Tools Sistem Keamanan Jaringan

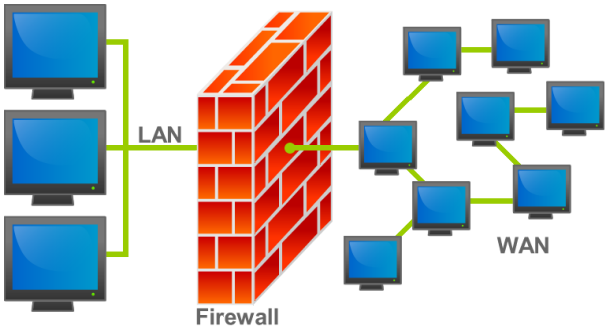
Tools Keamanan Jaringan

Tools keamanan jaringan merupakan perangkat keras maupun lunak yang membantu pengamanan jaringan komputer baik secara preventif (pencegahan) maupun represif.

Setiap tools dikelompokan berdasarkan tipe dari sistem keamanan jaringan itu sendiri seperti Firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), dan Unified Threat Management (UTM). Berikut ini adalah penjelasan masing-masing tipe dari tools keamanan jaringan

Firewall

Firewall merupakan salah satu tipe sistem keamanan pertahanan pertama dalam jaringan karena mengisolasi satu jaringan dari yang lain. Firewall dapat berupa sistem yang berdiri sendiri maupun disertakan dalam perangkat infrastruktur lain seperti router atau server. Dengan kata lain, firewall dapat berupa perangkat keras maupun perangkat lunak beberapa firewall tersedia sebagai peralatan yang berfungsi sebagai perangkat utama yang memisahkan dua jaringan.



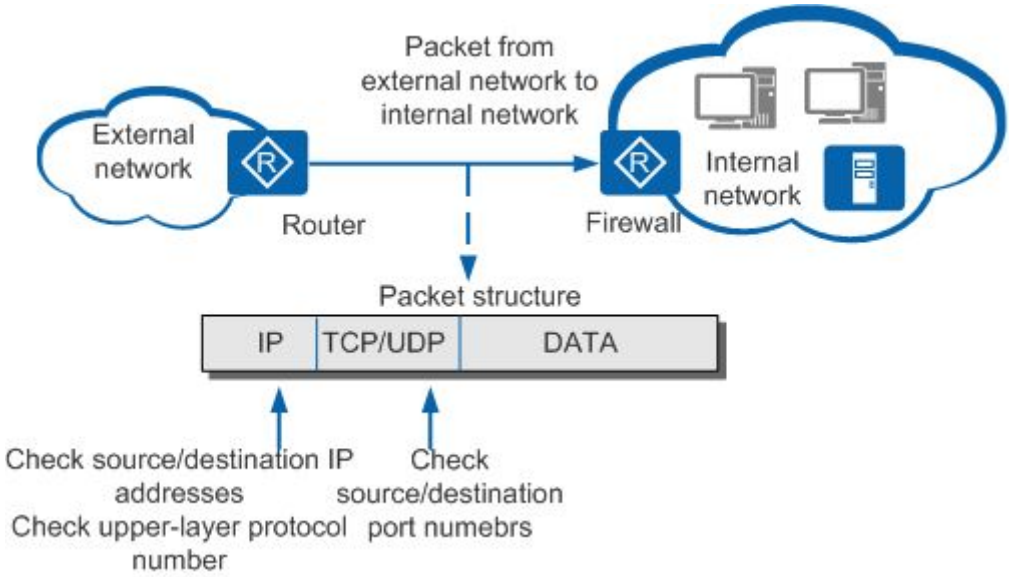
Gambar 1. Konsep Firewall

Firewall dapat memilih lalu lintas jaringan yang tidak diinginkan dan tidak diinginkan untuk memasuki sistem dalam firewall. Pemilihan tersebut didasarkan atas **peraturan organisasi.** Terdapat 2 tipe peraturan umum dalam firewall yaitu:

1. **Whitelisting** - Firewall **menolak semua** koneksi kecuali yang secara khusus terdaftar sebagai **dapat diterima**.
2. **Blacklisting** - Firewall **mengizinkan semua** koneksi kecuali yang secara khusus terdaftar sebagai **tidak dapat diterima**.

Untuk lebih detailnya terdapat empat tipe dari firewall sebagai berikut:

Packet-filtering firewall



Gambar 2. Packet-filtering Firewall

Packet-filtering firewall merupakan jenis firewall keamanan jaringan yang utama dan sederhana. Ini memiliki filter yang membandingkan paket masuk dan keluar dengan seperangkat aturan standar untuk memutuskan apakah akan mengizinkan mereka untuk melewatinya. Dalam kebanyakan kasus, kumpulan aturan (terkadang disebut access list) sudah ditentukan sebelumnya, berdasarkan berbagai metrik. Aturan dapat mencakup alamat IP sumber / tujuan, nomor port sumber / tujuan, dan protokol yang digunakan. Pemfilteran paket terjadi pada Layer 3 dan Layer 4 dari model OSI.

Stateful Packet-filtering firewall

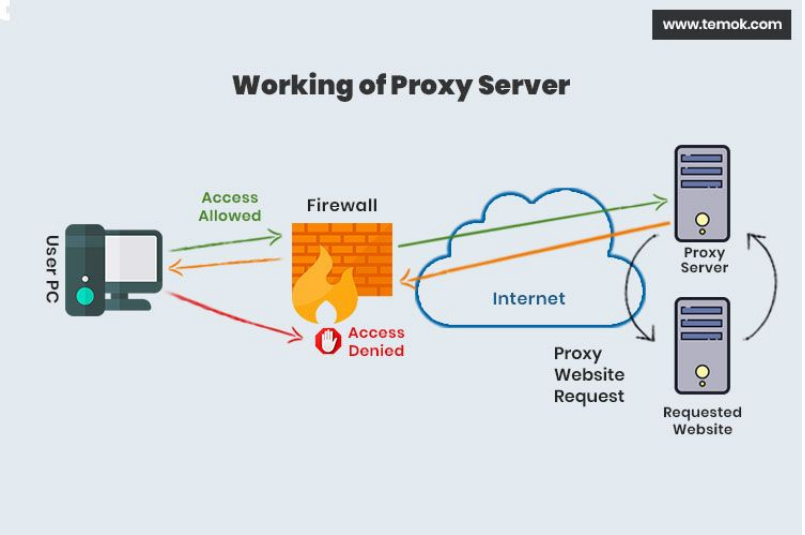
Teknik packet-filtering stateful hampir sama dengan paket filtering biasa namun menggunakan pendekatan yang baik, sambil tetap mempertahankan kemampuan dasar firewall packet-filtering. Hal utama adalah mereka bekerja di Layer 4 dan pasangan koneksi biasanya terdiri dari empat parameter berikut:

- The source address
- The source port
- The destination address
- The destination port

Perbedaan dari packet-filtering biasa yaitu dalam jenis ini, firewall dapat mempertahankan kondisi allow / deny suatu paket ketika paket tersebut sudah pernah melewati firewall tersebut. Tujuannya adalah dapat menghemat memori firewall yang bersangkutan

Proxy firewall

Firewall proxy memiliki target untuk lapisan Aplikasi dalam model OSI untuk operasinya. Proksi tersebut dapat digunakan di antara *remote user* (yang mungkin berada di jaringan publik seperti internet) dan server dedicated di internet. Sebenarnya, remote user tersebut hanya menggunakan sebuah proxy firewall sehingga dia tidak tahu identitas server yang sebenarnya dia komunikasikan. Demikian pula server hanya menemukan proxy dan tidak mengetahui pengguna sebenarnya.



Gambar 2. Firewal dan Proxy

Firewall proxy dapat menjadi mekanisme perisai dan penyaringan yang efektif antara jaringan publik dan jaringan internal atau pribadi yang dilindungi. Firewall jenis ini sangat efektif untuk aplikasi yang memiliki data sensitif karena aplikasi dilindungi oleh proxy dan seluruh tindakan dilakukan hanya pada tingkatan Layer aplikasi OSI,. Skema otentikasi, seperti kata sandi dan biometrik, dapat diatur untuk mengakses proxy, yang memperkuat implementasi keamanan. Sistem proxy ini memungkinkan admin jaringan menyetel firewall untuk menerima atau menolak paket berdasarkan alamat, informasi port, dan informasi aplikasi.

Kerugian utama dalam menggunakan firewall proxy aplikasi adalah kecepatan. Karena aktivitas firewall ini berlangsung di tingkat aplikasi dan melibatkan pemrosesan data dalam jumlah besar, proxy aplikasi dibatasi oleh kecepatan dan biaya. Namun demikian, proxy aplikasi menawarkan beberapa keamanan terbaik dari semua teknologi firewall.

Web application firewall (WAF)

Firewall aplikasi web dibangun untuk memberikan keamanan aplikasi web dengan menerapkan sekumpulan aturan ke percakapan HTTP. Karena aplikasi sedang online, mereka harus menjaga port tertentu tetap terbuka ke internet. Artinya, penyerang dapat

mencoba serangan situs web tertentu terhadap aplikasi dan database terkait, seperti pembuatan cross-site scripting (XSS) and SQL injection..

Sementara firewall proxy umumnya melindungi klien, WAF melindungi server. Fitur hebat lainnya dari WAF adalah bahwa mereka mendeteksi detect distributed denial of service (DDoS) terdistribusi pada tahap awal, menyerap volume lalu lintas dan mengidentifikasi sumber serangan.

Intrusion detection system (IDS)

Intrusion Detection System (disingkat IDS) adalah sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

IDS meningkatkan keamanan siber dengan menemukan peretas atau perangkat lunak berbahaya di jaringan sehingga Anda dapat segera menghapusnya untuk mencegah pelanggaran atau masalah lain, dan menggunakan data yang dicatat tentang peristiwa tersebut untuk lebih melindungi dari insiden intrusi serupa di masa mendatang. Berinvestasi dalam IDS yang memungkinkan Anda merespons serangan dengan cepat bisa jadi jauh lebih murah daripada memperbaiki kerusakan dari serangan dan menangani masalah hukum berikutnya.

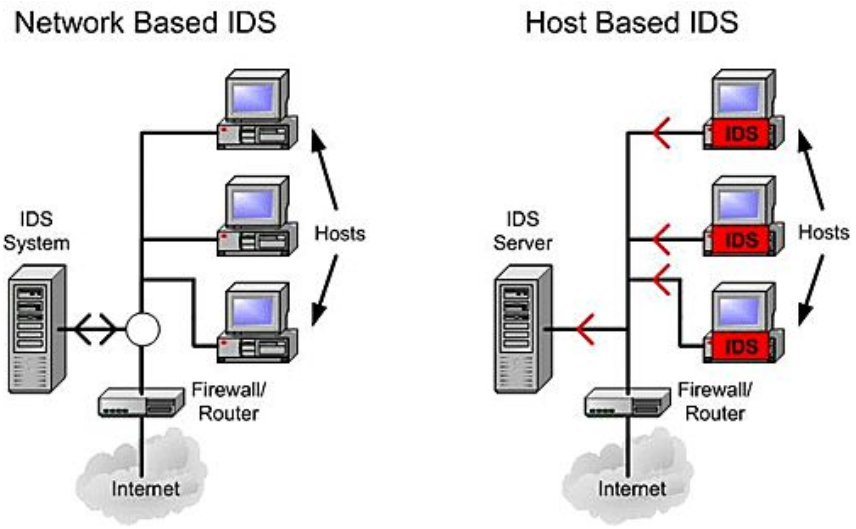
Dari waktu ke waktu, penyerang akan berhasil menyusupkan tindakan keamanan lainnya, seperti kriptografi, firewall, dan sebagainya. Informasi tentang penyusupan ini harus segera mengalir ke administrator - yang dapat dengan mudah diselesaikan menggunakan sistem deteksi intrusi.

Sistem IDS Sendiri dapat dikelompokan menjadi : Host-based, Network-based dan IPS

Host-based IDS

IDS berbasis host dirancang untuk memantau, mendeteksi, dan merespons aktivitas dan serangan pada host tertentu. Dalam kebanyakan kasus, penyerang menargetkan sistem tertentu di jaringan perusahaan yang memiliki informasi rahasia. Mereka akan sering mencoba menginstal program pemindaian dan mengeksploitasi kerentanan lain yang dapat merekam aktivitas pengguna pada host tertentu. Beberapa alat IDS berbasis host menyediakan manajemen kebijakan, analitik statistik, dan forensik data di tingkat host. IDS berbasis host paling baik digunakan saat penyusup mencoba mengakses file tertentu atau layanan lain yang berada di komputer host. Karena penyerang terutama berfokus pada kerentanan sistem operasi untuk membobol host, dalam banyak kasus, IDS berbasis host diintegrasikan ke dalam sistem operasi yang dijalankan oleh host.

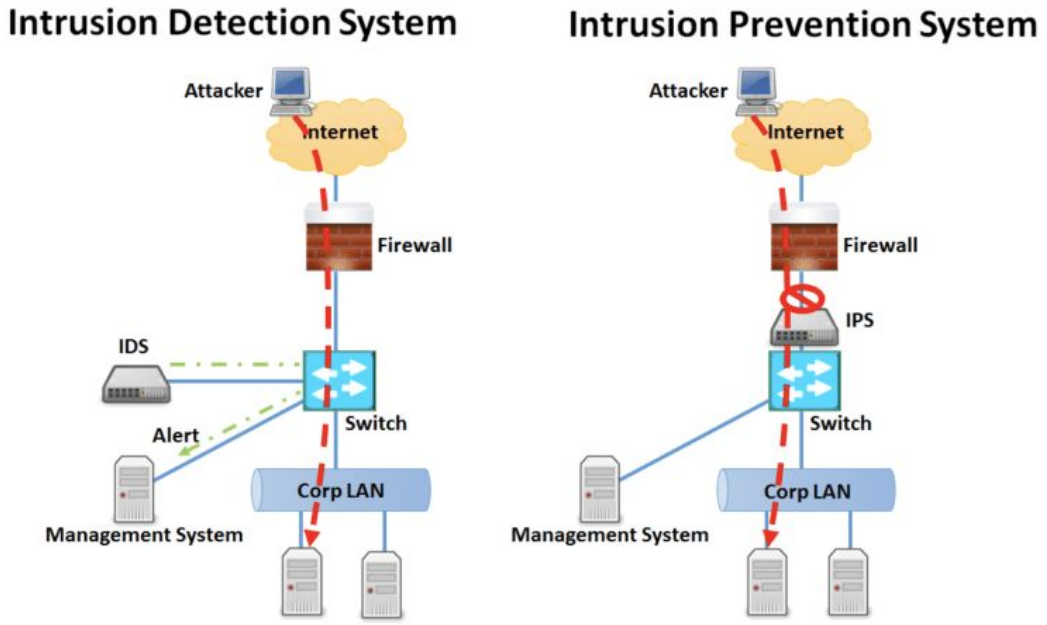
Network-based IDS



Gambar 3. Perbedaan Network dan Host IDS

IDS berbasis lalu lintas jaringan menangkap lalu lintas jaringan untuk mendeteksi penyusup. Paling sering, sistem ini bekerja sebagai sniffer paket yang membaca lalu lintas masuk dan menggunakan metrik khusus untuk menilai apakah jaringan telah disusupi. Berbagai protokol internet dan kepemilikan lainnya yang menangani pesan antara jaringan eksternal dan internal, seperti TCP / IP, NetBEUI, dan XNS, rentan terhadap serangan dan memerlukan cara tambahan untuk mendeteksi peristiwa berbahaya. Seringkali, sistem deteksi intrusi mengalami kesulitan bekerja dengan informasi dan lalu lintas terenkripsi dari jaringan pribadi virtual. Kecepatan di atas 1Gbps juga merupakan faktor penghambat, meskipun IDS berbasis jaringan yang modern dan mahal memiliki kemampuan untuk bekerja dengan cepat melebihi kecepatan ini.

Intrusion prevention system (IPS)



Gambar 4. Perbedaan IDS dan IPS

IPS adalah alat keamanan jaringan yang tidak hanya dapat melakukan penyusup, tetapi juga mencegah mereka menyerang yang diketahui dengan sukses. Sistem pencegahan intrusi menggabungkan kemampuan firewall dan sistem deteksi intrusi. Namun, menerapkan IPS pada skala yang efektif bisa jadi mahal, jadi bisnis harus menilai risiko TI mereka dengan cermat sebelum melakukan investasi. Selain itu, beberapa sistem pencegahan intrusi tidak Cipta dan sekuat beberapa firewall dan sistem deteksi intrusi, jadi IPS mungkin bukan solusi yang tepat ketika kecepatan merupakan syarat mutlak.

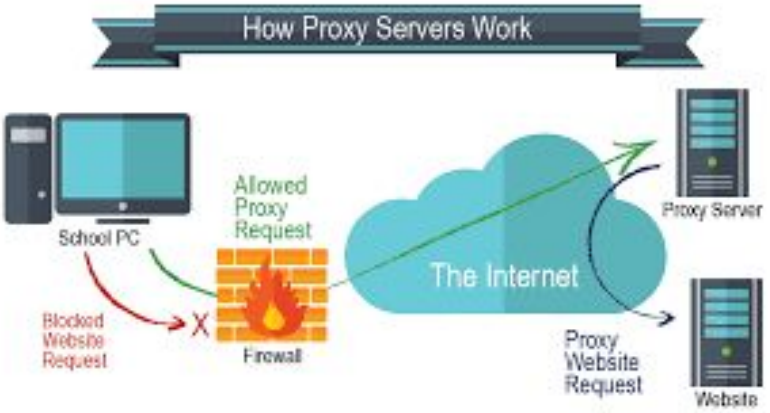
Satu perbedaan penting yang harus dibuat adalah pencegahan antara pencegahan intrusi dan respons aktif. Respons perangkat aktif secara dinamis mengubah atau mengubah jaringan atau akses kontrol, aliran sesi, atau paket individu berdasarkan pemicu dari inspeksi paket dan perangkat deteksi lainnya. Tanggapan aktif terjadi setelah peristiwa tersebut terjadi; dengan demikian, serangan paket tunggal akan berhasil pada percobaan pertama tetapi akan mencoba percobaan selanjutnya; misalnya, serangan DDoS akan berhasil pada paket pertama tetapi akan berubah setelahnya. Meskipun perangkat merespons secara aktif, aspek yang satu ini tidak sesuai sebagai solusi total. Perangkat pencegahan intrusi jaringan, di sisi lain, biasanya adalah perangkat di jaringan yang memeriksa paket dan membuat keputusan sebelum digunakannya ke tujuan. Jenis perangkat ini memiliki kemampuan untuk bertahan terhadap paket serangan tunggal pada upaya pertama yang memiliki atau menyerang secara inline. Yang paling penting, IPS harus melakukan inspeksi dan analisa paket dengan kecepatan kabel. Intrusion prevention system harus melakukan inspeksi paket untuk memeriksa intrusi, termasuk lapisan aplikasi dan serangan zero-day.

Unified threat management (UTM)

Tipe ini merupakan pendekatan keamanan informasi di mana satu instalasi perangkat keras atau perangkat lunak menyediakan beberapa fungsi keamanan (pencegahan intrusi, antivirus, pemfilteran konten, dan sebagainya). Ini kontras dengan metode tradisional yang memiliki solusi titik untuk setiap fungsi keamanan. UTM menyederhanakan manajemen keamanan informasi karena administrator keamanan memiliki satu titik manajemen dan pelaporan daripada harus mengatur beberapa produk dari vendor yang berbeda. Peralatan UTM dengan cepat mendapatkan popularitas, sebagian karena pendekatan all-in-one menyederhanakan pemasangan, konfigurasi, dan pemeliharaan. Pengaturan seperti itu menghemat waktu, uang, dan orang jika dibandingkan dengan pengelolaan beberapa sistem keamanan. Berikut adalah fitur-fitur yang dapat disediakan oleh UTM:

- Network firewall
- Intrusion detection
- Intrusion prevention
- Gateway anti-virus
- Proxy firewall
- Deep packet inspection
- Web proxy and content filtering
- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Virtual private network (VPN)
- Network tarpit

Proxy Server



Gambar 5. Cara kerja Proxy Server

Proxy Server bertindak sebagai negosiator untuk permintaan dari perangkat lunak klien yang mencari sumber daya dari server lain. Seorang klien terhubung ke Proxy Server dan meminta beberapa layanan (misalnya, situs web); Proxy Server mengevaluasi permintaan dan kemudian mengizinkan atau menolaknya. Sebagian besar Proxy Server

bertindak sebagai proxy penerusan dan digunakan untuk mengambil data atas nama klien yang mereka layani.

Jika Proxy Server dapat diakses oleh semua pengguna di internet, maka itu dikatakan sebagai Proxy Server "terbuka". Variasi adalah proxy terbalik, juga dikenal sebagai "pengganti". Ini adalah server internal yang digunakan sebagai front-end untuk mengontrol (dan melindungi) akses ke server di jaringan pribadi. Skenario sebaliknya digunakan untuk tugas-tugas seperti load-balancing, otentikasi, dekripsi, dan caching - respons dari Proxy Server dikembalikan seolah-olah mereka datang langsung dari server asli, sehingga klien tidak memiliki pengetahuan tentang server asli. Firewall aplikasi web (dijelaskan sebelumnya) dapat diklasifikasikan sebagai Proxy Server terbalik.

Proxy bisa transparan atau non transparan. Proksi transparan tidak mengubah permintaan atau tanggapan melebihi apa yang diperlukan untuk otentikasi dan identifikasi proksi; dengan kata lain, klien tidak perlu mengetahui keberadaan proxy. Proxy non transparent mengubah permintaan atau respons untuk menyediakan beberapa layanan tambahan ke agen pengguna, seperti layanan anotasi grup, transformasi jenis media, pengurangan protokol, atau pemfilteran anonimitas.

Dalam penerapannya, Proxy Server biasanya digunakan untuk pemfilteran lalu lintas (filter web) dan peningkatan kinerja (load balancer).

Spam Filter

Mail Gateway dapat digunakan tidak hanya untuk merutekan email tetapi juga untuk melakukan fungsi lain, seperti enkripsi, membatasi email, DLP. Selain itu, filter spam dapat mendeteksi email yang tidak diinginkan dan mencegahnya masuk ke kotak surat pengguna. Filter spam menilai email berdasarkan kebijakan atau pola yang dirancang oleh organisasi atau vendor. Filter yang lebih canggih menggunakan pendekatan heuristik yang mencoba mengidentifikasi spam melalui pola kata atau frekuensi kata yang mencurigakan. Pemfilteran dilakukan berdasarkan aturan yang telah ditetapkan, seperti memblokir email yang berasal dari alamat IP tertentu, email yang berisi kata-kata tertentu di baris subjek, dan sejenisnya. Meskipun filter spam biasanya digunakan untuk memindai pesan masuk, mereka juga dapat digunakan untuk memindai pesan keluar untuk membantu mengidentifikasi PC internal yang mungkin tertular virus.

Anti Virus

Perangkat lunak antivirus adalah salah satu alat keamanan yang paling banyak digunakan oleh individu dan organisasi. Ada berbagai cara solusi antivirus mengenali perangkat lunak berbahaya:

1. **Berdasarkan sign malware yang ada** - sign adalah cara paling populer untuk mendeteksi kode berbahaya. Sign ini pada dasarnya adalah sidik jari malware;

mereka dikumpulkan ke dalam database besar untuk digunakan oleh pemindai antivirus. Itulah mengapa sangat penting bahwa aplikasi antivirus selalu up-to-date - sehingga ada Sign terbaru. Deteksi berbasis Sign bekerja dengan mencari kumpulan kode atau data tertentu. Solusi antivirus membandingkan setiap file, kunci registri, dan program yang sedang berjalan dengan daftar itu dan mengkarantina apa pun yang cocok.

2. Menggunakan heuristik - Teknik yang sedikit lebih maju adalah heuristik. Alih-alih mengandalkan malware yang telah terlihat di alam liar, seperti yang dilakukan oleh Sign, heuristik mencoba mengidentifikasi malware yang sebelumnya tidak terlihat. Deteksi heuristik akan memindai file untuk fitur yang sering terlihat di malware, seperti upaya untuk mengakses sektor boot, menulis ke file EXE atau menghapus konten hard drive. Ambang batas harus ditetapkan oleh administrator untuk menentukan apa yang akan memicu deteksi malware. Ambang batas ini harus disetel dengan tepat agar pemindaian heuristik menjadi efektif. Sign heuristik adalah cara untuk memantau jenis perilaku "buruk" tertentu. Setiap virus memiliki ciri khasnya masing-masing. Karakteristik yang diketahui digunakan untuk membangun pertahanan terhadap virus di masa depan. Meskipun ada virus baru yang dibuat dan didistribusikan hampir setiap hari, virus yang paling umum beredar adalah salinan dari virus lama yang sama. Oleh karena itu, masuk akal untuk menggunakan fakta historis dari virus dan karakteristiknya untuk membuat pertahanan terhadap serangan di masa mendatang.
3. Berdasarkan panjang file - Metode lain untuk mendeteksi virus adalah menggunakan panjang file. Karena virus bekerja dengan menempelkan dirinya ke perangkat lunak sebagai pengganti, durasi perangkat lunak pengganti biasanya bertambah. Perangkat lunak antivirus membandingkan panjang file atau perangkat lunak asli dengan panjang file atau perangkat lunak setiap kali digunakan. Jika kedua panjangnya berbeda, ini menandakan keberadaan virus.
4. Berdasarkan checksum - Checksum adalah nilai yang dihitung dalam file untuk menentukan apakah data telah diubah oleh virus tanpa menambah panjang file. Checksum harus digunakan hanya jika sudah jelas bahwa file tersebut bebas virus saat pertama kali checksum dihitung; jika tidak, checksum dasar tidak valid. Gejala virus biasanya tergantung pada jenis virusnya. Ingatlah bahwa gejala tidak hanya terjadi pada satu virus; beberapa virus dapat memiliki gejala yang serupa. Beberapa gejala yang paling umum adalah sebagai berikut:
    - Komputer reboot yang sering atau tidak terduga
    - Ukuran data dan perangkat lunak tiba-tiba meningkat
    - Perubahan ekstensi file (umum dengan ransomware)
    - Hilangnya file data
    - Kesulitan menyimpan file yang terbuka
    - Kekurangan memori
    - Adanya suara atau teks yang aneh

Antivirus dapat menjadi bagian dari sistem perlindungan titik akhir yang tidak hanya menyediakan perlindungan virus saja namun juga memiliki fitur DLP, AppLocker, pemfilteran konten, dan kemampuan lainnya.