Firewall & IDS

Keamanan Siber

Always The First

Materi

- Pengertian Firewall
- Jenis Firewall
- Fungsi Firewall
- Sistem Kerja Firewall
- Intrusion Detection System (IDS)

Pengertian Firewall

- Firewall adalah sebuah sistem keamanan yang dirancang untuk melindungi jaringan komputer dari ancaman dan serangan yang dapat datang dari jaringan luar, seperti Internet.
- Fungsinya adalah untuk mengontrol lalu lintas data yang masuk dan keluar dari jaringan, serta memutus atau mengizinkan akses berdasarkan aturan-aturan yang telah ditentukan.

Jenis Firewall

- Network Firewall
- Host-Based Firewall
- Application Firewall

Network Firewall

- Network Firewall ditempatkan di antara jaringan internal dan jaringan eksternal (seperti Internet).
  - Bisa berupa perangkat keras (seperti firewall yang terintegrasi dengan router) atau perangkat lunak yang dijalankan di server khusus.
- Network Firewall melakukan pengaturan lalu lintas berdasarkan aturan-aturan yang telah ditetapkan, seperti memblokir akses dari alamat IP tertentu atau jenis layanan tertentu.

Host-based Firewall

- Firewall ini ada di dalam sistem atau perangkat sendiri.
  - Bisa berupa perangkat lunak yang diinstal di komputer atau server, dan mengontrol lalu lintas yang masuk dan keluar dari perangkat tersebut.
- Sistem operasi modern sering menyertakan firewall host yang dapat diaktifkan untuk memberikan lapisan perlindungan tambahan.

Application Firewall

- Firewall ini bekerja pada lapisan aplikasi, mengawasi lalu lintas berdasarkan protokol dan aturan aplikasi.
  - Biasanya membantu dalam melindungi aplikasi web dari serangan seperti SQL injection, cross-site scripting (XSS), dan lainnya dengan memahami konteks lalu lintas aplikasi.

Fungsi Firewall

- Access Control List (ACL)
- Network Address Translation (NAT)
- Packet / Traffic Filtering
- Intrusion Detection dan Intrusion Prevention

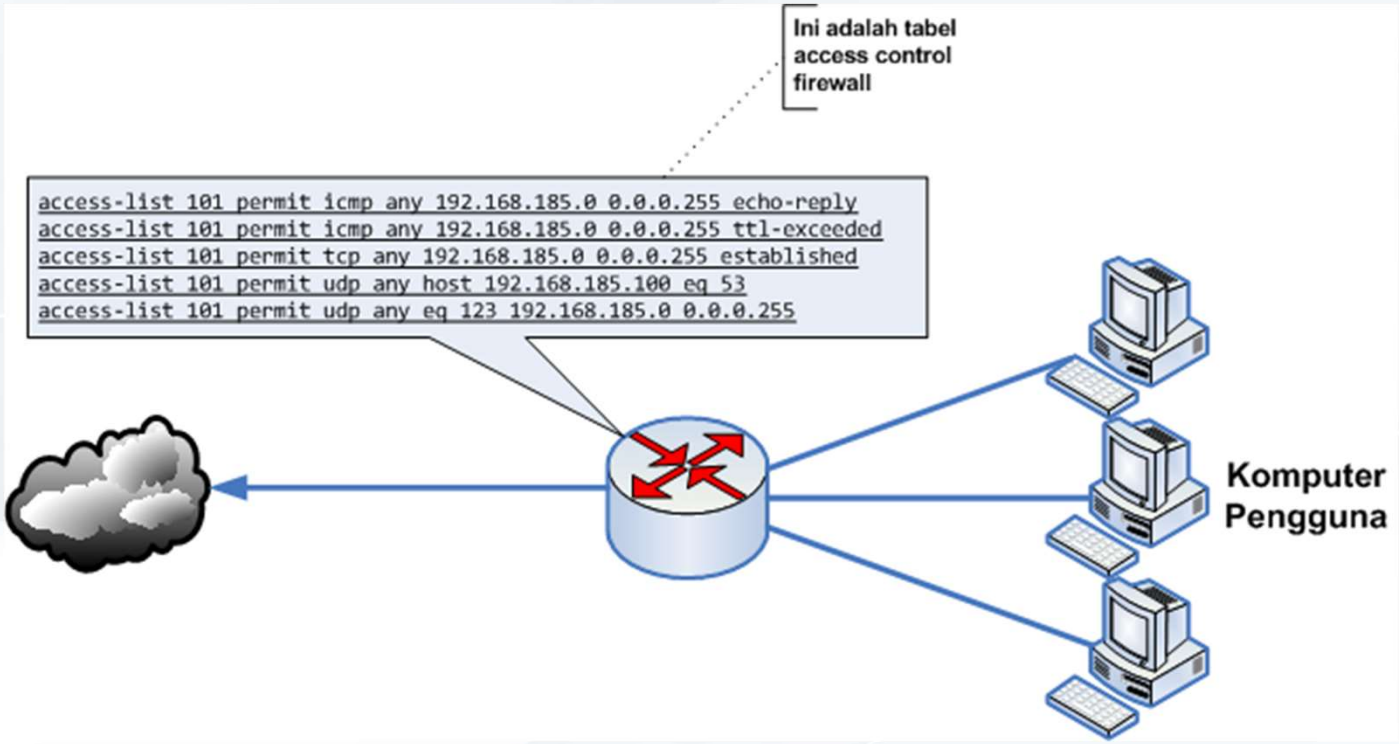
Access Control List (ACL)

- Access Control List (ACL) Firewall adalah komponen dalam jaringan yang digunakan untuk mengatur akses dan mengontrol lalu lintas data berdasarkan aturan yang telah ditentukan.
- ACL adalah daftar peraturan yang menentukan apa yang diperbolehkan dan apa yang diblokir dalam lalu lintas jaringan.
- Firewall ACL dapat diterapkan pada router, switch, atau perangkat jaringan lainnya untuk mengontrol aliran data.

Komponen ACL

- Source → asal paket, bisa berupa IP atau domain
- Destination → tujuan paket, bisa berupa IP atau domain
- Port → port asal dan port tujuan paket
- Protokol → protocol (TCP atau UDP, nama protokol) yang digunakan untuk berkomunikasi
- Aksi → hal / Tindakan yang dilakukan untuk proses komunikasi tersebut (permit atau deny)

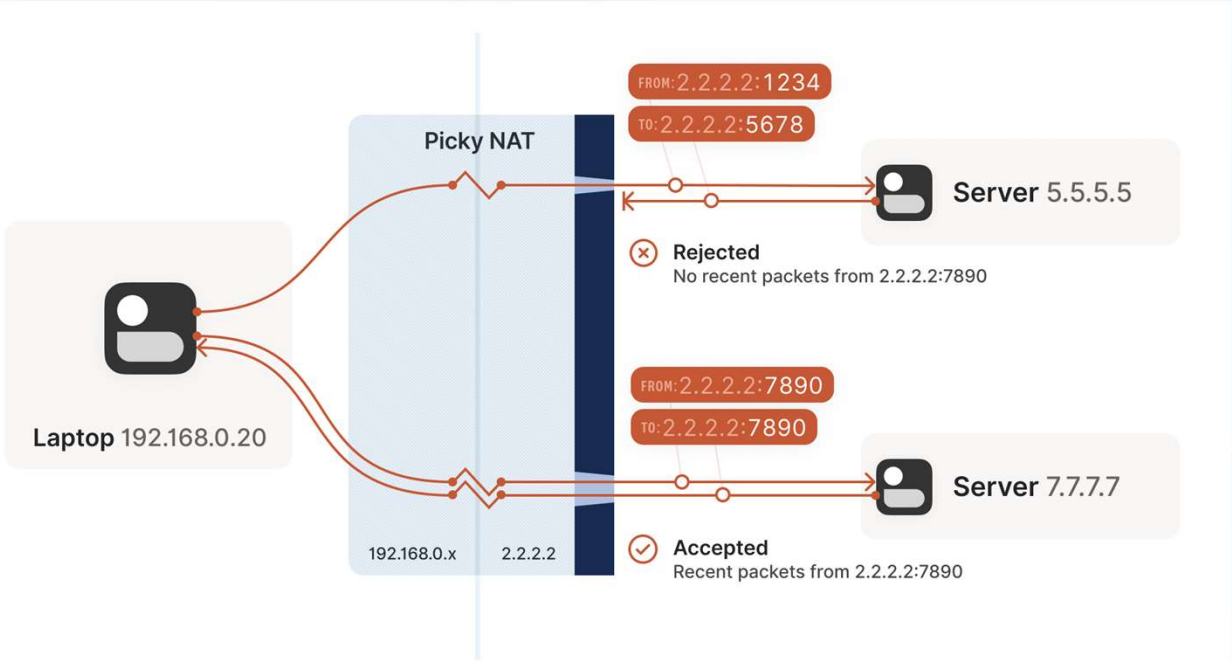
Contoh ACL


Ini adalah tabel
access control
firewall
access-list 101 permit icmp any 192.168.185.0 0.0.0.255 echo-reply
access-list 101 permit icmp any 192.168.185.0 0.0.0.255 ttl-exceeded
access-list 101 permit tcp any 192.168.185.0 0.0.0.255 established
access-list 101 permit udp any host 192.168.185.100 eq 53
access-list 101 permit udp any eq 123 192.168.185.0 0.0.0.255
Komputer
Pengguna

Network Address Translation (NAT)

- NAT (Network Address Translation) Firewall adalah jenis firewall yang bekerja dengan menggunakan teknik Network Address Translation (NAT) untuk mengubah atau mengalihkan alamat IP sumber atau tujuan dalam paket data yang melewati firewall.
- NAT Firewall umumnya digunakan untuk memungkinkan beberapa perangkat dalam jaringan lokal berbagi satu alamat IP publik yang terlihat di Internet.

Ilustrasi NAT Firewall



Cara kerja NAT Firewall (1)

- Private to Public
  - Ketika paket data keluar dari jaringan lokal (private network) ke Internet (public network), NAT Firewall akan mengganti alamat IP sumber dari perangkat dalam jaringan lokal dengan alamat IP publik yang terlihat di dunia luar.
  - Proses ini memungkinkan perangkat-perangkat dalam jaringan lokal untuk berbagi satu alamat IP publik.

Cara kerja NAT Firewall (2)

- Public to Private
  - Ketika paket data masuk dari Internet ke jaringan lokal, NAT Firewall akan mengganti alamat IP tujuan dari paket tersebut dengan alamat IP perangkat di dalam jaringan lokal yang sesuai.
  - Proses ini memastikan bahwa data yang ditujukan ke alamat IP publik tertentu diarahkan ke perangkat yang benar dalam jaringan lokal.

Keuntungan utama NAT Firewall (1)

- Perlindungan terhadap Serangan
  - Karena alamat IP perangkat di jaringan lokal tidak terlihat di luar, ini memberikan tingkat keamanan tambahan dengan mengurangi potensi langsung untuk serangan dari luar.

Keuntungan utama NAT Firewall (2)

- Penyembunyian Topologi Jaringan
  - Alamat IP internal jaringan tidak akan terlihat oleh pihak luar, menjaga kerahasiaan topologi jaringan.

Keuntungan utama NAT Firewall (3)

- Kemampuan Berbagi Koneksi Internet
  - Dengan mengalihkan alamat IP lokal menjadi alamat IP publik, beberapa perangkat dalam jaringan lokal dapat berbagi satu koneksi Internet.

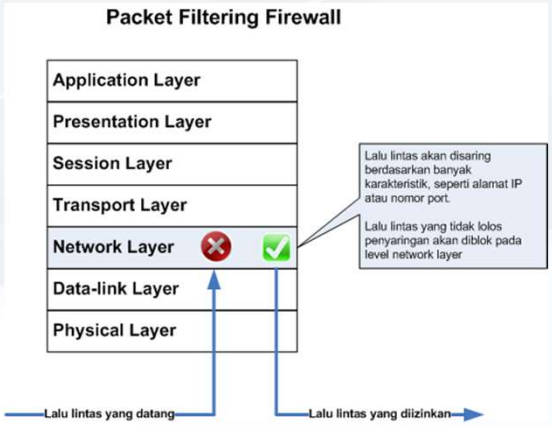
Keuntungan utama NAT Firewall (4)

- Kemampuan Mengatasi Keterbatasan Alamat IPv4
  - Karena alamat IPv4 terbatas, NAT memungkinkan beberapa perangkat dalam jaringan lokal berbagi satu alamat IP publik.

Packet / Traffic Filtering

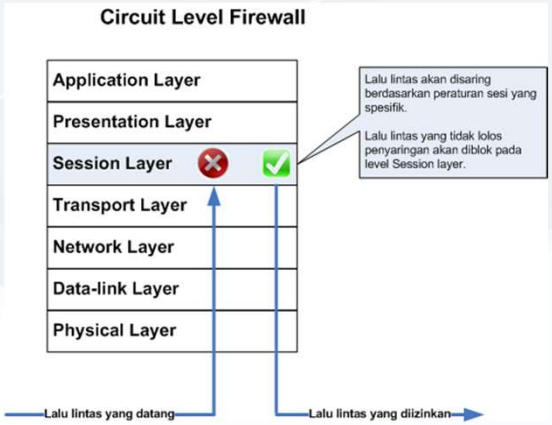
- Packet Filter Firewall adalah jenis firewall yang melakukan pengaturan lalu lintas berdasarkan informasi dalam header paket data.
- Proses ini adalah bentuk dasar dari firewall yang bekerja dengan menganalisis informasi di dalam paket data seperti alamat IP sumber dan tujuan, port sumber dan tujuan, serta protokol yang digunakan.
- Berdasarkan aturan yang telah ditetapkan, firewall ini memutuskan apakah paket tersebut harus diteruskan atau diblokir.

Packet Filtering Firewall



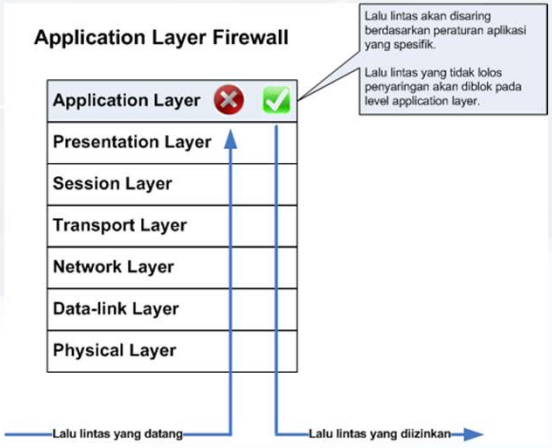
- Pada bentuk yang sederhana, firewall hanya melakukan pengujian terhadap alamat IP atau nama domain yang menjadi sumber paket dan akan menentukan apakah hendak meneruskan atau menolak paket tersebut
- Umumnya, hal ini dilakukan dengan mengaktifkan / menonaktifkan port TCP/IP dalam sistem firewall tersebut.

Circuit Level Firewall



- Firewall ini dianggap lebih aman dibandingkan dengan Packet-Filtering Firewall, karena pengguna eksternal tidak dapat melihat alamat IP jaringan internal dalam paket-paket yang ia terima, melainkan alamat IP dari firewall.
- Protokol yang populer digunakan sebagai Circuit-Level Gateway adalah SOCKS v5.

Application Layer Firewall



- Cara kerja Application-Level Firewall melibatkan pemeriksaan dan analisis mendalam terhadap data yang melewati firewall.
- Jenis Firewall ini bukan hanya tentang mengamati header paket atau koneksi, tetapi juga tentang memahami konten sebenarnya dari data yang dikirimkan.
- Jenis Firewall ini dapat memahami jenis aplikasi atau layanan yang digunakan dalam komunikasi dan menerapkan aturan-aturan yang sangat spesifik untuk melindungi jaringan.

Keuntungan Application-Level Firewall (1)

- Pemahaman Konteks Aplikasi:
  - Firewall ini dapat mengenali jenis aplikasi atau protokol yang digunakan, sehingga dapat memahami konteks dan tujuan dari komunikasi.
  - Misalnya, dapat mengenali lalu lintas HTTP dan memahami permintaan serta tanggapan dalam protokol tersebut.

Keuntungan Application-Level Firewall (2)

- Deteksi Serangan yang Lebih Mendalam
  - Karena firewall ini dapat menganalisis data secara mendalam, firewall mampu mendeteksi serangan yang lebih kompleks, seperti SQL injection, cross-site scripting (XSS), dan ancaman lain yang mungkin tidak terdeteksi oleh jenis firewall yang lebih sederhana.

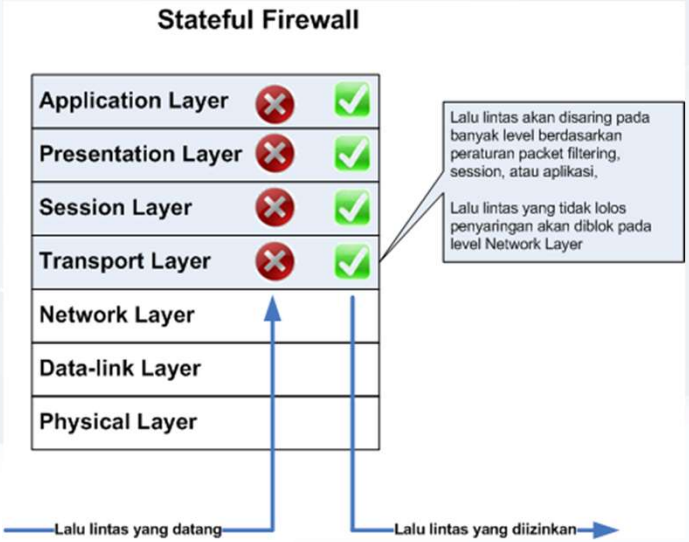
Keuntungan Application-Level Firewall (3)

- Kontrol yang Lebih Ketat
  - Application-Level Firewall memungkinkan pengaturan aturan yang sangat spesifik untuk jenis aplikasi atau layanan tertentu.
  - Tipe firewall jenis ini memberikan fleksibilitas yang lebih besar dalam mengelola lalu lintas dan akses.

Keuntungan Application-Level Firewall (4)

- Penyaringan dan Pemblokiran Berdasarkan Aplikasi
  - Firewall dapat memutus atau memblokir lalu lintas berdasarkan jenis aplikasi atau protokol.
  - Misalnya, memblokir akses ke media sosial atau layanan file sharing tertentu.

Stateful Firewall



- Cara kerja Stateful Firewall melibatkan pemahaman terhadap status koneksi atau sesi yang sedang berlangsung antara sumber dan tujuan dalam komunikasi jaringan.
- Ini memungkinkan firewall untuk memiliki pemahaman yang lebih dalam tentang konteks lalu lintas dan memungkinkannya untuk membuat keputusan yang lebih cerdas berdasarkan sejarah koneksi.

Ciri Utama dari Stateful Firewall (1)

- Pemahaman Status Koneksi:
- Firewall ini dapat mengenali apakah suatu koneksi adalah bagian dari sesi yang sudah ada atau merupakan koneksi baru.
- Hal ini memungkinkan firewall untuk mengevaluasi lalu lintas berdasarkan sejarah dan konteks koneksi.

Ciri Utama dari Stateful Firewall (2)

- Pengecekan Stateful
  - Firewall ini melakukan pengecekan pada level koneksi, memverifikasi apakah setiap paket masuk cocok dengan status koneksi yang ada dalam tabel internalnya.

Ciri Utama dari Stateful Firewall (3)

- Memori Koneksi
  - Stateful Firewall menyimpan informasi tentang koneksi yang sedang aktif dalam tabel koneksi. Ini bisa termasuk informasi tentang alamat IP, port, protokol, dan status koneksi.

Ciri Utama dari Stateful Firewall (4)

- Kontrol Lebih Cerdas
  - Dengan pemahaman tentang status koneksi, firewall ini dapat mengizinkan lalu lintas yang merupakan bagian dari koneksi yang telah diinisiasi oleh komputer dalam jaringan internal dan memblokir lalu lintas yang tidak berhubungan.

Iptables

- Iptables adalah sebuah aplikasi firewall di sistem operasi Linux yang berfungsi untuk mengatur, memfilter, dan memanipulasi lalu lintas jaringan yang melewati kernel Linux.
- Iptables bekerja dengan menggunakan tabel aturan (rules) yang menentukan tindakan yang harus dilakukan terhadap paket data yang masuk atau keluar dari jaringan.

Komponen Utama Iptables (1) - Chains

- Chains: Iptables memiliki beberapa chains default yang digunakan untuk mengorganisir aturan:
  - INPUT: Digunakan untuk memproses paket yang masuk ke server.
  - OUTPUT: Digunakan untuk memproses paket yang keluar dari server.
  - FORWARD: Digunakan untuk memproses paket yang diteruskan melalui server (misalnya, dalam konfigurasi router).

Komponen Utama Iptables (2) - Tables

- Tables: Iptables menggunakan beberapa tabel untuk mengatur jenis operasi tertentu:
  - filter: Tabel default yang digunakan untuk menyaring paket.
  - nat: Tabel yang digunakan untuk Network Address Translation (NAT), seperti pengalihan (port forwarding) dan penerjemahan alamat sumber/destinasi.
  - mangle: Tabel yang digunakan untuk mengubah header paket.
  - raw: Tabel yang digunakan untuk aturan-aturan yang tidak memerlukan koneksi pelacakan.

Komponen Utama Iptables (2) - Rules

- Rules: Setiap chain memiliki daftar aturan yang diterapkan secara berurutan.
- Aturan-aturan ini menentukan tindakan yang harus diambil terhadap paket yang cocok dengan kriteria tertentu.
- Tindakan tersebut dapat berupa:
  - ACCEPT: Menerima paket dan memprosesnya lebih lanjut.
  - DROP: Mengabaikan paket tanpa pemberitahuan.
  - REJECT: Menolak paket dengan mengirimkan pemberitahuan kepada pengirim.
  - LOG: Mencatat informasi tentang paket ke log sistem.

Contoh Penggunaan Iptables (1)

- Memblokir IP tertentu:

```
iptables -A INPUT -s 192.168.1.100 -j DROP
```

- Aturan ini akan memblokir semua paket yang datang dari IP 192.168.1.100.

Contoh Penggunaan Iptables (2)

- Mengizinkan lalu lintas HTTP:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

- Aturan ini akan mengizinkan semua lalu lintas masuk pada port 80 (HTTP).

Contoh Penggunaan Iptables (3)

- Melihat aturan yang ada:
  ```
  iptables -L
  ```
- Perintah ini akan menampilkan semua aturan yang saat ini diterapkan.

Contoh Penggunaan Iptables (4)

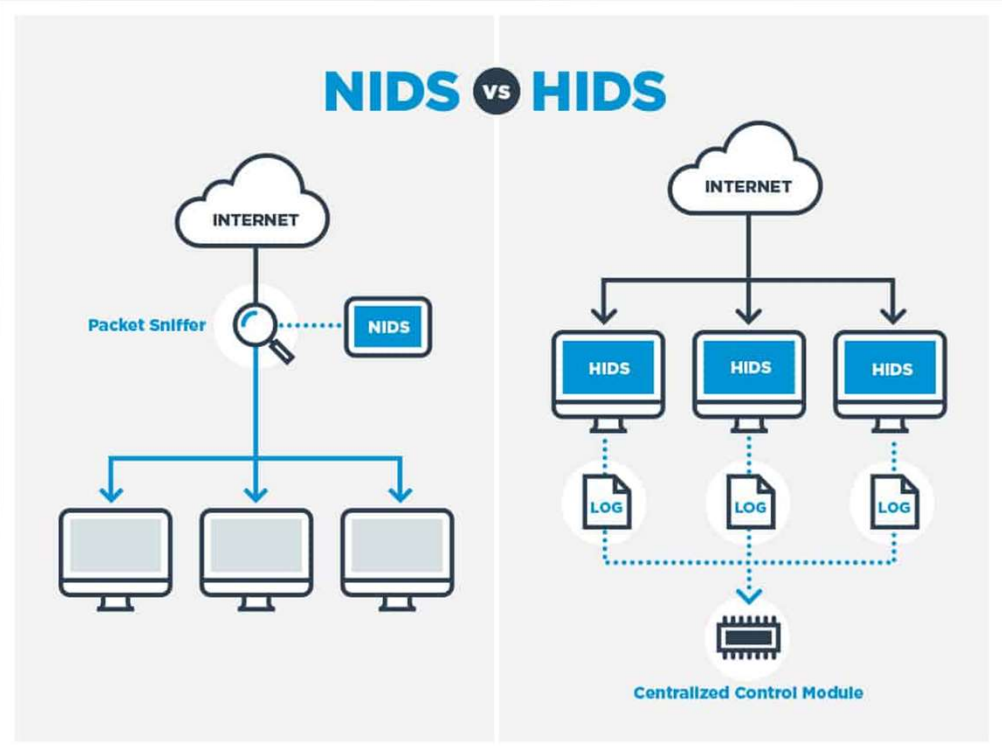
```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

- Penjelasan:
  - Pastikan fitur ip forwarding sudah aktif.
  - Baris pertama mengatur NAT untuk paket yang keluar melalui antarmuka eth0, memungkinkan komputer dalam jaringan lokal menggunakan IP publik dari antarmuka eth0 untuk koneksi internet.
  - Baris kedua mengizinkan paket yang berstatus terkait atau sudah ada (RELATED, ESTABLISHED) untuk diteruskan dari eth0 ke eth1.
  - Baris ketiga mengizinkan semua paket yang masuk dari eth1 dan keluar melalui eth0 untuk diteruskan.

Intrusion Detection System

- Intrusion Detection System adalah teknologi keamanan yang dirancang untuk memantau dan menganalisis lalu lintas jaringan atau aktivitas sistem guna mendeteksi tanda-tanda aktivitas yang berbahaya atau tidak sah.
- Tujuan utama dari IDS adalah untuk mengidentifikasi potensi pelanggaran keamanan, serangan, atau perilaku mencurigakan dalam jaringan atau sistem.

Jenis IDS


NIDS vs HIDS
INTERNET
Packet Sniffer
NIDS
INTERNET
HIDS
HIDS
HIDS
LOG
LOG
LOG
Centralized Control Module

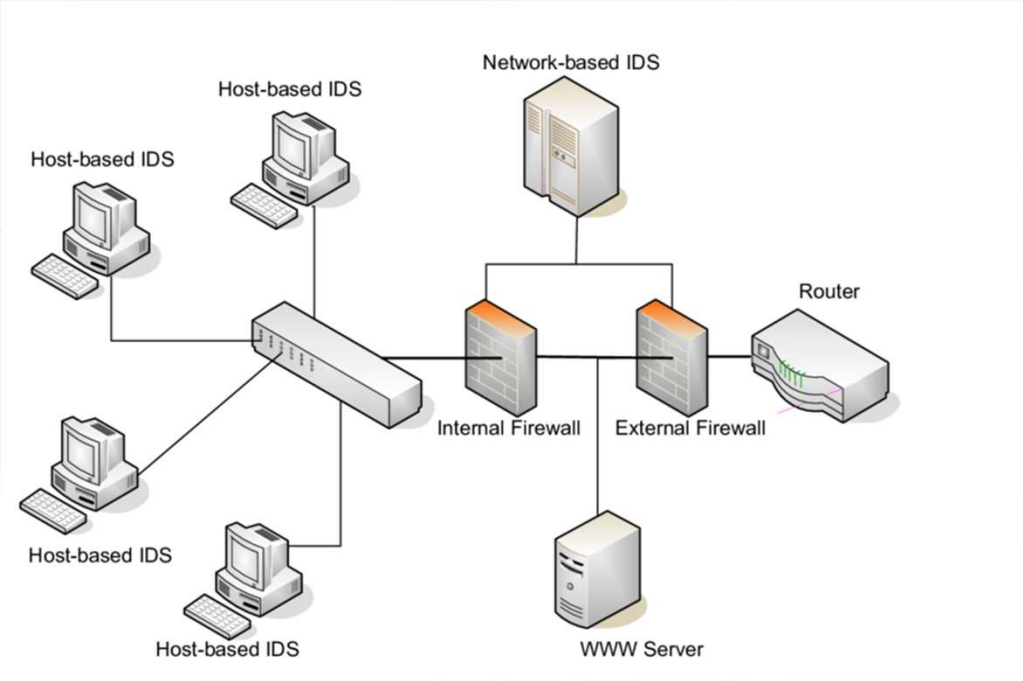
Network-based IDS (NIDS)

- Jenis IDS ini memantau lalu lintas jaringan saat melewati router, switch, dan perangkat jaringan lainnya.
- NIDS menganalisis paket data untuk mengidentifikasi pola yang sesuai dengan tanda tangan serangan yang diketahui atau perilaku yang tidak biasa.
- NIDS dapat ditempatkan pada titik kunci dalam jaringan untuk memonitor lalu lintas yang masuk atau keluar dari segmen tertentu.

Host-based IDS (HIDS)

- Jenis IDS ini beroperasi pada sistem atau host individu.
- HIDS memonitor aktivitas dan peristiwa yang terjadi pada satu sistem, seperti login, perubahan file, dan aktivitas tingkat sistem lainnya.
- HIDS sangat berguna untuk mendeteksi serangan yang berasal dari dalam jaringan atau untuk memantau server kritis dan titik akhir.

Penempatan NIDS dan HIDS



IDS rules

- IDS (Intrusion Detection System) rules, juga dikenal sebagai signatures atau aturan IDS, adalah petunjuk yang digunakan oleh IDS untuk mengidentifikasi serangan atau perilaku mencurigakan dalam lalu lintas jaringan atau aktivitas sistem.
- Setiap aturan berisi pola atau tanda tangan unik yang mencerminkan karakteristik serangan atau aktivitas tertentu.

Komponen IDS rules (1)

- Header
  - Bagian ini berisi informasi umum tentang aturan, seperti ID aturan, nama serangan yang diidentifikasi, dan keterangan singkat tentang serangan tersebut.
- Signature:
  - Bagian utama dari aturan, yang mencakup pola atau urutan data yang harus cocok dengan lalu lintas yang dianalisis.
  - Signature bisa mencakup data dalam header paket, konten payload, atau kombinasi dari keduanya.
  - Signature sering kali berdasarkan tanda-tanda unik dalam serangan atau aktivitas.

Komponen IDS rules (2)

- Kondisi:
  - Beberapa aturan mungkin memiliki kondisi tambahan yang harus dipenuhi sebelum aturan tersebut diterapkan.
  - Data pada bagian ini bisa berupa kondisi yang melibatkan alamat IP, port, protokol, atau aspek lain dari lalu lintas jaringan.
- Aksi:
  - Bagian ini menentukan tindakan yang harus diambil jika aturan cocok dengan lalu lintas yang dianalisis.
  - Tindakan ini bisa berupa log, peringatan, atau tindakan lebih lanjut seperti memblokir lalu lintas.

Contoh IDS rules:

- alert tcp any any -> any 1433 (msg:"Possible SQL Injection Attempt"; content:"' OR '1'='1"; sid:100001;)

Keterangan (1)

- alert tcp any any -> any 1433
  - Definisi dari lalu lintas yang ingin diawasi.
  - Aturan ini berlaku untuk koneksi TCP yang menuju atau berasal dari port 1433.
- msg:"Possible SQL Injection Attempt"
  - Pesan yang akan ditampilkan dalam peringatan jika aturan cocok.

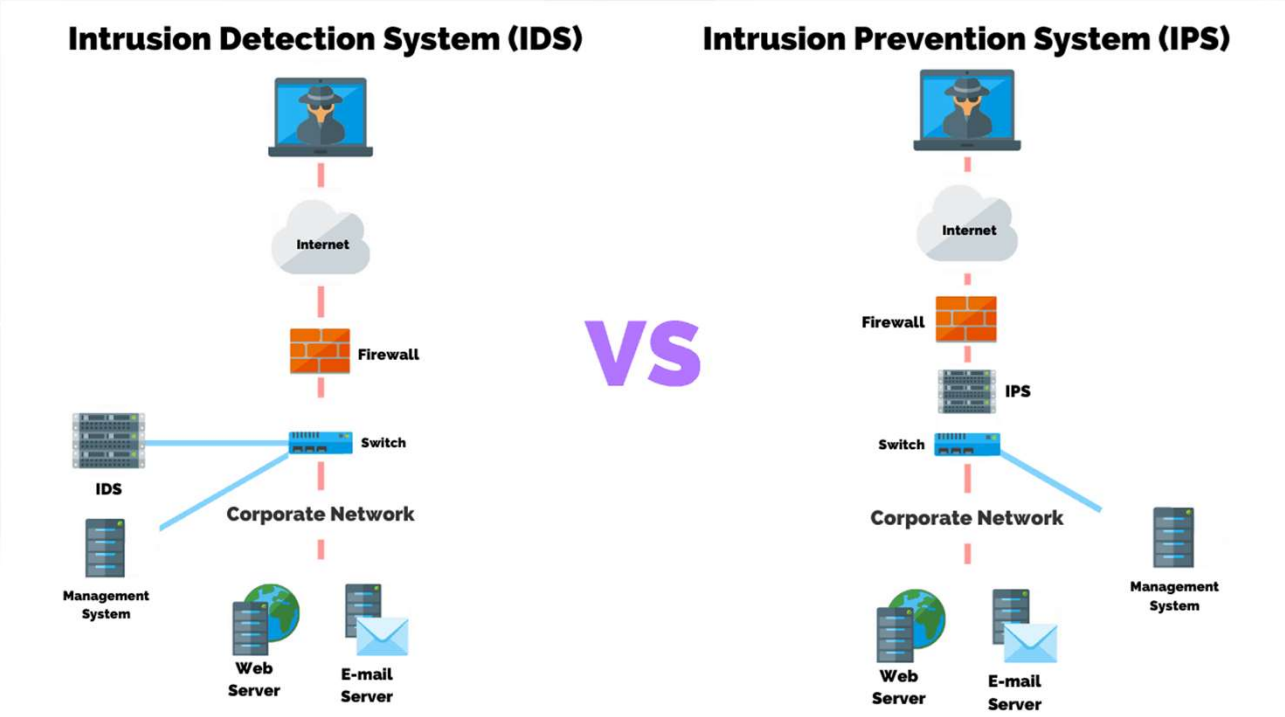
Keterangan (2)

- content:"' OR '1'='1"
  - Signature atau pola yang harus ada dalam lalu lintas untuk aturan ini cocok.
  - Dalam kasus ini, pola ini mencerminkan percobaan SQL injection dengan memasukkan kondisi yang selalu benar.
- Sid:100001
  - Nomor identifikasi unik untuk aturan.

Intrusion Prevention System (IPS)

- IPS adalah sebuah teknologi keamanan yang dirancang untuk mendeteksi dan mencegah serangan yang mencurigakan atau berbahaya pada jaringan atau sistem.
- Berbeda dengan Intrusion Detection System (IDS), yang hanya mendeteksi dan memberikan peringatan tentang serangan, IPS juga mengambil tindakan otomatis untuk mencegah serangan tersebut.

IDS vs IPS


Intrusion Detection System (IDS)
Internet
Firewall
Switch
IDS
Corporate Network
Management System
Web Server
E-mail Server
VS
Intrusion Prevention System (IPS)
Internet
Firewall
IPS
Switch
Corporate Network
Management System
Web Server
E-mail Server

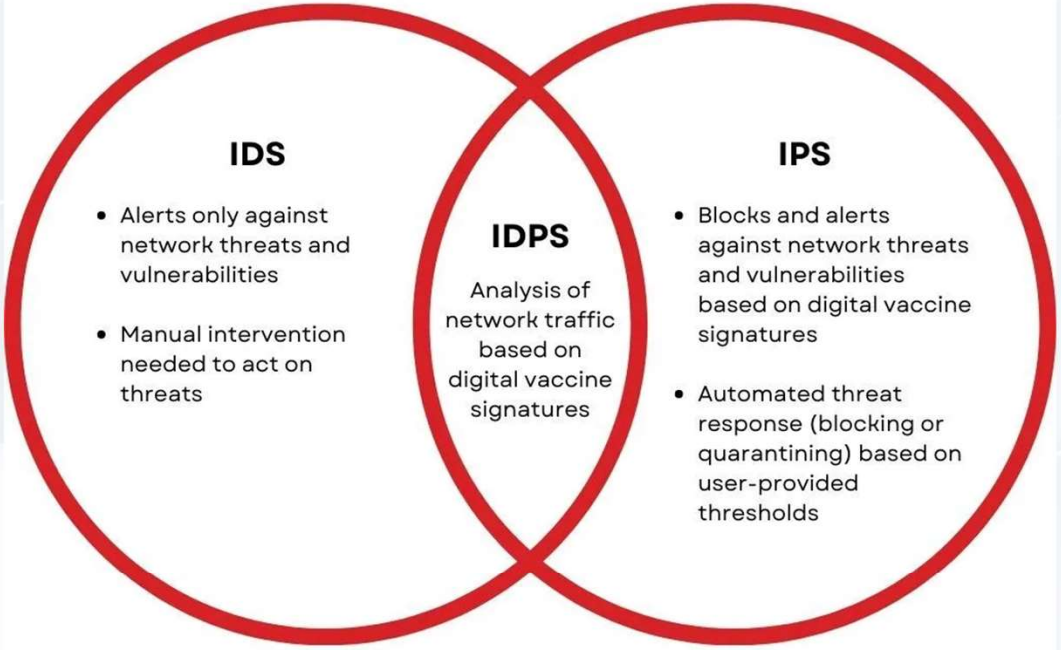
IDS vs. IPS

Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

IDS vs. IPS


IDS
Alerts only against network threats and vulnerabilities
Manual intervention needed to act on threats
IDPS
Analysis of network traffic based on digital vaccine signatures
IPS
Blocks and alerts against network threats and vulnerabilities based on digital vaccine signatures
Automated threat response (blocking or quarantining) based on user-provided thresholds

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI

INSTITUT TEKNOLOGI DAN PENDIDIKAN MAHADEWA · BALI ·

Kampus Merdeka INDONESIA JAYA

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First