Keamanan Internet AVG 2012

Panduan Pengguna

Revisi dokumen 2012.20 (3/29/2012)

Daftar Isi

1. Pendahuluan

Panduan pengguna ini memberikan dokumentasi yang komprehensif untuk **Keamanan Intenet AVG 2012**.

Keamanan Intenet AVG 2012 menyediakan beberapa lapis perlindungan untuk segala hal yang Anda lakukan online, yang berarti Anda tidak perlu khawatir dengan pencurian identitas, virus, atau mengunjungi situs berbahaya. Teknologi Awan Pelindung AVG dan Jaringan Perlindungan Komunitas AVG disertakan, yang artinya kami mengumpulkan informasi ancaman terbaru dan membaginya dengan komunitas kami untuk memastikan Anda menerima perlindungan terbaik:

- Berbelanja dan perbankan online secara aman dengan Firewall, Anti-Spam & AVG Identity Protection
- Tetap aman di jaringan sosial dengan AVG Social Networking Protection
- Jelajahi dan telusuri dengan penuh keyakinan bersama perlindungan seketika LinkScanner

2. Persyaratan Instalasi AVG

2.1. Sistem Operasi yang Didukung

Keamanan Intenet AVG 2012 ditujukan untuk melindungi workstation dengan sistem operasi berikut:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 dan x64, semua edisi)
- Windows 7 (x 86 dan x64, semua edisi)

(dan mungkin service pack yang lebih tinggi untuk sistem operasi tertentu)

***Catatan**: Komponen Identity Protection tidak didukung pada Windows XP x64. Pada sistem operasi ini Anda dapat menginstal Keamanan Intenet AVG 2012 tetapi tanpa komponen IDP.*

2.2. Persyaratan PK Minimum & yang Disarankan

Persyaratan perangkat keras minimum untuk **Keamanan Intenet AVG 2012**:

- Intel Pentium CPU 1,5 GHz
- memori RAM 512 MB
- 1.000 MB ruang kosong hard drive (untuk keperluan instalasi)

Persyaratan perangkat keras yang disarankan untuk **Keamanan Intenet AVG 2012**:

- Intel Pentium CPU 1,8 GHz
- memori RAM 512 MB
- 1.550 MB ruang kosong hard drive (untuk keperluan instalasi)

3. Proses Instalasi AVG

Ke mana saya mendapatkan file instalasi?

Untuk menginstal **Keamanan Intenet AVG 2012** pada komputer Anda, Anda perlu mendapatkan file instalasi terbaru. Untuk memastikan Anda menginstal versi **Keamanan Intenet AVG 2012** terbaru, Anda sebaiknya mengunduh file instalasi dari situs Web AVG (http://www.avg.com/). Bagian ***Pusat Dukungan/Unduh*** menyediakan tinjauan umum terstruktur atas file instalasi bagi setiap edisi AVG.

Jika Anda tidak yakin file mana yang perlu diunduh dan diinstal, Anda mungkin perlu menggunakan layanan ***Pilih produk*** di bagian bawah halaman Web. Setelah Anda menjawab tiga pertanyaan sederhana, layanan ini akan menetapkan file yang Anda perlukan. Tekan tombol ***Lanjutkan*** agar dialihkan ke daftar lengkap file unduhan yang telah disesuaikan untuk kebutuhan pribadi Anda.

Seperti apa proses instalasi tersebut?

Setelah Anda mengunduh dan menyimpan file instalasi pada hard disk, Anda dapat meluncurkan proses instalasi. Instalasi adalah serentetan dialog sederhana dan mudah dipahami. Setiap dialog secara ringkas menerangkan apa yang dilakukan setiap langkah pada proses instalasi. Berikut ini, kami menawarkan penjelasan terperinci atas setiap jendela dialog:

3.1. Selamat Datang: Pemilihan Bahasa

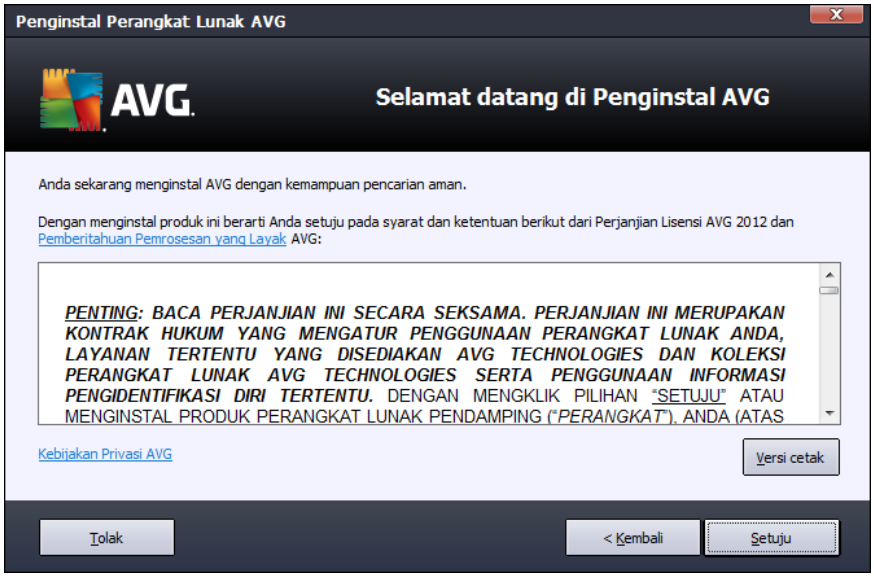
Proses instalasi dimulai dengan dialog ***Selamat datang di AVG Installer***:

Di dialog ini, Anda dapat memilih bahasa yang digunakan untuk proses instalasi. Di sudut kanan dialog, klik kotak kombo untuk menyusuri menu bahasa. Pilih bahasa yang diinginkan, dan proses instalasi akan dilanjutkan dalam bahasa yang Anda pilih.

Perhatian: Di saat ini, Anda hanya memilih bahasa untuk proses instalasi. Aplikasi Keamanan Intenet AVG 2012 akan diinstal dalam bahasa yang dipilih, dan dalam bahasa Inggris, yang selalu diinstal secara otomatis. Walau demikian, bisa saja menginstal bahasa lainnya dan menggunakan Keamanan Intenet AVG 2012 dalam salah satu bahasa ini. Anda akan diminta mengkonfirmasi pilihan bahasa alternatif dalam salah satu dialog pengaturan berikut bernama Opsi Khusus.

3.2. Selamat Datang: Perjanjian Lisensi

Pada langkah selanjutnya, dialog ***Selamat datang di AVG Installer*** menyediakan teks lengkap mengenai perjanjian lisensi AVG:



Silakan baca keseluruhan teks dengan seksama. Untuk mengonfirmasi bahwa Anda telah membaca, memahami dan menerima perjanjian, tekan tombol ***Terima***. Jika Anda tidak setuju dengan perjanjian lisensi tersebut, tekan tombol ***Tolak***, maka proses instalasi akan segera diakhiri.

Kebijakan Privasi AVG

Di samping perjanjian lisensi, dialog pengaturan ini juga menawarkan opsi untuk mempelajari lagi tentang kebijakan privasi AVG. Di sudut kiri bawah dialog Anda dapat melihat tautan ***Kebijakan Privasi AVG***. Klik agar dialihkan ke situs Web AVG (http://www.avg.com/) di mana Anda dapat menemukan prinsip-prinsip kebijakan privasi AVG Technologies selengkapnya.

Tombol kontrol

Dalam dialog pengaturan pertama, hanya ada dua tombol kontrol yang tersedia:

- ***Versi cetak*** – Klik untuk mencetak teks lengkap perjanjian lisensi AVG.

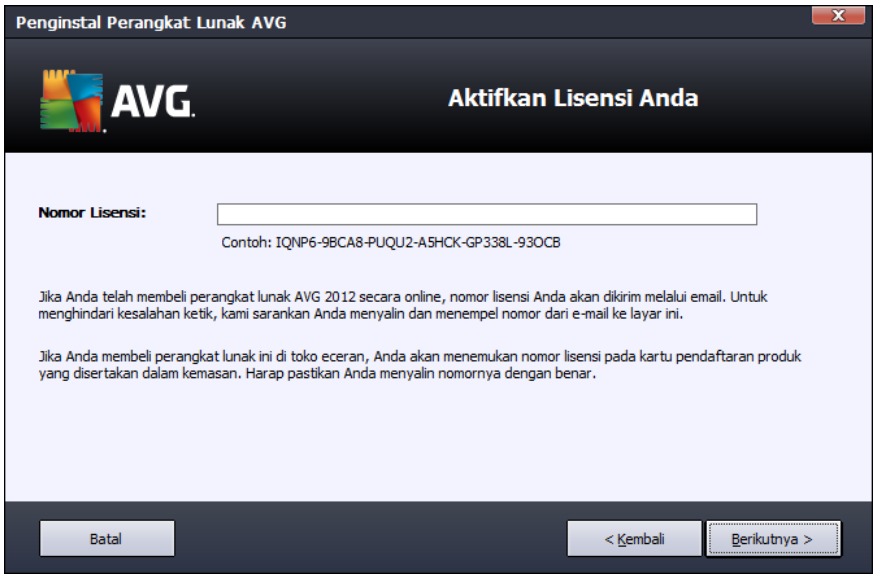
- ***Tolak*** – Klik untuk menolak perjanjian lisensi. Proses pengaturan akan segera ditutup. **Keamanan Intenet AVG 2012** tidak akan diinstal!

- ***Kembali*** – Klik untuk mundur satu langkah ke dialog pengaturan sebelumnya.

- ***Terima*** – Klik untuk mengkonfirmasi bahwa Anda telah membaca, memahami, dan menerima perjanjian lisensi. Instalasi akan dilanjutkan, dan Anda akan maju satu langkah ke dialog pengaturan berikut.

3.3. Aktifkan lisensi Anda

Dalam dialog ***Aktifkan Lisensi Anda***, Anda diminta untuk memasukkan nomor lisensi ke dalam bidang teks yang disediakan:



Tempat menemukan nomor lisensi

Nomor penjualan dapat ditemukan pada kemasan CD di kotak **Keamanan Intenet AVG 2012** Anda. Nomor lisensi ada dalam email konfirmasi yang telah Anda terima setelah membeli **Keamanan Intenet AVG 2012** Anda secara online. Anda harus mengetikkan angkanya persis seperti yang ditampilkan. Jika tersedia bentuk digital dari nomor lisensi tersebut (*dalam email*), disarankan menggunakan metode salin dan tempel untuk memasukkannya.

Cara menggunakan metode Salin & Tempel

Dengan metode ***Salin & Tempel*** untuk memasukkan nomor lisensi **Keamanan Intenet AVG 2012** Anda ke program akan memastikan nomor tersebut dimasukkan dengan benar. Harap ikuti langkah-langkah ini:

- Buka e-mail yang berisi nomor lisensi Anda.

- Klik tombol kiri mouse di permulaan nomor lisensi, tahan dan seret mouse ke ujung nomor, kemudian lepaskan tombol. Nomor tersebut sekarang telah disorot.
- Tekan terus ***Ctrl***, kemudian tekan ***C***. Ini akan menyalin nomor tersebut.
- Arahkan dan klik posisi tempat Anda ingin menempelkan nomor yang telah disalin.
- Tekan terus ***Ctrl***, kemudian tekan ***V***. Ini akan menempelkan nomor tersebut ke lokasi yang Anda pilih.

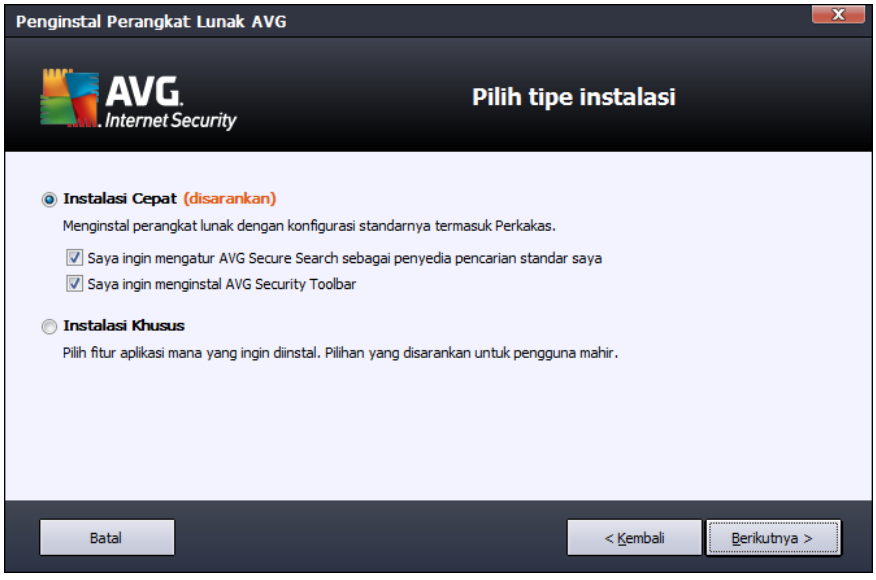
Tombol kontrol

Sebagaimana dalam dialog pengaturan pada umumnya, ada tiga tombol kontrol yang tersedia:

- ***Batalkan*** – Klik untuk keluar dari proses pengaturan dengan segera; **Keamanan Intenet AVG 2012** tidak akan diinstal!
- ***Kembali*** – Klik untuk mundur satu langkah ke dialog pengaturan sebelumnya.
- ***Berikutnya*** – Klik untuk melanjutkan instalasi dan maju satu langkah.

3.4. Pilih tipe instalasi

Dialog ***Pilih tipe instalasi*** menawarkan dua pilihan opsi instalasi: ***Cepat*** dan ***Instal Khusus***:



Instalasi cepat

Untuk sebagian besar pengguna, sangat disarankan untuk tetap menggunakan instalasi ***Cepat***

standar yang akan menginstal **Keamanan Intenet AVG 2012** dalam mode otomatis penuh dengan pengaturan yang telah ditetapkan oleh vendor program, termasuk Gadget AVG. Konfigurasi ini menyediakan keamanan maksimum yang dikombinasikan dengan penggunaan sumber daya yang optimal. Di masa mendatang, jika perlu mengubah konfigurasi, Anda akan selalu dapat melakukannya secara langsung dalam aplikasi **Keamanan Intenet AVG 2012**.

Dalam opsi ini, Anda dapat melihat dua kotak centang yang telah dikonfirmasi sebelumnya, dan sangat disarankan untuk tetap menandainya keduanya:

- ***Saya ingin mengatur AVG Secure Search sebagai penyedia penelusuran default saya*** – tetap tandai untuk mengonfirmasi bahwa Anda ingin menggunakan mesin AVG Secure Search yang bekerja sama sangat dekat dengan komponen LinkScanner untuk keamanan maksimum Anda secara online.

- ***Saya ingin menginstal AVG Security Toolbar*** – tetap tandai untuk menginstal AVG Security Toolbar yang menjaga keamanan maksimum Anda ketika menjelajah Internet.

Tekan tombol ***Berikutnya*** untuk melanjutkan ke dialog Instal AVG Security Toolbar berikut ini.

Instalasi khusus

Instal Khusus hanya boleh digunakan oleh pengguna berpengalaman dengan alasan yang kuat untuk menginstal **Keamanan Intenet AVG 2012** dengan pengaturan non-standar, misalnya, agar pas dengan persyaratan sistem tertentu.

Jika Anda memutuskan memilih opsi ini, bagian baru yang disebut ***Folder Tujuan*** muncul di dialog. Di sini, Anda harus menentukan lokasi di mana **Keamanan Intenet AVG 2012** harus diinstal. Secara default, **Keamanan Intenet AVG 2012** akan diinstal ke folder file program di drive C:, sebagaimana dinyatakan di bidang teks pada dialog. Jika Anda ingin mengubah lokasi ini, gunakan tombol ***Jelajah*** untuk menampilkan struktur drive dan pilih folder yang diinginkan. Untuk kembali ke tujuan default yang ditentukan sebelumnya oleh vendor perangkat lunak, gunakan tombol ***Default***.

Setelah itu, tekan tombol ***Berikutnya*** untuk melanjutkan ke dialog Opsi Khusus.

Tombol kontrol

Sebagaimana dalam dialog pengaturan pada umumnya, ada tiga tombol kontrol yang tersedia:

- ***Batalkan*** – Klik untuk keluar dari proses pengaturan dengan segera; **Keamanan Intenet AVG 2012** tidak akan diinstal!

- ***Kembali*** – Klik untuk mundur satu langkah ke dialog pengaturan sebelumnya.

- ***Berikutnya*** – Klik untuk melanjutkan instalasi dan maju satu langkah.

3.5. Opsi Khusus

Dialog ***Opsi Khusus*** memungkinkan Anda menentukan parameter terperinci pada instalasi:

Bagian ***Pemilihan Komponen*** menampilkan gambaran umum mengenai semua komponen **Keamanan Intenet AVG 2012** yang dapat diinstal. Jika pengaturan default tidak cocok untuk Anda, Anda dapat menghapus/menambah komponen tertentu.

Walau demikian, Anda hanya dapat memilih dari komponen yang telah disertakan dalam edisi AVG yang dibeli!

Sorot pilihan apa pun dalam daftar ***Pilihan Komponen***, dan keterangan singkat tentang komponen tersebut akan ditampilkan pada sisi kanan bagian ini. Untuk informasi terperinci tentang fungsionalitas masing-masing komponen, harap lihat bab Tinjauan Umum Komponen dalam dokumentasi ini. Untuk kembali ke konfigurasi default yang ditentukan sebelumnya oleh vendor perangkat lunak, gunakan tombol ***Default***.

Tombol kontrol

Sebagaimana dalam dialog pengaturan pada umumnya, ada tiga tombol kontrol yang tersedia:

- ***Batalkan*** – Klik untuk keluar dari proses pengaturan dengan segera; **Keamanan Intenet AVG 2012** tidak akan diinstal!
- ***Kembali*** – Klik untuk mundur satu langkah ke dialog pengaturan sebelumnya.
- ***Berikutnya*** – Klik untuk melanjutkan instalasi dan maju satu langkah.

3.6. Instal AVG Security Toolbar

Dalam dialog ***Instal AVG Security Toolbar*** putuskan apakah Anda ingin menginstal fitur AVG Security Toolbar. Jika Anda tidak mengubah pengaturan default, komponen ini akan diinstal secara otomatis ke dalam peramban Internet Anda (*peramban yang saat ini didukung adalah Microsoft Internet Explorer v. 6.0 atau yang lebih tinggi, dan Mozilla Firefox v. 3.0 atau yang lebih tinggi*) untuk memberi Anda suatu perlindungan online yang komprehensif selagi menjelajah Internet.

Selain itu, Anda punya opsi untuk memutuskan apakah Anda ingin memilih *AVG Secure Search (powered by Google)* sebagai penyedia penelusuran default Anda. Jika demikian, biarkan kotak ini tetap ditandai.

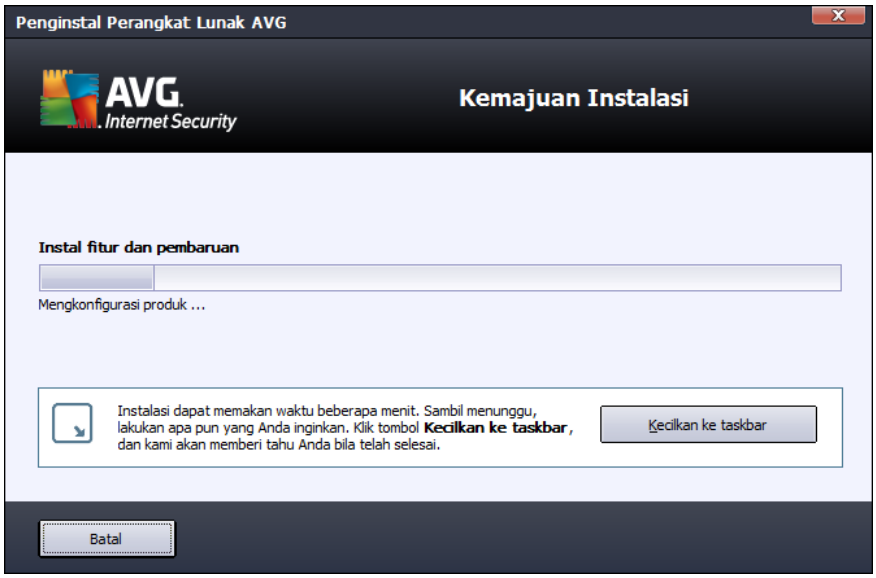
Tombol kontrol

Sebagaimana dalam dialog pengaturan pada umumnya, ada tiga tombol kontrol yang tersedia:

- ***Batalkan*** – Klik untuk keluar dari proses pengaturan dengan segera; **Keamanan Intenet AVG 2012** tidak akan diinstal!
- ***Kembali*** – Klik untuk mundur satu langkah ke dialog pengaturan sebelumnya.
- ***Berikutnya*** – Klik untuk melanjutkan instalasi dan maju satu langkah.

3.7. Kemajuan Instalasi

Dialog ***Kemajuan Instalasi*** menampilkan kemajuan proses instalasi, dan tidak memerlukan campur-tangan apapun:



Setelah proses instalasi selesai, Anda akan dialihkan ke dialog berikutnya secara otomatis.

Tombol kontrol

Dalam dialog ini, hanya ada satu tombol kontrol yang tersedia – ***Batal***. Tombol ini seharusnya hanya digunakan jika Anda ingin menghentikan proses instalasi yang sedang dijalankan. Harap diingat bahwa dalam hal demikian **Keamanan Intenet AVG 2012** Anda tidak akan diinstal!

3.8. Instalasi berhasil

Dialog ***Instalasi berhasil*** mengkonfirmasi bahwa **Keamanan Intenet AVG 2012** Anda telah terinstal lengkap dan dikonfigurasi:

Program Peningkatan Produk

Di dialog ini, Anda dapat memutuskan apakah Anda ingin berpartisipasi dalam Program Peningkatan Produk (*untuk perinciannya, lihat bab Pengaturan Lanjutan AVG/Program Peningkatan Produk*) yang mengumpulkan informasi anonim mengenai ancaman yang terdeteksi guna meningkatkan tingkatan keamanan Internet secara keseluruhan. Jika Anda setuju dengan pernyataan ini, harap biarkan opsi ***Saya setuju ikut serta dalam keamanan Web AVG 2012 dan Program Peningkatan Produk...*** tetap ditandai *(opsi telah dikonfirmasi secara default)*.

Komputer dihidupkan ulang

Untuk menyelesaikan proses instalasi Anda perlu menghidupkan ulang komputer Anda, pilih apakah Anda ingin ***Hidupkan Ulang Sekarang***, atau Anda ingin menunda tindakan ini – ***Hidupkan Ulang Nanti***.

4. Setelah Instalasi

4.1. Pendaftaran produk

Setelah menyelesaikan instalasi **Keamanan Intenet AVG 2012** daftarkan produk Anda secara online pada situs Web AVG (http://www.avg.com/). Setelah pendaftaran, Anda akan mendapatkan akses penuh ke Akun pengguna AVG, berita Pembaruan AVG, dan layanan lain yang disediakan khusus untuk pengguna terdaftar.

Cara termudah untuk mendaftar adalah langsung dari antarmuka pengguna **Keamanan Intenet AVG 2012**. Dalam menu utama, harap pilih item Bantuan/Daftarkan sekarang. Anda akan dialihkan ke halaman ***Pendaftaran*** pada situs Web AVG (http://www.avg.com/). Harap ikuti petunjuk yang diberikan di halaman tersebut.

4.2. Akses ke antarmuka pengguna

Dialog utama AVG dapat diakses dengan beberapa cara:

- klik dua kali ikon baki sistem AVG
- klik dua kali ikon AVG di desktop
- dari menu ***Start/All Programs/AVG 2012***

4.3. Pemindaian seluruh komputer

Ada kemungkinan risiko bahwa virus komputer telah terkirim ke komputer Anda sebelum instalasi **Keamanan Intenet AVG 2012**. Karena alasan ini, Anda harus menjalankan Pemindaian seisi komputer untuk memastikan tidak ada infeksi pada PC Anda. Pemindaian pertama mungkin membutuhkan beberapa waktu *(sekitar 1 jam)* namun disarankan untuk memulainya untuk memastikan komputer Anda tidak terganggu oleh ancaman. Untuk petunjuk mengenai menjalankan Pemindaian seisi komputer bacalah bab Pemindaian AVG.

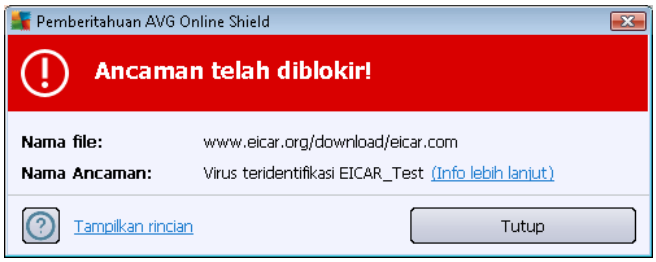
4.4. Tes Eicar

Untuk mengkonfirmasi bahwa **Keamanan Intenet AVG 2012** telah diinstal dengan benar, Anda dapat menjalankan tes EICAR.

Tes EICAR adalah metode standar dan benar-benar aman untuk memeriksa fungsi sistem antivirus. Ini aman diedarkan, karena ia bukan virus sungguhan, dan tidak berisi potongan kode virus. Kebanyakan produk bereaksi seolah-olah ia virus (*tetapi produk-produk tersebut biasanya melaporkannya dengan nama yang jelas, seperti "EICAR-AV-Test"*). Anda dapat mengunduh virus EICAR dari situs Web EICAR di www.eicar.com, dan di sana Anda juga akan menemukan semua informasi tes EICAR yang diperlukan.

Cobalah mengunduh file ***eicar.com***, dan simpan di disk lokal Anda. Segera setelah Anda mengonfirmasi mengunduh file tes, Online Shield (*bagian dari komponen LinkScanner*) akan bereaksi padanya dengan sebuah peringatan. Pemberitahuan ini menunjukkan bahwa AVG telah

terinstal pada komputer Anda dengan benar.



Dari situs Web http://www.eicar.com Anda juga dapat mengunduh versi terkompresi dari 'virus' EICAR (*yakni dalam bentuk eicar_com.zip*). Online Shield memungkinkan Anda mengunduh file ini dan menyimpannya ke disk lokal Anda namun kemudian Resident Shield (*dalam komponen Anti-Virus*) mendeteksi 'virus' saat Anda mencoba membukanya.

Jika AVG gagal mengenali file tes EICAR sebagai virus, Anda harus memeriksa lagi konfigurasi program!

4.5. Konfigurasi default AVG

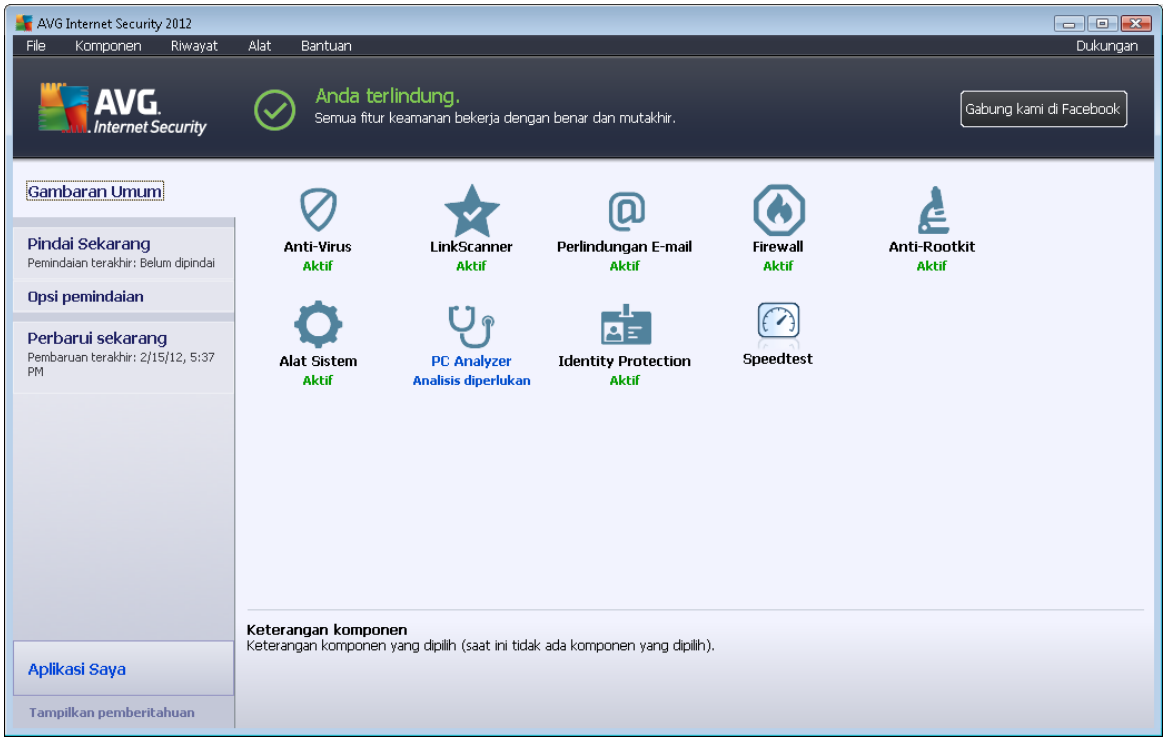
Konfigurasi default (*yakni cara aplikasi diatur tepat setelah instalasi*) **Keamanan Intenet AVG 2012** telah diatur oleh vendor perangkat lunak sehingga semua komponen dan fungsi telah disesuaikan untuk mencapai performa optimal.

Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG! Perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman.

Beberapa pengeditan kecil pada pengaturan Komponen AVG dapat diakses langsung dari antarmuka pengguna komponen tertentu. Jika Anda merasa Anda perlu mengubah konfigurasi AVG agar lebih sesuai dengan kebutuhan Anda, masuk ke Pengaturan Lanjutan AVG: pilih item menu sistem ***Alat/Pengaturan lanjutan*** dan edit konfigurasi AVG di dialog Pengaturan Lanjutan AVG yang baru dibuka.

5. Antarmuka Pengguna AVG

Keamanan Intenet AVG 2012 dibuka dengan jendela utama:



Jendela utama dibagi ke dalam beberapa bagian:

- ***Menu Sistem*** *(baris sistem teratas di jendela)* adalah navigasi standar yang memungkinkan Anda mengakses semua komponen, layanan, dan fitur **Keamanan Intenet AVG 2012** – perincian >>

- ***Info Status Keamanan*** *(bagian atas jendela)* memberi Anda informasi mengenai status terkini dari **Keamanan Intenet AVG 2012** Anda – perincian >>

- ***Tombol Bergabunglah dengan kami di Facebook*** *(bagian sebelah kanan atas jendela)* memungkinkan Anda bergabung dengan komunitas AVG di Facebook. Namun, tombol tersebut hanya muncul jika semua komponen benar-benar berfungsi dan bekerja dengan baik *(untuk perincian cara mengenali status komponen AVG, lihat bab Info Status Keamanan)*

- ***Tautan Cepat*** *(bagian kiri jendela)* memungkinkan Anda mengakses cepat berbagai tugas yang paling penting dan paling sering digunakan pada **Keamanan Intenet AVG 2012** – perincian >>

- ***Aplikasi Saya*** *(bagian kiri bawah jendela)* membuka tinjauan umum mengenai aplikasi tambahan yang tersedia untuk **Keamanan Intenet AVG 2012**: LiveKive, Family Safety, dan PC TuneUp

- ***Tinjauan Umum Komponen*** *(bagian tengah jendela)* memberikan tinjauan umum

mengenai semua komponen yang terinstal dalam **Keamanan Intenet AVG 2012** - perincian >>

- ***Ikon Baki Sistem*** *(sudut kanan bawah monitor, pada baki sistem)* menunjukkan status terkini **Keamanan Intenet AVG 2012** - perincian >>

- ***Gadget AVG*** *(Bilah sisi Windows, didukung dalam Windows Vista/7)* memungkinkan akses cepat ke pemindaian dan pembaruan dalam **Keamanan Intenet AVG 2012** – perincian >>

5.1. Menu Sistem

Menu sistem adalah navigasi standar yang digunakan dalam semua aplikasi Windows. Tombol diletakkan secara horizontal di bagian paling atas jendela utama **Keamanan Intenet AVG 2012**. Gunakan menu sistem untuk mengakses komponen, fitur dan layanan AVG tertentu.

Menu sistem dibagi ke dalam lima bagian:

5.1.1. File

- ***Keluar*** – menutup antarmuka pengguna **Keamanan Intenet AVG 2012**. Walau demikian, aplikasi AVG akan terus berjalan di latar belakang dan komputer Anda tetap terlindungi!

5.1.2. Komponen

Item Komponen pada menu sistem berisi tautan ke semua komponen AVG yang terinstal, yang membuka halaman dialog defaultnya dalam antarmuka pengguna:

- ***Tinjauan umum sistem*** – beralih ke dialog antarmuka pengguna default berisi tinjauan umum semua komponen yang terinstal dan statusnya

- ***Anti-Virus*** mendeteksi virus, spyware, worm, troya, pustaka atau file eksekusi yang tak diinginkan dalam sistem Anda, serta melindungi Anda dari adware jahat - perincian >>

- ***LinkScanner*** melindungi Anda dari serangan berbasis Web saat Anda menelusuri atau menjelajah Internet – perincian >>

- ***Perlindungan E-mail*** memeriksa SPAM pada e-mail masuk, dan memblokir virus, serangan phishing, atau ancaman lainnya – perincian >>

- ***Firewall*** mengontrol semua komunikasi di setiap port jaringan, yang melindungi Anda dari serangan jahat dan memblokir semua upaya penyusupan – perincian >>

- ***Anti-Rootkit*** memindai rootkit berbahaya yang bersembunyi dalam aplikasi, driver, atau pustaka – perincian >>

- ***Alat Sistem*** memberikan ringkasan terperinci mengenai lingkungan AVG dan informasi sistem operasi – perincian >>

- ***PC Analyzer*** memberikan informasi tentang status komputer Anda – perincian >>

- ***Identity Protection*** terus-menerus melindungi aset digital Anda dari ancaman baru dan

tidak dikenal – perincian >>

- ***Administrasi Jarak-Jauh*** hanya ditampilkan dalam AVG Business Edition jika Anda telah menentukannya saat proses instalasi agar komponen ini diinstal

5.1.3. Riwayat

- Hasil pemindaian – beralih ke antarmuka pengetesan AVG, tepatnya ke dialog Tinjauan Umum Hasil Pemindaian
- Deteksi Resident Shield – membuka dialog berisi tinjauan umum mengenai ancaman yang terdeteksi oleh Resident Shield
- Deteksi E-mail Scanner – membuka dialog berisi tinjauan umum mengenai lampiran pesan e-mail yang terdeteksi sebagai berbahaya oleh komponen Perlindungan E-mail
- Temuan Online Shield – membuka dialog berisi tinjauan umum mengenai ancaman yang terdeteksi oleh layanan Online Shield dalam komponen LinkScanner
- Gudang Virus – membuka antarmuka ruang karantina (Gudang Virus) tempat AVG membuang semua infeksi terdeteksi yang tidak dapat dipulihkan secara otomatis karena suatu alasan. Di dalam karantina ini, file terinfeksi diisolasi dan keamanan komputer Anda terjamin, dan file terinfeksi tersebut sekaligus disimpan seandainya nanti bisa diperbaiki
- Log riwayat kejadian – membuka antarmuka log riwayat yang berisi tinjauan umum semua tindakan **Keamanan Intenet AVG 2012** yang telah tercatat dalam log
- Log Firewall – membuka antarmuka pengaturan Firewall pada tab Log yang berisi gambaran umum terperinci mengenai semua tindakan Firewall

5.1.4. Alat

- Pindai komputer – Meluncurkan pemindaian seisi komputer.
- Pindai folder yang dipilih... – Beralih ke antarmuka pemindaian AVG dan memungkinkan Anda menentukan dalam struktur komputer; file dan folder mana yang harus dipindai.
- ***Pindai file...*** – Memungkinkan Anda menjalankan tes saat diperlukan melalui 1 file khusus. Klik opsi ini untuk membuka jendela baru dengan struktur disk Anda. Pilih file yang diinginkan, dan konfimasikan peluncuran pemindaian.
- Perbarui – Secara otomatis meluncurkan proses pembaruan pada **Keamanan Intenet AVG 2012**.
- ***Perbarui dari direktori...*** – Menjalankan proses pembaruan dari file pembaruan yang berada dalam folder tertentu pada disk lokal Anda. Walau demikian, opsi ini hanya disarankan saat darurat, misalnya situasi di mana tidak ada koneksi ke Internet (*misalnya, komputer Anda terinfeksi dan terputus dari Internet; komputer Anda terhubung ke jaringan tanpa akses ke Internet, dll.*). Dalam jendela yang baru dibuka, pilih folder di mana sebelumnya Anda meletakkan file pembaruan, dan luncurkan proses pembaruan.
- Pengaturan lanjutan... – Membuka dialog Pengaturan lanjutan AVG tempat Anda dapat

mengedit konfigurasi Keamanan Intenet AVG 2012. Umumnya, disarankan untuk tetap menggunakan pengaturan default aplikasi sebagaimana ditetapkan oleh vendor perangkat lunak.

- Pengaturan Firewall... – Membuka dialog mandiri untuk konfigurasi lanjutan pada komponen Firewall.

5.1.5. Bantuan

- ***Daftar Isi*** – membuka file bantuan AVG
- ***Dapatkan Bantuan*** – membuka situs Web AVG (http://www.avg.com/) di halaman pusat dukungan pelanggan
- ***Web AVG Anda*** – membuka situs Web AVG (http://www.avg.com/)
- ***Tentang Virus dan Ancaman*** – membuka Ensiklopedia Virus online di mana Anda dapat melihat informasi terperinci mengenai virus yang telah dikenali
- ***Aktifkan Ulang*** – membuka dialog ***Aktifkan AVG*** berisi data yang telah Anda masukkan di dialog Personalisasi AVG pada proses instalasi. Dalam dialog ini Anda dapat memasukkan nomor lisensi untuk mengganti nomor penjualan (*nomor yang Anda gunakan untuk menginstal AVG*), atau untuk mengganti nomor lisensi lama (*misalnya, saat meningkatkan ke produk AVG baru*).
- ***Daftar sekarang*** – menghubungkan ke halaman pendaftaran situs Web AVG (http://www.avg.com/). Harap isikan data pendaftaran Anda ; hanya pelanggan yang mendaftarkan produk AVG mereka yang dapat menerima dukungan teknis gratis.

Catatan**: Jika menggunakan versi uji coba* **Keamanan Intenet AVG 2012, dua item selanjutnya akan muncul sebagai* ***Beli sekarang*** *dan* ***Aktifkan****, yang memungkinkan Anda membeli versi lengkap dari program ini saat itu juga. Untuk* **Keamanan Intenet AVG 2012** *yang terinstal dengan nomor penjualan, item yang ditampilkan adalah* ***Daftarkan*** *dan* ***Aktifkan****.*

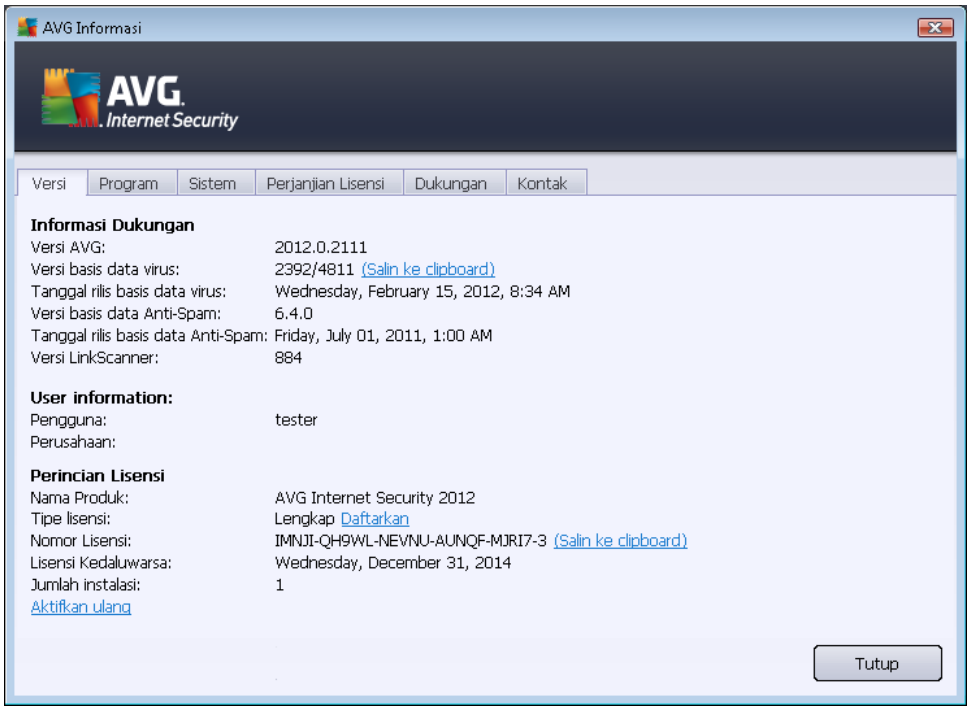
- ***Tentang AVG*** – membuka dialog ***Informasi*** berisi enam tab yang memberikan data mengenai nama program, program dan versi basis data virus, info sistem, perjanjian lisensi, dan informasi kontak ***AVG Technologies CZ***.

5.1.6. Dukungan

Tautan ***Dukungan*** akan membuka dialog ***Informasi*** baru bersama semua tipe informasi yang mungkin Anda perlukan saat mencoba menemukan bantuan. Dialog ini berisi data dasar mengenai program AVG yang telah Anda instal (*program / versi basis data*), perincian lisensi, dan daftar tautan dukungan cepat.

Dialog ***Informasi*** terbagi dalam enam tab:

Tab ***Versi*** terbagi ke dalam tiga bagian:

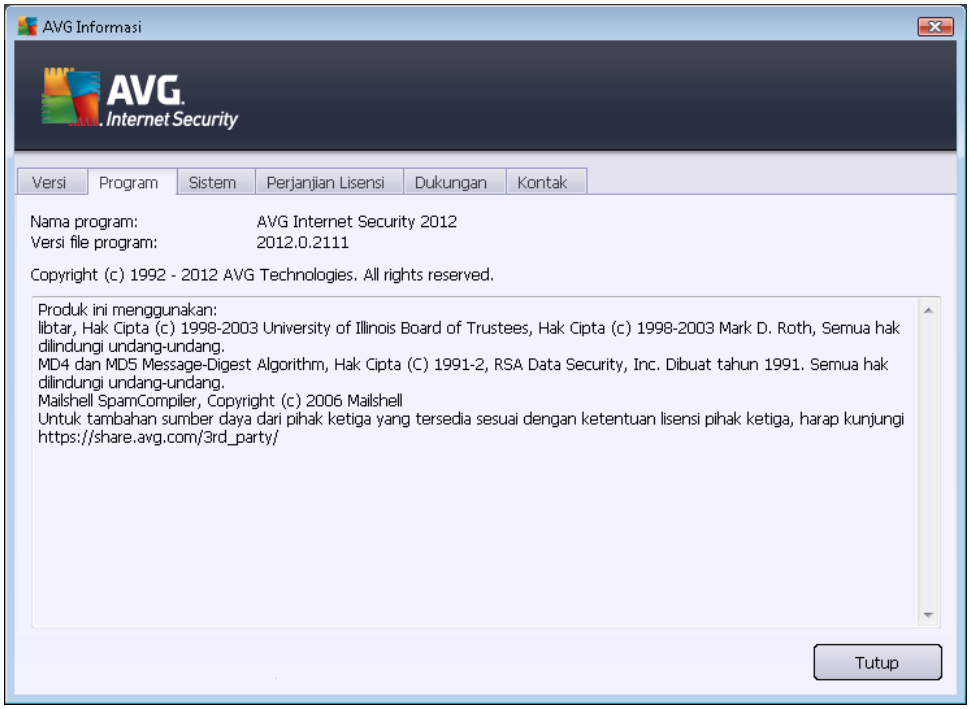


- ***Informasi Dukungan*** – Menyediakan informasi mengenai versi **Keamanan Intenet AVG 2012**, versi basis data virus, versi basis data Anti-Spam, dan versi LinkScanner.

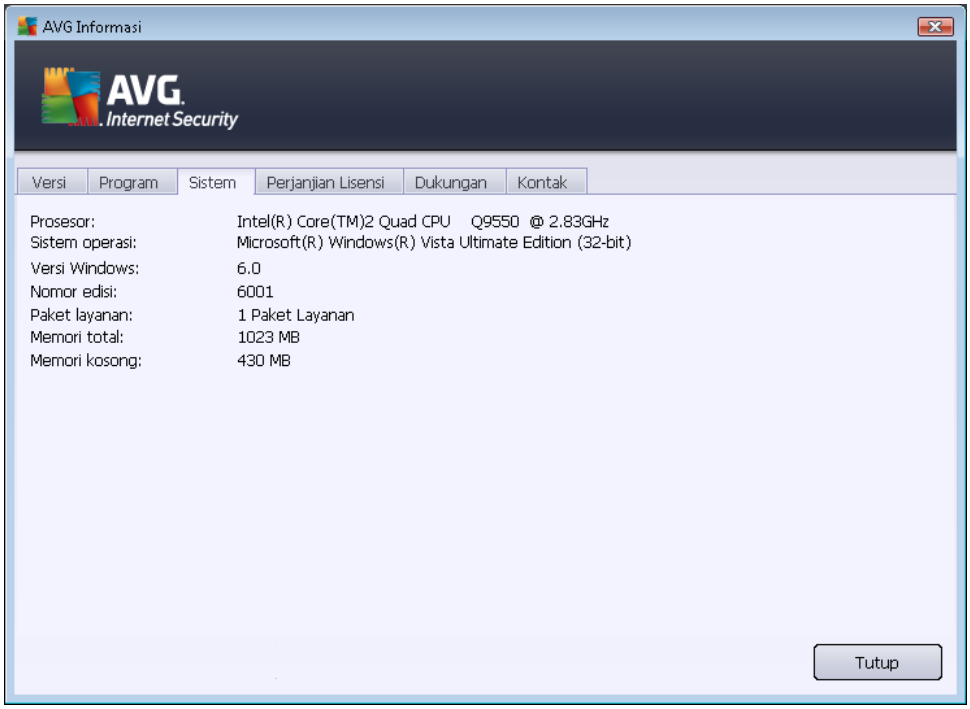
- ***Informasi Pengguna*** – Menyediakan informasi mengenai pengguna dan perusahaan yang berlisensi.

- ***Perincian Lisensi*** – Menyediakan informasi mengenai lisensi Anda *(nama produk, tipe lisensi, nomor lisensi, tanggal kedaluwarsa, dan jumlah pengguna*). Di bagian ini, Anda juga dapat menggunakan tautan ***Daftarkan*** untuk mendaftarkan **Keamanan Intenet AVG 2012** Anda secara online; ini memungkinkan Anda menggunakan dukungan teknis AVG secara penuh. Selain itu, gunakan tautan ***Aktifkan Ulang*** untuk membuka dialog ***Aktifkan AVG*** : isikan nomor lisensi Anda ke dalam bidang yang bersangkutan untuk menggantikan nomor penjualan Anda *(yang Anda gunakan selama instalasi Keamanan Intenet AVG 2012)*, atau untuk mengubah nomor lisensi Anda saat ini untuk yang lain *(misalnya saat meningkatkan ke produk AVG yang lebih tinggi).*

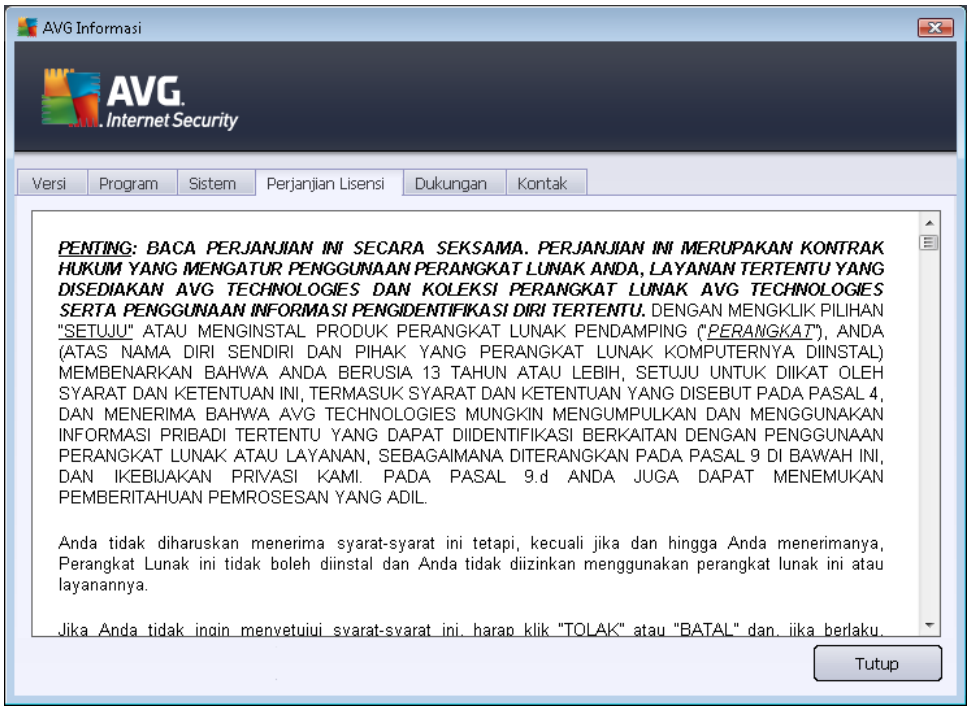
Pada tab ***Program*** Anda dapat menemukan informasi mengenai versi file program **Keamanan Intenet AVG 2012**, dan mengenai kode pihak ketiga yang digunakan dalam produk:



Tab ***Sistem*** menyediakan daftar parameter sistem operasi Anda *(tipe prosesor, sistem operasi dan versinya, nomor kompilasi, paket servis, total ukuran memori, dan ukuran memori yang masih kosong)*:

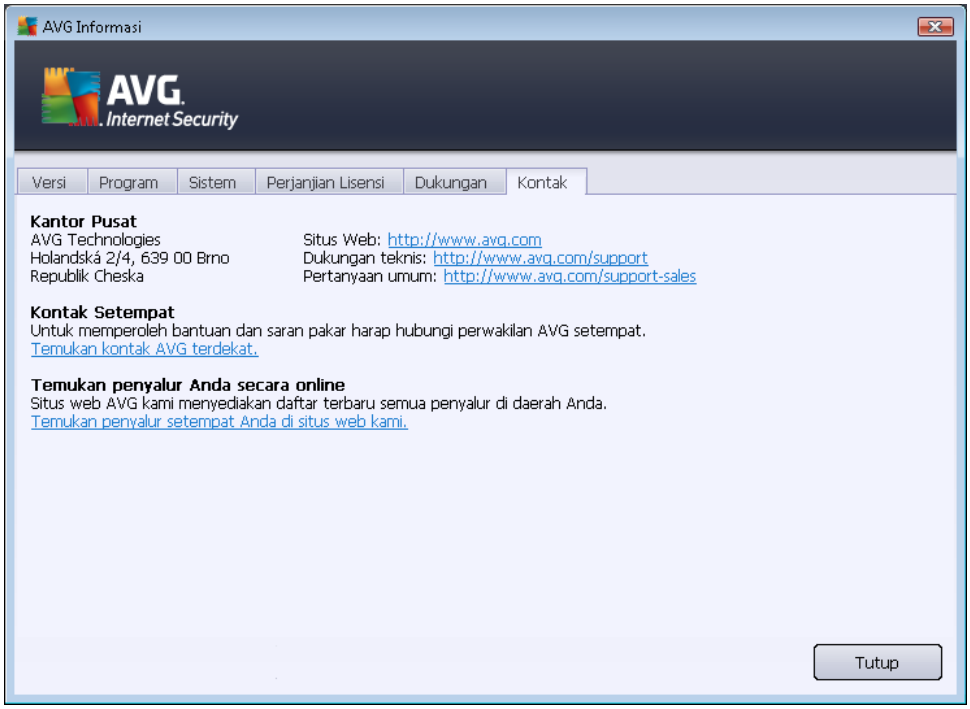


Pada tab ***Perjanjian Lisensi*** Anda dapat membaca perjanjian lisensi selengkapnya antara Anda dan AVG Technologies:



Tab ***Dukungan*** menampilkan daftar semua cara menghubungi dukungan pelanggan. Juga menyediakan tautan ke situs Web AVG (http://www.avg.com/), forum AVG, Tanya-Jawab, ... Selanjutnya Anda dapat menemukan informasi yang mungkin akan Anda gunakan saat menghubungi tim dukungan pelanggan:

Tab ***Kontak*** menyediakan daftar semua kontak ke AVG Technologies, juga kontak ke perwakilan dan penyalur AVG setempat:



5.2. Info Status Keamanan

Bagian ***Info Status Keamanan*** berada di bagian atas jendela utama **Keamanan Intenet AVG 2012**. Di bagian ini akan selalu Anda temukan informasi mengenai status keamanan saat ini atas **Keamanan Intenet AVG 2012** Anda. Lihat tinjauan umum mengenai berbagai ikon yang ditampilkan di bagian ini beserta artinya:

 – Ikon hijau menunjukkan bahwa ***Keamanan Intenet AVG 2012 Anda berfungsi penuh***. Komputer Anda terlindungi sepenuhnya, mutakhir dan semua komponen yang terinstal bekerja dengan benar.

 – Ikon kuning memperingatkan bahwa ***satu atau beberapa komponen salah konfigurasi*** dan Anda harus memperhatikan properti/pengaturannya. Tidak ada masalah kritis dalam **Keamanan Intenet AVG 2012** dan Anda barangkali telah memutuskan untuk menonaktifkan beberapa komponen karena suatu alasan. Anda tetap terlindungi!. Walau demikian, perhatikanlah masalah pengaturan komponen! Namanya akan tersedia di bagian ***Info Status Keamanan***.

Ikon kuning juga muncul jika karena suatu alasan Anda memutuskan untuk mengabaikan status kesalahan komponen. Opsi ***Abaikan status komponen*** tersedia dari menu konteks (

dibuka dengan klik kanan mouse Anda) di atas ikon komponen yang bersangkutan dalam tinjauan umum komponen pada jendela utama **Keamanan Intenet AVG 2012**. Pilih opsi ini untuk menyatakan Anda mengetahui status kesalahan komponen namun karena suatu alasan Anda ingin membiarkan **Keamanan Intenet AVG 2012** begitu dan Anda tidak ingin diperingatkan dengan ikon baki sistem. Anda mungkin perlu menggunakan opsi ini dalam situasi tertentu namun sangat disarankan untuk menonaktifkan opsi ***Abaikan status komponen*** secepatnya.

Atau ikon kuning juga akan ditampilkan jika **Keamanan Intenet AVG 2012** Anda meminta komputer dihidupkan ulang (***Hidupkan ulang diperlukan***). Perhatikan peringatan ini dan hidupkan ulang PC Anda menggunakan tombol ***Hidupkan ulang sekarang*** .

 – Ikon oranye menunjukkan bahwa ***Keamanan Intenet AVG 2012 dalam status kritis***! Satu atau beberapa komponen tidak berfungsi dengan benar dan **Keamanan Intenet AVG 2012** tidak dapat melindungi komputer Anda. Perhatikan segera untuk memperbaiki masalah yang dilaporkan. Jika Anda tidak dapat memperbaiki sendiri kesalahan tersebut, hubungi tim Dukungan teknis AVG.

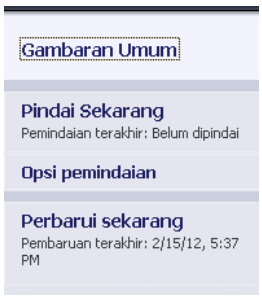
Jika Keamanan Intenet AVG 2012 tidak diatur pada kinerja optimal, tombol baru bernama Perbaiki (atau Perbaiki semua jika masalah melibatkan lebih dari satu komponen) akan muncul di sebelah informasi status keamanan. Tekan tombol untuk meluncurkan proses otomatis pemeriksaan dan konfigurasi program. Inilah cara mudah untuk mengatur Keamanan Intenet AVG 2012 ke performa optimal dan mencapai tingkat keamanan maksimum!

Sangatlah disarankan agar Anda memperhatikan Info Status Keamanan dan jika laporan menunjukkan adanya masalah, teruskan dan cobalah mengatasinya dengan segera. Jika tidak, komputer Anda berisiko!

Catatan: *informasi status Keamanan Intenet AVG 2012 juga dapat diperoleh kapan saja dari ikon baki sistem.*

5.3. Tautan Cepat

Tautan cepat berada di bagian kiri antarmuka pengguna **Keamanan Intenet AVG 2012**. Tautan ini memungkinkan Anda mengakses fitur aplikasi yang paling penting dan paling sering digunakan secara cepat, misalnya pemindaian dan pembaruan. Tautan cepat dapat diakses dari semua dialog antarmuka pengguna:



Tautan cepat secara grafis dibagi menjadi tiga bagian:

- ***Pindai sekarang*** – Secara default, tombol ini memberikan informasi mengenai pemindaian yang terakhir diluncurkan *(misalnya tipe pemindaian dan tanggal terakhir diluncurkan)*. Klik perintah ***Pindai sekarang*** untuk meluncurkan lagi pemindaian yang sama. Jika Anda ingin meluncurkan pemindaian lain, klik tautan ***Opsi pemindaian***. Dengan cara ini Anda dapat membuka antarmuka pemindaian AVG di mana Anda dapat menjalankan pemindaian, menjadwalkan pemindaian, atau mengedit parameternya. *(Untuk perinciannya, lihat bab Pemindaian AVG)*

- ***Opsi pemindaian*** - Gunakan tautan ini untuk beralih dari dialog AVG yang saat ini dibuka ke jendela default yang berisi gambaran umum mengenai semua komponen yang terinstal. *(Untuk perinciannya, lihat bab Gambaran Umum Komponen)*

- ***Perbarui sekarang*** – Tautan ini memberikan tanggal dan waktu pembaruan terakhir diluncurkan. Tekan tombol ini untuk menjalankan proses pembaruan dengan segera dan mengikuti kemajuannya. *(Untuk perinciannya, lihat bab Pembaruan AVG)*

Tautan cepat dapat diakses dari Antarmuka Pengguna AVG kapan saja. Setelah Anda menggunakan tautan cepat untuk menjalankan proses tertentu, pemindaian atau pembaruan, aplikasi akan beralih ke sebuah dialog baru namun tautan cepat tetap tersedia. Selanjutnya, proses yang berjalan ditampilkan secara grafis dalam navigasi, sehingga Anda mempunyai kontrol penuh atas jalannya semua proses yang diluncurkan dalam **Keamanan Intenet AVG 2012** pada saat itu.

5.4. Tinjauan Umum Komponen

Bagian Tinjauan Umum Komponen

Bagian ***Tinjauan Umum Komponen*** berada di bagian tengah antarmuka pengguna **Keamanan Intenet AVG 2012** Anda. Bagian ini dibagi ke dalam dua bagian:

- ***Tinjauan umum semua komponen yang terinstal*** terdiri dari panel-panel grafis untuk semua komponen yang terinstal. Setiap panel diberi label melalui ikon komponen dan menyediakan informasi mengenai aktif tidaknya komponen yang bersangkutan pada saat itu.

- ***Keterangan komponen*** berada di bagian bawah dialog ini. Keterangan menjelaskan secara singkat fungsionalitas dasar komponen. Juga menyediakan informasi mengenai status saat ini dari komponen yang dipilih.

Daftar komponen terinstal

Di bagian **Keamanan Intenet AVG 2012** ***Tinjauan Umum Komponen*** berisi informasi mengenai komponen berikut:

- ***Anti-Virus*** mendeteksi virus, spyware, worm, troya, pustaka atau file eksekusi yang tak diinginkan dalam sistem Anda, serta melindungi Anda dari adware jahat - perincian >>

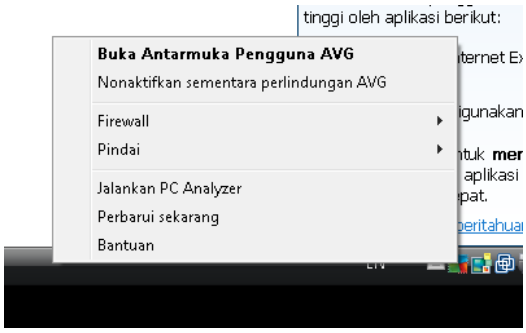
- ***LinkScanner*** melindungi Anda dari serangan berbasis Web saat Anda menelusuri atau menjelajah Internet – perincian >>
- ***Perlindungan E-mail*** memeriksa SPAM pada e-mail masuk, dan memblokir virus, serangan phishing, atau ancaman lainnya – perincian >>
- ***Firewall*** mengontrol semua komunikasi di setiap port jaringan, yang melindungi Anda dari serangan jahat dan memblokir semua upaya penyusupan – perincian >>
- ***Anti-Rootkit*** memindai rootkit berbahaya yang bersembunyi dalam aplikasi, driver, atau pustaka – perincian >>
- ***Alat Sistem*** memberikan ringkasan terperinci mengenai lingkungan AVG dan informasi sistem operasi – perincian >>
- ***PC Analyzer*** melakukan analisis yang memberikan informasi tentang status komputer Anda – perincian >>
- ***Identity Protection*** terus-menerus melindungi aset digital Anda dari ancaman baru dan tidak dikenal – perincian >>
- ***Administrasi Jarak-Jauh*** hanya ditampilkan dalam AVG Business Edition jika Anda telah menentukannya saat proses instalasi agar komponen ini diinstal

Tindakan yang dapat diakses

- ***Gerakkan mouse di atas ikon komponen*** untuk menyorotnya dalam tinjauan umum komponen. Pada saat yang sama, keterangan fungsionalitas dasar komponen akan muncul di bagian bawah antarmuka pengguna.
- ***Klik sekali ikon komponen*** untuk membuka antarmuka komponen yang berisi daftar data statistik dasar.
- ***Klik kanan di atas ikon komponen*** untuk membuka menu konteks yang berisi sejumlah opsi:
    - ***Buka*** – Klik opsi ini untuk membuka dialog komponen *(persis seperti mengklik sekali pada ikon komponen)*.
    - ***Abaikan status komponen ini*** – Pilih opsi ini untuk menyatakan Anda mengetahui status kesalahan komponen namun karena suatu alasan Anda ingin membiarkannya begitu dan Anda tidak ingin diperingatkan dengan ikon baki sistem.
    - ***Buka dalam Pengaturan lanjutan.....*** - Opsi ini hanya tersedia untuk beberapa komponen; misalnya komponen yang menyediakan kesempatan untuk pengaturan lanjutan.

5.5. Ikon Baki Sistem

Ikon Baki Sistem AVG *(pada Windows taskbar, sudut kanan bawah layar)* menunjukkan status terkini dari **Keamanan Intenet AVG 2012** Anda. Ini selalu terlihat pada baki sistem Anda, baik antarmuka pengguna **Keamanan Intenet AVG 2012** Anda dibuka atau ditutup:



Tampilan Ikon Baki Sistem AVG

- Jika warnanya penuh tanpa elemen tambahan berarti ikon menunjukkan bahwa semua komponen **Keamanan Intenet AVG 2012** aktif dan berfungsi penuh. Walau demikian, ikon tersebut juga dapat ditampilkan seperti ini bila salah satu komponen tidak berfungsi penuh namun pengguna memutuskan untuk mengabaikan status komponen. *(Setelah mengkonfirmasi opsi pengabaian status komponen, Anda menyatakan bahwa Anda mengetahui status kesalahan komponen namun karena suatu alasan Anda ingin membiarkannya begitu, dan Anda tidak ingin diperingatkan tentang situasi tersebut.)*

- Ikon dengan tanda seru menunjukkan bahwa komponen *(atau bahkan banyak komponen)* dalam status kesalahan. Selalu perhatikan peringatan demikian dan cobalah menghilangkan masalah konfigurasi komponen yang tidak diatur dengan benar. Agar dapat menerapkan perubahan dalam konfigurasi komponen, klik dua kali pada ikon baki sistem untuk membuka antarmuka pengguna aplikasi. Untuk informasi terperinci mengenai komponen apa saja yang berada dalam status kesalahan harap lihat bagian info status keamanan.

- Ikon baki sistem dapat ditampilkan dalam warna penuh dengan sinar lampu berkedip dan berputar. Versi grafik ini memberi sinyal atas proses pembaruan yang saat ini diluncurkan.

- Tampilan ikon yang berubah-ubah warna dengan panah menunjukkan **Keamanan Intenet AVG 2012** pemindaian baru saja berjalan.

Informasi Ikon Baki Sistem AVG

Ikon Baki Sistem AVG memberi tahu lebih jauh mengenai berbagai aktivitas saat ini dalam **Keamanan Intenet AVG 2012** dan kemungkinan perubahan status dalam program (*misalnya peluncuran otomatis untuk pemindaian atau pembaruan yang telah dijadwalkan, Tombol profil*

firewall, perubahan status komponen, kejadian status kesalahan, ...) melalui jendela pop-up yang dibuka dari ikon baki sistem:

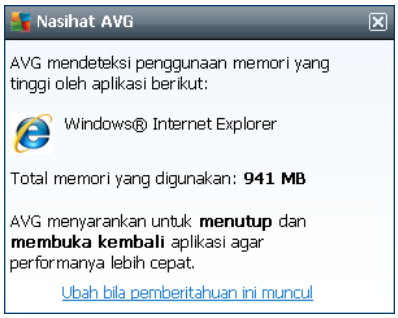
Tindakan dapat diakses dari Ikon Baki Sistem AVG

Ikon Baki Sistem AVG dapat digunakan sebagai tautan cepat untuk mengakses antarmuka pengguna **Keamanan Intenet AVG 2012**, tinggal klik dua kali pada ikonnya. Dengan mengklik kanan pada ikonnya Anda akan membuka menu konteks singkat berisi opsi berikut:

- ***Buka Antarmuka Pengguna AVG*** – Klik untuk membuka antarmuka pengguna **Keamanan Intenet AVG 2012**.
- ***Nonaktifkan perlindungan AVG untuk sementara*** – Anda mempunyai opsi untuk menonaktifkan seluruh perlindungan yang diberikan oleh **Keamanan Intenet AVG 2012** sekaligus. Ingatlah bahwa Anda tidak boleh menggunakan opsi ini kecuali jika sangat diperlukan! Dalam kebanyakan kasus, tidak diperlukan untuk menonaktifkan **Keamanan Intenet AVG 2012** sebelum menginstal perangkat lunak atau memasang driver baru, meskipun installer atau wizard perangkat lunak menyarankan bahwa program dan aplikasi yang berjalan ditutup terlebih dahulu untuk memastikan tidak ada gangguan yang tidak diinginkan selama proses instalasi. Jika Anda menonaktifkan **Keamanan Intenet AVG 2012** untuk sementara, Anda harus mengaktifkannya lagi begitu Anda selesai. Jika Anda terhubung dengan Internet atau jaringan selama perangkat lunak antivirus Anda dinonaktifkan, komputer Anda rentan terhadap serangan.
- ***Firewall*** – Klik untuk membuka menu konteks opsi pengaturan Firewall tempat Anda dapat mengedit parameter utama:Status firewall (*Firewall diaktifkan/Firewall dinonaktifkan/Mode darurat*), pengalihan ke mode permainan dan Profil firewall.
- ***Pemindaian*** – Klik untuk membuka menu konteks pemindaian yang telah ditetapkan (*Pemindaian Seisi Komputer, dan Pindai File atau Folder Tertentu*) dan pilih pemindaian yang diinginkan, pemindaian akan segera diluncurkan.
- ***Pemindaian sedang berjalan ...*** - Item ini hanya ditampilkan jika ada pemindaian yang sedang berjalan di komputer Anda. Untuk pemindaian ini, Anda dapat menentukan prioritasnya, selain menghentikan atau memberi jeda pada pemindaian yang sedang berjalan. Selanjutnya tindakan berikut dapat diakses: *Tentukan prioritas semua pemindaian, Jeda semua pemindaian*atau *Hentikan semua pemindaian*.
- ***Jalankan PC Analyzer*** – Klik untuk meluncurkan komponen PC Analyzer.
- ***Perbarui sekarang*** – Meluncurkan pembaruan dengan segera.
- ***Bantuan*** – Membuka halaman bantuan pada halaman awal.

5.6. AVG Advisor

AVG Advisor adalah fitur performa yang tetap memonitor semua proses yang berjalan dalam PC Anda untuk mendeteksi kemungkinan masalah dan menawarkan tips bagaimana menghindari masalah tersebut. ***AVG Advisor*** dapat dilihat berupa munculan geser melalui baki sistem.



AVG Advisor mungkin muncul dalam situasi berikut ini:

- Peramban internet yang sedang Anda gunakan kehabisan memori yang mungkin memperlambat pekerjaan Anda *(AVG Advisor hanya mendukung peramban Internet Explorer, Chrome, Firefox, Opera, dan Safari);*
- Sebuah proses yang berjalan di komputer Anda menghabiskan terlalu banyak memori dan memperlambat performa PC;
- Komputer Anda segera terhubung secara otomatis ke Wi-Fi yang tidak dikenal.

Di setiap situasi ini, ***AVG Advisor*** memperingatkan Anda tentang kemungkinan masalah yang mungkin terjadi serta memberikan nama dan ikon proses atau aplikasi yang bertentangan. ***AVG Advisor*** juga menyarankan langkah apa yang harus diambil untuk menghindari kemungkinan masalah tersebut.

5.7. Gadget AVG

Gadget AVG ditampilkan pada desktop Windows (*Bilah Sisi Windows*). Aplikasi ini hanya didukung dalam sistem operasi Windows Vista dan Windows 7. ***Gadget AVG*** menawarkan akses langsung ke fungsionalitas **Keamanan Intenet AVG 2012** yang terpenting yaitu pemindaian dan pembaruan:

Akses cepat ke pemindaian dan pembaruan

Jika perlu, ***Gadget AVG*** memungkinkan Anda menjalankan pemindaian atau pembaruan dengan segera:

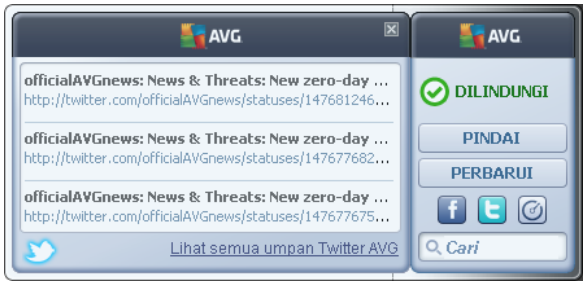
- ***Pindai sekarang*** – Klik tautan ***Pindai sekarang*** untuk memulai pemindaian seisi komputer secara langsung. Anda dapat mengawasi kemajuan proses pemindaian dalam antarmuka pengguna pada gadget lainnya. Tinjauan umum statistik singkat memberikan informasi tentang jumlah objek yang dipindai, ancaman yang terdeteksi dan ancaman yang dipulihkan. Selama pemindaian Anda selalu dapat melakukan jeda , atau menghentikan proses pemindaian. Untuk data terperinci yang berhubungan dengan hasil pindai, harap lihat dialog Tinjauan umum hasil pindai yang dapat dibuka langsung dari perkakas melalui opsi ***Tampilkan perincian*** *(hasil pindainya akan dicantumkan pada Pemindaian perkakas bilah samping)*.

- ***Perbarui sekarang*** – Klik tautan ***Perbarui sekarang*** untuk meluncurkan pembaruan langsung **Keamanan Intenet AVG 2012** dari dalam gadget:

Akses jaringan sosial

Gadget AVG juga menyediakan tautan cepat yang menghubungkan Anda ke jaringan sosial utama. Gunakan tombol yang terkait untuk terhubung ke komunitas AVG di Twitter, Facebook, atau LinkedIn:

- ***Tautan Twitter*** – Membuka antarmuka ***Gadget AVG*** baru yang menyediakan gambaran umum umpan AVG terbaru di Twitter. Ikuti tautan ***Lihat semua umpan Twitter AVG*** untuk membuka peramban Internet Anda di jendela baru, dan Anda akan dialihkan langsung ke situs Web Twitter, khususnya halaman yang ditujukan untuk berita terkait AVG:



- ***Tautan Facebook*** - Membuka peramban Internet Anda pada situs Web Facebook, khususnya pada halaman ***komunitas AVG***.

- ***LinkedIn*** - Opsi ini hanya tersedia dalam instalasi jaringan (*yaitu, tersedia karena Anda telah menginstal AVG menggunakan salah satu lisensi AVG Business Edition*), dan ini membuka peramban Internet Anda pada situs Web ***AVG SMB Community*** dalam jaringan sosial LinkedIn.

Fitur lainnya dapat diakses melalui gadget

- ***PC Analyzer*** - Membuka antarmuka pengguna di komponen PC Analyzer dan memulai analisis dengan segera.

- ***Kotak telusur*** - Ketik kata kunci dan segera dapatkan hasil telusur di jendela yang baru dibuka pada peramban Web default Anda.

6. Komponen AVG

6.1. Anti-Virus

Komponen ***Anti-Virus*** adalah komponen mendasar pada **Keamanan Intenet AVG 2012** Anda dan memadukan sejumlah fitur fundamental pada program keamanan:

- Mesin Pemindai
- Perlindungan Menetap
- Perlindungan Anti-spyware

6.1.1. Mesin Pemindai

Mesin pemindai yang merupakan basis komponen ***Anti-Virus*** akan memindai semua file dan aktivitas file *(membuka/menutup file, dsb.)* untuk virus yang dikenal. Semua virus yang terdeteksi akan diblokir agar tidak dapat berbuat apa pun kemudian dibersihkan atau dikarantina di Gudang virus.

Fitur penting pada perlindungan Keamanan Intenet AVG 2012 adalah tidak ada virus dikenal yang dapat berjalan pada komputer!

Metode deteksi

Umumnya perangkat lunak antivirus juga menggunakan pemindaian heuristik, yakni file dipindai untuk mengetahui karakteristik virus, sehingga disebut tanda tangan virus. Ini berarti pemindai antivirus dapat mendeteksi virus tak dikenal yang baru, jika virus baru tersebut memiliki karakteristik khas dari virus yang telah ada. ***Anti-Virus*** menggunakan metode deteksi berikut:

- *Pemindaian* – menelusuri string karakter yang merupakan karakteristik virus tertentu
- *Analisis heuristik* – emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual
- *Deteksi generik* – deteksi terhadap karakteristik petunjuk dari virus/sekelompok virus tertentu

Sementara satu teknologi mungkin gagal mendeteksi atau mengenali virus, ***Anti-Virus*** mengombinasikan beberapa teknologi untuk memastikan komputer terlindung dari virus. **Keamanan Intenet AVG 2012** juga dapat menganalisis dan mendeteksi aplikasi yang dapat dijalankan atau pustaka DLL yang mungkin tidak diinginkan dalam sistem. Kami menyebut ancaman demikian sebagai Program yang Mungkin Tidak Diinginkan *(berbagai macam spyware, adware, dsb.)*. Lagi pula, **Keamanan Intenet AVG 2012** memindai register sistem untuk mencari entri mencurigakan, file Internet sementara dan cookie pelacak, dan memungkinkan Anda memperlakukan semua item yang mungkin merusak dengan cara yang sama dengan infeksi lainnya.

Keamanan Intenet AVG 2012 memberikan perlindungan non-stop pada komputer Anda!

6.1.2. Perlindungan Menetap

Keamanan Intenet AVG 2012 memberi Anda perlindungan kontinu dalam bentuk perlindungan menetap. Komponen ***Anti-Virus*** memindai setiap file *(dengan ekstensi tertentu atau tanpa ekstensi sama sekali)* yang akan dibuka, disimpan, atau disalin. Ini melindungi area sistem pada komputer, dan media lepas-pasang (*flash disk, dsb.*). Jika menemukan virus dalam sebuah file yang telah diakses, ia akan menghentikan operasi yang sedang dilakukan dan tidak memperbolehkan virus mengaktifkan dirinya. Biasanya, Anda bahkan tidak melihat prosesnya, karena perlindungan menetap berjalan "di latar belakang". Anda hanya diberi tahu bila ancaman ditemukan; pada saat yang sama, ***Anti-Virus*** memblokir aktivasi ancaman dan menghapusnya.

Perlindungan menetap dimuat dalam memori komputer pada saat komputer dihidupkan, dan sangat penting bagi Anda untuk tetap mengaktifkannya sepanjang waktu.

6.1.3. Perlindungan Anti-Spyware

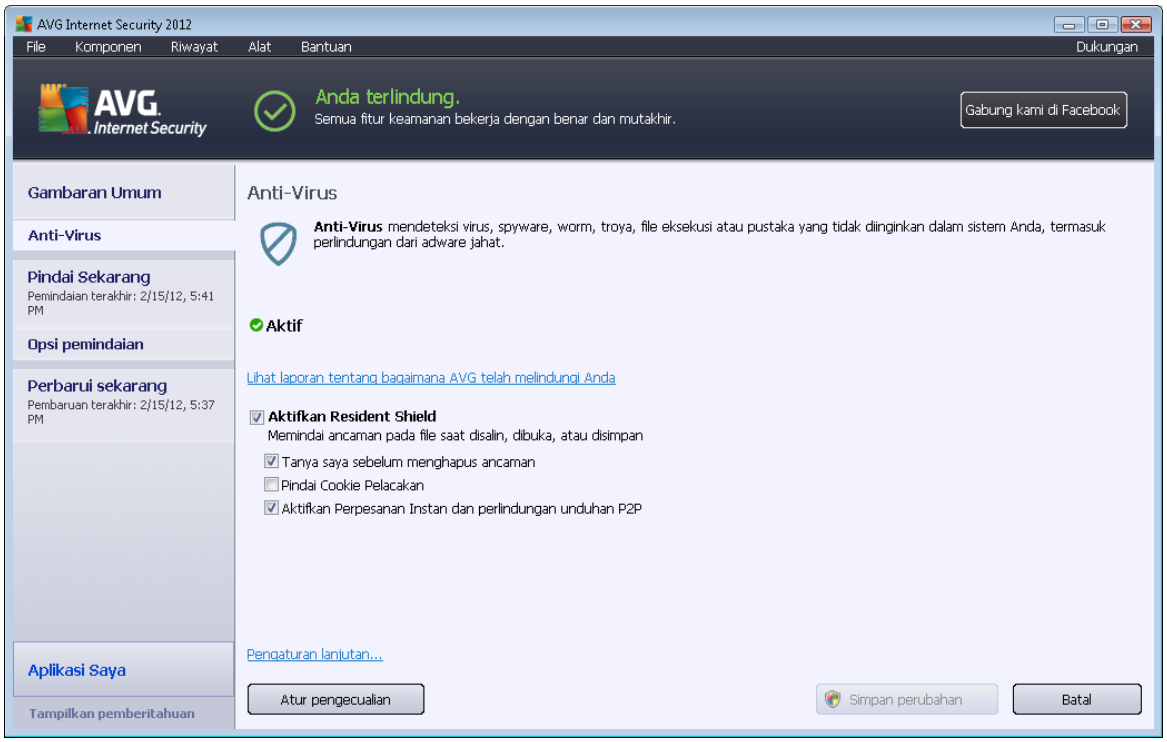
Anti-Spyware berisi basis data spyware yang digunakan untuk mengidentifikasi tipe definisi spyware yang telah dikenali. Para ahli spyware AVG bekerja keras untuk mengenali dan menguraikan pola spyware terbaru begitu mereka muncul, kemudian menambahkan definisi tersebut ke basis data. Melalui proses pembaruan, definisi baru ini diunduh ke komputer Anda sehingga Anda selalu terlindung dengan baik bahkan dari tipe spyware terbaru. ***Anti-Spyware*** memungkinkan Anda memindai adanya malware/spyware di komputer Anda secara lengkap. Komponen ini juga mendeteksi malware yang tidur dan tidak aktif, mis. malware yang telah diunduh tetapi belum diaktifkan.

Apa yang dimaksud dengan spyware?

Spyware biasanya ditetapkan sebagai tipe malware, yaitu perangkat lunak, yang mengumpulkan informasi dari komputer pengguna tanpa sepengetahuan atau persetujuan pengguna. Beberapa aplikasi spyware mungkin juga terinstal saat pembelian dan seringkali berisi iklan, jendela yang muncul atau tipe perangkat lunak tidak menyenangkan lainnya. Saat ini, sumber infeksi paling umum adalah situs Web dengan konten yang mungkin berbahaya. Metode transmisi lainnya, seperti e-mail atau transmisi melalui worm dan virus juga lazim. Perlindungan paling penting adalah menggunakan pemindai latar belakang yang selalu aktif, ***Anti-Spyware***, yang bekerja seperti Resident Shield dan memindai aplikasi Anda di latar belakang saat Anda menjalankannya.

6.1.4. Antarmuka Anti-Virus

Antarmuka komponen ***Anti-Virus*** menyediakan informasi singkat mengenai fungsionalitas komponen, informasi tentang status terkini komponen *(Aktif)*, dan opsi konfigurasi dasar komponen:



Opsi konfigurasi

Dialog ini menyediakan beberapa opsi konfigurasi dasar atas fitur yang tersedia dalam komponen ***Anti-Virus***. Berikut ini, Anda dapat menemukan keterangan singkatnya:

- ***Lihat laporan online untuk mengetahui cara AVG melindungi Anda*** – Tautan ini mengalihkan Anda ke halaman tertentu pada situs Web AVG (http://www.avg.com/). Di halaman tersebut, Anda dapat menemukan tinjauan umum statistik terperinci atas semua aktivitas **Keamanan Intenet AVG 2012** yang dilakukan pada komputer Anda dalam jangka waktu tertentu, dan secara total.

- ***Aktifkan Resident Shield*** – Opsi ini memungkinkan Anda mengaktifkan/menonaktifkan perlindungan tetap dengan mudah. Resident Shield memindai file saat disalin, dibuka atau disimpan. Bila ada virus atau semacam ancaman yang terdeteksi, Anda akan segera diperingatkan. Secara default, fungsi ini diaktifkan, dan kami sangat menyarankan Anda untuk membiarkannya! Dengan perlindungan menetap diaktifkan, Anda dapat memutuskan lebih lanjut cara memperlakukan kemungkinan infeksi yang terdeteksi:

    - ***Tanya saya sebelum menghapus ancaman*** – Tetap tandai opsi untuk mengonfirmasi bahwa Anda akan ditanya saat ancaman dideteksi sebelum dipindahkan ke Gudang Virus. Pilihan ini tidak mempengaruhi tingkat keamanan, dan

hanya mencerminkan preferensi Anda.

- ***Pindai Cookie Pelacak*** – Tidak tergantung pada opsi sebelumnya, Anda dapat memutuskan apakah ingin memindai cookie pelacak. *(Cookie adalah parsel teks yang dikirimkan oleh server ke peramban Web yang kemudian dikirim kembali tanpa perubahan oleh peramban setiap kali ia mengakses server itu. Cookie HTTP digunakan untuk autentikasi, pelacakan, dan pengelolaan informasi tertentu tentang pengguna, seperti preferensi situs atau isi keranjang belanja elektronik mereka.)* Dalam kasus tertentu, Anda dapat mengaktifkan opsi ini untuk mencapai tingkat keamanan maksimum, walau demikian ia telah dinonaktifkan secara default.

- ***Aktifkan perlindungan Perpesanan Instan dan unduhan P2P*** - Tandai item ini jika Anda ingin memverifikasi bahwa komunikasi perpesanan instan (*misalnya, ICQ, MSN Messenger, ...*) telah bebas virus.

- ***Pengaturan lanjutan***... – Klik tautan ini agar dialihkan ke dialog yang bersangkutan dalam Pengaturan lanjutan pada **Keamanan Intenet AVG 2012**. Di sana Anda dapat mengedit konfigurasi komponen secara terperinci. Walau demikian, harap perhatikan bahwa konfigurasi default semua komponen telah diatur agar **Keamanan Intenet AVG 2012** memberikan performa optimal, dan keamanan maksimum. Jika Anda tidak memiliki alasan kuat untuk itu, disarankan agar membiarkan konfigurasi default!

Tombol kontrol

Dalam dialog ini Anda dapat menggunakan tombol kontrol berikut:

- ***Atur pengecualian*** – Membuka dialog baru bernama ***Resident Shield – Pengecualian***. Konfigurasi pengecualian dari pemindaian Resident Shield juga dapat diakses dari menu utama, dengan urutan Pengaturan Lanjutan / Anti-Virus / Resident Shield / Pengecualian *(harap lihat bab terkait untuk keterangan terperinci)*. Dalam dialog ini Anda dapat menetapkan file dan folder yang harus dikecualikan dari pemindaian Resident Shield. Jika hal ini tidak penting, kami sangat menyarankan untuk tidak mengecualikan item apa pun! Dialog ini menyediakan tombol kontrol berikut:

  - *Tambah Jalur* – Menetapkan direktori *(atau direktori-direktori)* yang akan dikecualikan dari pemindaian dengan memilihnya satu per satu dari struktur navigasi disk lokal.

  - *Tambah File* – Menetapkan file yang akan dikecualikan dari pemindaian dengan memilihnya satu per satu dari struktur navigasi disk lokal.

  - *Edit Item* – Memungkinkan Anda mengedit jalur yang ditetapkan ke file atau folder yang dipilih.

  - *Hapus Item* – Memungkinkan Anda menghapus jalur ke item yang dipilih dari daftar.

  - *Edit Daftar* – Memungkinkan Anda mengedit seisi daftar pengecualian yang telah ditetapkan dalam dialog baru yang berfungsi seperti editor teks standar.

- ***Terapkan*** - Menyimpan semua perubahan pada pengaturan komponen yang dilakukan

dalam dialog ini dan mengembalikannya ke antarmuka pengguna utama **Keamanan Intenet AVG 2012** (*tinjauan umum komponen*).

- ***Batal*** – Membatalkan semua perubahan pada pengaturan komponen yang dilakukan dalam dialog ini. Tidak ada perubahan yang akan disimpan. Anda akan dikembalikan ke antarmuka pengguna utama **Keamanan Intenet AVG 2012** (*tinjauan umum komponen*).

6.1.5. Deteksi Resident Shield

Ancaman terdeteksi!

Resident Shield memindai file saat disalin, dibuka atau disimpan. Bila ada virus atau semacam ancaman yang terdeteksi, Anda akan segera diperingatkan melalui dialog berikut:

Dalam dialog peringatan ini Anda akan menemukan data tentang file yang terdeteksi dan dinyatakan sebagai terinfeksi(*Nama file*), nama infeksi yang dikenal (*Nama ancaman*), dan tautan ke Eksiklopedia virus tempat Anda dapat menemukan informasi terperinci tentang infeksi yang terdeteksi, jika diketahui *Info selebihnya*).

Selanjutnya, Anda harus memutuskan tindakan apa yang harus diambil sekarang. Sejumlah opsi berikut ini tersedia. ***Perhatikan bahwa, pada kondisi tertentu (jenis file yang terinfeksi, dan di mana lokasinya), tidak semua opsi ini tersedia!***

- ***Pulih*** – tombol ini hanya muncul jika infeksi yang terdeteksi dapat dipulihkan. Kemudian, infeksi akan dihapus dari file, dan file dipulihkan ke kondisi aslinya. Jika file itu sendiri yang adalah virus, gunakan fungsi ini untuk menghapusnya (*yakni memindahkannya ke Gudang Virus*)

- ***Pindahkan ke Gudang (Disarankan)*** – virus akan dipindahkan ke Gudang Virus

- ***Buka file*** - opsi ini mengalihkan Anda ke lokasi yang tepat di mana objek mencurigakan berada (*membuka jendela Windows Explorer baru*)

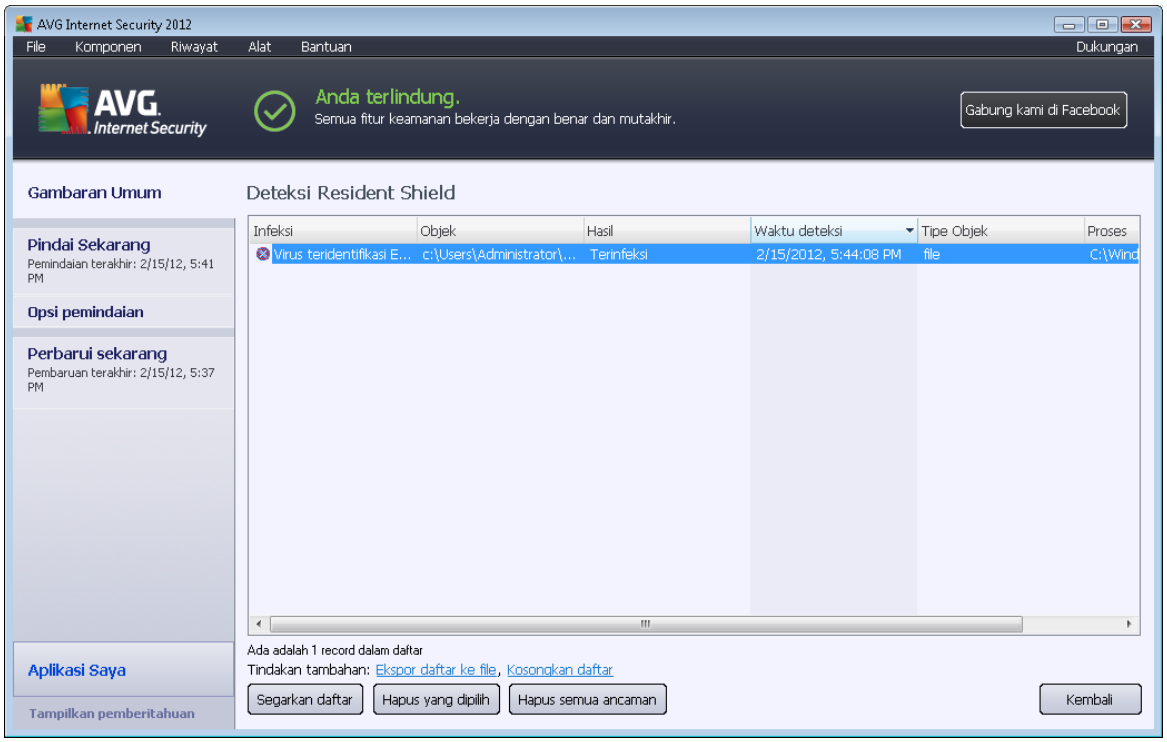
- ***Abaikan ancaman*** – kami sangat menyarankan untuk TIDAK menggunakan opsi ini kecuali Anda punya alasan yang sangat baik untuk melakukannya!

Catatan: *Ini mungkin terjadi karena ukuran objek yang terdeteksi melebihi batas ruang kosong dalam Gudang Virus. Jika demikian, sebuah pesan peringatan akan muncul memberi tahu Anda tentang masalah saat Anda mencoba memindah objek yang terinfeksi ke Gudang Virus. Walau demikian, ukuran Gudang Virus tidak dapat diubah. Ini telah ditetapkan berupa persentase ukuran nyata dari hard disk Anda yang dapat disesuaikan. Untuk menambah ukuran Gudang Virus Anda, masuk ke dialog Gudang Virus dalam Pengaturan Lanjutan AVG, melalui opsi 'Batasi ukuran Gudang Virus'.*

Di bagian bawah dialog, Anda dapat menemukan tautan ***Tampilkan perincian*** - klik untuk membuka jendela sembul dengan informasi terperinci tentang proses yang dijalankan ketika infeksi terdeteksi, dan proses identifikasi.

Tinjauan umum deteksi Resident Shield

Tinjauan umum keseluruhan atas semua ancaman yang terdeteksi oleh Resident Shield dapat ditemukan di dialog ***Deteksi Resident Shield*** yang dapat diakses melalui opsi menu sistem Riwayat / Deteksi Resident Shield:



Deteksi Resident Shield memberikan tinjauan umum mengenai berbagai objek yang terdeteksi oleh Resident Shield, yang telah dievaluasi sebagai berbahaya dan telah dipulihkan atau dipindahkan ke Gudang Virus. Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Infeksi*** – keterangan (bahkan mungkin nama) objek yang terdeteksi

- ***Objek*** – lokasi objek
- ***Hasil*** – tindakan yang dilakukan pada objek yang terdeteksi
- ***Waktu Deteksi*** – tanggal dan waktu objek terdeteksi
- ***Tipe Objek*** – tipe objek yang terdeteksi
- ***Proses*** – tindakan yang telah dilakukan untuk memanggil keluar objek yang mungkin berbahaya agar dapat dideteksi

Di bagian bawah dialog, pada daftar, Anda akan menemukan informasi mengenai jumlah total objek terdeteksi yang dicantumkan di atas. Selanjutnya Anda dapat mengekspor seluruh daftar objek yang terdeteksi dalam sebuah file (***Ekspor daftar ke file***) dan menghapus semua entri pada objek yang terdeteksi (***Kosongkan daftar***). Tombol ***Segarkan daftar*** akan memperbarui daftar temuan yang terdeteksi oleh ***Resident Shield***. Tombol ***Kembali*** akan mengembalikan Anda ke dialog utama AVG default (*tinjauan umum komponen*).

6.2. LinkScanner

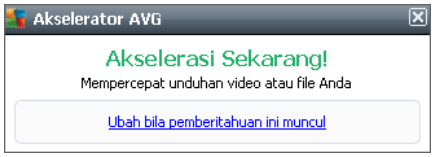
LinkScanner melindungi Anda dari ancaman yang "hari ini muncul dan besok menghilang" yang semakin meningkat jumlahnya di Web. Ancaman ini dapat disembunyikan di berbagai jenis situs Web, mulai situs pemerintah hingga perusahaan besar dan terkenal, hingga bisnis kecil; dan biasanya ancaman ini jarang berada pada situs tersebut lebih dari 24 jam. ***LinkScanner*** melindungi Anda dengan menganalisis halaman Web di balik semua tautan pada halaman situs yang Anda lihat dan memastikan tautan itu aman di saat yang paling menentukan – yaitu saat Anda akan mengklik tautan tersebut.

LinkScanner tidak ditujukan untuk perlindungan platform server!

Teknologi ***LinkScanner*** terdiri dari fitur utama berikut ini:

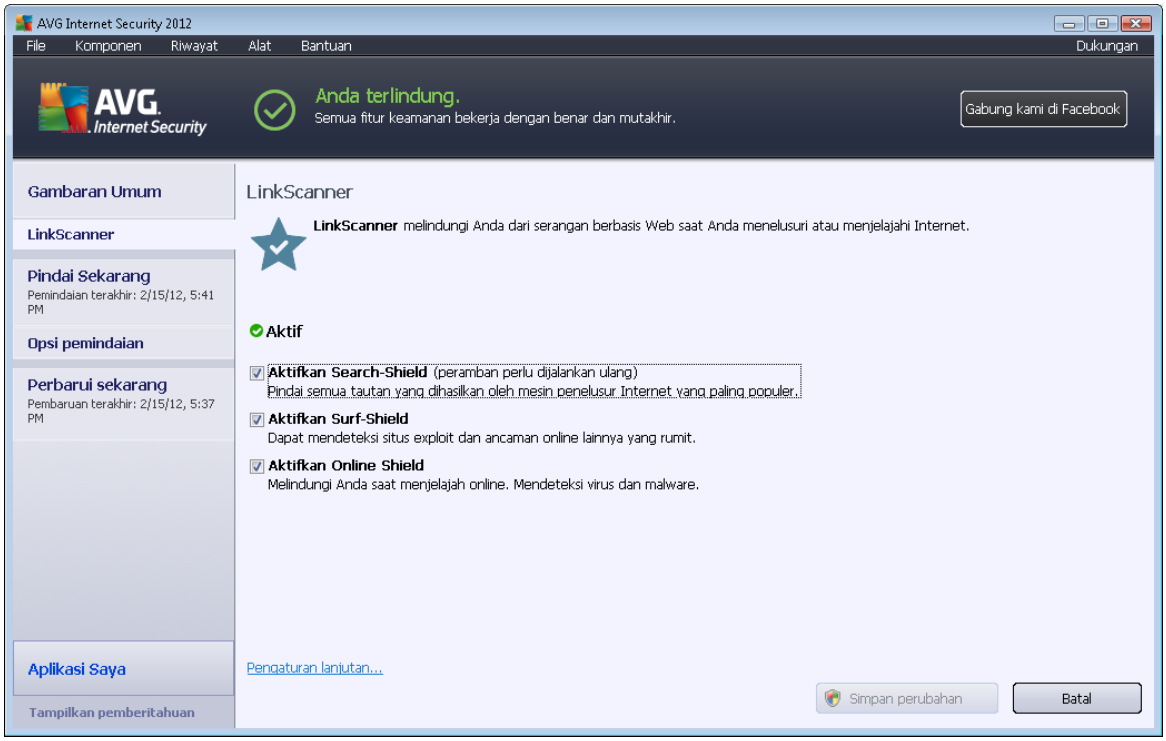
- Search-Shield berisi daftar situs Web *(alamat URL)* yang diketahui berbahaya. Saat menelusur dengan Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, dan Seznam, semua hasil penelusuran akan diperiksa sesuai daftar ini dan ikon keputusan akan ditampilkan *(untuk Yahoo! hanya ikon keputusan "situs Web terinfeksi" yang ditampilkan)*.
- Surf-Shield memindai konten situs Web yang Anda kunjungi, apa pun alamat situs Webnya. Bahkan jika situs Web tertentu tidak terdeteksi oleh Search-Shield *(mis. bila ada situs Web jahat baru yang dibuat, atau situs Web yang sebelumnya bersih sekarang berisi malware)*, situs akan terdeteksi dan diblokir oleh Surf-Shield begitu Anda mencoba mengunjunginya.
- Online Shield bekerja sebagai perlindungan seketika saat menelusuri Internet. Online Shield memindai isi halaman Web yang dikunjungi dan mungkin file yang dimasukkan di dalamnya bahkan sebelum halaman ditampilkan di peramban Web Anda atau diunduh ke komputer. Online Shield langsung mendeteksi virus dan spyware yang terdapat di halaman yang akan Anda unduh sehingga tidak ada ancaman yang sampai masuk ke komputer Anda.

- ***AVG Accelerator*** memungkinkan pemutaran video online lebih lancar dan membuat pengunduhan tambahan lebih mudah. Bila proses akselerasi video sedang berlangsung, Anda akan diberi tahu melalui jendela yang muncul di baki sistem.



6.2.1. Antarmuka LinkScanner

Dialog utama komponen LinkScanner memberikan keterangan singkat tentang fungsionalitas komponen dan informasi mengenai status terkininya *(Aktif)*:



Di bagian bawah dialog tersedia beberapa konfigurasi dasar komponen:

- ***Aktifkan Search-Shield*** – (*diaktifkan secara default*): Jangan tandai kotak ini hanya jika Anda mempunyai alasan yang kuat untuk menonaktifkan fungsionalitas Search Shield.
- ***Aktifkan Surf-Shield*** – (*diaktifkan secara default*): Perlindungan aktif (*seketika*) terhadap situs eksploitif saat mengaksesnya. Koneksi situs jahat yang telah dikenal dan konten eksploitifnya diblokir begitu ia diakses oleh pengguna melalui peramban Web (*atau aplikasi lain yang menggunakan HTTP*).
- ***Aktifkan Online Shield*** – (*diaktifkan secara default*): Pemindaian seketika atas halaman Web yang akan Anda kunjungi dari kemungkinan virus atau spyware. Jika terdeteksi, pengunduhan segera dihentikan agar tidak ada ancaman yang sampai masuk ke komputer

Anda.

6.2.2. Deteksi Search-Shield

Saat menelusuri Internet dengan mengaktifkan ***Search-Shield***, semua hasil penelusuran berasal dari mesin telusur terpopuler (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, dan SlashDot*) akan dievaluasi untuk mengetahui adanya tautan berbahaya atau mencurigakan. Dengan memeriksa tautan ini dan menandai tautan jahat, LinkScanner akan memperingatkan Anda sebelum mengklik tautan berbahaya atau mencurigakan, sehingga Anda bisa yakin hanya menuju ke situs Web yang aman.

Saat tautan dievaluasi pada halaman hasil telusur, Anda akan melihat tanda grafik di sebelah tautan yang memberi tahu bahwa verifikasi tautan sedang berlangsung. Saat evaluasi selesai, ikon informasi yang terkait akan ditampilkan:

 Halaman tertaut aman.

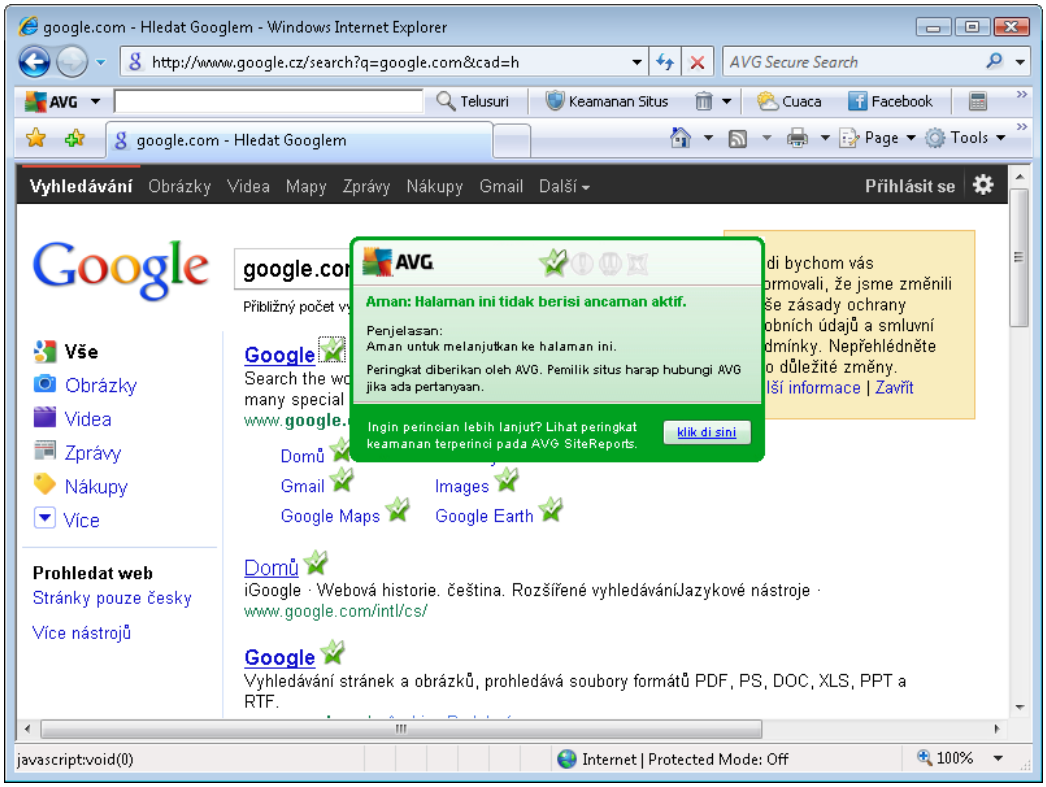
 Halaman tertaut tidak berisi ancaman namun agak mencurigakan (*asal atau motifnya meragukan, sehingga tidak disarankan untuk e-shopping dsb.*).

 Halaman tertaut mungkin aman, namun berisi tautan lebih lanjut ke halaman yang dipastikan berbahaya; atau memiliki kode yang mencurigakan, walaupun saat itu tidak secara langsung berisi ancaman.

 Halaman tertaut berisi ancaman yang aktif! Demi keamanan, Anda tidak akan diperbolehkan mengunjungi halaman ini.

 Halaman tertaut tidak dapat diakses, sehingga tidak dapat dipindai.

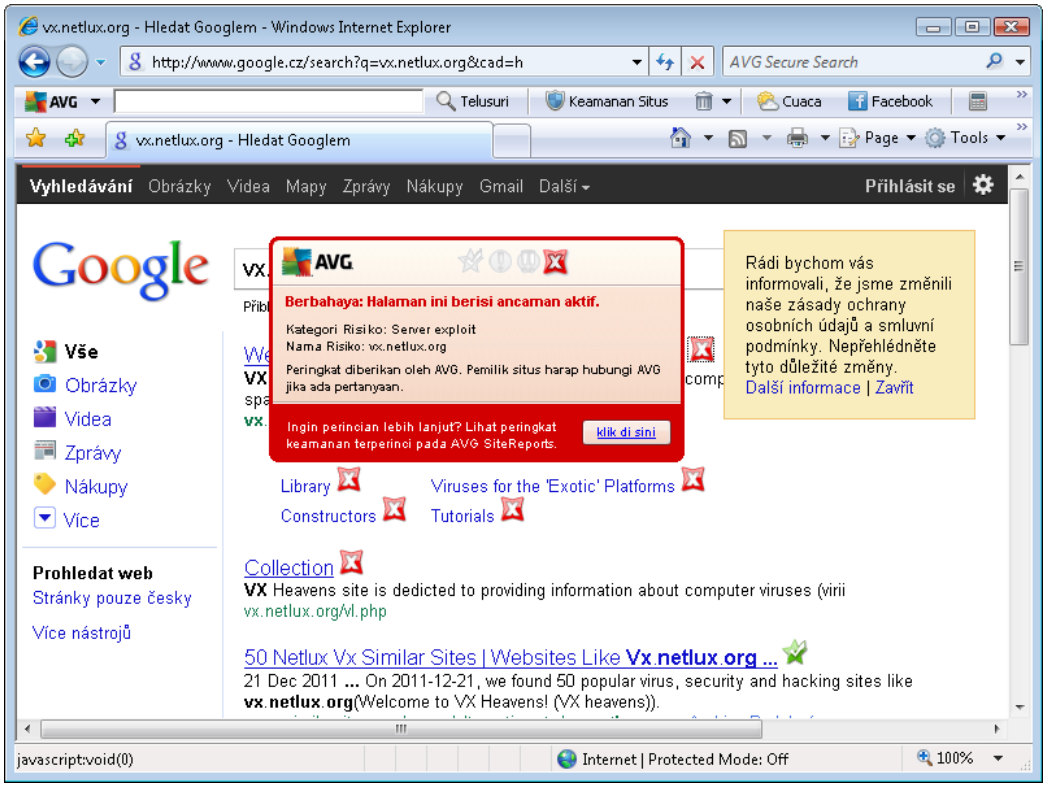
Melayangkan kursor di atas masing-masing ikon peringkat akan menampilkan perincian tentang tautan tertentu yang meragukan. Informasi ini berisi perincian tambahan mengenai ancaman (*jika ada*):



6.2.3. Deteksi Surf-Shield

Perlindungan tangguh ini akan memblokir berbagai konten jahat/perusak dari laman Web apa pun yang coba Anda buka, dan mencegahnya agar tidak diunduh ke komputer Anda. Bila fitur ini diaktifkan, mengklik tautan atau mengetikkan URL ke situs berbahaya akan mencegah Anda secara otomatis dari membuka halaman Web tersebut, dengan demikian akan melindungi Anda dari terinfeksi secara tidak sengaja. Penting diingat bahwa halaman Web yang telah dieksploitir dapat menginfeksi komputer Anda cukup dengan mengunjungi situs terinfeksi tersebut, karena alasan inilah saat Anda meminta halaman Web berbahaya berisi exploit atau ancaman serius lainnya, LinkScanner tidak akan memperbolehkan peramban Anda menampilkannya.

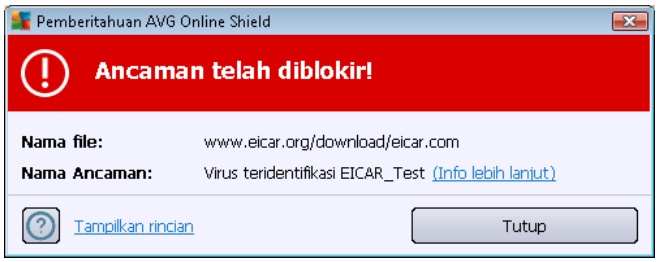
Jika Anda menemukan situs Web jahat dalam peramban Web, LinkScanner akan memperingatkan Anda dengan layar seperti ini:



Memasuki situs Web seperti ini sangat berisiko dan tidak disarankan!

6.2.4. Deteksi Online Shield

Online Shield memindai isi halaman Web yang dikunjungi dan mungkin file yang dimasukkan di dalamnya bahkan sebelum halaman ditampilkan di peramban Web Anda atau diunduh ke komputer. Bila ada ancaman yang terdeteksi, Anda akan segera diperingatkan dengan dialog berikut:

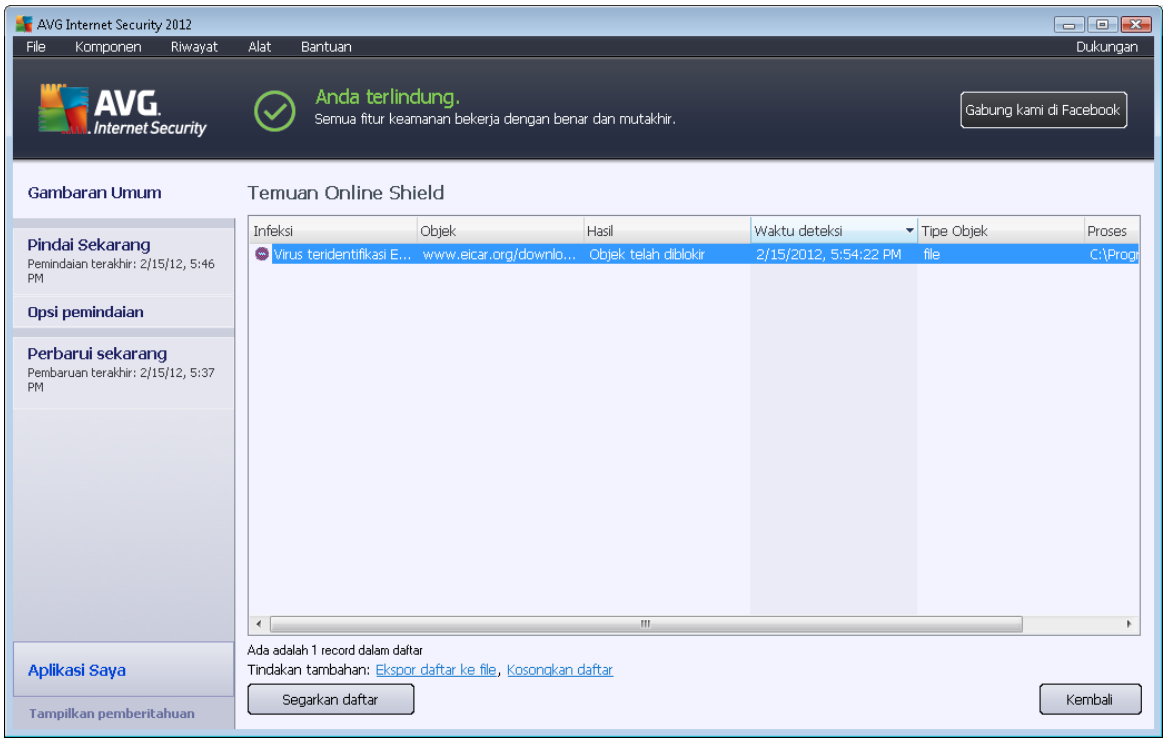


Dalam dialog peringatan ini, Anda akan menemukan data tentang file yang telah terdeteksi dan dinyatakan terinfeksi (*Nama file*), nama infeksi yang dikenali (*Nama ancaman*), dan tautan ke Eksiklopedia virus tempat Anda dapat menemukan infeksi yang terdeteksi (*jika dikenal*). Dialog ini menyediakan tombol berikut:

- ***Tampilkan perincian*** - klik tombol ***Tampilkan perincian*** untuk membuka jendela pop-up baru tempat Anda dapat menemukan informasi tentang proses yang sedang berjalan ketika infeksi terdeteksi, dan proses identifikasi.

- ***Tutup*** - klik tombol untuk menutup dialog peringatan.

Halaman Web yang dicurigai tidak akan dibuka dan deteksi ancaman akan direkam di log dalam daftar ***Temuan Online Shield*** – tinjauan umum ancaman yang terdeteksi ini dapat diakses melalui menu sistem Riwayat / Temuan Online Shield.



Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Infeksi*** – keterangan (*bahkan mungkin nama*) objek yang terdeteksi
- ***Objek*** – sumber objek (*halaman Web*)
- ***Hasil*** – tindakan yang dilakukan pada objek yang terdeteksi
- ***Waktu deteksi*** – tanggal dan waktu ancaman telah terdeteksi dan terblokir
- ***Tipe Objek*** – tipe objek yang terdeteksi
- ***Proses*** – tindakan yang telah dilakukan untuk memanggil keluar objek yang mungkin berbahaya agar dapat dideteksi

Di bagian bawah dialog, pada daftar, Anda akan menemukan informasi mengenai jumlah total objek terdeteksi yang dicantumkan di atas. Selanjutnya Anda dapat mengekspor seluruh daftar objek yang terdeteksi dalam sebuah file (***Ekspor daftar ke file***) dan menghapus semua entri pada objek yang terdeteksi (***Kosongkan daftar***).

Tombol kontrol

- ***Segarkan daftar*** – memperbarui daftar temuan yang terdeteksi oleh ***Online Shield***
- ***Kembali*** – mengembalikan ke dialog utama AVG *default (tinjauan umum komponen)*

6.3. Perlindungan E-mail

Salah satu sumber paling umum dari virus dan trojan adalah melalui e-mail. Phishing dan spam membuat e-mail menjadi sumber risiko yang jauh lebih besar. Akun e-mail gratis hampir bisa dipastikan akan menerima e-mail jahat demikian (*karena akun tersebut jarang memasang teknologi anti-spam*), dan pengguna rumahan sangat mengandalkan e-mail semacam itu. Juga pengguna rumahan, yang menyusuri situs tak dikenal dan mengisi formulir online dengan data pribadi (*misalnya alamat e-mail mereka*) akan menambah kemungkinan mereka terkena serangan melalui e-mail. Perusahaan-perusahaan biasanya menggunakan akun e-email perusahaan dan memasang filter anti-spam, dsb, untuk mengurangi risiko tersebut.

Komponen ***Perlindungan E-mail*** bertanggung jawab untuk memindai setiap pesan e-mail, yang dikirim atau diterima; kapan saja virus terdeteksi dalam e-mail, virus akan segera dipindahkan ke Gudang Virus. Komponen ini juga dapat memfilter jenis lampiran e-mail tertentu, dan menambahkan teks sertifikasi ke pesan bebas infeksi. ***Perlindungan E-mail*** terdiri dari dua fungsi utama:

- E-mail Scanner
- Anti-Spam

6.3.1. E-mail Scanner

E-mail Scanner Pribadi memindai Email masuk/keluar secara otomatis. Anda dapat menggunakannya dengan klien email yang tidak memiliki plug-in sendiri pada AVG (*tetapi juga dapat digunakan untuk memindai pesan email untuk klien email yang didukung AVG dengan plug-in khusus, yakni Microsoft Outlook, The Bat, dan Mozilla Thunderbird*). Pertama-tama, plug-in digunakan dengan aplikasi email seperti Outlook Express, Incredimail, dll.

Selama instalasi AVG, terdapat server otomatis yang dibuat untuk kontrol e-mail: satu server untuk memeriksa e-mail masuk dan yang kedua untuk memeriksa e-mail keluar. Dengan menggunakan dua server ini, e-mail akan diperiksa secara otomatis pada port 110 dan 25 (*port standar untuk mengirim/menerima e-mail*).

E-mail Scanner berfungsi sebagai antarmuka antara klien e-mail dan server e-mail di Internet.

- ***Email masuk:*** Saat menerima pesan dari server, komponen ***E-mail Scanner*** akan mengujinya untuk menemukan virus, membuang lampiran terinfeksi, dan menambahkan sertifikasi. Bila terdeteksi, virus akan segera dikarantina dalam Gudang Virus. Kemudian pesan diteruskan ke klien e-mail.
- ***Pesan keluar:*** Pesan dikirim dari klien e-mail ke E-mail Scanner; ia menguji pesan tersebut serta lampirannya untuk menemukan virus kemudian mengirimkan pesan tersebut ke server SMTP (*pemindaian pesan keluar dinonaktifkan secara default, dan dapat disetel secara manual*).

E-mail Scanner tidak ditujukan untuk platform server!

6.3.2. Anti-Spam

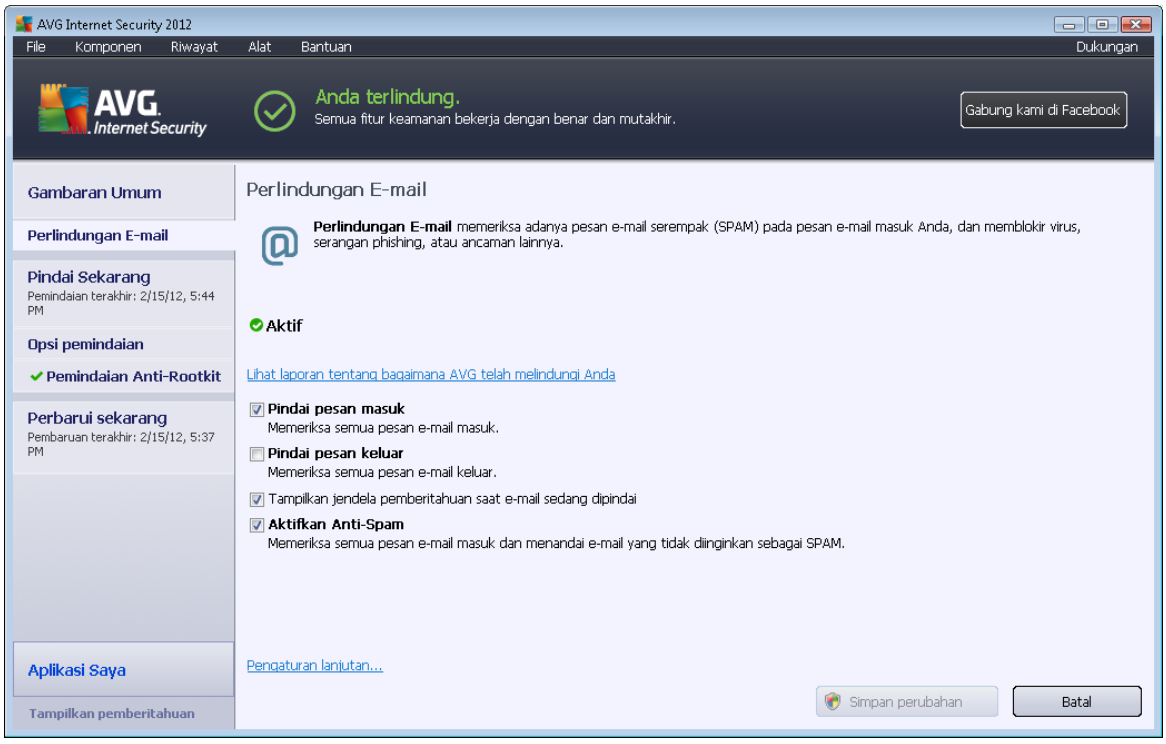
Bagaimana cara kerja Anti-Spam?

Anti-Spam memeriksa semua pesan e-mail masuk dan menandai e-mail yang tidak diinginkan sebagai spam. ***Anti-Spam*** dapat memodifikasi isi perihal email (*yang telah diidentifikasi sebagai spam*) dengan menambahkan string teks khusus. Sehingga Anda dengan mudah dapat menyaring email dalam klien email. ***Komponen Anti-Spam*** menggunakan beberapa metode analisis untuk memproses setiap pesan e-mail, menawarkan perlindungan maksimum yang dapat diberikan terhadap pesan e-mail yang tidak diinginkan. ***Anti-Spam*** menggunakan basis data yang diperbarui secara rutin untuk deteksi spam. Dapat juga menggunakan server RBL (*basis data umum dari alamat email "spammer yang dikenal"*) dan secara manual menambahkan alamat email ke Daftar Putih Anda (*jangan tandai sebagai spam*) dan Daftar Hitam (*selalu tandai sebagai spam*).

Apa yang dimaksud dengan spam?

Spam adalah e-mail yang tidak diundang, hampir semuanya mengiklankan produk atau layanan yang dikirimkan massal ke sejumlah besar alamat e-mail sekaligus, sehingga memenuhi kotak surat penerima. E-mail komersial resmi yang telah disetujui oleh konsumen tidak termasuk spam. Spam tidak hanya mengganggu, tetapi seringkali dapat menjadi sumber penipuan, virus, atau konten yang tidak pantas.

6.3.3. Antarmuka Perlindungan E-mail



Dalam dialog ***Perlindungan E-mail*** Anda dapat menemukan teks singkat yang menerangkan fungsionalitas komponen, dan informasi mengenai status terbarunya *(Aktif).* Gunakan tautan ***Lihat laporan online untuk mengetahui cara AVG melindungi Anda*** untuk meninjau statistik terperinci mengenai aktivitas dan deteksi **Keamanan Intenet AVG 2012** di halaman khusus pada situs Web AVG (http://www.avg.com/).

Pengaturan Dasar Perlindungan E-mail

Dalam dialog ***Perlindungan E-mail*** Anda dapat mengedit lebih lanjut beberapa fitur dasar fungsionalitas komponen:

- ***Pindai pesan masuk*** *(diaktifkan secara default)* - Tandai kotak untuk menetapkan bahwa semua email yang dikirimke akun Anda harus dipindai dari virus.
- ***Pindai pesan keluar*** *(dinonaktifkan secara default)* - Tandai kotak untuk mengonfirmasi bahwa semua email yang dikirim dari akun Anda harus dipindai dari virus.
- ***Tampilkan jendela pemberitahuan saat email dipindai*** *(diaktifkan secara default)* – Tandai item untuk mengkonfirmasi bahwa Anda ingin diberi tahu melalui dialog pemberitahuan yang ditampilkan di atas ikon AVG pada baki sistem selama memindai e-mail Anda.
- ***Aktifkan Anti-Spam*** *(diaktifkan secara default)* - Tandai item untuk menetapkan apakah Anda ingin email masuk difilter dari e-mail yang tidak diinginkan.

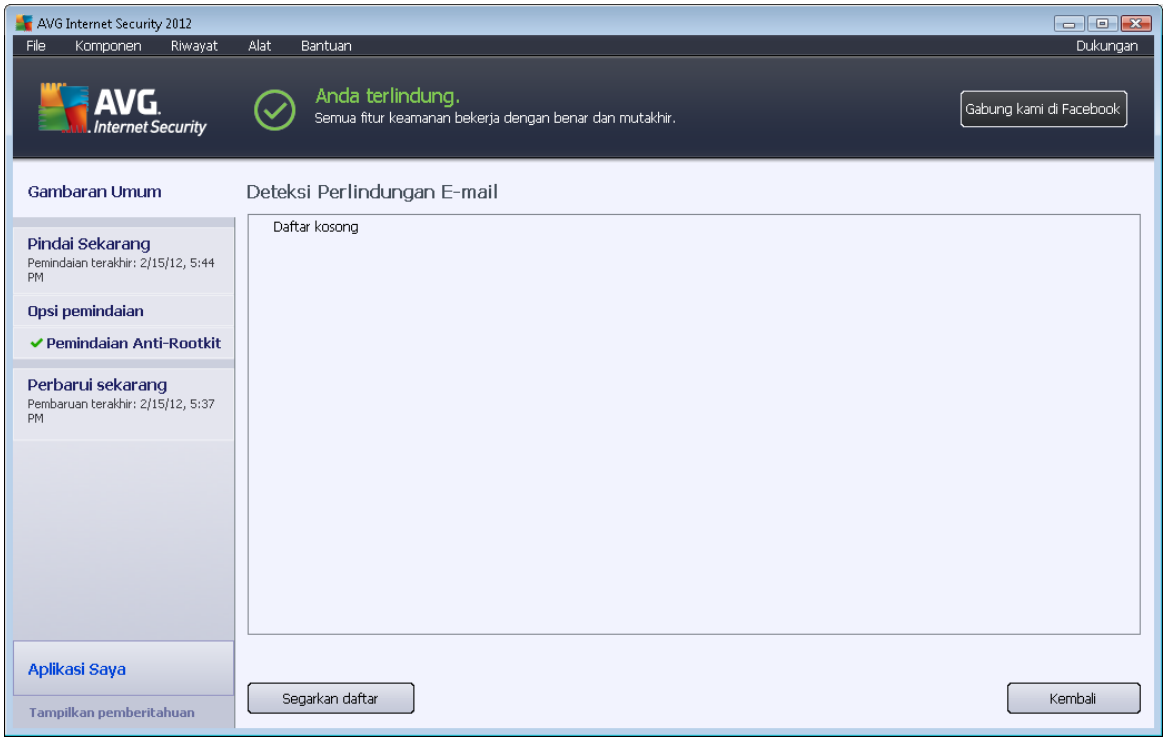
Vendor perangkat lunak telah mengatur semua komponen AVG untuk memberikan performa optimal. Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG. Semua perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman. Jika Anda perlu mengubah konfigurasi AVG, pilih item menu sistem Alat / Pengaturan lanjutan dan edit konfigurasi AVG dalam dialog Pengaturan Lanjutan AVG yang baru dibuka.

Tombol kontrol

Tombol kontrol yang tersedia dalam dialog ***Perlindungan E-mail*** adalah sebagai berikut:

- ***Simpan perubahan*** – tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini
- ***Batal*** – tekan tombol ini untuk kembali ke dialog utama AVG default (*tinjauan umum komponen*)

6.3.4. Deteksi Pemindai Email



Dalam dialog ***Deteksi E-mail Scanner*** (*dapat diakses melalui opsi menu sistem Riwayat / Deteksi E-mail Scanner*) Anda akan dapat melihat daftar semua temuan yang terdeteksi oleh komponen Perlindungan Email. Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Infeksi*** – keterangan (bahkan mungkin nama) objek yang terdeteksi
- ***Objek*** – lokasi objek
- ***Hasil*** – tindakan yang dilakukan pada objek yang terdeteksi
- ***Waktu Deteksi*** – tanggal dan waktu objek yang mencurigakan terdeteksi
- ***Tipe Objek*** – tipe objek yang terdeteksi

Di bagian bawah dialog, pada daftar, Anda akan menemukan informasi mengenai jumlah total objek terdeteksi yang dicantumkan di atas. Selanjutnya Anda dapat mengekspor seluruh daftar objek yang terdeteksi dalam sebuah file (***Ekspor daftar ke file***) dan menghapus semua entri pada objek yang terdeteksi (***Kosongkan daftar***).

Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka ***Deteksi E-mail Scanner*** adalah:

- ***Segarkan daftar*** – Memperbarui daftar ancaman yang terdeteksi.

- ***Kembali*** – Mengembalikan Anda ke dialog yang ditampilkan sebelumnya.

6.4. Firewall

Firewall adalah sebuah sistem yang memberlakukan kebijakan kontrol akses antara dua atau beberapa jaringan dengan cara memblokir/memperbolehkan lalu lintas. ***Firewall*** berisi sekumpulan aturan yang melindungi jaringan internal dari serangan yang berasal dari luar *(biasanya dari Internet)* dan mengontrol semua komunikasi pada setiap port jaringan tunggal. Komunikasi dievaluasi sesuai dengan aturan yang ditentukan, kemudian akan diperbolehkan atau dilarang. Jika ***Firewall*** mengenali adanya upaya penyusupan, ia akan "memblokir" upaya tersebut dan tidak memperbolehkan penyusup mengakses komputer.

Firewall dikonfigurasi untuk memperbolehkan atau menolak komunikasi internal/eksternal (dua arah, masuk atau keluar) melalui port yang ditentukan, dan bagi aplikasi perangkat lunak yang ditentukan. Misalnya, firewall dapat dikonfigurasi agar hanya memperbolehkan data Web mengalir masuk dan keluar dengan menggunakan Microsoft Explorer. Segala upaya untuk mentransmisikan data Web melalui peramban lain akan diblokir.

Firewall melindungi informasi yang dapat membuat orang mengenali Anda secara pribadi; agar tidak bisa dikirimkan dari komputer Anda tanpa seizin Anda. Ia mengontrol cara komputer Anda bertukar data dengan komputer lain di Internet atau jaringan lokal. Dalam sebuah organisasi, ***Firewall*** juga melindungi satu komputer dari serangan yang dilakukan pengguna internal pada komputer lain dalam jaringan.

Komputer yang tidak dilindungi oleh Firewall mudah menjadi target para peretas komputer dan pencuri data.

Rekomendasi: *Biasanya tidak disarankan untuk menggunakan lebih dari satu firewall pada satu komputer. Keamanan komputer tidak akan disempurnakan jika Anda menginstal lebih banyak firewall. Kemungkinan besar malah akan terjadi beberapa konflik antara kedua aplikasi ini. Karena itu, kami sarankan Anda menggunakan hanya satu firewall pada komputer Anda dan menonaktifkan semua firewall lain, sehingga meniadakan risiko kemungkinan konflik dan masalah apa pun yang berkaitan dengan hal ini.*

6.4.1. Prinsip-Prinsip Firewall

Di **Keamanan Intenet AVG 2012**, ***Firewall*** mengontrol semua lalu lintas di setiap port jaringan pada komputer Anda. Berdasarkan pada aturan yang ditetapkan, ***Firewall*** mengevaluasi aplikasi yang sedang dijalankan pada komputer *(dan ingin menghubungkan ke Internet/jaringan lokal)*, atau aplikasi yang mengakses komputer dari luar mencoba untuk menghubungkan ke PC Anda. Untuk masing-masing aplikasi ini, ***Firewall*** kemudian akan memperbolehkan atau melarang komunikasi untuk masing-masing aplikasi ini pada port jaringan. Secara default, jika aplikasi tidak dikenal *(yakni tidak memiliki aturan Firewall yang ditentukan)*, ***Firewall*** akan menanyakan apakah Anda ingin memperbolehkan atau memblokir upaya komunikasi tersebut.

AVG Firewall tidak ditujukan untuk platform server!

Apa yang dapat dilakukan AVG Firewall:

- Memperbolehkan atau memblokir upaya komunikasi aplikasi yang dikenal secara otomatis,

atau meminta konfirmasi Anda

- Menggunakan profil lengkap dengan aturan yang telah ditetapkan, sesuai kebutuhan Anda
- Mengalihkan profil secara otomatis saat menghubung ke berbagai jaringan, atau menggunakan beberapa adaptor jaringan

6.4.2. Profil Firewall

Firewall memungkinkan Anda menentukan aturan keamanan spesifik berdasarkan apakah komputer Anda berada di suatu domain, atau komputer tunggal, atau bahkan notebook. Setiap opsi ini memerlukan tingkat perlindungan yang berbeda, dan tingkat perlindungan tersebut dicakup oleh profil yang terkait. Singkatnya, profil Firewall adalah konfigurasi spesifik dari komponen Firewall, dan Anda dapat menggunakan beberapa konfigurasi yang telah ditentukan tersebut.

Profil yang tersedia

- ***Perbolehkan semua*** – adalah profil sistem Firewall yang telah ditetapkan oleh pabrikan dan selalu tersedia. Bila profil ini diaktifkan, semua komunikasi jaringan diperbolehkan dan tidak ada aturan kebijakan keamanan yang diterapkan, seolah perlindungan Firewall dinonaktifkan (yakni, semua aplikasi diperbolehkan namun paket masih akan diperiksa – untuk menonaktifkan sama sekali pemfilteran, Anda perlu menonaktifkan Firewall). Profil sistem ini tidak dapat digandakan, dihapus, dan pengaturannya tidak dapat diubah.
- ***Blokir semua*** – adalah profil sistem Firewall yang telah ditetapkan oleh pabrikan dan selalu tersedia. Bila profil ini diaktifkan, semua komunikasi jaringan akan diblokir, komputer tidak dapat diakses dari jaringan luar, dan tidak dapat berkomunikasi keluar. Profil sistem ini tidak dapat digandakan, dihapus, dan pengaturannya tidak dapat diubah.
- ***Profil khusus*** – profil khusus memungkinkan Anda memanfaatkan pengalihan profil otomatis yang khususnya berguna jika Anda sering menghubungkan ke beragam jaringan *(misalnya dengan notebook).* Profil akan dibuat secara otomatis setelah instalasi **Keamanan Intenet AVG 2012**, dan meliputi semua kebutuhan individu akan aturan kebijakan Firewall. Opsi berikut ini tersedia:
  - ***Terhubung langsung ke Internet*** – cocok untuk komputer desktop rumah biasa atau notebook yang terhubung langsung ke Internet, tanpa perlindungan ekstra. Opsi ini juga disarankan bila Anda menghubungkan notebook ke beragam jaringan yang tidak dikenal dan mungkin tidak diamankan (*misalnya di warung Internet, kamar hotel, dsb.*).Aturan kebijakan Firewall yang terketat pada profil ini memastikan bahwa komputer seperti itu terlindungi dengan memadai.
  - ***Komputer di domain*** – cocok untuk komputer dalam jaringan lokal, biasanya di sekolah atau kantor. Diasumsikan bahwa jaringan dikelola secara profesional dan dilindungi oleh beberapa tingkat perlindungan tambahan, sehingga tingkat keamanan bisa lebih rendah dari kasus yang disebutkan di atas, yang memungkinkan akses ke folder yang dibagi, unit disk dll.
  - ***Jaringan rumah kecil atau kantor*** – cocok untuk komputer dalam jaringan kecil, biasanya di rumah atau di perusahaan kecil. Biasanya, jenis jaringan ini tidak

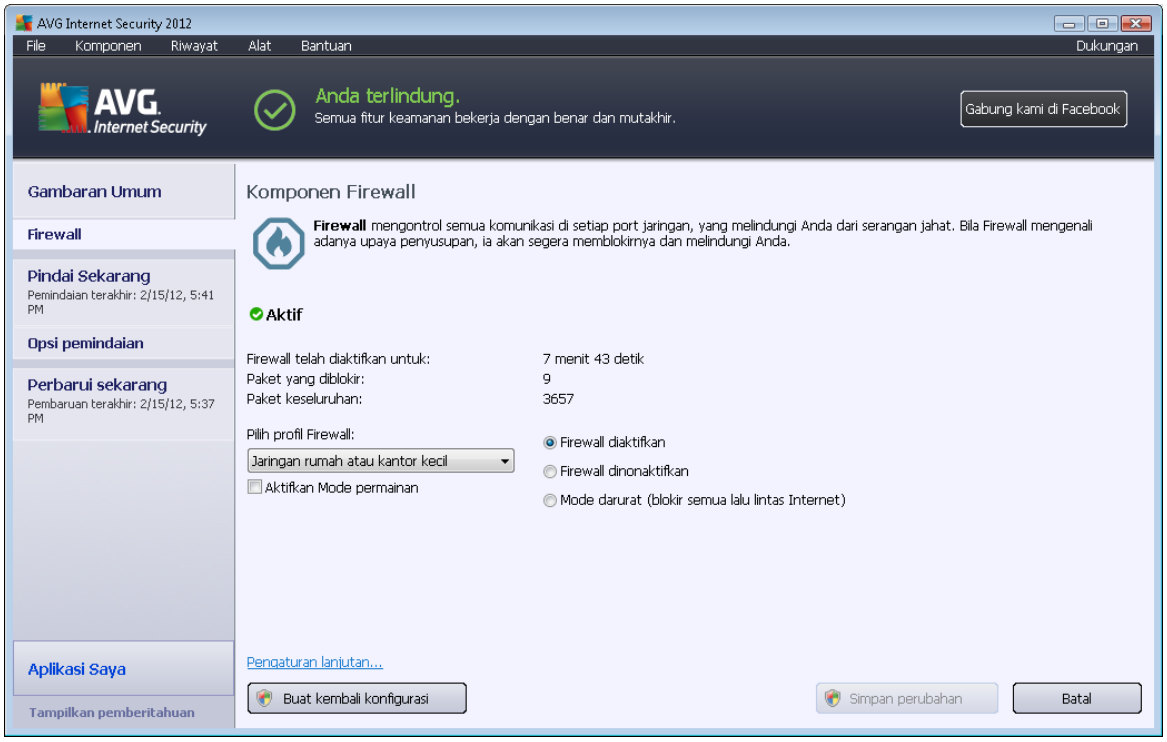
memiliki administrator "sentral", dan hanya terdiri atas beberapa komputer yang terhubung bersama, biasanya berbagi printer, scanner atau perangkat yang sama, yang harus ditunjukkan aturan Firewall.

Pengalihan profil

Fitur pengalihan profil memungkinkan Firewall untuk beralih secara otomatis ke profil yang ditentukan bila menggunakan adaptor jaringan tertentu, atau bila terhubung ke tipe jaringan tertentu. Jika belum ada profil yang ditetapkan untuk suatu area jaringan, maka pada saat koneksi berikutnya ke area itu, Firewall akan menampilkan dialog yang meminta Anda untuk menetapkan profil. Anda dapat menetapkan profil untuk semua antarmuka atau area jaringan lokal dan menetapkan pengaturan lebih lanjut dalam dialog Profil Area dan Adaptor, di mana Anda juga dapat menonaktifkan fitur ini jika tidak ingin menggunakannya (*maka, untuk jenis koneksi apa pun, profil default akan digunakan*).

Umumnya, pengguna notebook yang menggunakan berbagai tipe koneksi mendapatkan manfaat dari fitur ini. Jika Anda menggunakan komputer desktop, dan hanya menggunakan satu tipe koneksi (*mis. koneksi kabel ke Internet*), Anda tidak perlu direpotkan dengan pengalihan profil karena kemungkinan besar Anda tidak akan menggunakannya.

6.4.3. Antarmuka Firewall



Dialog utama bernama ***Komponen Firewall*** menyediakan beberapa informasi dasar mengenai fungsionalitas komponen, statusnya *(Aktif)*, dan tinjauan umum atas statistik komponen:

- ***Firewall telah diaktifkan selama*** – waktu yang dilalui sejak Firewall terakhir diluncurkan

- ***Paket yang diblokir*** - jumlah paket yang diblokir dari seluruh jumlah paket yang diperiksa
- ***Paket keseluruhan*** – jumlah semua paket yang telah diperiksa selama Firewall dijalankan

Pengaturan Dasar Firewall

- ***Pilih Profil Firewall*** – dari menu turun-bawah pilih salah satu profil yang ditetapkan (*untuk keterangan terperinci mengenai setiap profil dan penggunaan yang disarankan, harap lihat bab Profil Firewall*)
- ***Aktifkan Mode Permainan*** – Tandai opsi ini untuk memastikan bahwa saat menjalankan aplikasi layar penuh (*permainan, presentasi, film, dsb.*), Firewall tidak akan menampilkan dialog yang menanyakan apakah Anda ingin memperbolehkan atau memblokir komunikasi untuk aplikasi yang tidak dikenal. Jika saat itu ada aplikasi yang tidak dikenal mencoba berkomunikasi melalui jaringan, Firewall akan memperbolehkan atau memblokir upaya tersebut secara otomatis sesuai dengan pengaturan pada profil saat ini. ***Catatan:*** Dengan mode permainan yang diaktifkan, semua tugas yang dijadwalkan (pemindaian, pembaruan) ditunda sampai aplikasi ditutup.
- Lebih jauh lagi, di bagian pengaturan dasar ini, Anda dapat memilih dari tiga opsi alternatif yang menetapkan status komponen Firewall saat ini:
  - ***Firewall diaktifkan*** *(secara default)* – pilih opsi ini untuk memperbolehkan komunikasi ke berbagai aplikasi yang ditetapkan sebagai 'diperbolehkan' dalam kumpulan aturan yang telah ditetapkan dalam profil Firewall yang dipilih.
  - ***Firewall dinonaktifkan*** – opsi ini akan menonaktifkan Firewall sama sekali, semua lalu lintas jaringan diperbolehkan namun tidak diperiksa!
  - ***Mode darurat (memblokir semua lalu lintas Internet)*** – pilih opsi ini untuk memblokir semua lalu lintas pada setiap port jaringan tunggal; Firewall tetap berjalan namun semua lalu lintas jaringan dihentikan.

Perhatikan: *Vendor perangkat lunak telah mengatur semua komponen Keamanan Intenet AVG 2012 untuk memberikan performa optimal. Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG. Semua perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman. Jika Anda perlu mengubah konfigurasi Firewall, pilih item menu sistem* ***Alat/ Pengaturan Firewall*** *dan edit konfigurasi Firewall dalam dialog Pengaturan Firewall yang baru dibuka.*

Tombol kontrol

- ***Membuat kembali konfigurasi*** – tekan tombol ini untuk menimpa konfigurasi Firewall saat ini, dan untuk kembali ke konfigurasi default berdasarkan deteksi otomatis.
- ***Simpan perubahan*** – tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini.

- ***Batal*** – tekan tombol ini untuk kembali ke dialog utama AVG default (*tinjauan umum komponen*).

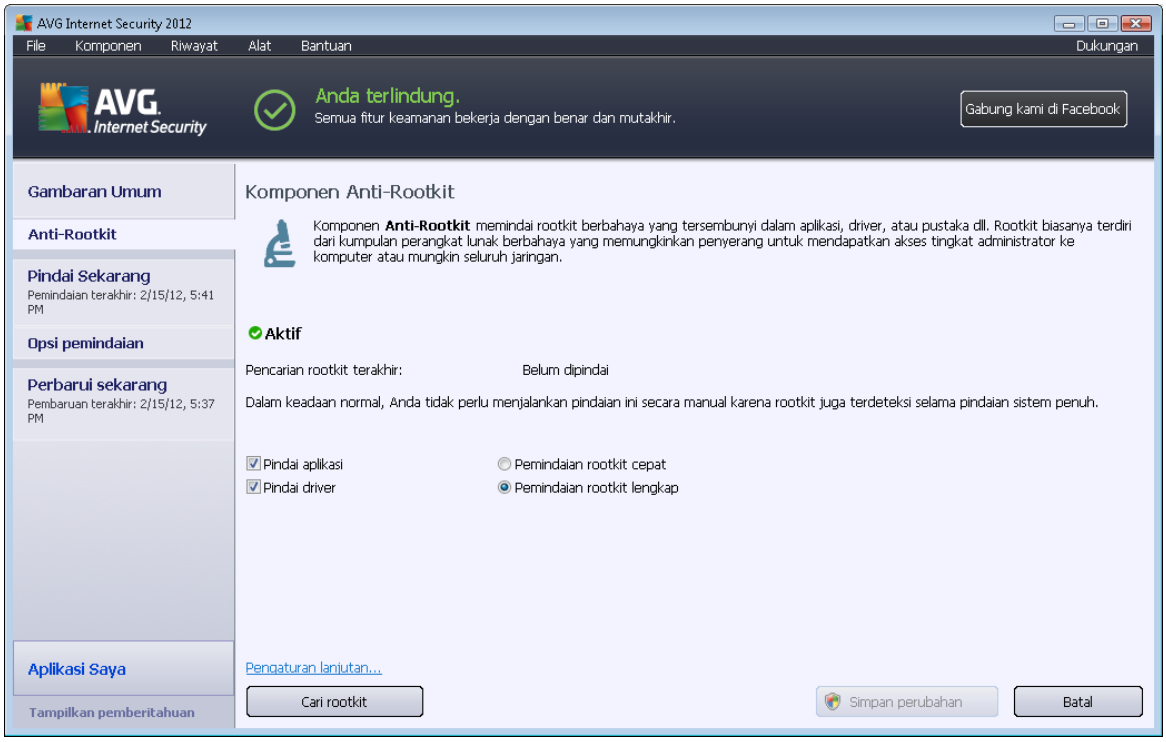
6.5. Anti-Rootkit

Anti-Rootkit adalah alat khusus untuk mendeteksi dan menghilangkan rootkit berbahaya secara efektif, misalnya program dan teknologi yang dapat menyamarkan kehadiran perangkat lunak jahat pada komputer Anda. ***Anti-Rootkit*** mampu mendeteksi rootkit berdasarkan seperangkat aturan yang ditentukan. Perhatikan, semua rootkit dideteksi *(tidak hanya yang terinfeksi)*. Seandainya ***Anti-Rootkit*** menemukan rootkit, tidak berarti rootkit tersebut terinfeksi. Kadang, rootkit digunakan sebagai driver atau bagian dari aplikasi yang benar.

Apa yang dimaksud dengan rootkit?

Rootkit adalah program yang dirancang untuk mengambil alih kontrol utama pada sistem komputer, tanpa seizin pemilik sistem dan manajer yang berwenang. Akses ke perangkat keras jarang diperlukan karena rootkit dimaksudkan untuk mengambil kontrol sistem operasi yang berjalan pada perangkat keras tersebut. Biasanya, rootkit mengaburkan kehadirannya pada sistem dengan menyusup ke atau mengelakkan mekanisme keamanan sistem operasi standar. Seringkali, mereka juga berupa Trojan, yang memperdaya pengguna agar menganggapnya aman dijalankan pada sistem mereka. Berbagai teknik digunakan untuk melakukan hal ini termasuk merahasiakan proses yang sedang berjalan dari program pemantau, atau menyembunyikan file atau data sistem dari sistem operasi.

6.5.1. Antarmuka Anti-Rootkit



Dialog ***Anti-Rootkit*** memberikan penjelasan singkat mengenai fungsionalitas komponen, memberi tahu mengenai status terbaru komponen *(Aktif)*, serta memberikan informasi mengenai waktu terakhir tes ***Anti-Rootkit*** diluncurkan (*penelusuran rootkit terakhir; tes rootkit adalah proses default yang berjalan dalam Pemindaian Seisi Komputer*). Dialog ***Anti-Rootkit*** selanjutnya memberikan tautan Alat/Pengaturan Lanjutan. Gunakan tautan untuk diarahkan kembali ke lingkungan konfigurasi lanjutan komponen ***Anti-Rootkit***.

Vendor perangkat lunak telah mengatur semua komponen AVG untuk memberikan performa optimal. Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG. Semua perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman.

Pengaturan dasar Anti-Rootkit

Di bagian bawah dialog, Anda dapat mengatur beberapa fungsi dasar dari pemindaian kehadiran rootkit. Pertama, tandai kotaknya untuk menetapkan objek yang harus dipindai:

- ***Pindai aplikasi***
- ***Pindai driver***

Selanjutnya Anda dapat memilih mode pemindaian rootkit:

- ***Pemindaian rootkit cepat*** – Memindai semua proses yang berjalan, driver yang dimuat dan folder sistem (*biasanya c:\Windows*).
- ***Pemindaian rootkit lengkap*** – Memindai semua proses yang berjalan, driver yang dimuat, folder sistem (*biasanya c:\Windows*), ditambah semua disk lokal (*termasuk flash-disk, namun tidak termasuk drive floppy-disk/drive CD*).

Tombol kontrol

- ***Telusuri rootkit*** – Karena pemindaian rootkit bukan bagian implisit dari Pindai seisi komputer, Anda dapat menjalankan langsung pemindaian rootkit dari antarmuka ***Anti-Rootkit*** menggunakan tombol ini.
- ***Simpan perubahan*** – Tekan tombol ini untuk menyimpan semua perubahan yang dibuat dalam antarmuka ini dan kembali ke dialog utama AVG default (*tinjauan umum komponen*).
- ***Batalkan*** – Tekan tombol ini untuk kembali ke dialog utama AVG default (*tinjauan umum komponen*) tanpa menyimpan perubahan yang telah Anda buat.

6.6. Alat Sistem

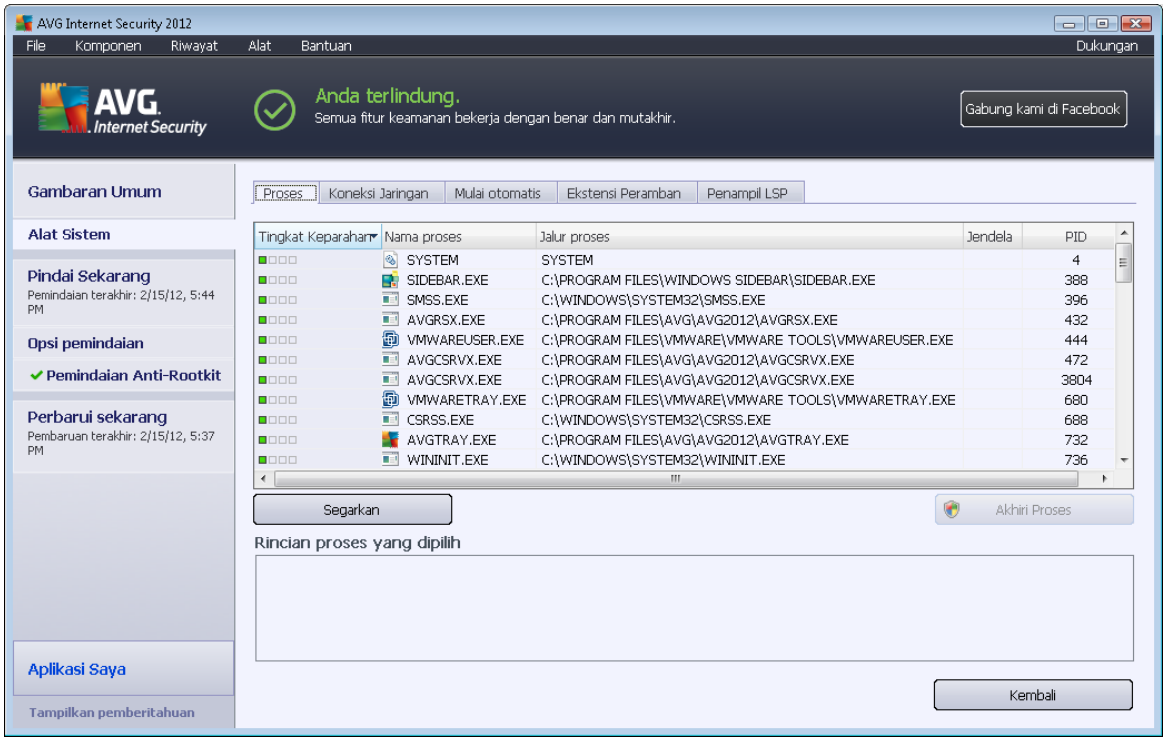
Alat Sistem merujuk pada alat yang menyediakan ringkasan terperinci mengenai lingkungan dan sistem operasi **Keamanan Intenet AVG 2012**. Komponen ini menampilkan gambaran umum:

- Proses – daftar proses (*yakni aplikasi yang berjalan*) yang saat ini aktif pada komputer Anda

- Koneksi jaringan – daftar koneksi yang saat ini aktif
- Mulai Otomatis – daftar semua aplikasi yang dijalankan selama menjalankan ulang sistem Windows
- Ekstensi Peramban – daftar plugin (*yakni aplikasi*) yang terinstal di dalam peramban Internet Anda
- Penampil LSP – daftar Layered Service Provider (*LSP*)

Gambaran umum tertentu juga dapat diedit namun ini hanya disarankan bagi pengguna yang sangat berpengalaman!

6.6.1. Proses



Dialog ***Proses*** berisi daftar proses (*yakni aplikasi yang berjalan*) yang saat ini aktif pada komputer Anda. Daftar ini dibagi ke dalam beberapa kolom:

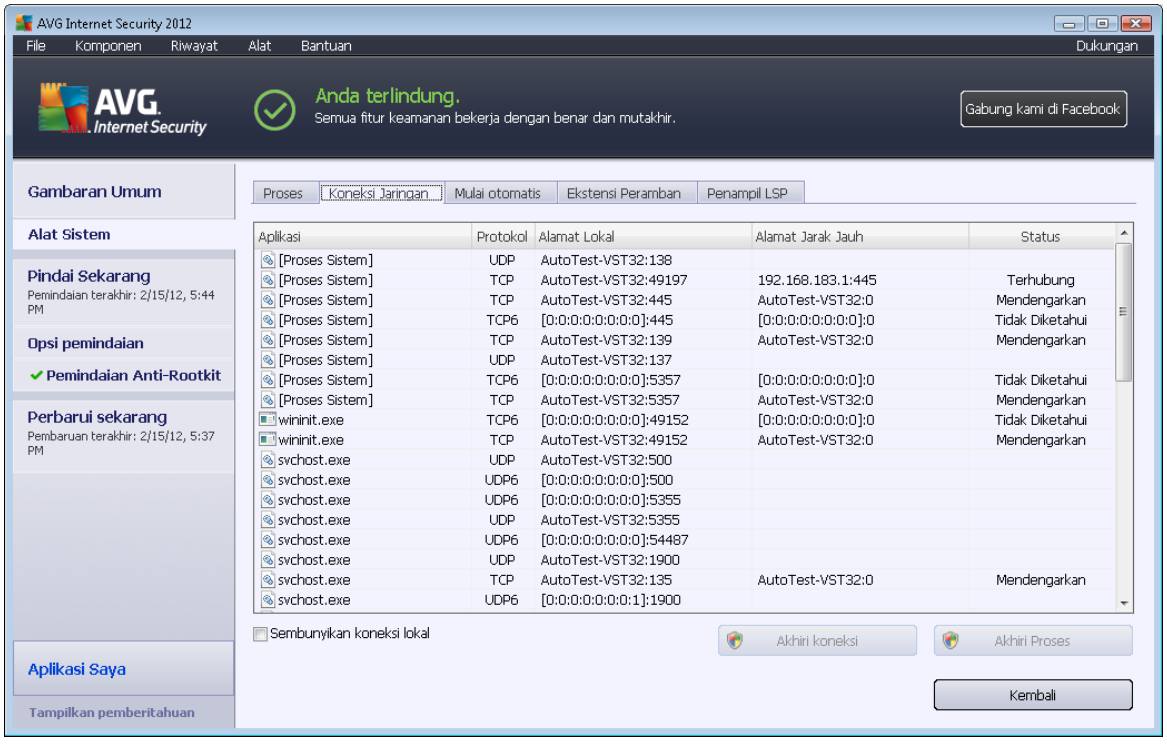
- ***Tingkat Keseriusan*** – identifikasi grafis dari keseriusan proses yang bersangkutan pada skala empat-tingkat dari kurang penting (■□□□) hingga kritis (■■■■)
- ***Nama proses*** – nama proses yang berjalan
- ***Jalur proses*** – jalur fisik ke proses yang berjalan
- ***Jendela*** – jika berlaku, menunjukkan nama jendela aplikasi
- ***PID*** – nomor identifikasi proses merupakan pengenal proses internal Windows

Tombol kontrol

Tombol kontrol yang tersedia dalam tab ***Proses*** adalah sebagai berikut:

- ***Segarkan*** – memperbarui daftar proses sesuai dengan status terkini
- ***Akhiri Proses*** - Anda dapat memilih satu atau beberapa aplikasi kemudian mengakhirinya dengan menekan tombol ini. ***Kami sangat menyarankan untuk tidak mengakhiri aplikasi apa pun, kecuali jika Anda sangat yakin bahwa aplikasi tersebut adalah ancaman nyata!***
- ***Kembali*** – mengembalikan Anda ke dialog utama AVG default (*tinjauan umum komponen*)

6.6.2. Koneksi Jaringan



Dialog ***Koneksi Jaringan*** berisi daftar koneksi yang saat ini aktif. Daftar ini dibagi ke dalam kolom-kolom berikut:

- ***Aplikasi*** – nama aplikasi yang terkait dengan koneksi (*kecuali Windows 2000 yang informasinya tidak tersedia*)
- ***Protokol*** – tipe protokol transmisi yang digunakan untuk koneksi:
  - TCP – protokol yang digunakan bersama dengan Internet Protocol (IP) untuk mengirim informasi melalui Internet

- UDP – alternatif untuk protokol TCP

- ***Alamat lokal*** – alamat IP dari komputer lokal dan nomor port yang digunakan
- ***Alamat jarak jauh*** – alamat IP dari komputer jarak jauh dan nomor port yang dihubungi. Jika memungkinkan, nama host komputer jarak jauh juga akan dicari.
- ***Status*** – menunjukkan status yang paling memungkinkan saat ini (*Terhubung, Server harus menutup, Dengar, Aktif tutup selesai, Pasif tutup, Aktif tutup*)

Untuk mencantumkan koneksi eksternal saja, centang kotak ***Sembunyikan koneksi lokal*** di bagian bawah dialog di bawah daftar.

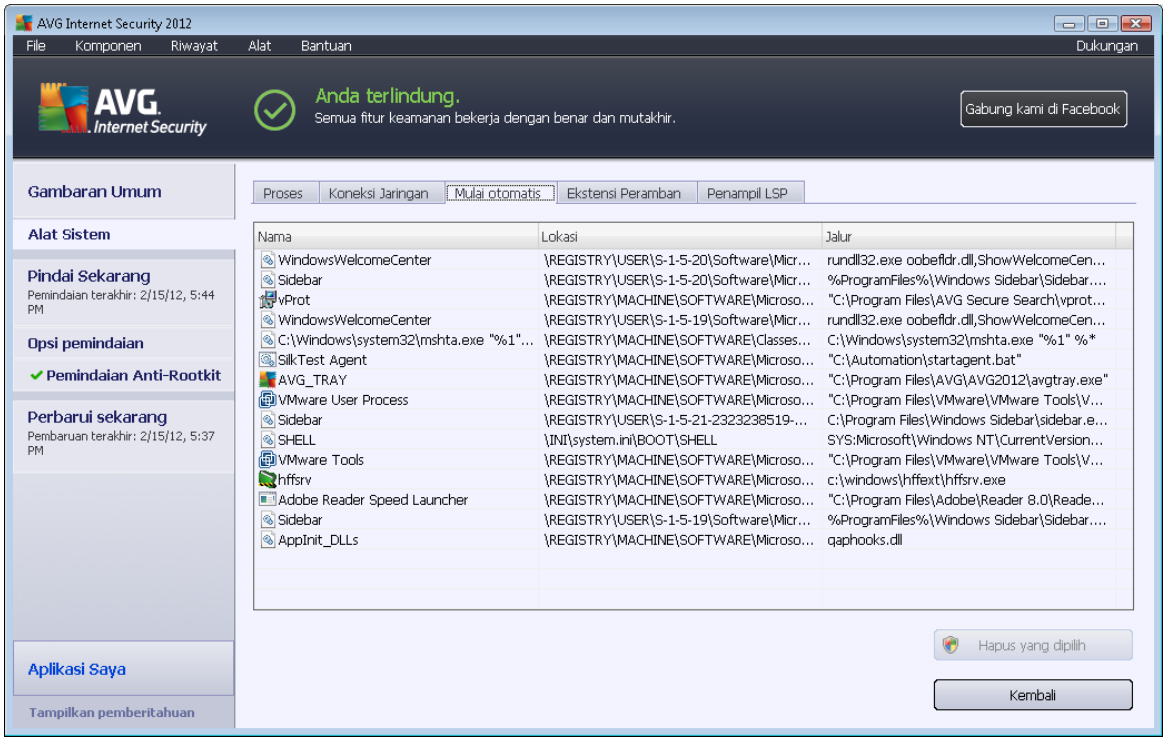
Tombol kontrol

Tombol kontrol yang tersedia dalam tab ***Koneksi Jaringan*** adalah sebagai berikut:

- ***Akhiri Koneksi*** – menutup satu atau beberapa koneksi yang dipilih dalam daftar
- ***Akhiri Proses*** – menutup satu atau beberapa aplikasi yang terkait dengan koneksi yang dipilih dalam daftar
- ***Kembali*** – mengembalikan ke dialog utama AVG default (tinjauan umum komponen).

Kadang-kadang Anda hanya dapat mengakhiri aplikasi yang saat itu dalam keadaan terhubung. Kami sangat menyarankan untuk tidak mengakhiri koneksi apa pun, kecuali jika Anda sangat yakin bahwa koneksi tersebut adalah ancaman nyata!

6.6.3. Mulai otomatis



Dialog ***Mulai Otomatis*** menampilkan daftar semua aplikasi yang dijalankan selama menjalankan ulang sistem Windows. Sering sekali, beberapa aplikasi malware menambahkan diri mereka sendiri ke entri register start-up secara otomatis.

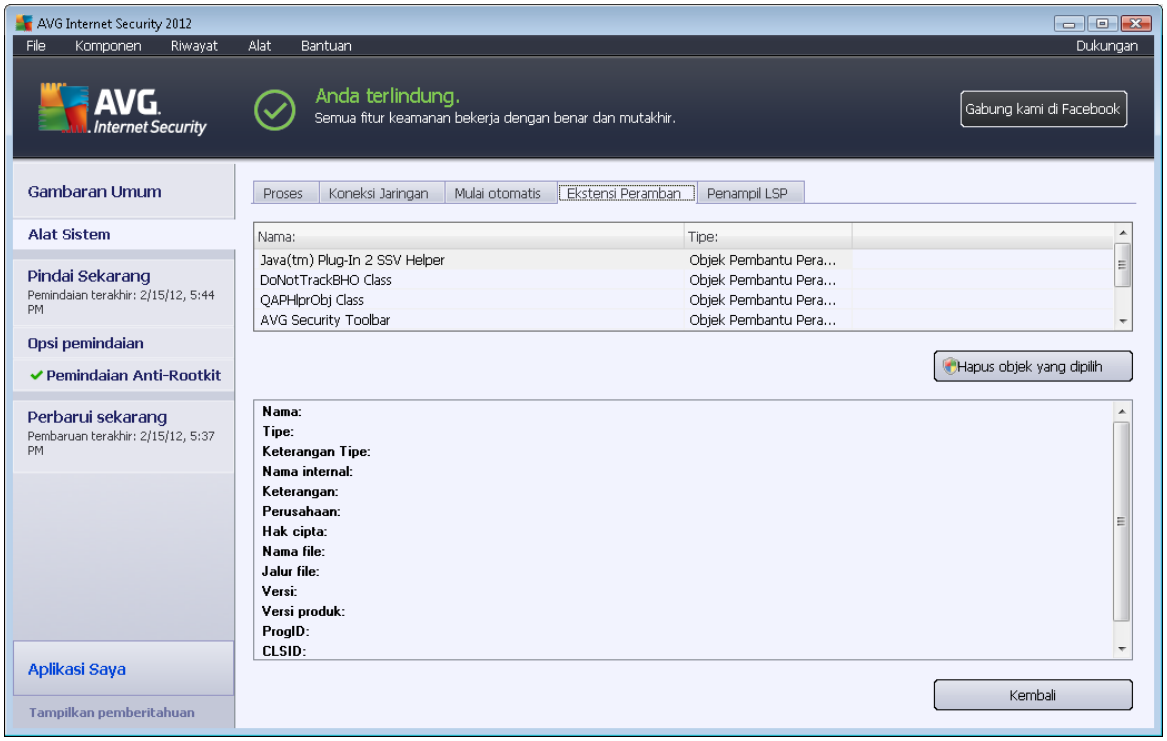
Tombol kontrol

Tombol kontrol yang tersedia dalam tab ***Mulai otomatis*** adalah sebagai berikut:

- ***Hapus yang dipilih*** – tekan tombol ini untuk menghapus satu atau beberapa entri yang dipilih.
- ***Kembali*** – mengembalikan Anda ke dialog utama AVG *(tinjauan umum komponen).*

Kami sangat menyarankan untuk tidak menghapus aplikasi apa pun dalam daftar ini, kecuali jika Anda sangat yakin bahwa aplikasi tersebut adalah ancaman nyata!

6.6.4. Ekstensi Peramban



Dialog ***Ekstensi Peramban*** berisi daftar plugin (*yakni aplikasi*) yang terinstal di dalam peramban Internet Anda. Daftar ini dapat berisi plugin aplikasi biasa maupun program yang berpotensi malware. Klik pada objek dalam daftar untuk memperoleh informasi terperinci mengenai plugin yang dipilih yang akan ditampilkan di bagian bawah dialog.

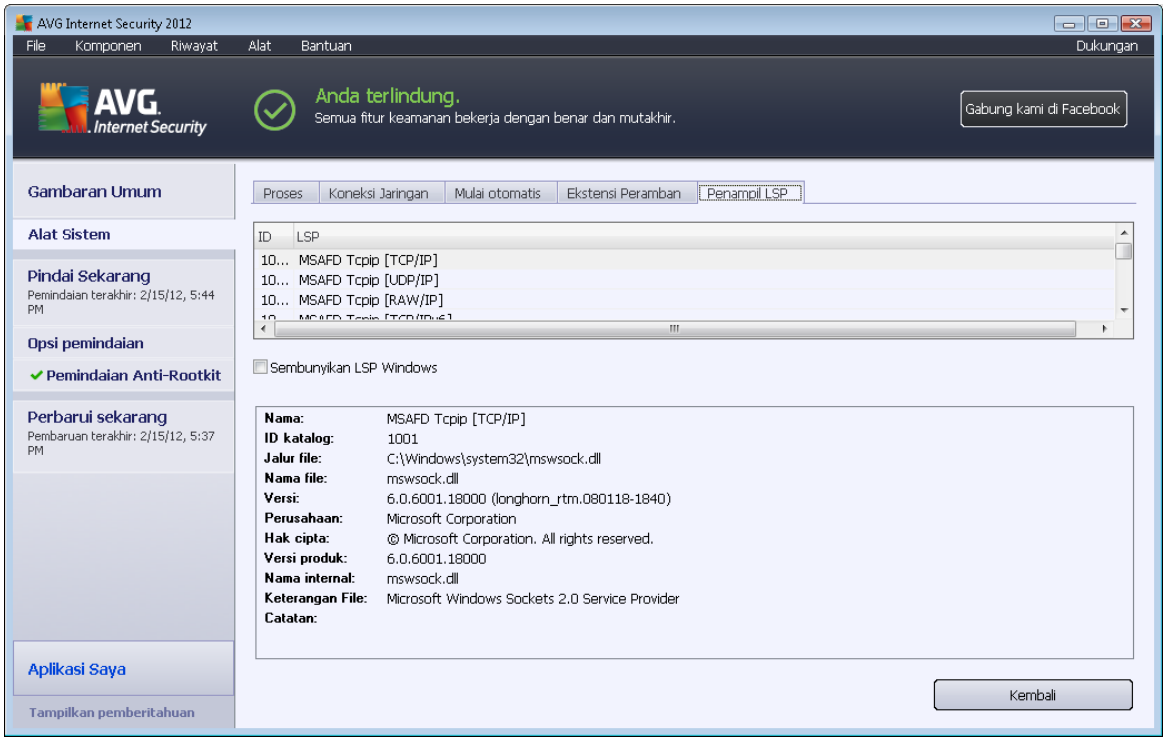
Tombol kontrol

Tombol kontrol yang tersedia dalam tab ***Ekstensi Peramban*** adalah sebagai berikut:

- ***Hapus objek yang dipilih*** – menghapus plugin yang saat ini disorot dalam daftar. ***Kami sangat menganjurkan untuk tidak menghapus plugin apa pun dari daftar ini, kecuali jika Anda sangat yakin bahwa plugin tersebut adalah ancaman nyata!***

- ***Kembali*** – mengembalikan Anda ke dialog utama AVG *(tinjauan umum komponen).*

6.6.5. Penampil LSP



Dialog ***Penampil LSP*** menampilkan daftar Layered Service Provider (LSP).

Layered Service Provider (LSP) adalah driver sistem yang tertaut dengan layanan jaringan sistem operasi Windows. Di sini Anda dapat mengakses semua data yang masuk dan keluar komputer, termasuk mengubah data ini. Beberapa LSP diperlukan agar Windows dapat menghubungkan Anda ke komputer lain, termasuk Internet. Walau demikian, aplikasi malware tertentu juga dapat menginstal dirinya sendiri sebagai LSP, sehingga memiliki akses ke semua data yang dikirimkan oleh komputer Anda. Oleh karena itu, tinjauan ini dapat membantu Anda memeriksa semua kemungkinan ancaman LSP.

Pada keadaan tertentu, LSP yang rusak juga dapat diperbaiki (*misalnya bila file telah dihapus tetapi entri registernya masih belum berubah*). Tombol baru untuk memperbaiki masalah ini akan ditampilkan bila LSP yang dapat diperbaiki ditemukan.

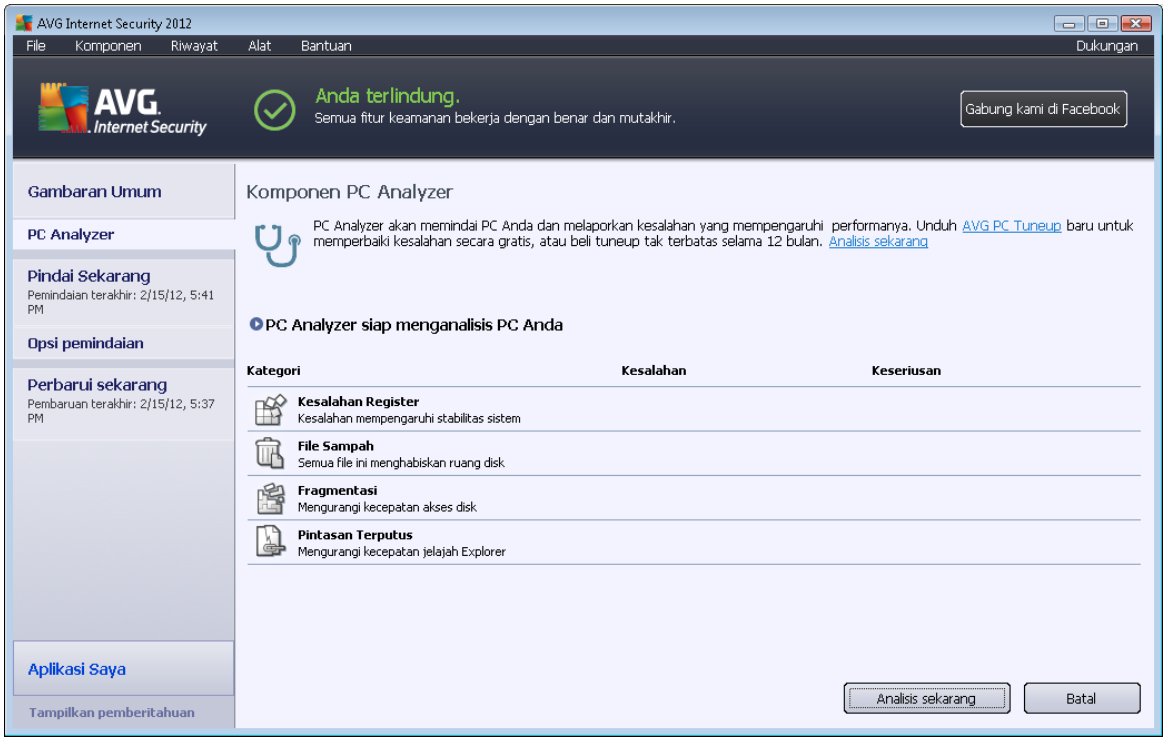
Tombol kontrol

Tombol kontrol yang tersedia dalam tab ***Penampil LSP***adalah sebagai berikut:

- ***Sembunyikan LSP Windows*** – untuk menyertakan LSP Windows dalam daftar, jangan tandai item ini.
- ***Kembali*** – mengembalikan Anda ke dialog utama AVG default (*tinjauan umum komponen*).

6.7. PC Analyzer

Komponen ***PC Analyzer*** dapat melakukan pemindaian masalah sistem pada komputer Anda, dan memberi Anda tinjauan umum yang transparan tentang apa yang mungkin mengganggu kinerja keseluruhan komputer. Dalam antarmuka pengguna komponen, Anda dapat melihat bagan yang dibagi menjadi empat baris yang mengacu pada kategori berikut: kesalahan register, file sampah, fragmentasi dan pintasan rusak:



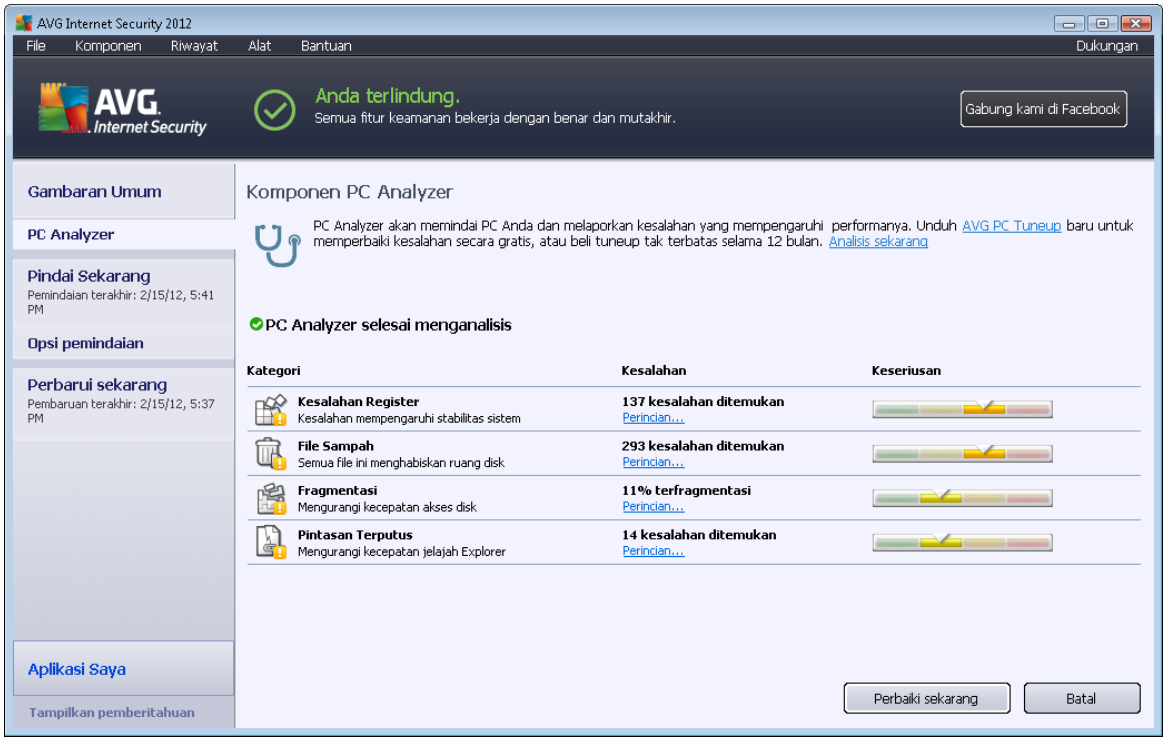
- ***Kesalahan Register*** akan menunjukkan jumlah kesalahan dalam Register Windows. Karena memperbaiki Register memerlukan pengetahuan tingkat lanjut, kami tidak menyarankan untuk mencoba dan memperbaikinya sendiri.

- ***File Sampah*** akan menunjukkan jumlah file yang kemungkinan besar tidak diperlukan. Biasanya, file sampah berisi berbagai jenis file sementara, dan berbagai file dalam Recycle Bin.

- ***Fragmentasi*** akan menghitung persentase hard disk yang terfragmentasi, yaitu yang digunakan dalam waktu lama sehingga sebagian besar file sekarang tersebar di berbagai bagian disk fisik. Anda dapat menggunakan beberapa alat defragmentasi untuk memperbaiki ini.

- ***Pintasan Terputus*** akan memberi tahu Anda mengenai pintasan yang tidak lagi berfungsi, mengarahkan ke lokasi yang tidak ada dll.

Untuk mulai menganalisis sistem Anda, tekan tombol ***Analisis sekarang***. Anda akan dapat melihat kemajuan analisis dan hasilnya langsung pada bagan:



Tinjauan umum hasil menampilkan banyaknya masalah sistem yang terdeteksi (***Kesalahan***) yang dibagi berdasarkan kategori terkait yang diuji. Hasil analisis juga ditampilkan secara grafis pada poros dalam kolom ***Keseriusan***.

Tombol kontrol

- ***Analisis sekarang*** (*ditampilkan sebelum bintang analisis*) - tekan tombol ini untuk meluncurkan analisis saat ini atas komputer Anda
- ***Perbaiki sekarang*** (*ditampilkan setelah analisis selesai*) - tekan tombol ini untuk membuka situs Web AVG (http://www.avg.com/) pada halaman yang memberikan informasi terperinci dan terkini, terkait dengan komponen ***PC Analyzer***
- ***Batal*** – tekan tombol ini untuk menghentikan analisis yang sedang berjalan, atau kembali ke komponen default dialog utama AVG (*tinjauan umum komponen*) setelah analisis selesai

6.8. Identity Protection

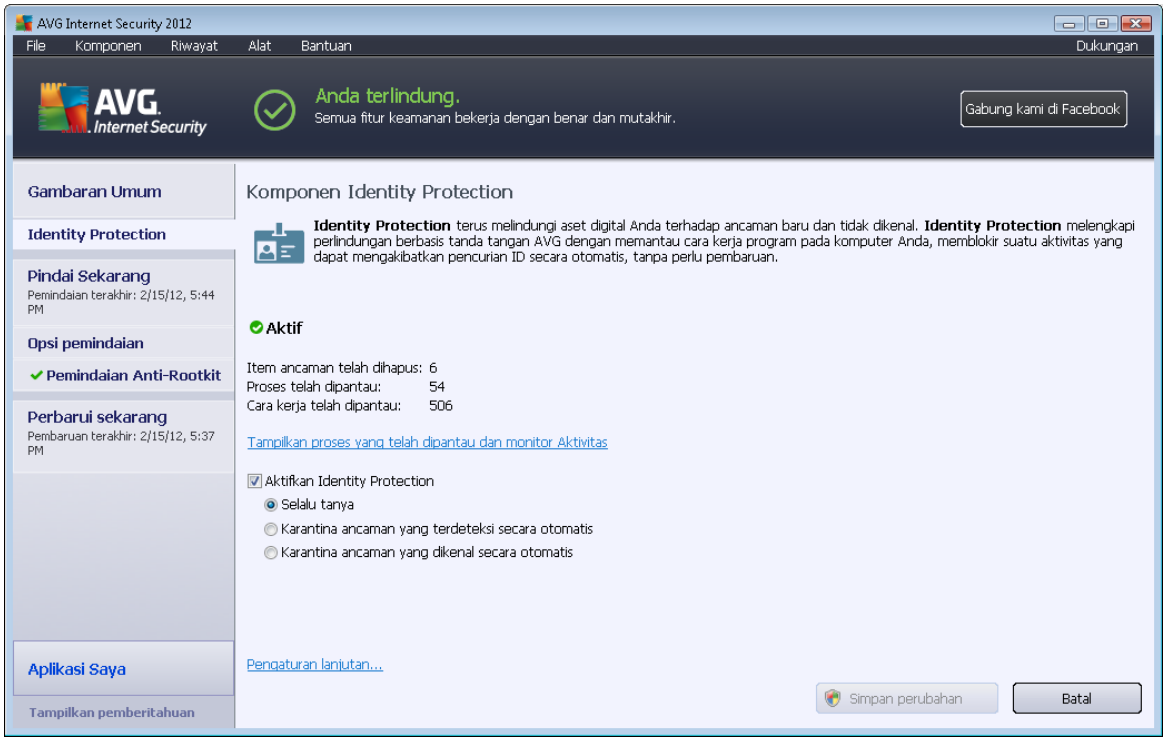
Identity Protection merupakan komponen anti-malware yang melindungi Anda dari semua jenis malware (*spyware, bot, pencurian identitas, ...*) menggunakan teknologi perilaku dan memberikan perlindungan setiap hari dari virus baru. ***Identity Protection*** difokuskan untuk mencegah pencuri identitas berhasil mencuri kata sandi Anda, perincian rekening bank, nomor kartu kredit dan data digital bernilai lainnya dengan menggunakan semua jenis perangkat lunak jahat (*malware*) yang menarget PC Anda. Ini memastikan bahwa semua program yang dijalankan pada PC Anda atau di jaringan berbagi Anda beroperasi dengan benar. ***Identity Protection*** menemukan dan memblokir

perilaku mencurigakan secara terus-menerus dan melindungi komputer Anda dari semua malware baru.

Identity Protection memberikan perlindungan seketika bagi komputer Anda terhadap berbagai ancaman baru, bahkan yang tidak dikenal. Ia memantau semua proses *(termasuk yang tersembunyi)* dan lebih dari 285 macam pola perilaku, dan dapat menentukan apakah sesuatu yang membahayakan terjadi dalam sistem Anda. Oleh karena itu, ia dapat mengetahui ancaman yang bahkan belum diterangkan dalam basis data virus. Bila sebuah kode yang tidak dikenal masuk ke komputer Anda, kode tersebut segera diamati dan dipantau apakah menunjukkan perilaku jahat. Jika ternyata file tersebut jahat, ***Identity Protection*** akan memindahkan kode tersebut ke Gudang Virus dan membatalkan semua perubahan pada sistem yang telah dilakukannya *(injeksi kode, perubahan register, pembukaan port, dsb.)*. Anda tidak perlu memulai pemindaian untuk tetap terlindungi. Teknologi ini sangat proaktif, jarang memerlukan pembaruan, dan selalu siaga.

Identity Protection adalah perlindungan pelengkap untuk Anti-Virus. Kami sangat menyarankan Anda menginstal kedua komponen, untuk mendapatkan perlindungan penuh bagi PC Anda!

6.8.1. Identity Protection Antarmuka



Dialog ***Identity Protection*** memberikan keterangan singkat tentang fungsionalitas dasar komponen, statusnya *(Aktif)*, dan beberapa data statistik:

- ***Item ancaman telah dihapus*** – memberikan jumlah aplikasi yang terdeteksi sebagai malware, dan telah dihapus
- ***Proses telah dipantau*** – jumlah aplikasi yang saat ini berjalan yang dipantau oleh IDP

- ***Cara kerja telah dipantau*** – jumlah tindakan spesifik yang berjalan dalam aplikasi yang dipantau

Di bawah ini Anda dapat menemukan tautan Tampilkan proses yang diawasi dan Pengawasan aktivitas yang akan membawa Anda ke antarmuka pengguna komponen Alat sistem tempat Anda dapat menemukan tinjauan terperinci tentang seluruh proses yang diawasi.

Pengaturan Dasar Identity Protection

Di bagian bawah dialog, Anda dapat mengedit beberapa fitur dasar dari fungsionalitas komponen:

- ***Aktifkan Identity Protection*** - (*diaktifkan secara default*): tandai untuk mengaktifkan komponen IDP, dan untuk membuka opsi pengeditan lebih lanjut.

  Dalam beberapa kasus, ***Identity Protection*** mungkin melaporkan bahwa beberapa file yang sah bersifat mencurigakan atau berbahaya. Karena ***Identity Protection*** mendeteksi ancaman berdasarkan cara kerjanya, hal ini biasanya terjadi saat beberapa program berusaha memantau penekanan tombol, menginstal program lain atau ada driver baru yang diinstal pada komputer. Karena itu, pilih salah satu opsi berikut yang menetapkan cara kerja komponen ***Identity Protection*** jika ada deteksi aktivitas yang mencurigakan:

  - ***Selalu tanya*** – jika aplikasi terdeteksi sebagai malware, Anda akan ditanya apakah akan memblokirnya (*opsi ini diaktifkan secara default dan disarankan untuk tidak mengubahnya kecuali Anda memiliki alasan kuat untuk mengubahnya*)
  - ***Karantina ancaman yang terdeteksi secara otomatis*** - semua aplikasi yang terdeteksi sebagai malware akan diblokir secara otomatis
  - ***Karantina ancaman yang dikenal secara otomatis*** - hanya aplikasi yang benar-benar pasti terdeteksi sebagai malware yang akan diblokir

- ***Pengaturan lanjutan...*** – Klik tautan ini untuk dialihkan ke dialog yang bersangkutan dalam Pengaturan lanjutan pada **Keamanan Intenet AVG 2012**. Di sana Anda dapat mengedit konfigurasi komponen secara terperinci. Namun, harap perhatikan bahwa konfigurasi default pada semua komponen telah diatur agar **Keamanan Intenet AVG 2012** memberikan performa optimal dan keamanan maksimum. Jika Anda tidak memiliki alasan kuat untuk itu, disarankan agar membiarkan konfigurasi default!

Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka ***Identity Protection*** adalah sebagai berikut:

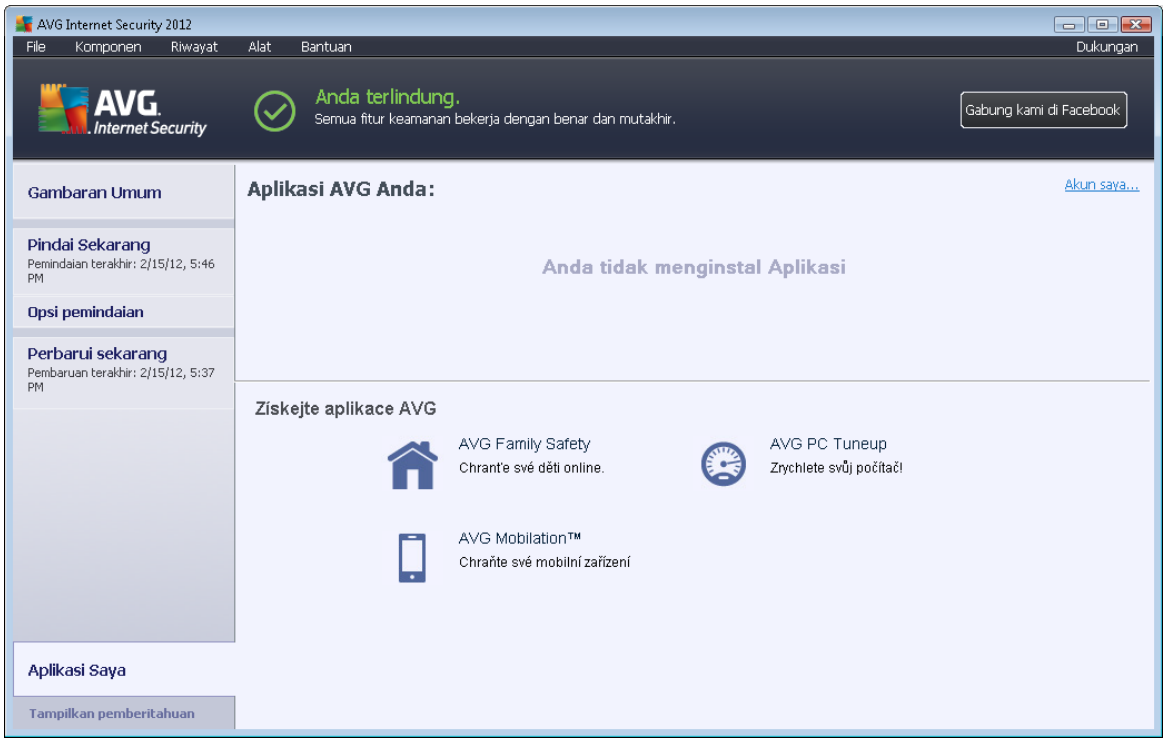
- ***Simpan perubahan*** – tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini
- ***Batal*** – tekan tombol ini untuk kembali ke dialog utama AVG default (*tinjauan umum komponen*)

6.9. Administrasi Jarak Jauh

Komponen ***Administrasi Jarak Jauh*** hanya ditampilkan dalam antarmuka pengguna **Keamanan Intenet AVG 2012** jika Anda telah menginstal produk Business Edition *(untuk informasi mengenai lisensi yang digunakan untuk instalasi, harap lihat tab Versi pada dialog Informasi yang dapat dibuka melalui item menu sistem Dukungan)*. Untuk keterangan terperinci mengenai berbagai opsi komponen dan fungsionalitasnya dalam sistem AVG Remote Administration, bacalah dokumentasi spesifik khusus untuk topik ini. Dokumentasi tersedia untuk diunduh di situs Web AVG (http://www.avg.com/), di bagian ***Pusat Dukungan/Unduhan/Dokumentasi***.

7. Aplikasi Saya

Dialog ***Aplikasi Saya*** *(dapat diakses melalui tombol Aplikasi Saya langsung dari dialog utama AVG)* memberikan gambaran umum mengenai aplikasi mandiri AVG, keduanya sudah diinstal pada komputer Anda atau siap untuk diinstal, bebas pilih:



Dialog ini dibagi menjadi 2 bagian:

- ***Aplikasi AVG Anda*** – memberikan gambaran umum mengenai aplikasi mandiri AVG yang sudah dinstal pada komputer Anda;
- ***Dapatkan Aplikasi AVG*** – menawarkan gambaran umum mengenai aplikasi mandiri AVG yang dapat membuat Anda tertarik. Aplikasi-aplikasi ini siap untuk diinstal. Penawaran ini berubah secara dinamis berdasarkan lisensi Anda, lokasi, dan kriteria lainnya. Untuk informasi terperinci mengenai aplikasi-aplikasi ini, silakan kunjungi situs Web AVG (http://www.avg.com/).

Setelah itu, temukan gambaran umum singkat mengenai semua aplikasi yang tersedia dan penjelasan singkat mengenai fungsionalitasnya:

7.1. AVG Family Safety

AVG Family Safety membantu Anda melindungi anak-anak dari situs Web, konten media, dan penelusuran online yang tidak pantas, serta memberi Anda laporan mengenai aktivitas online mereka. ***AVG Family Safety*** menggunakan teknologi tekanan-tombol untuk memantau aktivitas anak Anda di ruang obrolan dan pada situs jejaring sosial. Jika ditemukan kata, frasa, atau bahasa yang diketahui digunakan untuk menipu anak-anak saat online, Anda segera diberi tahu melalui

SMS atau email. Aplikasi ini memungkinkan Anda mengatur tingkat perlindungan yang sesuai untuk masing-masing dari anak Anda dan memantau mereka secara terpisah melalui login unik.

Untuk mengetahui informasi terperinci, harap kunjungi halaman Web AVG khusus, tempat Anda juga dapat mengunduh komponen dengan segera. Untuk melakukannya, Anda dapat menggunakan tautan AVG Family Safety dalam dialog Aplikasi Saya.

7.2. AVG LiveKive

AVG LiveKive dikhususkan untuk pencadangan data online di server aman. ***AVG LiveKive*** secara otomatis mencadangkan semua file, foto, dan musik Anda ke satu tempat yang aman, sehingga Anda dapat berbagi dengan keluarga dan teman dan mengaksesnya dari perangkat apa saja yang berkemampuan Web, termasuk perangkat iPhone dan Android. ***AVG LiveKive*** meliputi fitur:

- Tindakan keamanan jika komputer dan/atau harddisk Anda korup
- Akses ke data Anda dari perangkat yang terhubung ke Internet
- Mudah dikelola
- Berbagi dengan siapa saja yang Anda izinkan

Untuk mengetahui informasi terperinci, harap kunjungi halaman Web khusus AVG, di mana Anda juga dapat mengunduh komponen dengan segera. Untuk melakukannya, Anda dapat menggunakan tautan AVG LiveKive dalam dialog Aplikasi Saya.

7.3. AVG Mobilation

AVG Mobilation melindungi ponsel Anda dari virus dan malware dan dapat melacak ponsel cerdas Anda dari jarak jauh jika Anda terpisah dari ponsel tersebut. Fitur ***AVG Mobilation*** meliputi:

- *Pemindai File* memungkinkan pemindaian keamanan pada file di berbagai lokasi penyimpanan;
- *Task Killer* memungkinkan Anda menghentikan aplikasi jika perangkat berjalan lambat atau macet;
- *App Locker* memungkinkan Anda mengunci dan melindungi satu atau beberapa aplikasi dari penyalahgunaan dengan kata sandi;
- *Tuneup* mengumpulkan berbagai parameter sistem *(pengukur kondisi baterai, penggunaan penyimpanan, ukuran dan lokasi instalasi aplikasi, dsb.)* ke dalam sebuah tampilan sentralisasi tunggal untuk membantu Anda mengontrol performa sistem;
- *App Backup* memungkinkan Anda mencadangkan aplikasi ke kartu SD dan mengembalikannya di lain waktu;
- *Fitur Spam dan Scam* memungkinkan Anda menandai pesan SMS sebagai spam dan melaporkan situs Web sebagai scam;

- *Menghapus data pribadi* dari jarak jauh jika ponsel Anda dicuri;

- *Safe Web Surfing* menawarkan pemantauan seketika pada halaman Web yang Anda kunjungi.

Untuk mengetahui informasi terperinci, harap kunjungi halaman Web AVG khusus, tempat Anda juga dapat mengunduh komponen dengan segera. Untuk melakukannya, Anda dapat menggunakan tautan AVG Mobilation di dialog Aplikasi Saya.

7.4. AVG PC TuneUp

Aplikasi ***AVG PC TuneUp*** adalah alat tingkat lanjut untuk analisis dan koreksi sistem terperinci, misalnya bagaimana kecepatan dan keseluruhan performa komputer Anda dapat ditingkatkan. ***AVG PC Tuneup*** meliputi fitur:

- *Pembersih Disk* – Menghapus file sampah yang memperlambat komputer Anda.
- *Perapi Disk* - Merapikan drive disk dan mengoptimalkan penempatan file sistem.
- *Pembersih Register* – Memperbaiki kesalahan register untuk meningkatkan stabilitas PC.
- *Perapi Register* – Merapikan register dengan mengurangi celah yang menghabiskan memori.
- *Dokter Disk* – Mencari sektor rusak, cluster hilang, dan kesalahan direktori serta memperbaikinya.
- *Pengoptimal Internet* - Membuat pengaturan terbaik untuk koneksi Internet khusus.
- *Penghapus Jejak* – Menghapus riwayat penggunaan komputer dan Internet.
- *Penyapu Disk* – Membersihkan ruang kosong pada disk untuk mencegah pemulihan data sensitif.
- *Penghancur File* – Menghapus file yang dipilih tanpa bisa dipulihkan lagi pada disk atau stik USB.
- *Pemulihan File* – Memulihkan file yang terhapus secara tidak sengaja dari disk, stik USB, atau kamera.
- *Pencari File Duplikat* – Membantu menemukan dan menghapus file duplikat yang memboroskan ruang disk.
- *Pengatur Layanan* – Menonaktifkan layanan tidak perlu yang memperlambat komputer.
- *Pengatur Startup* – Memungkinkan pengguna mengatur program yang akan dijalankan secara otomatis pada saat Windows dimulai.
- *Pengatur Hapus Instalasi* – Menghapus tuntas instalasi program perangkat lunak yang

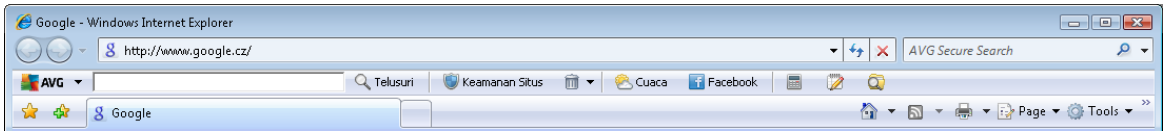
tidak lagi Anda perlukan.

- *Pengatur Penyempurnaan* - Memungkinkan pengguna menyetel ratusan pengaturan Windows yang tersembunyi.
- *Pengatur Tugas* - Menampilkan daftar semua proses yang sedang dijalankan, layanan, dan file terkunci.
- *Penjelajah Disk* - Menampilkan file apa saja yang paling banyak memakan tempat di komputer.
- *Informasi Sistem* – Memberikan informasi terperinci tentang perangkat keras yang terpasang dan perangkat lunak yang terinstal.

Untuk mengetahui informasi terperinci, harap kunjungi halaman Web AVG khusus, tempat Anda juga dapat mengunduh komponen dengan segera. Untuk melakukannya, Anda dapat menggunakan tautan AVG PC TuneUp dalam dialog Aplikasi Saya.

8. AVG Security Toolbar

AVG Security Toolbar adalah alat yang erat bekerja sama dengan komponen LinkScanner, dan menjaga keamanan maksimum Anda saat menjelajah Internet. Dalam **Keamanan Intenet AVG 2012**, instalasi ***AVG Security Toolbar*** bersifat opsional; selama proses instalasi Anda diminta memutuskan apakah komponen tersebut harus diinstal. ***AVG Security Toolbar*** tersedia secara langsung dalam peramban Internet Anda. Untuk saat ini, peramban Internet yang didukung adalah Internet Explorer (*versi 6.0 dan yang lebih tinggi*), dan/atau Mozilla Firefox (*versi 3.0 dan yang lebih tinggi*). Tidak ada peramban lain yang didukung *(jika Anda menggunakan peramban Internet alternatif, misalnya Avant Browser, maka Anda dapat mengalami cara kerja yang tidak diharapkan)*.

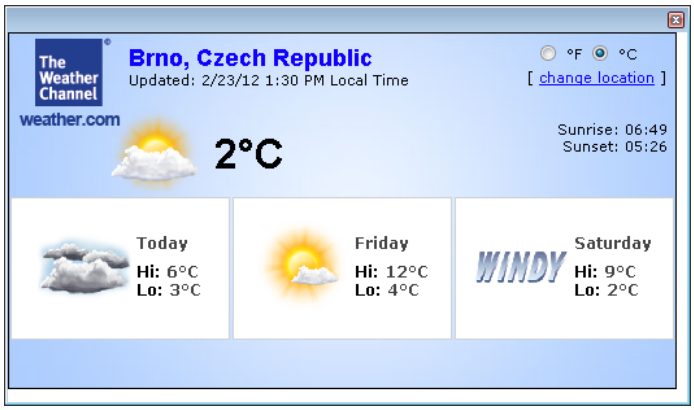


AVG Security Toolbar terdiri dari item berikut:

- ***Logo AVG*** dengan menu buka-bawah:
  - ***Gunakan AVG Secure Search*** - Memungkinkan Anda menelusuri langsung dari ***AVG Security Toolbar*** dengan mesin ***AVG Secure Search***. Semua hasil telusur terus-menerus diperiksa oleh layanan Search-Shield, dan Anda dapat merasa benar-benar aman saat online.
  - ***Tingkat Ancaman Saat Ini*** - Membuka halaman Web lab virus yang berisi tampilan grafis mengenai tingkat ancaman saat ini di Web.
  - ***Lab Ancaman AVG*** – Membuka situs Web ***Lab Ancaman AVG*** tertentu *(pada http://www.avgthreatlabs.com)* tempat Anda dapat menemukan informasi mengenai berbagai situs Web keamanan dan tingkat ancaman saat ini secara online.
  - ***Bantuan Bilah Alat*** – Membuka bantuan online yang mencakup semua fungsionalitas ***AVG Security Toolbar***.
  - ***Kirim Masukan Produk*** – Membuka halaman Web berisi formulir yang dapat Anda isi dan memberi tahu kami apa yang Anda rasakan tentang ***AVG Security Toolbar***.
  - ***Tentang...*** – Membuka jendela baru berisi informasi mengenai versi ***AVG Security Toolbar*** yang saat ini terinstal.
- ***Bidang telusur*** - Menelusuri Internet menggunakan ***AVG Security Toolbar*** agar benar-benar aman dan nyaman karena semua hasil telusur yang ditampilkan seratus persen aman. Masukkan kata kunci atau kalimat ke dalam bidang penelusuran, dan tekan tombol ***Telusuri*** *(atau Enter)*. Semua hasil telusur terus-menerus diperiksa oleh layanan Search-Shield *(dalam komponen LinkScanner)*.
- ***Keamanan Situs*** – Tombol ini akan membuka dialog baru yang membuktikan informasi pada tingkat ancaman saat ini (*Aman saat ini*) dari halaman yang sedang Anda kunjungi. Ikhtisar singkat ini dapat diperluas, dan ditampilkan dengan perincian lengkap tentang semua kegiatan keamanan yang berkaitan dengan halaman, tepat dalam jendela peramban (*Lihat laporan lengkap*):

- ***Hapus*** – Tombol 'tong sampah' menyediakan menu roll down, tempat Anda dapat memilih apakah Anda ingin menghapus informasi tentang jelajah, unduhan, formulir online, atau menghapus semua riwayat penelusuran Anda sekaligus.

- ***Cuaca*** – Tombol ini membuka dialog baru yang memberikan informasi mengenai cuaca saat ini di lokasi Anda, serta prakiraan cuaca untuk dua hari mendatang. Informasi ini rutin diperbarui setiap 3-6 jam. Dalam dialog, Anda dapat mengubah lokasi yang diinginkan secara manual, dan memutuskan apakah Anda ingin melihat info suhu dalam Celsius atau Fahrenheit.



- ***Facebook*** – Tombol ini memungkinkan Anda menghubungkan ke jaringan sosial Facebook langsung dari dalam ***AVG Security Toolbar***.

- Tombol pintasan untuk akses cepat ke aplikasi ini: ***Calculator***, ***Notepad***, ***Windows Explorer***.

9. AVG Do Not Track

AVG Do Not Track membantu Anda mengidentifikasi situs web yang sedang mengumpulkan data tentang aktivitas online Anda. Salah satu ikon di peramban Anda menampilkan situs web atau pengiklan yang mengumpulkan data tentang aktivitas Anda dan memberi Anda pilihan untuk mengizinkan atau tidak mengizinkannya.

- ***AVG Do Not Track*** memberikan informasi tambahan untuk Anda tentang kebijakan privasi layanan terkait, begitu juga tautan langsung untuk Keluar dari layanan, jika tersedia.
- Selain itu, ***AVG Do Not Track*** mendukung protokol W3C DNT untuk secara otomatis memberitahu situs yang tidak ingin dilacak. Pemberitahuan ini diaktifkan secara default, tetapi dapat diubah kapan pun.
- ***AVG Do Not Track*** diberikan berdasarkan syarat dan ketentuan ini.
- ***AVG Do Not Track diaktifkan secara default, tetapi dapat dengan mudah dinonaktifkan kapan pun.*** Petunjuknya dapat ditemukan di artikel Tanya-Jawab Menonaktifkan fitur AVG Do Not Track.
- Untuk informasi selanjutnya tentang ***AVG Do Not Track***, silakan kunjungi situs web kami.

Saat ini, fungsionalitas ***AVG Do Not Track*** hanya didukung di peramban Mozilla Firefox, Chrome, dan Internet Explorer. *(Di Internet Explorer, ikon AVG Do Not Track terletak di sisi kanan batang perintah. Jika Anda mengalami masalah melihat ikon AVG Do Not Track dengan pengaturan standar peramban, pastikan bahwa Anda telah mengaktifkan batang perintah. Jika Anda masih tidak dapat melihat ikon tersebut, tarik batang perintah ke kiri untuk membuka semua ikon dan tombol yang tersedia dalam toolbar ini.)*

9.1. Antarmuka AVG Do Not Track

Ketika online, ***AVG Do Not Track*** segera memperingatkan Anda bila ada aktivitas pengumpulan data yang terdeteksi. Anda akan melihat dialog berikut ini:

Semua layanan pengumpulan data yang terdeteksi didaftar berdasarkan nama di ***Trackers pada tinjauan umum*** halaman ini. Ada tiga tipe aktivitas pengumpulan data yang dikenali oleh ***AVG Do Not Track***:

- ***Web Analytics*** *(diperbolehkan secara default):* Layanan yang digunakan untuk meningkatkan kinerja dan pengalaman situs web terkait. Dalam kategori ini Anda dapat menemukan layanan seperti Google Analytics, Omniture, atau Yahoo Analytics. Kami menyarankan untuk tidak memblokir layanan web analytics, karena situs web mungkin tidak bekerja sesuai yang dimaksudkan.

- ***Social Buttons*** *(diperbolehkan secara default):* Elemen yang didesain untuk meningkatkan pengalaman berjejaring sosial. Tombol sosial dijalankan dari jejaring sosial ke situs yang sedang Anda kunjungi. Tombol tersebut dapat mengumpulkan data tentang aktivitas online Anda jika Anda masuk. Contoh-contoh tombol Sosial antara lain: Plugin Sosial Facebook, Tombol Twitter, dan Google +1.

- ***Ad Networks*** *(beberapa diblokir secara default):* Layanan yang mengumpulkan atau membagikan data tentang aktivitas online Anda ke banyak situs, baik secara langsung maupun tidak langsung, untuk menawari Anda Iklan yang dipersonalisasi dan tidak seperti Iklan yang berbasis konten. Layanan ini ditentukan berdasarkan kebijakan privasi masing-masing jaringan Iklan sebagaimana tersedia di situs web jaringan Iklan tersebut. Beberapa jaringan iklan diblokir secara default.

Catatan: *Tergantung pada layanan yang berjalan di latar belakang situs web, 3 bagian yang diterangkan di atas mungkin tidak muncul pada dialog AVG Do Not Track.*

Dialog ini juga berisi dua hipertatut:

- ***Apa itu pelacakan?*** - klik tautan ini di bagian atas dialog agar Anda diarahkan kembali ke laman web khusus yang menyediakan penjelasan terperinci tentang prinsip-prinsip pelacakan, dan keterangan tipe-tipe pelacakan spesifik.

- ***Pengaturan*** - klik tautan di bagian bawah dialog agar Anda diarahkan kembali ke laman web, agar Anda dapat menetapkan konfigurasi spesifik berbagai parameter ***AVG Do Not Track*** *(lihat bab pengaturan AVG Do Not Track untuk informasi lengkap)*

9.2. Informasi tentang proses pelacakan

Daftar layanan pengumpulan data yang terdeteksi hanya menyediakan nama layanan tertentu. Untuk membuat keputusan cepat tentang apakah masing-masing layanan harus diblokir atau diizinkan, Anda mungkin perlu tahu lebih banyak. Gerakkan mouse Anda ke masing-masing item daftar. Sebuah gelembung informasi muncul dengan memberikan data terperinci tentang layanan. Anda akan mengetahui apakah layanan pelacakannya mengumpulkan data pribadi Anda atau data lain yang tersedia; apakah data sedang dibagi dengan subjek pihak ketiga lain, dan apakah data yang dikumpulkan sedang disimpan untuk kemungkinan tujuan lebih lanjut.

Di bagian bawah gelembung informasi, Anda dapat melihat hyperlink ***Kebijakan Privasi*** yang mengarahkan Anda ke situs web khusus untuk kebijakan privasi dari masing-masing layanan yang terdeteksi.

9.3. Memblokir proses pelacakan

Dengan daftar semua Ad Networks / Social Buttons / Web Analytics, Anda sekarang memiliki opsi untuk mengontrol layanan mana yang harus diblokir. Anda dapat memakai dua cara:

- ***Blokir Semua*** - Klik tombol ini yang terletak di bagian bawah dialog untuk menyatakan Anda tidak menginginkan aktivitas pengumpulan data sama sekali. *(Namun, harap ingat bahwa tindakan ini mungkin merusak fungsionalitas di laman web terkait di mana layanan ini sedang berjalan!)*

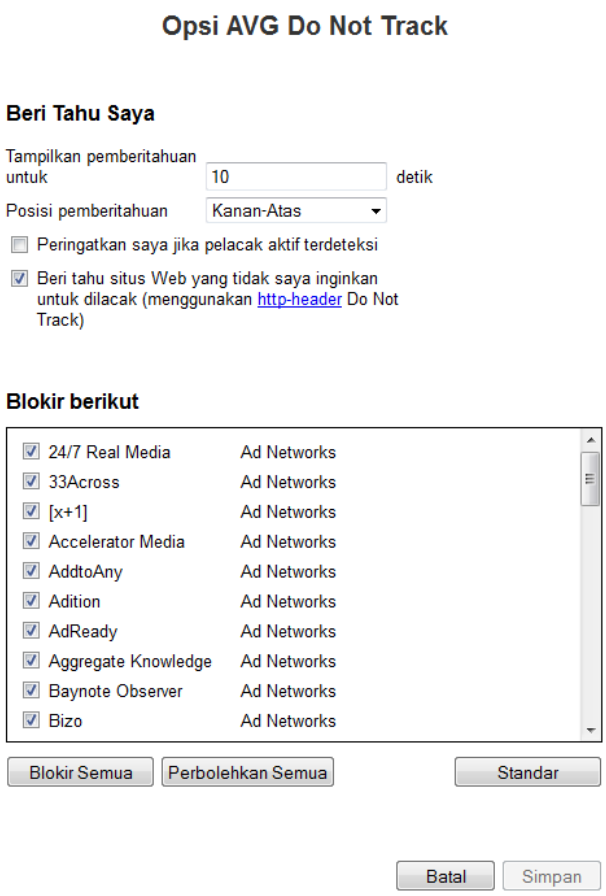
-  - Jika Anda tidak ingin memblokir semua sistem yang terdeteksi sekaligus, Anda dapat menentukan apakah layanan tersebut harus diizinkan atau diblokir satu per satu. Anda mungkin memperbolehkan untuk menjalankan beberapa sistem yang terdeteksi *(misalnya: Web Analytics):* sistem ini menggunakan data yang dikumpulkan untuk pengoptimalan situs web mereka sendiri, dan dengan cara ini mereka membantu meningkatkan lingkungan Internet secara umum bagi semua pengguna. Namun, pada saat yang sama Anda dapat memblokir aktivitas pengumpulan data semua proses yang diklasifikasikan sebagai Ad Networks. Cukup klik ikon  di samping masing-masing layanan untuk memblokir pengumpulan data *(nama proses akan muncul sebagai dicoret)*, atau untuk memperbolehkan pengumpulan data kembali.

9.4. Pengaturan AVG Do Not Track

Langsung dalam dialog ***AVG Do Not Track***, hanya ada satu opsi konfigurasi: di bagian bawah Anda dapat melihat kotak centang ***Peringatkan saya jika pelacak aktif terdeteksi***. Secara standar, item ini dibatalkan. Tandai kotak centang untuk mengonfirmasi bahwa Anda ingin diberi tahu setiap kali memasuki laman web yang berisi layanan pengumpulan data baru yang belum diblokir. Ketika

ditandai, jika ***AVG Do Not Track*** mendeteksi layanan pengumpulan data baru di halaman yang saat ini Anda kunjungi, dialog pemberitahuan muncul pada layar Anda. Jika tidak, Anda hanya dapat melihat layanan yang baru terdeteksi dengan ikon ***AVG Do Not Track*** *(yang terletak di batang perintah peramban Anda)* yang berubah warnanya dari hijau ke kuning.

Namun, di bagian bawah dialog ***AVG Do Not Track***, Anda dapat menemukan tautan ***Pengaturan***. Klik tautan agar diarahkan ke halaman web khusus yang di dalamnya Anda dapat menentukan ***Opsi AVG Do Not Track*** terperinci Anda:



- ***Posisi pemberitahuan*** *(Kanan-Atas secara standar)* - Buka menu roll-down untuk menentukan di posisi mana Anda menginginkan dialog ***AVG Do Not Track*** muncul di monitor Anda.
- ***Tampilkan pemberitahuan selama*** *(10 secara standar)* - Di bidang ini, Anda harus menentukan selama berapa lama *(dalam detik)* Anda ingin melihat pemberitahuan ***AVG Do Not Track*** di layar Anda. Anda dapat menentukan angka mulai dari 0 sampai 60 detik *(selama 0, pemberitahuan tidak akan muncul pada layar Anda sama sekali)*.
- ***Peringatkan saya jika pelacak aktif terdeteksi*** *(nonaktif secara default)* - Tandai kotak centang untuk mengonfirmasi bahwa Anda ingin diberi tahu setiap kali memasuki laman web yang berisi layanan pengumpulan data baru yang belum diblokir. Ketika ditandai, jika

AVG Do Not Track mendeteksi layanan pengumpulan data baru di halaman yang saat ini Anda kunjungi, dialog pemberitahuan muncul pada layar Anda. Jika tidak, Anda hanya dapat melihat layanan yang baru terdeteksi dengan ikon ***AVG Do Not Track*** *(yang terletak di batang perintah peramban Anda)* yang berubah warnanya dari hijau ke kuning.

- ***Beri tahu situs web yang tidak saya inginkan untuk dilacak*** *(aktif secara standar)* - Centang pilihan ini untuk mengonfirmasi bahwa Anda menginginkan ***AVG Do Not Track*** untuk menginformasikan penyedia layanan pelacakan yang terdeteksi yang tidak Anda inginkan untuk dilacak.

- ***Blokir*** *berikut (semua layanan pengumpulan data tercantum diperbolehkan secara standar)* – Di bagian ini, Anda dapat melihat sebuah kotak dengan daftar layanan pengumpulan data yang dapat diklasifikasikan sebagai Ad Networks. Secara standar, ***AVG Do Not Track*** memblokir beberapa Ad Networks secara otomatis dan keputusan pemblokiran ini tetap bergantung Anda apakah sisanya harus diblokir juga, atau dibiarkan diizinkan. Untuk melakukannya, cukup klik tombol ***Blokir Semua*** di bawah daftar.

Tombol kontrol yang tersedia dalam halaman ***AVG Do Not Track Options*** adalah sebagai berikut:

- ***Blokir Semua*** – klik untuk sekaligus memblokir semua layanan yang tercantum dalam kotak di atas yang diklasifikasikan sebagai Jaringan Iklan;

- ***Perbolehkan Semua*** – klik untuk sekaligus membuka semua layanan yang sebelumnya diblokir yang tercantum dalam kotak di atas dan diklasifikasikan sebagai Jaringan Iklan;

- ***Standar*** – klik untuk menghapus semua pengaturan khusus Anda, dan untuk kembali ke konfigurasi standar;

- ***Simpan*** – klik untuk menerapkan dan menyimpan semua konfigurasi yang Anda tetapkan;

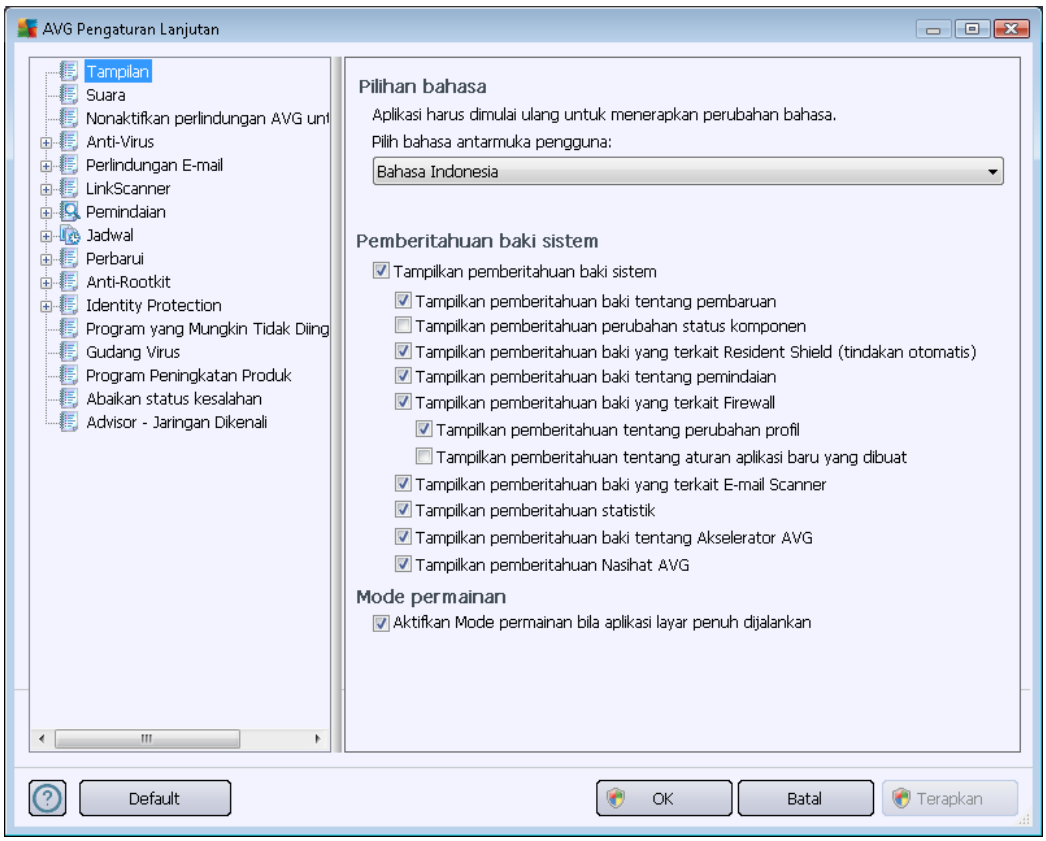
- ***Batal*** – klik untuk membatalkan semua pengaturan yang telah Anda tetapkan sebelumnya.

10. Pengaturan Lanjutan AVG

Dialog konfigurasi lanjutan **Keamanan Intenet AVG 2012** akan membuka jendela baru bernama ***Pengaturan AVG Lanjutan***. Jendela ini terbagi dua bagian: bagian kiri menawarkan navigasi dengan susunan terstruktur ke berbagai opsi konfigurasi program. Pilih komponen yang ingin Anda ubah konfigurasinya (*atau bagian spesifiknya*) untuk membuka dialog pengeditan di bagian sebelah kanan jendela.

10.1. Tampilan

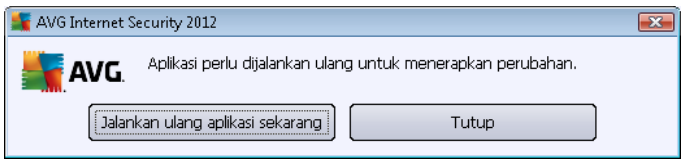
Item pertama pada struktur navigasi, ***Tampilan***, mengacu pada pengaturan umum antarmuka pengguna **Keamanan Intenet AVG 2012**, dan menyediakan beberapa opsi mendasar pada cara kerja aplikasi:



Pemilihan bahasa

Di bagian ***Pemilihan bahasa*** Anda dapat memilih bahasa yang diinginkan dari menu buka-bawah. Bahasa yang dipilih kemudian akan digunakan untuk seluruh antarmuka pengguna **Keamanan Intenet AVG 2012**. Menu buka-bawah hanya menawarkan bahasa yang sebelumnya telah Anda pilih untuk diinstal selama proses instalasi (*lihat bab Opsi khusus*) plus Bahasa Inggris (*Bahasa Inggris selalu diinstal secara otomatis, secara default*). Untuk menyelesaikan perpindahan **Keamanan Intenet AVG 2012** Anda ke bahasa lain, Anda harus menjalankan ulang aplikasi. Harap ikuti langkah-langkah ini:

- Dalam menu buka-bawah, pilih bahasa yang diinginkan pada aplikasi
- Konfirmasi pilihan Anda dengan menekan tombol ***Terapkan*** *(sudut kanan bawah dialog)*
- Tekan tombol ***OK*** untuk mengkonfirmasi
- Sebuah dialog baru akan muncul yang memberi tahu Anda bahwa untuk mengubah bahasa aplikasi, Anda perlu menjalankan ulang **Keamanan Intenet AVG 2012**
- Tekan tombol ***Jalankan ulang aplikasi sekarang*** untuk menyetujui menjalankan ulang program, dan tunggu sebentar hingga perubahan bahasa diberlakukan:



Pemberitahuan baki sistem

Dalam bagian ini Anda dapat menyembunyikan tampilan pemberitahuan baki sistem mengenai status aplikasi **Keamanan Intenet AVG 2012**. Secara default, pemberitahuan sistem diperbolehkan untuk ditampilkan. Sangat disarankan untuk membiarkan konfigurasi ini! Pemberitahuan sistem misalnya memberi tahu diluncurkannya pemindaian atau proses pembaruan, atau mengenai perubahan status komponen **Keamanan Intenet AVG 2012** . Anda harus memperhatikan pemberitahuan ini!

Walau demikian, jika karena beberapa alasan Anda tidak ingin diberi tahu dengan cara ini, atau Anda hanya ingin melihat pemberitahuan tertentu *(berhubungan dengan komponen Keamanan Intenet AVG 2012 tertentu)*, Anda dapat menentukan dan menetapkan preferensi dengan memberi tanda/mengosongkan kotak centang pada opsi berikut:

- ***Tampilkan pemberitahuan baki sistem*** *(diaktifkan, secara default)* – Secara default, semua pemberitahuan ditampilkan. Jangan tandai item ini untuk menonaktifkan sama sekali tampilan semua pemberitahuan sistem. Bila diaktifkan, Anda dapat memilih lebih lanjut pemberitahuan spesifik yang akan ditampilkan:
  - ***Tampilkan pemberitahuan baki tentang pembaruan*** *(diaktifkan, secara default)* – Memutuskan apakah informasi mengenai peluncuran proses pembaruan **Keamanan Intenet AVG 2012**, kemajuannya, dan finalisasinya harus ditampilkan.
  - ***Tampilkan pemberitahuan perubahan status komponen*** *(dinonaktifkan, secara default)* – Memutuskan apakah informasi mengenai aktivitas/inaktivitas komponen, atau kemungkinan masalahnya harus ditampilkan. Saat melaporkan status kesalahan komponen, opsi ini sama dengan fungsi informatif ikon baki sistem yang melaporkan masalah dalam komponen **Keamanan Intenet AVG 2012**.
  - ***Tampilkan pemberitahuan baki menyangkut Resident Shield (tindakan otomatis)*** *(diaktifkan, secara default)* – Memutuskan apakah informasi mengenai penyimpanan, penyalinan, dan proses pembukaan file harus ditampilkan atau

disembunyikan (*konfigurasi ini hanya menunjukkan apakah opsi Pulihkan otomatis pada Resident Shield telah diaktifkan*).

- ***Tampilkan pemberitahuan baki tentang pemindaian*** *(diaktifkan, secara default)* – memutuskan apakah informasi mengenai peluncuran otomatis atas pemindaian terjadwal, kemajuannya, dan hasilnya harus ditampilkan.

- ***Tampilkan pemberitahuan baki menyangkut Firewall*** *(diaktifkan, secara default)* - Memutuskan apakah informasi mengenai status dan proses, misalnya peringatan aktivasi/deaktivasi komponen Firewall, kemungkinan pemblokiran lalu lintas, dsb. harus ditampilkan. Item ini menyediakan dua opsi pilihan yang lebih spesifik *(untuk penjelasan terperinci masing-masing, harap baca bab Firewall pada dokumen ini)*:

  - ***Tampilkan pemberitahuan tentang perubahan profil*** *(diaktifkan, secara default)* – Memberi tahu Anda tentang perubahan otomatis atas profil Firewall.

  - ***Tampilkan pemberitahuan tentang aturan aplikasi baru yang dibuat*** *(dinonaktifkan, secara default)* – Memberi tahu Anda tentang pembuatan otomatis aturan Firewall untuk aplikasi baru berdasarkan daftar aman.

- ***Tampilkan pemberitahuan baki menyangkut E-mail Scanner*** *(diaktifkan, secara default)* – Memutuskan apakah informasi mengenai pemindaian semua pesan e-mail yang masuk dan keluar akan ditampilkan.

- ***Tampilkan pemberitahuan statistik*** *(diaktifkan, secara default)* - Biarkan opsi ini ditandai untuk memperbolehkan pemberitahuan peninjauan statistik secara rutin ditampilkan di baki sistem.

- ***Tampilkan pemberitahuan baki tentang AVG Accelerator*** *(diaktifkan, secara default)* - Memutuskan apakah informasi tentang aktivitas ***AVG Accelerator*** harus ditampilkan. Layanan ***AVG Accelerator*** memungkinkan pemutaran video online lebih lancar dan membuat pengunduhan tambahan lebih mudah.

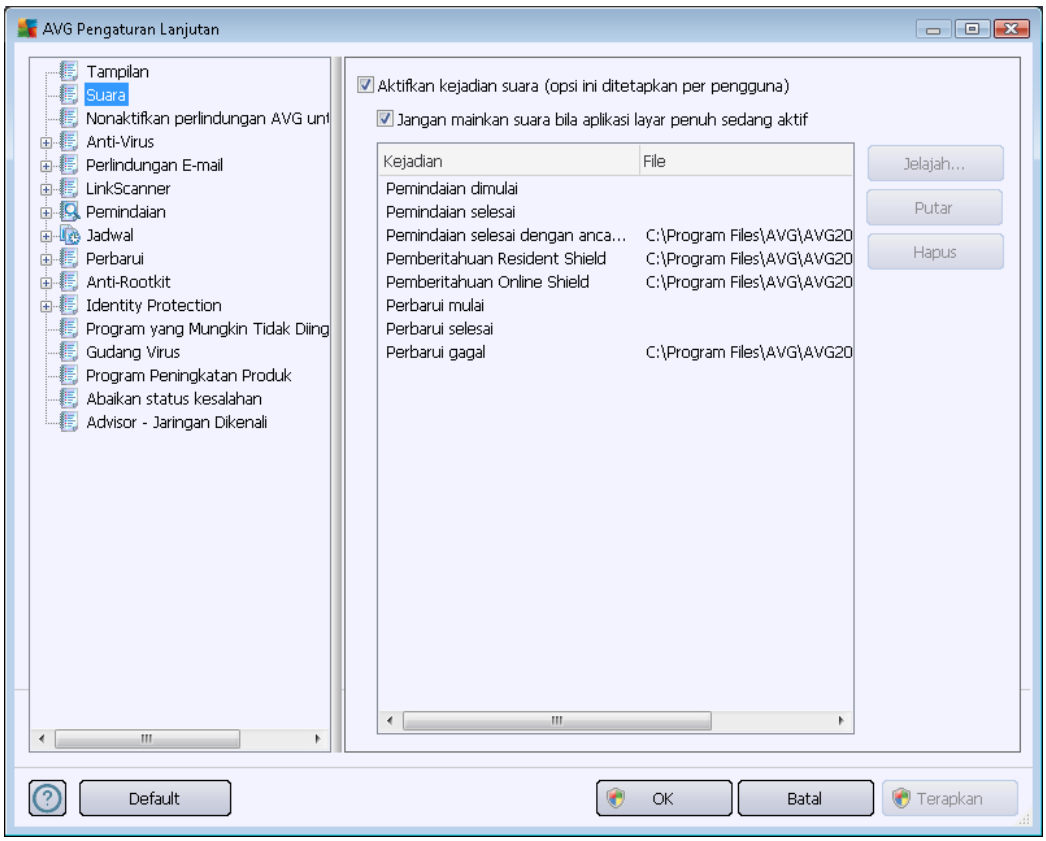
- ***Tampilkan pemberitahuan performa AVG Advice*** *(diaktifkan, secara default)* - ***AVG Advice*** memantau performa peramban Internet yang didukung *(Internet Explorer, Chrome, Firefox, Opera, dan Safari)*, dan akan memberi tahu Anda jika peramban terlalu banyak menggunakan memori dari jumlah yang disarankan. Dalam situasi demikian, performa komputer Anda mungkin melambat secara signifikan, dan dianjurkan untuk menjalankan ulang peramban Internet Anda untuk mempercepat prosesnya. Biarkan item ***Tampilkan pemberitahuan performa AVG Advice*** diaktifkan agar diberi tahu.

Mode permainan

Fungsi AVG ini dirancang untuk aplikasi layar-penuh bila balon informasi AVG (*misalnya saat dimulainya pemindaian yang telah dijadwalkan*) dirasa mengganggu (*hal ini dapat menyembunyikan aplikasi atau merusak grafiknya*). Untuk menghindari hal ini, biarkan kotaknya ditandai untuk ***Aktifkan mode permainan bila aplikasi layar penuh dijalankan*** (*pengaturan default*).

10.2. Suara

Dalam dialog ***Suara*** Anda dapat menetapkan apakah Anda ingin diberi tahu tentang tindakan tertentu **Keamanan Intenet AVG 2012** dengan pemberitahuan suara:



Pengaturan ini hanya berlaku untuk akun pengguna aktif. Maksudnya, setiap pengguna dapat mengatur sendiri suaranya. Jika Anda ingin memperbolehkan pemberitahuan suara, biarkan opsi ***Aktifkan kejadian suara*** tetap ditandai (*opsi diaktifkan secara default*) untuk mengaktifkan daftar semua tindakan yang relevan. Selanjutnya, Anda mungkin perlu menandai opsi ***Jangan mainkan suara bila aplikasi layar penuh sedang aktif*** untuk membungkam pemberitahuan suara bila merasa terganggu *(lihat juga bagian Mode permainan pada bab Pengaturan lanjutan/Tampilan dalam dokumen ini)*.

Tombol kontrol

- ***Cari di*** – Setelah memilih kejadian yang bersangkutan dari daftar, gunakan tombol ***Cari di*** untuk mencari file suara yang diinginkan di disk Anda, yang akan digunakan. *(Perhatikan bahwa hanya file suara *.wav yang didukung untuk saat ini!)*

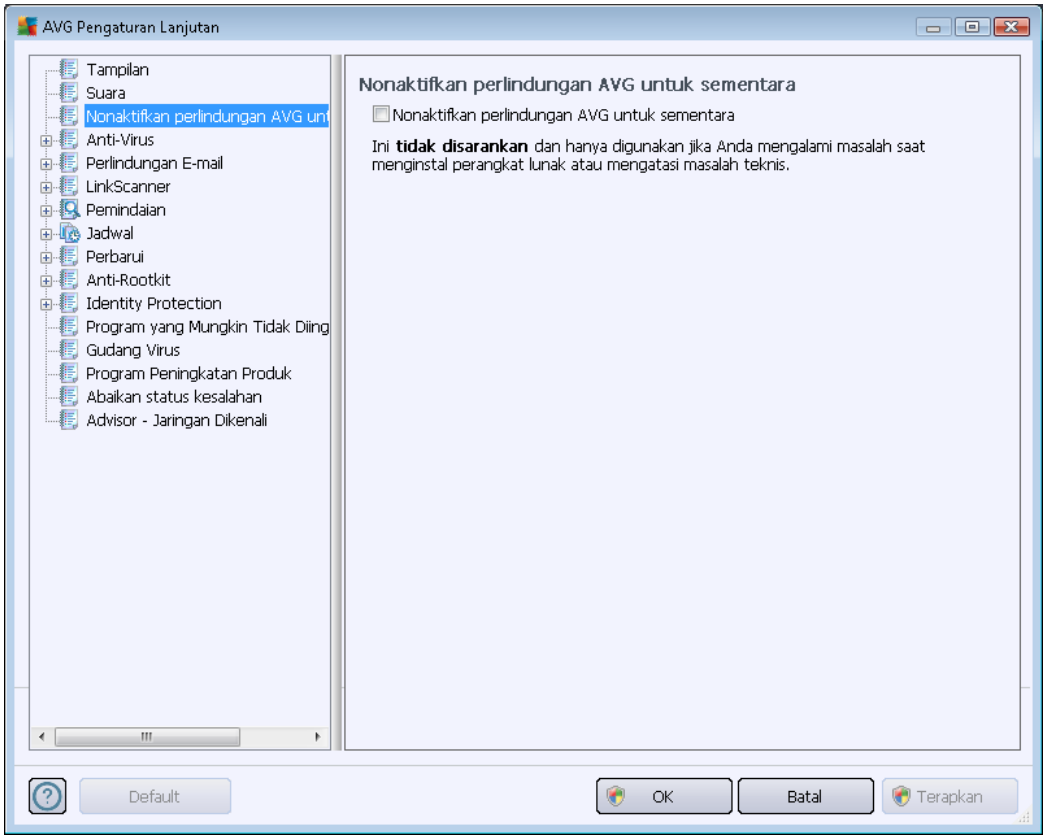
- ***Putar*** – Untuk mendengarkan suara yang dipilih, sorot kejadian dalam daftar dan tekan tombol ***Putar***.

- ***Hapus*** – Gunakan tombol ***Hapus*** untuk menghapus suara yang ditetapkan untuk kejadian tertentu.

10.3. Menonaktifkan perlindungan AVG untuk sementara

Dalam dialog ***Nonaktifkan perlindungan AVG untuk sementara*** Anda mempunyai opsi untuk menonaktifkan seluruh perlindungan yang diberikan oleh **Keamanan Intenet AVG 2012** sekaligus.

Ingatlah bahwa Anda tidak boleh menggunakan opsi ini kecuali jika sangat diperlukan!

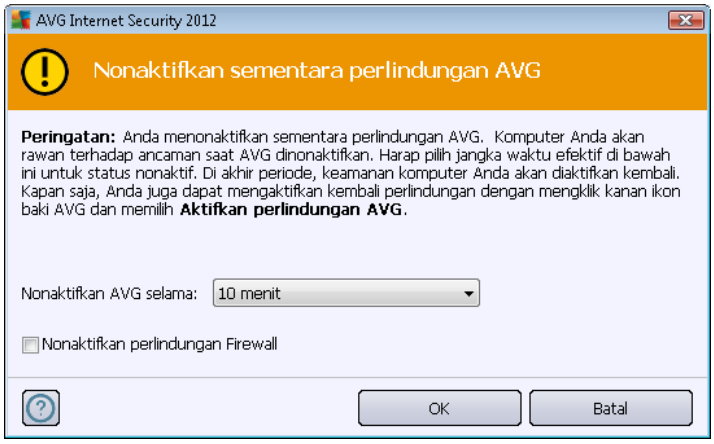


Umumnya, ***tidak perlu*** menonaktifkan **Keamanan Intenet AVG 2012** sebelum menginstal perangkat lunak atau driver baru, meskipun penginstal atau wizard perangkat lunak menyarankan agar program dan aplikasi yang berjalan ditutup terlebih dahulu untuk memastikan tidak ada gangguan yang tidak diinginkan selama proses instalasi. Jika Anda ternyata mengalami masalah selama instalasi, coba nonaktifkan perlindungan menetap (*Aktifkan Resident Shield*) terlebih dahulu. Jika Anda menonaktifkan **Keamanan Intenet AVG 2012** untuk sementara, Anda harus mengaktifkannya lagi begitu Anda selesai. Jika Anda terhubung dengan Internet atau jaringan selama perangkat lunak antivirus Anda dinonaktifkan, komputer Anda rentan terhadap serangan.

Cara menonaktifkan perlindungan AVG

- Tandai kotak centang ***Nonaktifkan perlindungan AVG untuk sementara***, dan konfirmasi pilihan Anda dengan menekan tombol ***Terapkan***

- Dalam dialog ***Nonaktifkan perlindungan AVG untuk sementara***yang baru dibuka, tetapkan berapa lama Anda ingin menonaktifkan **Keamanan Intenet AVG 2012**. Secara default, perlindungan akan dinonaktifkan selama 10 menit, yang seharusnya cukup untuk tugas umum seperti menginstal perangkat lunak baru, dsb. Perhatikan bahwa batas waktu awal yang dapat diatur adalah 15 menit dan tidak dapat diganti dengan nilai Anda sendiri demi alasan keamanan. Setelah jangka waktu yang ditetapkan, semua komponen yang tadi dinonaktifkan akan diaktifkan lagi secara otomatis.

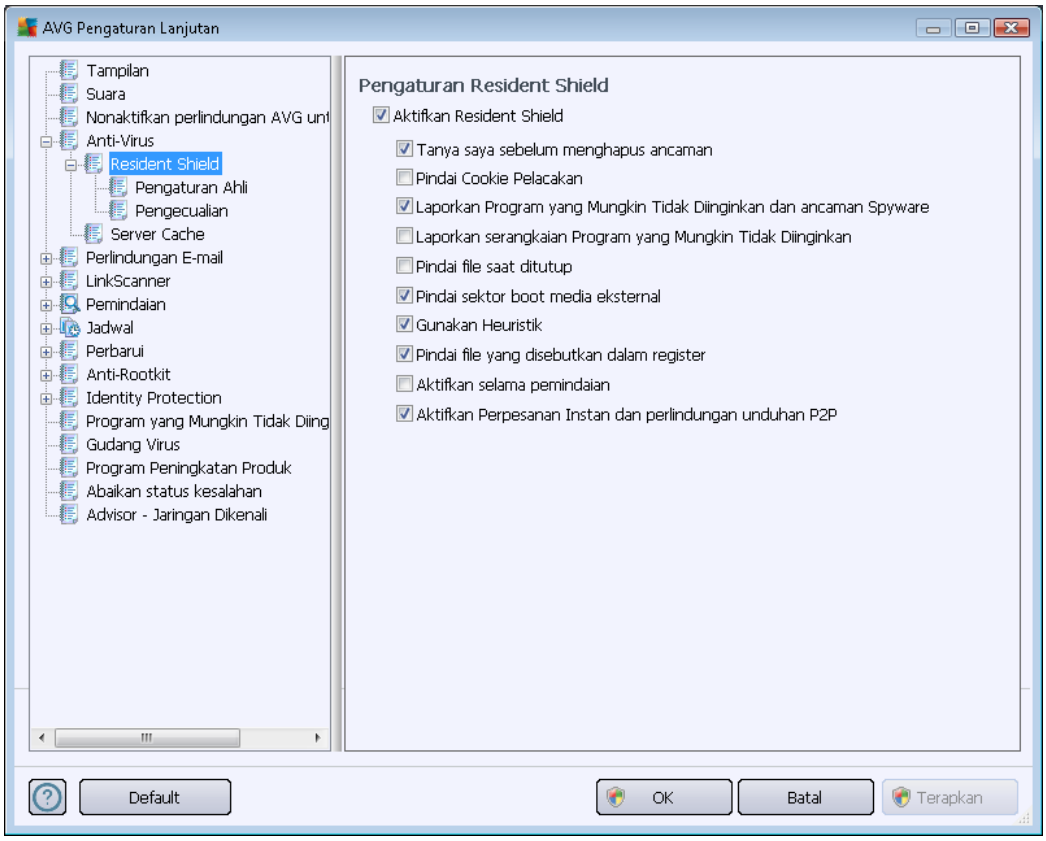


10.4. Anti-Virus

Komponen ***Anti-Virus*** melindungi komputer Anda secara kontinu dari semua tipe virus dan spyware yang dikenal *(termasuk malware nonaktif dan tidur, yakni malware yang terunduh namun belum diaktifkan)*.

10.4.1. Resident Shield

Resident Shield melakukan perlindungan langsung atas file dan folder dari virus, spyware dan malware lainnya.



Dalam dialog ***Pengaturan Resident Shield***, Anda dapat mengaktifkan atau menonaktifkan sepenuhnya perlindungan menetap dengan menandai atau tidak menandai item ***Aktifkan Resident Shield*** (*opsi ini telah diaktifkan secara default*). Selain itu, Anda dapat memilih fitur perlindungan menetap yang harus diaktifkan:

- ***Tanya saya sebelum menghapus ancaman*** (*diaktifkan secara default*) – Tandai untuk memastikan bahwa Resident Shield tidak akan melakukan tindakan apapun secara otomatis; melainkan akan menampilkan dialog yang menjelaskan ancaman yang terdeteksi, yang memungkinkan Anda memutuskan apa yang harus dilakukan. Jika Anda membiarkan kotak ini tidak ditandai, **Keamanan Intenet AVG 2012** otomatis akan memulihkan infeksi, dan jika tidak memungkinkan, objek tersebut akan dipindahkan ke Gudang Virus.

- ***Pindai Cookie Pelacak*** (*dinonaktifkan secara default*) – Parameter ini menentukan cookie yang harus dideteksi selama pemindaian. (*cookie HTTP digunakan untuk autentikasi, pelacakan, dan pengelolaan informasi tertentu tentang pengguna, seperti preferensi situs atau isi keranjang belanja elektronik mereka.*)

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – Tandai untuk mengaktifkan mesin Anti-Spyware, dan memindai

spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang memang sengaja diinstal. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*) – Tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai file saat ditutup*** (*dinonaktifkan secara default*) – Pemindaian saat ditutup memastikan bahwa AVG akan memindai berbagai objek aktif (misalnya aplikasi, dokumen, …) saat sedang dibuka, dan saat sedang ditutup; fitur ini membantu Anda melindungi komputer terhadap beberapa tipe virus canggih.

- ***Pindai sektor boot media eksternal*** (*diaktifkan secara default*)

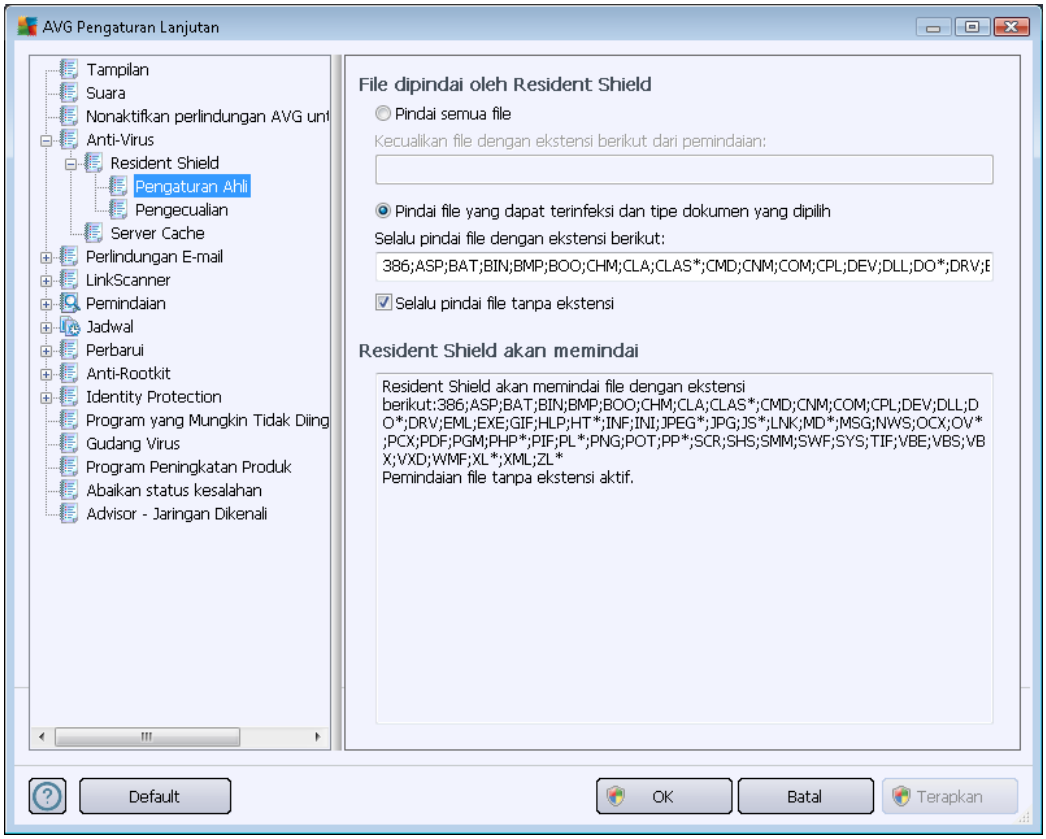
- ***Gunakan Heuristik*** (*diaktifkan secara default*) – Analisis heuristik akan digunakan untuk deteksi (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*).

- ***Pindai file yang disebutkan dalam register*** (*diaktifkan secara default*) – Parameter ini menentukan apakah AVG akan memindai semua file eksekusi yang ditambahkan ke register startup agar infeksi yang dikenal tidak dijalankan saat berikutnya komputer dihidupkan.

- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default*) - Dalam kondisi tertentu (*dalam keadaan sangat darurat*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma paling menyeluruh yang akan memeriksa semua objek yang mungkin mengancam, secara mendalam. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Aktifkan perlindungan Perpesanan Instan dan perlindungan unduhan P2P*** (*diaktifkan secara default*) - Tandai pilihan ini jika Anda ingin memastikan komunikasi perpesanan instan (*misalnya ICQ, MSN Messenger, …*) dan unduhan P2Pbebas virus.

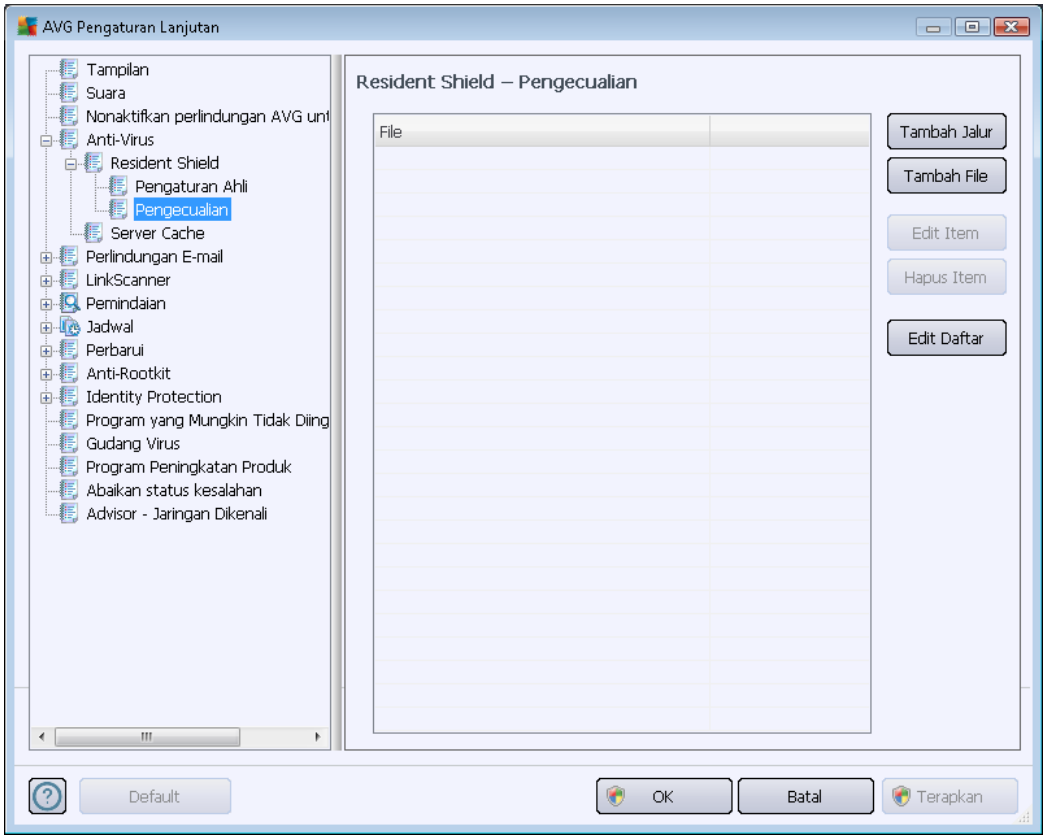
Dalam dialog ***File dipindai oleh Resident Shield*** Anda dapat mengkonfigurasi file yang akan dipindai (*menurut ekstensi tertentu*):



Tandai kotak yang bersangkutan untuk memutuskan apakah Anda ingin ***Pindai semua file*** atau ***Pindai file yang dapat terinfeksi dan tipe dokumen yang dipilih*** saja. Jika Anda memutuskan memilih opsi terakhir, maka Anda dapat menetapkan lebih jauh daftar ekstensi yang menentukan file apa saja yang dikecualikan dari pemindaian, dan daftar ekstensi file yang harus dipindai dalam keadaan apa pun.

Tandai ***Selalu pindai file tanpa ekstensi*** (*secara default*) untuk memastikan bahwa bahkan file tanpa ekstensi dan format yang tidak dikenal akan dipindai oleh Resident Shield. Kami sarankan untuk tetap mengaktifkan fitur ini, karena file tanpa ekstensi mencurigakan.

Bagian di bawah ini yang disebut ***Resident Shield akan memindai*** lalu meringkas pengaturan yang aktif, menampilkan tinjauan umum terperinci tentang apa yang akan dipindai oleh ***Resident Shield***.



Dialog ***Resident Shield – Pengecualian*** menyediakan kesempatan untuk menentukan file dan/atau folder yang harus dikecualikan dari pemindaian ***Resident Shield***.

Jika hal ini tidak penting, kami sangat menyarankan untuk tidak mengecualikan item apa pun!

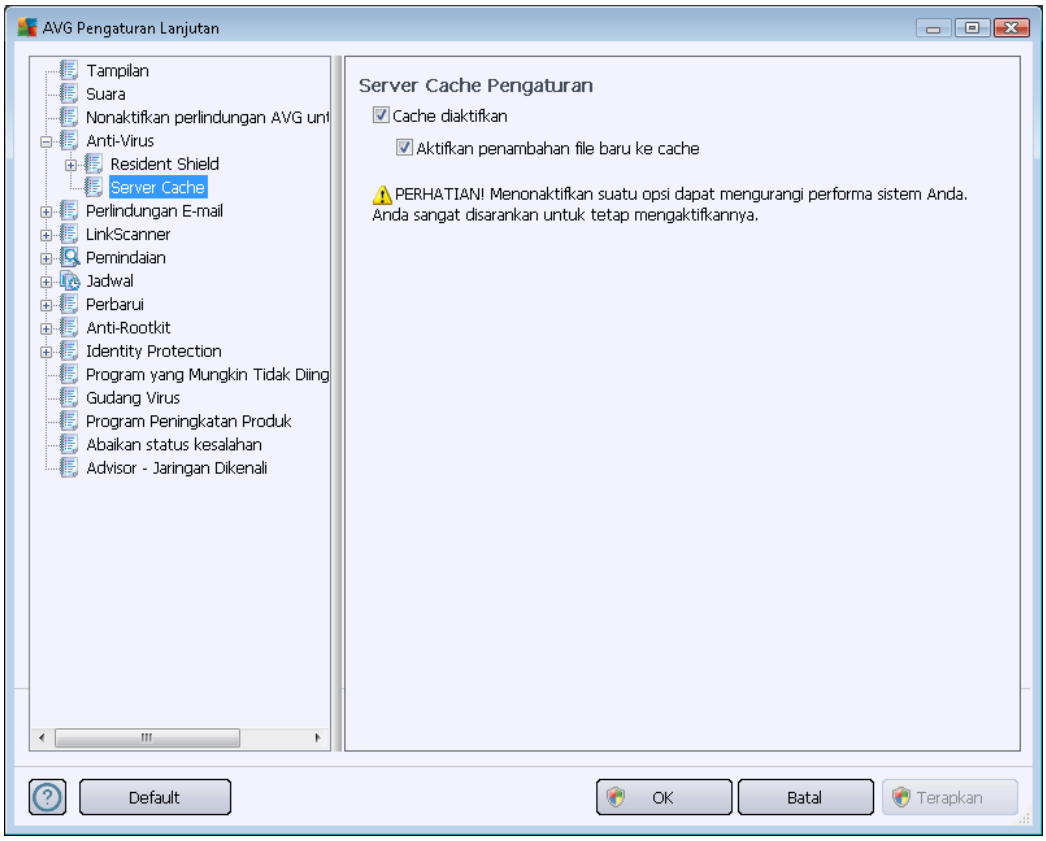
Tombol kontrol

Dialog ini menyediakan tombol kontrol berikut:

- ***Tambah Jalur*** – menetapkan direktori yang akan dikecualikan dari pemindaian dengan memilihnya satu per satu dari struktur navigasi disk lokal
- ***Tambah File*** – menetapkan file yang akan dikecualikan dari pemindaian dengan memilihnya satu per satu dari struktur navigasi disk lokal
- ***Edit Jalur*** – memungkinkan Anda mengedit jalur yang ditetapkan ke file yang dipilih
- ***Hapus Jalur*** – memungkinkan Anda menghapus jalur ke folder terpilih, dari daftar
- ***Edit Daftar*** – memungkinkan Anda mengedit seisi daftar pengecualian yang telah ditetapkan dalam dialog baru yang berfungsi seperti editor teks standar

10.4.2. Server Cache

Dialog ***Pengaturan Server Cache*** merujuk pada proses server cache yang dirancang untuk mempercepat semua tipe pemindaian **Keamanan Intenet AVG 2012**:



Server cache ini mengumpulkan dan menyimpan informasi file terpercaya (*file dianggap terpercaya jika ditandai dengan tanda tangan digital dari sumber terpercaya*). File ini kemudian secara otomatis dianggap aman, dan tidak perlu dipindai kembali; karena itu file ini akan dilompati selama pemindaian.

Dialog ***Pengaturan Server Cache*** menawarkan opsi konfigurasi berikut:

- ***Cache diaktifkan*** (*diaktifkan secara default*) – kosongkan kotaknya untuk menonaktifkan ***Server Cache*** dan mengosongkan memori cache. Perhatikan, pemindaian mungkin melambat, dan performa komputer Anda secara keseluruhan akan menurun, karena setiap file yang sedang digunakan akan dipindai untuk mencari virus dan spyware terlebih dahulu.
- ***Aktifkan penambahan file baru ke cache*** (*diaktifkan secara default*) – hapus centang pada kotak untuk menghentikan penambahan file lainnya ke memori cache. File yang sudah ditambahkan ke cache akan disimpan dan digunakan hingga aktivitas cache dinonaktifkan sama sekali, atau hingga pembaruan basis data virus berikutnya.

Kecuali jika Anda mempunyai alasan kuat untuk menonaktifkan server cache, kami sangat menyarankan agar Anda membiarkan pengaturan default dan tetap mengaktifkan kedua opsi! Jika tidak, Anda mungkin mengalami penurunan yang signifikan pada kecepatan sistem dan

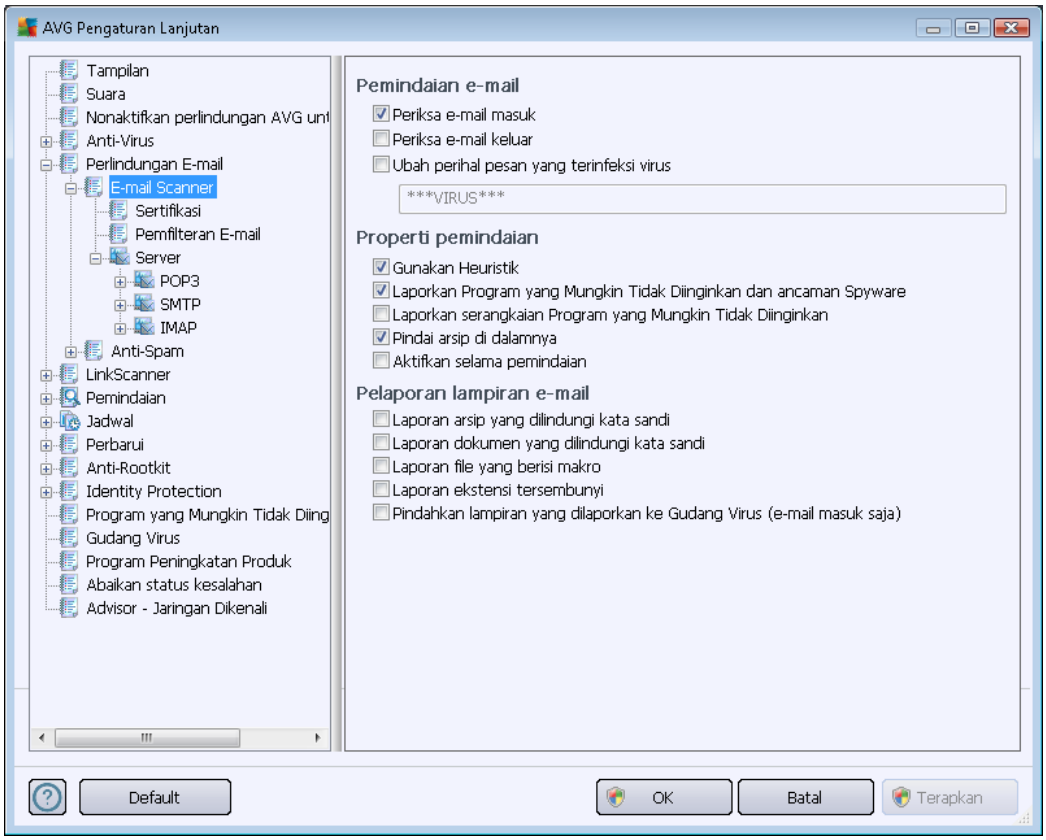
performa.

10.5. Perlindungan e-mail

Di bagian ***Perlindungan e-mail*** Anda dapat mengedit konfigurasi terperinci dari E-mail Scanner dan Anti-Spam:

10.5.1. E-mail Scanner

Dialog ***E-mail Scanner*** terbagi ke dalam tiga bagian:



Pemindaian e-mail

Di bagian ini, Anda dapat menetapkan pengaturan dasar ini untuk pesan email masuk dan/atau keluar:

- ***Periksa email masuk*** (*diaktifkan secara default*) – tandai untuk mengaktifkan/ menonaktifkan opsi pemindaian semua pesan email yang dikirimkan ke klien email Anda
- ***Periksa email keluar*** (*dinonaktifkan secara default*) – tandai untuk mengaktifkan/ menonaktifkan opsi pemindaian semua pesan email yang dikirim dari akun Anda
- ***Modifikasi perihal pesan yang terinfeksi virus*** (*dinonaktifkan secara default*) – jika Anda ingin diperingatkan jika ada pesan email yang dipindai terdeteksi sebagai terinfeksi, tandai pilihan ini dan isi teks yang diinginkan ke dalam bidang teks. Nilai ini kemudian

ditambahkan ke bidang "Perihal" setiap pesan email terinfeksi untuk memudahkan identifikasi dan pemfilteran. Nilai defaultnya adalah ***VIRUS*** yang kami sarankan untuk tetap digunakan.

Properti pemindaian

Di bagian ini, Anda dapat menentukan bagaimana pesan email akan dipindai:

- ***Gunakan Heuristik*** (*diaktifkan secara default*) – tandai untuk menggunakan metode deteksi heuristik saat memindai pesan e-mail. Bila opsi ini aktif, Anda dapat memfilter lampiran e-mail tidak hanya berdasarkan ekstensinya tetapi juga isi sebenarnya dari lampiran tersebut akan dipertimbangkan. Pemfilteran dapat diatur dalam dialog Pemfilteran E-mail.

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – tandai untuk mengaktifkan mesin Anti-Spyware, dan memindai spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang memang sengaja diinstal. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*) – tandai kotak ini untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai di dalam arsip*** (*diaktifkan secara default*) – tandai untuk memindai isi arsip yang terlampir ke pesan email.

- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default*) – dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi virus atau exploit*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai bahkan area yang paling sulit terinfeksi di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

Pelaporan lampiran e-mail

Di bagian ini, Anda dapat mengatur laporan tambahan tentang file yang mungkin membahayakan atau mencurigakan. Perhatikan bahwa tidak ada dialog peringatan yang ditampilkan, hanya teks sertifikasi yang akan ditambahkan di akhir pesan e-mail, dan semua laporan tersebut akan terdaftar dalam dialog Deteksi E-mail Scanner:

- ***Laporkan arsip yang dilindungi kata sandi*** – arsip (*ZIP, RAR, dll.*) yang dilindungi kata sandi tidak mungkin dipindai dari virus; tandai kotak ini untuk melaporkannya sebagai mungkin berbahaya.

- ***Laporkan dokumen yang dilindungi kata sandi*** – dokumen yang dilindungi kata sandi tidak mungkin dipindai dari virus; tandai kotak ini untuk melaporkannya sebagai mungkin

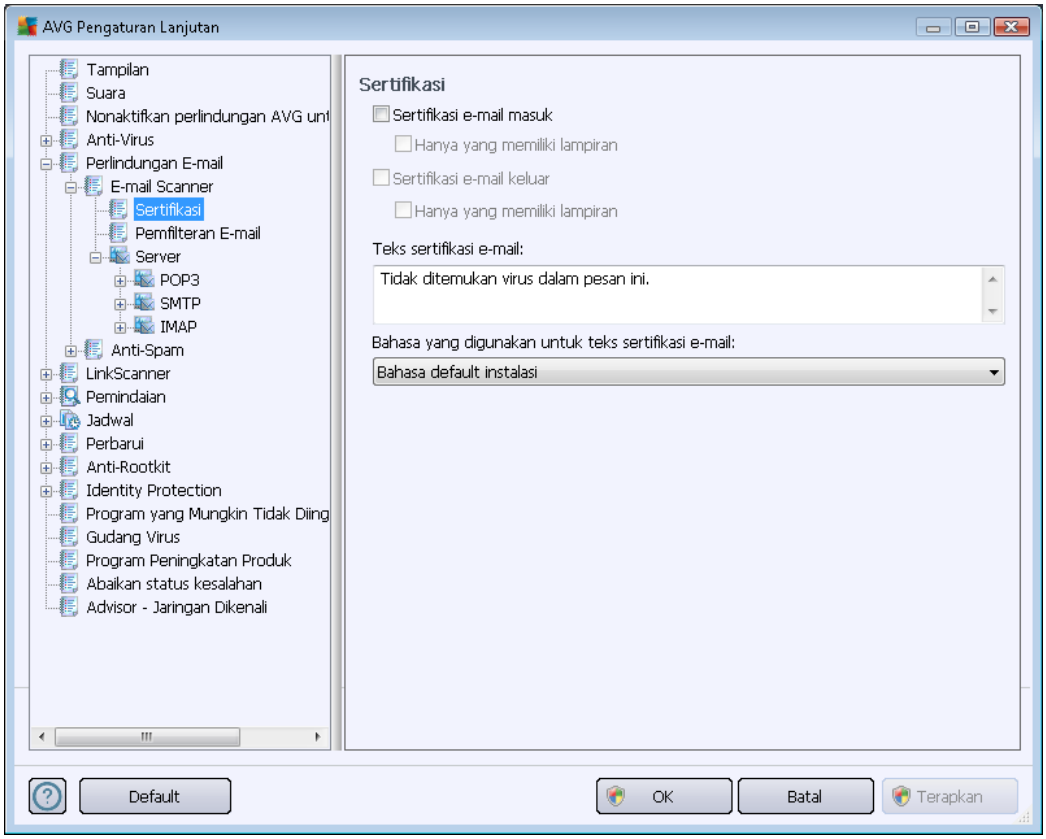
berbahaya.

- ***Laporkan file yang berisi makro*** – makro adalah urutan langkah yang telah ditetapkan untuk mempermudah tugas pengguna (*makro MS Word sudah dikenal luas*). Oleh karena itu, makro dapat berisi petunjuk yang mungkin berbahaya, dan Anda mungkin ingin menandai kotak ini untuk memastikan file dengan makro akan dilaporkan sebagai mencurigakan.

- ***Laporkan ekstensi tersembunyi*** – ekstensi tersembunyi dapat membuat, mis. file dapat dijalankan yang mencurigakan "sesuatu.txt.exe", tampak sebagai file teks biasa yang tidak berbahaya "sesuatu.txt"; tandai kotak ini untuk melaporkannya sebagai berpotensi membahayakan.

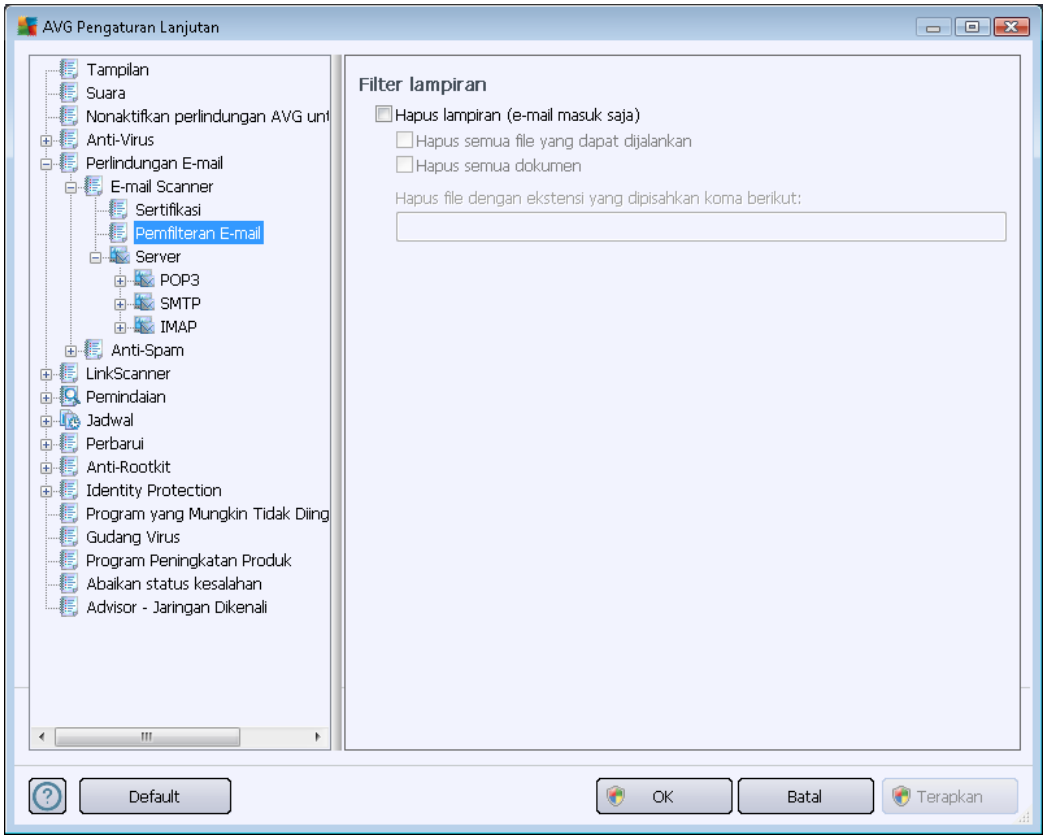
- ***Pindahkan lampiran yang dilaporkan ke Gudang Virus*** – menentukan apakah Anda ingin diberi tahu melalui e-mail tentang arsip yang dilindungi kata sandi, dokumen yang dilindungi kata sandi, file berisi makro dan/atau file dengan ekstensi tersembunyi yang terdeteksi sebagai lampiran pada pesan e-mail yang dipindai. Jika pesan-pesan demikian teridentifikasi selama pemindaian, tetapkan apakah objek terinfeksi yang terdeteksi harus dipindah ke Gudang Virus.

Dalam dialog ***Sertifikasi*** Anda dapat menandai kotak tertentu untuk memutuskan apakah Anda ingin mengotorisasi email masuk (***Sertifikasi e-mail masuk***) dan/atau email keluar (***Sertifikasi e-mail keluar***). Untuk setiap opsi ini Anda dapat menetapkan lebih jauh parameter ***Hanya dengan lampiran*** sehingga sertifikasi hanya ditambahkan pada pesan e-mail yang berisi lampiran:



Secara default, teks sertifikasi terdiri dari informasi dasar yang berbunyi *Tidak ditemukan virus dalam pesan ini.* Walau demikian, informasi ini dapat ditambah atau diubah menurut kebutuhan Anda: tuliskan teks sertifikasi yang diinginkan ke dalam bidang ***Teks sertifikasi e-mail***. Di bagian ***Bahasa yang digunakan untuk teks sertifikasi e-mail*** Anda dapat menentukan lebih jauh dalam bahasa apa bagian sertifikasi yang dibuat secara otomatis tersebut (*Tidak ditemukan virus dalam pesan ini*) harus ditampilkan.

Catatan: *Harap diingat bahwa teks default hanya akan ditampilkan dalam bahasa yang diminta, dan teks yang telah Anda sesuaikan tidak akan diterjemahkan secara otomatis!*



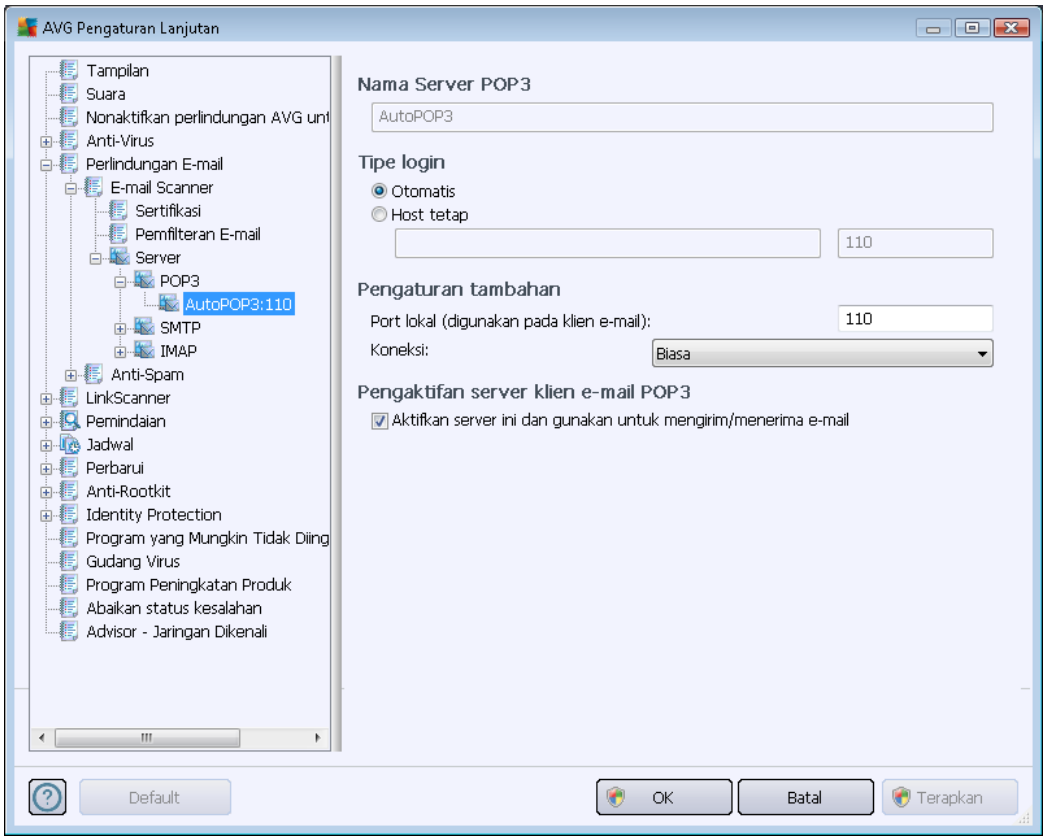
Dialog ***Filter lampiran*** memungkinkan Anda mengatur parameter untuk pemindaian lampiran pesan email. Secara default, opsi ***Hapus lampiran*** dinonaktifkan. Jika Anda memutuskan untuk mengaktifkannya, semua pesan e-mail yang terdeteksi sebagai infeksi atau mungkin berbahaya akan dihapus secara otomatis. Jika Anda ingin menetapkan tipe lampiran tertentu yang harus dihapus, pilih opsi yang terkait:

- ***Hapus semua file yang dapat dijalankan*** – semua file *.exe akan dihapus
- ***Hapus semua dokumen*** – semua file *.doc, *.docx, *.xls, *.xlsx akan dihapus
- ***Hapus file dengan ekstensi yang dipisahkan koma ini*** – akan menghapus semua file dengan ekstensi yang ditetapkan

Di bagian ***Server***, Anda dapat mengedit parameter server E-mail Scanner:

- Server POP3
- Server SMTP
- Server IMAP

Selain itu, Anda dapat menetapkan server baru bagi email masuk atau keluar, dengan tombol ***Tambah server baru***.

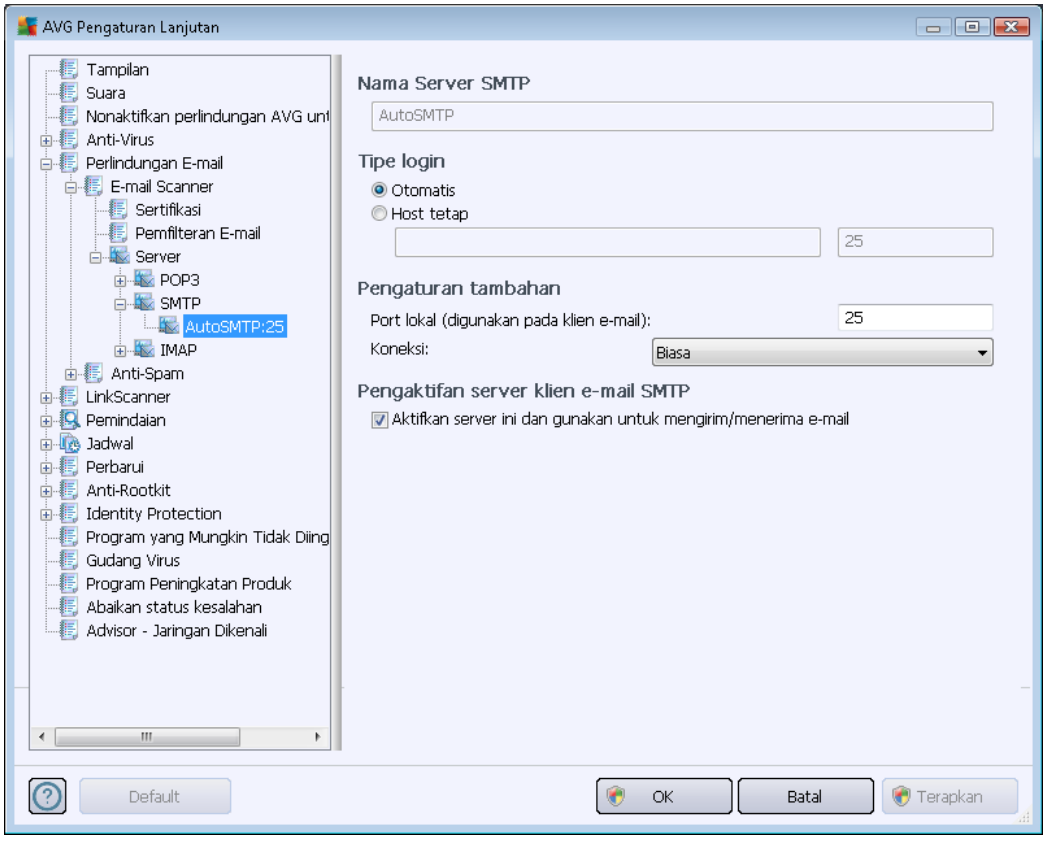


Dalam dialog ini (*dibuka melalui **Server / POP3***) Anda dapat mengatur server baru E-mail Scanner dengan menggunakan protokol POP3 untuk email masuk:

- ***Nama Server POP3*** – di bidang ini Anda dapat menentukan nama server yang baru ditambahkan (*untuk menambahkan server POP3, klik tombol kanan mouse di atas pilihan POP3 pada menu navigasi kiri*). Untuk membuat server "AutoPOP3" secara otomatis, bidang ini dinonaktifkan.
- ***Tipe login*** – menetapkan metode untuk menentukan server e-mail yang digunakan bagi e-mail masuk:
  - ***Otomatis*** - Login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda.
  - ***Host tetap*** – Dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server e-mail Anda. Nama login tetap tidak berubah. Untuk nama, Anda dapat menggunakan nama domain (*misalnya, pop.acme.com*) serta alamat IP (*misalnya, 123.45.67.89*). Jika server Email menggunakan port non-standar, Anda dapat menentukan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (*misalnya, pop.acme.com:8200*).

Port standar untuk komunikasi POP3 adalah 110.

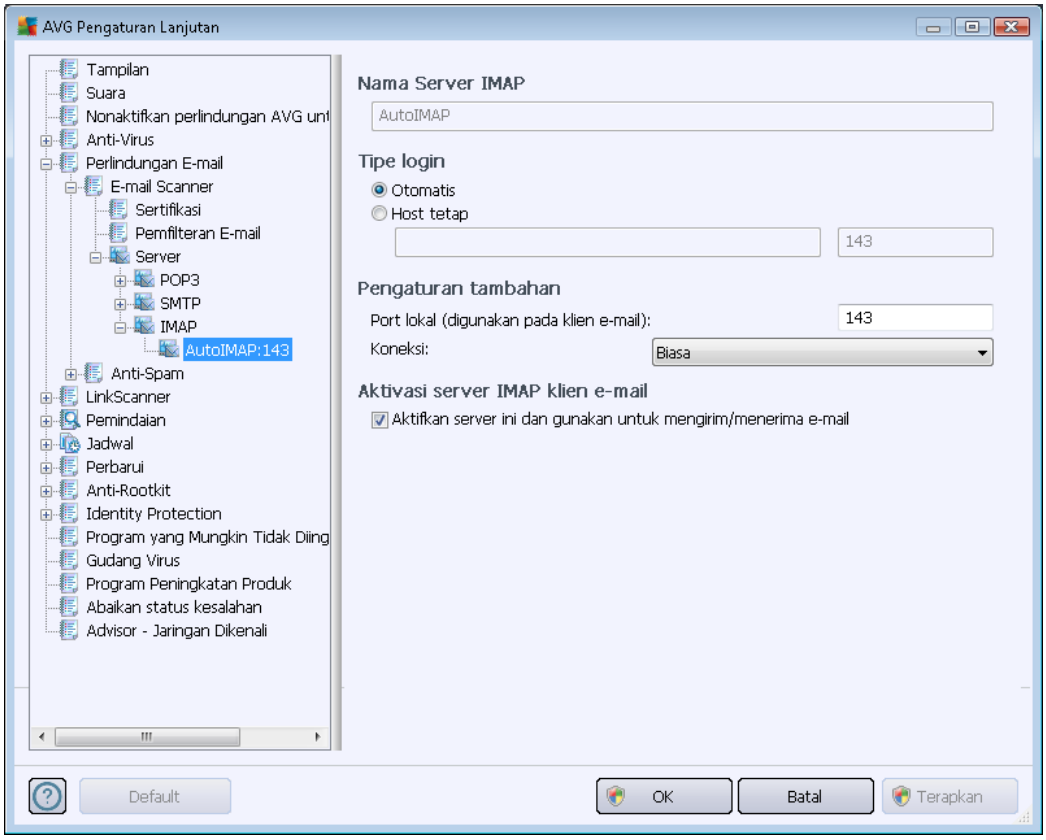
- ***Pengaturan tambahan*** – menentukan parameter yang lebih terperinci:
  - ***Port lokal*** – menentukan port yang akan dicari oleh aplikasi e-mail Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi POP3 dalam aplikasi e-mail Anda.
  - ***Koneksi*** – dalam menu buka-bawah ini, Anda dapat menentukan jenis koneksi yang akan digunakan (*biasa/SSL/SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini juga hanya tersedia bila server e-mail tujuan mendukungnya.
- ***Aktivasi server POP3 klien e-mail*** - tandai/jangan tandai item ini untuk mengaktifkan atau menonaktifkan server POP3 yang ditentukan



Dalam dialog ini (*dibuka melalui **Server / SMTP***) Anda dapat mengatur server baru E-mail Scanner dengan menggunakan protokol SMTP untuk email keluar:

- ***Nama Server SMTP*** – pada bidang ini, Anda dapat menentukan nama server yang baru ditambahkan (*untuk menambahkan server SMTP, klik tombol kanan mouse di atas pilihan SMTP pada menu navigasi kiri*). Untuk membuat server "AutoSMTP" secara otomatis, bidang ini dinonaktifkan.

- ***Tipe login*** – menetapkan metode untuk menentukan server email yang digunakan bagi email keluar:
    - ***Otomatis*** – login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda
    - ***Host tetap*** – Dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server e-mail Anda. Anda dapat menggunakan nama domain (*misalnya, smtp.acme.com*) ataupun alamat IP (*misalnya, 123.45.67.89*) untuk nama server. Jika server Email menggunakan port non-standar, Anda dapat menetapkan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (*misalnya, smtp.acme.com:8200*). Port standar untuk komunikasi SMTP adalah 25.
- ***Pengaturan tambahan*** – menentukan parameter yang lebih terperinci:
    - ***Port lokal*** – menentukan port yang akan dicari oleh aplikasi e-mail Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi SMTP dalam aplikasi e-mail Anda.
    - ***Koneksi*** – dalam menu buka-bawah ini, Anda dapat menentukan jenis koneksi yang akan digunakan (*biasa/SSL/SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini hanya tersedia bila server e-mail tujuan mendukungnya.
- ***Aktivasi server SMTP klien e-mail*** – tandai/kosongkan kotak ini untuk mengaktifkan/ menonaktifkan server SMTP yang ditentukan di atas



Dalam dialog ini (dibuka melalui ***Server / IMAP***) Anda dapat mengatur server baru E-mail Scanner dengan menggunakan protokol IMAP untuk Email keluar:

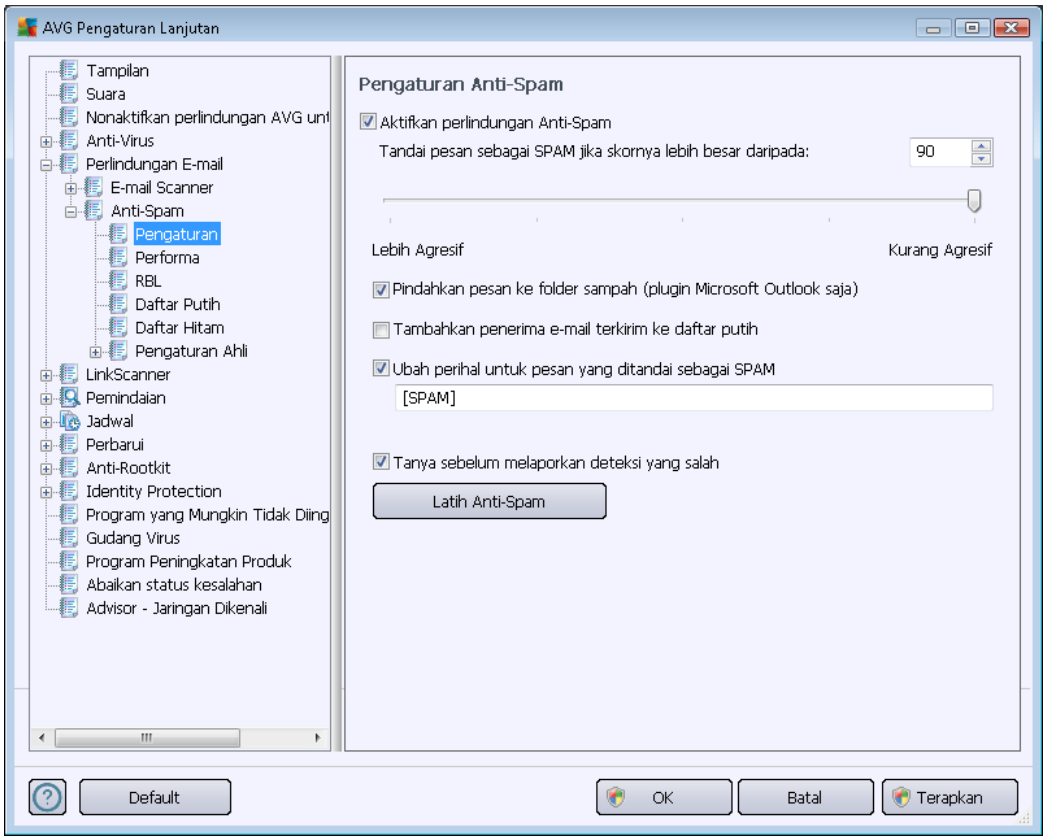
- ***Nama Server IMAP*** – di bidang ini Anda dapat menentukan nama server yang baru ditambahkan (*untuk menambah server IMAP, klik tombol kanan mouse di atas item IMAP pada menu navigasi kiri*). Untuk membuat server "AutoIMAP" secara otomatis, bidang ini dinonaktifkan
- ***Tipe login*** – menetapkan metode untuk menentukan server email yang digunakan bagi email keluar:
  - ***Otomatis*** – login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda
  - ***Host tetap*** – Dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server e-mail Anda. Anda dapat menggunakan nama domain (*misalnya, smtp.acme.com*) ataupun alamat IP (*misalnya, 123.45.67.89*) untuk nama server. Jika server Email menggunakan port non-standar, Anda dapat menetapkan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (*misalnya, imap.acme.com:8200*). Port standar untuk komunikasi IMAP adalah 143.
- ***Pengaturan tambahan*** – menentukan parameter yang lebih terperinci:

- ***Port lokal*** – menentukan port yang akan dicari oleh aplikasi e-mail Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi IMAP dalam aplikasi email Anda.

- ***Koneksi*** – dalam menu buka-bawah ini, Anda dapat menentukan jenis koneksi yang akan digunakan (*biasa/SSL/SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini hanya tersedia bila server e-mail tujuan mendukungnya.

- ***Aktivasi server IMAP klien Email*** – tandai/kosongkan kotak ini untuk mengaktifkan/menonaktifkan server IMAP yang ditetapkan di atas

10.5.2. Anti-Spam



Dalam dialog ***Pengaturan Anti-Spam*** Anda dapat menandai/tidak menandai kotak ***Aktifkan perlindungan Anti-Spam*** untuk memperbolehkan/melarang anti-spam memindai komunikasi e-mail. Opsi ini diaktifkan secara default, dan seperti biasanya, disarankan untuk membiarkan konfigurasi ini kecuali Anda memiliki alasan kuat untuk mengubahnya.

Berikutnya, Anda juga dapat memilih ukuran penilaian yang lebih atau kurang agresif. Filter ***Anti-Spam*** memberikan skor pada setiap pesan (*yakni seberapa mirip isi pesan tersebut dengan SPAM*) berdasarkan sejumlah teknik pemindaian dinamis. Anda dapat menyesuaikan pengaturan ***Tandai pesan sebagai spam jika skornya lebih besar dari*** dengan mengetikkan nilai atau dengan

menggerakkan bilah geser ke kiri atau ke kanan (*kisaran nilai dibatasi pada 50-90*).

Secara umum kami sarankan untuk mengatur ambang batas antara 50-90, atau jika Anda benar-benar tidak yakin, ke 90. Inilah tinjauan umum mengenai ambang batas skor:

- ***Nilai 80-90*** – Pesan e-mail yang hampir bisa dipastikan sebagai spam akan difilter. Beberapa pesan bukan-spam mungkin turut salah difilter.
- ***Nilai 60-79*** – Dianggap sebagai konfigurasi yang sangat agresif. Pesan e-mail yang kemungkinan adalah spam akan difilter. Pesan bukan-spam hampir bisa dipastikan turut tertangkap.
- ***Nilai 50-59*** – Konfigurasi sangat agresif. Pesan e-mail bukan-spam hampir bisa dipastikan akan tertangkap sebagai pesan spam nyata. Kisaran ambang batas ini tidak disarankan untuk penggunaan biasa.

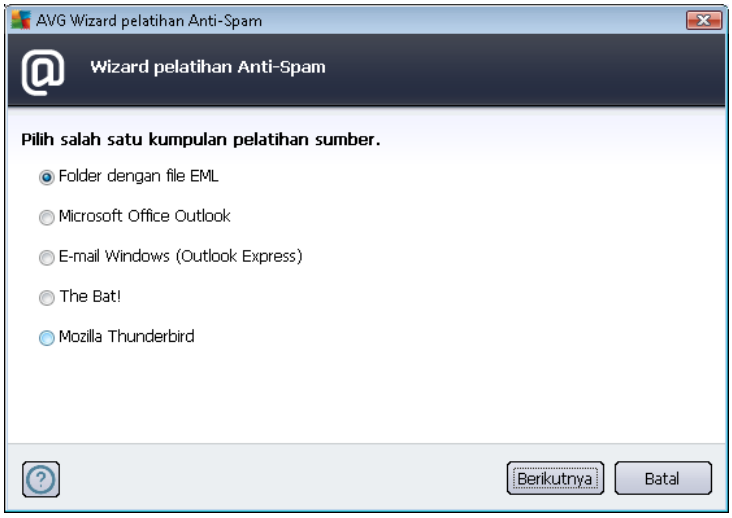
Dalam dialog ***Pengaturan Anti-Spam*** Anda dapat menentukan lebih jauh bagaimana seharusnya memperlakukan pesan e-mail spam yang terdeteksi:

- ***Pindahkan pesan ke folder sampah*** *(plugin Microsoft Outlook saja)* - Centang kotak ini untuk menetapkan bahwa setiap pesan spam yang terdeteksi secara otomatis harus dipindahkan ke folder sampah tertentu dalam klien email Anda. Saat ini, fitur ini tidak didukung di klien email lainnya.
- ***Tambahkan penerima email terkirim ke daftar-putih*** - Centang kotak ini untuk mengonfirmasi bahwa semua penerima email terkirim dapat dipercaya, dan semua perpesanan email yang berasal dari akun email mereka dapat disampaikan.
- ***Ubah perihal pesan yang ditandai sebagai SPAM*** - Centang kotak ini jika Anda ingin semua pesan yang terdeteksi sebagai spam ditandai dengan kata atau karakter tertentu dalam bidang perihal email; teks yang diinginkan dapat diketik di bidang teks yang telah diaktifkan.
- ***Tanya sebelum melaporkan deteksi yang salah*** – Asalkan selama proses instalasi Anda setuju untuk berpartisipasi dalam Program Peningkatan Produk. Jika demikian, Anda mengizinkan pelaporan ancaman yang terdeteksi ke AVG. Pelaporan ini dilakukan secara otomatis. Namun demikian, Anda dapat menandai kotak ini untuk mengonfirmasi bahwa Anda ingin ditanyai sebelum spam yang terdeteksi dilaporkan kepada AVG guna memastikan bahwa pesan tersebut betul-betul spam.

Tombol kontrol

Tombol Latih Anti-Spam akan membuka Wizard Pelatihan Anti-Spam yang diterangkan secara terperinci dalam bab berikutnya.

Dialog pertama ***Wizard Pelatihan Anti-Spam*** meminta Anda untuk memilih sumber pesan e-mail yang akan digunakan untuk pelatihan. Biasanya, Anda nanti perlu menggunakan e-mail yang salah ditandai sebagai SPAM, maupun pesan spam yang belum dikenali.



Ada beberapa opsi yang dapat dipilih berikut ini:

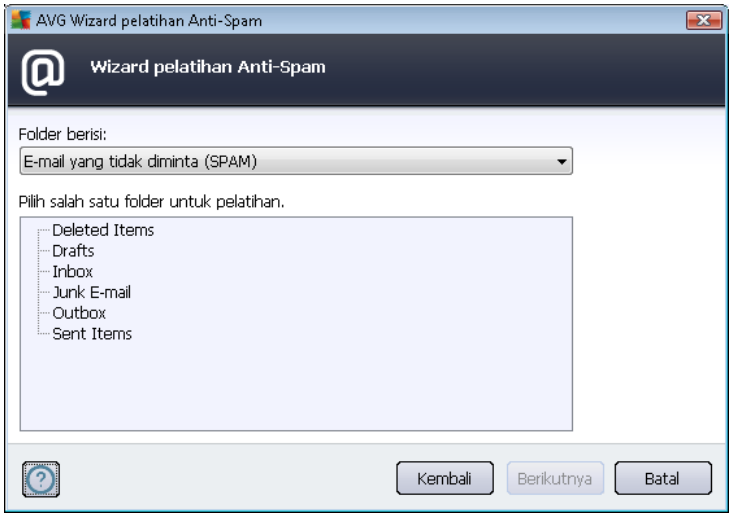
- ***Klien e-mail tertentu*** – jika Anda menggunakan salah satu klien e-mail yang tercantum (*MS Outlook, Outlook Express, The Bat!*), tinggal pilih opsi yang terkait
- ***Folder dengan file EML*** – jika Anda menggunakan program e-mail lain, Anda harus menyimpan pesan ke folder tertentu (*dalam format .eml*), atau memastikan Anda mengetahui lokasi folder pesan klien e-mail Anda. Kemudian pilih ***Folder dengan file EML*** , yang memungkinkan Anda untuk menemukan folder yang diinginkan pada langkah berikutnya

Untuk proses pelatihan yang lebih cepat dan mudah, adalah ide yang bagus untuk mengurutkan e-mail dalam folder terlebih dahulu, sehingga folder yang akan digunakan untuk pelatihan hanya berisi pesan pelatihan (baik diinginkan, maupun tidak diinginkan). Namun, itu tidak perlu dilakukan, karena Anda akan dapat memfilter e-mail nanti.

Pilih opsi yang sesuai dan klik ***Berikutnya*** untuk melanjutkan wizard.

Dialog yang ditampilkan dalam langkah ini tergantung pada pilihan Anda sebelumnya.

Folder dengan file EML



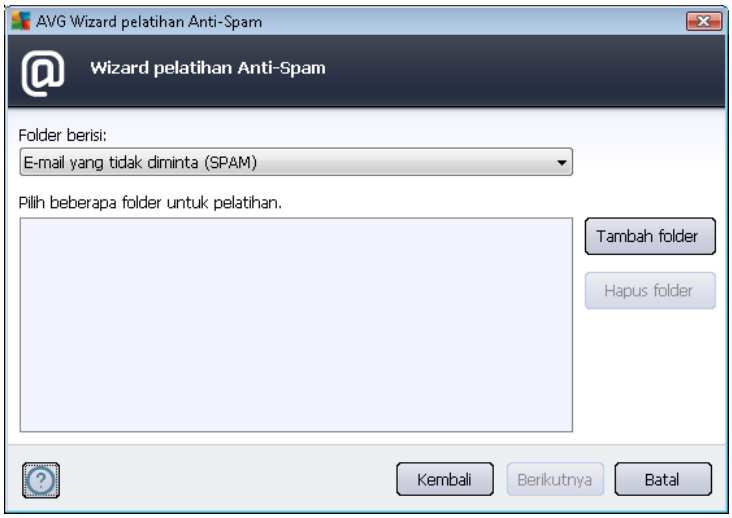
Dalam dialog ini, pilih folder dengan pesan yang ingin Anda gunakan untuk pelatihan. Tekan tombol ***Tambah folder*** untuk menemukan folder dengan file .eml (*pesan e-mail tersimpan*). Folder yang dipilih akan ditampilkan dalam dialog.

Dalam menu buka-bawah ***Folder berisi***, atur salah satu dari dua opsi – apakah folder yang dipilih berisi pesan yang diinginkan (*HAM*), atau tidak diinginkan (*SPAM*). Perhatikan bahwa Anda dapat memfilter pesan di langkah berikutnya, jadi folder tidak harus hanya berisi e-mail pelatihan. Anda juga dapat menghapus folder terpilih yang tidak diinginkan dengan mengklik tombol ***Hapus folder***.

Bila selesai, klik ***Berikutnya*** dan lanjutkan ke Opsi pemfilteran pesan.

Klien e-mail tertentu

Setelah Anda mengkonfirmasi salah satu opsi, dialog baru akan muncul.

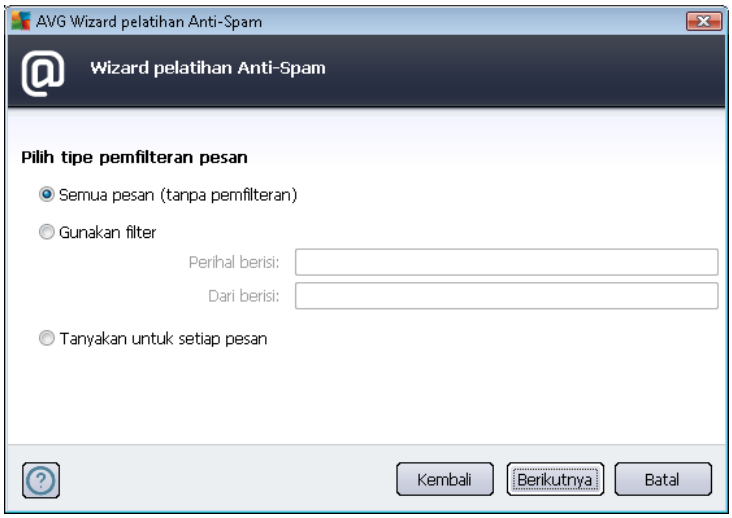


Catatan: *Untuk Microsoft Office Outlook, Anda akan dikonfirmasi untuk memilih profil MS Office*

Outlook terlebih dahulu.

Dalam menu buka-bawah ***Folder berisi***, atur salah satu dari dua opsi – apakah folder yang dipilih berisi pesan yang diinginkan (*HAM*), atau tidak diinginkan (*SPAM*). Perhatikan bahwa Anda dapat memfilter pesan di langkah berikutnya, jadi folder tidak harus hanya berisi e-mail pelatihan. Struktur navigasi klien e-mail yang dipilih sudah ditampilkan di bagian utama dialog. Temukan folder yang diinginkan dalam struktur tersebut lalu sorot dengan mouse.

Bila selesai, klik ***Berikutnya*** dan lanjutkan ke Opsi pemfilteran pesan.

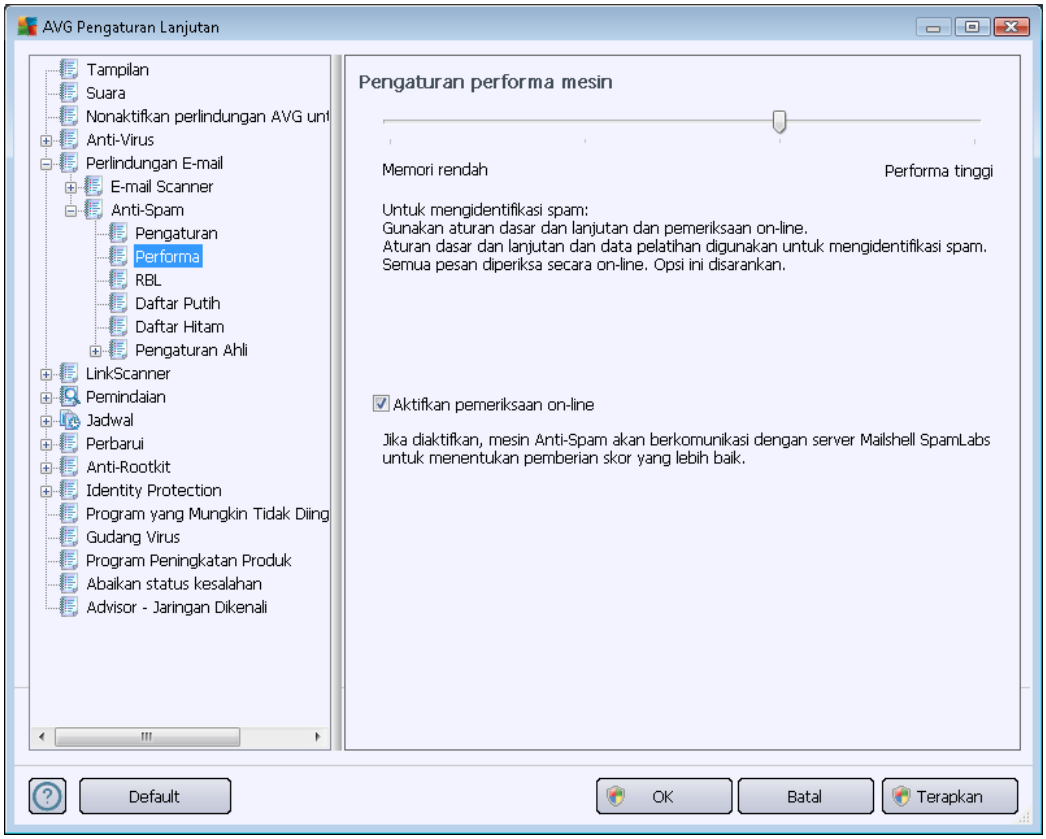


Dalam dialog ini, Anda dapat mengatur pemfilteran pesan e-mail.

- ***Semua pesan (tanpa pemfilteran)*** – Jika Anda yakin folder yang dipilih hanya berisi pesan yang ingin Anda digunakan untuk pelatihan, pilih opsi ***Semua pesan (tanpa pemfilteran)***.
- ***Gunakan filter*** – Untuk pemfilteran lebih lanjut, pilih opsi ***Gunakan filter***. Anda dapat memasukkan kata (*nama*), bagian kata, atau frasa yang akan dicari di bidang perihal dan/ atau pengirim e-mail. Semua pesan yang cocok dengan kriteria yang dimasukkan akan digunakan untuk pelatihan, tanpa ada pertanyaan lagi. Bila Anda mengisi kedua bidang teks, alamat yang hanya cocok dengan salah satu dari kedua ketentuan tersebut juga akan digunakan!
- ***Tanyakan untuk setiap pesan*** – Jika Anda tidak yakin tentang pesan yang terdapat dalam folder, dan ingin wizard menanyakan setiap pesan *(sehingga Anda dapat memutuskan apakah akan digunakan untuk pelatihan atau tidak)*, pilih opsi ***Tanyakan untuk setiap pesan***.

Bila opsi yang sesuai telah dipilih, klik ***Berikutnya***. Dialog berikut hanya sebagai informasi, yang memberitahu Anda bahwa wizard siap memproses pesan. Untuk memulai pelatihan, klik lagi tombol ***Berikutnya***. Pelatihan kemudian akan dimulai sesuai kondisi yang dipilih sebelumnya.

Dialog ***Pengaturan performa mesin*** (*ditautkan ke item* ***Performa*** *pada navigasi kiri*) menyediakan pengaturan performa komponen ***Anti-Spam***:



Gerakkan geseran ke kiri atau ke kanan untuk mengubah tingkat performa pemindaian yang berkisar antara mode ***Memori rendah*** / ***Performa tinggi***.

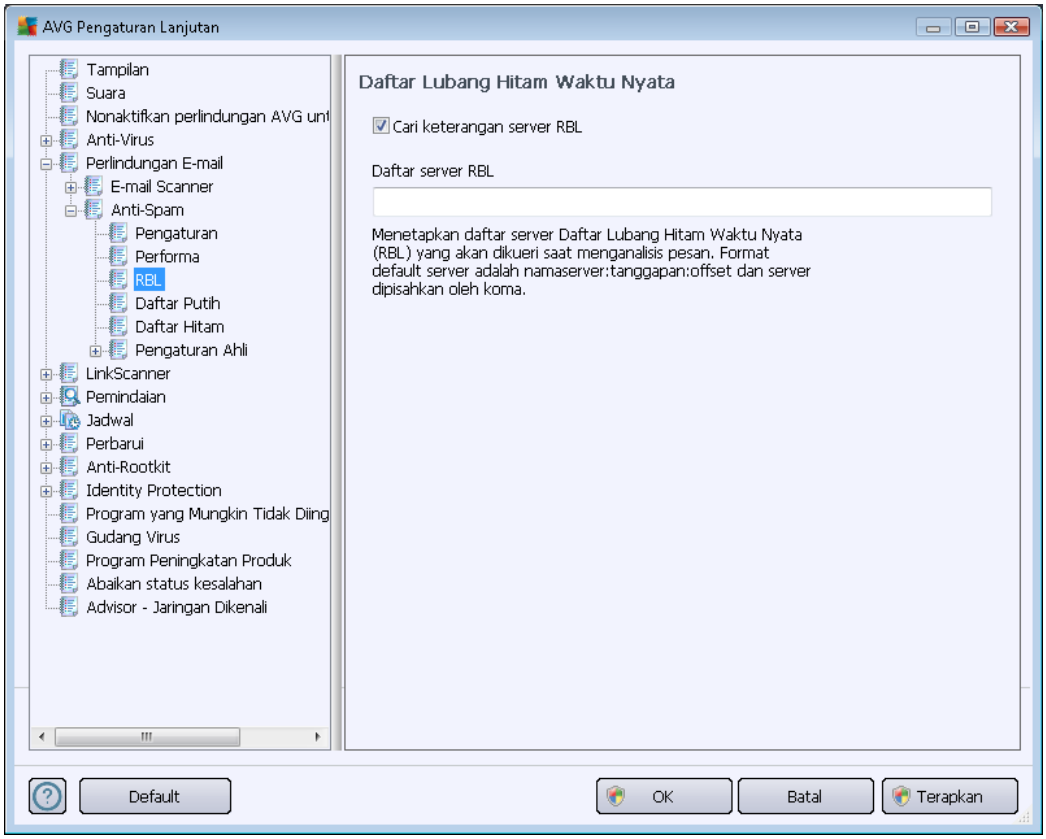
- ***Memori rendah*** – selama proses pemindaian untuk mengenali spam, tidak ada aturan yang akan digunakan. Hanya data pelatihan yang akan digunakan untuk identifikasi. Mode ini tidak disarankan untuk penggunaan biasa, kecuali perangkat keras komputer benar-benar lemah.

- ***Performa tinggi*** - mode ini akan menghabiskan banyak memori. Selama proses pemindaian untuk mengenali spam, fitur berikut akan digunakan: aturan dan cache basis data spam, aturan dasar dan lanjutan, basis data alamat IP dan basis data spammer.

Item ***Aktifkan pemeriksaan online*** diaktifkan secara default. Ini menghasilkan deteksi spam yang lebih akurat melalui komunikasi dengan server Mailshell, yakni data yang telah dipindai akan dibandingkan dengan basis data online Mailshell.

Umumnya disarankan untuk mempertahankan pengaturan default dan hanya mengubahnya jika Anda punya alasan yang kuat untuk melakukannya. Semua perubahan pada konfigurasi ini hanya boleh dilakukan oleh pengguna yang sudah ahli!

Item ***RBL*** akan membuka dialog pengeditan yang disebut ***Daftar Lubang Hitam Seketika*** di mana Anda dapat mengaktifkan/menonaktifkan fungsi ***Tanya server RBL***:

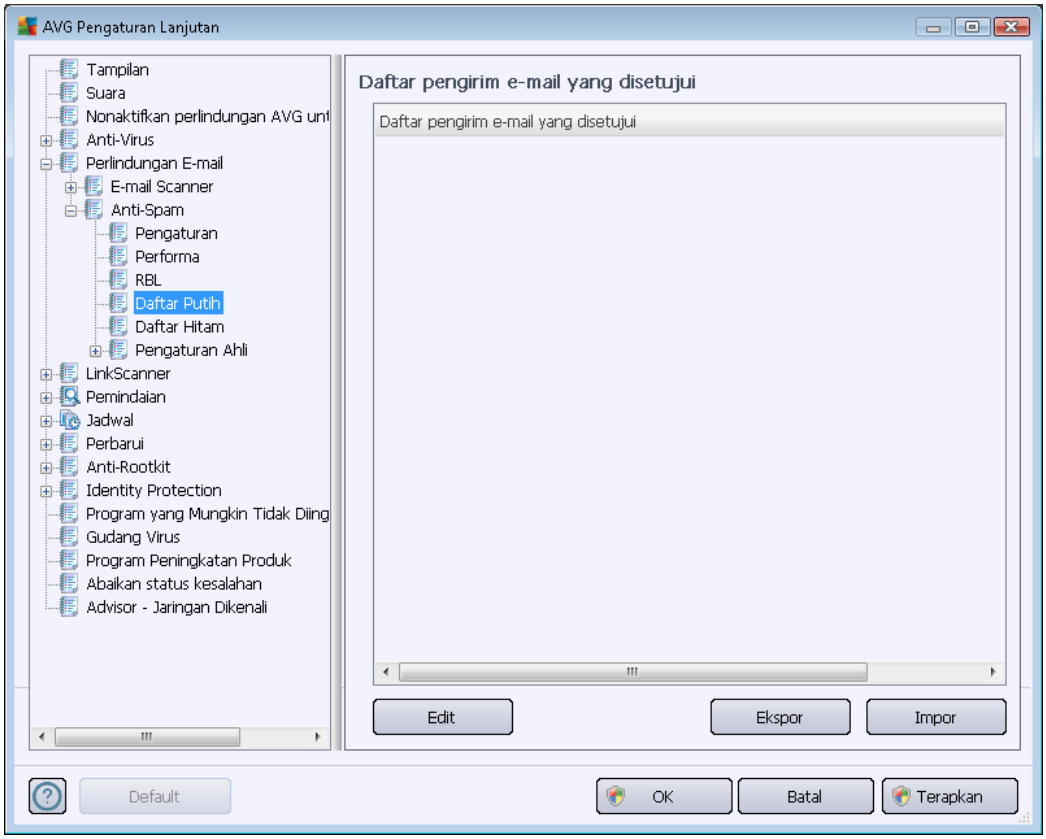


Server RBL (*Daftar Lubang Hitam Seketika*) adalah server DNS dengan basis data ekstensif tentang pengirim spam yang telah dikenal. Bila fitur ini diaktifkan, semua pesan e-mail akan diverifikasi terhadap basis data server RBL dan ditandai sebagai spam jika identik dengan suatu entri basis data. Basis data server RBL ini berisi sidik jari spam terbaru, untuk memberikan deteksi spam yang terbaik dan paling akurat. Fitur ini terutama bermanfaat bagi pengguna yang menerima spam dalam jumlah besar yang biasanya tidak terdeteksi oleh mesin Anti-Spam.

Daftar server RBL memungkinkan Anda menentukan lokasi server RBL tertentu (*harap diperhatikan bahwa mengaktifkan fitur ini pada beberapa sistem dan konfigurasi akan memperlambat proses penerimaan email, karena setiap pesan email harus diverifikasi terhadap basis data server RBL).*

Tidak ada data pribadi yang dikirim ke server!

Item ***Daftar Putih*** membuka dialog ***Daftar pengirim e-mail yang disetujui*** yang berisi daftar global berbagai alamat e-mail dan domain pengirim yang disetujui, yang pesannya tidak akan ditandai sebagai spam.



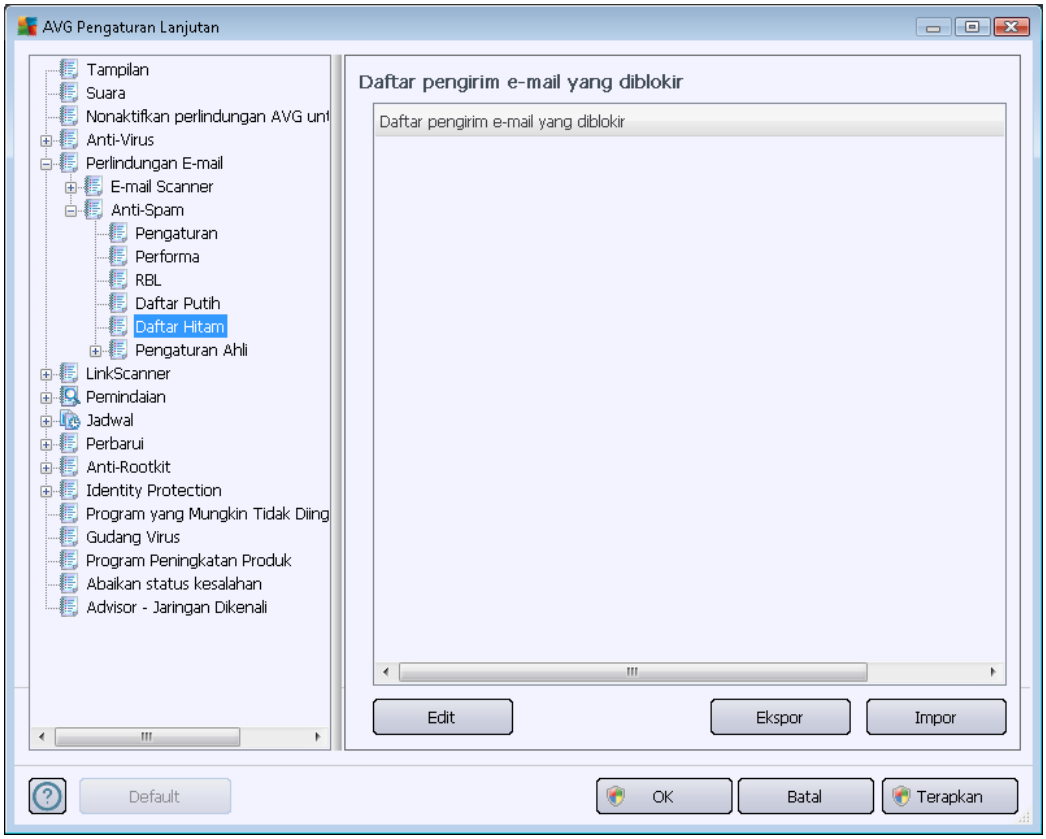
Dalam antarmuka pengeditan, Anda dapat mengompilasi daftar pengirim yang Anda yakin tidak akan mengirimi Anda pesan yang tidak diinginkan (spam). Anda juga dapat mengompilasi daftar nama domain lengkap (*misalnya avg.com*), yang Anda tahu tidak akan membuat pesan spam. Setelah Anda membuat daftar pengirim dan/atau nama domain, Anda dapat mengisinya dengan salah satu metode berikut: dengan memasukkan langsung setiap alamat e-mail atau dengan mengimpor seluruh daftar alamat sekaligus.

Tombol kontrol

Tombol kontrol berikut ini tersedia:

- ***Edit*** – tekan tombol ini untuk membuka dialog, di mana Anda dapat memasukkan daftar alamat secara manual (*Anda juga dapat menggunakan salin dan tempel*). Masukkan satu item (*pengirim, nama domain*) per baris.
- ***Ekspor*** – jika Anda memutuskan untuk mengekspor record karena suatu tujuan, Anda dapat melakukannya dengan menekan tombol ini. Semua record akan disimpan ke file teks biasa.
- ***Impor*** – jika Anda sudah membuat file teks dari berbagai alamat email/nama domain, Anda bisa langsung mengimpornya dengan memilih tombol ini. Isi file hanya boleh berisi satu item (*alamat, nama domain*) per baris.

Item ***Daftar Hitam*** membuka dialog berisi daftar global berbagai alamat e-mail dan nama domain pengirim yang diblokir, yang pesannya selalu ditandai sebagai spam.



Dalam antarmuka pengeditan, Anda dapat mengompilasi daftar pengirim yang Anda perkirakan akan mengirimi Anda pesan yang tidak diinginkan *(spam)*. Anda juga dapat mengompilasi daftar nama domain lengkap (*misalnya spammingcompany.com*), yang Anda perkirakan atau pernah terima pesan spam darinya. Semua e-mail dari alamat/domain yang tercantum akan dikenali sebagai spam. Setelah Anda membuat daftar pengirim dan/atau nama domain, Anda dapat mengisinya dengan salah satu metode berikut: dengan memasukkan langsung setiap alamat e-mail atau dengan mengimpor seluruh daftar alamat sekaligus.

Tombol kontrol

Tombol kontrol berikut ini tersedia:

- ***Edit*** – tekan tombol ini untuk membuka dialog, di mana Anda dapat memasukkan daftar alamat secara manual (*Anda juga dapat menggunakan salin dan tempel*). Masukkan satu item (*pengirim, nama domain*) per baris.
- ***Ekspor*** – jika Anda memutuskan untuk mengekspor record karena suatu tujuan, Anda dapat melakukannya dengan menekan tombol ini. Semua record akan disimpan ke file teks biasa.

- ***Impor*** – jika Anda sudah membuat file teks dari berbagai alamat email/nama domain, Anda bisa langsung mengimpornya dengan memilih tombol ini.

Cabang Pengaturan Lanjutan berisi opsi pengaturan lengkap untuk komponen Anti-Spam. Pengaturan ini khusus ditujukan untuk pengguna berpengalaman, umumnya administrator jaringan yang perlu mengkonfigurasi perlindungan anti-spam secara terperinci untuk perlindungan terbaik server e-mail. Oleh karena itu, tidak ada bantuan tambahan untuk setiap dialog; namun, tersedia keterangan singkat untuk masing-masing opsi langsung di antarmuka penggunanya.

Kami sangat menyarankan untuk tidak mengubah pengaturan apa pun kecuali Anda menguasai pengaturan lanjutan Spamcatcher (MailShell Inc.). Setiap perubahan yang tidak sesuai dapat menurunkan performa atau mengakibatkan kesalahan fungsionalitas komponen.

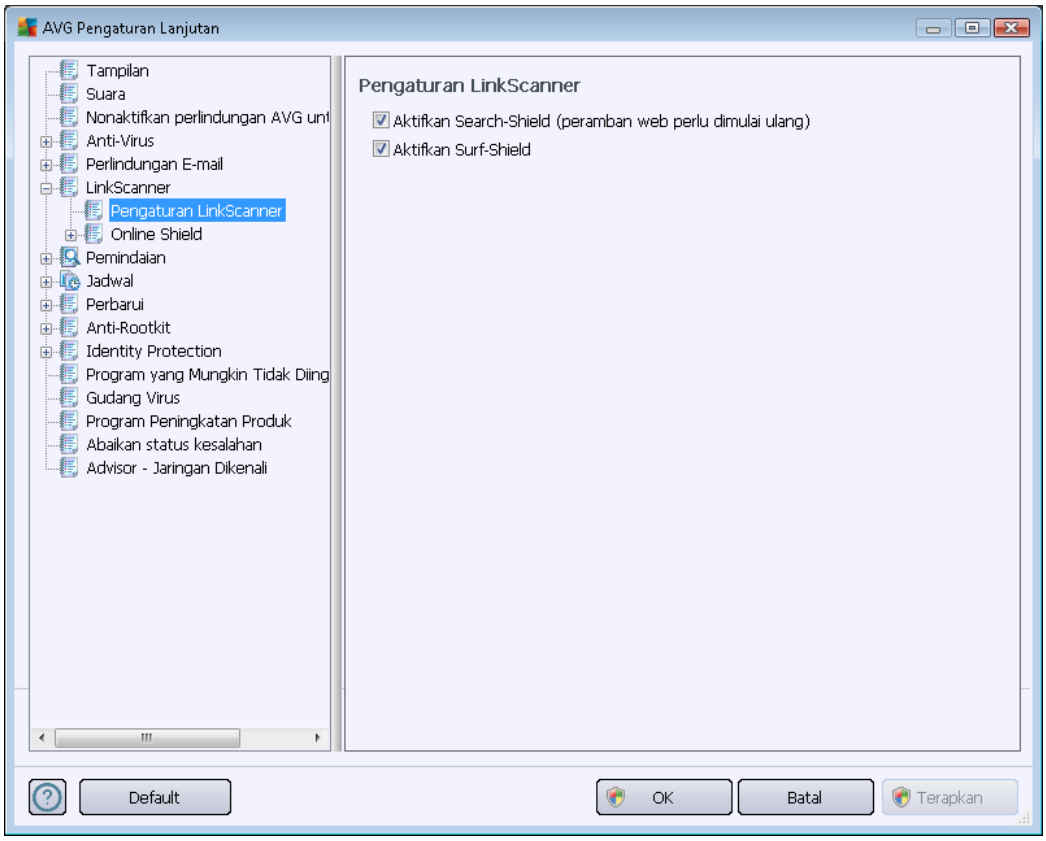
Jika Anda tetap merasa perlu mengubah konfigurasi Anti-Spam pada tingkat lanjut, ikutilah petunjuk yang disediakan langsung dalam antarmuka pengguna. Umumnya, dalam setiap dialog Anda akan menemukan satu fitur spesifik dan Anda dapat mengeditnya – keterangannya selalu disertakan dalam dialognya:

- ***Cache*** – sidik jari, reputasi domain, LegitRepute
- ***Pelatihan*** - entri kata maksimum, ambang batas pelatihan otomatis, bobot
- ***Pemfilteran*** - daftar bahasa, daftar negara, IP yang disetujui, IP yang diblokir, negara yang diblokir, charset yang diblokir, pengirim bohong-bohongan
- ***RBL*** – server RBL, multihit, ambang batas, batas waktu, IP maksimum
- ***Koneksi Internet*** – batas waktu, server proxy, autentikasi proxy

10.6. LinkScanner

10.6.1. Pengaturan LinkScanner

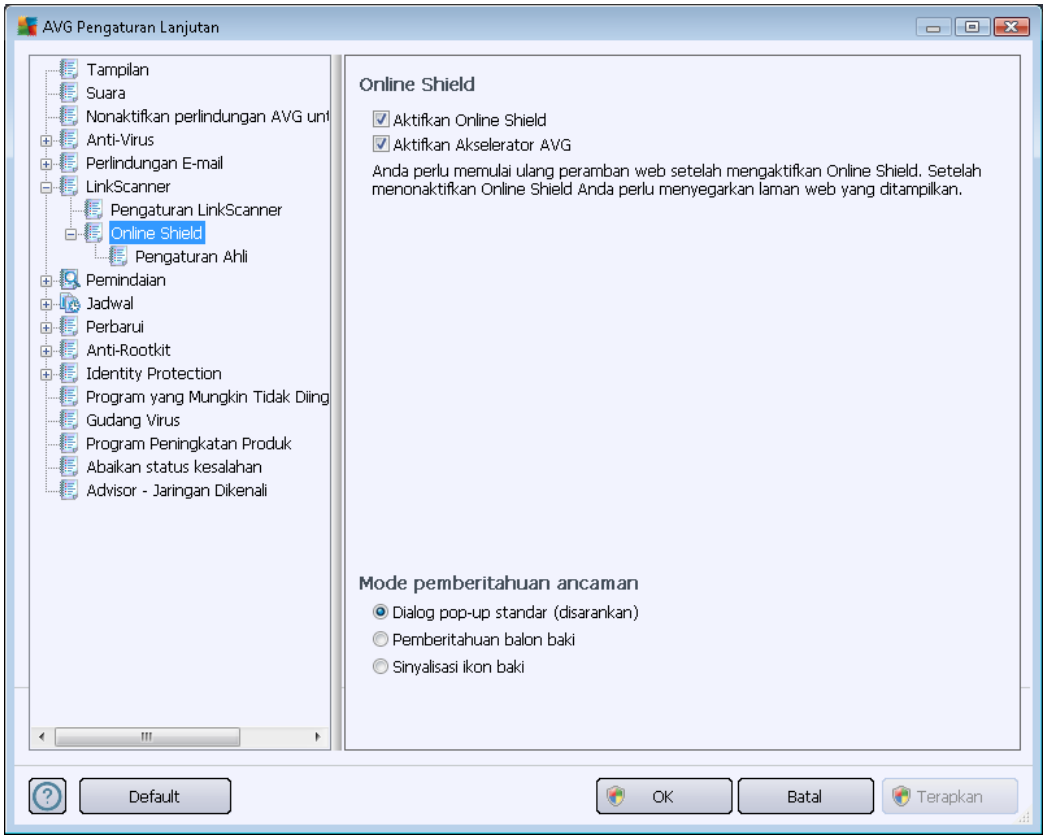
Dialog pengaturan ***LinkScanner*** memungkinkan Anda mengaktifkan/menonaktifkan fitur dasar LinkScanner:



- ***Aktifkan Search-Shield*** – (*aktif secara default*): ikon pemberi tahu mengenai penelusuran yang dilakukan dengan Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, atau SlashDot agar memeriksa konten situs yang dihasilkan oleh mesin telusur.

- ***Aktifkan Surf-Shield*** – (*diaktifkan secara default*): perlindungan (*waktu-nyata*) aktif terhadap situs eksploitif saat mengaksesnya. Koneksi situs jahat yang telah dikenal dan konten eksploitifnya diblokir begitu ia diakses oleh pengguna melalui peramban Web (*atau aplikasi lain yang menggunakan HTTP*).

10.6.2. Online Shield



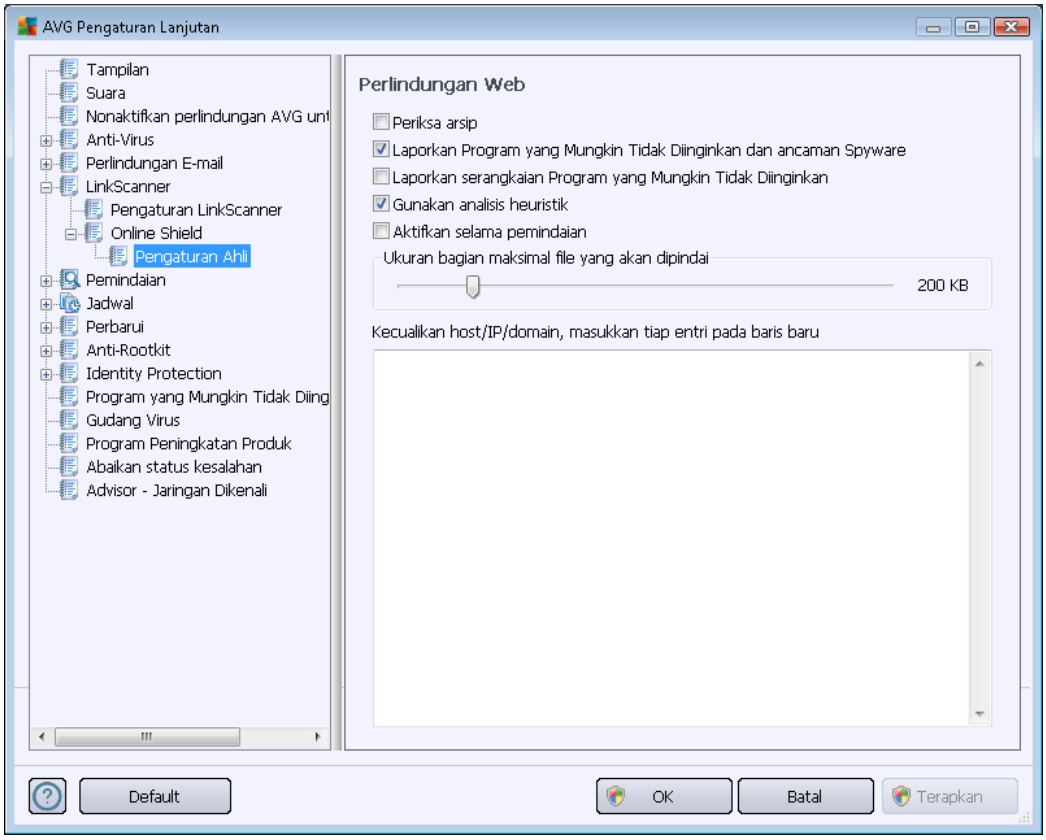
Dialog ***Online Shield*** menyediakan opsi berikut:

- ***Aktifkan Online Shield*** *(diaktifkan secara default)* – Mengaktifkan/menonaktifkan seluruh layanan ***Online Shield***. Untuk pengaturan lanjutan selebihnya pada ***Online Shield*** harap lanjutkan ke dialog berikutnya bernama Perlindungan Web.

- ***Aktifkan AVG Accelerator*** *(diaktifkan secara default)* - Mengaktifkan/menonaktifkan layanan ***AVG Accelerator*** yang memungkinkan pemutaran video online menjadi lebih halus dan membuat pengunduhan tambahan jadi lebih mudah.

Mode pemberitahuan ancaman

Di bagian bawah dialog, pilih dengan cara apa Anda ingin diberi tahu tentang kemungkinan ancaman yang terdeteksi: lewat dialog standar yang muncul, lewat pemberitahuan balon baki, atau lewat info ikon baki.



Dalam dialog ***Perlindungan Web***, Anda dapat mengedit konfigurasi komponen yang menyangkut pemindaian konten situs Web. Antarmuka pengeditan memungkinkan Anda untuk mengkonfigurasi beberapa opsi dasar berikut:

- ***Aktifkan Perlindungan Web*** – opsi ini mengkonfirmasi bahwa ***Online Shield*** harus melakukan pemindaian atas isi halaman www. Asalkan opsi ini diaktifkan (*secara default*), Anda dapat mengaktifkan/menonaktifkan item ini:
    - ***Periksa arsip*** – (*dinonaktifkan secara default*): memindai isi arsip yang mungkin telah dimasukkan di halaman www yang akan ditampilkan.
    - ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** – (*diaktifkan secara default*): tandai untuk mengaktifkan mesin Anti-Spyware, dan memindai spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang memang sengaja diinstal. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.
    - ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** -(*dinonaktifkan secara default*): tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal

ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Gunakan analisis heuristik*** - (*diaktifkan secara default*): memindai isi halaman yang akan ditampilkan, menggunakan metode analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*).

- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default*) – dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi virus atau exploit*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai bahkan area yang paling sulit terinfeksi di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Ukuran bagian file maksimum yang akan dipindai*** – jika file yang disertakan ada di halaman yang ditampilkan, Anda juga dapat memindai isinya bahkan sebelum diunduh ke komputer Anda. Namun, pemindaian file besar akan memakan waktu lama dan halaman Web mungkin diunduh jauh lebih pelan. Anda dapat menggunakan bilah geser untuk menetapkan ukuran maksimum file yang masih akan dipindai dengan ***Online Shield***. Sekalipun file yang telah diunduh lebih besar dari yang ditetapkan, sehingga tidak akan dipindai dengan Online Shield, Anda masih terlindungi: seandainya file terinfeksi, ***Resident Shield*** akan segera mendeteksinya.

- ***Kecualikan host/IP/domain*** – dalam bidang teks, Anda dapat mengetikkan nama pasti dari sebuah server (*host, alamat IP, alamat IP dengan mask, atau URL*) atau domain yang tidak perlu dipindai oleh ***Online Shield***. Karena itu kecualikan hanya host yang Anda benar-benar yakini tidak akan menyediakan konten situs Web berbahaya.

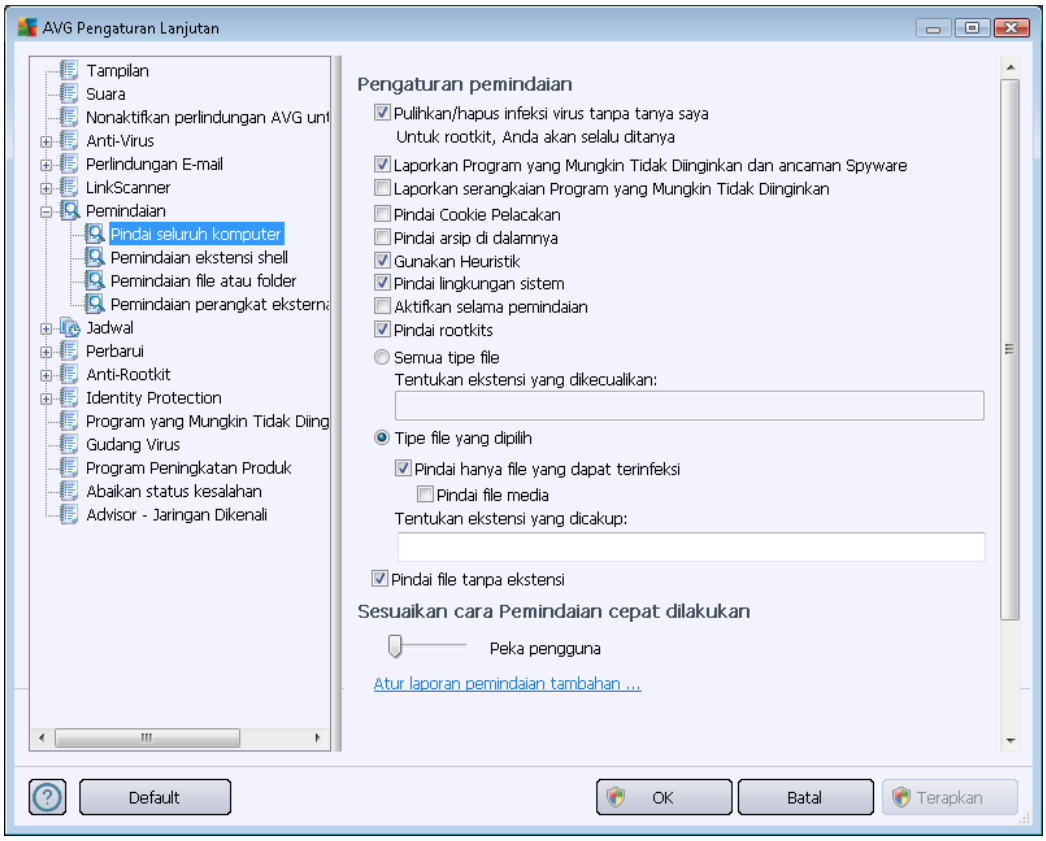
10.7. Pemindaian

Pengaturan pindai lanjutan terbagi ke dalam empat kategori yang merujuk pada tipe pemindaian tertentu sebagaimana ditentukan oleh vendor perangkat lunak:

- ***Pindai Seluruh Komputer*** - pemindaian standar yang ditentukan untuk seluruh komputer
- ***Pemindaian Ekstensi Shell*** - pemindaian tertentu atas objek yang dipilih, langsung dari lingkungan Windows Explorer
- ***Pemindaian file atau folder*** – pemindaian standar yang ditentukan atas area yang dipilih pada komputer Anda
- ***Pemindaian Perangkat Lepas-Pasang*** – pemindaian tertentu atas perangkat lepas-pasang yang dipasang pada komputer Anda

10.7.1. Pemindaian seisi komputer

Opsi ***Pemindaian Seisi Komputer*** memungkinkan Anda mengedit parameter salah satu pemindaian yang telah ditetapkan oleh vendor perangkat lunak, Pindai seisi komputer:



Pengaturan pindai

Bagian ***Pengaturan pindai*** menyediakan daftar parameter pemindaian yang secara opsional dapat diaktifkan/dinonaktifkan:

- ***Pulihkan/hapus infeksi tanpa bertanya pada saya*** (*diaktifkan secara default*) – jika ada virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.
- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – tandai untuk mengaktifkan mesin Anti-Spyware, dan memindai spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak sengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.
- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan*

secara default) – tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai Cookie Pelacak*** (*dinonaktifkan secara default*) – parameter komponen Anti-Spyware ini menetapkan bahwa cookie harus dideteksi selama pemindaian ; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*)

- ***Pindai di dalam arsip*** (*dinonaktifkan secara default*) – parameter ini menetapkan bahwa pemindaian harus memeriksa semua file yang tersimpan dalam arsip, misalnya, ZIP, RAR, ...

- ***Gunakan Heuristik*** (*diaktifkan secara default*): analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian

- ***Pindai lingkungan sistem*** (*diaktifkan secara default*) – pemindaian juga akan memeriksa area sistem komputer Anda.

- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default*) – dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi virus atau exploit*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pindai rootkit*** (*aktifkan secara default*) – pemindaian Anti-Rootkit menelusuri komputer Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Selanjutnya, Anda harus menentukan apakah Anda ingin memindai

- ***Semua tipe file*** dengan memungkinkan penetapan pengecualian dari pemindaian dengan memberikan daftar file ekstensi yang dipisah koma (*setelah disimpan, koma akan berganti menjadi titik koma*) untuk file yang tidak boleh dipindai;

- ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak ditandai, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

- Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya

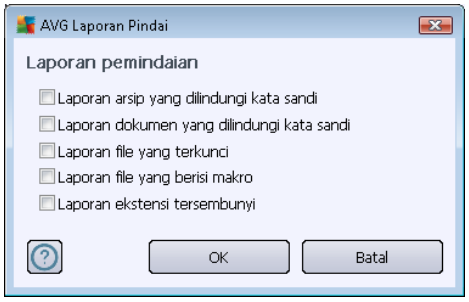
kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

Sesuaikan secepat apa Pemindaian selesai

Di bagian ***Sesuaikan kecepatan melakukan pemindaian*** Anda dapat menentukan lebih jauh kecepatan pemindaian sesuai dengan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu namun penggunaan sumber daya sistem akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan penggunaan sumber daya sistem dengan memperpanjang waktu pemindaian.

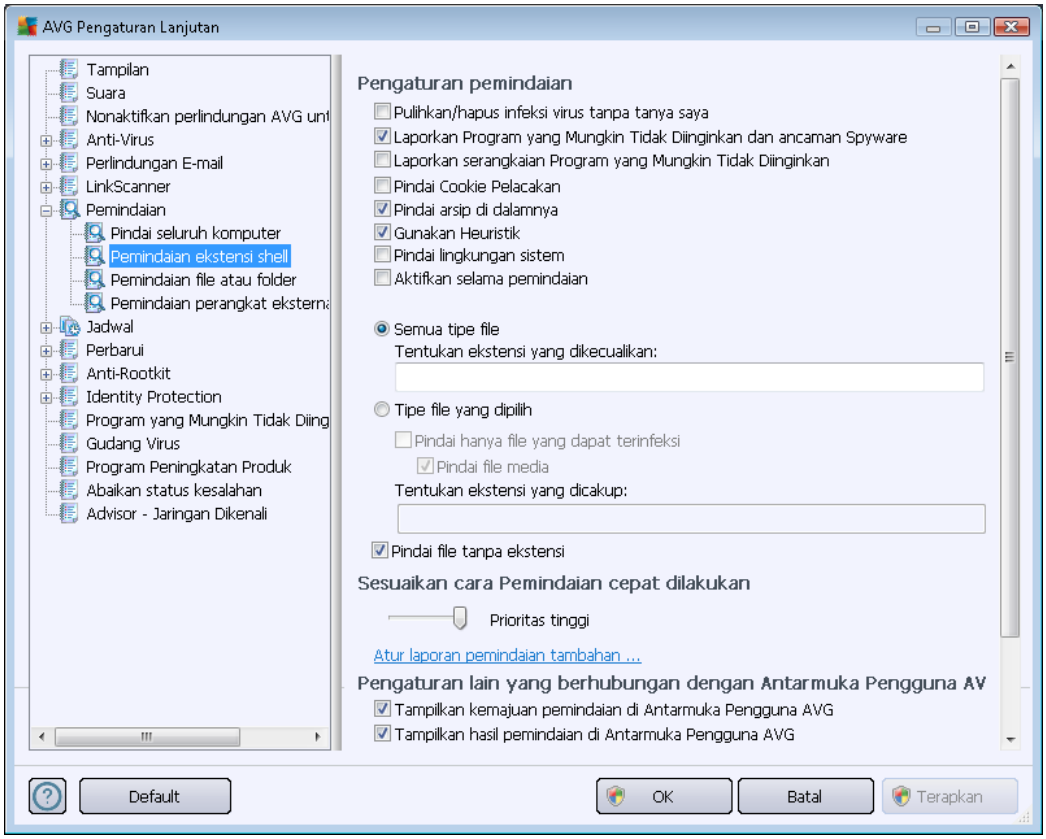
Atur laporan pemindaian tambahan ...

Klik tautan ***Atur laporan pindai tambahan ...*** untuk membuka jendela dialog mandiri bernama ***Laporan pindai*** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:



10.7.2. Pemindaian ekstensi shell

Seperti pada fungsi Pemindaian Seisi Komputer sebelumnya, fungsi yang dinamai ***Pemindaian ekstensi shell*** ini juga menawarkan beberapa opsi untuk mengedit pemindaian yang sudah ditentukan oleh vendor perangkat lunak. Kali ini konfigurasi berhubungan dengan pemindaian objek tertentu yang diluncurkan langsung dari lingkungan Windows Explorer (*ekstensi shell*), lihat bab Pemindaian di Windows Explorer:



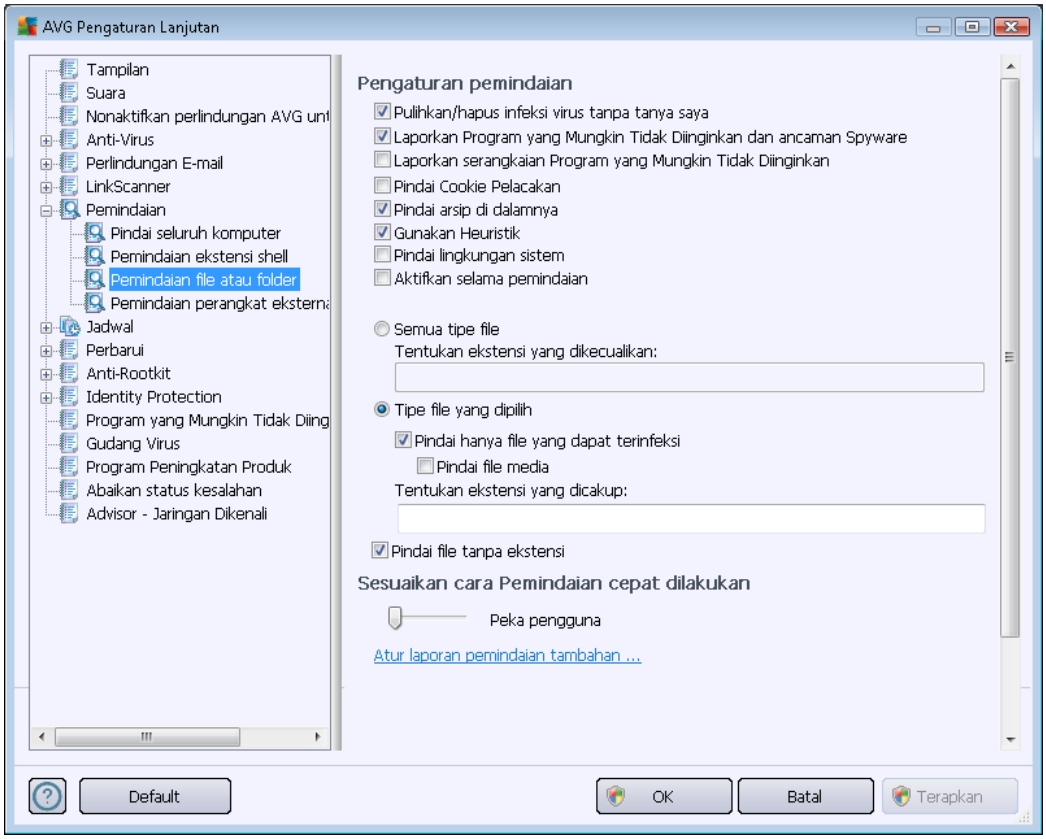
Daftar parameter identik dengan yang tersedia untuk Pindai seluruh komputer. Akan tetapi, pengaturan default berbeda *misalnya, Pindai Seluruh Komputer secara default tidak memeriksa arsip tetapi memindai lingkungan sistem; sementara Pemindaian Ekstensi Shell melakukan sebaliknya.*).

Catatan: *Untuk keterangan mengenai parameter tertentu, bacalah bab Pengaturan Lanjutan AVG / Pemindaian / Pindai Seluruh Komputer.*

Dibandingkan dengan dialog Pemindaian Seisi Komputer, dialog ***Pemindaian ekstensi shell*** juga berisi bagian bernama ***Pengaturan lainnya terkait dengan Antarmuka Pengguna AVG***, tempat Anda dapat menentukan apakah Anda ingin kemajuan dan hasil pemindaian dapat diakses dari antarmuka pengguna AVG. Juga, Anda dapat menentukan bahwa hasil pemindaian seharusnya hanya ditampilkan jika ada infeksi yang terdeteksi selama pemindaian.

10.7.3. Pemindaian file atau folder

Antarmuka pengeditan untuk ***Pindai file atau folder tertentu*** identik dengan dialog pengeditan Pindai Seluruh Komputer. Semua opsi konfigurasinya sama; walau demikian, pengaturan default lebih ketat untuk Pindai seluruh komputer:

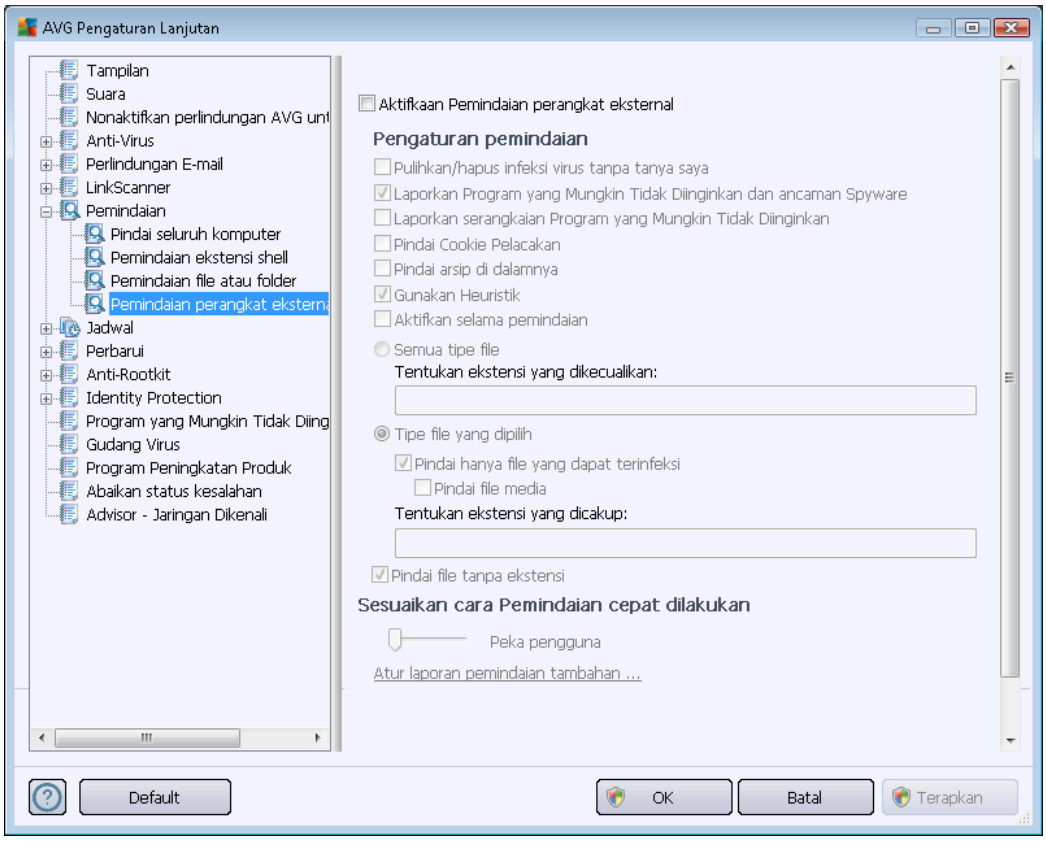


Semua parameter yang diatur dalam dialog konfigurasi ini hanya berlaku untuk area yang dipilih bagi pemindaian dengan Pindai file atau folder tertentu!

Catatan: *Untuk keterangan mengenai parameter tertentu, bacalah bab Pengaturan Lanjutan AVG / Pemindaian / Pindai Seluruh Komputer.*

10.7.4. Pemindaian perangkat eksternal

Antarmuka pengeditan untuk ***Pemindaian perangkat eksternal*** juga sangat mirip dengan dialog pengeditan Pindai Seluruh Komputer.



Pemindaian perangkat eksternal diluncurkan secara otomatis begitu Anda memasang perangkat eksternal ke komputer Anda. Secara default, pemindaian ini dinonaktifkan. Walau demikian, sangatlah penting memindai ancaman potensial pada perangkat eksternal karena merupakan sumber infeksi utama. Untuk menyiapkan pemindaian ini dan agar diluncurkan secara otomatis bila diperlukan, tandai opsi ***Aktifkan pemindaian perangkat eksternal***.

Catatan: *Untuk keterangan mengenai parameter tertentu, bacalah bab Pengaturan Lanjutan AVG / Pemindaian / Pindai Seluruh Komputer.*

10.8. Jadwal

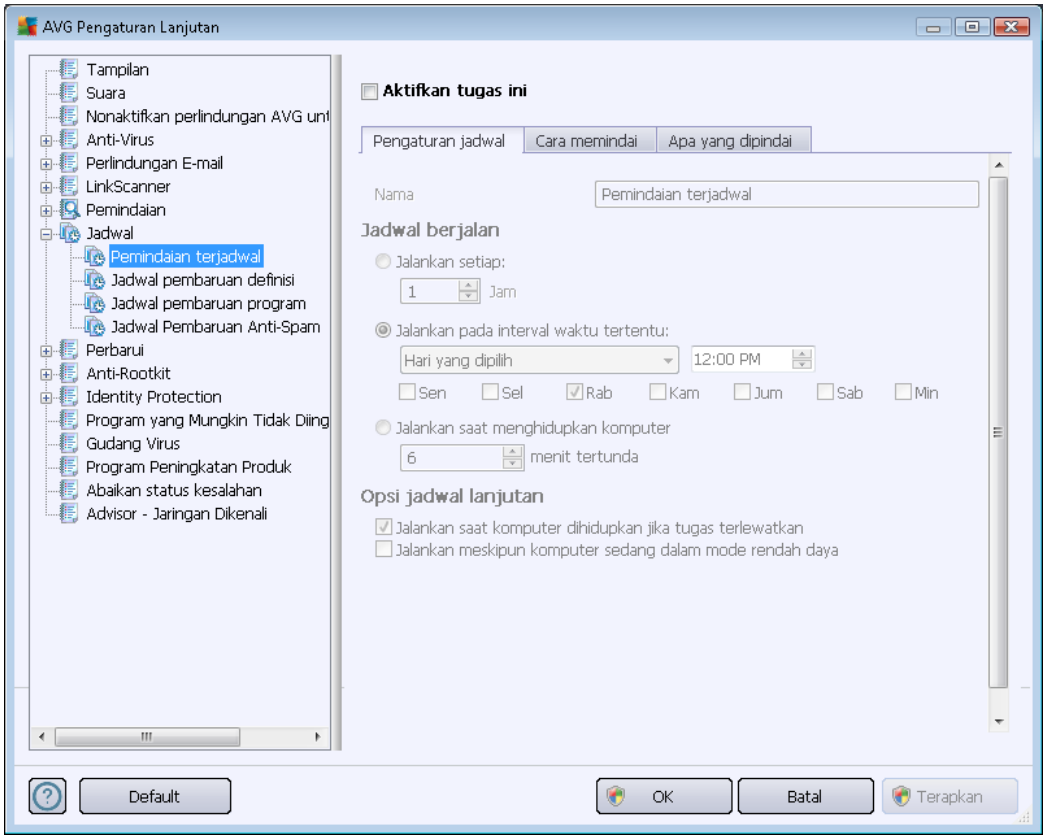
Di bagian ***Jadwal*** Anda dapat mengedit pengaturan default:

- Pemindaian terjadwal
- Jadwal pembaruan definisi
- Jadwal pembaruan program

- Jadwal pembaruan Anti-Spam

10.8.1. Pemindaian Terjadwal

Parameter pemindaian terjadwal dapat diedit (*atau jadwal baru yang telah diatur*) pada ketiga tab. Pada tiap tab, Anda dapat menandai/tidak menandai item ***Aktifkan tugas ini*** terlebih dahulu untuk menonaktifkan tes terjadwal untuk sementara, dan mengaktifkannya lagi saat diperlukan:



Berikutnya, dalam bidang teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) terdapat nama yang ditetapkan ke jadwal ini oleh vendor program. Untuk jadwal yang baru ditambah (*Anda dapat menambahkan jadwal baru dengan mengklik kanan di atas item* ***Pemindaian terjadwal*** *dalam struktur navigasi di sebelah kiri*) Anda dapat menetapkan nama Anda sendiri, dan dalam hal ini bidang teks akan terbuka untuk pengeditan. Cobalah selalu gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah mengenali pemindaian tersebut nanti dari jadwal lain.

Contoh: *Tidaklah tepat untuk memberi nama pemindaian dengan "Pemindaian baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang sebenarnya diperiksa oleh pemindaian tersebut. Sebaliknya, sebuah contoh nama deskriptif yang baik misalnya "Pemindaian area sistem", dll. Yang juga tidak perlu ditetapkan dalam nama pemindaian adalah apakah pemindaian itu untuk seluruh komputer atau pun hanya untuk pemindaian atas file atau folder yang dipilih – pemindaian Anda akan selalu menjadi versi spesifik dari pindai file atau folder yang dipilih.*

Dalam dialog ini, Anda dapat menentukan lebih lanjut parameter pemindaian berikut:

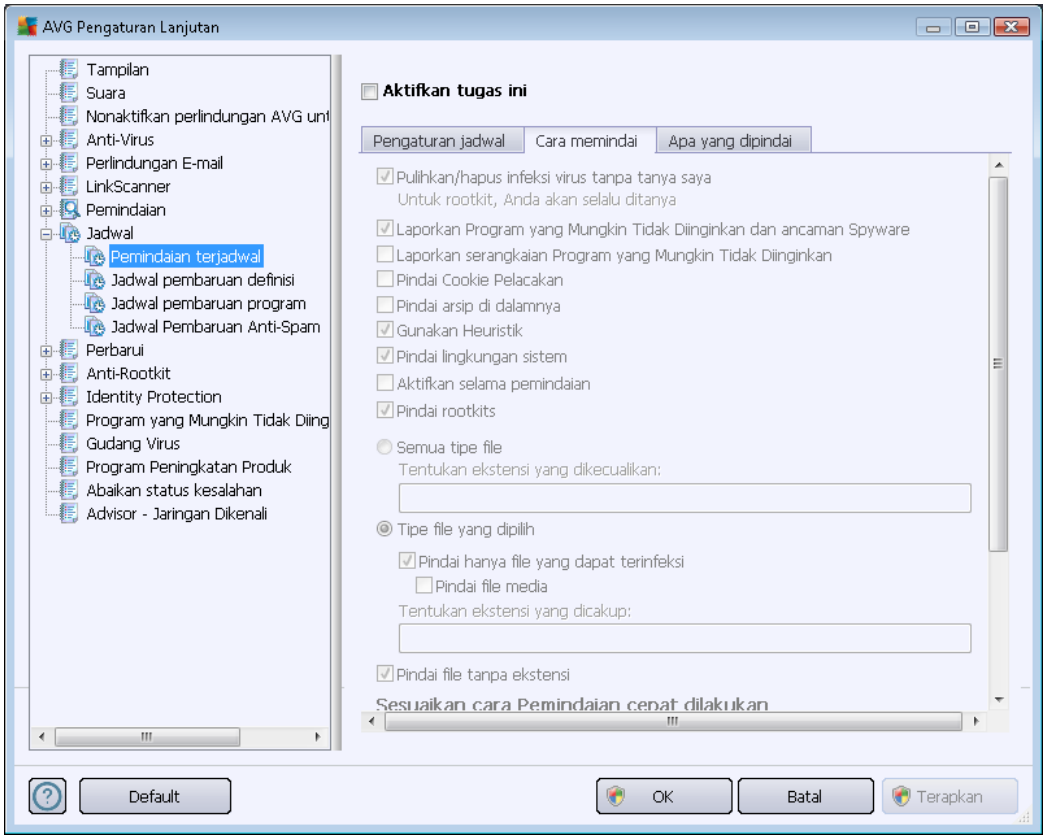
Jadwal berjalan

Di sini, Anda dapat menetapkan interval waktu untuk peluncuran pemindaian yang baru dijadwalkan. Penentuan waktu dapat ditentukan dengan pengulangan peluncuran pemindaian setelah periode waktu tertentu (***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada interval waktu tertentu ...***), atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pemindaian (***Jalankan saat menghidupkan komputer***).

Opsi jadwal lanjutan

Di bagian ini Anda dapat menentukan dalam kondisi apa pemindaian harus/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya. Setelah pemindaian terjadwal diluncurkan pada waktu yang ditetapkan, Anda akan diberi tahu mengenai hal ini melalui jendela yang muncul di atas ikon baki sistem AVG:

Sebuah ikon baki sistem AVG akan kemudian muncul (*dengan penuh warna bersama sinar berkedip*) yang memberi tahu adanya pemindaian terjadwal yang sedang dijalankan. Klik kanan pada ikon pemindaian AVG yang sedang berjalan untuk membuka konteks menu yang dapat Anda gunakan untuk memutuskan akan melakukan jeda atau bahkan menghentikan pemindaian yang sedang berjalan, dan juga mengubah prioritas pemindaian yang sedang berjalan saat itu.



Pada tab ***Cara memindai*** Anda akan menemukan daftar parameter pemindaian yang secara opsional dapat diaktifkan/dinonaktifkan. Secara default, hampir semua parameter diaktifkan dan fungsionalitasnya diterapkan selama pemindaian. ***Kecuali Anda mempunyai alasan yang kuat untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditetapkan***:

- ***Pulihkan/hapus infeksi virus tanpa bertanya pada saya*** *(diaktifkan secara default):* jika virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** *(diaktifkan secara default):* tandai untuk mengaktifkan mesin Anti-Spyware, dan memindai spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak sengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*): tandai kotak ini untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat

memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai Cookie Pelacak*** (*dinonaktifkan secara default*): parameter komponen Anti-Spyware ini menetapkan bahwa cookie harus terdeteksi selama pemindaian (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*)

- ***Pindai di dalam arsip*** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut tersimpan dalam arsip, misalnya, ZIP, RAR, ...

- ***Gunakan Heuristik*** (*diaktifkan secara default*): analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian;

- ***Pindai lingkungan sistem*** (*diaktifkan secara default*): pemindaian juga akan memeriksa area sistem komputer Anda;

- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default):* dalam kondisi khusus (*dicurigai bahwa komputer Anda terinfeksi*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pindai rootkit*** *(diaktifkan secara default): Pemindaian* Anti-Rootkit menelusuri komputer Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Selanjutnya, Anda harus menentukan apakah Anda ingin memindai

- ***Semua tipe file*** dengan memungkinkan penetapan pengecualian dari pemindaian dengan memberikan daftar file ekstensi yang dipisah koma (*setelah disimpan, koma akan berganti menjadi titik koma*) untuk file yang tidak boleh dipindai;

- ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak ditandai, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

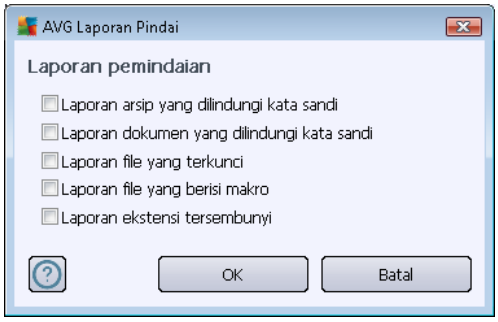
- Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

Sesuaikan secepat apa Pemindaian selesai

Di bagian ***Sesuaikan kecepatan melakukan pemindaian*** Anda dapat menentukan lebih jauh kecepatan pemindaian sesuai dengan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu namun penggunaan sumber daya sistem akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan penggunaan sumber daya sistem dengan memperpanjang waktu pemindaian.

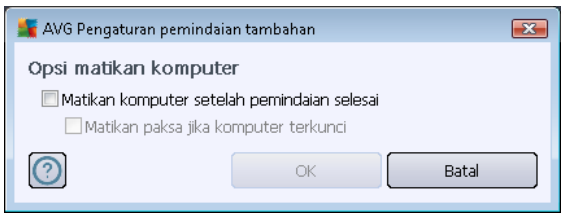
Atur laporan pemindaian tambahan

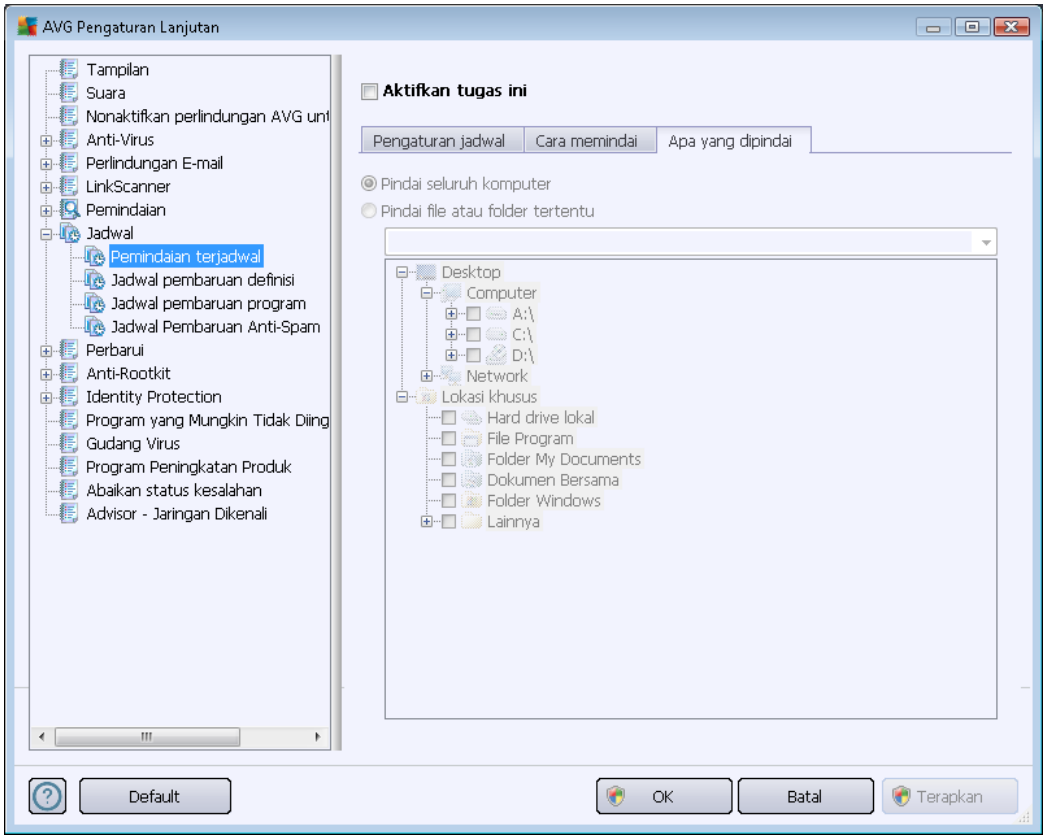
Klik tautan ***Atur laporan pindai tambahan ...*** untuk membuka jendela dialog mandiri bernama ***Laporan pindai*** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:



Pengaturan pindai tambahan

Klik ***Pengaturan pemindaian tambahan ...*** untuk membuka dialog baru ***Opsi matikan komputer*** di mana Anda dapat memutuskan apakah komputer harus dimatikan secara otomatis setelah proses pemindaian selesai. Dengan mengkonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (***Matikan paksa jika komputer terkunci***).

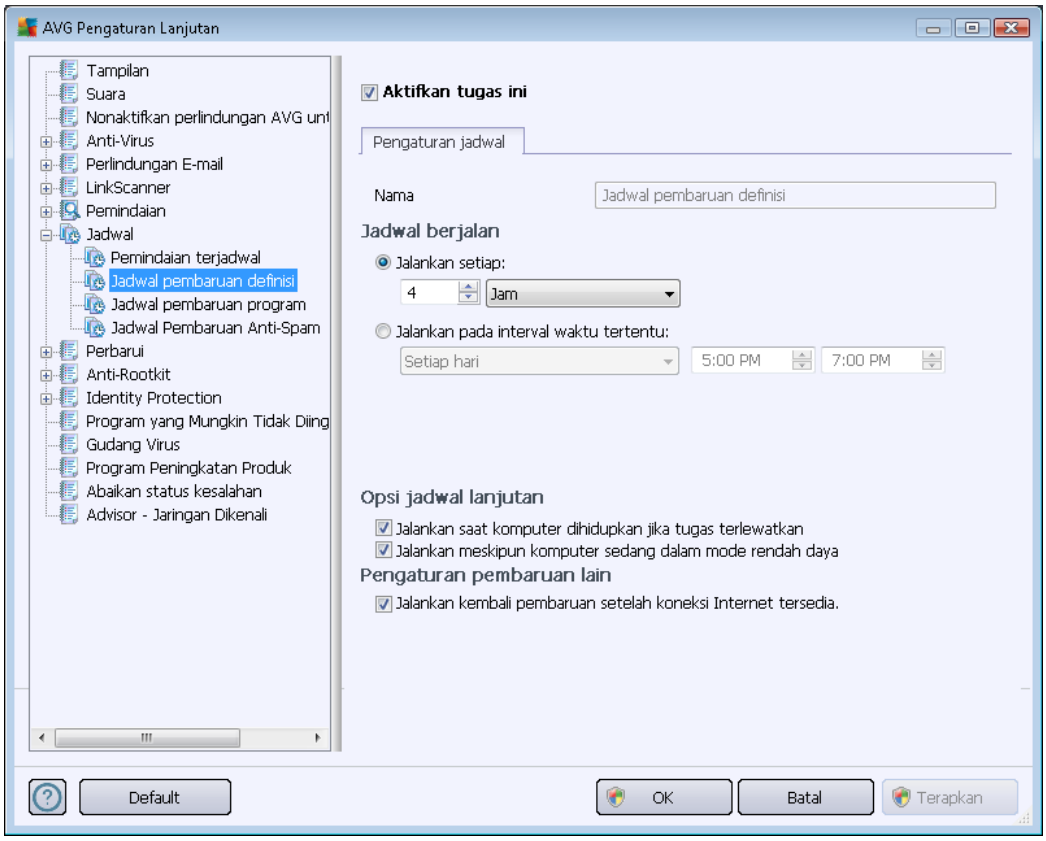




Pada tab ***Apa yang dipindai*** Anda dapat menentukan apakah Anda ingin menjadwalkan pemindaian seluruh komputer atau pemindaian file atau folder. Jika Anda memilih pemindaian file atau folder, di bagian bawah dialog ini akan diaktifkan struktur yang ditampilkan dan Anda dapat menetapkan folder yang akan dipindai.

10.8.2. Jadwal Pembaruan Definisi

Jika ***benar-benar perlu***, Anda dapat mengosongkan item ***Aktifkan tugas ini*** untuk menonaktifkan pembaruan definisi yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Dalam dialog ini Anda dapat mengatur beberapa parameter terperinci atas jadwal pembaruan definisi. Dalam bidang teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) ada nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Di bagian ini, tetapkan interval waktu untuk peluncuran pembaruan definisi yang baru dijadwalkan. Penentuan waktu dapat ditentukan dengan pengulangan peluncuran pembaruan setelah periode waktu tertentu (***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada waktu tertentu ...***).

Opsi jadwal lanjutan

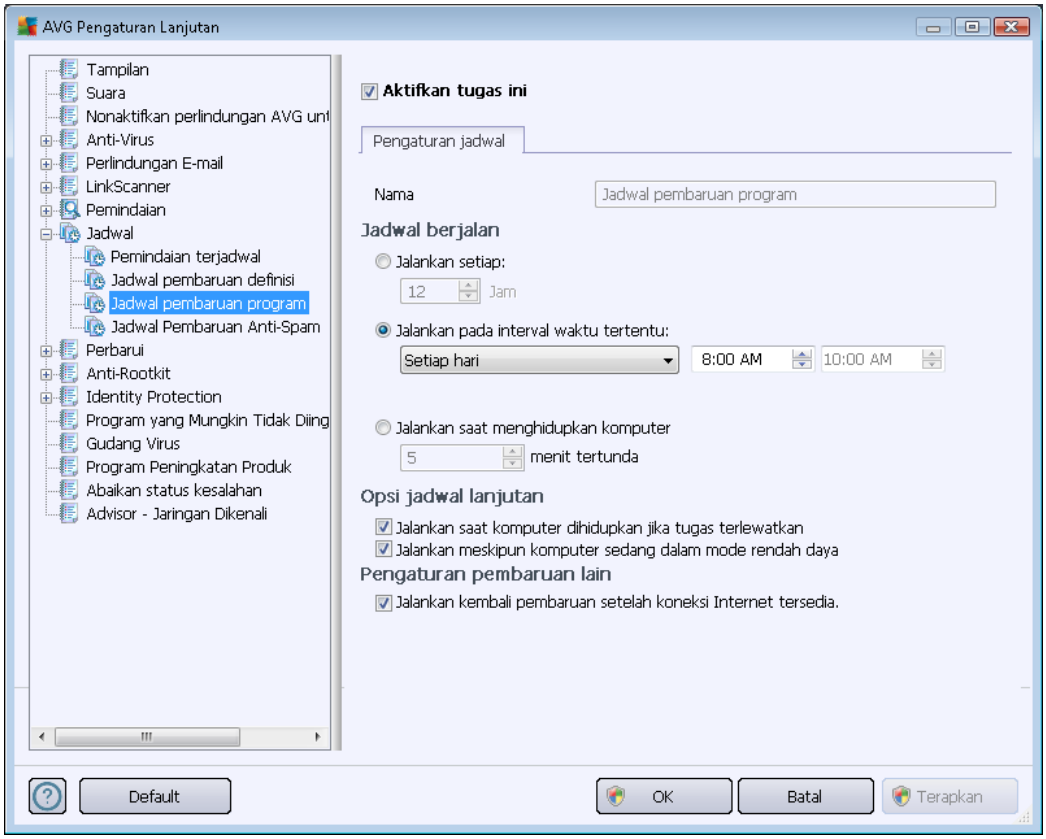
Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan definisi harus diluncurkan/tidak diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

Pengaturan pembaruan lain

Akhirnya, tandai opsi ***Jalankan lagi pembaruan begitu koneksi Internet tersedia*** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan gagal, pembaruan akan segera diluncurkan lagi setelah koneksi Internet pulih. Setelah pembaruan terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela yang muncul di atas ikon baki sistem AVG (*asalkan Anda telah membiarkan konfigurasi default pada dialog Pengaturan Lanjutan/Tampilan*).

10.8.3. Jadwal Pembaruan Program

Jika ***benar-benar perlu***, Anda dapat mengosongkan item ***Aktifkan tugas ini*** untuk menonaktifkan pembaruan program yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Dalam bidang teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) ada nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Di sini, tetapkan interval waktu untuk peluncuran pembaruan program yang baru dijadwalkan. Penentuan waktu dapat ditentukan dengan pengulangan peluncuran pembaruan setelah periode waktu tertentu (***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (

Jalankan pada waktu tertentu ...), atau mungkin dengan menentukan kejadian untuk dikaitkan dengan peluncuran pembaruan (***Tindakan berdasar pengaktifan komputer***).

Opsi jadwal lanjutan

Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan program boleh/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

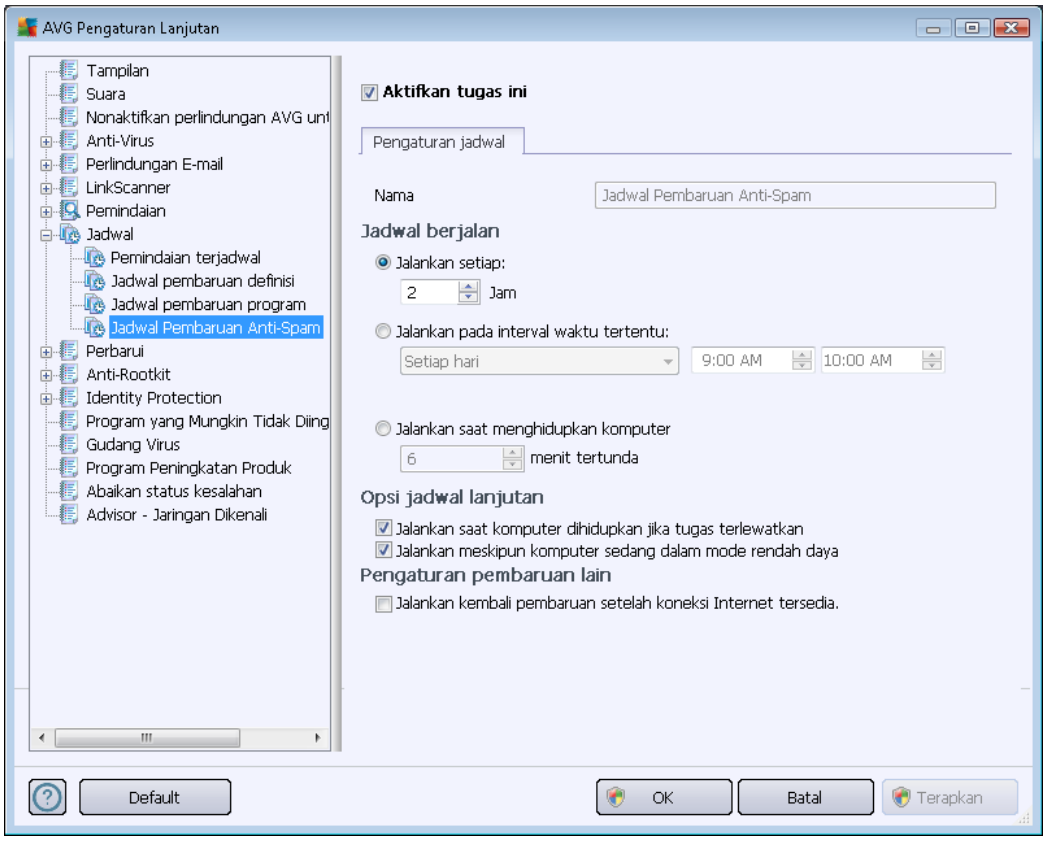
Pengaturan pembaruan lain

Tandai opsi ***Jalankan pembaruan lagi segera setelah koneksi Internet tersedia*** untuk memastikan bahwa jika koneksi Internet putus dan proses pembaruan gagal, maka ia akan diluncurkan lagi segera setelah koneksi Internet pulih. Setelah pembaruan terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela yang muncul di atas ikon baki sistem AVG (*asalkan Anda telah membiarkan konfigurasi default pada dialog Pengaturan Lanjutan/Tampilan*).

Catatan: *Jika terjadi konflik waktu antara pembaruan program terjadwal dan pemindaian terjadwal, maka proses pembaruan akan lebih diprioritaskan dan pemindaian akan disela.*

10.8.4. Jadwal Pembaruan Anti-Spam

Jika benar-benar perlu, Anda dapat mengosongkan item ***Aktifkan tugas ini*** untuk menonaktifkan pembaruan Anti-Spam yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Dalam dialog ini Anda dapat mengatur beberapa parameter terperinci atas jadwal pembaruan. Dalam bidang teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) ada nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Di sini, tetapkan interval waktu untuk jadwal baru peluncuran pembaruan Anti-Spam. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan Anti-Spam yang berulang setelah periode waktu tertentu (***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada waktu tertentu ...***), atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan (***Tindakan berdasar startup komputer***).

Opsi jadwal lanjutan

Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan Anti-Spam harus/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

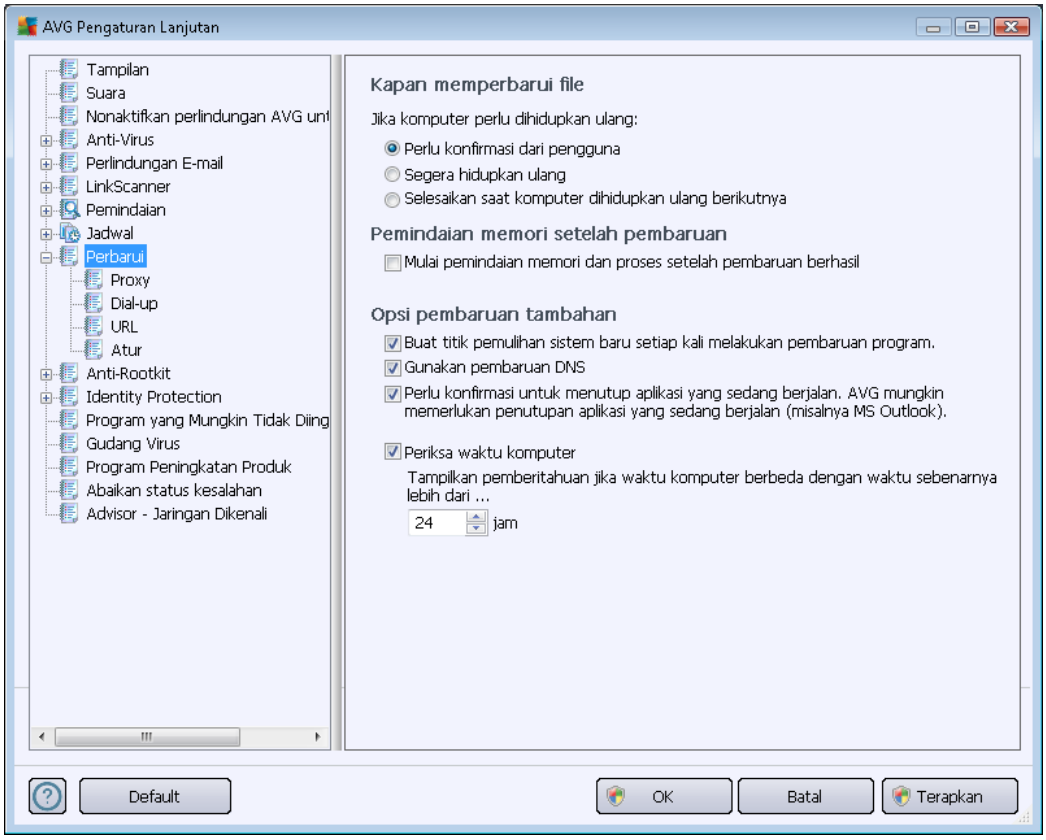
Pengaturan pembaruan lain

Tandai opsi ***Jalankan lagi pembaruan begitu koneksi Internet tersedia*** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan anti-spam gagal, ia akan segera diluncurkan lagi setelah koneksi Internet pulih.

Setelah pemindaian terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela yang muncul di atas ikon baki sistem AVG (*asalkan Anda membiarkan konfigurasi default pada dialog Pengaturan Lanjutan/Tampilan).*

10.9. Perbarui

Item navigasi ***Perbarui*** membuka dialog baru di mana Anda dapat menetapkan parameter umum yang menyangkut Pembaruan AVG:



Kapan memperbarui file

Di bagian ini, Anda dapat memilih dari tiga opsi alternatif yang akan digunakan jika proses pembaruan mengharuskan PC dihidupkan ulang. Penuntasan pembaruan dapat dijadwalkan saat PC dihidupkan ulang berikutnya, atau Anda dapat menghidupkan ulang segera:

- ***Minta konfirmasi dari pengguna*** *(secara default)* – Anda akan dimintai persetujuan untuk menghidupkan ulang PC yang diperlukan buat menuntaskan proses pembaruan

- ***Hidupkan ulang segera*** – secara otomatis komputer akan dihidupkan ulang segera setelah proses pembaruan selesai, dan persetujuan Anda tidak akan diperlukan

- ***Selesaikan saat komputer dihidupkan ulang berikutnya*** – penuntasan proses pembaruan akan ditunda hingga saat berikutnya komputer dihidupkan ulang. Harap diingat bahwa opsi ini hanya disarankan jika Anda yakin komputer akan dihidupkan ulang secara rutin, setidaknya sekali sehari!

Pemindaian memori setelah pembaruan

Centang kotak ini untuk menentukan bahwa Anda ingin meluncurkan pemindaian memori baru setelah setiap pembaruan yang berhasil selesai. Pembaruan yang terakhir diunduh dapat berisi definisi virus baru, dan definisi ini dapat segera diterapkan dalam pemindaian.

Opsi pembaruan tambahan

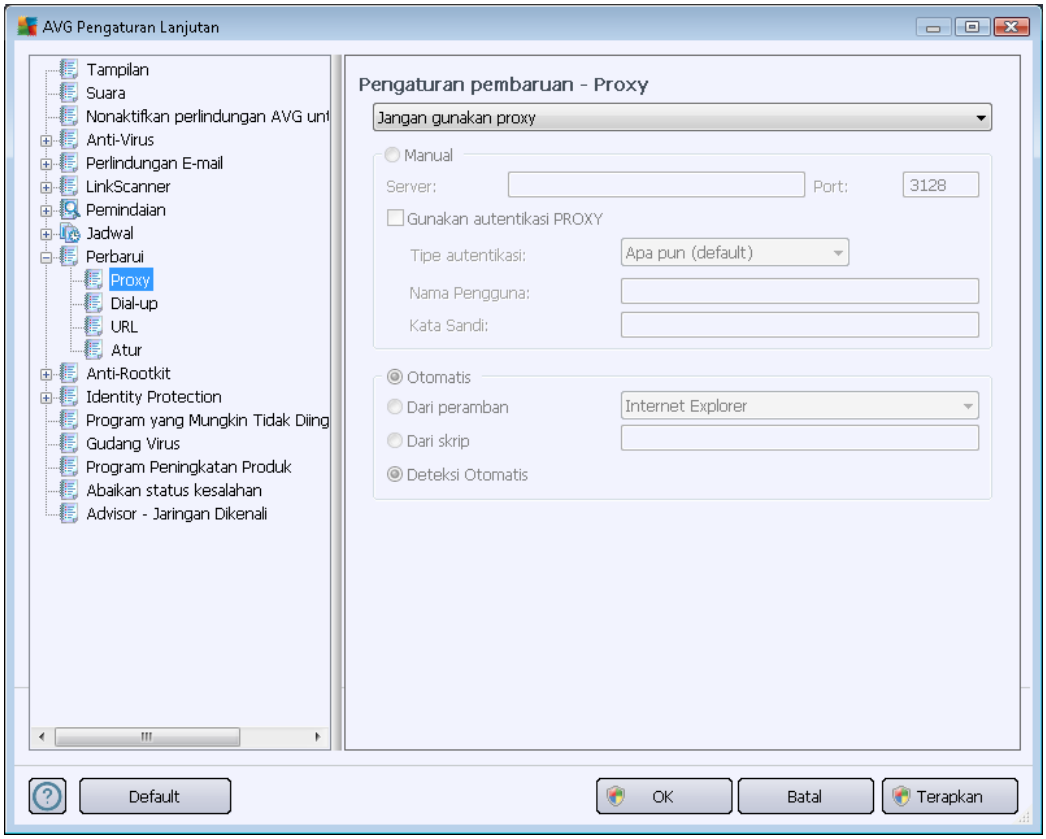
- ***Buat titik pemulihan sistem baru setiap kali melakukan pembaruan program*** – sebelum setiap peluncuran pembaruan program AVG, akan dibuat titik pemulihan sistem. Seandainya proses pembaruan gagal dan sistem operasi crash, Anda dapat memulihkan OS ke konfigurasi aslinya dari titik ini. Opsi ini dapat diakses melalui Start / All Programs / Accessories / System tools / System Restore, namun segala perubahan hanya disarankan untuk pengguna yang berpengalaman! Biarkan kotak ini dicentang jika Anda ingin menggunakan fungsionalitas ini.

- ***Gunakan pembaruan DNS*** (*diaktifkan secara default*) – bila item ini ditandai, setelah pembaruan diluncurkan, **Keamanan Intenet AVG 2012** akan mencari informasi tentang versi basis data virus terbaru dan versi program terbaru pada server DNS. Kemudian, hanya file pembaruan yang benar-benar diperlukan saja yang akan diunduh dan diterapkan. Dengan cara ini, total jumlah data yang diunduh akan diminimalkan, dan proses pembaruan berjalan lebih cepat.

- ***Minta konfirmasi sebelum menutup aplikasi yang berjalan*** (*diaktifkan secara default*) akan membantu Anda memastikan tidak ada penutupan aplikasi yang sedang berjalan tanpa seizin Anda – jika diperlukan untuk menuntaskan proses pembaruan.

- ***Periksa waktu komputer*** – tandai opsi ini untuk menyatakan Anda ingin pembaruan ditampilkan seandainya waktu komputer berbeda dengan waktu yang benar lebih dari jumlah jam yang ditetapkan.

10.9.1. Proxy



Server proxy adalah server mandiri atau layanan yang berjalan pada PC, yang menjamin koneksi ke Internet lebih aman. Sesuai aturan jaringan yang ditentukan, Anda nanti dapat mengakses Internet baik secara langsung atau melalui server proxy; keduanya juga dapat diperbolehkan sekaligus. Kemudian, dalam item pertama pada dialog ***Pengaturan pembaruan – Proxy*** Anda harus memilih dari menu kotak kombo apakah Anda ingin:

- ***Gunakan proxy***
- ***Jangan gunakan proxy*** – pengaturan default
- ***Cobalah koneksi menggunakan poxy dan jika gagal, hubungkan langsung***

Jika Anda memilih suatu opsi menggunakan server proxy, Anda nanti harus menentukan beberapa data lebih lanjut. Pengaturan server dapat dikonfigurasi secara manual atau secara otomatis.

Konfigurasi manual

Jika Anda memilih konfigurasi manual (tandai opsi ***Manual*** *untuk mengaktifkan bagian dialognya*) Anda harus menentukan item berikut:

- ***Server*** – menentukan alamat IP server atau nama server

- ***Port*** – menentukan nomor port yang memungkinkan akses Internet (*secara default, nomor ini diatur ke 3128 namun dapat diatur berbeda – jika Anda tidak yakin, hubungi administrator jaringan Anda*)

Server proxy juga dapat dikonfigurasi dengan aturan tertentu untuk setiap pengguna. Jika server proxy Anda telah diatur dengan cara ini, tandai opsi ***Gunakan autentikasi PROXY*** untuk memverifikasi bahwa nama pengguna dan kata sandi Anda sudah sah untuk menghubungkan ke Internet melalui server proxy.

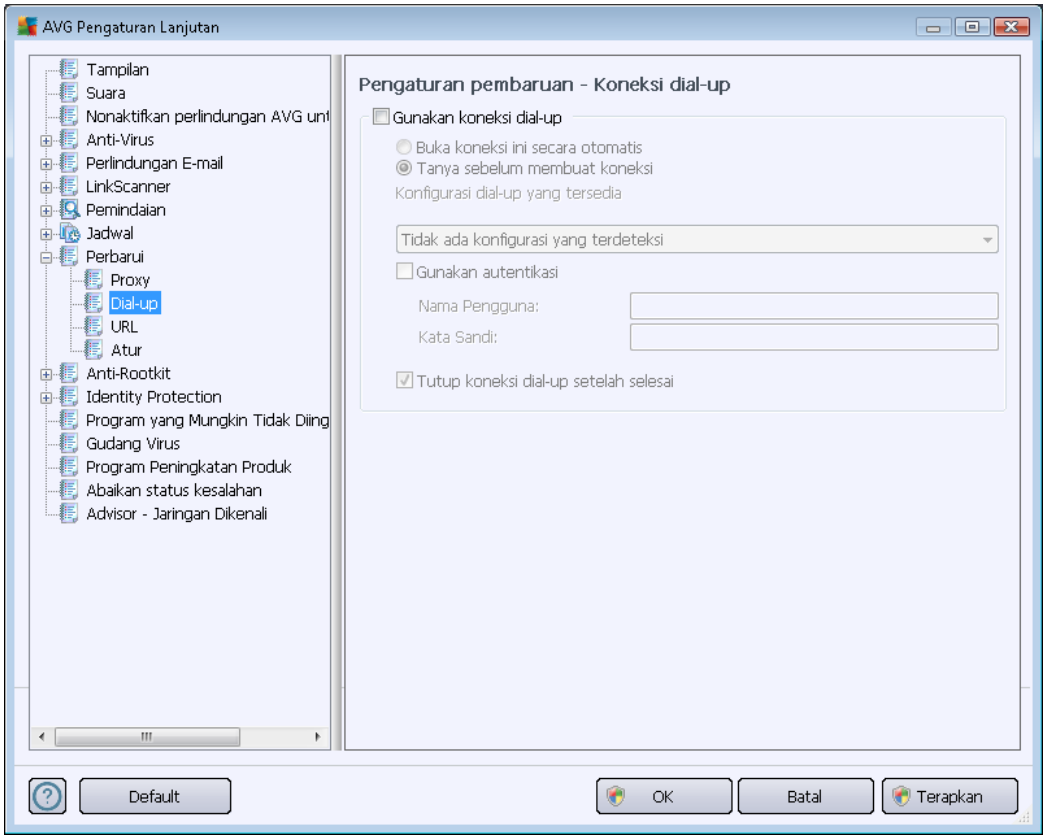
Konfigurasi otomatis

Jika Anda memilih konfigurasi otomatis (*centang opsi **Otomatis** untuk mengaktifkan bagian dialognya*) maka pilih dari mana konfigurasi proxy akan diambil:

- ***Dari peramban*** - konfigurasi akan dibaca dari peramban Internet default Anda
- ***Dari skrip*** – konfigurasi akan dibaca dari skrip yang telah diunduh dengan fungsi yang menghasilkan alamat proxy
- ***Deteksi otomatis*** – konfigurasi akan dideteksi secara otomatis, langsung dari server proxy

10.9.2. Dial-up

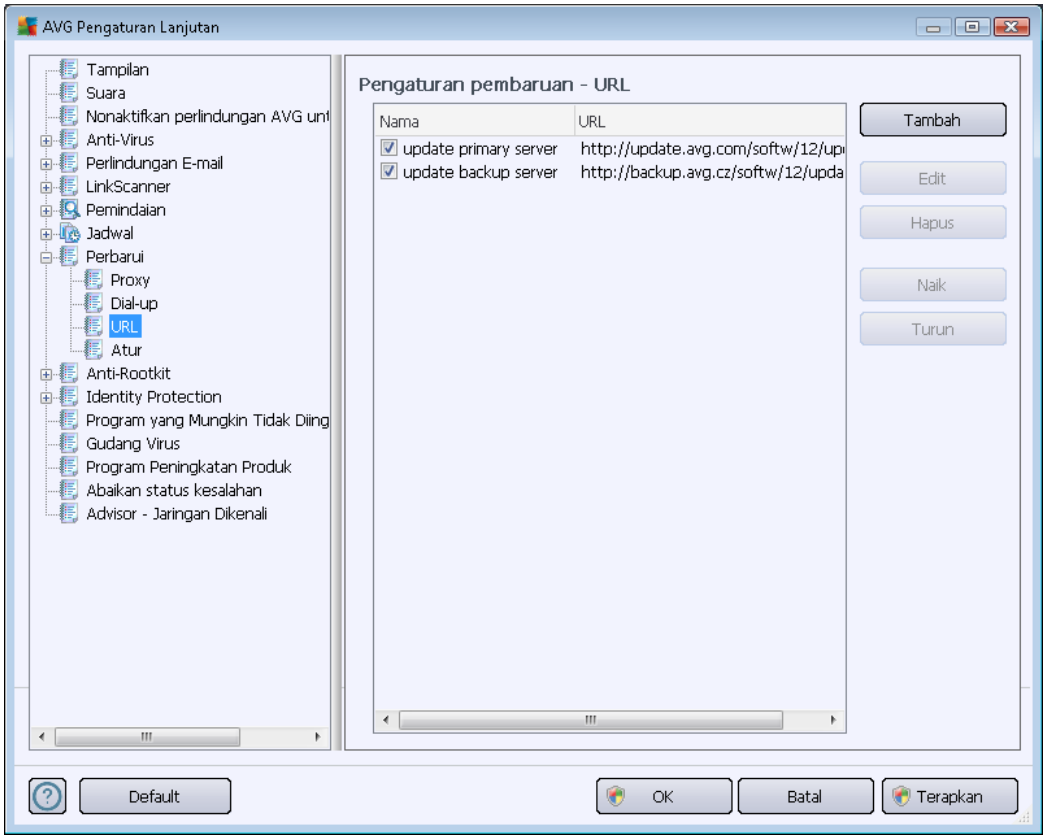
Semua parameter opsional yang ditentukan dalam dialog ***Perbarui pengaturan – Koneksi dial-up*** mengacu pada koneksi dial-up ke Internet. Bidang-bidang dialog tidak aktif hingga Anda menandai opsi ***Gunakan koneksi dial-up*** yang akan mengaktifkan bidang-bidang tersebut:



Tetapkan apakah Anda ingin menghubungkan ke Internet secara otomatis (***Buka koneksi ini secara otomatis***) atau Anda ingin mengonfirmasi setiap koneksi secara manual (***Tanya sebelum koneksi***). Untuk koneksi otomatis, Anda selanjutnya harus memilih apakah koneksi harus ditutup setelah pembaruan selesai (***Tutup koneksi dial-up bila selesai***).

10.9.3. URL

Dialog ***URL*** menyediakan daftar alamat Internet dari mana Anda dapat mengunduh file pembaruan:



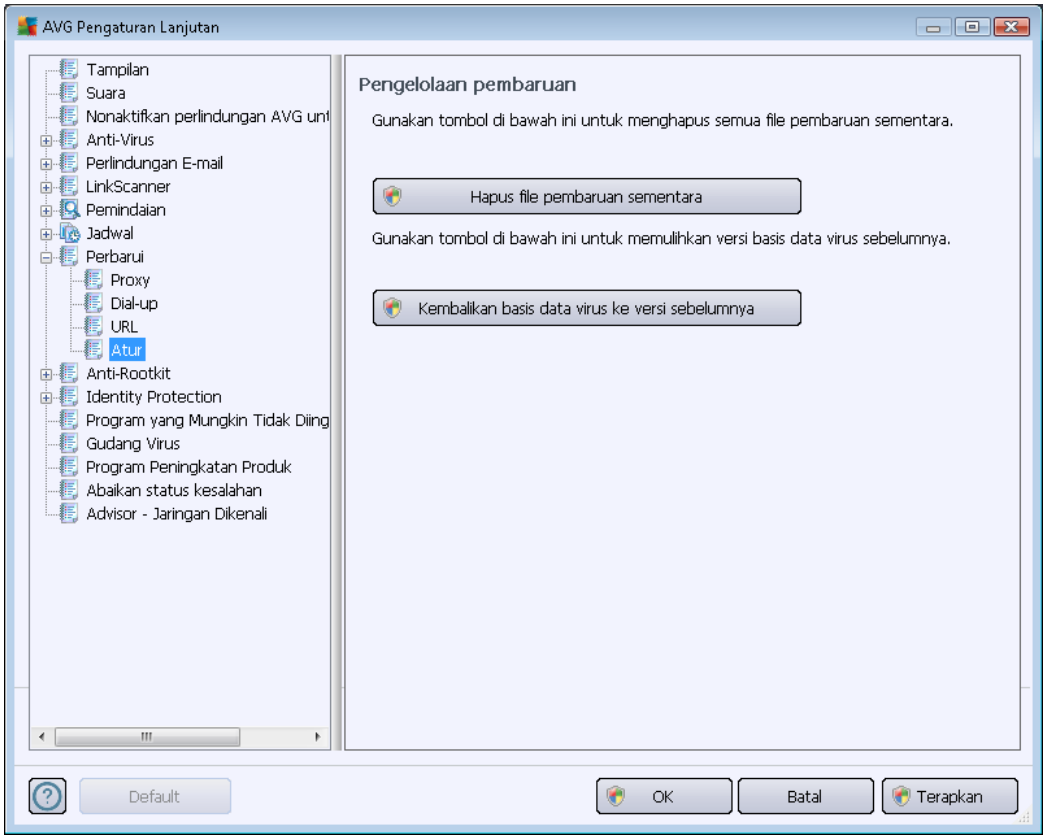
Tombol kontrol

Daftar ini dan itemnya dapat diubah dengan menggunakan tombol kontrol berikut:

- ***Tambah*** – membuka dialog di mana Anda dapat menetapkan URL baru untuk ditambahkan ke daftar
- ***Edit*** – membuka sebuah dialog di mana Anda dapat mengedit parameter URL yang dipilih
- ***Hapus*** – menghapus URL yang dipilih dari daftar
- ***Pindah ke Atas*** – memindah URL yang dipilih satu posisi ke atas dalam daftar
- ***Pindah ke Bawah*** – memindah URL yang dipilih satu posisi ke bawah dalam daftar

10.9.4. Atur

Dialog ***Manajemen pembaruan*** menyediakan dua opsi yang dapat diakses melalui dua tombol:

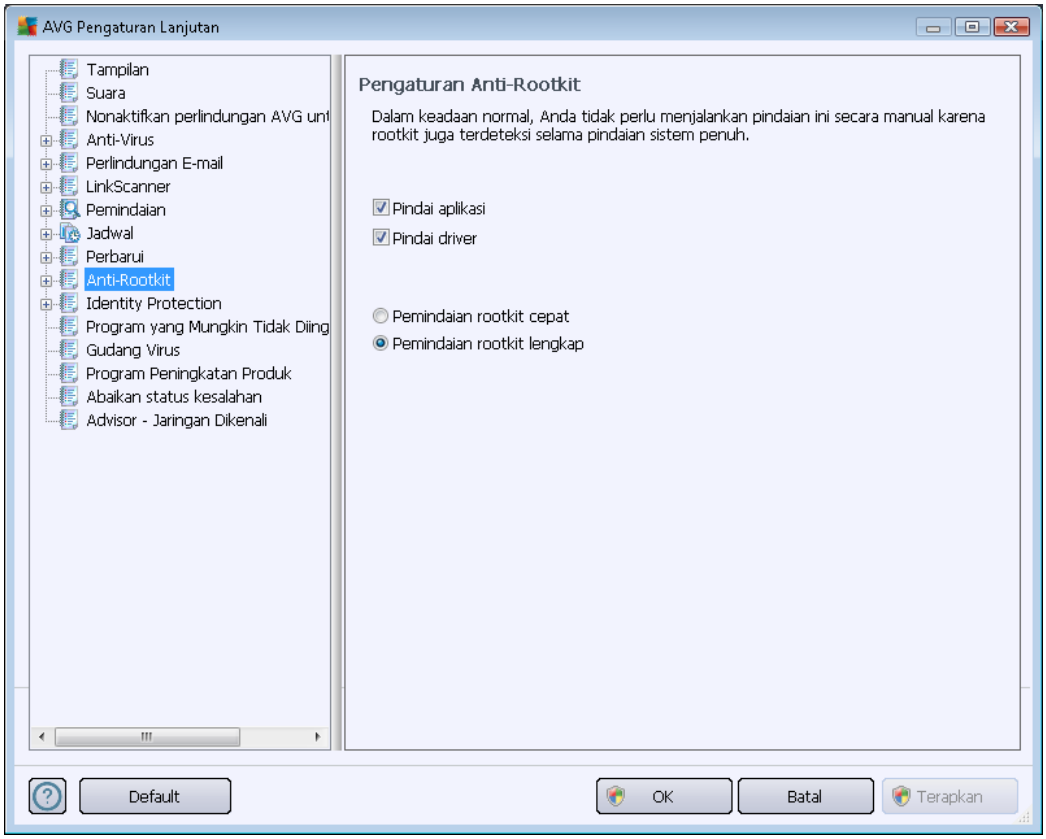


- ***Hapus file pembaruan sementara*** – tekan tombol ini untuk menghapus semua file pembaruan sementara dari hard disk Anda (*secara default, file ini akan tetap disimpan selama 30 hari*)

- ***Kembalikan basis data virus ke versi sebelumnya*** – tekan tombol ini untuk menghapus versi basis data virus terbaru dari hard disk Anda, dan mengembalikan ke versi yang telah disimpan sebelumnya (*versi basis data virus baru akan menjadi bagian dari pembaruan berikutnya*)

10.10. Anti-Rootkit

Dalam dialog ***pengaturan Anti-Rootkit*** Anda dapat mengedit konfigurasi dan parameter khusus komponen Anti-Rootkit pada pemindaian anti-rootkit. Pemindaian anti-rootkit adalah proses default yang telah disertakan dalam Pemindaian Seisi Komputer:



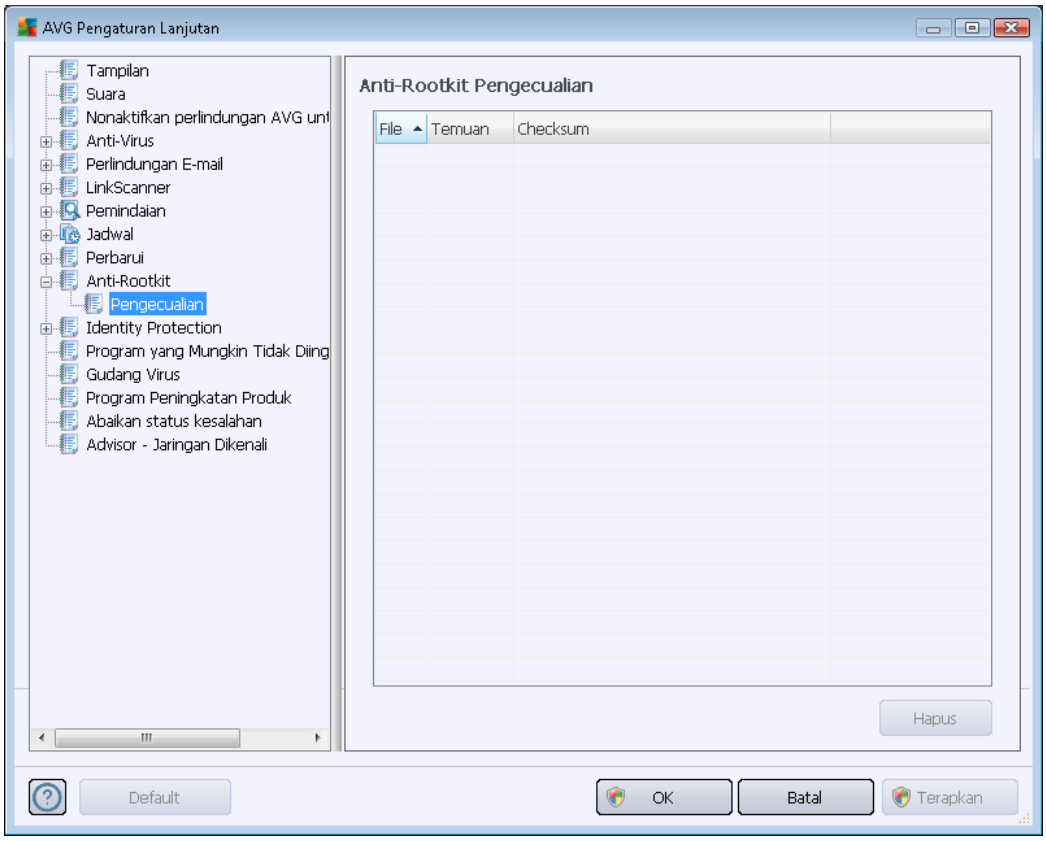
Pengeditan semua fungsi komponen Anti-Rootkit yang diberikan dalam dialog ini juga dapat diakses langsung dari antarmuka komponen Anti-Rootkit.

Pindai aplikasi dan ***Pindai driver*** memungkinkan Anda menetapkan secara terperinci apa yang harus disertakan dalam pemindaian anti-rootkit. Pengaturan ini ditujukan untuk pengguna mahir; kami sarankan untuk tetap mengaktifkan semua opsi. Selanjutnya Anda dapat memilih mode pemindaian rootkit:

- ***Pemindaian rootkit cepat*** – memindai semua proses yang berjalan, driver yang dimuat dan folder sistem (*biasanya c:\Windows*)
- ***Pemindaian rootkit lengkap*** – memindai semua proses yang berjalan, driver yang dimuat, folder sistem (*biasanya c:\Windows*), ditambah semua disk lokal (*termasuk flash-disk, namun tidak termasuk floppy-disk/drive CD*)

10.10.1. Pengecualian

Dalam dialog ***Pengecualian Anti-Rootkit*** Anda dapat menetapkan file tertentu *(misalnya beberapa driver yang mungkin salah dideteksi sebagai rootkit)* yang harus dikecualikan dari pemindaian ini:

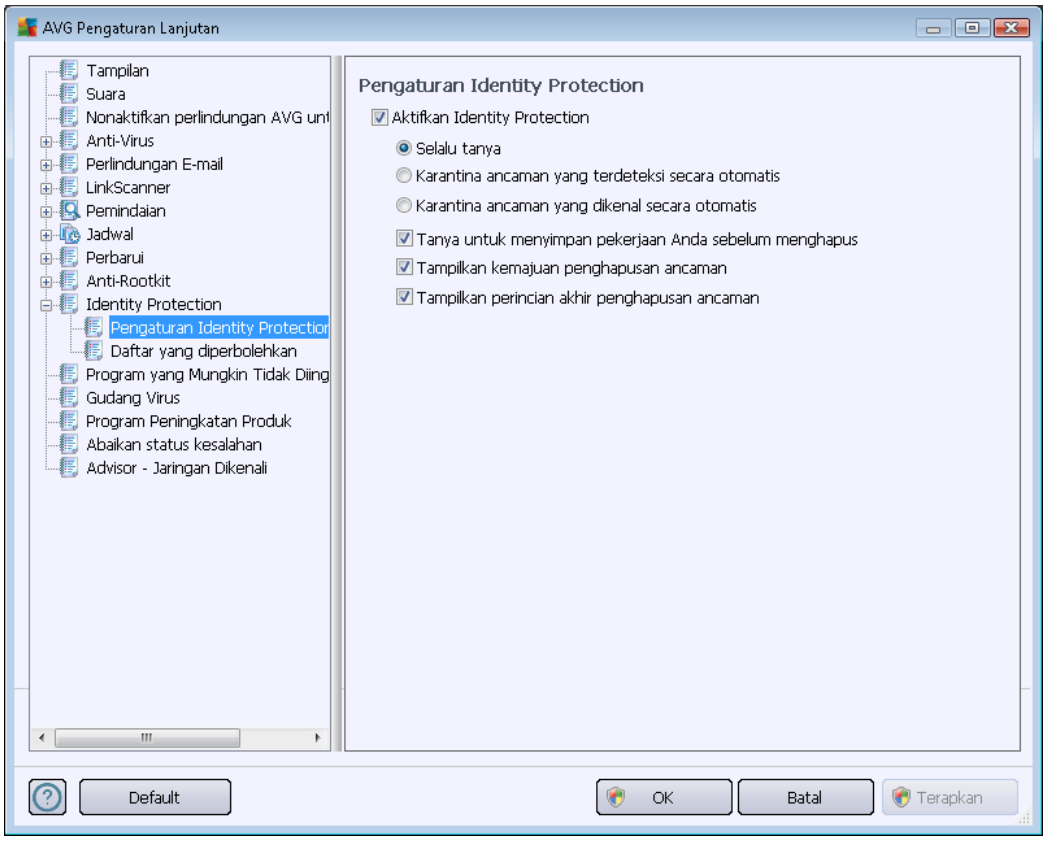


10.11. Identity Protection

Identity Protection adalah komponen anti-malware yang melindungi Anda dari semua jenis malware (*spyware, bot, pencurian identitas, ...*) menggunakan teknologi perilaku dan memberikan perlindungan setiap hari dari virus baru *(untuk penjelasan terperinci mengenai fungsionalitas komponen, lihat bab Identity Protection*).

10.11.1. Pengaturan Identity Protection

Dialog ***Pengaturan Identity Protection*** memungkinkan Anda mengaktifkan atau menonaktifkan fitur dasar komponen Identity Protection:



Aktifkan Identity Protection (*diaktifkan secara default*) – jangan centang untuk menonaktifkan komponen Identity Protection.

Kami sangat menyarankan agar Anda tidak melakukannya jika tidak perlu!

Bila Identity Protection diaktifkan, Anda dapat menetapkan apa yang dilakukan bila ancaman terdeteksi:

- ***Selalu tanya*** (*diaktifkan secara default*) - saat ancaman terdeteksi, Anda akan ditanyai apakah ia harus dipindahkan ke karantina untuk memastikan tidak terhapusnya aplikasi yang ingin Anda jalankan.
- ***Karantina ancaman yang terdeteksi secara otomatis*** – centang kotak ini untuk menentukan bahwa Anda ingin semua ancaman yang mungkin terdeteksi segera dipindahkan ke ruang aman di Gudang Virus. Dengan menyimpan pengaturan default, saat ancaman terdeteksi, Anda akan ditanyai apakah ancaman harus dipindahkan ke karantina untuk memastikan tidak terhapusnya aplikasi yang ingin Anda jalankan.
- ***Karantina ancaman yang dikenal secara otomatis*** – biarkan item ini ditandai jika Anda ingin agar semua aplikasi yang terdeteksi sebagai kemungkinan malware untuk dipindah

segera dan secara otomatis ke Gudang Virus.

Lebih lanjut Anda dapat menetapkan item tertentu untuk mengaktifkan fungsionalitas Identity Protection lainnya secara opsional:

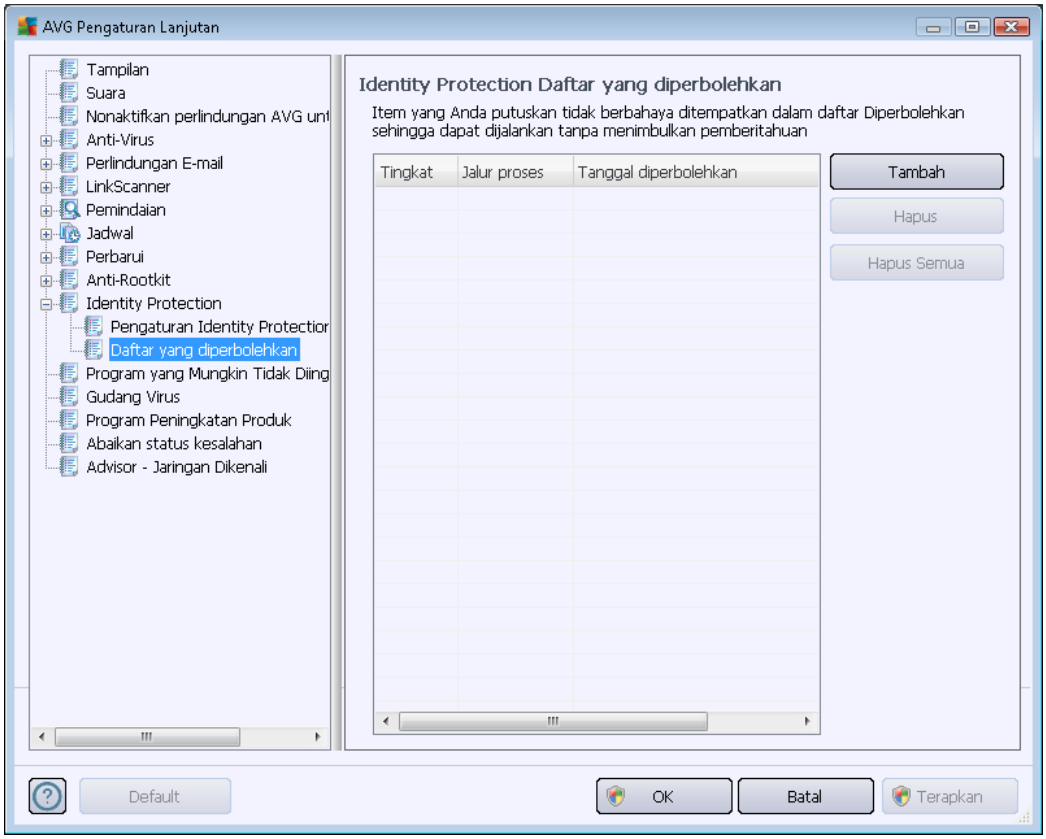
- ***Tanya untuk menyimpan pekerjaan Anda sebelum penghapusan*** - (*diaktifkan secara default*) – biarkan item ini dicentang jika Anda ingin diperingatkan sebelum aplikasi yang dideteksi sebagai kemungkinan malware dipindahkan ke karantina. Jika Anda sedang bekerja dengan aplikasi itu, pekerjaan Anda mungkin hilang dan Anda perlu menyimpannya dulu. Secara default, item ini diaktifkan dan kami sangat menyarankan untuk tetap membiarkannya.

- ***Tampilkan kemajuan penghapusan malware*** - (*diaktifkan secara default*) – dengan aktifnya item ini, saat potensi malware terdeteksi, dialog baru akan terbuka untuk menampilkan kemajuan pemindahan malware ke karantina.

- ***Tampilkan perincian akhir penghapusan ancaman*** - (*diaktifkan secara default*) – dengan aktifnya item ini, ***Identity Protection*** menampilkan informasi terperinci mengenai setiap objek yang dipindahkan ke karantina (*tingkat keseriusan, lokasi, dll.*).

10.11.2. Daftar yang Diperbolehkan

Jika dalam dialog ***Pengaturan Identity Protection*** Anda memutuskan untuk tidak menandai item ***Karantina ancaman yang terdeteksi secara otomatis***, setiap kali terdeteksi malware yang mungkin berbahaya, Anda akan ditanya apakah harus menghapusnya. Jika Anda kemudian menetapkan aplikasi yang mencurigakan ini (*terdeteksi berdasarkan perilakunya*) sebagai aman, dan Anda mengkonfirmasinya agar tetap disimpan di komputer Anda, aplikasi ini akan ditambahkan ke ***Daftar yang Diperbolehkan Identity Protection***, dan tidak akan dilaporkan lagi sebagai item yang mungkin berbahaya:



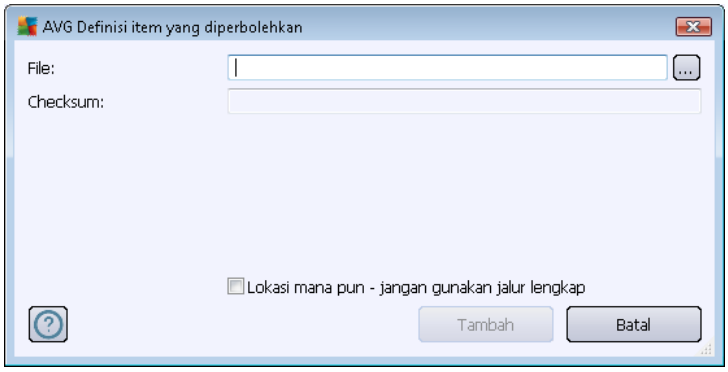
Daftar yang Diperbolehkan Identity Protection menyediakan informasi berikut mengenai setiap aplikasi:

- ***Tingkat*** – identifikasi grafis dari keseriusan proses yang bersangkutan pada skala empat-tingkat dari kurang penting (■□□□) hingga kritis (■■■■)
- ***Jalur proses*** - jalur ke aplikasi (*proses*) lokasi file eksekusi
- ***Tanggal yang diperbolehkan*** – tanggal saat Anda secara manual menetapkan aplikasi sebagai aman

Tombol kontrol

Tombol kontrol yang tersedia dalam dialog ***Daftar yang diperbolehkan Identity Protection*** adalah sebagai berikut:

- ***Tambah*** - tekan tombol ini untuk menambah aplikasi baru ke daftar yang diperbolehkan. Dialog berikut akan muncul:

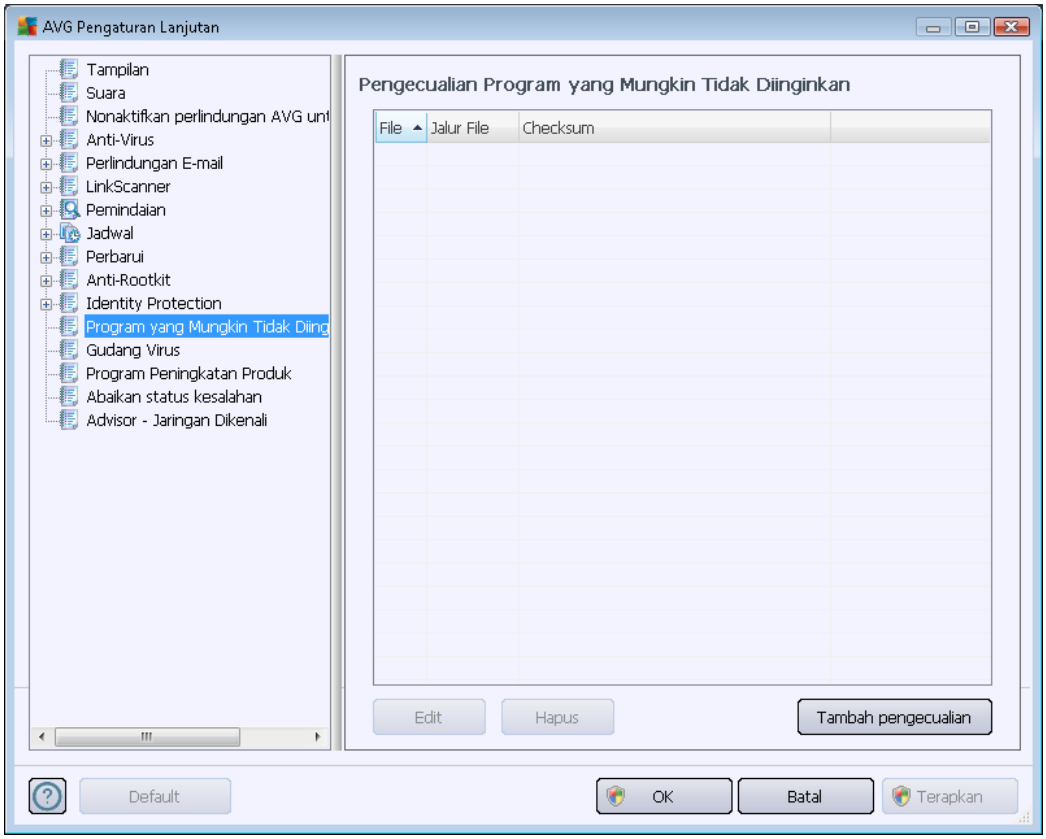


- ***File*** – ketikkan jalur lengkap ke file (*aplikasi*) yang ingin Anda tandai sebagai pengecualian
- ***Checksum*** – menampilkan 'tanda tangan' unik atas file yang dipilih. Checksum ini adalah string karakter yang dibuat secara otomatis, yang memungkinkan AVG dengan jelas membedakan file yang dipilih dari file lainnya. Checksum dibuat dan ditampilkan setelah penambahan file berhasil.
- ***Sembarang lokasi – jangan gunakan jalur lengkap*** – jika Anda ingin menetapkan file ini sebagai pengecualian hanya untuk lokasi tertentu, jangan tandai kotak ini

- ***Hapus*** - tekan untuk menghapus aplikasi yang dipilih dari daftar
- ***Hapus semua*** - tekan untuk menghapus semua aplikasi yang tercantum

10.12. Program yang Mungkin Tidak Diinginkan

Keamanan Intenet AVG 2012 dapat menganalisis dan mendeteksi aplikasi yang dapat dijalankan atau pustaka DLL yang mungkin tidak diinginkan dalam sistem. Dalam beberapa kasus, pengguna mungkin ingin membiarkan beberapa program yang tidak diinginkan di komputer (program yang sengaja diinstal). Beberapa program, khususnya yang gratisan, termasuk adware. Adware tersebut mungkin terdeteksi dan dilaporkan oleh **Keamanan Intenet AVG 2012** *sebagai program yang mungkin tidak diinginkan*. Jika Anda ingin membiarkan program tersebut pada komputer Anda, Anda dapat menetapkannya sebagai pengecualian program yang mungkin tidak diinginkan:



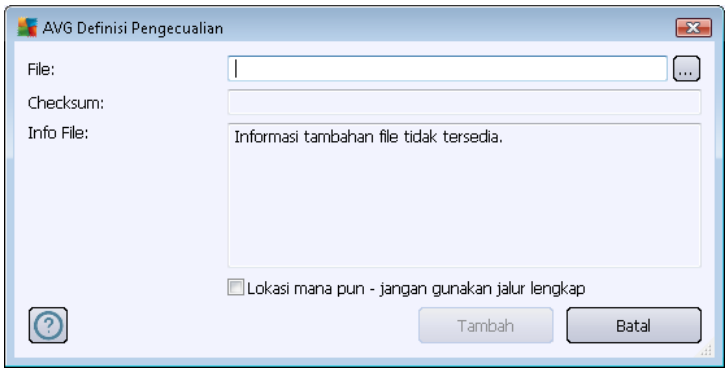
Dialog ***Pengecualian Program yang Mungkin Tidak Diinginkan*** menampilkan daftar pengecualian yang telah ditetapkan dan yang saat ini berlaku dari program yang mungkin tidak diinginkan. Anda dapat mengedit daftar ini, menghapus item yang ada, atau menambahkan pengecualian baru. Informasi berikut dapat ditemukan dalam daftar untuk setiap pengecualian baru:

- ***File*** – memberikan nama pasti dari aplikasi yang bersangkutan
- ***Jalur File*** - menunjukkan jalur menuju lokasi aplikasi.
- ***Checksum*** – menampilkan 'tanda tangan' unik atas file yang dipilih. Checksum ini adalah string karakter yang dibuat secara otomatis, yang memungkinkan AVG dengan jelas membedakan file yang dipilih dari file lainnya. Checksum dibuat dan ditampilkan setelah penambahan file berhasil.

Tombol kontrol

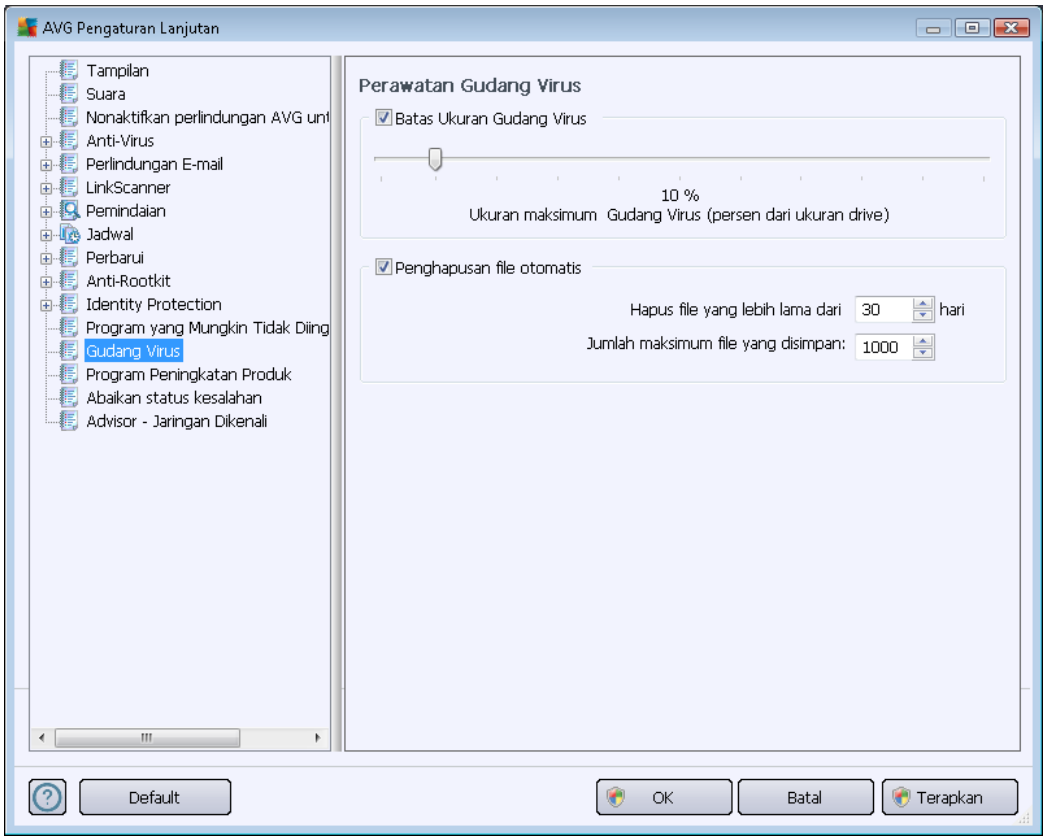
- ***Edit*** – membuka dialog pengeditan (*sama dengan dialog untuk penentuan pengecualian baru, lihat di bawah*) dari pengecualian yang sudah ditetapkan di mana Anda dapat mengubah parameter pengecualian
- ***Hapus*** - menghapus item yang dipilih dari daftar pengecualian
- ***Tambah pengecualian*** – membuka dialog pengeditan di mana Anda dapat menetapkan

parameter pengecualian baru yang akan dibuat:



- ***File*** – ketikkan jalur lengkap ke file yang ingin Anda tandai sebagai pengecualian
- ***Checksum*** – menampilkan 'tanda tangan' unik atas file yang dipilih. Checksum ini adalah string karakter yang dibuat secara otomatis, yang memungkinkan AVG dengan jelas membedakan file yang dipilih dari file lainnya. Checksum dibuat dan ditampilkan setelah penambahan file berhasil.
- ***Info File*** – menampilkan informasi tambahan tentang file *(lisensi/informasi versi, dsb.)*
- ***Sembarang lokasi – jangan gunakan jalur lengkap*** – jika Anda ingin menetapkan file ini sebagai pengecualian hanya untuk lokasi tertentu, jangan tandai kotak ini. Jika kotak centang ditandai, file yang ditentukan ditetapkan sebagai pengecualian di mana pun file itu berada *(walau demikian, Anda harus mengisi jalur lengkap ke file tersebut, file kemudian akan digunakan sebagai contoh unik untuk kemungkinan dua file dengan nama yang sama muncul di sistem Anda)*.

10.13. Gudang Virus



Dialog ***Perawatan Gudang Virus*** memungkinkan Anda menentukan beberapa parameter yang menyangkut administrasi berbagai objek yang tersimpan dalam Gudang Virus:

- ***Batasi ukuran Gudang Virus*** – Gunakan geseran untuk mengatur ukuran maksimum Gudang Virus. Ukuran ditetapkan secara proporsional, dibandingkan dengan ukuran disk lokal Anda.

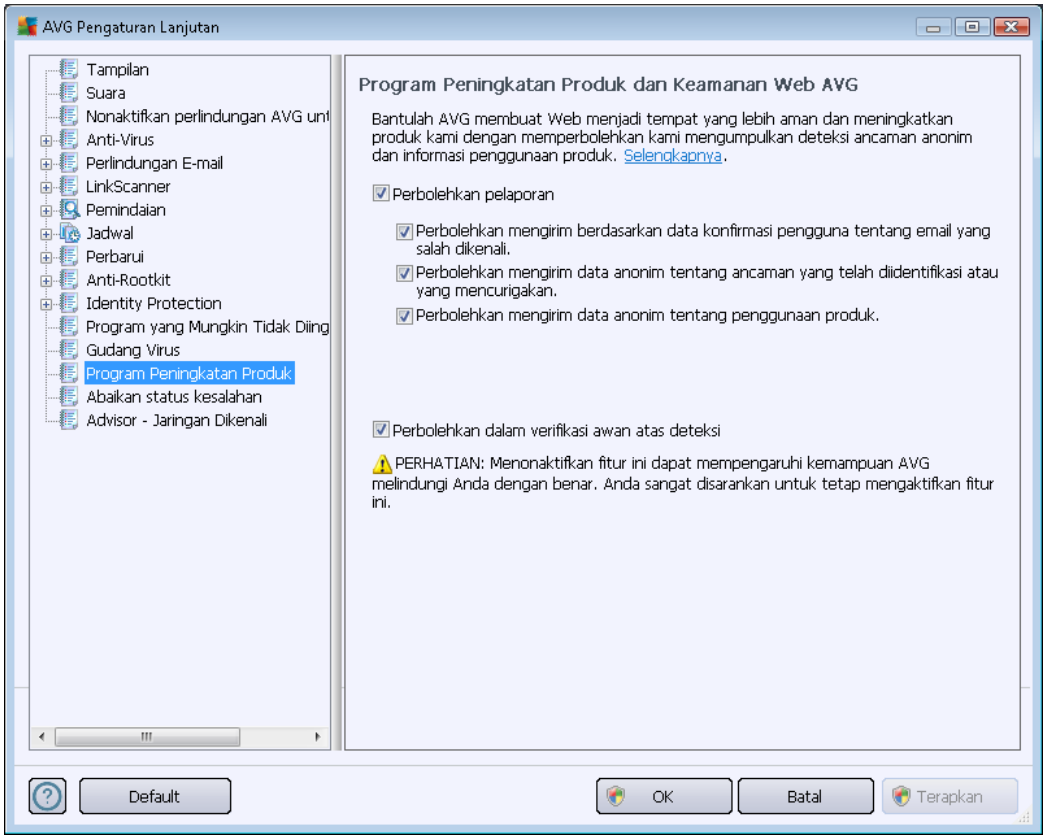
- ***Penghapusan file otomatis*** – Di bagian ini, tentukan lama maksimum untuk menyimpan objek dalam Gudang Virus (***Hapus file yang lebih lama dari ... hari***), dan jumlah maksimum file yang disimpan dalam Gudang Virus (***Jumlah maksimum file yang disimpan***).

10.14. Program Peningkatan Produk

Dialog ***Keamanan Web dan Program Peningkatan Produk AVG*** mengundang Anda untuk berpartisipasi dalam peningkatan produk AVG dan membantu kami meningkatkan tingkat keamanan Internet secara keseluruhan. Biarkan opsi ***Izinkan pelaporan*** tetap ditandai untuk memungkinkan pelaporan ancaman yang terdeteksi ke laboratorium AVG. Ini membantu kami mengumpulkan informasi mutakhir mengenai ancaman terbaru dari semua peserta di seluruh dunia, dan sebagai timbal baliknya kami dapat menyempurnakan perlindungan bagi semua orang.

Pelaporan ini dilakukan secara otomatis, sehingga tidak mengganggu kenyamanan Anda.

Tidak ada data pribadi yang disertakan dalam laporan tersebut. Pelaporan ancaman yang terdeteksi bersifat opsional, walau demikian, kami minta Anda membiarkan opsi ini diaktifkan. Ini akan membantu kami meningkatkan perlindungan untuk Anda dan pengguna AVG lainnya.



Dalam dialog, opsi pengaturan berikut ini tersedia:

- ***Perbolehkan pelaporan*** *(diaktifkan secara default)* - Jika Anda ingin membantu kami meningkatkan lebih lanjut **Keamanan Intenet AVG 2012**, tetap tandai kotak centang. Ini akan mengaktifkan pelaporan semua ancaman yang ditemukan ke AVG, sehingga kami dapat mengumpulkan informasi terbaru mengenai malware dari semua peserta di seluruh dunia, dan dengan demikian dapat meningkatkan perlindungan bagi siapa saja. Pelaporan ini dilakukan secara otomatis, sehingga tidak mengganggu kenyamanan Anda, dan tidak ada data pribadi yang disertakan dalam laporan tersebut.
    - ***Perbolehkan mengirim menurut data konfirmasi pengguna tentang email yang salah diidentifikasi*** *(diaktifkan secara default)* – mengirim informasi tentang pesan email yang salah diidentifikasi sebagai spam atau tentang pesan spam yang tidak terdeteksi oleh komponen Anti-Spam. Saat mengirim jenis informasi ini, Anda akan diminta konfirmasi.
    - ***Perbolehkan mengirim data anonim tentang ancaman yang dikenali atau dicurigai*** *(diaktifkan secara default)* – mengirim informasi tentang kode atau pola perilaku yang positif berbahaya atau mencurigakan *(boleh jadi berupa virus, spyware, atau halaman Web jahat yang coba Anda akses)* yang terdeteksi pada komputer

Anda.

- ***Perbolehkan mengirim data anonim tentang penggunaan produk*** *(diaktifkan secara default)* – mengirim statistik dasar tentang penggunaan aplikasi, seperti jumlah deteksi, pemindaian yang diluncurkan, pembaruan berhasil atau tidak berhasil, dsb.

- ***Perbolehkan di verifikasi awan atas deteksi*** *(diaktifkan secara default)* – ancaman yang terdeteksi akan diperiksa apakah benar-benar terinfeksi untuk memilah peringatan palsu.

Ancaman yang paling umum

Saat ini, ada lebih banyak ancaman di luar sana dari sekedar virus biasa. Pembuat program dan situs Web berbahaya sangat inovatif, dan berbagai bentuk ancaman baru cukup sering timbul, sebagian besar muncul di Internet. Berikut ini beberapa yang paling umum:

- ***Virus*** adalah kode jahat yang menyalin dan menyebarkan diri, sering tanpa diketahui hingga terjadi kerusakan. Virus tertentu merupakan ancaman serius, menghapus atau dengan sengaja mengubah file yang ditemuinya, sementara virus lain dapat melakukan sesuatu yang terkesan tidak berbahaya, seperti memutar musik tertentu. Namun, semua virus adalah berbahaya karena sifat dasarnya yang dapat menggandakan diri – bahkan virus yang sederhana dapat memenuhi memori komputer dalam seketika, dan menyebabkan kemacetan.

- ***Worm*** adalah subkategori virus yang, tidak seperti virus biasa, tidak memerlukan objek "pembawa" untuk ditempeli; worm mengirim dirinya sendiri ke komputer lain, biasanya melalui e-mail, dan akibatnya sering membebani server e-mail dan sistem jaringan secara berlebihan.

- ***Spyware*** biasanya ditetapkan dalam kategori malware (*malware = semua perangkat lunak jahat/perusak, termasuk virus*) yang meliputi program – umumnya kuda Troya – yang bertujuan mencuri informasi pribadi, kata sandi, nomor kartu kredit, atau menembus komputer dan memungkinkan penyerang untuk mengontrolnya dari jauh; tentu saja, semua itu tanpa sepengetahuan atau seizin pengguna.

- ***Program yang Mungkin Tidak Diinginkan*** adalah tipe spyware yang mungkin, meski tidak selalu, berbahaya bagi komputer Anda. Contoh spesifik PUP adalah adware, perangkat lunak yang dirancang untuk menyebarkan iklan, biasanya dengan menampilkan iklan pop-up yang mengganggu, tetapi tidak membahayakan.

- ***Cookie pelacak*** juga dapat dianggap sebagai sejenis spyware, karena file kecil ini, yang disimpan di peramban Web dan dikirimkan secara otomatis ke situs Web "induk" setiap kali Anda mengunjunginya lagi, dapat berisi data seperti riwayat penjelajahan dan informasi yang serupa lainnya.

- ***Exploit*** adalah kode berbahaya yang memanfaatkan kesalahan atau kelemahan sistem operasi, peramban Internet, atau program baku lainnya

- ***Phishing*** adalah upaya untuk mendapatkan data pribadi yang sensitif dengan meniru organisasi yang terpercaya dan dikenal. Biasanya, calon korban dihubungi melalui e-mail

massal yang meminta mereka, misalnya, memperbarui informasi rekening bank. Untuk melakukannya, korban diundang untuk mengikuti tautan yang diberikan yang mengarah ke situs Web palsu bank tersebut.

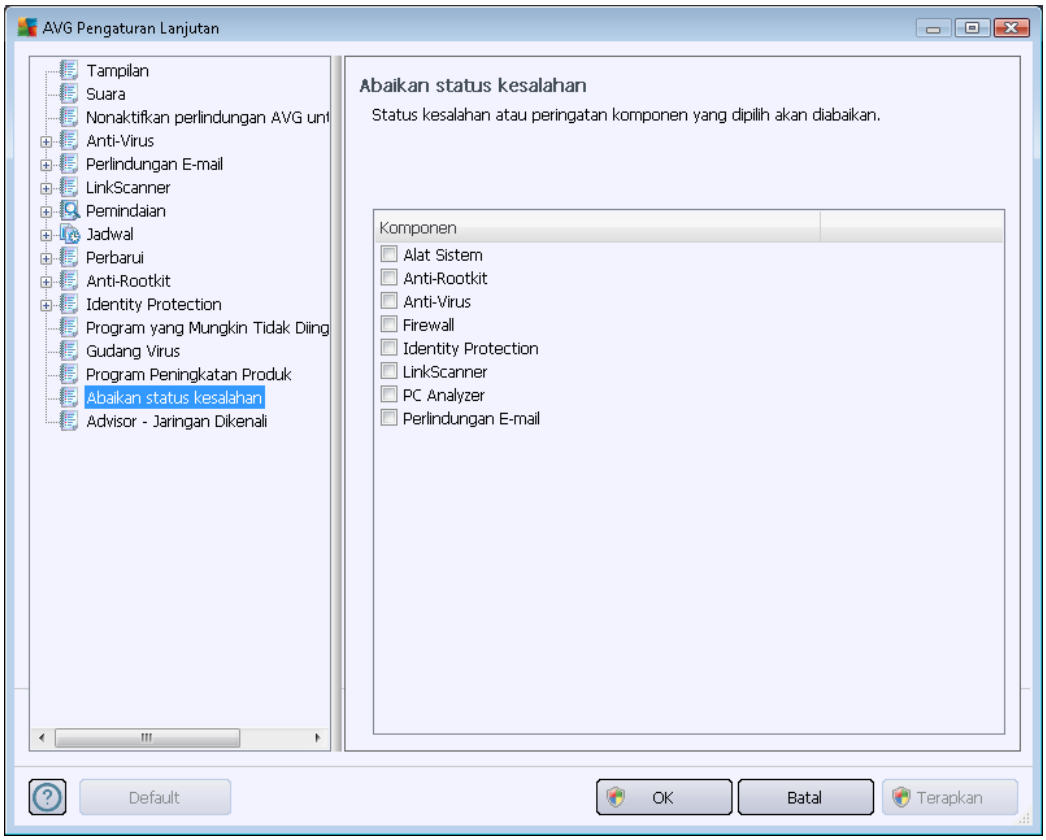
- ***Hoax*** (berita palsu) adalah e-mail massal yang berisi informasi berbahaya, mengkhawatirkan, atau hanya mengganggu dan tidak berguna sama sekali. Banyak ancaman di atas yang menggunakan pesan e-mail hoax untuk menyebarkannya.

- ***Situs Web berbahaya*** adalah situs Web yang dengan sengaja menginstal perangkat lunak berbahaya pada komputer Anda, dan situs yang diretas melakukan hal yang sama, hanya sebenarnya situs ini adalah situs resmi yang telah diretas oleh pengunjung yang menularkan infeksi.

Untuk melindungi Anda dari semua jenis ancaman ini, Keamanan Intenet AVG 2012 dilengkapi dengan komponen khusus: Untuk keterangan singkat mengenai hal ini, lihat bab Tinjauan Umum Komponen.

10.15. Abaikan status kesalahan

Dalam dialog ***Abaikan status kesalahan***, Anda dapat menandai komponen-komponen yang tidak perlu diberitahukan kepada Anda:



Secara default, tidak ada komponen yang dipilih dalam daftar ini. Berarti jika ada komponen yang sedang dalam status kesalahan, Anda akan segera diberitahu melalui:

- ikon baki sistem – saat semua bagian AVG bekerja dengan benar, ikon-ikonnya ditampilkan dalam empat warna; walau demikian, jika terjadi kesalahan, ikon akan tampak bersama tanda seru berwarna kuning,

- keterangan teks mengenai masalah yang ada di bagian Info Status Keamanan pada jendela utama AVG

Mungkin ada situasi di mana karena suatu alasan Anda perlu menonaktifkan komponen untuk sementara (*hal ini tidak disarankan, Anda harus tetap mengaktifkan semua komponen selamanya dan dalam konfigurasi default, namun hal ini mungkin saja terjadi*). Dalam hal itu, ikon baki sistem secara otomatis melaporkan status kesalahan komponen tersebut. Walau demikian, dalam hal ini kita tidak dapat membicarakan tentang kesalahan sebenarnya karena Anda sengaja melakukannya, dan Anda mengetahui akan potensi risikonya. Di saat yang sama, saat ditampilkan dalam warna abu-abu, ikon tersebut tidak dapat melaporkan dengan sebenarnya segala kemungkinan kesalahan lebih lanjut yang mungkin muncul.

Untuk situasi ini, dalam dialog di atas Anda dapat memilih komponen yang mungkin sedang mengalami kesalahan (*atau telah dinonaktifkan*) dan Anda tidak ingin diberitahu mengenai hal tersebut. Opsi yang sama *(Abaikan status komponen)* juga tersedia secara langsung untuk beberapa komponen tertentu dari tinjauan umum komponen dalam jendela utama AVG.

10.16. Advisor – Jaringan Dikenali

AVG Advisor memiliki fitur yang memantau jaringan yang terhubung dengan Anda, dan jika jaringan baru ditemukan *(dengan nama jaringan yang sudah digunakan, yang dapat menyebabkan kekacauan),* Anda akan diberi tahu dan disarankan untuk memeriksa keamanan jaringan. Jika Anda memutuskan bahwa jaringan baru yang akan terhubung dengan Anda aman, Anda juga dapat menyimpannya ke daftar ini; AVG Advisor kemudian akan mengingat atribut unik dari jaringan tersebut *(terutama alamat MAC)*, dan tidak akan menampilkan pemberitahuan di lain waktu.

Dalam jendela dialog ini, Anda dapat menandai mana jaringan yang sebelumnya telah Anda simpan sebagai jaringan dikenal. Anda dapat menghapus masing-masing entri dengan menekan tombol ***Hapus***; masing-masing jaringan tersebut kemudian akan dianggap tidak dikenal dan berpotensi tidak aman lagi.

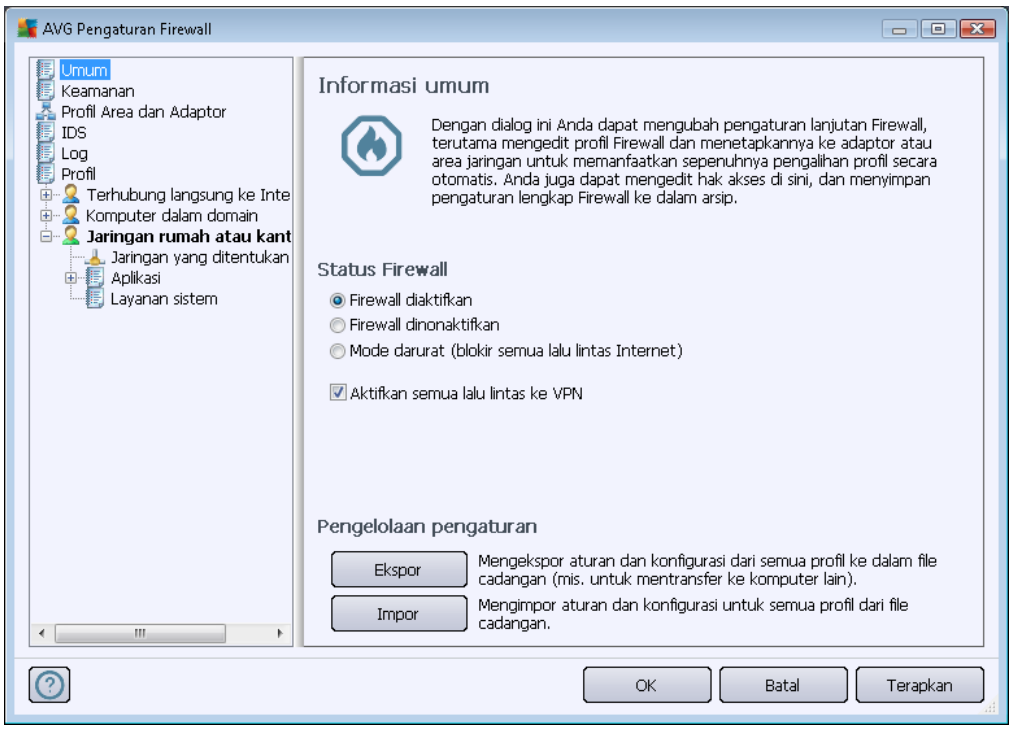
11. Pengaturan Firewall

Konfigurasi Firewall akan dibuka dalam jendela baru berisi sejumlah dialog di mana Anda dapat mengatur parameter lebih lanjut dari komponen tersebut.

Walau demikian, vendor perangkat lunak telah mengatur semua komponen Keamanan Intenet AVG 2012 untuk memberikan performa optimal. Jika Anda tidak memiliki alasan kuat untuk melakukannya, jangan ubah konfigurasi default. Semua perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman!

11.1. Umum

Dialog ***Informasi umum*** terbagi dalam 2 bagian:



Status Firewall

Pada bagian ***status Firewall*** Anda dapat mengubah status Firewall sesuai peningkatan kebutuhan:

- ***Firewall diaktifkan*** – pilih opsi ini untuk memperbolehkan komunikasi ke berbagai aplikasi yang ditetapkan sebagai 'diperbolehkan' dalam kumpulan aturan yang telah ditentukan dalam profil Firewall yang dipilih.
- ***Firewall dinonaktifkan*** – opsi ini akan menonaktifkan Firewall sama sekali, semua lalu lintas jaringan diperbolehkan namun tidak diperiksa!
- ***Mode darurat (memblokir semua lalu lintas Internet)*** – pilih opsi ini untuk memblokir

semua lalu lintas pada setiap port jaringan tunggal; Firewall tetap berjalan namun semua lalu lintas jaringan dihentikan.

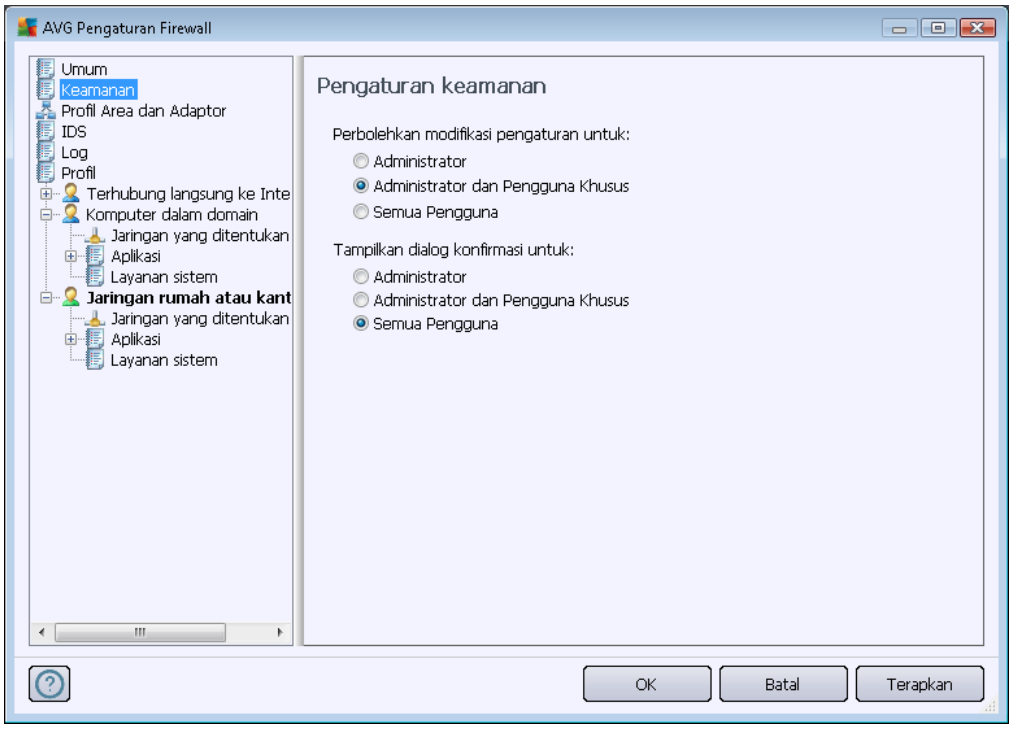
- ***Aktifkan semua lalu lintas ke VPN*** *(diaktifkan secara default)* – jika Anda menggunakan koneksi VPN *(Virtual Private Network)*, misalnya untuk menghubungkan ke kantor dari rumah, kami sarankan menandai kotak ini. ***AVG Firewall*** secara otomatis akan mencari ke seluruh adapter jaringan Anda, menemukan adapter yang digunakan untuk koneksi VPN, dan memperbolehkan semua aplikasi menghubungkan ke jaringan target *(hanya berlaku untuk aplikasi yang belum ditetapkan ke aturan Firewall tertentu)*. Pada sistem standar dengan adapter jaringan umum, langkah sederhana ini akan menghindarkan Anda dari keharusan mengatur aturan terperinci untuk setiap aplikasi yang perlu Anda gunakan melalui VPN.

Catatan: *Untuk mengaktifkan koneksi VPN, Anda perlu memperbolehkan komunikasi ke protokol sistem berikut: GRE, ESP, L2TP, PPTP. Ini dapat dilakukan dalam dialog Layanan sistem.*

Manajemen pengaturan

Di bagian ***Manajemen pengaturan*** Anda dapat ***Ekspor*** atau ***Import*** konfigurasi Firewall; misalnya mengekspor aturan dan pengaturan Firewall ke file cadangan, atau dengan kata lain mengimpor seisi file cadangan.

11.2. Keamanan



Dalam dialog ***Pengaturan keamanan*** Anda dapat menentukan aturan umum cara kerja Firewall, apa

pun profil yang dipilih:

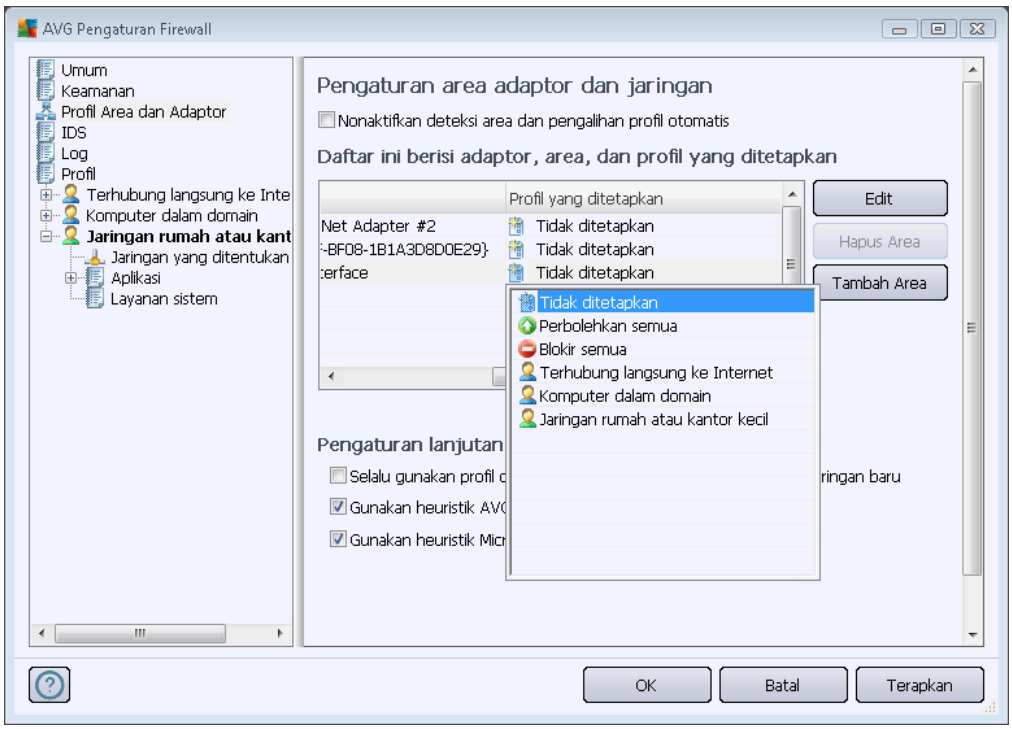
- ***Izinkan modifikasi pengaturan pada*** – menetapkan siapa yang diperbolehkan mengubah konfigurasi Firewall.
- ***Tampilkan dialog konfirmasi untuk*** – menetapkan kepada siapa dialog konfirmasi (*dialog yang menanyakan keputusan dalam situasi yang tidak tercakup oleh aturan Firewall yang telah ditentukan*) harus ditampilkan.

Dalam kedua kasus, Anda dapat menetapkan hak tertentu ke salah satu dari beberapa grup pengguna berikut:

- ***Administrator*** – mengontrol PC sepenuhnya dan berhak menetapkan setiap pengguna ke berbagai grup dengan kewenangan yang telah ditentukan secara spesifik.
- ***Administrator dan Pengguna Khusus*** – administrator dapat menetapkan pengguna ke grup tertentu (*Pengguna Khusus*) dan menentukan kewenangan anggota grup.
- ***Semua Pengguna*** – pengguna yang tidak ditetapkan ke grup tertentu.

11.3. Profil Area dan Adaptor

Dalam dialog ***Pengaturan area jaringan dan adapter***, Anda dapat mengedit pengaturan yang berhubungan dengan penetapan profil yang telah ditentukan ke adapter tertentu dan jaringan yang bersangkutan:



- ***Nonaktifkan deteksi area dan alih profil otomatis*** *(dinonaktifkan secara default)* – Salah satu profil yang ditentukan dapat diberikan ke setiap tipe antarmuka jaringan, sesuai masing-masing area. Jika Anda tidak ingin menentukan profil tertentu, akan digunakan satu profil umum. Walau demikian, jika Anda memutuskan untuk membedakan berbagai profil dan menetapkannya ke berbagai adapter dan area spesifik, dan kemudian – karena beberapa alasan – Anda ingin mengubah pengaturan ini untuk sementara, centang opsi ***Nonaktifkan deteksi area dan alih profil otomatis***.

- ***Tampilkan daftar adapter, area dan profil yang ditetapkan*** – Dalam daftar ini Anda dapat menemukan tinjauan umum berbagai adapter dan area yang terdeteksi. Untuk masing-masing, Anda dapat menetapkan profil tertentu dari menu profil yang ditentukan. Untuk membuka menu ini, klik kiri item yang bersangkutan dalam daftar adapter *(dalam kolom profil yang Ditetapkan)*, dan pilih profil dari menu konteks.

Pengaturan lanjutan

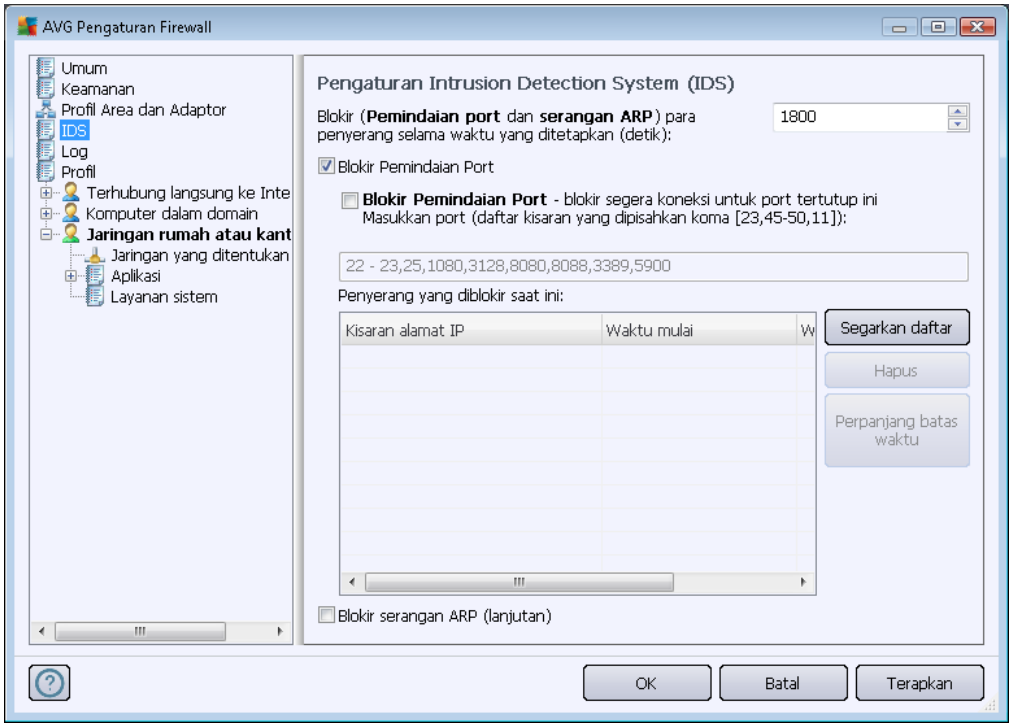
  - ***Selalu gunakan profil default dan jangan tampilkan dialog deteksi jaringan baru*** – Bila komputer Anda menghubungkan ke jaringan baru, Firewall akan memberi tahu Anda dan menampilkan dialog yang meminta Anda memilih tipe koneksi jaringan, dan menetapkan profil Firewall. Jika Anda tidak ingin dialog tersebut ditampilkan, tandai kotak ini.

  - ***Gunakan heuristik AVG untuk deteksi jaringan baru*** – Memungkinkan pengumpulan informasi tentang jaringan yang baru terdeteksi dengan mekanisme AVG sendiri (*walau demikian, opsi ini hanya tersedia pada OS VISTA, dan yang lebih tinggi*).

  - ***Gunakan heuristik Microsoft untuk deteksi jaringan baru*** – Memungkinkan pengambilan informasi tentang jaringan yang baru terdeteksi dari layanan Windows (*opsi ini hanya tersedia pada Windows Vista dan yang lebih tinggi*).

11.4. IDS

Intrusion Detection System adalah fitur analisis perilaku khusus yang dirancang untuk mengenali dan memblokir upaya komunikasi mencurigakan yang mencoba menggunakan port tertentu pada komputer Anda. Anda dapat mengkonfigurasi parameter IDS dalam dialog ***Pengaturan Intrusion Detections System (IDS)***:



Dialog pengaturan ***Intrusion Detection System (IDS)*** menawarkan opsi konfigurasi berikut:

- ***Blokir (Pemindaian port dan serangan ARP) penyerang selama waktu yang ditetapkan*** – Di sini Anda dapat menetapkan berapa detik harus mengunci port, bila terdeteksi upaya komunikasi yang mencurigakan pada port tersebut. Secara default, interval waktu ditentukan pada 1800 detik (*30 menit*).

- ***Blokir Pemindaian Port*** *(diaktifkan secara default)* – tandai kotak ini untuk memblokir upaya komunikasi pada semua port TCP dan UDP yang masuk ke komputer dari luar. Untuk koneksi seperti itu, lima upaya diperbolehkan, dan upaya ke enam diblokir. Item diaktifkan secara default, dan disarankan untuk membiarkan pengaturan ini. Jika Anda tetap mengaktifkan opsi ***Blokir Pemindaian Port***, maka tersedia beberapa konfigurasi yang lebih terperinci *(jika tidak, item berikut akan dinonaktifkan)*:

    - ***Blokir Pemindaian Port*** – Tandai kotak ini untuk segera memblokir semua upaya komunikasi pada port yang ditentukan dalam bidang teks di bawah ini. Masing-masing port atau kisaran port harus dipisah dengan koma. Ada daftar port disarankan yang telah ditentukan jika Anda ingin menggunakan fitur ini.

    - Penyerang yang diblokir saat ini – Bagian ini mencantumkan semua upaya komunikasi yang saat ini sedang diblokir oleh Firewall. Riwayat lengkap upaya yang diblokir dapat dilihat dalam dialog Log (*tab Log pemindaian port*).

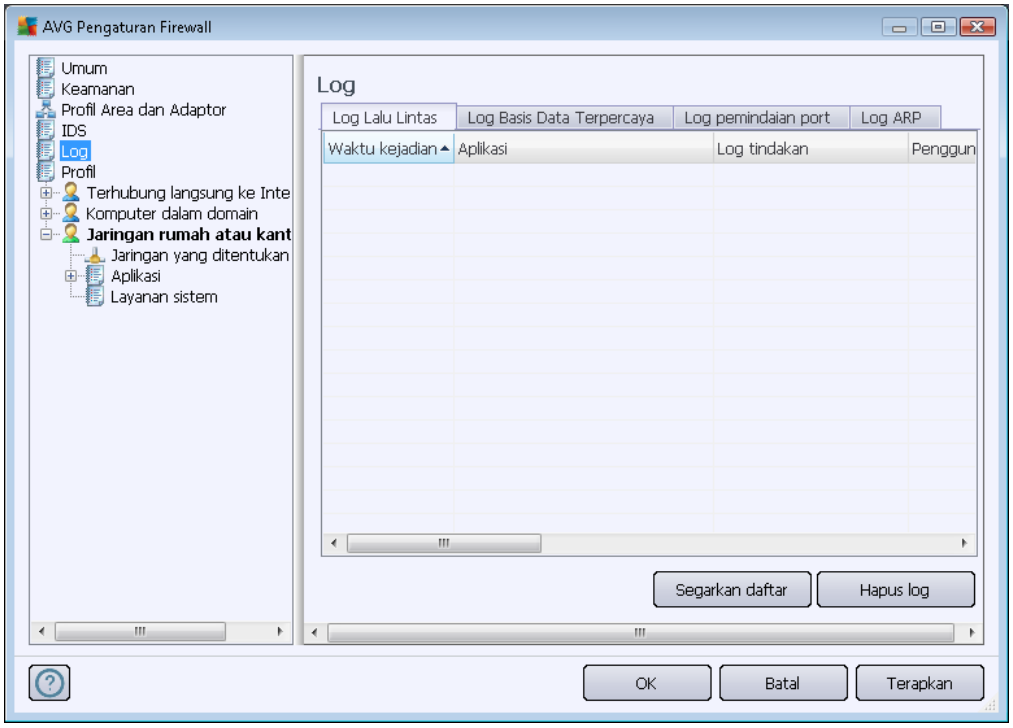
- ***Blokir serangan ARP (lanjutan)*** *(dinonaktifkan secara default)* - Tandai opsi ini untuk mengaktifkan pemblokiran atas upaya komunikasi jenis khusus di dalam jaringan lokal yang terdeteksi oleh ***IDS*** sebagai hal yang mungkin berbahaya. Waktu yang diatur dalam ***Blokir penyerang selama jangka waktu yang ditentukan*** berlaku. Kami menyarankan agar hanya pengguna mahir, yang mengenal dengan baik tipe dan tingkat risiko jaringan

lokal mereka, yang menggunakan fitur ini.

Tombol kontrol

- ***Segarkan daftar*** – tekan tombol untuk memperbarui daftar (*untuk memasukkan semua upaya blokir terakhir*)
- ***Hapus*** - tekan untuk membatalkan blokir terpilih
- ***Perpanjang batas waktu*** – tekan untuk memperpanjang jangka waktu pemblokiran upaya terpilih. Dialog baru dengan opsi perpanjangan akan muncul, yang memungkinkan Anda mengatur waktu dan tanggal tertentu, atau durasi tak terbatas.

11.5. Log



Dialog ***Log*** memungkinkan Anda meninjau daftar semua tindakan dan kejadian Firewall yang telah tercatat dalam log yang berisi keterangan terperinci tentang parameter yang relevan (*waktu kejadian, nama aplikasi, tindakan lognya, nama pengguna, PID, arah lalu lintas, tipe protokol, jumlah port jarak jauh dan lokal, dll.*) pada empat tab:

- ***Log Lalu Lintas*** - memberikan informasi mengenai aktivitas semua aplikasi yang telah mencoba menghubungkan ke jaringan.
- ***Log Basis Data Terpercaya*** - *Basis data terpercaya* adalah basis data internal AVG yang mengumpulkan informasi mengenai aplikasi yang disertifikasi dan dipercaya yang selalu diperbolehkan untuk berkomunikasi secara online. Saat suatu aplikasi baru pertama kali

mencoba menghubungkan ke jaringan (*yakni pada saat belum ada aturan firewall yang ditetapkan untuk aplikasi ini*), perlu dicari tahu apakah komunikasi jaringan diperbolehkan untuk aplikasi tersebut. Pertama, AVG menelusuri *Basis data terpercaya*, dan jika aplikasi tersebut terdaftar, maka ia akan diberi akses ke jaringan secara otomatis. Hanya setelah itulah, bila tidak ada informasi mengenai aplikasi ini yang tersedia dalam basis data, Anda akan ditanyai dalam dialog mandiri apakah Anda mau memperbolehkan aplikasi tersebut mengakses jaringan.

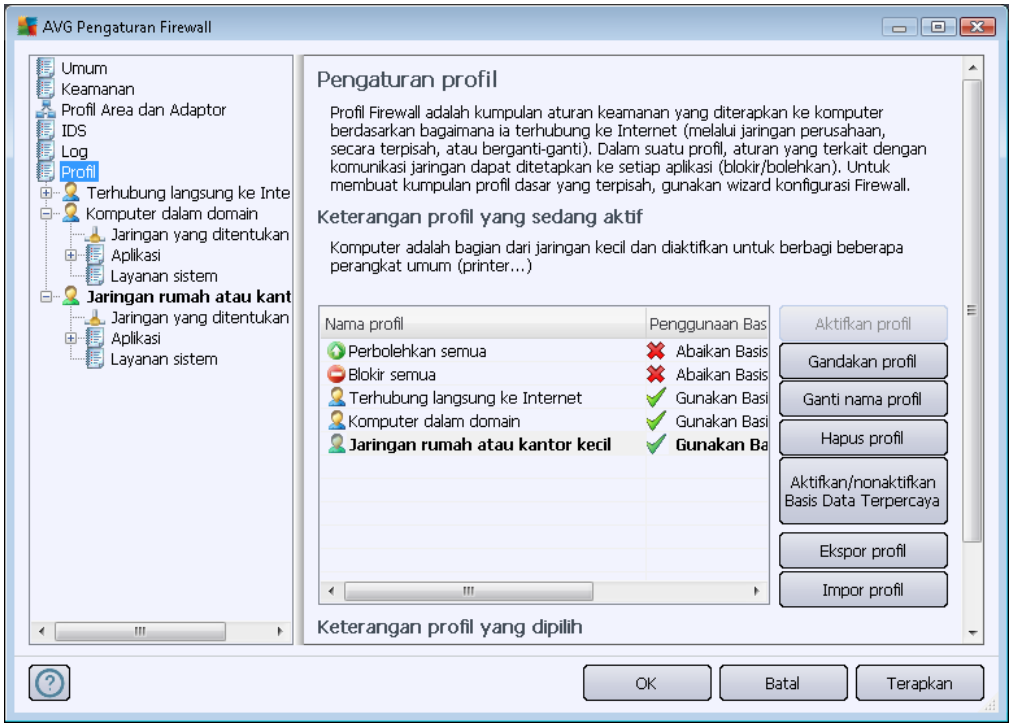
- ***Log pemindaian port*** – merekam semua aktivitas Intrusion Detection System.
- ***Log ARP*** – merekam info mengenai pemblokiran upaya komunikasi khusus di dalam jaringan lokal (*opsi Blokir serangan ARP*) yang terdeteksi oleh Intrusion Detection System sebagai berpotensi bahaya.

Tombol kontrol

- ***Segarkan daftar*** – Semua parameter yang terekam dalam log dapat disusun menurut atribut yang dipilih: secara kronologis (*tanggal*) atau menurut abjad (*kolom lainnya*) – tinggal klik judul kolomnya. Gunakan tombol ***Segarkan daftar*** untuk memperbarui informasi yang ditampilkan saat ini.
- ***Hapus log*** – Tekan untuk menghapus semua entri dalam diagram.

11.6. Profil

Dalam dialog ***Pengaturan profil*** Anda dapat menemukan semua profil yang tersedia:



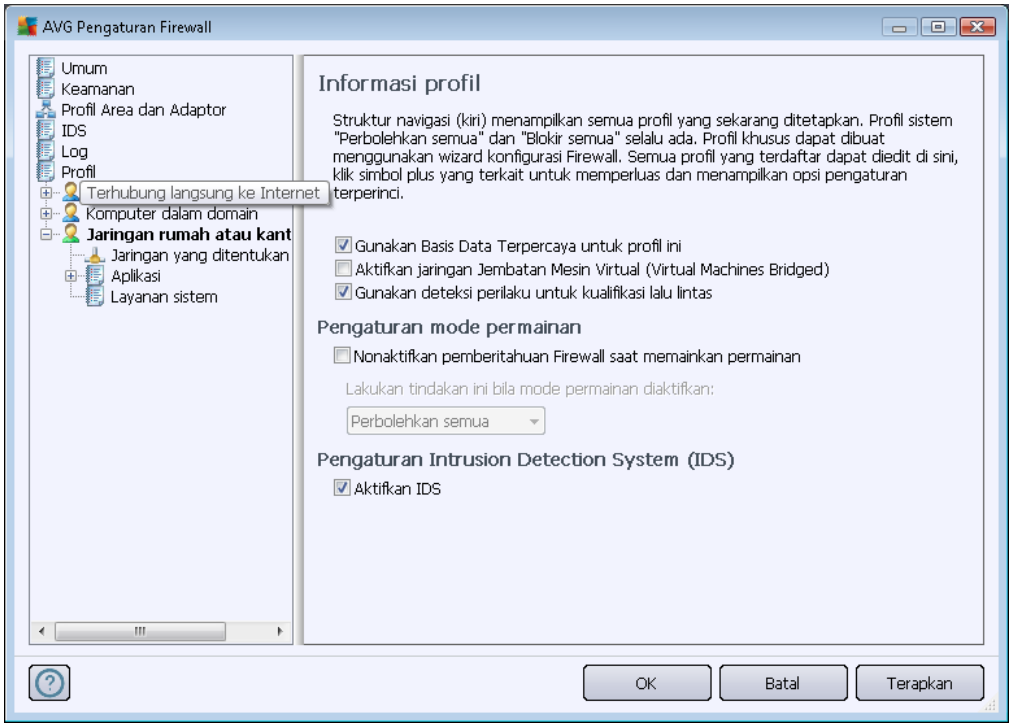
Profil sistem *(Perbolehkan semua, Blokir semua)* tidak dapat diedit. Walau demikian, semua profil *khusus (Terhubung langsung ke Internet, Komputer dalam domain, Jaringan kantor atau rumah kecil)* dapat diedit dalam dialog ini menggunakan tombol kontrol berikut:

- ***Aktifkan profil*** – Tombol ini akan mengaktifkan profil yang dipilih, yang berarti konfigurasi profil yang dipilih akan digunakan oleh Firewall untuk mengontrol lalu lintas jaringan.
- ***Gandakan profil*** – Membuat salinan identik dari profil yang dipilih; nanti Anda dapat mengedit dan mengganti nama salinan tersebut untuk membuat profil baru berdasarkan file asli yang telah digandakan.
- ***Ganti nama profil*** – Memungkinkan Anda menentukan nama baru untuk profil yang dipilih.
- ***Hapus profil*** – Menghapus profil yang dipilih dari daftar.
- ***Aktifkan/Nonaktifkan Basis Data Terpercaya*** – Untuk profil yang dipilih, Anda dapat memutuskan untuk menggunakan informasi *Basis Data Terpercaya* (*Basis Data Terpercaya adalah basis data internal AVG yang mengumpulkan data mengenai aplikasi yang dipercaya dan disertifikasi sehingga selalu diperbolehkan untuk berkomunikasi secara online.*).
- ***Ekspor profil*** – Merekam konfigurasi profil yang dipilih ke dalam file yang akan disimpan untuk kemungkinan penggunaan nanti.
- ***Impor profil*** – Mengkonfigurasi pengaturan profil yang dipilih berdasarkan data yang diekspor dari file konfigurasi cadangan.

Di bagian bawah dialog, carilah keterangan mengenai profil yang saat ini dipilih dalam daftar di atas.

Berdasarkan jumlah profil yang ditentukan, yang telah disebutkan dalam daftar di dalam dialog ***Profil*** , struktur menu navigasi kiri akan turut berubah. Setiap profil yang telah ditentukan akan membuat cabang tertentu di bawah item ***Profil***. Beberapa profil tertentu nanti dapat diedit dalam dialog berikut (*yang identik untuk semua profil*):

11.6.1. Informasi Profil



Dialog ***Informasi profil*** adalah dialog pertama dari suatu bagian di mana Anda dapat mengedit konfigurasi setiap profil dalam dialog tersendiri yang mengacu pada parameter tertentu dari profil tersebut.

- ***Gunakan Basis Data Terpercaya untuk profil ini*** (*diaktifkan secara default*) – Tandai opsi ini untuk mengaktifkan *Basis Data Terpercaya* (*Yakni basis data internal AVG yang mengumpulkan informasi mengenai aplikasi yang disertifikasi dan dipercaya untuk berkomunikasi secara online. Jika belum ada aturan yang ditetapkan untuk aplikasi yang bersangkutan, maka perlu dicari tahu apakah aplikasi tersebut dapat diberi akses ke jaringan. AVG menelusuri Basis Data Terpercaya terlebih dahulu, dan jika aplikasi terdaftar, maka ia akan dianggap aman dan akan diperbolehkan untuk berkomunikasi melalui jaringan. Jika tidak, Anda akan diminta untuk memutuskan apakah aplikasi diperbolehkan untuk berkomunikasi melalui jaringan*) untuk profil terkait

- ***Aktifkan Jaringan Berpenghubung Mesin Virtual*** (*dinonaktifkan secara default*) Tandai item ini untuk memperbolehkan mesin virtual di VMware menghubungkan langsung ke jaringan.

- ***Gunakan deteksi perilaku untuk kualifikasi lalu lintas*** (*diaktifkan secara default*) – Tandai opsi ini untuk memperbolehkan Firewall menggunakan fungsionalitas Identity Protection saat mengevaluasi aplikasi – Identity Protection dapat memberi tahu apakah aplikasi menunjukkan perilaku mencurigakan, ataukah dapat dipercaya dan diperbolehkan untuk berkomunikasi secara online.

Pengaturan mode permainan

Di bagian ***Pengaturan mode permainan*** Anda dapat memutuskan dan mengkonfirmasi dengan menandai item apakah Anda ingin agar pesan informasi Firewall ditampilkan sekalipun saat aplikasi layar-penuh sedang berjalan pada komputer Anda (*biasanya ini permainan, namun berlaku untuk aplikasi layar-penuh apa saja, misalnya presentasi PPT*), karena pesan informasi kadang agak mengganggu.

Jika Anda menandai item ***Nonaktifkan pemberitahuan Firewall saat bermain game***, dalam menu turun-bawah, pilih tindakan yang akan diambil jika ada aplikasi baru yang belum ditetapkan aturannya mencoba berkomunikasi melalui jaringan (*aplikasi yang biasanya memunculkan dialog tanya*) semua aplikasi ini dapat diperbolehkan atau diblokir.

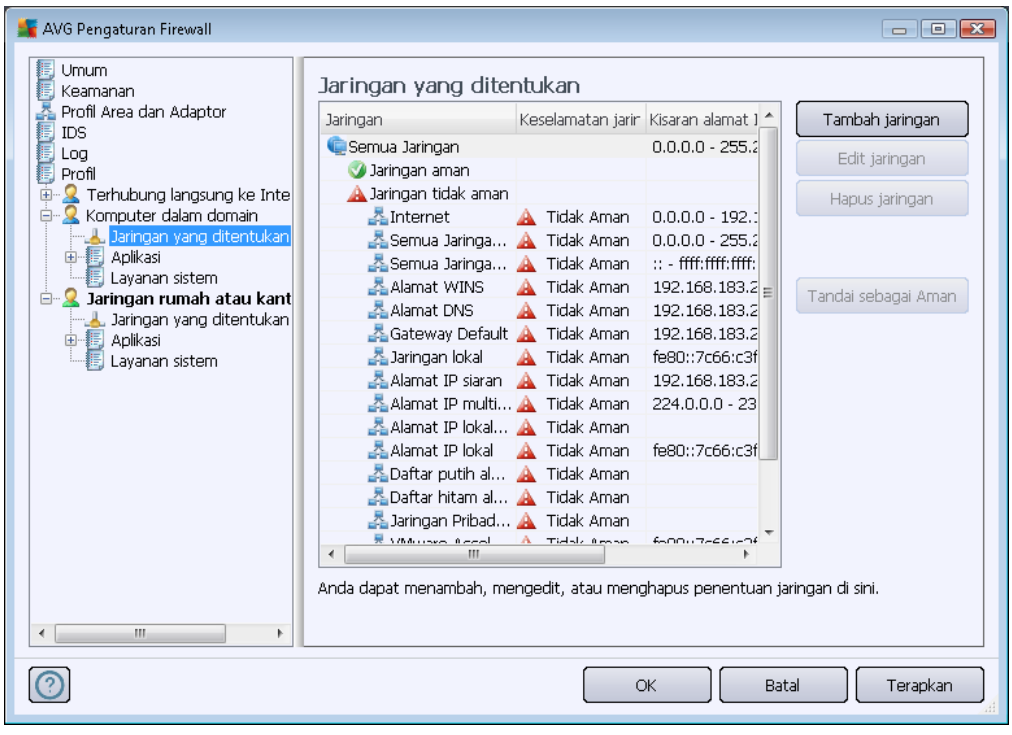
Dengan mode permainan yang diaktifkan, semua tugas yang dijadwalkan (*pemindaian, pembaruan*) ditunda sampai aplikasi ditutup.

Pengaturan Intrusion Detection System (IDS)

Tandai kotak centang ***Aktifkan IDS*** untuk mengaktifkan fitur analisis perilaku khusus yang dirancang untuk mengidentifikasi dan memblokir upaya komunikasi yang mencurigakan melalui port tertentu pada komputer Anda *(untuk perincian pengaturan fitur ini, baca bab IDS pada dokumentasi ini).*

11.6.2. Jaringan Yang Ditentukan

Dialog ***Jaringan yang ditentukan*** menyediakan daftar semua jaringan yang terhubung ke komputer Anda.



Daftar ini memberikan informasi berikut mengenai setiap jaringan yang terdeteksi:

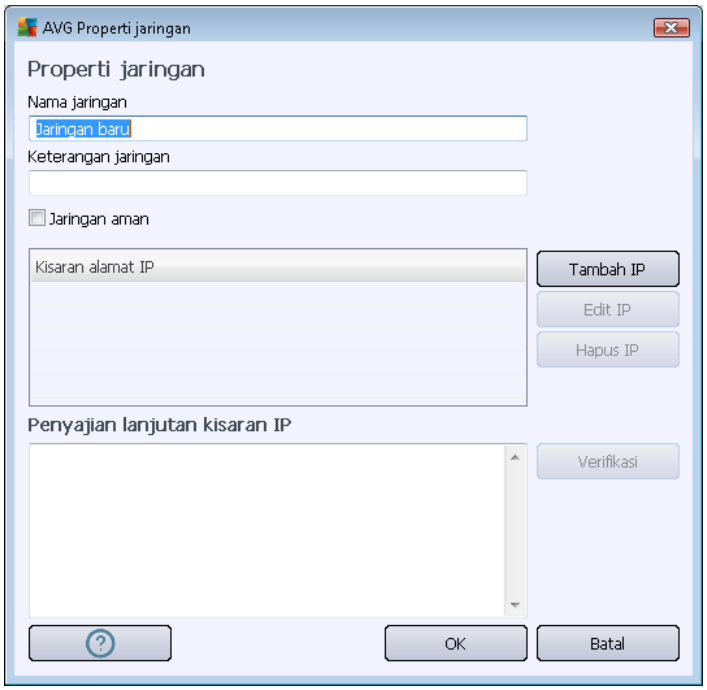
- ***Jaringan*** – Menyediakan daftar nama semua jaringan ke mana komputer terhubung.

- ***Keamanan jaringan*** – Secara default, semua jaringan dianggap tidak aman, dan hanya jika Anda yakin suatu jaringan aman, Anda dapat menetapkannya demikian (*klik item daftar yang merujuk ke jaringan tersebut dan pilih Aman dari menu konteks*) – semua jaringan aman akan dimasukkan ke dalam suatu kelompok yang dapat digunakan aplikasi untuk berkomunikasi dengan kumpulan aturan aplikasi yang diatur ke Perbolehkan untuk aman.

- ***Kisaran alamat IP*** – Setiap jaringan akan dideteksi secara otomatis dan ditetapkan dalam bentuk kisaran alamat IP.

Tombol kontrol

- ***Tambah jaringan*** – Membuka jendela dialog ***Properti jaringan*** di mana Anda dapat mengedit berbagai parameter jaringan yang baru ditentukan:



Dalam dialog ini, Anda dapat menetapkan ***Nama jaringan***, memberikan ***Keterangan jaringan*** dan mungkin dapat menetapkan jaringan sebagai aman. Jaringan baru tersebut dapat ditentukan secara manual dalam dialog tersendiri yang dibuka melalui tombol ***Tambah IP*** (atau ***Edit IP*** / ***Hapus IP***), dalam dialog ini Anda dapat menetapkan jaringan dengan memberikan kisaran IP atau masknya. Untuk jaringan dalam jumlah besar yang harus ditentukan sebagai bagian dari jaringan yang baru dibuat, Anda dapat menggunakan opsi ***Representasi kisaran IP lanjutan***: masukkan daftar semua jaringan ke dalam bidang teksnya (*semua format standar didukung*), dan tekan tombol ***Verifikasi*** untuk memastikan bahwa format ini dapat dikenali. Kemudian tekan ***OK*** untuk mengkonfirmasi dan menyimpan data.

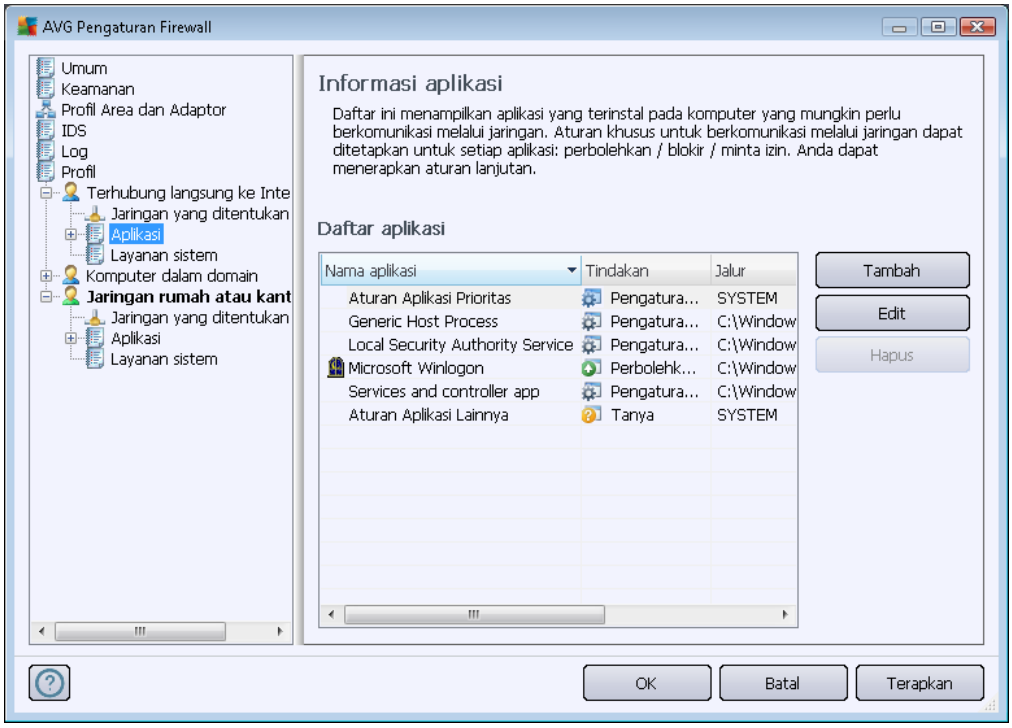
- ***Edit jaringan*** – Membuka jendela dialog ***Properti jaringan*** (*lihat di atas*) di mana Anda dapat mengedit berbagai parameter jaringan yang sudah ditentukan (*dialognya sama dengan dialog untuk menambah jaringan baru, lihat keterangan dalam paragraf sebelumnya*).

- ***Hapus jaringan*** – Menghapus catatan jaringan yang dipilih dari daftar jaringan.

- ***Tandai sebagai aman*** – Secara default, semua jaringan dianggap tidak aman, dan hanya jika Anda yakin bahwa jaringan tersebut aman, Anda dapat menggunakan tombol ini untuk menyatakan jaringan itu aman (*dan begitu pula sebaliknya, setelah jaringan ditetapkan sebagai aman, teks tombol akan berubah menjadi "Tandai sebagai tidak aman"*).

11.6.3. Aplikasi

Dialog ***Informasi aplikasi*** berisi daftar semua aplikasi terinstal yang mungkin perlu berkomunikasi melalui jaringan, dan ikon untuk tindakan yang ditetapkan:



Aplikasi dalam ***Daftar aplikasi*** adalah aplikasi yang terdeteksi pada komputer Anda (*dan telah ditetapkan dengan tindakan tertentu*). Tipe tindakan berikut dapat digunakan:

- - Memungkinkan komunikasi untuk semua jaringan
- - Memungkinkan komunikasi untuk jaringan yang ditetapkan sebagai Aman saja
- - Blokir komunikasi
- - Tampilkan dialog pertanyaan (*pengguna akan dapat memutuskan akan membolehkan atau memblokir komunikasi saat aplikasi berupaya untuk berkomunikasi*

melalui jaringan)

- - Pengaturan lanjutan yang ditetapkan

Perhatikan bahwa hanya aplikasi yang sudah terinstal yang dapat dideteksi, maka jika Anda menginstal aplikasi baru nanti, Anda harus menetapkan aturan Firewall untuknya. Secara default, bila aplikasi baru mencoba untuk menghubung melalui jaringan untuk yang pertama kali, Firewall akan membuat sebuah aturan baginya secara otomatis sesuai dengan Basis Data Terpercaya, atau menanyakan apakah Anda ingin memperbolehkan atau memblokir komunikasi tersebut. Untuk selanjutnya, Anda akan dapat menyimpan jawaban sebagai aturan permanen (yang nanti akan dicantumkan dalam dialog ini).

Tentu saja, Anda juga dapat menentukan aturan untuk aplikasi baru saat itu juga – dalam dialog ini, tekan ***Tambah*** dan masukkan perincian aplikasi.

Selain aplikasi, daftar ini juga berisi dua item khusus:

- ***Aturan Aplikasi Prioritas*** (*di bagian atas daftar*) bersifat pilihan, dan selalu diterapkan sebelum aturan aplikasi masing-masing.
- ***Aturan Aplikasi Lainnya*** (*di bagian bawah daftar*) digunakan sebagai "jalan terakhir", bila tidak ada aturan aplikasi tertentu yang berlaku, mis. untuk aplikasi yang tidak dikenal dan tidak ditentukan. Pilih tindakan yang harus dijalankan bila aplikasi tersebut mencoba berkomunikasi lewat jaringan:
  - *Blokir* – komunikasi akan selalu diblokir.
  - *Perbolehkan* – komunikasi akan diperbolehkan lewat setiap jaringan.
  - *Tanyakan* – Anda akan diminta untuk memutuskan apakah komunikasi harus diperbolehkan atau diblokir.

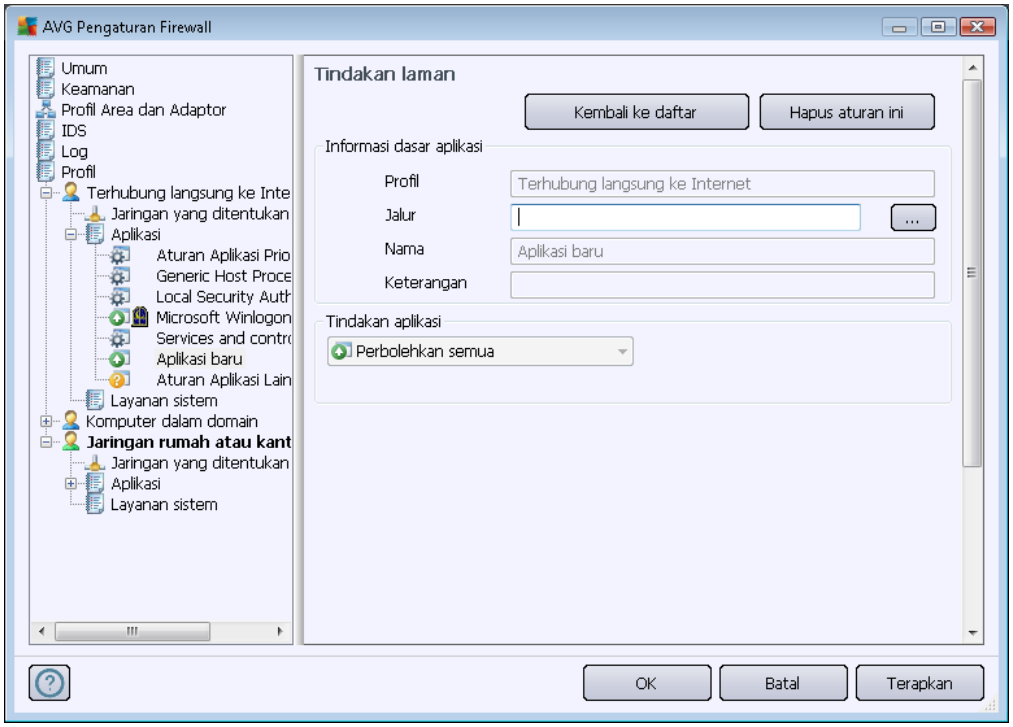
Item ini memiliki opsi pengaturan yang berbeda dengan aplikasi umum dan hanya ditujukan bagi pengguna berpengalaman. Kami sangat menyarankan agar Anda tidak memodifikasi pengaturan!

Tombol kontrol

Daftar ini dapat diedit menggunakan tombol kontrol berikut:

- ***Tambah*** – Membuka dialog kosong Tindakan Halaman untuk menetapkan aturan aplikasi baru.
- ***Edit*** – Membuka dialog Tindakan Halaman yang sama dengan data yang disediakan untuk mengedit kumpulan aturan aplikasi yang ada.
- ***Hapus*** – Menghapus aplikasi yang dipilih dari daftar.

Dalam dialog ***Tindakan halaman***, Anda dapat menentukan pengaturan masing-masing aplikasi secara terperinci:



Tombol kontrol

Dua tombol kontrol tersedia di bagian atas dialog:

- ***Kembali ke daftar*** – Tekan tombol ini untuk menampilkan tinjauan umum atas semua aturan aplikasi yang telah ditentukan.
- ***Hapus aturan ini*** – Tekan tombol ini untuk menghapus aturan aplikasi yang saat ini ditampilkan. ***Perhatikan, tindakan ini tidak dapat dibalikkan!***

Informasi dasar aplikasi

Di bagian ini, masukkan ***Nama*** aplikasi, dan jika diinginkan ***Keterangan*** (*komentar singkat untuk informasi Anda*). Di bidang ***Jalur***, masukkan jalur lengkap ke aplikasi tersebut (*file yang dapat dijalankan*) pada disk; atau temukan aplikasi tersebut dalam tampilan struktur dengan mudah setelah menekan tombol "***...***".

Tindakan aplikasi

Pada menu buka bawah, Anda dapat memilih aturan Firewall untuk aplikasi tersebut, mis. apa yang

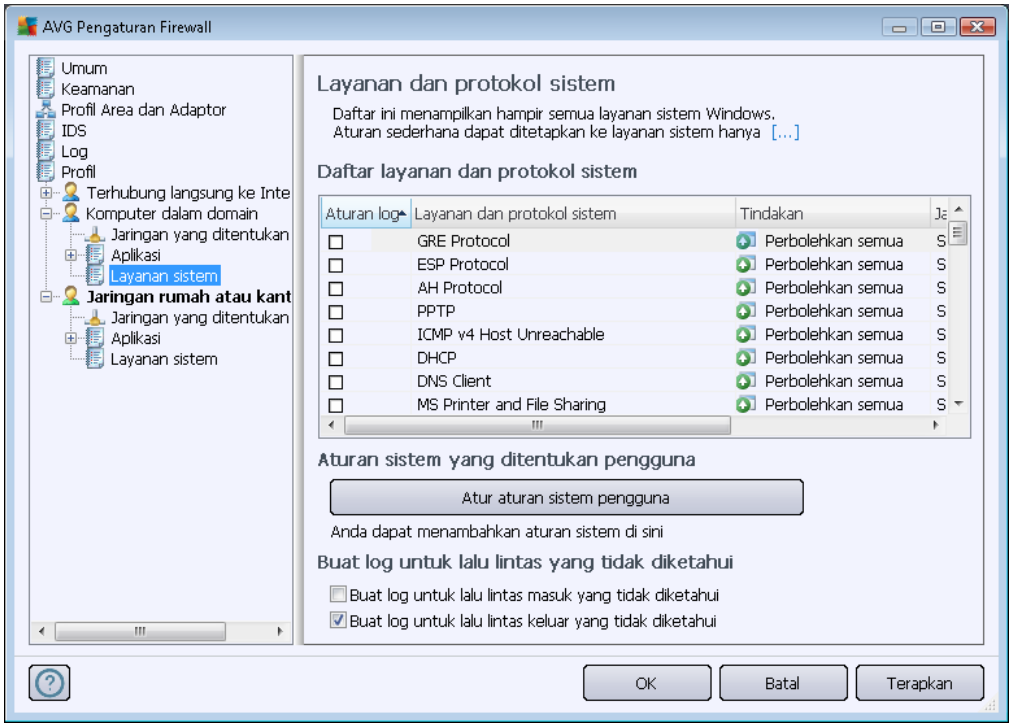
harus dilakukan Firewall bila aplikasi tersebut mencoba berkomunikasi melalui jaringan:

- ***Perbolehkan untuk semua*** – Memperbolehkan aplikasi berkomunikasi melalui semua jaringan dan adaptor yang ditetapkan tanpa dibatasi.
- ***Perbolehkan untuk aman*** – Hanya memperbolehkan aplikasi berkomunikasi melalui jaringan yang ditetapkan sebagai aman *(terpercaya)*.
- ***Blokir*** – Melarang komunikasi secara otomatis; aplikasi tidak diperbolehkan berkomunikasi ke jaringan mana pun.
- ***Tanya*** – Menampilkan dialog yang memungkinkan Anda memutuskan untuk memperbolehkan atau memblokir upaya komunikasi pada saat itu.
- ***Pengaturan lanjutan*** – Menampilkan opsi pengaturan lebih lanjut dan terperinci di bagian bawah dialog, di bagian ***Aturan aplikasi terperinci***. Perincian tersebut akan diterapkan sesuai dengan urutan dalam daftar, sehingga Anda dapat menggeser aturan ***Naik*** atau ***Turun*** dalam daftar sesuai kebutuhan untuk mengatur prioritasnya. Setelah mengklik aturan tertentu dalam daftar, tinjauan umum tentang perincian peraturan tersebut akan ditampilkan di bagian bawah dialog. Nilai yang bergaris bawah warna biru dapat diubah dengan mengklik dalam dialog pengaturannya. Untuk menghapus aturan yang disorot, tekan saja ***Hapus***. Untuk menentukan aturan baru, gunakan tombol ***Tambah*** untuk membuka dialog ***Ubah perincian aturan*** yang memungkinkan Anda menetapkan semua perincian yang diperlukan.

11.6.4. Layanan Sistem

Segala pengeditan dalam dialog Layanan sistem dan protokol ditujukan untuk PENGGUNA BERPENGALAMAN SAJA!

Dialog ***Layanan sistem dan protokol*** menampilkan daftar layanan sistem dan protokol standar Windows yang mungkin perlu berkomunikasi melalui jaringan:



Daftar layanan dan protokol sistem

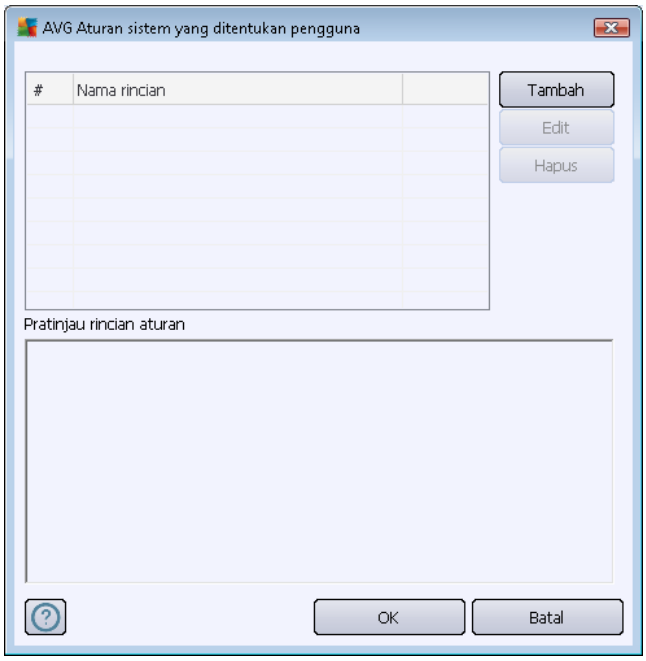
Bagan ini berisi kolom berikut:

- ***Catat tindakan aturan*** – Kotak ini memungkinkan Anda mengaktifkan pencatatan setiap aplikasi aturan dalam log.
- ***Layanan sistem dan protokol*** – Kolom ini menampilkan nama masing-masing layanan sistem.
- ***Tindakan*** – Kolom ini menampilkan ikon untuk tindakan yang ditetapkan:
  - Memungkinkan komunikasi untuk semua jaringan
  - Memungkinkan komunikasi untuk jaringan yang ditetapkan sebagai Aman saja
  - Blokir komunikasi
- ***Jaringan*** – Kolom ini menyatakan aturan sistem yang diterapkan pada jaringan tertentu.

Untuk mengedit pengaturan suatu item dalam daftar ini (*termasuk tindakan yang ditetapkan*), klik kanan pada item tersebut dan pilih ***Edit***. ***Akan tetapi, pengeditan aturan sistem hanya boleh dilakukan oleh pengguna mahir; sangatlah tidak disarankan mengedit aturan sistem!***

Aturan sistem yang ditentukan pengguna

Untuk membuka dialog baru bagi penentuan aturan layanan sistem Anda (*lihat gambar di bawah*), tekan tombol ***Atur aturan sistem pengguna***. Bagian atas dari dialog ***Aturan sistem yang ditentukan pengguna*** menampilkan tinjauan umum semua perincian aturan sistem yang saat ini diedit, sedangkan bagian bawah menampilkan perincian yang dipilih. Perincian aturan yang ditentukan pengguna dapat diedit, ditambah, atau dihapus dengan menekan tombol terkait; perincian aturan yang ditentukan pabrikan hanya dapat diedit:



Perhatikan bahwa pengaturan aturan terperinci ini sifatnya tingkat lanjut, terutama ditujukan bagi administrator jaringan yang memerlukan kontrol penuh atas konfigurasi Firewall. Jika Anda tidak mengerti mengenai tipe protokol komunikasi, nomor port jaringan, definisi alamat IP, dll., jangan memodifikasi pengaturan ini! Jika Anda benar-benar perlu mengubah konfigurasi, harap lihat file dialog bantuan terkait untuk perincian spesifik.

Buat log untuk lalu lintas yang tidak diketahui

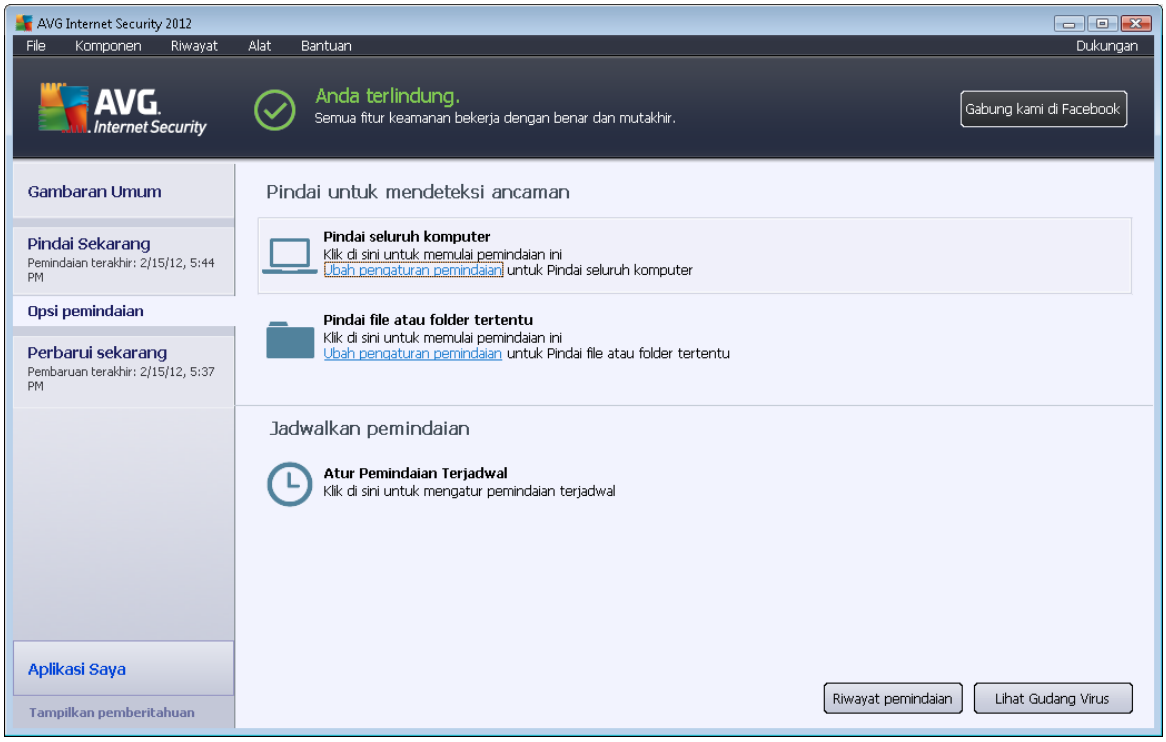
- ***Catat lalu lintas masuk tidak dikenal*** *(dinonaktifkan secara default)* – Tandai kotak ini untuk mencatat dalam Log setiap upaya tidak dikenal untuk menghubung ke komputer Anda dari luar.

- ***Catat lalu lintas keluar tidak dikenal*** *(diaktifkan secara default)* – Tandai kotak ini untuk mencatat dalam Log setiap upaya tidak dikenal dari komputer Anda untuk menghubung ke lokasi di luar.

12. Pemindaian AVG

Secara default, **Keamanan Intenet AVG 2012** tidak menjalankan pemindaian, karena setelah pemindaian awal, Anda harus terlindungi sepenuhnya oleh komponen menetap dari **Keamanan Intenet AVG 2012** yang akan selalu menjaga, dan tidak akan membiarkan kode jahat apa pun memasuki komputer Anda sama sekali. Tentu saja, Anda dapat menjadwalkan pemindaian untuk dijalankan pada interval rutin, atau secara manual menjalankan pemindaian sesuai dengan kebutuhan Anda kapan saja.

12.1. Antarmuka Pemindaian



Antarmuka pemindaian AVG dapat diakses melalui tautan cepat ***Opsi pemindaian***. Klik tautan ini untuk beralih ke dialog ***Pindai ancaman***. Dalam dialog ini Anda akan menemukan yang berikut:

- gambaran umum pemindaian yang ditentukan – tiga tipe pemindaian yang ditentukan oleh vendor perangkat lunak siap digunakan segera saat diperlukan atau telah dijadwalkan:
  - Pemindaian seluruh komputer
  - Pindai file atau folder tertentu
- Bagian menjadwalkan pemindaian – di mana Anda dapat menentukan tes baru dan membuat jadwal baru bila diperlukan.

Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka pengetesan adalah sebagai berikut:

- ***Riwayat pemindaian*** - menampilkan dialog gambaran umum hasil pemindaian berisi seluruh riwayat pemindaian
- ***Lihat Gudang Virus*** - membuka jendela baru berisi Gudang Virus – tempat di mana indeksi yang terdeteksi dikarantina

12.2. Pemindaian Yang Ditetapkan

Salah satu fitur utama **Keamanan Intenet AVG 2012** adalah pemindaian saat diperlukan. Tes saat diperlukan dirancang untuk memindai berbagai bagian komputer Anda bila muncul kecurigaan mengenai kemungkinan infeksi virus. Bagaimana pun, sangat disarankan untuk melakukan tes demikian secara rutin sekalipun menurut Anda tidak ada virus yang dapat ditemukan pada komputer Anda.

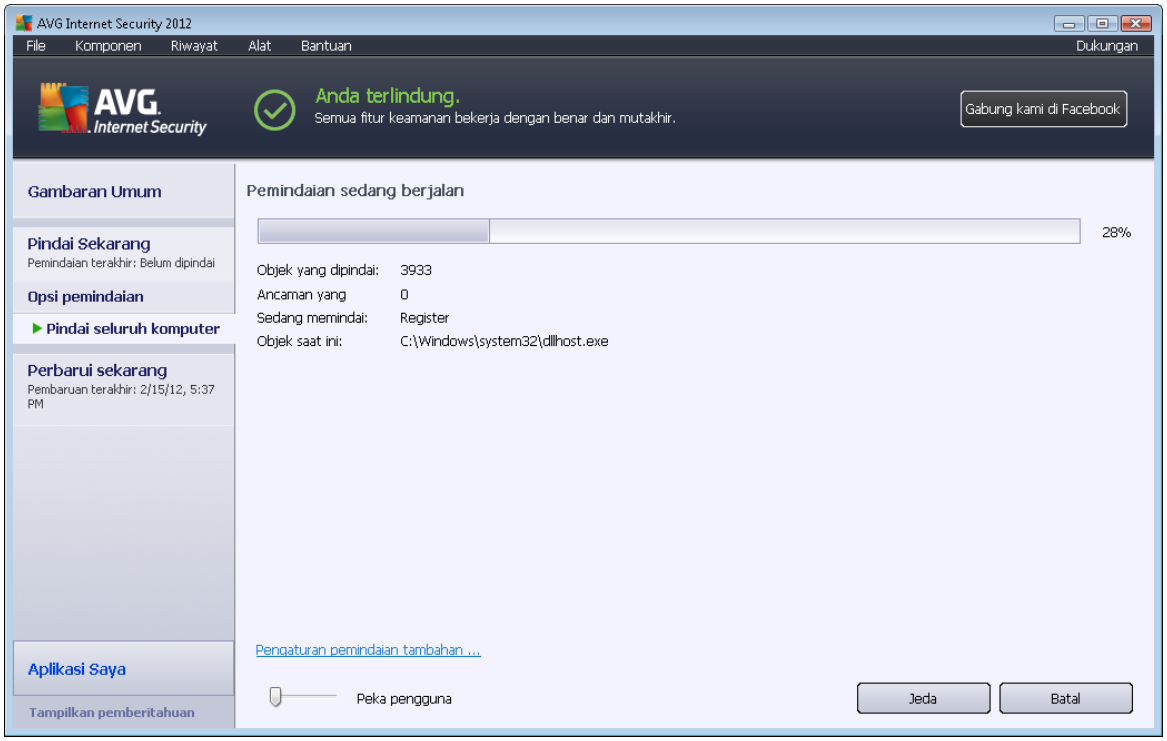
Dalam **Keamanan Intenet AVG 2012** Anda akan menemukan tipe pemindaian yang sudah ditetapkan oleh vendor perangkat lunak:

12.2.1. Pemindaian Seisi Komputer

Pemindaian Seisi Komputer – memindai seisi komputer Anda untuk mencari kemungkinan infeksi dan/atau program yang mungkin tidak diinginkan. Tes ini akan memindai semua hard drive komputer Anda, akan mendeteksi dan memulihkan virus yang ditemukan, atau memindahkan infeksi yang terdeteksi ke Gudang Virus. Pemindaian seisi komputer Anda harus dijadwalkan pada workstation sedikitnya sekali seminggu.

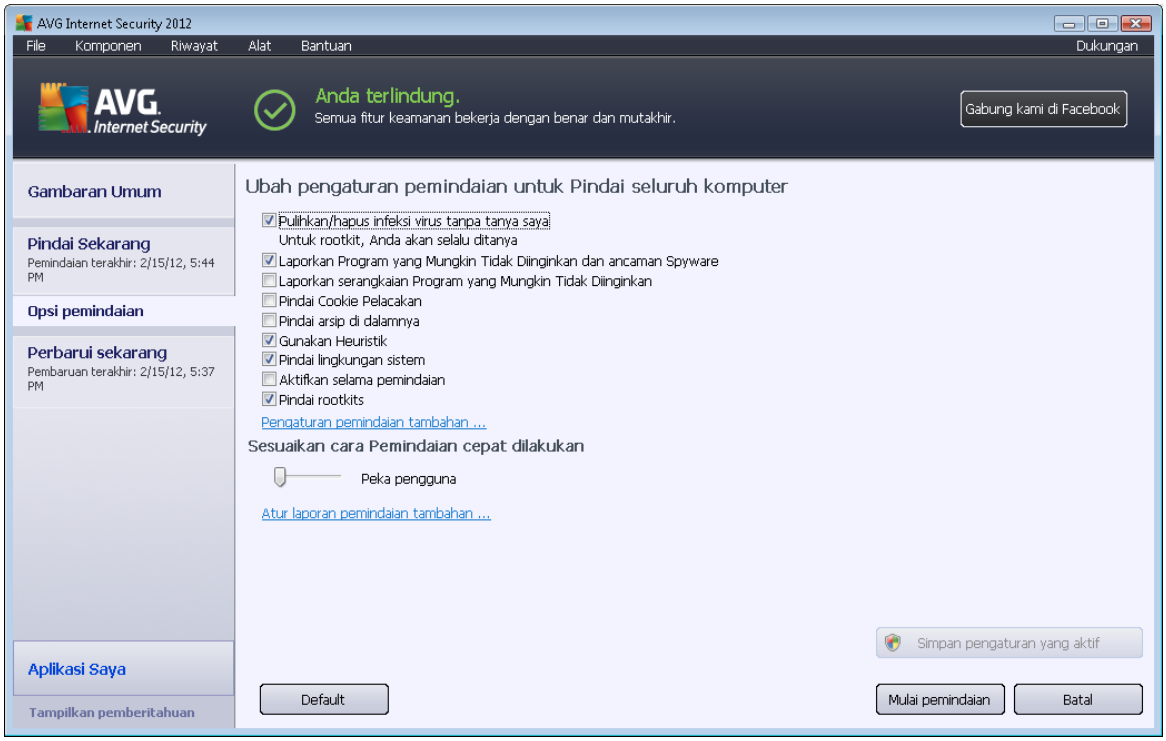
Peluncuran pemindaian

Pemindaian Seisi Komputer dapat diluncurkan langsung dari antarmuka pemindaian dengan mengklik ikon pindai. Tidak ada pengaturan tertentu lainnya yang harus dikonfigurasi untuk tipe pemindaian ini, pemindaian akan segera dimulai dalam dialog ***Pemindaian sedang dijalankan*** (*lihat cuplikan layar*). Pemindaian dapat dihentikan untuk sementara (***Jeda***) atau dibatalkan (***Hentikan***) jika perlu.



Mengedit konfigurasi pemindaian

Anda mempunyai opsi untuk mengedit pengaturan default yang telah ditetapkan untuk ***Pemindaian seisi komputer***. Buka tautan ***Ubah pengaturan pindai*** untuk membuka dialog ***Ubah pengaturan pindai untuk Pemindaian Seisi Komputer*** *(dapat diakses dari antarmuka pemindaian melalui tautan Ubah pengaturan pindai untuk Pemindaian seisi komputer)*. ***Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!***



- ***Parameter pemindaian*** – dalam daftar parameter pemindaian, Anda dapat mengaktifkan/menonaktifkan parameter tertentu bila diperlukan:

    - ***Pulihkan / hapus infeksi virus tanpa bertanya pada saya*** (*diaktifkan secara default*) – Jika ada virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus .

    - ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – Tandai untuk mengaktifkan mesin Anti-Spyware dan memindai spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak sengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.

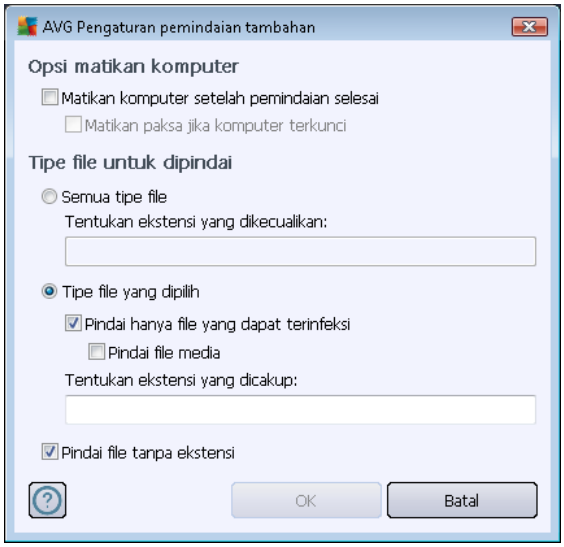
    - ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*) – Tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

    - ***Pindai Cookie Pelacak*** (*dinonaktifkan secara default*) – Parameter komponen Anti-Spyware ini menentukan bahwa cookie harus terdeteksi; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang*

pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka).

- ***Pindai di dalam arsip*** (*dinonaktifkan secara default*) – Parameter ini menentukan bahwa pemindaian harus memeriksa semua file yang tersimpan dalam arsip, misalnya, ZIP, RAR, ...
- ***Gunakan Heuristik*** (*diaktifkan secara default*) – Analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- ***Pindai lingkungan sistem*** (*diaktifkan secara default*) – Pemindaian juga akan memeriksa area sistem komputer Anda.
- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default*) – Dalam kondisi khusus (*dicurigai bahwa komputer Anda terinfeksi*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- ***Pindai rootkit*** (*aktifkan secara default*) – pemindaian Anti-Rootkit menelusuri komputer Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

- ***Pengaturan pindai tambahan*** – tautan ini akan membuka dialog ***Pengaturan pindai tambahan*** di mana Anda dapat menentukan parameter berikut:



- ***Opsi matikan komputer*** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (***Matikan paksa jika komputer terkunci***).

- ***Tipe file untuk pemindaian*** – sselanjutnya Anda harus memutuskan apa yang ingin Anda pindai:

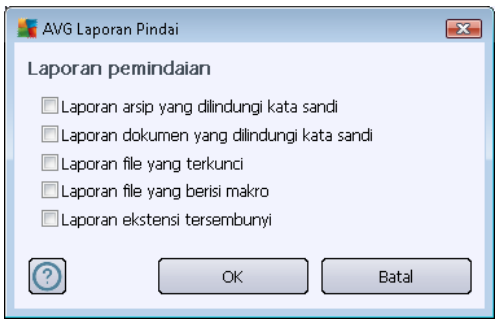
  - ***Semua tipe file*** dengan kemungkinan penetapan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai;

  - ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak ditandai, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

  - Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

- ***Sesuaikan secepat apa Pemindaian selesai*** - Anda dapat menggunakan penggeser untuk mengganti prioritas proses pemindaian. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Sebagai alternatif, Anda dapat menjalankan proses pemindaian lebih lambat yang berarti beban sumber daya sistem akan diminimumkan (*berguna saat Anda perlu menggunakan komputer tersebut namun Anda tidak peduli berapa lama pemindaian akan berlangsung*), atau lebih cepat dengan kebutuhan sumber daya sistem yang bertambah (*misalnya saat komputer ditinggalkan untuk sementara*).

- ***Atur laporan pindai tambahan*** – tautan ini akan membuka dialog baru ***Laporan pindai*** di mana Anda dapat memilih kemungkinan tipe temuan apa saja yang harus dilaporkan:



Peringatan: *Pengaturan pindai ini sama dengan parameter pemindaian yang baru ditetapkan – seperti diterangkan dalam bab Pemindaian AVG / Menjadwalkan pemindaian/ Cara Memindai. Seandainya Anda harus memutuskan untuk mengubah konfigurasi default* ***Pindai seisi komputer*** *maka Anda dapat menyimpan pengaturan baru sebagai konfigurasi default untuk digunakan bagi semua pemindaian seisi komputer selanjutnya.*

12.2.2. Pindai File atau Folder Tertentu

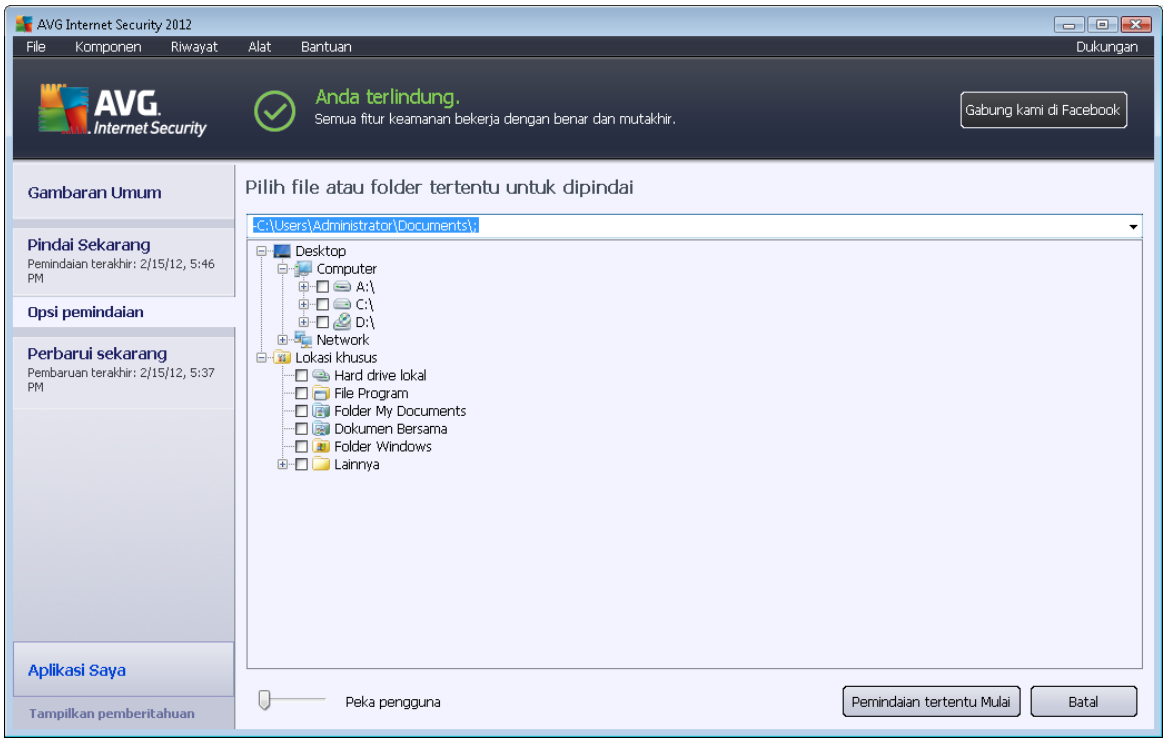
Pindai file atau folder tertentu – hanya memindai area komputer Anda yang telah dipilih untuk dipindai (*folder, hard disk, diskет floppy, atau CD yang dipilih, dll.*). Kemajuan pemindaian jika terdeteksi virus dan penyembuhannya sama dengan pemindaian seisi komputer: virus yang ditemukan akan dipulihkan atau dipindahkan ke Gudang Virus. Pemindaian file atau folder dapat digunakan untuk mengatur tes Anda sendiri dan menjadwalkannya berdasarkan kebutuhan.

Peluncuran pemindaian

Pindai file atau folder tertentu dapat diluncurkan langsung dari antarmuka pemindaian dengan mengklik ikon pindai. Sebuah dialog baru bernama ***Pilih file atau folder tertentu untuk pemindaian*** akan dibuka. Dalam struktur komputer Anda, pilih folder yang ingin dipindai. Jalur ke setiap folder yang dipilih akan dibuat secara otomatis dan muncul dalam kotak teks di bagian atas dialog ini.

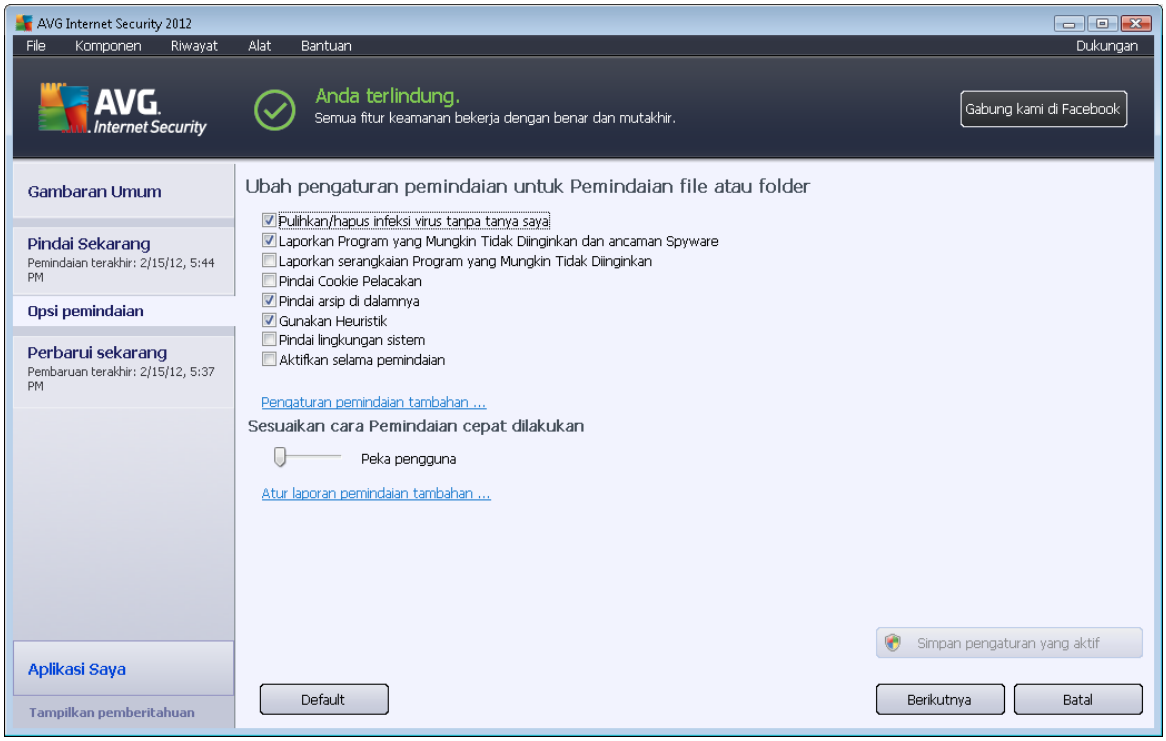
Juga ada kemungkinan untuk memindai folder tertentu sementara semua subfoldernya dikecualikan dari pemindaian ini; untuk melakukannya ketikkan tanda kurang "**-**" di depan jalur yang telah dibuat secara otomatis (*lihat cuplikan layar*). Untuk mengecualikan seluruh folder dari pemindaian, gunakan tanda "**!**" parameter.

Terakhir, untuk meluncurkan pemindaian, tekan tombol ***Mulai pindai***; proses pemindaiannya sendiri pada dasarnya sama dengan Pemindaian seisi komputer.



Mengedit konfigurasi pindai

Anda mempunyai opsi untuk mengedit pengaturan default yang telah ditetapkan pada ***Pindai file atau folder tertentu***. Tekan tautan ***Ubah pengaturan pindai*** untuk masuk ke dialog ***Ubah pengaturan pindai untuk Pindai file atau folder tertentu***. ***Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!***



- ***Parameter pemindaian*** – dalam daftar parameter pemindaian, Anda dapat mengaktifkan/menonaktifkan parameter tertentu bila diperlukan:
    - ***Pulihkan/hapus infeksi tanpa bertanya pada saya*** (*diaktifkan secara default*) – jika ada virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.
    - ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – tandai untuk mengaktifkan mesin Anti-Spyware, dan memindai spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak sengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.
    - ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*) – tandai kotak ini untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai Cookie Pelacak*** (*dinonaktifkan secara default*) – parameter komponen Anti-Spyware ini menetapkan bahwa cookie harus terdeteksi; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).

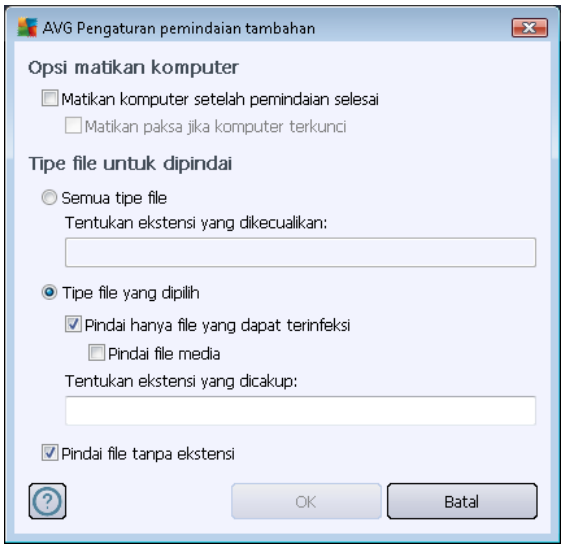
- ***Pindai di dalam arsip*** (*diaktifkan secara default*) – parameter ini menetapkan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut tersimpan dalam arsip, misalnya, ZIP, RAR, ...

- ***Gunakan Heuristik*** (*diaktifkan secara default*) – analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk mendeteksi virus selama pemindaian.

- ***Pindai lingkungan sistem*** (*dinonaktifkan secara default*) – pemindaian juga akan memeriksa area sistem komputer Anda.

- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default*) – dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi virus atau exploit*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pengaturan pindai tambahan*** – tautan ini akan membuka dialog ***Pengaturan pindai tambahan*** di mana Anda dapat menentukan parameter berikut:



  - ***Opsi matikan komputer*** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (***Matikan paksa jika komputer terkunci***).

  - ***Tipe file untuk pemindaian*** – selanjutnya Anda harus memutuskan apakah Anda

ingin memindai:

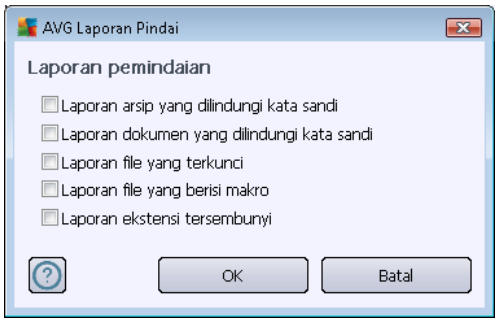
- ***Semua tipe file*** dengan kemungkinan penetapan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai;

- ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak ditandai, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

- Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

- ***Prioritas proses pindai*** – Anda dapat menggunakan bilah geser untuk mengubah prioritas proses pindai. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Sebagai alternatif, Anda dapat menjalankan proses pemindaian lebih lambat yang berarti beban sumber daya sistem akan diminimumkan (*berguna saat Anda perlu menggunakan komputer tersebut namun Anda tidak peduli berapa lama pemindaian akan berlangsung*), atau lebih cepat dengan kebutuhan sumber daya sistem yang bertambah (*misalnya saat komputer ditinggalkan untuk sementara*).

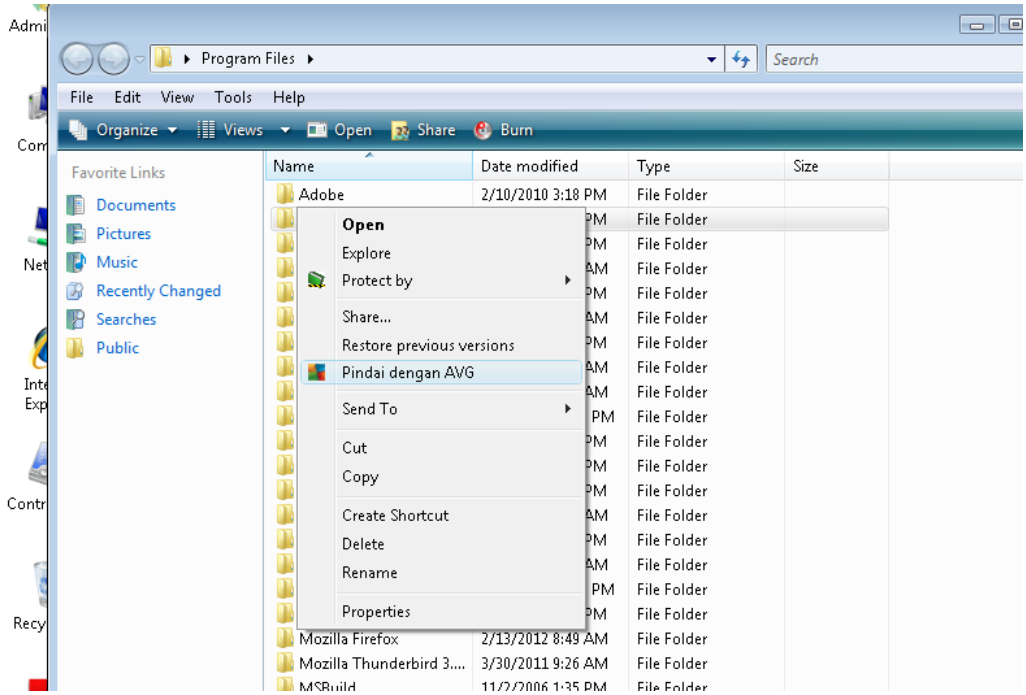
- ***Atur laporan pindai tambahan*** – tautan ini akan membuka dialog baru ***Laporan Pindai*** di mana Anda dapat memilih kemungkinan tipe temuan apa saja yang harus dilaporkan:



Peringatan: *Pengaturan pindai ini sama dengan parameter pemindaian yang baru ditetapkan – seperti diterangkan dalam bab Pemindaian AVG / Menjadwalkan pemindaian/ Cara Memindai. Seandainya Anda harus memutuskan untuk mengubah konfigurasi default* ***Pindai file atau folder tertentu*** *maka Anda dapat menyimpan pengaturan baru sebagai konfigurasi default untuk digunakan bagi semua pemindaian file atau folder selanjutnya. Selain itu, konfigurasi ini akan digunakan sebagai template bagi semua pemindaian yang baru Anda jadwalkan (semua pemindaian khusus berdasarkan pada konfigurasi saat ini pada Pindai file atau folder yang dipilih).*

12.3. Memindai dalam Windows Explorer

Di samping pemindaian yang telah ditetapkan, yang diluncurkan untuk seisi komputer atau area yang dipilih, **Keamanan Intenet AVG 2012** juga menyediakan opsi untuk pemindaian cepat atas objek tertentu secara langsung di lingkungan Windows Explorer. Jika Anda ingin membuka file tidak dikenal dan Anda tidak bisa memastikan isinya, Anda mungkin perlu memeriksanya bila diperlukan. Ikuti langkah-langkah ini:



- Dalam Windows Explorer, sorot file *(atau folder)* yang ingin Anda periksa
- Klik kanan mouse Anda di atas objek untuk membuka menu konteks
- Pilih opsi ***Pindai dengan AVG*** agar file dipindai dengan **Keamanan Intenet AVG 2012**

12.4. Pemindaian Baris Perintah

Dalam **Keamanan Intenet AVG 2012** ada opsi untuk menjalankan pemindaian dari baris perintah. Anda dapat menggunakan opsi ini untuk kejadian di server, atau saat membuat skrip batch yang akan diluncurkan secara otomatis setelah komputer melakukan boot. Dari baris perintah, Anda dapat meluncurkan pemindaian bersama sebagian besar parameter yang ditawarkan dalam antarmuka pengguna grafis AVG.

Untuk meluncurkan pemindaian AVG dari baris perintah, jalankan perintah berikut dalam folder di mana AVG terinstal:

- ***avgscanx*** untuk OS 32 bit
- ***avgscana*** untuk OS 64 bit

Sintaksis perintah

Sintaksis perintah mengikuti:

- ***avgscanx /parameter*** ... misalnya, ***avgscanx /comp*** untuk memindai seisi komputer
- ***avgscanx /parameter /parameter*** .. dengan beberapa parameter sekaligus, ini harus ditempatkan dalam satu baris dan dipisahkan dengan spasi serta karakter garis-miring
- jika parameter mengharuskan diberikannya nilai tertentu (seperti parameter ***/scan*** yang memerlukan informasi mengenai pemilihan area pada komputer yang akan dipindai, maka Anda harus memberikan jalur yang persis ke bagian yang dipilih tersebut), nilai-nilainya dipisah dengan titik koma, sebagai contoh: ***avgscanx /scan=C:\;D:***

Parameter pemindaian

Untuk menampilkan tinjauan umum seluruh parameter yang tersedia, ketikkan perintah tersebut dengan parameter /? atau /HELP (mis. ***avgscanx /?***). Satu-satunya parameter wajib adalah /SCAN untuk menentukan area komputer yang harus dipindai. Untuk penjelasan lebih lanjut mengenai opsi ini, lihat tinjauan umum parameter baris perintah.

Untuk menjalankan pemindaian, tekan ***Enter***. Selama pemindaian, Anda dapat menghentikan proses dengan ***Ctrl+C*** atau ***Ctrl+Pause***.

Pemindaian CMD diluncurkan dari antarmuka grafis

Bila Anda menjalankan komputer dalam Safe Mode di Windows, maka kemungkinan Anda juga dapat meluncurkan pemindaian baris perintah dari antarmuka pengguna grafis. Pemindaiannya sendiri akan diluncurkan dari baris perintah, dialog ***Penyusun Baris Perintah*** hanya memungkinkan Anda menentukan sebagian besar parameter pemindaian dalam antarmuka grafis yang mudah.

Berhubung dialog ini hanya dapat diakses dalam Safe Mode di Windows, untuk melihat keterangan terperinci mengenai dialog ini bacalah file bantuan yang dibuka langsung dari dialog.

12.4.1. Parameter Pemindaian CMD

Pada yang berikut ini, carilah daftar semua parameter yang tersedia untuk pemindaian baris perintah:

- ***/SCAN*** Pindai file atau folder tertentu */SCAN=path;path (misalnya /SCAN=C:\;D:\)*
- ***/COMP*** Pemindaian seluruh komputer
- ***/HEUR*** Gunakan analisis heuristik
- ***/EXCLUDE*** Kecualikan jalur atau file dari pemindaian

- ***/@*** File perintah /nama file/
- ***/EXT*** Pindai ekstensi ini /misalnya EXT=EXE,DLL/
- ***/NOEXT*** Jangan pindai ekstensi ini /misalnya NOEXT=JPG/
- ***/ARC*** Pindai arsip
- ***/CLEAN*** Bersihkan secara otomatis
- ***/TRASH*** Pindahkan file terinfeksi ke Gudang Virus
- ***/QT*** Pengujian cepat
- ***/LOG*** Buat file hasil pemindaian
- ***/MACROW*** Laporkan makro
- ***/PWDW*** Laporkan file yang dilindungi kata sandi
- ***/ARCBOMBSW*** Laporkan bom arsip *(arsip yang dikompresi secara berulang kali)*
- ***/IGNLOCKED*** Abaikan file terkunci
- ***/REPORT*** Laporkan ke file /nama file/
- ***/REPAPPEND*** Tambahkan ke file laporan
- ***/REPOK*** Laporkan file yang tidak terinfeksi sebagai OK
- ***/NOBREAK*** Jangan perbolehkan CTRL-BREAK untuk menggugurkan
- ***/BOOT*** Aktifkan pemeriksaan MBR/BOOT
- ***/PROC*** Pindai proses aktif
- ***/PUP*** Laporkan Program yang mungkin tidak diinginkan
- ***/PUPEXT*** Laporkan serangkaian Program yang mungkin tidak diinginkan
- ***/REG*** Pindai register
- ***/COO*** Pindai cookie
- ***/?*** Tampilkan bantuan untuk topik ini
- ***/HELP*** Tampilkan bantuan untuk topik ini
- ***/PRIORITY*** Atur prioritas pindai /Low, Auto, High/ *(lihat Pengaturan lanjutan/ Pemindaian)*

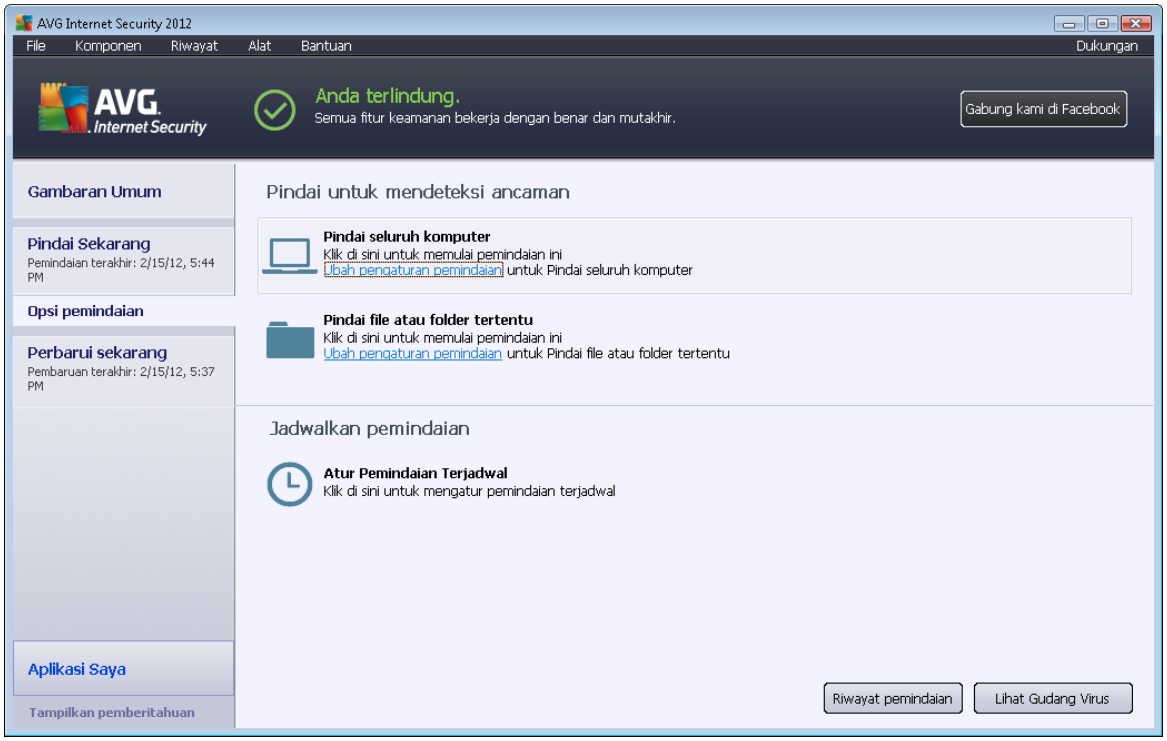
- ***/SHUTDOWN*** Matikan komputer setelah pemindaian selesai
- ***/FORCESHUTDOWN*** Matikan paksa komputer setelah pemindaian selesai
- ***/ADS*** Pindai Aliran Data Alternatif *(hanya NTFS)*
- ***/HIDDEN*** Laporkan file dengan ekstensi tersembunyi
- ***/INFECTABLEONLY*** Pindai file dengan ekstensi terinfeksi saja
- ***/THOROUGHSCAN*** Aktifkan pemindaian menyeluruh
- ***/CLOUDCHECK*** Periksa positif palsu
- ***/ARCBOMBSW*** Laporkan file arsip yang dikompresi ulang

12.5. Penjadwalan Pemindaian

Dengan **Keamanan Intenet AVG 2012** Anda dapat menjalankan pemindaian saat diperlukan (misalnya saat Anda mencurigai adanya infeksi yang terbawa ke komputer Anda) atau berdasarkan rencana yang telah dijadwalkan. Sangat disarankan untuk menjalankan pemindaian berdasarkan jadwal: dengan cara ini Anda dapat memastikan komputer terlindung dari segala kemungkinan terinfeksi, dan Anda tidak perlu memikirkan apakah telah meluncurkan dan kapan meluncurkan pemindaian.

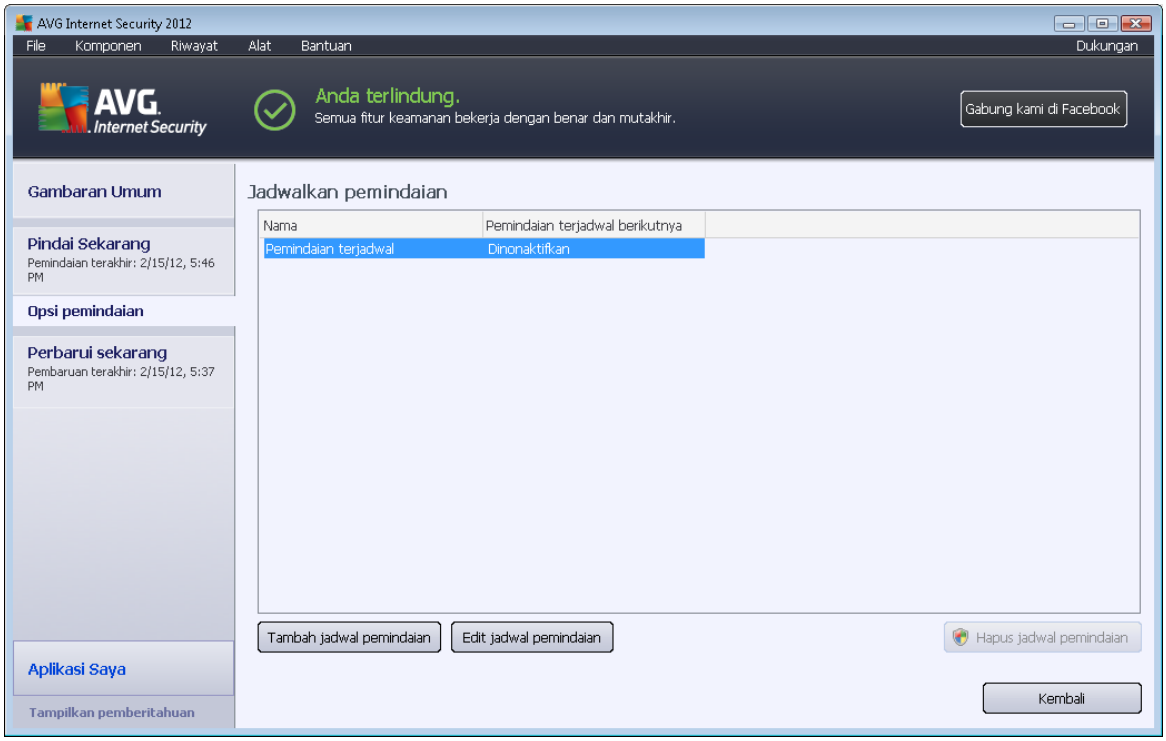
Anda harus meluncurkan Pemindaian Seisi Komputer secara rutin, sedikitnya sekali seminggu. Walau demikian, jika memungkinkan, luncurkan pemindaian seisi komputer Anda setiap hari – sebagaimana diatur dalam konfigurasi default jadwal pemindaian. Jika komputer "selalu dihidupkan" maka Anda dapat menjadwalkan pemindaian di luar jam kerja. Jika komputer kadang dimatikan, maka pemindaian jadwal akan terjadi saat komputer dihidupkan bila tugas tersebut telah lewat.

Untuk membuat jadwal pemindaian baru, lihat Antarmuka pemindaian AVG dan cari bagian bawah yang bernama ***Jadwalkan pemindaian***:



Jadwalkan pemindaian

Klik ikon grafis di bagian ***Jadwalkan pemindaian*** untuk membuka dialog ***Jadwalkan pemindaian*** baru di mana Anda dapat menemukan daftar semua pemindaian terjadwal saat ini:



Anda dapat mengedit / menambahkan pemindaian menggunakan tombol kontrol berikut:

- ***Tambah jadwal pemindaian*** – tombol ini membuka dialog ***Pengaturan pemindaian terjadwal***, tab Pengaturan jadwal. Dalam dialog ini, Anda dapat menentukan parameter tes yang baru ditetapkan.

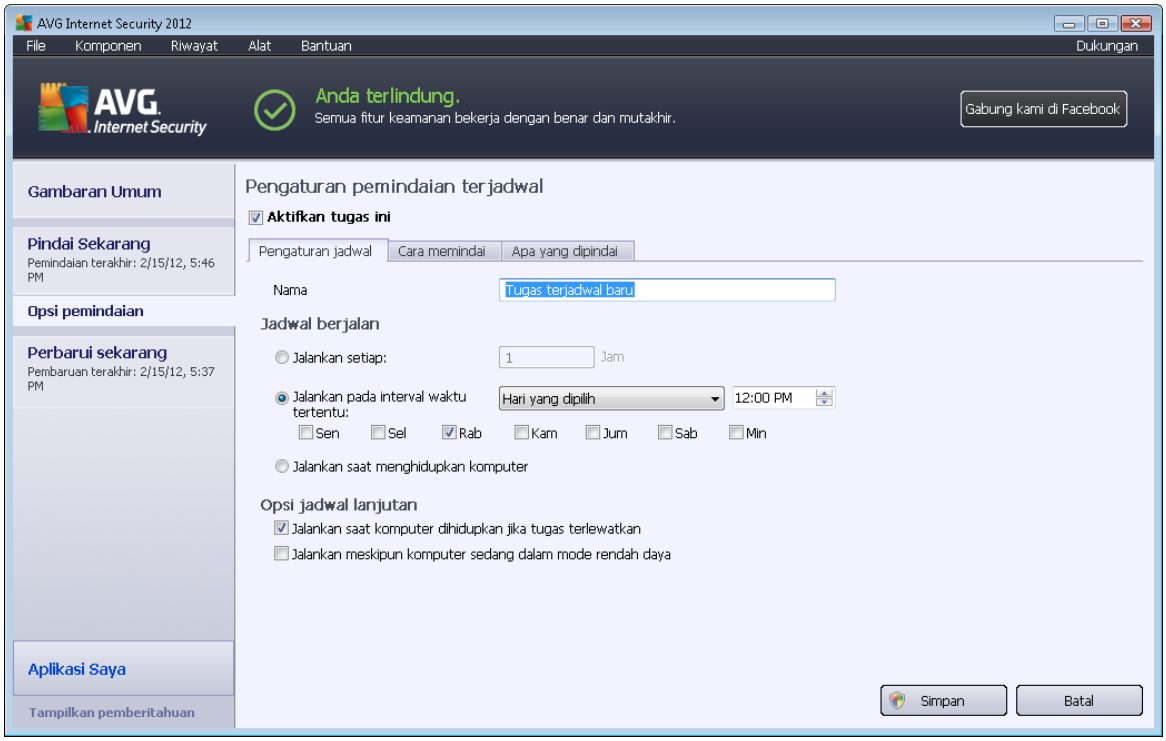
- ***Edit jadwal pemindaian*** – tombol ini hanya digunakan jika sebelumnya Anda telah memilih tes yang ada dari daftar tes terjadwal. Jika tombol muncul sebagai aktif maka Anda dapat mengkliknya untuk beralih ke dialog ***Pengaturan pemindaian terjadwal***, tab Pengaturan jadwal. Parameter tes yang dipilih sudah ditentukan di sini dan dapat diedit.

- ***Hapus jadwal pemindaian*** – tombol ini juga aktif jika sebelumnya Anda telah memilih tes yang ada dari daftar tes terjadwal. Tes ini nanti dapat dihapus dari daftar dengan menekan tombol kontrol. Walau demikian, Anda hanya dapat menghapus tes Anda sendiri; ***Jadwal pemindaian seisi komputer*** yang telah ditetapkan dalam pengaturan default tidak dapat dihapus.

- ***Kembali*** – kembali ke antarmuka pemindaian AVG

12.5.1. Pengaturan Jadwal

Jika Anda ingin menjadwalkan tes baru dan peluncuran rutinnya, buka dialog ***Pengaturan tes terjadwal*** (*klik tombol* ***Tambah jadwal pemindaian*** *dalam dialog* ***Jadwalkan pemindaian***). Dialog ini terbagi ke dalam tiga tab: ***Pengaturan jadwal*** *(lihat gambar di bawah; tab default tempat Anda akan dialihkan secara otomatis*), Cara memindai, dan Apa yang dipindai.



Pada tab ***Pengaturan jadwal*** Anda dapat mencentang/tidak mencentang item ***Aktifkan tugas ini*** terlebih dahulu untuk menonaktifkan tes terjadwal untuk sementara, dan mengaktifkannya lagi saat diperlukan.

Berikutnya, berikan nama pada pemindaian yang akan dibuat dan dijadwalkan. Ketikkan nama ke bidang teks melalui item ***Nama***. Cobalah gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah mengenali pemindaian tersebut nanti dari jadwal lain.

Contoh: *Tidaklah tepat untuk memberi nama pemindaian dengan "Pemindaian baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang sebenarnya diperiksa oleh pemindaian tersebut. Sebaliknya, sebuah contoh nama deskriptif yang baik misalnya "Pemindaian area sistem", dll. Yang juga tidak perlu ditetapkan dalam nama pemindaian adalah apakah pemindaian itu untuk seluruh komputer atau pun hanya untuk pemindaian atas file atau folder yang dipilih – pemindaian Anda akan selalu menjadi versi spesifik dari pindai file atau folder yang dipilih.*

Dalam dialog ini, Anda dapat menentukan lebih lanjut parameter pemindaian berikut:

- ***Jadwal berjalan*** – menetapkan interval waktu untuk peluncuran pemindaian terjadwal yang baru. Penentuan waktu dapat ditentukan dengan pengulangan peluncuran pemindaian setelah periode waktu tertentu (***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada waktu tertentu ...***), atau mungkin dengan menentukan kejadian untuk mengaitkan peluncuran pemindaian dengan (***Tindakan berdasar pengaktifan komputer***).

- ***Opsi jadwal lanjutan*** – di bagian ini Anda dapat menentukan dalam kondisi apa pemindaian harus/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sama sekali.

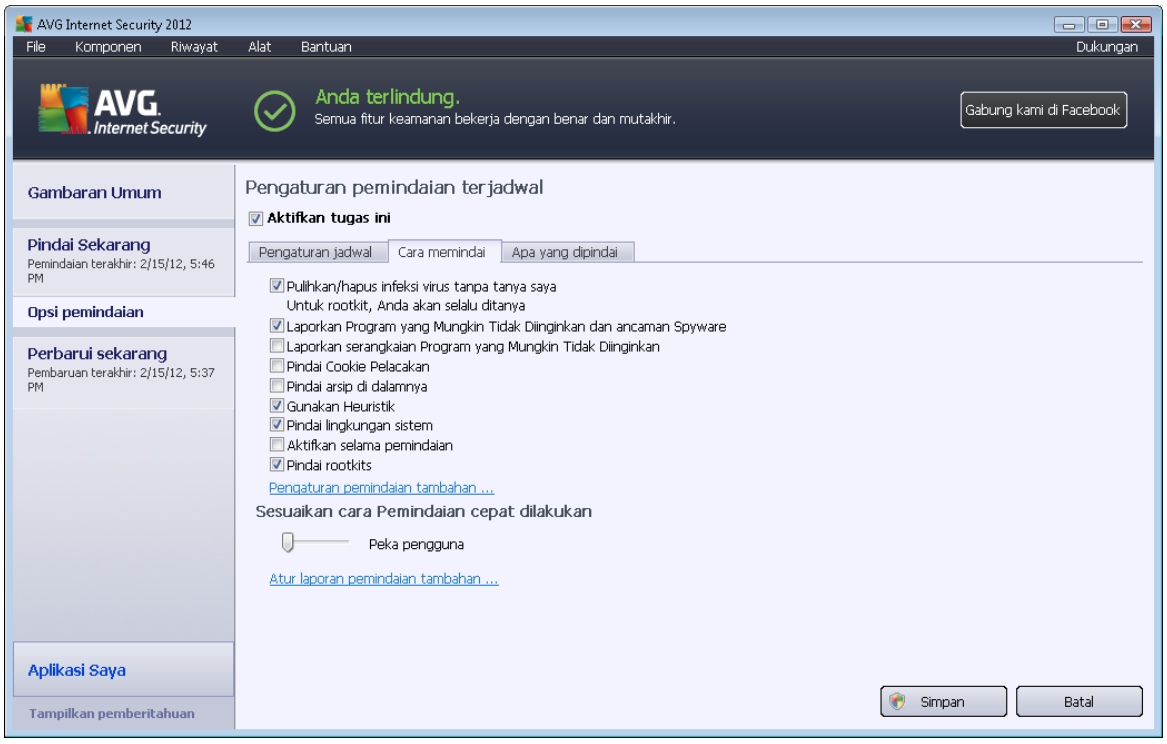
Tombol kontrol pada dialog Pengaturan pemindaian terjadwal

Ada dua tombol kontrol yang tersedia pada ketiga tab di dialog ***Pengaturan pemindaian terjadwal*** *(Pengaturan jadwal, Cara memindai, dan Apa yang dipindai)* dan semua ini mempunyai fungsionalitas yang sama, di tab apa pun saat itu Anda berada:

- ***Simpan*** – menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG. Dengan demikian, jika Anda ingin mengonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.

- ***Batalkan*** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG.

12.5.2. Cara Memindai



Pada tab ***Cara memindai*** Anda akan menemukan daftar parameter pemindaian yang secara opsional dapat diaktifkan/dinonaktifkan. Secara default, hampir semua parameter diaktifkan dan fungsionalitasnya diterapkan selama pemindaian. Kecuali Anda mempunyai alasan yang kuat untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditetapkan:

- ***Pulihkan / hapus infeksi virus tanpa bertanya pada saya*** (*diaktifkan secara default*): jika virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Seandainya file yang terinfeksi tidak dapat dipulihkan secara otomatis, atau jika Anda memutuskan untuk menonaktifkan opsi ini, Anda akan diberi tahu

saat deteksi virus dan harus memutuskan apa yang akan dilakukan dengan infeksi yang terdeteksi. Tindakan yang disarankan adalah menghapus file yang terinfeksi ke Gudang Virus.

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*): tandai untuk mengaktifkan mesin Anti-Spyware, dan memindai spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak sengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*): tandai kotak ini untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, namun dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai Cookie Pelacak*** (*dinonaktifkan secara default*): parameter komponen Anti-Spyware ini menetapkan bahwa cookie harus terdeteksi selama pemindaian (*(cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).

- ***Pindai di dalam arsip*** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut dikemas dalam suatu tipe arsip, misalnya, ZIP, RAR, ...

- ***Gunakan Heuristik*** (*diaktifkan secara default*): analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk mendeteksi virus selama pemindaian.

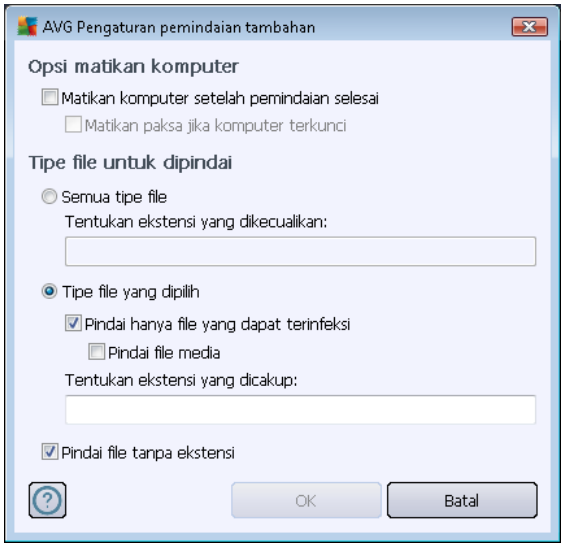
- ***Pindai lingkungan sistem*** (*diaktifkan secara default*): pemindaian juga akan memeriksa area sistem komputer Anda.

- ***Aktifkan pemindaian menyeluruh*** (*dinonaktifkan secara default*) – dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi virus atau exploit*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pindai rootkit*** (*diaktifkan secara default*): Pemindaian Anti-Rootkit menelusuri komputer Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Kemudian, Anda dapat mengubah konfigurasi pemindaian seperti berikut:

- ***Pengaturan pindai tambahan*** – tautan ini akan membuka dialog ***Pengaturan pindai tambahan*** di mana Anda dapat menentukan parameter berikut:



- ***Opsi matikan komputer*** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (***Matikan paksa jika komputer terkunci***).

- ***Tipe file untuk pemindaian*** – sselanjutnya Anda harus memutuskan apa yang ingin Anda pindai:

  - ***Semua tipe file*** dengan kemungkinan penetapan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai;

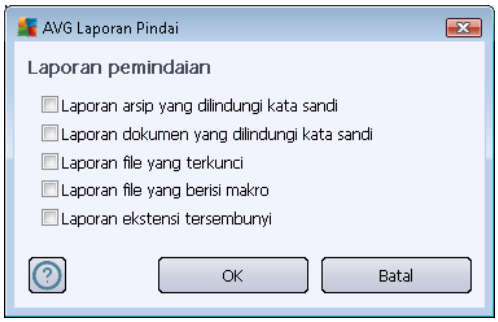
  - ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak ditandai, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

  - Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

- ***Sesuaikan secepat apa Pemindaian selesai*** - Anda dapat menggunakan penggeser untuk mengganti prioritas proses pemindaian. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Sebagai alternatif, Anda dapat menjalankan proses pemindaian lebih lambat yang berarti beban sumber daya sistem akan diminimumkan (*berguna saat Anda perlu menggunakan komputer tersebut namun Anda tidak peduli berapa lama pemindaian akan berlangsung*), atau lebih cepat dengan

kebutuhan sumber daya sistem yang bertambah (*misalnya saat komputer ditinggalkan untuk sementara*).

- ***Atur laporan pindai tambahan*** – tautan ini akan membuka dialog baru ***Laporan pindai*** di mana Anda dapat memilih kemungkinan tipe temuan apa saja yang harus dilaporkan:



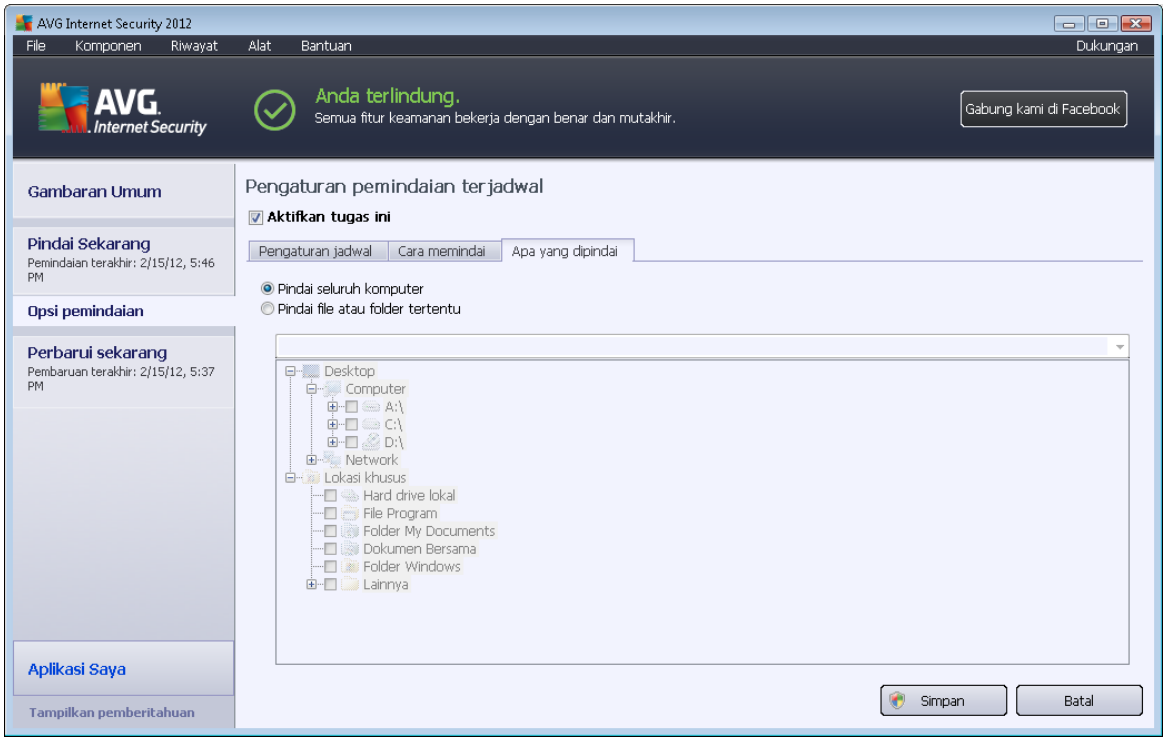
Tombol kontrol

Ada dua tombol kontrol yang tersedia pada ketiga tab di ***dialog*** Pengaturan pemindaian terjadwal *(Pengaturan jadwal, Cara memindai, dan Apa yang dipindai)* dan semua ini mempunyai fungsionalitas yang sama di tab apa pun saat itu Anda berada:

- ***Simpan*** – menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG. Dengan demikian, jika Anda ingin mengonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.

- ***Batalkan*** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG.

12.5.3. Apa yang Dipindai



Pada tab ***Apa yang dipindai*** Anda dapat menetapkan apakah Anda ingin menjadwalkan pemindaian seisi komputer atau pemindaian file atau folder.

Jika Anda memilih untuk memindai file atau folder tertentu, maka struktur yang ditampilkan di bagian bawah dialog ini akan diaktifkan dan Anda dapat menentukan folder yang akan dipindai (*perluas item dengan mengklik tanda plus hingga Anda menemukan folder yang ingin Anda pindai*). Anda dapat memilih beberapa folder dengan menandai kotaknya masing-masing. Folder yang dipilih akan ditampilkan dalam bidang teks di bagian atas dialog, dan menu buka-bawah akan menyimpan riwayat pemindaian yang Anda pilih untuk digunakan kemudian. Atau, masukkan jalur lengkap ke folder yang diinginkan secara manual (*jika memasukkan beberapa jalur, pisahkan dengan titik koma tanpa menambah spasi*).

Dalam struktur, Anda juga dapat melihat cabang ***Lokasi khusus***. Berikut ini, temukan daftar lokasi yang akan dipindai setelah kotaknya ditandai:

- ***Hard drive lokal*** – semua hard drive komputer Anda
- ***File program***
    - C:\Program Files\
    - *dalam versi 64-bit* C:\Program Files (x86)
- ***Folder My Documents***

- *untuk Win XP:* C:\Documents and Settings\Default User\My Documents\
- *untuk Windows Vista/7*: C:\Users\user\Documents\

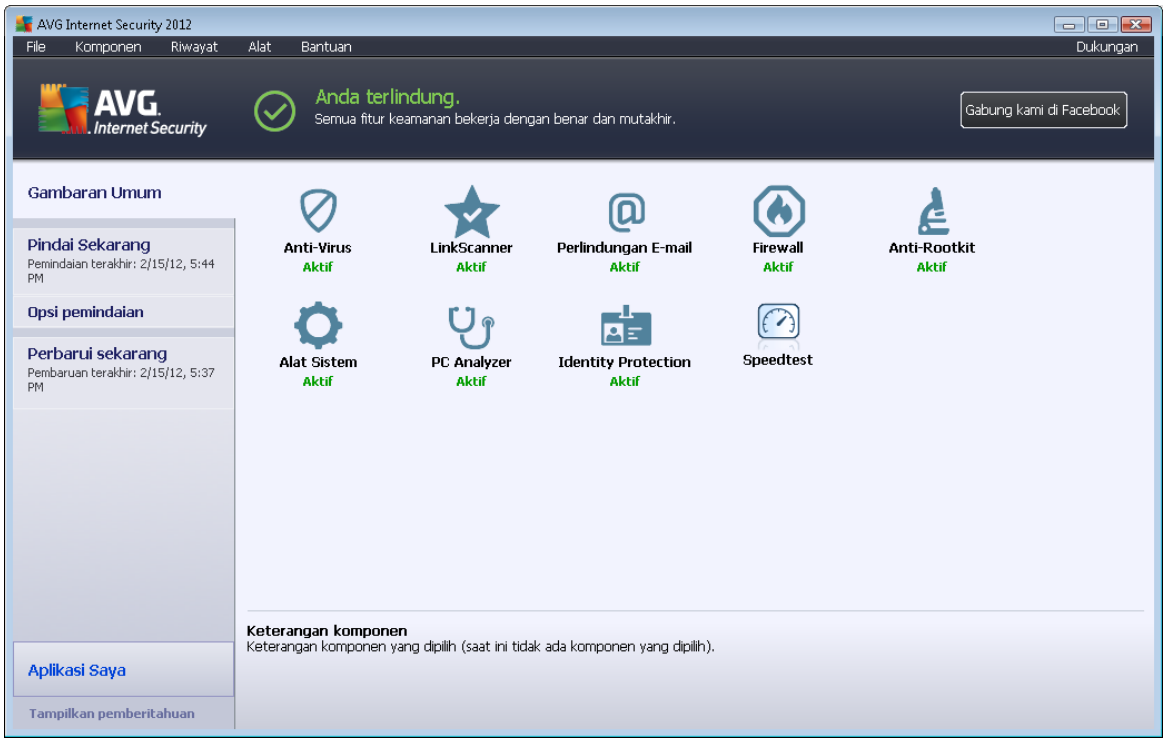
- ***Dokumen Bersama***
  - *untuk Win XP*: C:\Documents and Settings\All Users\Documents\
  - *untuk Windows Vista/7*: C:\Users\Public\Documents\
- ***Folder Windows*** – C:\Windows\
- ***Lainnya***
  - *Drive sistem* – hard drive tempat menginstal sistem operasi Anda (biasanya C:)
  - *Folder sistem* – C:\Windows\System32\
  - *Folder File Sementara* – C:\Documents and Settings\User\Local\ (*Windows XP*); atau C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *File Internet Sementara* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); atau C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Tombol kontrol

Dua tombol kontrol yang sama tersedia pada ketiga tab di dialog ***Pengaturan pemindaian terjadwal*** *(Pengaturan jadwal, Cara memindai, dan Apa yang dipindai)*:

- ***Simpan*** – menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG. Dengan demikian, jika Anda ingin mengonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.
- ***Batalkan*** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG.

12.6. Tinjauan Umum Hasil Pemindaian



Dialog ***Gambaran umum hasil pemindaian*** dapat diakses dari antarmuka pemindaian AVG melalui tombol ***Riwayat pemindaian***. Dialog ini menyediakan daftar semua pemindaian yang telah diluncurkan sebelumnya dan informasi mengenai statusnya:

- ***Nama*** – tujuan pemindaian; bisa berupa nama salah satu pemindaian yang ditentukan, atau nama yang Anda berikan pada pemindaian yang dijadwalkan sendiri. Setiap nama berisi ikon yang menunjukkan hasil pemindaian:

  – ikon hijau memberitahu ada infeksi terdeteksi selama pemindaian

  – ikon biru memberitahu ada infeksi terdeteksi selama pemindaian namun objek yang terinfeksi telah dihapus secara otomatis

  – ikon merah memberitahu ada infeksi terdeteksi selama pemindaian dan tidak dapat dihapus!

  Setiap ikon mungkin penuh atau terpotong separuh – ikon penuh menyatakan pemindaian telah dilakukan dan selesai dengan benar; ikon terpotong separuh berarti pemindaian dibatalkan atau terputus.

  Catatan: *Untuk informasi terperinci mengenai setiap pemindaian, lihat dialog Hasil Pemindaian yang dapat diakses melalui tombol Lihat perincian (di bagian bawah dialog ini).*

- ***Waktu mulai*** – tanggal dan waktu pemindaian diluncurkan

- ***Waktu selesai*** - tanggal dan waktu pemindaian selesai
- ***Objek yang diuji*** – jumlah objek yang telah diperiksa selama pemindaian
- ***Infeksi*** – jumlah infeksi virus yang terdeteksi/dihapus
- ***Spyware*** - jumlah spyware yang terdeteksi/dihapus
- ***Peringatan*** – jumlah objek mencurigakan
- ***Rootkit*** – jumlah rootkit
- ***Informasi log pemindaian*** - informasi yang berhubungan dengan tindakan dan hasil pemindaian (biasanya saat finalisasi atau interupsi)

Tombol kontrol

Tombol kontrol untuk dialog ***Gambaran umum hasil pemindaian*** adalah:

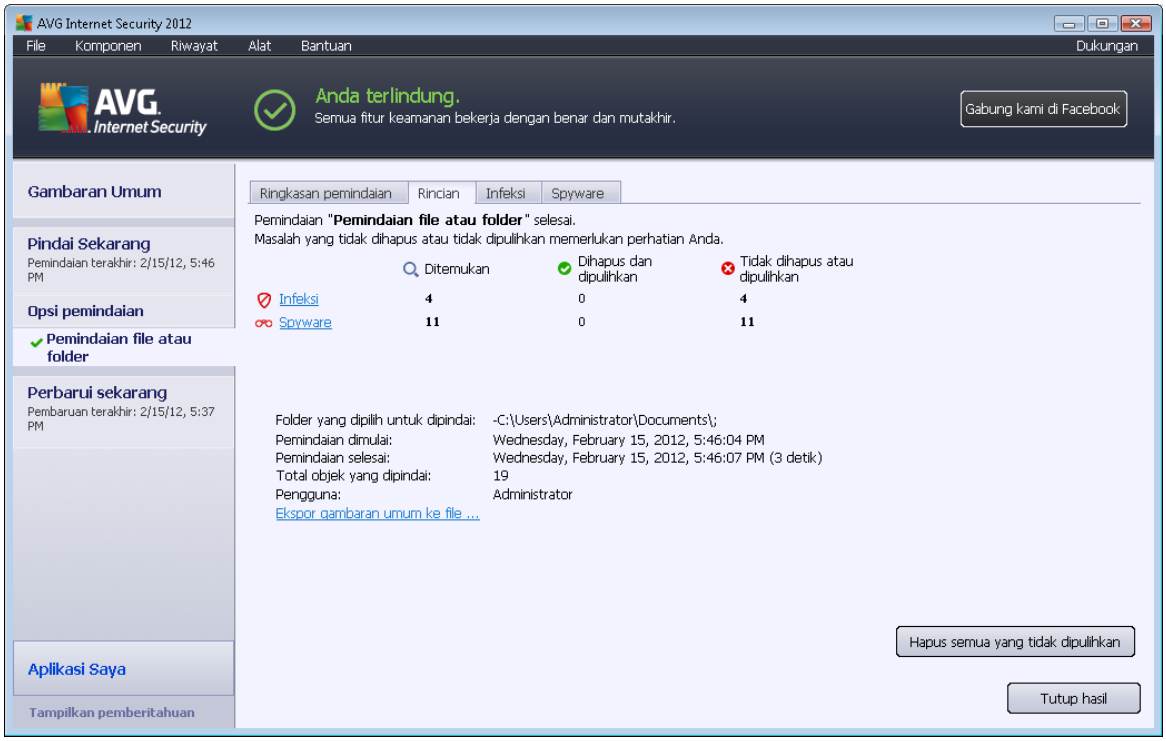
- ***Lihat perincian*** – tekan tombol ini untuk berpindah ke dialog Hasil pemindaian untuk melihat data terperinci mengenai pemindaian yang dipilih
- ***Hapus hasil*** – tekan untuk menghapus item yang dipilih dari tinjauan umum hasil pemindaian
- ***Kembali*** – mengembalikan ke dialog default antarmuka pemindaian AVG

12.7. Perincian Hasil Pemindaian

Jika dalam dialog Tinjauan Umum Hasil Pemindaian telah dipilih pemindaian tertentu, Anda nanti dapat mengklik tombol ***Lihat perincian*** untuk beralih ke dialog ***Hasil Pemindaian*** yang menyediakan data terperinci mengenai tindakan dan hasil pemindaian yang dipilih. Dialog dibagi ke dalam beberapa tab:

- Tinjauan Umum Hasil – tab ini ditampilkan terus dan menyediakan data statistik yang menerangkan kemajuan pemindaian
- Infeksi – tab ini hanya ditampilkan jika infeksi virus telah terdeteksi selama pemindaian
- Spyware – tab ini hanya ditampilkan jika spyware telah terdeteksi selama pemindaian
- Peringatan – tab ini ditampilkan jika, misalnya, cookie telah terdeteksi selama pemindaian
- Rootkit – tab ini hanya ditampilkan jika rootkit telah terdeteksi selama pemindaian
- Informasi – tab ini hanya ditampilkan jika beberapa kemungkinan ancaman telah terdeteksi namun tidak dapat dimasukkan sebagai salah satu dari kategori di atas; maka tab ini akan menyediakan pesan peringatan mengenai temuan tersebut. Selain itu, di sini Anda akan menemukan informasi mengenai objek yang tidak dapat dipindai *(misalnya arsip yang dilindungi kata sandi)*.

12.7.1. Tab Tinjauan Umum Hasil



Pada tab ***Hasil pemindaian*** Anda dapat menemukan statistik terperinci berisi informasi mengenai:

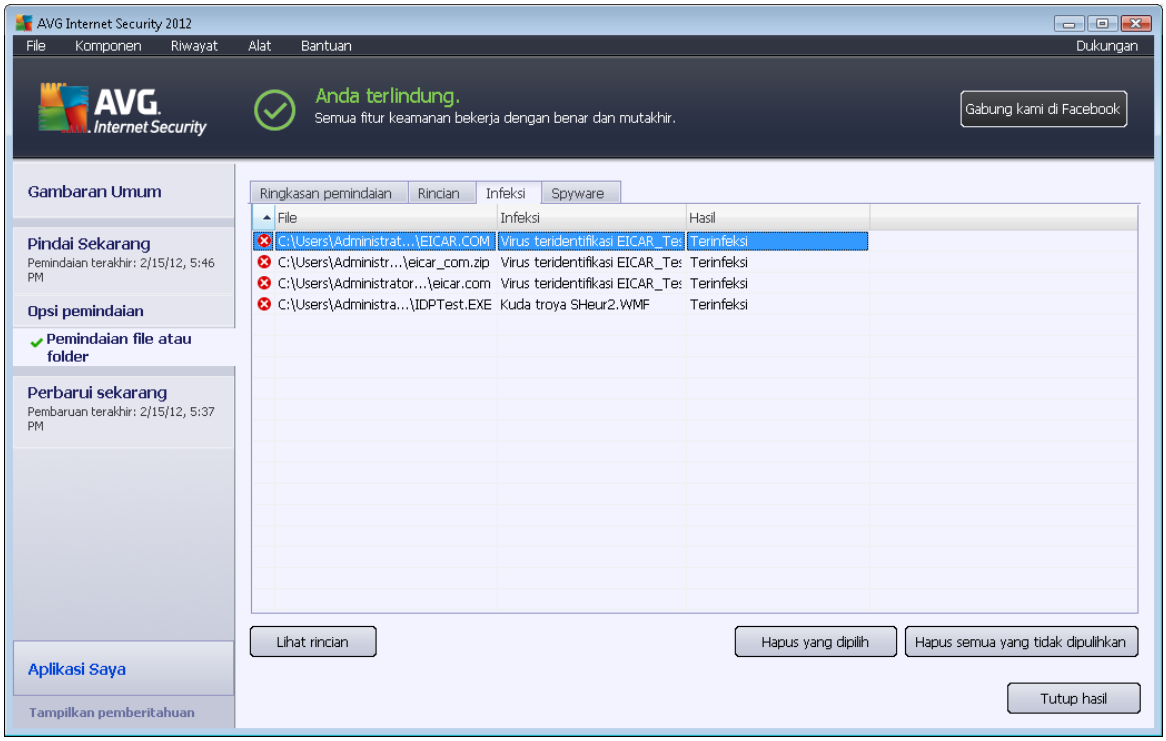
- infeksi virus / spyware yang terdeteksi
- infeksi virus / spyware yang dihapus
- jumlah infeksi virus / spyware yang tidak dapat dihapus atau dipulihkan

Selain itu, Anda akan menemukan informasi mengenai tanggal dan waktu yang pasti dari peluncuran pemindaian, jumlah total objek yang telah dipindai, durasi pemindaian dan jumlah kesalahan yang terjadi selama pemindaian.

Tombol kontrol

Hanya ada satu tombol kontrol yang tersedia dalam dialog ini. Tombol ***Tutup hasil*** mengembalikan ke dialog Tinjauan umum hasil pemindaian.

12.7.2. Tab Infeksi



Tab ***Infeksi*** hanya ditampilkan dalam dialog ***Hasil pemindaian*** jika infeksi virus terdeteksi selama pemindaian. Tab ini terdiri dari tiga bagian yang memberikan informasi berikut:

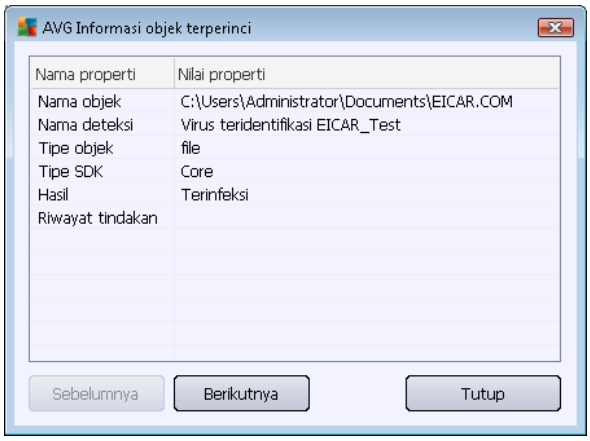
- ***File*** – jalur lengkap ke lokasi asli dari objek yang terinfeksi
- ***Infeksi*** - nama virus yang terdeteksi (*untuk perincian mengenai virus tertentu, lihatlah Ensiklopedia Virus online*)
- ***Hasil*** – menentukan status terkini dari objek terinfeksi yang terdeteksi selama pemindaian:
    - ***Terinfeksi*** - objek terinfeksi terdeteksi dan dibiarkan di lokasi aslinya (*misalnya, jika Anda telah menonaktifkan opsi pemulihan otomatis dalam pengaturan pemindaian tertentu*)
    - ***Dipulihkan*** - objek terinfeksi dipulihkan secara otomatis dan dibiarkan di lokasi aslinya
    - ***Dipindahkan ke Gudang Virus*** - objek yang terinfeksi telah dipindahkan ke karantina Gudang Virus
    - ***Dihapus*** - objek yang terinfeksi dihapus
    - ***Ditambahkan ke pengecualian PUP*** – temuan telah dievaluasi sebagai pengecualian dan telah ditambahkan ke daftar pengecualian PUP *(dikonfigurasi dalam dialog Pengecualian PUP pada pengaturan lanjutan)*

- ***File terkunci – belum diuji*** - objek yang bersangkutan telah dikunci sehingga AVG tidak dapat memindainya
- ***Objek yang mungkin berbahaya*** - objek telah terdeteksi sebagai objek yang mungkin berbahaya namun tidak terinfeksi (*ia bisa berisi makro, misalnya*); informasi harus diartikan sebagai peringatan saja
- ***Boot ulang diperlukan untuk menyelesaikan tindakan*** - objek yang terinfeksi tidak dapat dihapus, untuk menghapusnya Anda harus menghidupkan ulang komputer Anda

Tombol kontrol

Ada tiga tombol kontrol yang tersedia dalam dialog ini:

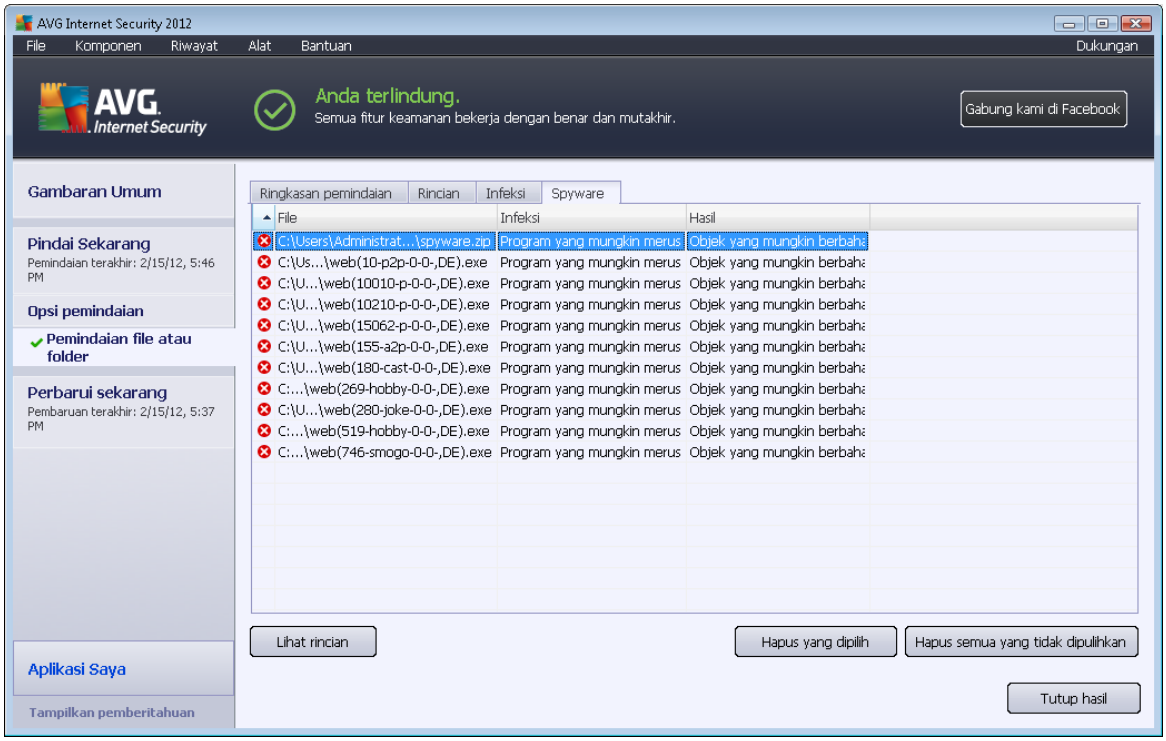
- ***Lihat perincian*** – tombol ini membuka jendela dialog baru bernama ***Perincian informasi objek***:



  Dalam dialog ini Anda dapat menemukan informasi terperinci tentang objek terinfeksi yang terdeteksi (*misalnya nama dan lokasi objek terinfeksi, tipe objek, tipe SDK, hasil deteksi dan riwayat tindakan terkait objek yang terdeteksi.*). Dengan menggunakan tombol ***Sebelumnya***/***Berikutnya*** Anda dapat melihat informasi mengenai temuan tertentu. Gunakan tombol ***Tutup*** untuk menutup dialog ini.

- ***Hapus yang dipilih*** – gunakan tombol ini untuk memindahkan temuan yang dipilih ke Gudang Virus
- ***Hapus semua yang tidak terpulihkan*** – tombol ini akan menghapus semua temuan yang tidak dapat dipulihkan atau dipindahkan ke Gudang Virus
- ***Tutup hasil*** - mengakhiri gambaran umum informasi terperinci dan mengembalikan ke dialog Gambaran umum hasil pemindaian

12.7.3. Tab Spyware



Tab ***Spyware*** hanya ditampilkan dalam dialog ***Hasil pemindaian*** jika spyware terdeteksi selama pemindaian. Tab ini terdiri dari tiga bagian yang memberikan informasi berikut:

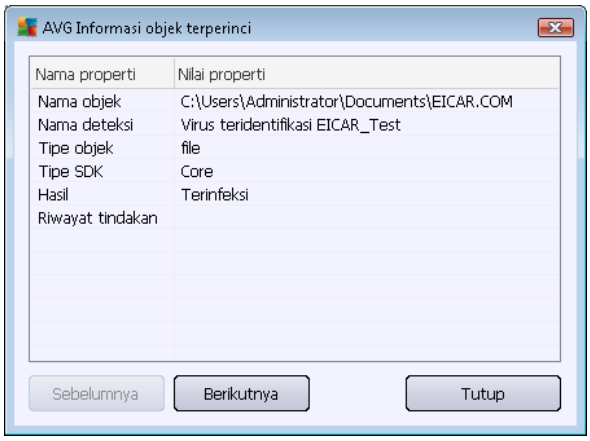
- ***File*** – jalur lengkap ke lokasi asli dari objek yang terinfeksi
- ***Infeksi*** – nama spyware *yang terdeteksi (untuk perincian mengenai virus tertentu, harap lihat di Ensiklopedia Virus online)*
- ***Hasil*** – menentukan status terkini dari objek yang terdeteksi selama pemindaian:
    - ***Terinfeksi*** – objek yang terinfeksi telah terdeteksi dan dibiarkan di lokasi aslinya *(misalnya, jika Anda telah menonaktifkan opsi pemulihan otomatis dalam pengaturan pemindaian tertentu)*
    - ***Dipulihkan***- objek terinfeksi yang dipulihkan secara otomatis dan dibiarkan di lokasi aslinya
    - ***Dipindahkan ke Gudang Virus*** - objek yang terinfeksi telah dipindahkan ke karantina Gudang Virus
    - ***Dihapus*** - objek yang terinfeksi dihapus
    - ***Ditambahkan ke pengecualian PUP*** – temuan telah dievaluasi sebagai pengecualian dan telah ditambahkan ke daftar pengecualian PUP *(dikonfigurasi dalam dialog Pengecualian PUP pada pengaturan lanjutan)*

- ***File terkunci – belum dites*** – objek yang bersangkutan telah dikunci sehingga AVG tidak dapat memindainya
- ***Objek yang mungkin berbahaya*** – objek telah terdeteksi sebagai objek yang mungkin berbahaya namun tidak terinfeksi (ia bisa berisi makro, misalnya); informasi ini peringatan saja
- ***Boot ulang diperlukan untuk menyelesaikan tindakan*** - objek yang terinfeksi tidak dapat dihapus, untuk menghapusnya Anda harus menghidupkan ulang komputer Anda

Tombol kontrol

Ada tiga tombol kontrol yang tersedia dalam dialog ini:

- ***Lihat perincian*** – tombol ini membuka jendela dialog baru bernama ***Perincian informasi objek***:



  Dalam dialog ini Anda dapat menemukan informasi terperinci tentang objek terinfeksi yang terdeteksi (*misalnya nama dan lokasi objek terinfeksi, tipe objek, tipe SDK, hasil deteksi dan riwayat tindakan terkait objek yang terdeteksi.*). Dengan menggunakan tombol ***Sebelumnya***/***Berikutnya*** Anda dapat melihat informasi mengenai temuan tertentu. Gunakan tombol ***Tutup*** untuk meninggalkan dialog ini.

- ***Hapus yang dipilih*** – gunakan tombol ini untuk memindahkan temuan yang dipilih ke Gudang Virus
- ***Hapus semua yang tidak terpulihkan*** – tombol ini akan menghapus semua temuan yang tidak dapat dipulihkan atau dipindahkan ke Gudang Virus
- ***Tutup hasil*** - mengakhiri tinjauan umum informasi terperinci dan mengembalikan ke dialog Tinjauan umum hasil pemindaian

12.7.4. Tab Peringatan

Tab ***Peringatan*** menampilkan informasi mengenai objek "dicurigai" (*biasanya berupa file*) yang terdeteksi selama pemindaian. Bila terdeteksi oleh Resident Shield, file ini akan diblokir agar tidak dapat diakses. Contoh umum temuan semacam ini adalah: file tersembunyi, cookie, kunci register yang mencurigakan, arsip atau dokumen yang dilindungi kata sandi, dll. File semacam itu tidak memberikan ancaman langsung apa pun pada komputer atau keamanan Anda. Informasi tentang file ini berguna jika ada adware atau spyware yang terdeteksi di komputer Anda. Jika dalam hasil pengujian **Keamanan Intenet AVG 2012** hanya mendeteksi Peringatan, maka tidak perlu dilakukan tindakan.

Berikut keterangan singkat tentang contoh umum objek semacam itu:

- ***File tersembunyi*** - File tersembunyi secara default tidak terlihat di Windows, dan beberapa virus atau ancaman lainnya mungkin mencoba menghindari deteksi dengan menyimpan filenya dengan atribut ini. Jika **Keamanan Intenet AVG 2012** melaporkan file tersembunyi yang Anda curigai jahat, Anda dapat memindahkannya ke Gudang Virus.
- ***Cookie*** – Cookie merupakan file teks biasa yang digunakan oleh situs Web untuk menyimpan informasi pengguna tertentu, yang kemudian digunakan untuk memuat layout situs Web khusus, nama pengguna yang diisikan sebelumnya, dsb.
- ***Kunci register mencurigakan*** - Beberapa malware menyimpan informasinya dalam register Windows, untuk memastikan bahwa informasi itu dimuat saat komputer diaktifkan atau untuk memperluas pengaruhnya pada sistem operasi.

12.7.5. Tab Rootkit

Tab ***Rootkit*** menampilkan informasi mengenai rootkit yang terdeteksi selama pemindaian anti-rootkit yang telah disertakan dalam Pemindaian Seisi Komputer.

Rootkit adalah program yang dirancang untuk mengambil alih kontrol utama pada sistem komputer, tanpa seizin pemilik sistem dan manajer yang berwenang. Akses ke perangkat keras jarang diperlukan karena rootkit dimaksudkan untuk mengambil kontrol sistem operasi yang berjalan pada perangkat keras tersebut. Biasanya, rootkit mengaburkan kehadirannya pada sistem dengan menyusup ke atau mengelakkan mekanisme keamanan sistem operasi standar. Seringkali, mereka juga berupa Trojan, yang memperdaya pengguna agar menganggapnya aman dijalankan pada sistem mereka. Berbagai teknik digunakan untuk melakukan hal ini termasuk merahasiakan proses yang sedang berjalan dari program pemantau, atau menyembunyikan file atau data sistem dari sistem operasi.

Struktur tab ini pada dasarnya sama seperti Tab Infeksi atau Tab Spyware.

12.7.6. Tab Informasi

Tab ***Informasi*** berisi data mengenai "temuan" yang tidak dapat dikategorikan sebagai infeksi, spyware, dll. Temuan tersebut tidak bisa dicap positif berbahaya namun tetap patut Anda perhatikan. Pemindaian **Keamanan Intenet AVG 2012** dapat mendeteksi file yang mungkin tidak terinfeksi, namun mencurigakan. File-file ini dilaporkan sebagai Peringatan, atau sebagai Informasi.

Informasi keseriusan dapat dilaporkan untuk salah satu alasan berikut:

- ***Kemasan run-time*** – File dikemas dengan salah satu pengemas run-time yang tidak umum, yang mungkin menunjukkan upaya untuk menghindari pemindaian file tersebut. Namun, tidak semua laporan file tersebut menunjukkan virus.

- ***Kemasan run-time rekursif*** – Serupa dengan di atas, namun lebih jarang di antara perangkat lunak umum. File tersebut mencurigakan dan penghapusan atau pengiriman untuk analisis harus dipertimbangkan.

- ***Arsip atau dokumen yang dilindungi kata sandi*** – File yang dilindungi kata sandi tidak dapat dipindai oleh **Keamanan Intenet AVG 2012** (*atau program anti-malware lain pada umumnya*).

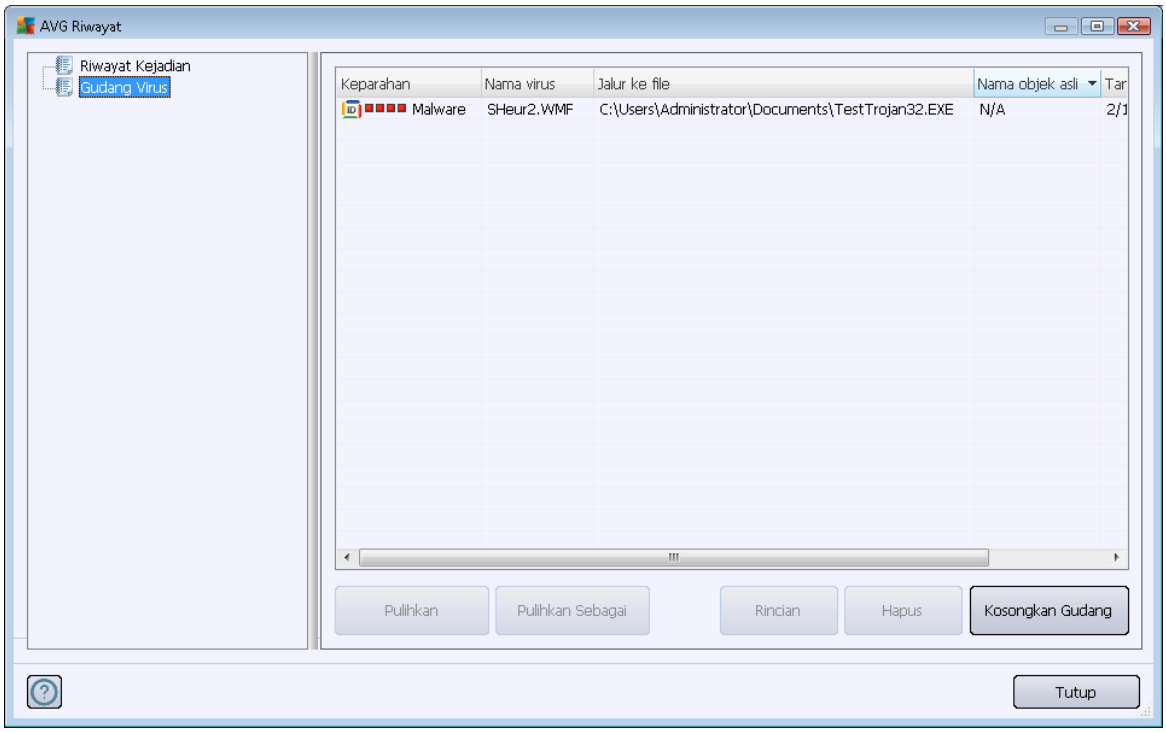
- ***Dokumen dengan makro*** – Dokumen yang dilaporkan berisi makro, yang mungkin jahat/ merusak.

- ***Ekstensi tersembunyi*** - File dengan ekstensi tersembunyi mungkin tampak seperti mis. gambar, tetapi sebenarnya file yang dapat dijalankan (*mis. gambar.jpg.exe*). Ekstensi kedua tidak terlihat dalam Windows secara default, dan **Keamanan Intenet AVG 2012** melaporkan file tersebut untuk mencegahnya dibuka tanpa sengaja.

- ***Jalur file yang tidak benar*** – Jika ada file sistem penting yang dijalankan selain dari jalur default (*mis. winlogon.exe dijalankan selain dari Folder windows*), **Keamanan Intenet AVG 2012** melaporkan perbedaan ini. Dalam beberapa kasus, virus menggunakan nama proses sistem standar agar kehadiran mereka pada sistem tidak mencurigakan.

- ***File terkunci*** – File yang dilaporkan terkunci, sehingga tidak dapat dipindai oleh **Keamanan Intenet AVG 2012**. Hal ini biasanya berarti bahwa beberapa file terus-menerus digunakan oleh sistem (*mis. file swap*).

12.8. Gudang Virus



Gudang Virus merupakan lingkungan aman untuk manajemen objek yang dicurigai/terinfeksi, yang terdeteksi selama tes AVG. Begitu objek yang terinfeksi telah terdeteksi selama pemindaian, dan AVG tidak dapat memulihkannya secara otomatis, Anda akan diminta untuk memutuskan apa yang harus dilakukan dengan objek yang dicurigai tersebut. Solusi yang disarankan adalah memindah objek tersebut ke ***Gudang Virus*** untuk penanganan lebih lanjut. Kegunaan utama ***Gudang Virus*** adalah menyimpan setiap file yang dihapus selama jangka waktu tertentu, sampai Anda benar-benar yakin tidak memerlukannya lagi di lokasi aslinya. Jika Anda menyadari bahwa hilangnya file menyebabkan masalah, Anda dapat mengirim file tersebut untuk dianalisis, atau mengembalikannya ke lokasi asli.

Antarmuka ***Gudang Virus*** membuka jendela tersendiri dan menyediakan gambaran umum informasi mengenai objek terinfeksi yang telah dikarantina:

- ***Keseriusan*** – jika Anda memutuskan untuk menginstal komponen Identity Protection dalam **Keamanan Intenet AVG 2012** Anda, maka identifikasi grafis dari keseriusan temuan dengan skala empat tingkat mulai dari dapat diterima (■□□□) hingga sangat berbahaya (■■■■) akan disediakan di bagian ini; dan informasi mengenai tipe infeksi (*berdasarkan tingkat infeksinya – semua objek yang disebutkan dapat positif terinfeksi atau mungkin terinfeksi*)

- ***Nama Virus*** – menentukan nama infeksi yang terdeteksi sesuai dengan Ensiklopedia Virus *(online)*

- ***Jalur ke file*** – jalur lengkap ke lokasi asli file infeksi yang terdeteksi

- ***Nama objek asli*** – semua objek terdeteksi yang tercantum dalam bagan telah diberi label dengan nama standar yang diberikan oleh AVG selama proses pemindaian. Seandainya objek mempunyai nama asli tertentu yang dikenal (*misalnya nama lampiran e-mail yang tidak mencerminkan isi sesungguhnya dari lampiran tersebut*), ia akan tersedia dalam kolom ini.

- ***Tanggal penyimpanan*** – tanggal dan waktu file yang dicurigai terdeteksi dan dipindahkan ke Gudang Virus

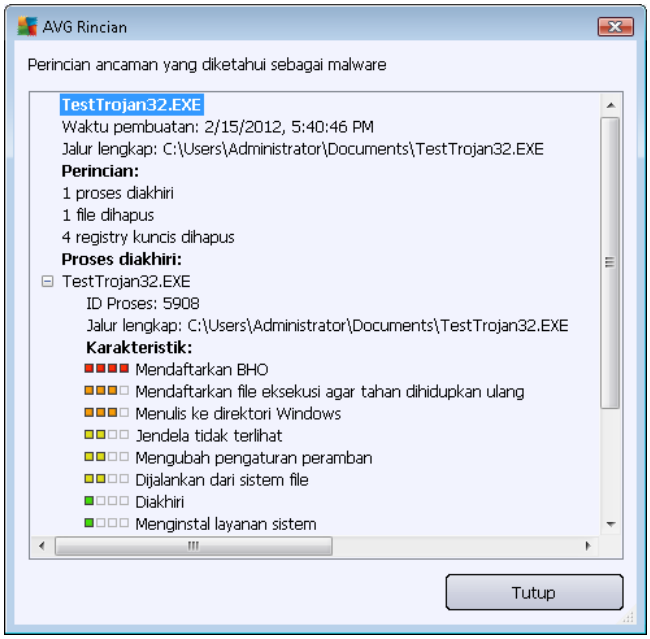
Tombol kontrol

Tombol kontrol berikut dapat diakses dari antarmuka ***Gudang Virus***:

- ***Pulihkan*** - mengembalikan file yang terinfeksi ke lokasi aslinya pada disk Anda

- ***Pulihkan Sebagai*** – memindai file yang terinfeksi ke folder yang dipilih

- ***Perincian*** – tombol ini hanya berlaku untuk ancaman yang dideteksi oleh Identity Protection. Jika diklik, tombol ini akan menampilkan gambaran umum secara singkat tentang perincian ancaman (*file/proses yang terinfeksi, karakteristik proses, dll.*). Perhatikan bahwa untuk semua item lain yang dideteksi oleh selain IDP, tombol ini akan berwarna abu-abu dan tidak aktif!



- ***Hapus*** – menghapus sama sekali file yang terinfeksi dari ***Gudang Virus*** dan tidak akan dapat dikembalikan

- ***Kosongkan Gudang*** – menghapus sama sekali semua isi ***Gudang Virus***. Dengan menghapus file dari ***Gudang Virus***, maka file tersebut akan dihapus dari disk dan tidak akan dapat dikembalikan (*tidak dipindahkan ke Recycle Bin*).

13. Pembaruan AVG

Tidak ada perangkat lunak keamanan yang dapat menjamin perlindungan sesungguhnya dari berbagai tipe ancaman, kecuali jika rutin diperbarui! Penulis virus selalu mencari kelemahan baru yang dapat mereka eksploitir dalam perangkat lunak maupun sistem operasi. Virus baru, malware baru, serangan peretas baru muncul setiap hari. Karena alasan ini, vendor perangkat lunak terus mengeluarkan pembaruan dan penambal keamanan, untuk memperbaiki berbagai lubang keamanan yang ditemukan.

Mengingat semua ancaman komputer baru yang merebak, dan kecepatan penyebarannya, sangatlah penting untuk memperbarui **Keamanan Intenet AVG 2012** Anda secara rutin. Solusi terbaik adalah membiarkan pengaturan default program di mana pembaruan otomatis telah dikonfigurasi. Harap diingat bahwa jika basis data virus **Keamanan Intenet AVG 2012** Anda tidak diperbarui, program tidak akan dapat mendeteksi ancaman terbaru!

Sangatlah penting memperbarui AVG Anda secara rutin! Pembaruan definisi virus penting harus dilakukan setiap hari jika memungkinkan. Pembaruan program yang kurang penting bisa dilakukan setiap minggu.

13.1. Peluncuran pembaruan

Untuk memberikan keamanan maksimum, **Keamanan Intenet AVG 2012** secara default dijadwalkan untuk mencari pembaruan baru setiap empat jam. Karena pembaruan AVG tidak dirilis berdasarkan jadwal tetap, tapi disesuaikan dengan reaksi terhadap jumlah dan keseriusan ancaman baru, pemeriksaan ini sangat penting untuk memastikan basis data virus AVG selalu up-to-date.

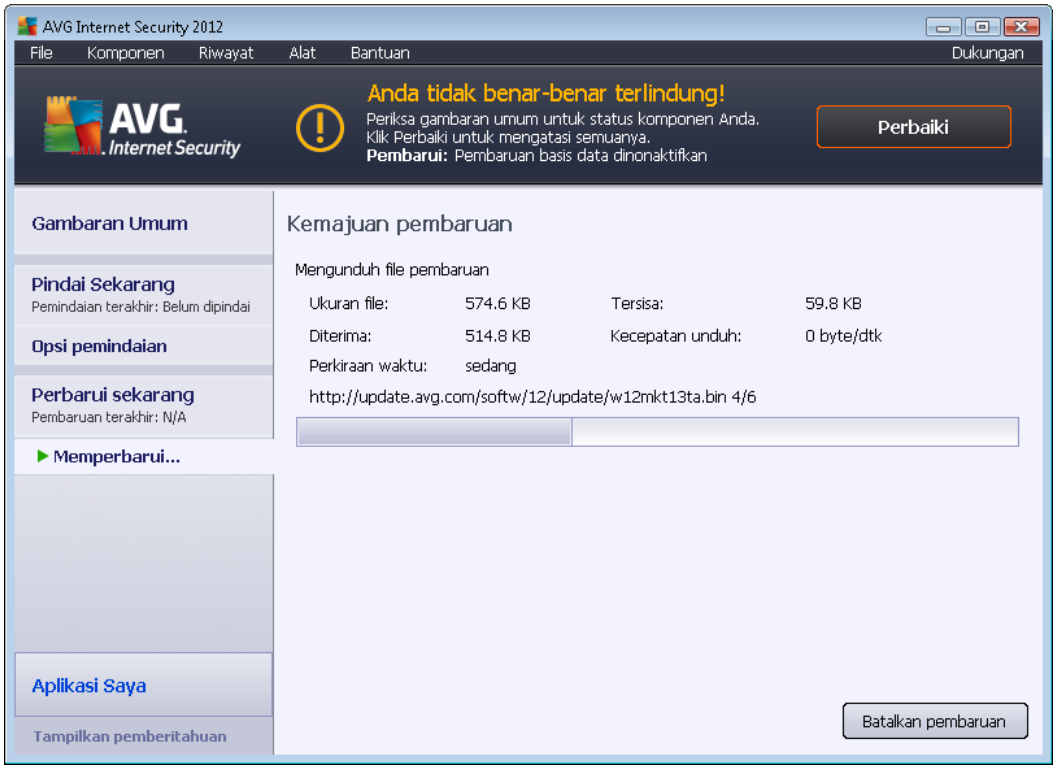
Jika ingin mengurangi jumlah peluncuran pembaruan, Anda dapat mengatur sendiri parameter peluncuran pembaruan. Walau demikian, sangatlah disarankan untuk meluncurkan pembaruan setidaknya sekali sehari! Konfigurasi dapat diedit di bagian Pengaturan lanjutan/Jadwal, khususnya dalam dialog berikut:

- Jadwal pembaruan definisi
- Jadwal pembaruan program
- Jadwal pembaruan Anti-Spam

Jika Anda ingin memeriksa file pembaruan baru dengan segera, gunakan tautan cepat Perbarui sekarang dalam antarmuka pengguna utama. Tautan ini selalu tersedia dari dialog antarmuka pengguna mana saja.

13.2. Kemajuan pembaruan

Begitu Anda memulai pembaruan, AVG akan memverifikasi terlebih dahulu apakah ada file pembaruan baru yang tersedia. Jika ya, **Keamanan Intenet AVG 2012** akan mulai mengunduhnya dan meluncurkan proses pembaruannya. Selama proses pembaruan, Anda akan dialihkan ke antarmuka ***Perbarui*** tempat Anda dapat melihat progres proses dalam bentuk grafis serta gambaran umum parameter statistik yang relevan *(ukuran file pembaruan, data yang diterima, kecepatan unduh, waktu yang dilalui, ...)*:



***Catatan**: Sebelum peluncuran pembaruan program AVG, akan dibuat titik pemulihan sistem. Seandainya proses pembaruan gagal dan sistem operasi crash, Anda selalu dapat memulihkan sistem operasi ke konfigurasi aslinya dari titik ini. Opsi ini dapat diakses melalui menu Windows: Start / All Programs / Accessories / System tools / System Restore. Hanya disarankan untuk pengguna yang berpengalaman!*

13.3. Tingkat pembaruan

Keamanan Intenet AVG 2012 menyediakan dua tingkat pembaruan untuk dipilih:

- ***Pembaruan definisi*** berisi perubahan yang diperlukan agar perlindungan anti-virus, anti-spam dan anti-malware tetap bisa diandalkan. Biasanya, ini tidak termasuk segala perubahan pada kode dan hanya memperbarui basis data definisi. Pembaruan ini akan diterapkan begitu tersedia.

- ***Pembaruan program*** berisi beragam perubahan program, perbaikan dan peningkatan.

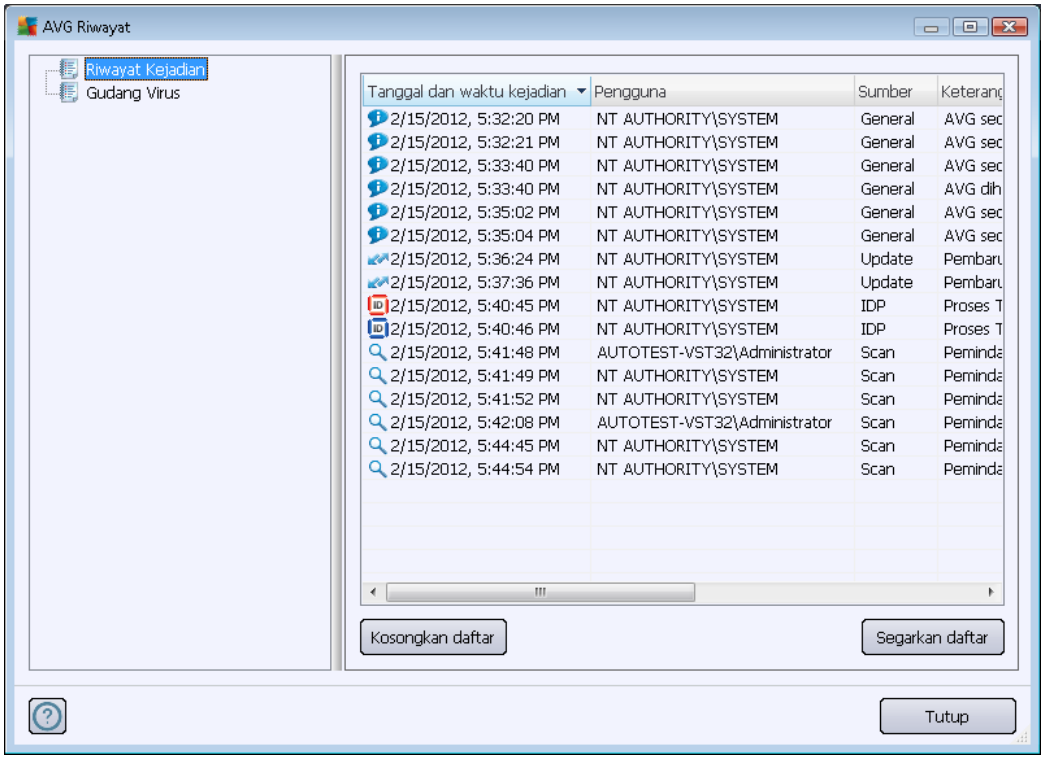
Saat menjadwalkan pembaruan, Anda dapat menetapkan parameter tertentu bagi kedua tingkat pembaruan:

- Jadwal pembaruan definisi

- Jadwal pembaruan program

***Catatan:** Jika terjadi konflik waktu antara pembaruan program terjadwal dan pemindaian terjadwal, maka proses pembaruan akan lebih diprioritaskan dan pemindaian akan disela.*

14. Riwayat Kejadian



Dialog ***Riwayat*** dapat diakses dari menu sistem melalui item ***Riwayat/Log Riwayat Kejadian***. Dalam dialog ini Anda dapat menemukan ringkasan kejadian penting yang terjadi selama operasi **Keamanan Intenet AVG 2012**. ***Riwayat*** merekam tipe kejadian berikut:

- Informasi tentang pembaruan aplikasi AVG
- Informasi mengenai pemindaian mulai, selesai atau berhenti (*termasuk tes yang dilakukan secara otomatis*)
- Informasi mengenai kejadian yang berhubungan dengan deteksi virus (*oleh Resident Shield atau pemindaian*) termasuk lokasi kejadian
- Kejadian penting lainnya

Untuk setiap kejadian, tercantum informasi berikut:

- ***Tanggal dan waktu kejadian*** menunjukkan tanggal dan waktu persis kejadian
- ***Pengguna*** menampilkan nama pengguna yang saat itu login pada saat kejadian
- ***Sumber*** memberikan informasi mengenai komponen sumber atau bagian lain dari sistem AVG yang memicu kejadian tersebut
- ***Keterangan kejadian*** berisi ringkasan apa yang sebenarnya terjadi

Tombol kontrol

- ***Kosongkan daftar*** – tekan tombol untuk menghapus semua entri dalam daftar kejadian
- ***Segarkan daftar*** – tekan tombol untuk memperbarui semua entri dalam daftar kejadian

15. Tanya-Jawab dan Dukungan Teknis

Seandainya Anda mempunyai kesulitan dalam hal penjualan atau teknis dengan aplikasi **Keamanan Intenet AVG 2012** Anda, ada sejumlah cara untuk mencari bantuan. Harap pilih dari opsi berikut ini:

- ***Dapatkan Dukungan***: Tepat dalam aplikasi AVG, Anda dapat mengunjungi halaman dukungan pelanggan khusus pada situs Web AVG (http://www.avg.com/). Pilih item menu utama ***Bantuan / Dapatkan Dukungan*** untuk dialihkan ke situs Web AVG dengan fasilitas dukungan yang tersedia. Untuk melanjutkan, harap ikuti petunjuk di halaman Web.

- ***Dukungan (tautan menu utama)***: Menu aplikasi AVG (*di bagian atas antarmuka pengguna utama*) berisi tautan ***Dukungan*** yang akan membuka dialog baru berisi semua jenis informasi yang mungkin Anda perlukan saat mencoba menemukan bantuan. Dialog ini berisi data dasar mengenai program AVG yang telah Anda instal (*program / versi basis data*), perincian lisensi, dan daftar tautan dukungan cepat:

- ***Pemecahan masalah dalam file bantuan***: Bagian ***Pemecahan masalah*** baru tersedia langsung di file bantuan yang telah disertakan dalam **Keamanan Intenet AVG 2012** *(untuk membuka file bantuan, tekan tombol F1 di setiap dialog pada aplikasi)*. Bagian ini menyediakan daftar situasi yang paling sering terjadi bila pengguna ingin mencari bantuan profesional untuk masalah teknis. Harap pilih situasi yang paling mirip dengan masalah Anda, dan klik untuk membuka petunjuk terperinci yang mengarahkan pada solusi masalah.

- ***Pusat Dukungan Situs Web AVG***: Atau, Anda dapat mencari solusi bagi masalah Anda pada situs Web AVG (http://www.avg.com/). Di bagian ***Pusat Dukungan*** Anda dapat menemukan tinjauan umum terstruktur atas grup tema yang menyangkut masalah penjualan dan teknis.

- ***Pertanyaan yang sering diajukan***: Pada situs Web AVG (http://www.avg.com/) Anda juga dapat menemukan bagian terstruktur terpisah dan menyatu atas pertanyaan yang sering diajukan. Bagian ini dapat diakses melalui opsi menu ***Pusat Dukungan/Tanya-Jawab***. Sekali lagi, semua pertanyaan terbagi rapi dalam kategori penjualan, teknis, dan virus.

- ***Tentang virus & ancaman***: Bab khusus mengenai situs Web AVG (http://www.avg.com/) dikhususkan untuk masalah virus *(halaman Web ini dapat diakses dari menu utama melalui opsi Bantuan / Tentang Virus dan Ancaman)*. Dalam menu, pilih ***Pusat Dukungan/ Tentang virus & ancaman*** untuk masuk ke halaman yang menyediakan tinjauan umum terstruktur atas informasi yang berhubungan dengan ancaman online. Anda juga dapat menemukan petunjuk tentang cara menghapus virus, spyware, dan nasihat mengenai cara agar tetap terlindungi.

- ***Forum diskusi***: Anda juga dapat menggunakan forum diskusi pengguna AVG di http://forums.avg.com.