private Network (VPN) atau Jaringan Pribadi Maya** sama dengan Jaringan Pribadi (Private Network/PN) pada umumnya, di mana satu jaringan komputer suatu lembaga atau perusahaan di suatu daerah atau negara terhubung dengan jaringan komputer dari satu grup perusahaan yang sama di daerah atau negara lain.
- **Perbedaannya** hanyalah pada media penghubung antar jaringan, yaitu:
  - Pada PN, media penghubungnya masih milik perusahaan / grup itu sendiri.
  - Pada VPN, media penghubungnya adalah jaringan publik, seperti Internet.

CARA MEMBENTUK VPN

KEAMANAN JARINGAN KOMPUTER

1. TUNNELLING
   - VPN ini dibuat dengan suatu tunnel (lorong) di dalam jaringan publik untuk menghubungkan antara jaringan yang satu dan jaringan lain dari suatu grup atau perusahaan.yang ingin membangun VPN tersebut.
   - Seluruh komunikasi data antar jaringan pribadi akan melalui tunnel ini, sehingga orang atau user dari jaringan publik yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak, atau mencuri data yang melintasi tunnel ini.
   - Ada beberapa metode Tunelling yang umum dipakai, di antaranya:
     - IPX To IP Tunnelling.
     - PPP To IP Tunnelling.

CARA MEMBENTUK VPN

KEAMANAN JARINGAN KOMPUTER

IPX To IP TUNNELING:

- IPX To IP Tunnelling biasa digunakan dalam jaringan VPN Novell Netware. Jadi, dua jaringan Novell yang terpisah akan tetap dapat saling melakukan komunikasi data melalui jaringan publik internet melalui tunnel ini tanpa khawatir akan adanya gangguan pihak ke-3 yang ingin mengganggu atau mencuri data.
- Pada IPX To IP Tunnelling, paket data dengan protokol IPX (standar protokol Novell) akan dibungkus (encapsulated) terlebih dahulu oleh protokol IP (Standar Protokol Internet), sehingga dapat melalui tunnel ini pada jaringan publik internet.

CARA MEMBENTUK VPN

KEAMANAN JARINGAN KOMPUTER

PPP To IP TUNNELING:

- Sama halnya untuk PPP To IP Tunnelling, di mana PPP protokol di-encapsulated oleh IP protokol.

Beberapa vendor hardware router, seperti **Cisco, Shiva, Bay Networks** sudah menambahkan kemampuan VPN dengan teknologi Tunnelling pada hardware mereka.

CARA MEMBENTUK VPN

KEAMANAN JARINGAN KOMPUTER

2. FIREWALL

- **IP Hiding / Mapping**

  Kemampuan ini mengakibatkan IP Address dalam jaringan dipetakan atau ditranslasikan ke suatu IP Address baru. Dengan demikian, IP Address dalam jaringan tidak akan dikenali di internet.

- **Privilege Limitation**

  Kita dapat membatasi para user dalam jaringan sesuai dengan otorisasi atau hak yang diberikan kepadanya. Misalnya, User A hanya boleh mengakses home page, sedangkan User B boleh mengakses home page, e-mail, dan news.

CARA MEMBENTUK VPN

KEAMANAN JARINGAN KOMPUTER

- **Outside Limitation**

  Kita dapat membatasi para user dalam jaringan hanya untuk mengakses ke alamat-alamat tertentu di internet di luar dari jaringan kita.

- **Inside Limitation**

  Kadang-kadang kita masih memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu komputer (misalnya: Web Server) dalam jaringan kita. Selain itu, tidak diperbolehkan atau memang sama sekali tidak dizinkan untuk mengakses seluruh komputer yang terhubung ke jaringan kita.

CARA MEMBENTUK VPN

KEAMANAN JARINGAN KOMPUTER

- Password and Encrypted Authentication

  Beberapa user di luar jaringan memang diizinkan untuk masuk ke jaringan kita untuk mengakses data dan sebagainya, dengan terlebih dahulu harus memasukkan password khusus yang sudah terenkripsi.

ABCs of Information Security Awareness

A — Always Properly Logout After Completion of Online Transaction

B — Be Careful What You Click

C — Clear Cookies and Delete Browsing History at the End of Session and Stay Safe

D — Do not Carry Your PIN Number in Wallets Better to Memorize Your PIN

E — Enlighten Yourself On Cyber Security Measures

F — Following Basic Rules of Social Networking Can Prevent Damaging Your Online Relationships

G — Giving Out Your Personal Information Online is not Advisable

H — Help Yourself to Maintain a Positive Online Presence

I — Install Anti-virus Protection

J — Join Hands to Stop Spreading Fake News

K — Keep Software Up to Date

L — Lock Your Devices When Not in Use

M — Monitor Your Account for Any Suspicious Activity

N — Never Believe On Forward Messages, Check Source And URL

O — Only Install Apps and Software From Trusted Sources

P — Pay Extra Attention While Using Public Wifi

Q — Quarantine All Unused Apps

R — Respect the Privacy of Others

S — Scan Any File Downloaded From Internet Before Opening/ Using/ Installing

T — Turn On Automatic Updates For Your Operating System

U — Use Strong Passwords With Personal Acronym

V — Verify With Whom You Are Interacting Online

W — Watch Out For Online Scams

X — Xtra Precaution For Your Online Financial Transactions

Y — Your Priority On Cyber Security Make You Cyber Aware Citizen

Z — Zero Participation in Dark Web