



Keamanan Internet AVG 2011

Panduan Pengguna

Revisi dokumen 2011.21 (16.5.2011)

Hak cipta AVG Technologies CZ, s.r.o. Semua hak dilindungi undang-undang.
Semua merek dagang lain adalah hak milik dari pemiliknya masing-masing.

Produk ini menggunakan Algoritma MD5 Message-Digest RSA Data Security, Inc., Hak cipta (C) 1991-2, RSA Data Security, Inc. Diciptakan 1991.

Produk ini menggunakan kode dari pustaka C-SaCzech, Hak cipta (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Produk ini menggunakan pustaka kompresi zlib, Hak cipta (c) 1995-2002 Jean-loup Gailly dan Mark Adler.

Produk ini menggunakan pustaka kompresi libbz2, Hak cipta (c) 1996-2002 Julian R. Seward.



Daftar Isi

1. Pendahuluan	8
2. Persyaratan Instalasi AVG	9
2.1 Sistem Operasi yang Didukung	9
2.2 Persyaratan PK Minimum & yang Disarankan	9
3. Opsi Instalasi AVG	10
4. Proses Instalasi AVG	11
4.1 Selamat Datang	11
4.2 Aktifkan Lisensi AVG Anda	12
4.3 Pilih tipe instalasi	13
4.4 Opsi Khusus	14
4.5 Instal AVG Security Toolbar	15
4.6 Kemajuan Instalasi	16
4.7 Instalasi berhasil	16
5. Setelah Instalasi	18
5.1 Pendaftaran produk	18
5.2 Akses ke antarmuka pengguna	18
5.3 Pemindaian seluruh komputer	18
5.4 Tes Eicar	18
5.5 Konfigurasi default AVG	19
6. Antarmuka Pengguna AVG	20
6.1 Menu Sistem	21
6.1.1 File	21
6.1.2 Komponen	21
6.1.3 Riwayat	21
6.1.4 Alat	21
6.1.5 Bantuan	21
6.2 Info Status Keamanan	24
6.3 Tautan Cepat	25
6.4 Gambaran Umum Komponen	25
6.5 Statistik	27
6.6 Ikon Baki Sistem	27
6.7 Gadget AVG	28



7. Komponen AVG	31
7.1 Anti-Virus	31
7.1.1 Prinsip-Prinsip Anti-Virus	31
7.1.2 Antarmuka Anti-Virus	31
7.2 Anti-Spyware	32
7.2.1 Prinsip-Prinsip Anti-Spyware	32
7.2.2 Antarmuka Anti-Spyware	32
7.3 Anti-Spam	34
7.3.1 Prinsip-Prinsip Anti-Spam	34
7.3.2 Antarmuka Anti-Spam	34
7.4 Firewall	35
7.4.1 Prinsip-Prinsip Firewall	35
7.4.2 Profil Firewall	35
7.4.3 Antarmuka Firewall	35
7.5 Link Scanner	39
7.5.1 Prinsip-Prinsip Link Scanner	39
7.5.2 Antarmuka Link Scanner	39
7.5.3 Search-Shield	39
7.5.4 Surf-Shield	39
7.6 Perisai Tetap	43
7.6.1 Prinsip-Prinsip Perisai Tetap	43
7.6.2 Antarmuka Perisai Tetap	43
7.6.3 Deteksi Perisai Tetap	43
7.7 Family Safety	48
7.8 AVG LiveKive	48
7.9 Pemindai E-mail	48
7.9.1 Prinsip-Prinsip Pemindai E-mail	48
7.9.2 Antarmuka Pemindai E-mail	48
7.9.3 Deteksi Pemindai E-mail	48
7.10 Pengatur Pembaruan	52
7.10.1 Prinsip-Prinsip Pengatur Pembaruan	52
7.10.2 Antarmuka Pengatur Pembaruan	52
7.11 Lisensi	54
7.12 Administrasi Jarak Jauh	55
7.13 Online Shield	56
7.13.1 Prinsip-Prinsip Online Shield	56
7.13.2 Antarmuka Online Shield	56



7.13.3 Deteksi Online Shield	56
7.14 Anti-Rootkit	59
7.14.1 Prinsip-Prinsip Anti-Rootkit	59
7.14.2 Antarmuka Anti-Rootkit	59
7.15 Alat Sistem	61
7.15.1 Proses	61
7.15.2 Koneksi Jaringan	61
7.15.3 Mulai otomatis	61
7.15.4 Ekstensi Peramban	61
7.15.5 Penampil LSP	61
7.16 PC Analyzer	67
7.17 Perlindungan ID	68
7.17.1 Prinsip-Prinsip Perlindungan ID	68
7.17.2 Antarmuka Perlindungan ID	68
7.18 Security Toolbar	70
8. AVG Security Toolbar	72
8.1 Antarmuka AVG Security Toolbar	72
8.1.1 Tombol logo AVG	72
8.1.2 Kotak telusur yang didukung AVG Secure Search (powered by Google)	72
8.1.3 Status Halaman	72
8.1.4 Berita AVG	72
8.1.5 Berita	72
8.1.6 Hapus Riwayat	72
8.1.7 Pemberitahu E-mail	72
8.1.8 Info Cuaca	72
8.1.9 Facebook	72
8.2 Opsi AVG Security Toolbar	79
8.2.1 Tab Umum	79
8.2.2 Tab Tombol yang Berguna	79
8.2.3 Tab Keamanan	79
8.2.4 Tab Opsi Lanjutan	79
9. Pengaturan Lanjutan AVG	84
9.1 Tampilan	84
9.2 Suara	86
9.3 Abaikan Kondisi Kerusakan	88
9.4 Perlindungan Identitas	89
9.4.1 Pengaturan Perlindungan Identitas	89



9.4.2 Daftar yang Diperbolehkan	89
9.5 Gudang Virus	93
9.6 Pengecualian PUP	93
9.7 Anti-Spam	95
9.7.1 Pengaturan	95
9.7.2 Performa	95
9.7.3 RBL	95
9.7.4 Daftar Putih	95
9.7.5 Daftar Hitam	95
9.7.6 Pengaturan Lanjutan	95
9.8 Online Shield	106
9.8.1 Perlindungan Web	106
9.8.2 Perpesanan Instan	106
9.9 Link Scanner	110
9.10 Pemindaian	111
9.10.1 Pindai Seisi Komputer	111
9.10.2 Pemindaian Ekstensi Shell	111
9.10.3 Pindai File atau Folder Tertentu	111
9.10.4 Pemindaian Perangkat Eksternal	111
9.11 Jadwal	116
9.11.1 Pemindaian Terjadwal	116
9.11.2 Jadwal Pembaruan Basis Data Virus	116
9.11.3 Jadwal Pembaruan Program	116
9.11.4 Jadwal Pembaruan Anti-Spam	116
9.12 Pemindai E-mail	127
9.12.1 Sertifikasi	127
9.12.2 Pemfilteran E-mail	127
9.12.3 Server	127
9.13 Perisai Tetap	136
9.13.1 Pengaturan Lanjutan	136
9.13.2 Item yang dikecualikan	136
9.14 Server Cache	140
9.15 Anti-Rootkit	141
9.16 Perbarui	142
9.16.1 Proxy	142
9.16.2 Dial-up	142
9.16.3 URL	142
9.16.4 Atur	142



9.17 Menonaktifkan perlindungan AVG untuk sementara	149
9.18 Program Peningkatan Produk	149
10. Pengaturan Firewall	152
10.1 Umum	152
10.2 Keamanan	153
10.3 Profil Area dan Adaptor	154
10.4 IDS	155
10.5 Log	157
10.6 Profil	159
11. Pemindaian AVG	161
11.1 Antarmuka Pemindaian	161
11.2 Pemindaian Yang Ditetapkan	162
11.2.1 Pemindaian Seisi Komputer	162
11.2.2 Pindai File atau Folder Tertentu	162
11.2.3 Pemindaian Anti-Rootkit	162
11.3 Memindai dalam Windows Explorer	172
11.4 Pemindaian Baris Perintah	173
11.4.1 Parameter Pemindaian CMD	173
11.5 Penjadwalan Pemindaian	175
11.5.1 Pengaturan Jadwal	175
11.5.2 Cara Memindai	175
11.5.3 Apa yang Dipindai	175
11.6 Gambaran Umum Hasil Pemindaian	185
11.7 Perincian Hasil Pemindaian	186
11.7.1 Tab Gambaran Umum Hasil	186
11.7.2 Tab Infeksi	186
11.7.3 Tab Spyware	186
11.7.4 Tab Peringatan	186
11.7.5 Tab Rootkit	186
11.7.6 Tab Informasi	186
11.8 Gudang Virus	193
12. Pembaruan AVG	196
12.1 Tingkat Pembaruan	196
12.2 Tipe Pembaruan	196
12.3 Proses Pembaruan	196



13. Riwayat Kejadian	198
14. Tanya-Jawab dan Dukungan Teknis	200



1. Pendahuluan

Panduan pengguna ini memberikan dokumentasi yang komprehensif untuk **Keamanan Intenet AVG 2011**.

Selamat atas pembelian Keamanan Intenet AVG 2011!

Keamanan Intenet AVG 2011 adalah salah satu jajaran produk AVG peraih penghargaan yang dirancang untuk memberi Anda ketenangan pikiran dan keamanan total untuk PC Anda. Sebagaimana dengan semua produk AVG, **Keamanan Intenet AVG 2011** telah dirancang ulang sepenuhnya, dari nol, untuk mewujudkan perlindungan keamanan AVG yang telah terkenal dan diakui dengan cara baru yang lebih mudah digunakan dan efisien. Produk **Keamanan Intenet AVG 2011** Anda yang baru memiliki antarmuka praktis yang digabungkan dengan pemindaian yang lebih agresif dan lebih cepat. Makin banyak fitur keamanan yang dibuat otomatis demi kepraktisan Anda, dan berbagai opsi pengguna baru yang 'cerdas' telah disertakan sehingga Anda dapat menyesuaikan berbagai fitur keamanan dengan gaya hidup Anda. Tidak ada lagi kemudahan penggunaan yang dikorbankan demi keamanan!

AVG telah dirancang dan dikembangkan untuk melindungi aktivitas komputer dan jaringan Anda. Nikmati pengalaman perlindungan penuh dari AVG.

Semua penawaran produk AVG

- Perlindungan yang relevan dengan cara Anda menggunakan komputer dan Internet: perbankan dan berbelanja, meramban dan menelusur, mengobrol dan mengirim email, atau mengunduh file dan jejaring sosial - AVG memiliki produk perlindungan yang tepat untuk Anda
- Perlindungan tanpa kerepotan yang dipercayai lebih dari 11 juta orang di seluruh dunia dan dimotori oleh jaringan global periset berpengalaman tinggi.
- Perlindungan yang dijaga oleh dukungan ahli setiap waktu



2. Persyaratan Instalasi AVG

2.1. Sistem Operasi yang Didukung

Keamanan Intenet AVG 2011 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 [Perlindungan ID](#) tidak didukung pada Windows XP x64. Pada sistem operasi ini Anda dapat menginstal Keamanan Intenet AVG 2011 tetapi tanpa komponen IDP.

2.2. Persyaratan PK Minimum & yang Disarankan

Persyaratan perangkat keras minimum untuk **Keamanan Intenet AVG 2011**:

- Intel Pentium CPU 1,5 GHz
- memori RAM 512 MB
- Ruang kosong hard drive 750 MB (untuk keperluan instalasi)

Persyaratan perangkat keras yang disarankan untuk **Keamanan Intenet AVG 2011**:

- Intel Pentium CPU 1,8 GHz
- memori RAM 512 MB
- Ruang kosong hard drive 1400 MB (untuk keperluan instalasi)



3. Opsi Instalasi AVG

AVG dapat diinstal dari file instalasi yang tersedia pada CD instalasi Anda, atau Anda dapat mengunduh file instalasi terbaru dari situs Web AVG (<http://www.avg.com/>).

Sebelum Anda mulai menginstal AVG, kami sangat menyarankan agar Anda mengunjungi situs Web AVG (<http://www.avg.com/>) untuk memeriksa file instalasi baru. Dengan cara ini dipastikan Anda menginstal versi terbaru Keamanan Internet AVG 2011.

Selama proses instalasi, Anda akan ditanya nomor lisensi/penjualan. Pastikan Anda menyiapkannya sebelum memulai instalasi. Nomor penjualan dapat ditemukan pada kemasan CD. Jika Anda telah membeli salinan AVG secara online, nomor lisensi Anda akan dikirimkan melalui e-mail.



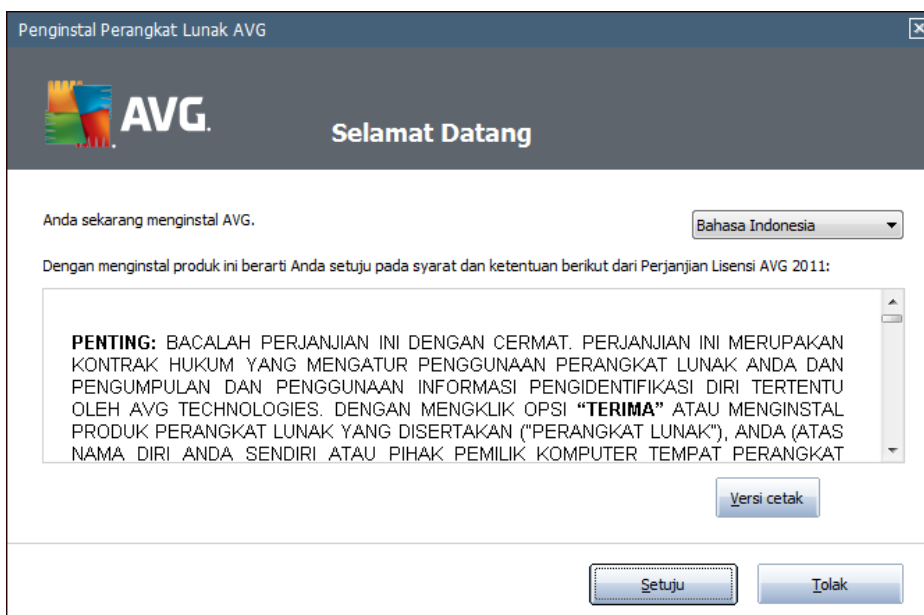
4. Proses Instalasi AVG

Untuk menginstal **Keamanan Internet AVG 2011** pada komputer Anda, Anda perlu mendapatkan file instalasi terbaru. Anda dapat menggunakan file instalasi dari CD yang menjadi bagian dari edisi kemasan Anda namun file ini mungkin kedaluwarsa. Karenanya kami sarankan untuk mendapatkan file instalasi terbaru secara online. Anda dapat mengunduh file dari situs web AVG (<http://www.avg.com/>), di bagian [Pusat Dukungan / Unduh](#).

Instalasi adalah rangkaian jendela dialog yang berisi keterangan singkat mengenai apa yang dilakukan di setiap langkah. Berikut ini, kami menyediakan penjelasan untuk setiap jendela dialog:

4.1. Selamat Datang

Proses instalasi dimulai dengan jendela dialog **Selamat Datang**. Di sini Anda dapat memilih bahasa yang digunakan dalam proses instalasi, dan bahasa default yang digunakan antarmuka pengguna AVG. Pada bagian atas jendela dialog temukan menu buka bawah dengan daftar bahasa yang Anda dapat pilih dari:



Perhatian: Di sini, Anda memilih bahasa hanya untuk proses instalasi. Bahasa yang Anda pilih akan diinstal sebagai bahasa default untuk antarmuka pengguna AVG, selain bahasa Inggris yang diinstal secara otomatis. Jika Anda ingin menginstal bahasa tambahan lainnya untuk antarmuka pengguna, harap tentukan dalam salah satu dialog pengaturan berikut bernama [Opsi Khusus](#).

Selanjutnya, dialog memberikan teks lengkap perjanjian lisensi AVG. Harap dibaca dengan saksama. 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.



4.2. Aktifkan Lisensi AVG Anda

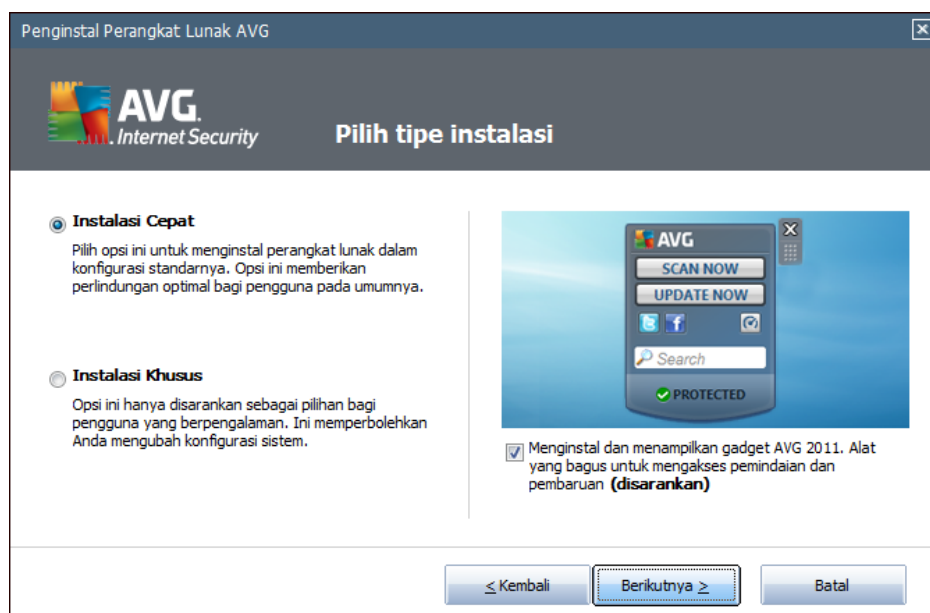
Dalam dialog **Aktifkan Lisensi Anda**, Anda diminta untuk memasukkan nomor lisensi ke dalam bidang teks yang disediakan.

Nomor penjualan dapat ditemukan pada kemasan CD di kotak **Keamanan Internet AVG 2011** Anda. Nomor lisensi ada dalam email konfirmasi yang telah Anda terima setelah membeli **Keamanan Internet AVG 2011** 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.

Tekan tombol **Berikutnya** untuk melanjutkan proses instalasi.



4.3. Pilih tipe instalasi



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

Untuk sebagian besar pengguna, sangat disarankan untuk tetap menggunakan **Instalasi Cepat** standar yang akan menginstal AVG dalam mode otomatis penuh bersama pengaturan yang telah ditetapkan oleh vendor program. 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 AVG. Jika Anda sudah memilih opsi **Instalasi Cepat**, tekan tombol **Berikutnya** untuk melanjutkan ke dialog [Instal AVG Security Toolbar](#) berikutnya.

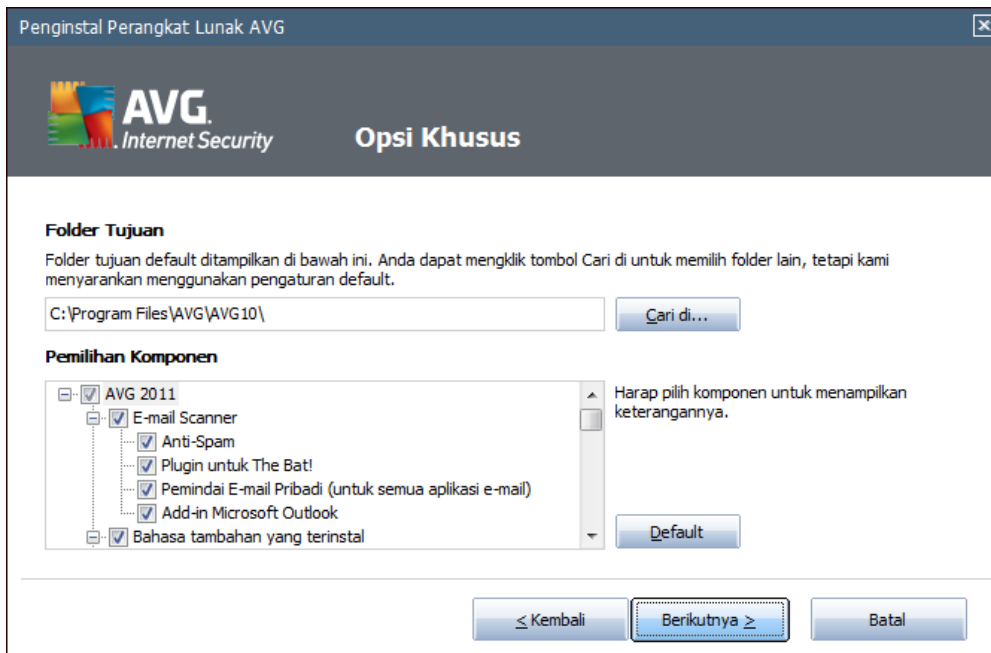
Instalasi Khusus hanya boleh digunakan oleh pengguna berpengalaman dengan alasan yang sah untuk menginstal AVG dengan pengaturan non-standar, misalnya, agar pas dengan persyaratan sistem tertentu. Setelah memilih opsi ini, tekan tombol **Berikutnya** untuk melanjutkan ke dialog [Opsi Khusus](#).

Di bagian kanan dialog, Anda dapat menemukan kotak centang terkait dengan [Gadget AVG](#) (yang didukung pada Windows Vista/Windows 7). Jika Anda ingin menginstal gadget, tandai kotak tersebut. [Gadget AVG](#) kemudian akan dapat diakses dari Bilah Sisi Windows jika Anda segera mengakses fitur terpenting pada **Keamanan Internet AVG 2011**, yaitu. [pemindaian](#) dan [pembaruan](#).



4.4. Opsi Khusus

Dialog **Opsi Khusus** memungkinkan Anda menentukan dua parameter instalasi:



Folder Tujuan

Dalam bagian dialog **Folder Tujuan** Anda dapat menentukan lokasi tempat **Keamanan Internet AVG 2011** akan diinstal. Secara default, AVG akan diinstal ke folder Program Files yang berada di drive C:. Jika Anda ingin mengubah lokasi ini, gunakan tombol **Jelajah** untuk menampilkan struktur drive, dan pilih foldernya.

Pemilihan Komponen

Bagian **Pemilihan Komponen** menampilkan gambaran umum mengenai semua komponen **Keamanan Internet AVG 2011** 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, silakan baca bab [Gambaran Singkat Komponen](#) dalam dokumentasi ini. Untuk kembali ke konfigurasi default yang ditentukan sebelumnya oleh vendor perangkat lunak, gunakan tombol **Default**.

Tekan tombol **Berikutnya** untuk melanjutkan.



4.5. 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 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 menjelajahi 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.



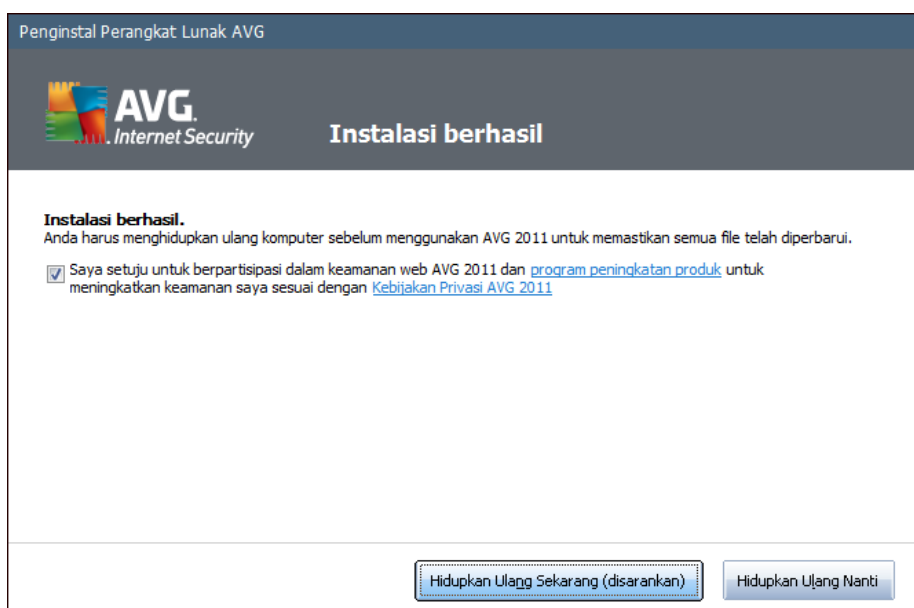
4.6. Kemajuan Instalasi

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



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

4.7. Instalasi berhasil





Dialog **Instalasi berhasil** mengonfirmasi bahwa **Keamanan Internet AVG 2011** Anda telah terinstal lengkap dan dikonfigurasi.

Dalam dialog ini, silakan sediakan informasi kontak Anda sehingga Anda dapat menerima semua informasi dan berita terkait produk. Di bawah formulir registrasi, Anda akan menemukan dua opsi berikut:

- ***Ya, kabari saya tentang berita keamanan dan penawaran khusus AVG 2011 melalui email*** - tandai kotak centang ini untuk menyatakan Anda ingin diberitahu tentang apa yang baru dalam dunia keamanan internet dan ingin menerima informasi tentang penawaran khusus, perbaikan dan peningkatan produk AVG.
- ***Saya setuju untuk berpartisipasi dalam keamanan Web AVG 2011 dan Program Peningkatan Produk ...*** - tandai kotak ini jika Anda ingin berpartisipasi dalam Program Peningkatan Produk (untuk perincian lihat bab [Pengaturan Lanjutan / Program Peningkatan Produk AVG](#)) yang menghimpun semua informasi anonim tentang ancaman yang terdeteksi untuk dapat meningkatkan keseluruhan tingkat keamanan Internet.

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

Catatan: Jika menggunakan lisensi bisnis AVG, dan dalam hal ini Anda sebelumnya memilih untuk menginstal fungsi Administrasi Jarak Jauh (lihat [Opsi Khusus](#)), dialog Instalasi berhasil akan muncul dengan antarmuka berikut:

Anda perlu menentukan parameter AVG DataCenter - harap berikan string koneksi ke AVG DataCenter dalam bentuk `server:port`. Jika saat ini informasi tersebut tidak tersedia, biarkan bidang ini kosong dan Anda dapat mengatur konfigurasinya nanti di dalam dialog **Pengaturan Lanjutan / Administrasi Jarak Jauh**. Untuk informasi terperinci mengenai AVG Remote Administration, harap baca panduan pengguna AVG Business Edition; dapat diunduh dari situs Web AVG (<http://www.avg.com/>).



5. Setelah Instalasi

5.1. Pendaftaran produk

Setelah menyelesaikan instalasi **Keamanan Internet AVG 2011**, daftarkan produk Anda secara online pada situs web AVG (<http://www.avg.com/>), di halaman **Pendaftaran** (*ikuti petunjuk yang diberikan langsung pada halaman ini*). Setelah pendaftaran, Anda akan mendapatkan akses penuh ke Akun pengguna AVG, berita Pembaruan AVG, dan layanan lain yang disediakan khusus untuk pengguna terdaftar.

5.2. Akses ke antarmuka pengguna

[Antarmuka Pengguna AVG](#) dapat diakses dengan beberapa cara:

- klik dua kali [ikon baki sistem AVG](#)
- klik dua kali ikon AVG di desktop
- klik dua kali baris status yang berada di bagian bawah [Gadget AVG](#) (*jika terinstal; didukung pada Windows Vista/ Windows 7*)
- dari menu **Start/ Programs/AVG 2011/Antarmuka Pengguna AVG**
- dari [AVG Security Toolbar](#) via opsi **Luncurkan AVG**

5.3. Pemindaian seluruh komputer

Ada kemungkinan risiko bahwa virus komputer telah terkirim ke komputer Anda sebelum instalasi **Keamanan Internet AVG 2011**. Karena alasan ini, Anda harus menjalankan [Pindai seluruh komputer](#) untuk memastikan tidak ada infeksi di PC Anda.

Untuk petunjuk tentang menjalankan [Pindai seluruh komputer](#) bacalah bab [Pemindaian AVG](#).

5.4. Tes Eicar

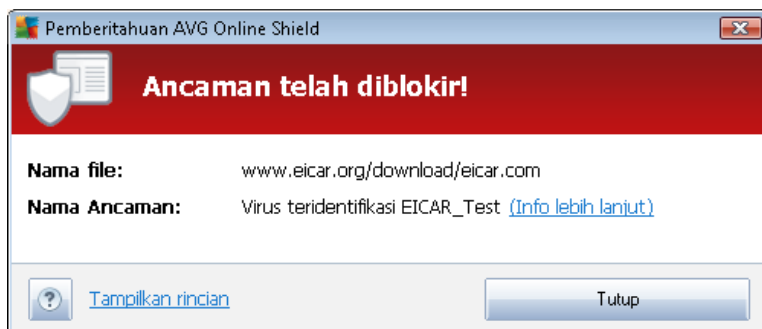
Untuk mengkonfirmasi bahwa **Keamanan Internet AVG 2011** telah diinstal dengan benar, Anda dapat menjalankan tes EICAR.

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](#) 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 [Perisai Tetap](#) mendeteksi 'virus' karena Anda mencoba membukanya. **Jika AVG gagal mengenali file tes EICAR sebagai virus, Anda harus memeriksa lagi konfigurasi program!**

5.5. Konfigurasi default AVG

Konfigurasi default (yakni cara aplikasi diatur tepat setelah instalasi) **Keamanan Internet AVG 2011** telah diatur oleh vendor perangkat lunak sehingga semua komponen dan fungsi telah disesuaikan untuk mencapai performa optimal.

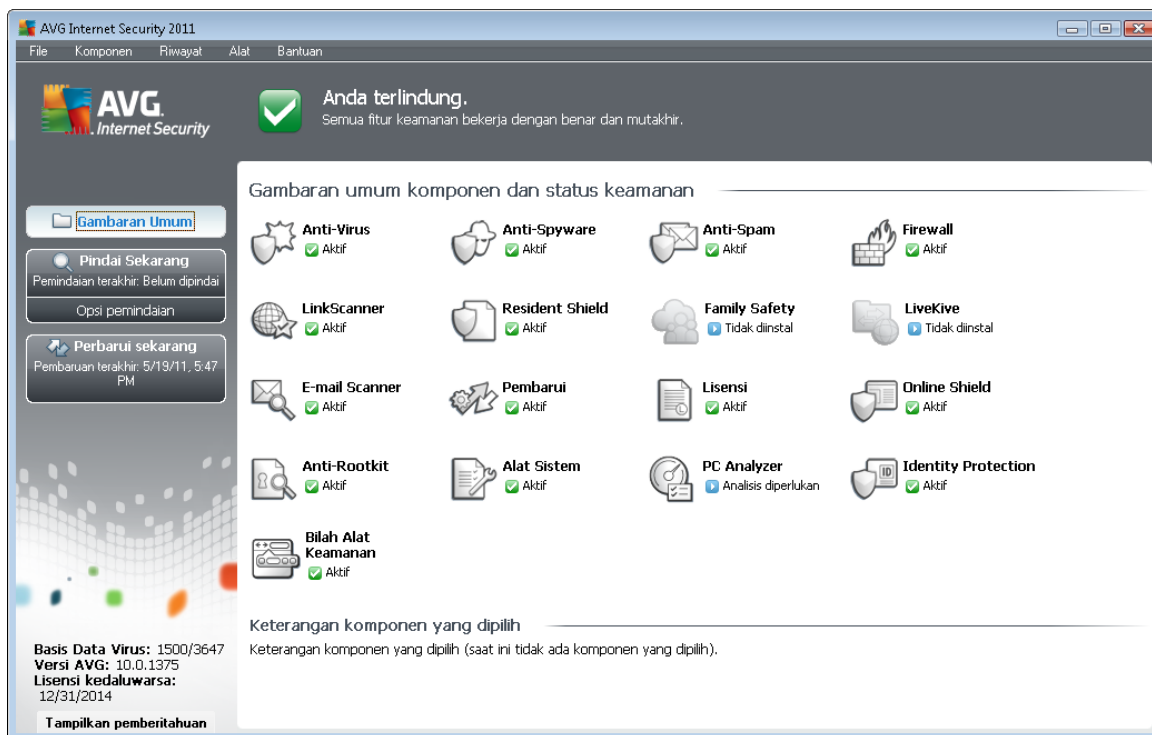
Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG! Perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman.

Beberapa pengeditan kecil pada pengaturan [Komponen AVG](#) dapat diakses langsung dari antarmuka pengguna komponen tertentu. Jika Anda merasa perlu mengubah konfigurasi AVG agar lebih pas dengan kebutuhan Anda, buka [Pengaturan Lanjutan AVG](#): pilih item menu sistem **Alat/ Pengaturan lanjutan** dan edit konfigurasi AVG dalam dialog [Pengaturan Lanjutan AVG](#) yang baru dibuka.



6. Antarmuka Pengguna AVG

Keamanan Internet AVG 2011 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 AVG - [perincian >>](#)
- **Info Status Keamanan** (bagian atas jendela) memberi Anda informasi mengenai status terkini dari program AVG - [perincian >>](#)
- **Tautan Cepat** (bagian kiri jendela) memungkinkan Anda mengakses cepat berbagai tugas AVG yang paling penting dan paling sering digunakan - [perincian >>](#)
- **Gambaran Umum Komponen** (bagian tengah jendela) memberikan gambaran umum mengenai semua komponen AVG yang terinstal - [perincian >>](#)
- **Statistik** (bagian kiri bawah jendela) memberi Anda semua data statistik menyangkut operasi program - [perincian >>](#)
- **Ikon Baki Sistem** (sudut kanan bawah monitor, pada baki sistem) menunjukkan status terkini AVG - [perincian >>](#)
- **Gadget AVG** (Bilah sisi Windows, didukung dalam Windows Vista/7), memungkinkan akses cepat ke pemindaian dan pembaruan AVG - [perincian >>](#)



6.1. Menu Sistem

Menu sistem adalah navigasi standar yang digunakan dalam semua aplikasi Windows. Tombol diletakkan secara horizontal di bagian paling atas jendela utama **Keamanan Internet AVG 2011**. Gunakan menu sistem untuk mengakses komponen, fitur dan layanan AVG tertentu.

Menu sistem dibagi ke dalam lima bagian:

6.1.1. File

- **Keluar** - menutup antarmuka pengguna **Keamanan Internet AVG 2011**. Walau demikian, aplikasi AVG akan terus berjalan di latar belakang dan komputer Anda tetap terlindungi!

6.1.2. Komponen

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

- **Gambaran umum sistem** - beralih ke dialog antarmuka pengguna default berisi [gambaran umum semua komponen yang terinstal dan statusnya](#)
- **Anti-Virus** memastikan bahwa komputer Anda terlindung dari berbagai virus yang mencoba memasuki komputer Anda - [perincian >>](#)
- **Anti-Spyware** memastikan bahwa komputer Anda terlindungi dari spyware dan adware - [perincian >>](#)
- **Anti-Spam** memeriksa semua pesan e-mail masuk dan menandai e-mail yang tidak diinginkan sebagai SPAM - [perincian >>](#)
- **Firewall** mengontrol cara komputer Anda bertukar data dengan Internet atau jaringan lokal - [perincian >>](#)
- **Link Scanner** memeriksa hasil telusur yang ditampilkan dalam peramban Internet Anda - [perincian >>](#)
- **Pemindai E-mail** memeriksa adanya virus pada semua e-mail yang masuk dan keluar - [perincian >>](#)
- **Family Safety** membantu memantau aktivitas online anak Anda dan melindunginya dari konten situs Web yang tidak pantas - [perincian >>](#)
- **LiveKive** menyediakan pencadangan otomatis atas data Anda secara online - [perincian >>](#)
- **Perisai Tetap** berjalan di latar belakang dan memindai file saat disalin, dibuka atau disimpan - [perincian >>](#)
- **Pengatur Pembaruan** mengontrol semua pembaruan AVG - [perincian >>](#)
- **Lisensi** menampilkan nomor lisensi, tipe dan tanggal kedaluwarsa - [perincian >>](#)



- **Online Shield** memindai semua data yang akan diunduh oleh peramban Web - [perincian >>](#)
- **Anti-Rootkit** mendeteksi berbagai program dan teknologi yang mencoba menyamarkan malware - [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 >>](#)
- **Perlindungan Identitas** - komponen anti-malware berfokus untuk mencegah pencuri identitas mencuri harta digital pribadi Anda - [perincian >>](#)
- **Security Toolbar** memungkinkan Anda menggunakan fungsionalitas AVG yang dipilih, langsung dari peramban Internet Anda - [perincian >>](#)
- **Remote Administration** hanya ditampilkan dalam AVG Business Edition jika Anda telah menentukannya saat [proses instalasi](#) agar komponen ini diinstal

6.1.3. Riwayat

- **Hasil pemindaian** - beralih ke antarmuka pengetesan AVG, tepatnya ke dialog [Gambaran Umum Hasil Pemindaian](#)
- **Deteksi Perisai Tetap** - membuka dialog berisi gambaran umum mengenai ancaman yang terdeteksi oleh [Perisai Tetap](#)
- **Deteksi Pemindai E-mail** - membuka dialog berisi gambaran umum mengenai lampiran pesan e-mail yang terdeteksi sebagai ancaman oleh komponen [Pemindai E-mail](#)
- **Temuan Online Shield** - membuka dialog berisi gambaran umum mengenai ancaman yang terdeteksi oleh [Online Shield](#)
- **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 gambaran umum semua tindakan **Keamanan Internet AVG 2011** yang telah tercatat dalam log
- **Firewall** - membuka antarmuka pengaturan Firewall pada tab [Log](#) yang berisi gambaran umum terperinci mengenai semua tindakan Firewall

6.1.4. Alat

- **Pindai komputer** - beralih ke [antarmuka pemindaian AVG](#) dan meluncurkan pemindaian seisi komputer.
- **Pindai folder yang dipilih** - beralih ke [antarmuka pemindaian AVG](#) dan memungkinkan



Anda menetapkan file dan folder mana yang harus dipindai dalam struktur komputer Anda.

- **Pindai file** - memungkinkan Anda menjalankan pengujian saat diperlukan terhadap satu file yang dipilih dari struktur pada disk Anda.
- **Perbarui** - secara otomatis meluncurkan proses pembaruan **Keamanan Internet AVG 2011**.
- **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** di mana Anda dapat mengedit konfigurasi **Keamanan Internet AVG 2011**. Umumnya, disarankan untuk tetap menggunakan pengaturan default aplikasi sebagaimana ditetapkan oleh vendor perangkat lunak.
- **Pengaturan Firewall** - membuka dialog mandiri untuk konfigurasi lanjutan komponen **Firewall**.

6.1.5. Bantuan

- **Daftar Isi** - membuka file bantuan AVG
- **Dapatkan Bantuan Online** - 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 dalam dialog **Personalisasi AVG** pada **proses instalasi**. Dalam dialog ini Anda dapat memasukkan nomor lisensi untuk menggantikan 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/>). Masukkan data pendaftaran Anda; hanya pelanggan yang mendaftarkan produk AVG mereka yang dapat menerima dukungan teknis gratis.

Catatan: Jika menggunakan versi uji coba **Keamanan Internet AVG 2011**, dua item selanjutnya akan muncul sebagai **Beli sekarang** dan **Aktifkan**, yang memungkinkan Anda membeli versi lengkap dari program ini saat itu juga. Untuk **Keamanan Internet AVG 2011** yang terinstal dengan nomor penjualan, item yang ditampilkan adalah **Daftarkan** dan **Aktifkan**. Untuk informasi lebih lanjut harap baca bagian **Lisensi** pada dokumentasi ini.

- **Tentang AVG** - membuka dialog **Informasi** berisi lima tab yang menyediakan data



mengenai nama program, program dan versi basis data virus, info sistem, perjanjian lisensi, dan informasi kontak **AVG Technologies CZ**.

6.2. Info Status Keamanan

Bagian **Info Status Keamanan** berada di bagian atas jendela utama AVG. Di bagian ini akan selalu Anda temukan informasi mengenai status keamanan saat ini atas **Keamanan Internet AVG 2011** Anda. Lihat gambaran umum mengenai berbagai ikon yang ditampilkan di bagian ini beserta artinya:



- Ikon hijau menunjukkan bahwa AVG Anda berfungsi penuh. Komputer Anda terlindungi sepenuhnya, mutakhir dan semua komponen yang terinstal bekerja dengan benar.



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

Ikon ini juga muncul jika karena suatu alasan Anda memutuskan untuk [mengabaikan status kesalahan komponen](#) (opsi "*Abaikan status komponen*" tersedia dalam menu konteks yang dibuka dengan cara mengklik kanan pada ikon komponen yang bersangkutan dalam tinjauan umum komponen pada jendela utama AVG). Anda mungkin perlu menggunakan opsi ini dalam situasi tertentu namun sangat disarankan untuk menonaktifkan opsi "**Abaikan status komponen**" secepatnya.



- Ikon merah menunjukkan bahwa AVG dalam status kritis! Satu atau beberapa komponen tidak berfungsi dengan benar dan AVG 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](#).

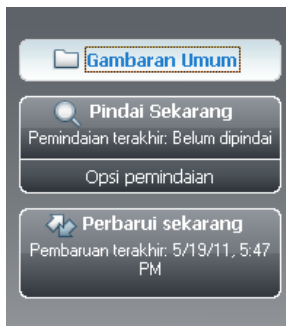
Jika AVG tidak disetel pada kinerja optimal, tombol baru bernama Perbaiki (atau Perbaiki semua jika masalah melibatkan lebih dari satu komponen) muncul di dekat informasi status keamanan. Tekan tombol untuk meluncurkan proses otomatis pemeriksaan dan konfigurasi program. Ini adalah cara mudah untuk menyetel AVG pada kinerja 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 AVG juga dapat diperoleh kapan saja dari [ikon baki sistem](#).

6.3. Tautan Cepat

Tautan cepat (di bagian kiri [Antarmuka Pengguna AVG](#)) memungkinkan Anda dengan seketika mengakses berbagai fitur AVG yang paling penting dan paling sering digunakan:



- **Gambaran umum** - gunakan tautan ini untuk beralih dari antarmuka AVG yang saat ini dibuka ke antarmuka default yang berisi gambaran umum semua komponen terinstal - lihat bab [Gambaran Umum Komponen >>](#)
- **Pindai sekarang** - secara default, tombol ini memberikan informasi (*tipe pemindaian, tanggal terakhir diluncurkan*) tentang pemindaian yang terakhir diluncurkan. Anda dapat melakukan perintah **Pindai sekarang** untuk meluncurkan pemindaian yang sama lagi, atau ikuti tautan **Opsi pemindaian** untuk membuka antarmuka pemindaian AVG tempat Anda dapat menjalankan pemindaian, menjadwalkan pemindaian, atau mengedit parameternya - lihat bab [Pemindaian AVG >>](#)
- **Perbarui sekarang** - tautan memberikan tanggal terakhir peluncuran proses pembaruan. Tekan tombol untuk membuka antarmuka pembaruan, dan menjalankan proses pembaruan AVG segera - lihat bab [Pembaruan AVG >>](#)

Tautan ini dapat diakses dari antarmuka pengguna kapan saja. Setelah Anda menggunakan tautan cepat untuk menjalankan proses tertentu, GUI akan mengalihkan ke sebuah dialog baru namun tautan cepat tetap tersedia. Selain itu, proses yang berjalan akan digambarkan secara grafis.

6.4. Gambaran Umum Komponen

Bagian **Gambaran Umum Komponen** berada di bagian tengah [Antarmuka Pengguna AVG](#). Bagian ini dibagi ke dalam dua bagian:

- Gambaran umum semua komponen yang terinstal terdiri dari sebuah panel berisi ikon komponen dan informasi apakah komponen tersebut aktif atau tidak aktif
- Keterangan komponen yang dipilih

Di bagian **Keamanan Internet AVG 2011 Tinjauan Umum Komponen** berisi informasi mengenai komponen berikut:

- **Anti-Virus** memastikan bahwa komputer Anda terlindung dari berbagai virus yang mencoba memasuki komputer Anda - [perincian >>](#)



- **Anti-Spyware** memastikan bahwa komputer Anda terlindungi dari spyware dan adware - [perincian >>](#)
- **Anti-Spam** memeriksa semua pesan e-mail masuk dan menandai e-mail yang tidak diinginkan sebagai SPAM - [perincian >>](#)
- **Firewall** mengontrol cara komputer Anda bertukar data dengan Internet atau jaringan lokal - [perincian >>](#)
- **Link Scanner** memeriksa hasil telusur yang ditampilkan dalam peramban Internet Anda - [perincian >>](#)
- **Pemindai E-mail** memeriksa adanya virus pada semua e-mail yang masuk dan keluar - [perincian >>](#)
- **Perisai Tetap** berjalan di latar belakang dan memindai file saat disalin, dibuka atau disimpan - [perincian >>](#)
- **Family Safety** membantu memantau aktivitas online anak Anda dan melindunginya dari konten situs Web yang tidak pantas - [perincian >>](#)
- **LiveKive** menyediakan pencadangan otomatis atas data Anda secara online - [perincian >>](#)
- **Pengatur Pembaruan** mengontrol semua pembaruan AVG - [perincian >>](#)
- **Lisensi** menampilkan nomor lisensi, tipe dan tanggal kedaluwarsa - [perincian >>](#)
- **Online Shield** memindai semua data yang akan diunduh oleh peramban Web - [perincian >>](#)
- **Anti-Rootkit** mendeteksi berbagai program dan teknologi yang mencoba menyamarkan malware - [perincian >>](#)
- **Alat Sistem** memberikan ringkasan terperinci mengenai lingkungan AVG dan informasi sistem operasi - [perincian >>](#)
- **PC Analyzer** memberikan informasi tentang status komputer Anda - [perincian >>](#)
- **Perlindungan Identitas** - komponen anti-malware berfokus untuk mencegah pencuri identitas mencuri harta digital pribadi Anda - [perincian >>](#)
- **Security Toolbar** memungkinkan Anda menggunakan fungsionalitas AVG yang dipilih, langsung dari peramban Internet Anda - [perincian >>](#)
- **Remote Administration** hanya ditampilkan dalam AVG Business Edition jika Anda telah menentukannya saat [proses instalasi](#) agar komponen ini diinstal

Klik sekali ikon suatu komponen untuk menyorotnya dalam gambaran umum komponen. Pada saat yang sama, keterangan fungsionalitas dasar komponen akan muncul di bagian bawah antarmuka pengguna. Klik dua kali ikon tersebut untuk membuka antarmuka komponen yang berisi daftar data



statistik dasar.

Klik kanan mouse Anda di atas ikon komponen untuk membuka menu konteks: di samping membuka antarmuka grafis komponen tersebut, Anda juga dapat memilih **Abaikan status komponen**. Pilih opsi ini untuk menyatakan Anda mengetahui [status kesalahan komponen](#) namun karena suatu alasan Anda ingin membiarkan AVG begitu dan Anda tidak ingin diperingatkan dengan [ikon baki sistem](#).

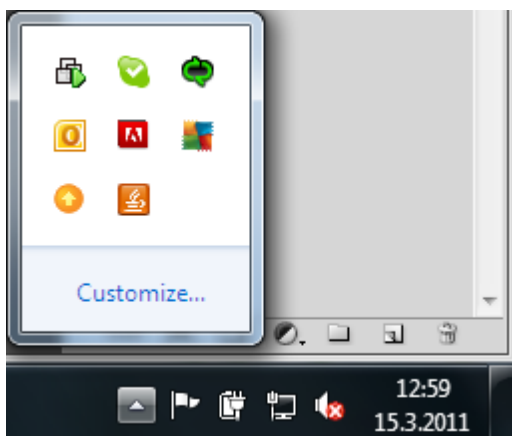
6.5. Statistik

Bagian **Statistik** berada di bagian kiri bawah [Antarmuka Pengguna AVG](#). Ini menyediakan daftar informasi mengenai operasi program:

- **DB Virus** - memberi tahu tentang versi basis data virus yang saat ini terinstal
- **Versi AVG** - memberi tahu Anda tentang versi AVG yang terinstal (*nomornya dalam format 10.0.xxxx, dengan 10.0 merupakan versi lini produk, dan xxxx menyatakan nomor pembuatan*)
- **Lisensi kedaluwarsa** - menyediakan tanggal kedaluwarsa lisensi AVG Anda

6.6. Ikon Baki Sistem

Ikon Baki Sistem (pada Windows taskbar) menunjukkan status terkini dari **Keamanan Internet AVG 2011** Anda. Ini selalu terlihat pada baki sistem Anda, baik jendela utama AVG Anda sedang dibuka ataupun ditutup:

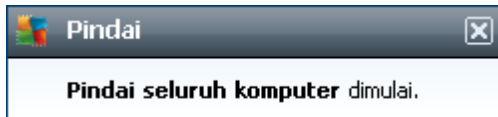


Jika berwarna penuh , **Ikon Baki Sistem** menunjukkan bahwa semua komponen AVG aktif dan berfungsi penuh. Selain itu, ikon baki sistem AVG dapat ditampilkan dalam sepuh warna jika AVG dalam status kesalahan namun Anda mengetahui situasi ini sepenuhnya dan sengaja memutuskan untuk [Abaikan status komponen](#). Ikon dengan tanda seru  menunjukkan adanya masalah (*komponen yang tidak aktif, status kesalahan, dll.*). Klik dua kali **Ikon Baki Sistem** untuk membuka jendela utama dan mengedit komponen.

Ikon baki sistem memberi tahu lebih jauh mengenai berbagai aktivitas AVG saat ini dan kemungkinan perubahan status dalam program (*misalnya peluncuran otomatis untuk pemindaian*



atau pembaruan yang telah dijadwalkan, Pengalihan profil Firewall, perubahan status komponen, terjadinya status kesalahan, ...melalui jendela yang muncul dari ikon baki sistem AVG:



Ikon Baki Sistem juga dapat digunakan sebagai tautan cepat untuk mengakses jendela utama AVG kapan saja - klik dua kali ikon tersebut. Dengan mengklik kanan pada **Ikon Baki Sistem** Anda akan membuka menu konteks singkat berisi opsi berikut:

- **Buka Antarmuka Pengguna AVG** - klik untuk membuka [Antarmuka Pengguna AVG](#)
- **Pemindaian** - klik untuk membuka menu konteks
- **Firewall** - klik untuk membuka menu konteks opsi pengaturan [Firewall](#) tempat Anda dapat mengedit parameter utama: [Status firewall](#) (*Aktifkan firewall/ Nonaktifkan firewall/Mode darurat*), [pengalihan ke mode permainan](#) dan [Profil firewall](#)
- **Jalankan PC Analyzer** - klik untuk meluncurkan komponen [PC Analyzer](#)
- **Pemindaian yang sedang berjalan** - item ini ditampilkan hanya 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*.
- **Perbarui sekarang** - meluncurkan pembaruan [dengan segera](#)
- **Bantuan** - membuka halaman bantuan pada halaman awal

6.7. 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 Internet AVG 2011** yang terpenting yaitu [pemindaian](#) dan [pembaruan](#):



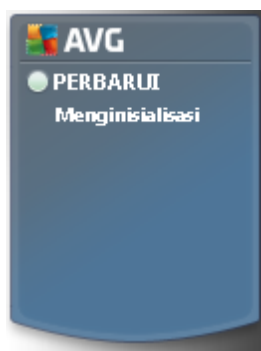
Gadget AVG menyediakan opsi akses cepat berikut:



- **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. Gambaran 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 AVG langsung dari dalam gadget:



- **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 diarahkan ulang 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 (*misalnya disediakan karena Anda telah menginstal AVG menggunakan salah satu lisensi edisi AVG Business*), dan ini membuka peramban Internet Anda di situs Web **AVG SMB Community** dalam jaringan sosial LinkedIn
- **PC Analyzer**  - membuka antarmuka pengguna dalam komponen [PC Analyzer](#)
- **Kotak telusur** - ketikkan kata kunci dan dapatkan hasil telusur dengan segera di jendela yang baru dibuka pada peramban Web default Anda



7. Komponen AVG

7.1. Anti-Virus

7.1.1. Prinsip-Prinsip Anti-Virus

Mesin pemindai perangkat lunak antivirus 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. 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.

Fitur penting pada perlindungan antivirus adalah bahwa tidak ada virus dikenal yang dapat berjalan pada komputer!

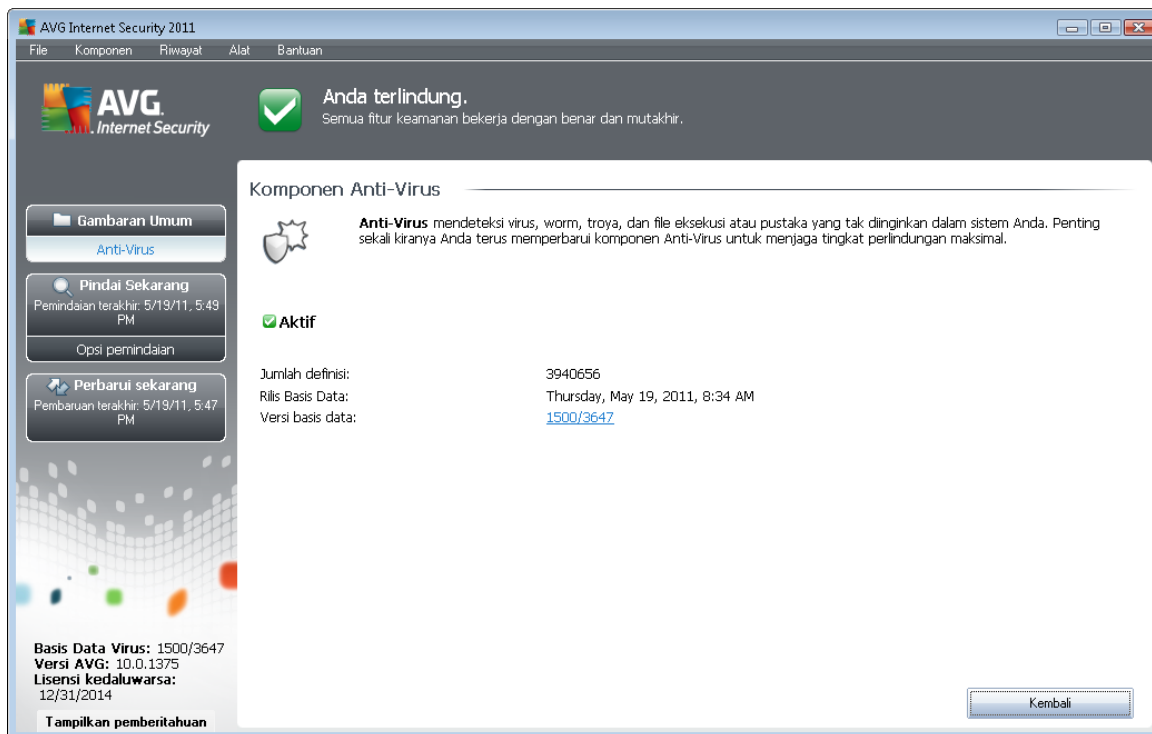
Sementara satu teknologi mungkin gagal mendeteksi atau mengenali virus, **Anti-Virus** menggabungkan beberapa teknologi untuk memastikan komputer terlindung dari virus:

- 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

AVG juga dapat menganalisis dan mendeteksi aplikasi atau pustaka DLL yang dapat dijalankan yang mungkin tidak diinginkan dalam sistem. Kami menyebut ancaman demikian sebagai Program yang Mungkin Tidak Diinginkan (berbagai macam spyware, adware, dsb.). Lagi pula, AVG 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.



7.1.2. Antarmuka Anti-Virus



Antarmuka komponen **Anti-Virus** memberikan sejumlah informasi dasar mengenai fungsionalitas komponen, yakni informasi tentang status terkini komponen (*Komponen Anti-Virus aktif.*), dan gambaran umum singkat mengenai statistik **Anti-Virus** :

- **Jumlah definisi** - angka yang menunjukkan jumlah virus yang didefinisikan dalam versi basis data virus terbaru
- **Rilis basis data** - menentukan kapan dan pukul berapa basis data virus diperbarui
- **Versi basis data** - menetapkan jumlah versi basis data virus terbaru, dan jumlah ini terus bertambah setiap kali basis virus diperbarui

Hanya ada satu tombol pengoperasian yang tersedia dalam antarmuka komponen ini (**Kembali**) - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (*gambaran umum komponen*).

7.2. Anti-Spyware

7.2.1. Prinsip-Prinsip Anti-Spyware

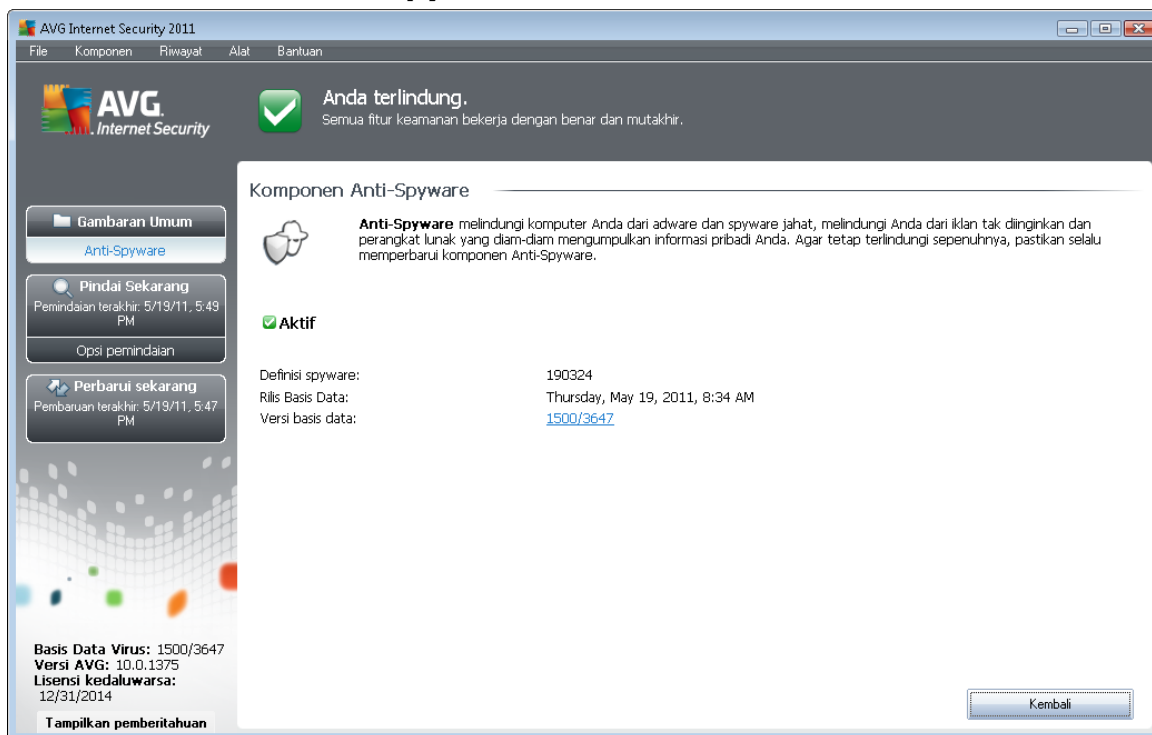
Spyware biasanya ditetapkan sebagai tipe malware, yaitu perangkat lunak, yang mengumpulkan informasi dari komputer pengguna tanpa sepengetahuan atau persetujuan pengguna. Beberapa aplikasi spyware mungkin juga terinstal saat pembelian dan seringkali berisi iklan, jendela pop up atau tipe perangkat lunak 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 perisai tetap dan memindai aplikasi Anda di latar belakang saat Anda menjalankannya.

Ada juga potensi risiko yang ditransmisikan malware ke komputer Anda sebelum instalasi AVG, atau karena Anda telah lalai memperbarui **Keamanan Internet AVG 2011** dengan [basis data terbaru dan pembaruan program](#). Karena alasan ini, AVG memungkinkan Anda memindai penuh malware/spyware di komputer Anda dengan menggunakan fitur pemindaian. Komponen ini juga mendeteksi malware yang tidur dan tidak aktif, mis. malware yang telah diunduh tetapi belum diaktifkan.

7.2.2. Antarmuka Anti-Spyware



Antarmuka komponen **Anti-Spyware** memberikan gambaran umum singkat mengenai fungsionalitas komponen, informasi mengenai status komponen saat ini, dan beberapa statistik **Anti-Spyware**:

- **Definisi spyware** - angka yang menyediakan jumlah contoh spyware yang didefinisikan dalam versi basis data spyware terbaru
- **Rilis basis data** - menentukan kapan dan pukul berapa basis data spyware diperbarui
- **Versi basis data** - menentukan jumlah versi basis data spyware terbaru, dan jumlah ini terus bertambah setiap kali basis virus diperbarui

Hanya ada satu tombol pengoperasian yang tersedia dalam antarmuka komponen ini (**Kembali**) - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (*gambaran umum komponen*).



7.3. Anti-Spam

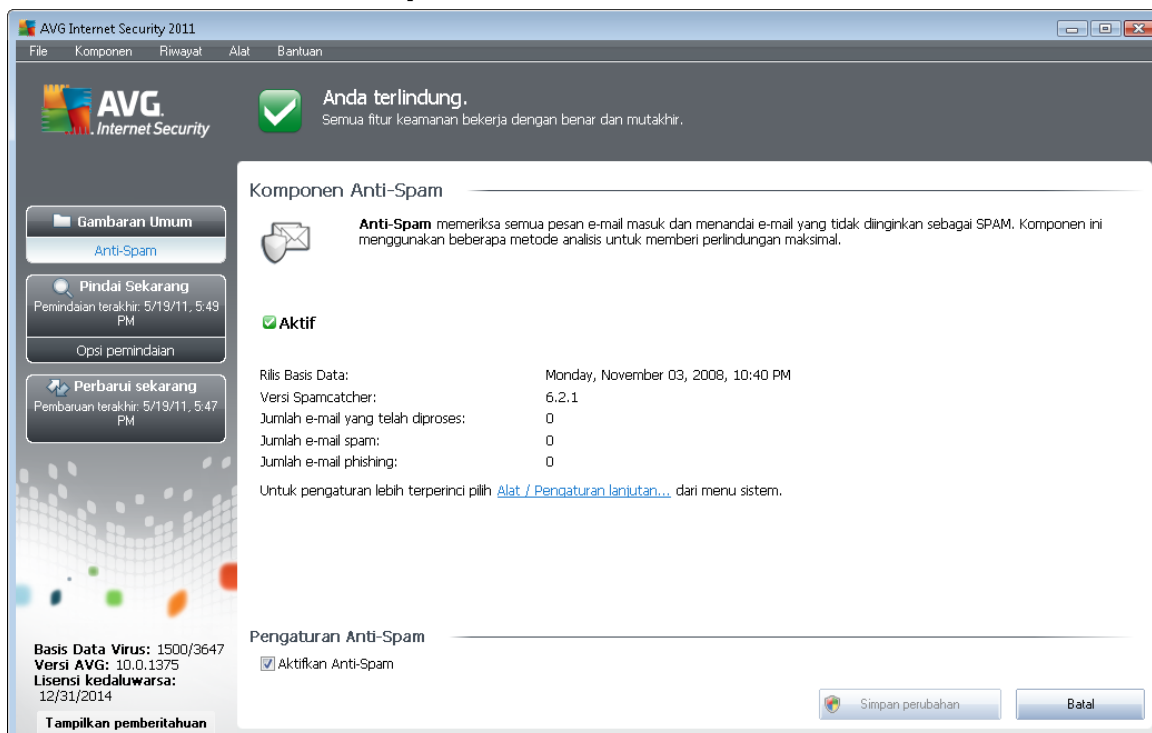
Spam adalah e-mail yang tidak diundang, hampir semuanya mengiklankan produk atau layanan yang dikirimkan massal ke sejumlah besar alamat e-mail sekaligus, sehingga memenuhi kotak surat penerima. E-mail komersial resmi yang telah disetujui oleh konsumen tidak termasuk spam. Spam tidak hanya mengganggu,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

7.3.1. Prinsip-Prinsip Anti-Spam

AVG Anti-Spam memeriksa semua pesan e-mail masuk dan menandai e-mail yang tidak diinginkan sebagai spam. **AVG 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 **AVG 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. **AVG 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*).

7.3.2. Antarmuka Anti-Spam



Dalam dialog komponen **Anti-Spam** Anda akan menemukan teks singkat yang menjelaskan fungsionalitas komponen, informasi mengenai status terbaru dan statistik berikut:

- **Rilis basis data** - menentukan kapan dan pukul berapa basis data spam diperbarui dan



dipublikasikan

- **Versi Spamcatcher** - menentukan nomor versi terbaru mesin anti-spam
- **Jumlah email yang diproses** - menentukan jumlah pesan email yang dipindai sejak mesin anti-spam terakhir diluncurkan
- **Jumlah email spam** - dari semua email yang dipindai, menentukan berapa banyak pesan yang ditandai sebagai spam
- **Jumlah email phishing** - dari semua email yang dipindai, menentukan berapa banyak pesan yang ditandai sebagai upaya phishing.

Dialog **Anti-Spam** selanjutnya menyediakan tautan [Alat/Pengaturan Lanjutan](#). Gunakan tautan ini untuk mengarahkan kembali ke lingkungan konfigurasi lanjutan semua komponen **Keamanan Internet AVG 2011**.

Perhatikan: Penjual 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.

Hanya ada satu tombol pengoperasian yang tersedia dalam antarmuka komponen ini (**Kembali**) - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (gambaran umum komponen).

7.4. 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; 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.

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.

7.4.1. Prinsip-Prinsip Firewall

Di AVG, komponen **Firewall** mengontrol semua lalu lintas di setiap port jaringan pada komputer Anda. Berdasarkan 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 dengan 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.

Catatan: 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 menghubungkan ke berbagai jaringan, atau menggunakan beberapa adaptor jaringan

7.4.2. 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:**

- o **Terhubung langsung ke Internet** – sesuai untuk komputer rumah biasa yang terhubung langsung ke Internet atau notebook yang terhubung ke Internet di luar jaringan perusahaan yang aman. Pilih opsi ini jika Anda menghubungkan dari rumah, atau Anda berada dalam jaringan perusahaan kecil tanpa kontrol pusat. Pilih juga opsi ini bila bepergian dan menghubungkan dengan notebook Anda dari berbagai tempat yang tidak dikenal dan mungkin berbahaya (*warnet, kamar hotel dll.*). Aturan yang lebih membatasi akan dibuat, karena diasumsikan bahwa komputer ini tidak memiliki perlindungan tambahan sehingga memerlukan perlindungan maksimum.
- o **Komputer di domain** – sesuai untuk komputer dalam jaringan lokal, mis. jaringan sekolah atau perusahaan. Diasumsikan bahwa jaringan dilindungi dengan tindakan tambahan tertentu sehingga tingkat keamanannya mungkin lebih rendah daripada komputer mandiri.
- o **Jaringan rumah atau kantor kecil** – sesuai untuk komputer dalam jaringan kecil, mis. di rumah atau usaha kecil, umumnya hanya beberapa komputer yang saling terhubung, tanpa administrator "pusat".

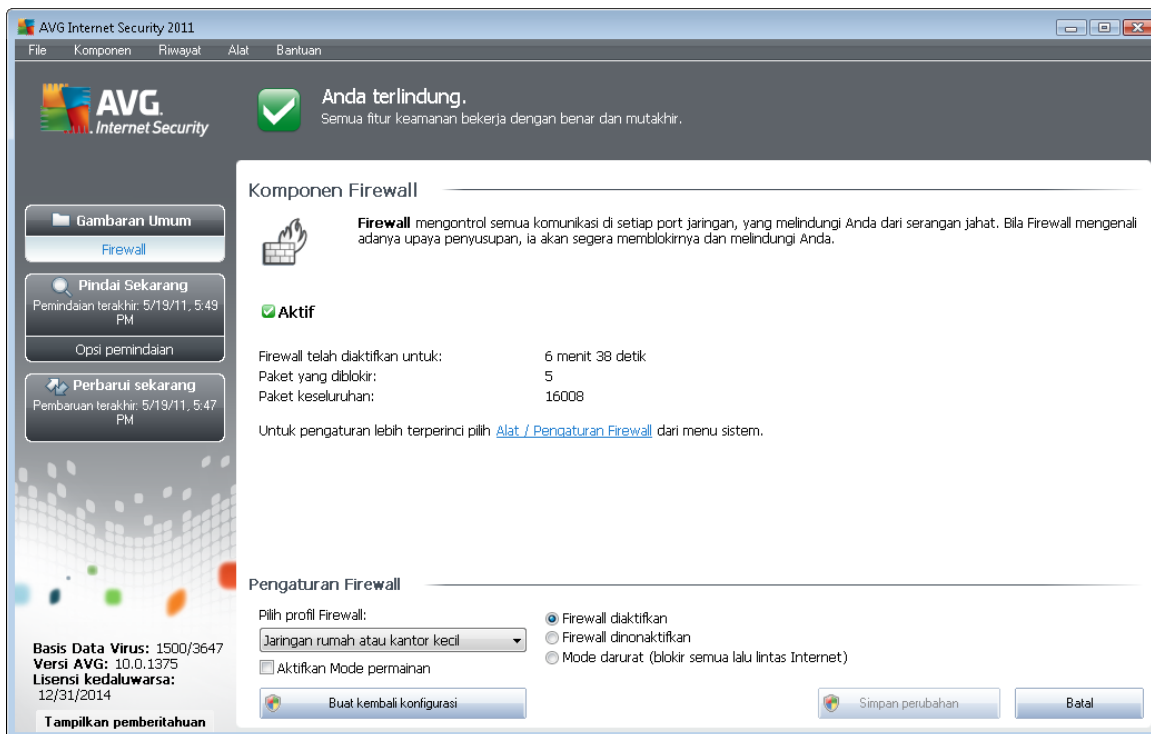
Pengalihan profil

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.

7.4.3. Antarmuka Firewall



Antarmuka **Firewall** memberikan beberapa informasi dasar mengenai fungsionalitas komponen, statusnya dan gambaran singkat statistik **Firewall**:

- **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 Firewall

- **Pilih profil Firewall** - dari menu gulir-bawah, pilih satu profil yang ditentukan - setiap saat tersedia dua profil (*profil default bernama **Perbolehkan semua dan Blokir semua***), profil lain ditambahkan secara manual melalui pengeditan profil dalam dialog [Profil](#) di [Pengaturan 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.



- **Status Firewall:**

- o **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
- o **Firewall dinonaktifkan** - opsi ini akan menonaktifkan [Firewall](#) sama sekali, semua lalu lintas jaringan diperbolehkan namun tidak diperiksa!
- o **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: Penjual 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 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
- **Batalan** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (gambaran umum komponen)

7.5. Link Scanner

7.5.1. Prinsip-Prinsip Link Scanner

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.

Teknologi **LinkScanner** terdiri atas dua fitur, [Search-Shield](#) dan [Surf-Shield](#):

- [Search-Shield](#) berisi daftar situs Web (alamat URL) yang diketahui berbahaya. Saat menelusur dengan Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, atau SlashDot, semua hasil penelusuran akan diperiksa sesuai daftar ini dan ikon keputusan akan ditampilkan (untuk hasil telusur



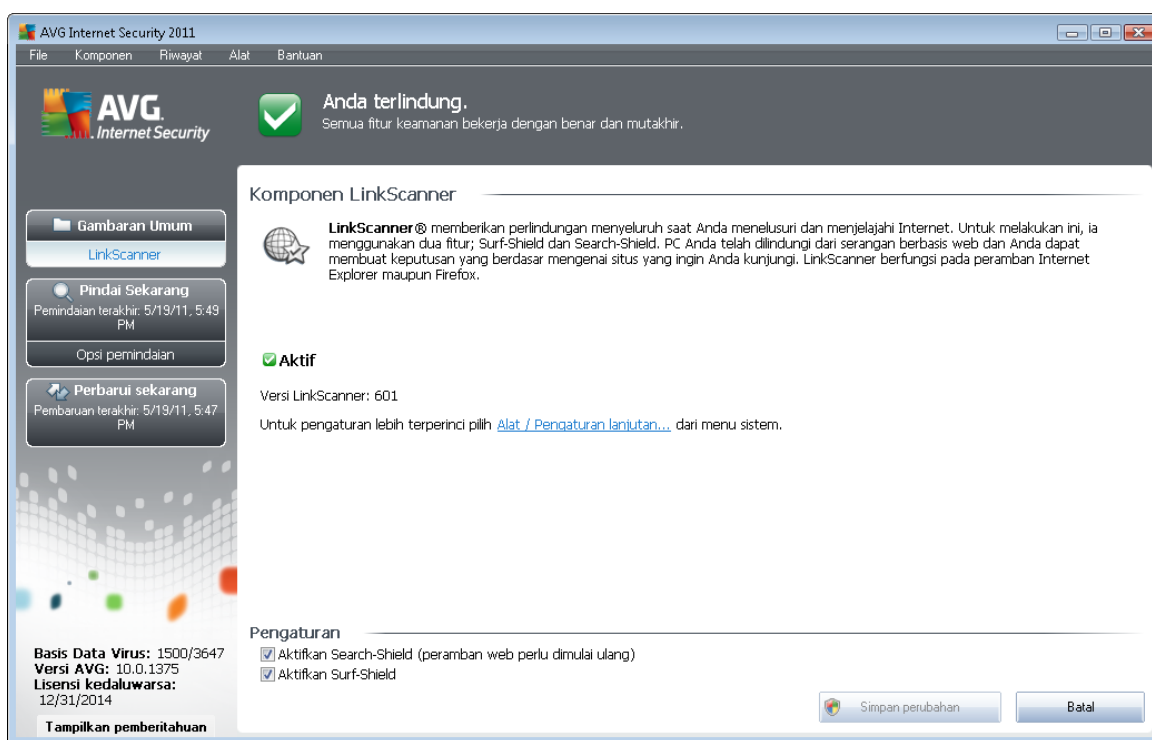
Yahoo, hanya ikon keputusan "situs Web exploit" yang ditampilkan).

- **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 situs Web jahat baru dibuat, atau situs Web yang sebelumnya bersih sekarang berisi malware), situs akan terdeteksi dan diblokir oleh **Surf-Shield** begitu Anda mencoba mengunjunginya.

Catatan: Link Scanner tidak ditujukan untuk platform server!

7.5.2. Antarmuka Link Scanner

Antarmuka komponen **LinkScanner** memberikan keterangan singkat tentang fungsionalitas komponen dan informasi mengenai status terkini. Selanjutnya, Anda dapat menemukan informasi mengenai nomor versi basis data **LinkScanner** terbaru (Versi Link Scanner).



Pengaturan LinkScanner

Di bagian bawah dialog, Anda dapat mengedit beberapa opsi:

- **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 (seketika) aktif terhadap



situs eksploitatif saat mengaksesnya. Koneksi situs jahat yang telah dikenal dan konten eksploitatifnya diblokir begitu ia diakses oleh pengguna melalui peramban Web (atau aplikasi lain yang menggunakan HTTP).

7.5.3. 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, **AVG Link Scanner** akan memperingatkan Anda sebelum mengklik tautan berbahaya atau mencurigakan tersebut, 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 (*ikon ini tidak akan ditampilkan untuk hasil telusur Yahoo! JP yang 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.

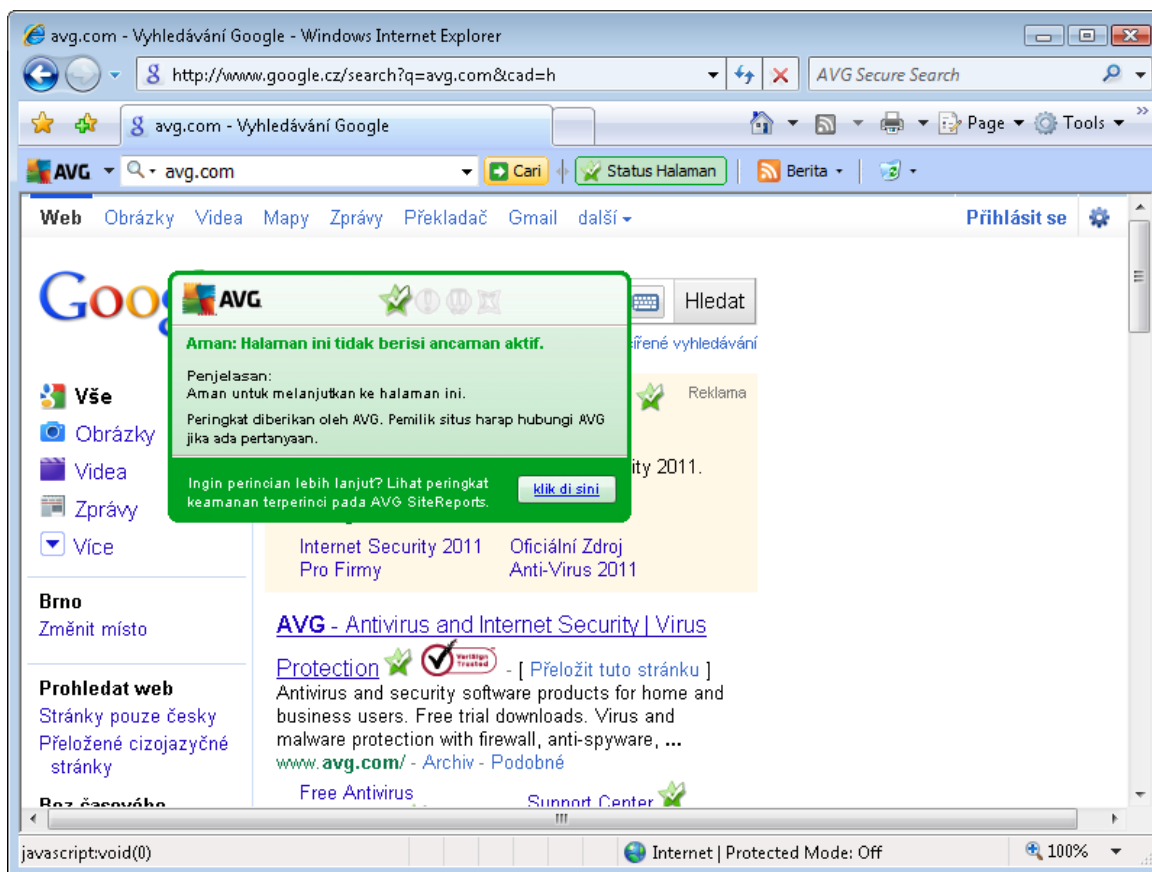


Halaman tertaut berisi ancaman yang aktif! Demi keamanan, Anda tidak akan diperbolehkan mengunjungi halaman ini.



Halaman tertaut tidak dapat diakses, sehingga tidak dapat dipindai.

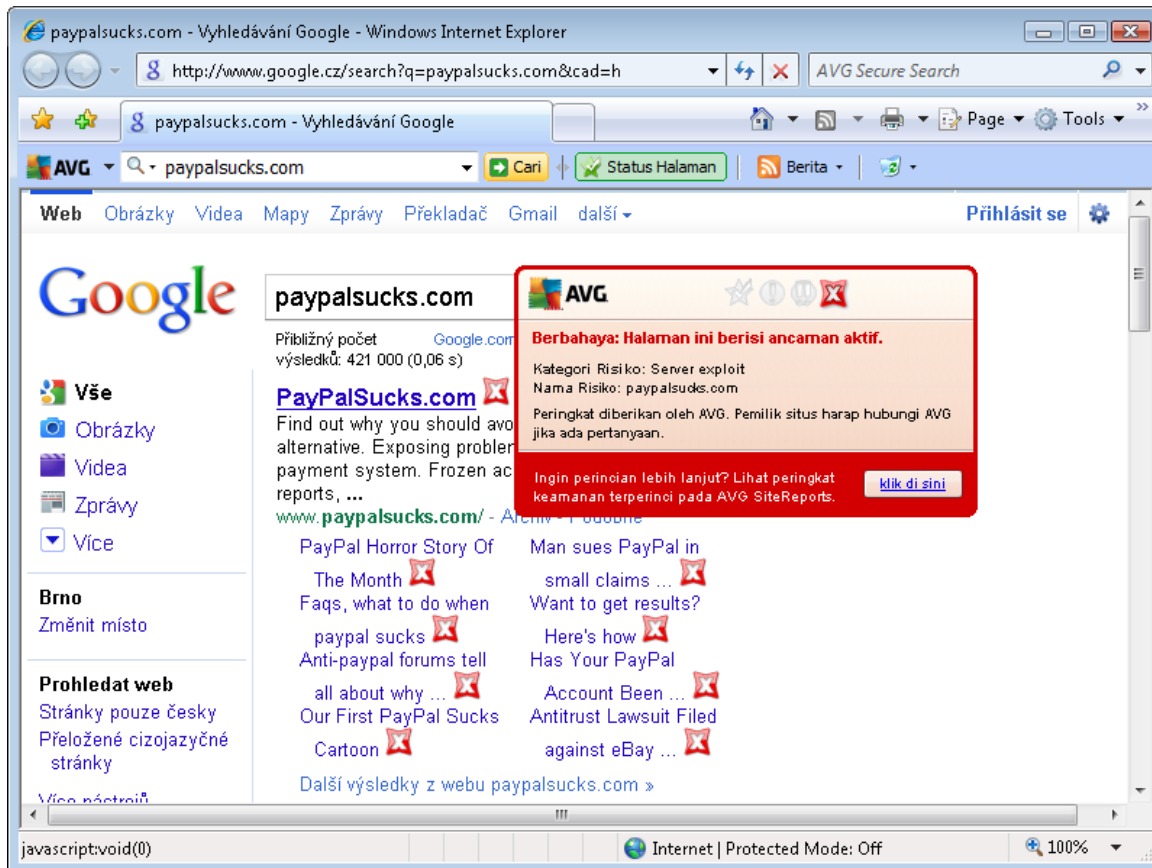
Melayangkan kursor di atas masing-masing ikon peringkat akan menampilkan perincian tentang tautan tertentu yang meragukan. Informasi ini berisi perincian tambahan mengenai ancaman (*jika ada*):



7.5.4. Surf-Shield

Perlindungan tangguh ini akan memblokir berbagai konten jahat/perusak dari halaman 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, [AVG Link Scanner](#) tidak akan memperbolehkan peramban Anda menampilkannya.

Jika Anda menemukan situs web jahat dalam peramban web, [AVG LinkScanner](#) akan memperingatkan Anda dengan layar seperti ini:



Memasuki situs web seperti ini sangat berisiko dan tidak disarankan!

7.6. Perisai Tetap

7.6.1. Prinsip-Prinsip Perisai Tetap

Komponen **Perisai Tetap** melindungi komputer Anda secara terus-menerus. Komponen ini memindai setiap file yang dibuka, disimpan, atau disalin, dan mengamankan area sistem komputer. Bila **Perisai Tetap** 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 proses ini, karena dijalankan "di latar belakang", dan Anda hanya akan diberi tahu jika ditemukan ancaman; pada saat yang sama, **Perisai Tetap** memblokir pengaktifan ancaman tersebut dan menghapusnya. **Perisai Tetap** dimuat ke dalam memori komputer Anda selama menghidupkan ulang sistem.

Apa yang dapat dilakukan oleh **Perisai Tetap**:

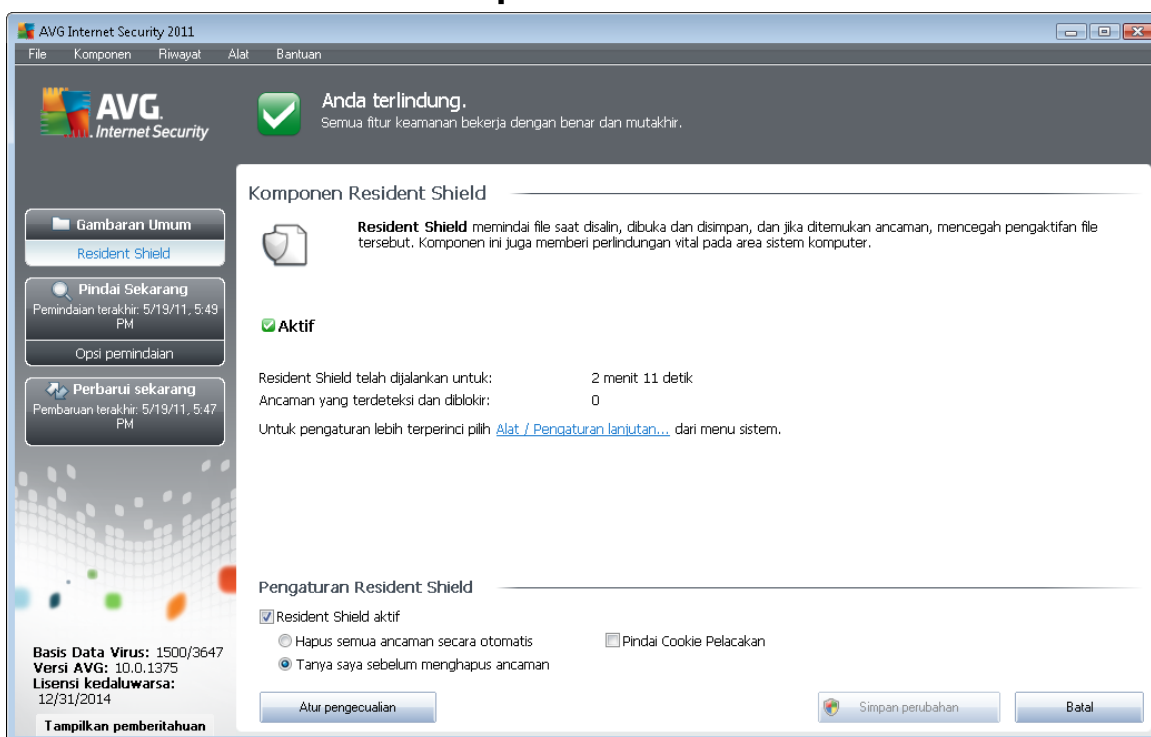
- Memindai jenis kemungkinan ancaman tertentu
- Memindai media eksternal (*flash disk, dll.*)



- Memindai file dengan ekstensi tertentu atau tanpa ekstensi sama sekali
- Memperbolehkan pengecualian dari pemindaian – file atau folder tertentu yang tidak boleh dipindai

Peringatan: Perisai Tetap dimuat dalam memori komputer pada saat komputer dihidupkan, dan sangat penting bagi Anda untuk tetap mengaktifkannya sepanjang waktu!

7.6.2. Antarmuka Perisai Tetap



Selain gambaran umum fungsional **Perisai Tetap** dan informasi tentang status komponen, antarmuka **Perisai Tetap** juga menyajikan beberapa data statistik:

- **Perisai Tetap telah dijalankan selama** - menyediakan waktu sejak komponen terakhir diluncurkan
- **Ancaman yang terdeteksi dan diblokir** - jumlah infeksi terdeteksi yang telah dicegah untuk dijalankan/dibuka (*jika perlu, nilai ini dapat direset; misalnya untuk keperluan statistik - Reset nilai*)

Pengaturan Perisai Tetap

Di bagian bawah jendela dialog, Anda akan menemukan bagian bernama **Pengaturan Perisai Tetap** di mana Anda dapat mengedit beberapa pengaturan dasar untuk fungsionalitas komponen (konfigurasi terperinci, sebagaimana dengan komponen lainnya, tersedia melalui item **Alat/ Pengaturan lanjutan** pada menu sistem).



Opsi **Perisai Tetap aktif** memungkinkan Anda mengaktifkan/menonaktifkan perlindungan tetap dengan mudah. Secara default, fungsi ini aktif. Dengan perlindungan tetap diaktifkan, Anda dapat memutuskan lebih lanjut cara memperlakukan kemungkinan infeksi yang terdeteksi (dihapus):

- o secara otomatis (**Hapus semua ancaman secara otomatis**)
- o atau hanya setelah persetujuan pengguna (**Tanya saya sebelum menghapus ancaman**)

Pilihan ini tidak mempengaruhi tingkat keamanan, dan hanya mencerminkan preferensi Anda.

Dalam kedua kasus, Anda masih dapat memilih apakah Anda ingin **Pindai cookie pelacak**. Dalam kasus tertentu, Anda dapat mengaktifkan opsi ini untuk mencapai tingkat keamanan maksimum, walau demikian ia telah dinonaktifkan secara default. (cookie = *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 belanjaan elektronik mereka*).

Perhatikan: Penjual 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 antarmuka **Perisai Tetap** adalah sebagai berikut:

- **Atur pengecualian** - membuka dialog [Perisai Tetap - Item Pengecualian](#) tempat Anda menetapkan folder dan file yang harus dibiarkan dari pemindaian [Perisai Tetap](#)
- **Simpan perubahan** - tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini
- **Batal** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (gambaran umum komponen)

7.6.3. Deteksi Perisai Tetap

Perisai Tetap 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 yang harus dilakukan sekarang - tersedia pilihan berikut:

Perhatikan bahwa, pada kondisi tertentu (jenis file yang terinfeksi, dan di mana lokasinya), tidak semua opsi ini tersedia!

- **Hapus ancaman sebagai Pengguna Mahir** - centang kotak ini jika Anda menduga tidak memiliki hak akses yang memadai sebagai pengguna biasa untuk menghapus ancaman. Pengguna Mahir memiliki hak akses yang lebih luas, dan jika ancaman terdapat dalam folder sistem tertentu, Anda mungkin perlu mencentang kotak ini agar berhasil menghapusnya.
- **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](#)*)
- **Pindah ke Gudang** - virus akan dipindahkan ke [Gudang Virus AVG](#)
- **Buka file** - opsi ini mengalihkan Anda ke lokasi yang tepat di mana objek mencurigakan berada (*membuka jendela Windows Explorer baru*)
- **Abaikan** - kami sangat menyarankan untuk TIDAK menggunakan opsi ini kecuali Anda

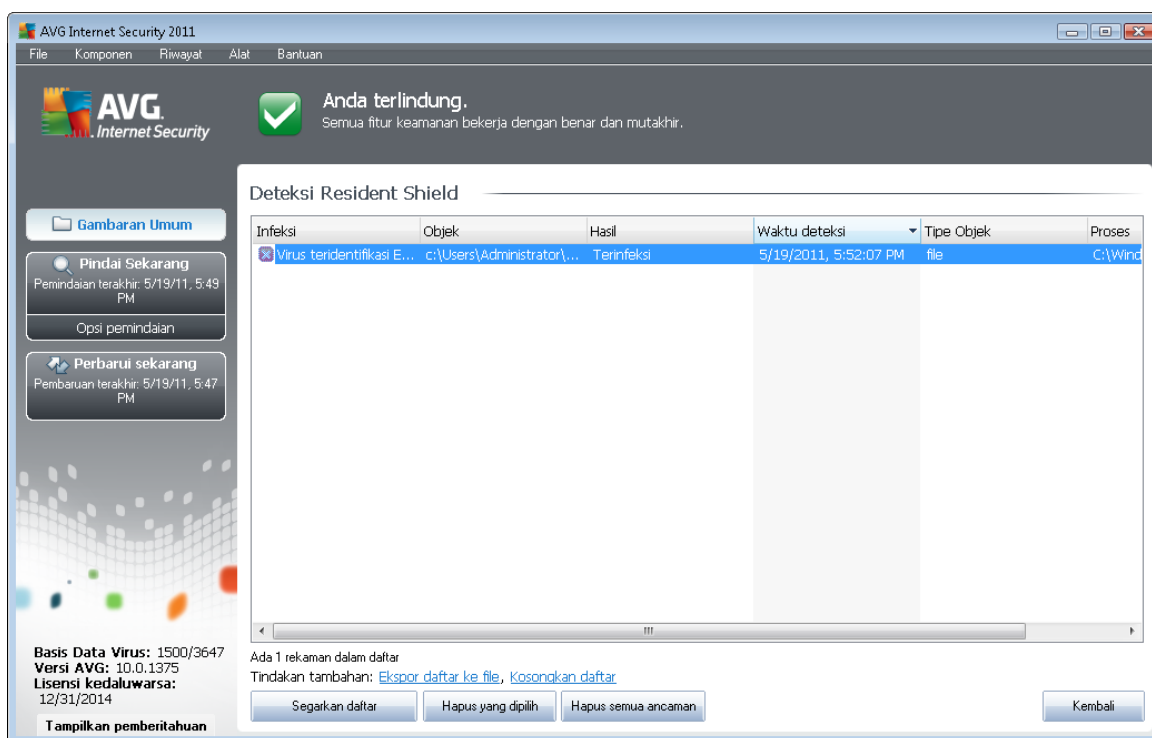


punya alasan yang sangat baik untuk melakukannya!

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.

Seluruh gambaran umum semua ancaman yang terdeteksi oleh [Perisai Tetap](#) dapat ditemukan di dialog **Deteksi Perisai Tetap** yang dapat diakses melalui opsi menu sistem [Riwayat / Deteksi Perisai Tetap](#):



Deteksi Perisai Tetap memberikan gambaran umum mengenai berbagai objek yang terdeteksi oleh [Perisai Tetap](#), 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 **Perisai Tetap**. Tombol **Kembali** akan mengembalikan Anda ke [antarmuka pengguna AVG](#) default (*gambaran umum komponen*).

7.7. Family Safety

AVG Family Safety membantu Anda melindungi anak-anak Anda dari situs Web, konten media, dan penelusuran online yang tidak pantas, serta memberi Anda laporan mengenai aktivitas online mereka. Anda dapat mengatur tingkat perlindungan yang sesuai untuk tiap anak Anda dan memantau mereka masing-masing melalui login unik.

Komponen hanya aktif bila produk **AVG Family Safety** telah diinstal di komputer Anda. Jika Anda belum menginstal produk **AVG Family Safety**, klik ikonnya dalam antarmuka pengguna **Keamanan Internet AVG 2011** dan Anda akan dialihkan ke situs Web produk di mana Anda dapat menemukan semua perincian yang diperlukan.

7.8. AVG LiveKive

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.

Komponen hanya aktif bila produk **AVG LiveKive** telah diinstal pada komputer Anda. Jika Anda belum menginstal produk **AVG LiveKive**, klik ikonnya dalam antarmuka pengguna **Keamanan Internet AVG 2011** dan Anda akan dialihkan ke situs Web produk di mana Anda dapat menemukan semua perincian yang diperlukan.

7.9. Pemindai 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-mail perusahaan dan memasang filter anti-spam, dsb, untuk mengurangi risiko tersebut.



7.9.1. Prinsip-Prinsip Pemindai E-mail

Pemindai E-mail 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, dan The Bat*). Pertama-tama, plug-in digunakan dengan aplikasi email seperti like Outlook Express, Mozilla, Incredimail, dll.

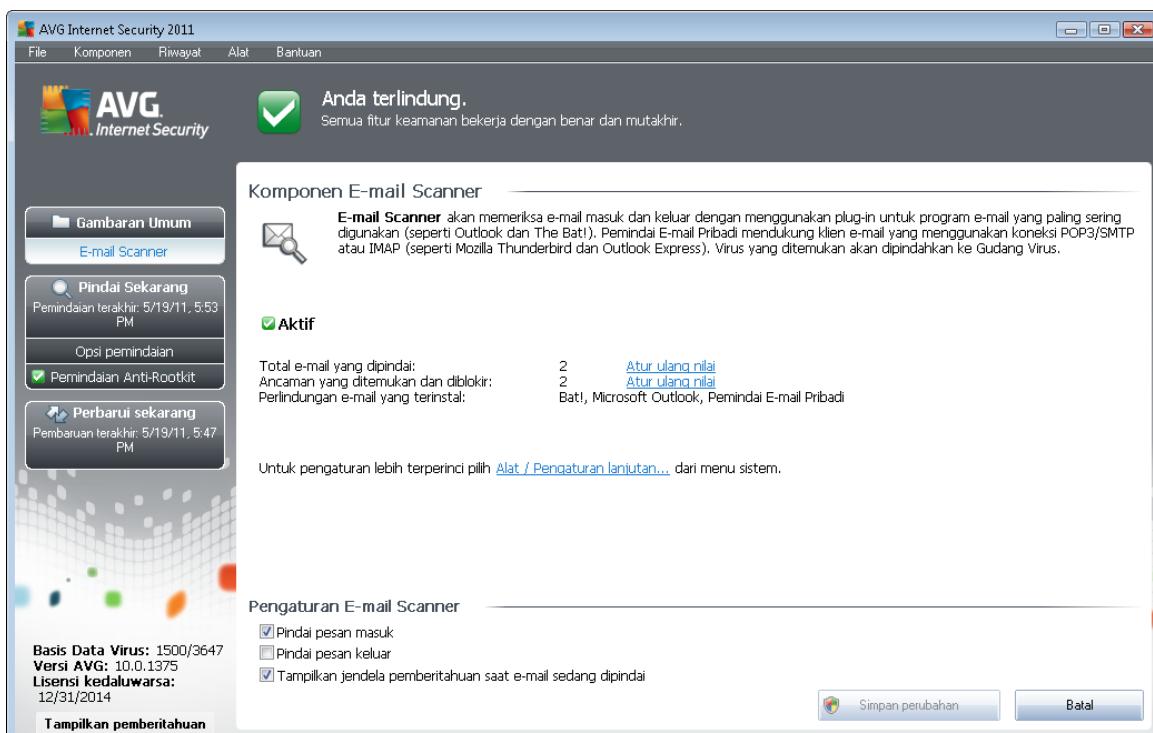
Selama instalasi [AVG](#), terdapat server otomatis yang dibuat untuk kontrol e-mail: satu server untuk memeriksa e-mail masuk dan yang kedua untuk memeriksa e-mail keluar. Dengan menggunakan dua server ini, e-mail akan diperiksa secara otomatis pada port 110 dan 25 (*port standar untuk mengirim/menerima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

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

- **Email masuk:** Saat menerima pesan dari server, komponen **Pemindai E-mail** 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 Pemindai E-mail; 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*).

Catatan: Pemindai E-mail AVG tidak ditujukan untuk platform server!

7.9.2. Antarmuka Pemindai E-mail





Dalam dialog komponen **Pemindai Email** Anda dapat menemukan teks singkat yang menerangkan fungsionalitas komponen, dan informasi mengenai status terbarunya dan statistik berikut ini:

- **Total e-mail yang dipindai** - jumlah pesan e-mail yang telah dipindai sejak **Pemindai E-mail** terakhir diluncurkan (*jika perlu, nilai ini dapat direset; seperti untuk keperluan statistik - Reset nilai*)
- **Ancaman ditemukan dan diblokir** - menyediakan jumlah infeksi yang terdeteksi dalam pesan e-mail sejak **Pemindai E-mail** terakhir diluncurkan
- **Perlindungan e-mail yang diinstal** - informasi tentang plugin perlindungan e-mail tertentu yang mengacu pada klien e-mail default Anda yang diinstal

Pengaturan E-mail Scanner

Di bagian bawah dialog, Anda dapat menemukan bagian bernama **Pengaturan Pemindai E-mail** di mana Anda dapat mengedit beberapa fitur dasar dari fungsionalitas komponen:

- **Pindai pesan masuk** - centang item ini untuk menentukan bahwa semua e-mail yang dikirimkan ke akun Anda harus dipindai untuk menemukan virus. Secara default, item ini diaktifkan, dan disarankan untuk tidak mengubah pengaturan ini!
- **Pindai pesan keluar** - centang item ini untuk mengonfirmasi bahwa semua e-mail yang terkirim dari akun Anda harus dipindai virusnya. Secara default, item ini tidak aktif.
- **Tampilkan ikon pemberitahuan saat email dipindai** - centang item ini untuk mengonfirmasi bahwa Anda ingin diberi tahu melalui dialog pemberitahuan yang ditampilkan di atas ikon AVG pada baki sistem selama memindai email Anda melalui komponen [Pemindai Email](#). Secara default, item ini diaktifkan, dan disarankan untuk tidak mengubah pengaturan ini!

Konfigurasi lanjutan komponen **Pemindai E-mail** dapat diakses melalui item **Alat/Pengaturan lanjutan** pada menu sistem; walau demikian konfigurasi lanjutan hanya disarankan untuk pengguna berpengalaman!

Perhatikan: Penjual 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

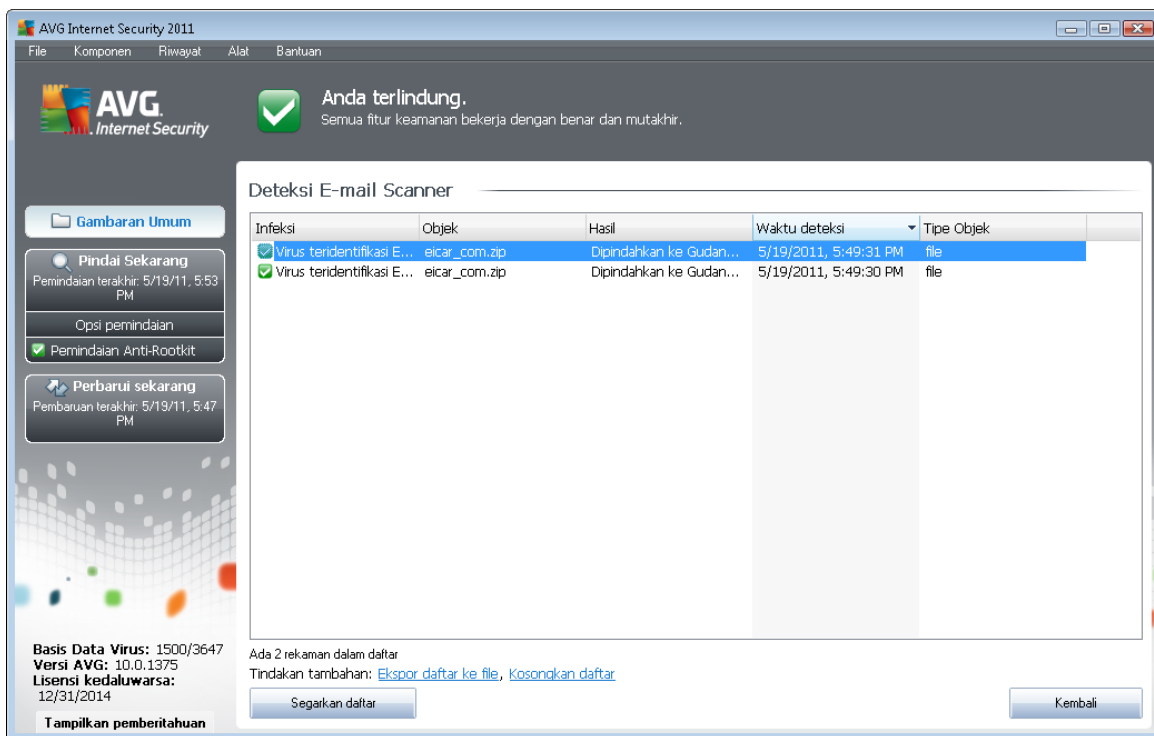
Tombol kontrol yang tersedia dalam antarmuka **Pemindai E-mail** adalah sebagai berikut:

- **Simpan perubahan** - tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini
- **Batal** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (



gambaran umum komponen)

7.9.3. Deteksi Pemindai E-mail



Dalam dialog **Deteksi Pemindai Email** (dapat diakses melalui opsi menu sistem *Riwayat / Deteksi Pemindai Email*) Anda akan dapat melihat daftar semua temuan yang terdeteksi oleh komponen **Pemindai 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 Pemindai E-mail** adalah:



- **Segarkan daftar** - memperbarui daftar ancaman yang terdeteksi
- **Kembali** - mengalihkan Anda kembali ke dialog yang ditampilkan sebelumnya

7.10. Pengatur Pembaruan

7.10.1. Prinsip-Prinsip Pengatur Pembaruan

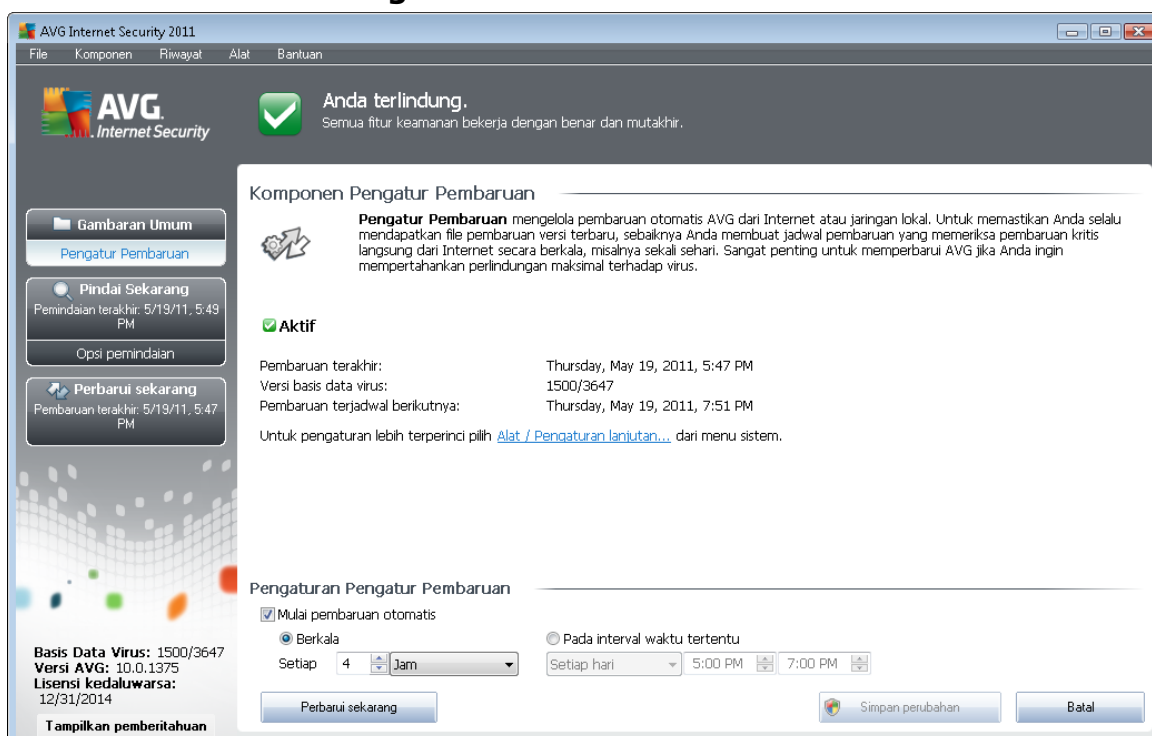
Tidak ada perangkat lunak keamanan yang dapat menjamin perlindungan sesungguhnya dari berbagai tipe ancaman, kecuali jika rutin diperbarui! Penulis virus selalu mencari kelemahan baru yang dapat mereka eksploitir dalam perangkat lunak maupun sistem operasi. Virus baru, malware baru, serangan peretas baru muncul setiap hari. Karena alasan ini, vendor perangkat lunak terus mengeluarkan pembaruan dan penambal keamanan, untuk memperbaiki berbagai lubang keamanan yang ditemukan.

Sangatlah penting memperbarui AVG Anda secara rutin!

Pengatur pembaruan membantu Anda mengontrol pembaruan rutin. Dalam komponen ini Anda dapat menjadwalkan unduh otomatis atas file pembaruan baik dari Internet ataupun jaringan lokal. Pembaruan definisi virus penting harus dilakukan setiap hari jika memungkinkan. Pembaruan program yang kurang penting bisa dilakukan setiap minggu.

Catatan: Perhatikanlah bab [Pembaruan AVG](#) untuk informasi lebih lanjut mengenai tipe dan tingkat pembaruan!

7.10.2. Antarmuka Pengatur Pembaruan





Antarmuka **Pengatur Pembaruan** menampilkan informasi mengenai fungsionalitas komponen dan status saat ini, dan menyediakan data statistik yang relevan.

- **Pembaruan terkini** - menetapkan tanggal dan waktu pembaruan basis data terakhir
- **Versi basis data virus** - menunjukkan nomor versi basis data virus terbaru, dan nomor ini terus bertambah setiap kali basis virus diperbarui
- **Pembaruan terjadwal berikutnya** - menetapkan tanggal dan waktu pembaruan basis data berikutnya

Pengaturan Pengatur Pembaruan

Di bagian bawah dialog, Anda dapat menemukan bagian **Pengaturan Pengatur Pembaruan** di mana Anda dapat mengubah aturan peluncuran proses pembaruan. Anda dapat menentukan apakah ingin agar file pembaruan diunduh secara otomatis (**Mulai pembaruan otomatis**) atau bila diperlukan saja. Secara default, opsi **Mulai pembaruan otomatis** telah diaktifkan dan kami sarankan untuk membiarkannya! Mengunduh file pembaruan terbaru secara rutin sangatlah penting agar perangkat lunak keamanan berfungsi dengan semestinya!

Lebih lanjut, Anda dapat menentukan kapan pembaruan harus diluncurkan:

- o **Secara berkala** - menentukan interval waktu
- o **Pada interval waktu tertentu** - tentukan saat pembaruan harus diluncurkan

Secara default, pembaruan diatur setiap 4 jam. Anda disarankan untuk tetap menggunakan pengaturan ini kecuali Anda punya alasan yang kuat untuk mengubahnya!

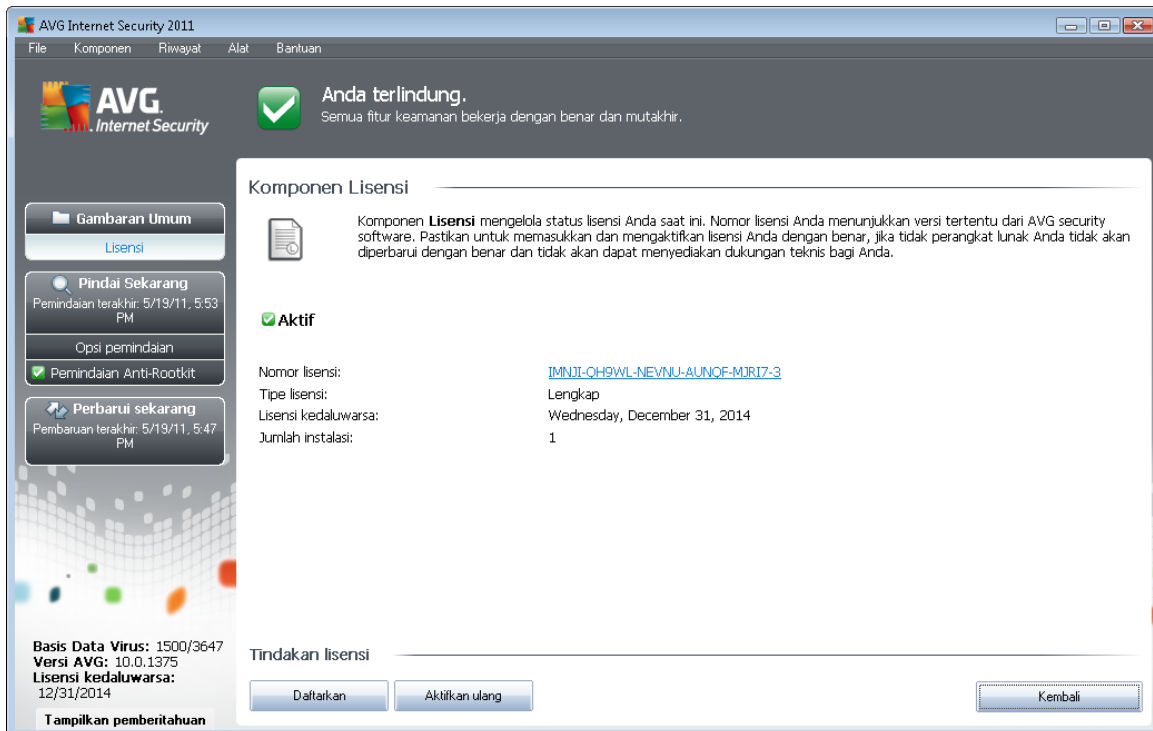
Perhatikan: Penjual perangkat lunak telah mengatur semua komponen AVG untuk memberikan performa optimal. Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG. Semua perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman. Jika Anda perlu mengubah konfigurasi AVG, 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 antarmuka **Pengatur Pembaruan** adalah sebagai berikut:

- **Perbarui sekarang** - meluncurkan [pembaruan dengan segera](#) saat diperlukan
- **Simpan perubahan** - tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini
- **Batalkan** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (gambaran umum komponen)

7.11. Lisensi



Dalam antarmuka komponen **Lisensi** Anda akan menemukan teks singkat yang menjelaskan fungsionalitas komponen, dan informasi status saat ini dan informasi berikut:

- **Nomor lisensi** - memberikan bentuk singkat nomor lisensi Anda (*untuk alasan keamanan empat simbol terakhir dihilangkan*). Saat memasukkan nomor lisensi, Anda harus benar-benar persis mengetikkannya seperti yang ditampilkan. Oleh karena itu, kami sangat menyarankan agar Anda selalu menggunakan metode "salin & tempel" untuk perubahan apa pun terhadap nomor lisensi.
- **Tipe lisensi** - menentukan tipe produk yang diinstal.
- **Lisensi kedaluwarsa** - tanggal ini menentukan masa berlaku lisensi Anda. Jika Anda ingin terus menggunakan **Keamanan Internet AVG 2011** setelah tanggal ini, Anda harus memperpanjang lisensi Anda. Perpanjangan lisensi dapat dilakukan secara online pada [situs Web AVG](http://www.avg.com/).
- **Jumlah kursi** - jumlah workstation yang dapat Anda instal dengan **Keamanan Internet AVG 2011**.

Tombol kontrol

- **Daftar** - menghubungkan ke halaman pendaftaran situs Web AVG (<http://www.avg.com/>). Masukkan data pendaftaran Anda; hanya pelanggan yang mendaftarkan produk AVG mereka yang dapat menerima dukungan teknis gratis.

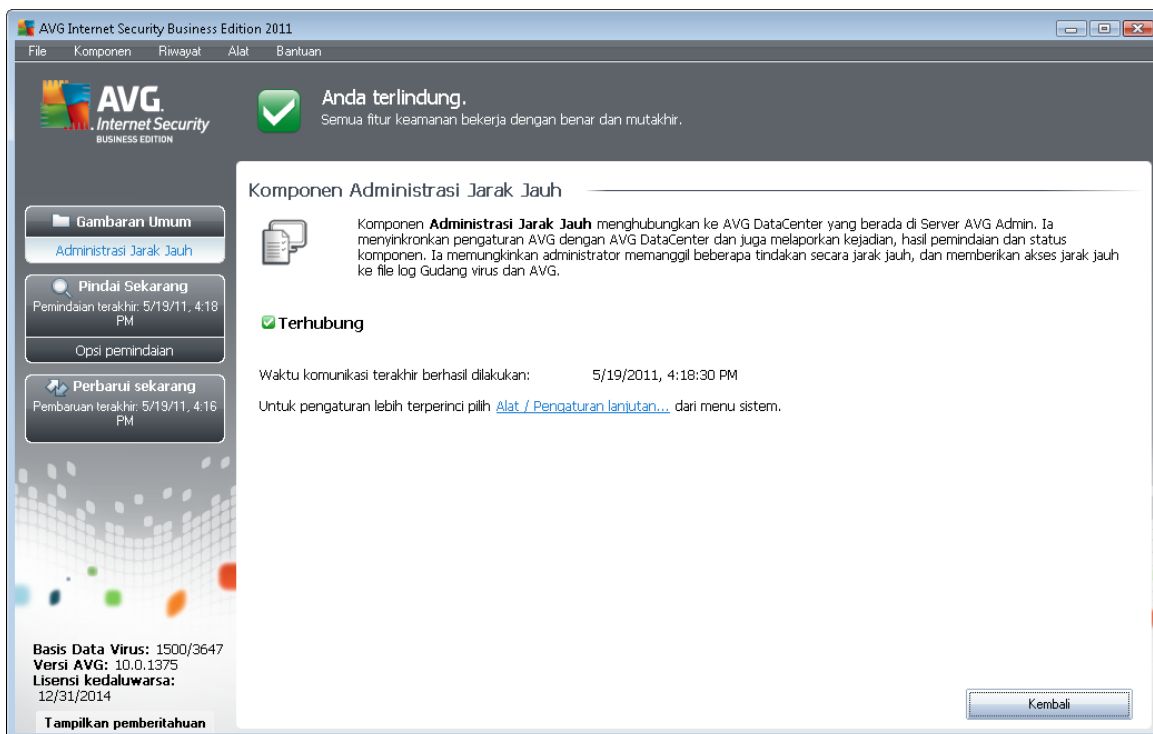


- **Aktifkan Ulang** - membuka dialog **Aktifkan AVG** berisi data yang telah Anda masukkan dalam dialog **Personalisasi AVG** pada [proses instalasi](#). Dalam dialog ini Anda dapat memasukkan nomor lisensi untuk menggantikan nomor penjualan (*nomor yang Anda gunakan untuk menginstal AVG*), atau untuk mengganti nomor lisensi lama (*misalnya, saat meningkatkan ke produk AVG baru*).

Catatan: Jika menggunakan versi uji coba **Keamanan Internet AVG 2011**, tombol akan muncul sebagai **Beli sekarang** dan **Aktifkan**, yang memungkinkan Anda membeli versi lengkap dari program ini saat itu juga. Untuk **Keamanan Internet AVG 2011** yang terinstal dengan nomor penjualan, tombol yang ditampilkan adalah **Daftarkan** dan **Aktifkan**.

- **Kembali** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (gambaran umum komponen).

7.12. Administrasi Jarak Jauh



Komponen **Administrasi Jarak Jauh** hanya ditampilkan pada antarmuka pengguna **Keamanan Internet AVG 2011** jika Anda telah menginstal produk Business Edition (*lihat komponen [Lisensi](#)*). Dalam dialog **Administrasi Jarak Jauh** Anda dapat menemukan informasi tentang komponen yang aktif dan terhubung dengan server. Semua pengaturan komponen **Administrasi Jarak Jauh** dilakukan melalui **Pengaturan Lanjutan/Administrasi Jarak Jauh**.

Untuk keterangan terperinci atas berbagai opsi komponen dan fungsionalitasnya dalam sistem AVG Remote Administration, bacalah dokumentasi spesifik khusus untuk topik ini. Dokumentasi ini tersedia untuk diunduh di [situs Web AVG \(www.avg.com\)](http://www.avg.com), di bagian **Pusat dukungan/Unduhan/Dokumentasi**.



Tombol kontrol

- **Kembali** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (*gambaran umum komponen*).

7.13. Online Shield

7.13.1. Prinsip-Prinsip Online Shield

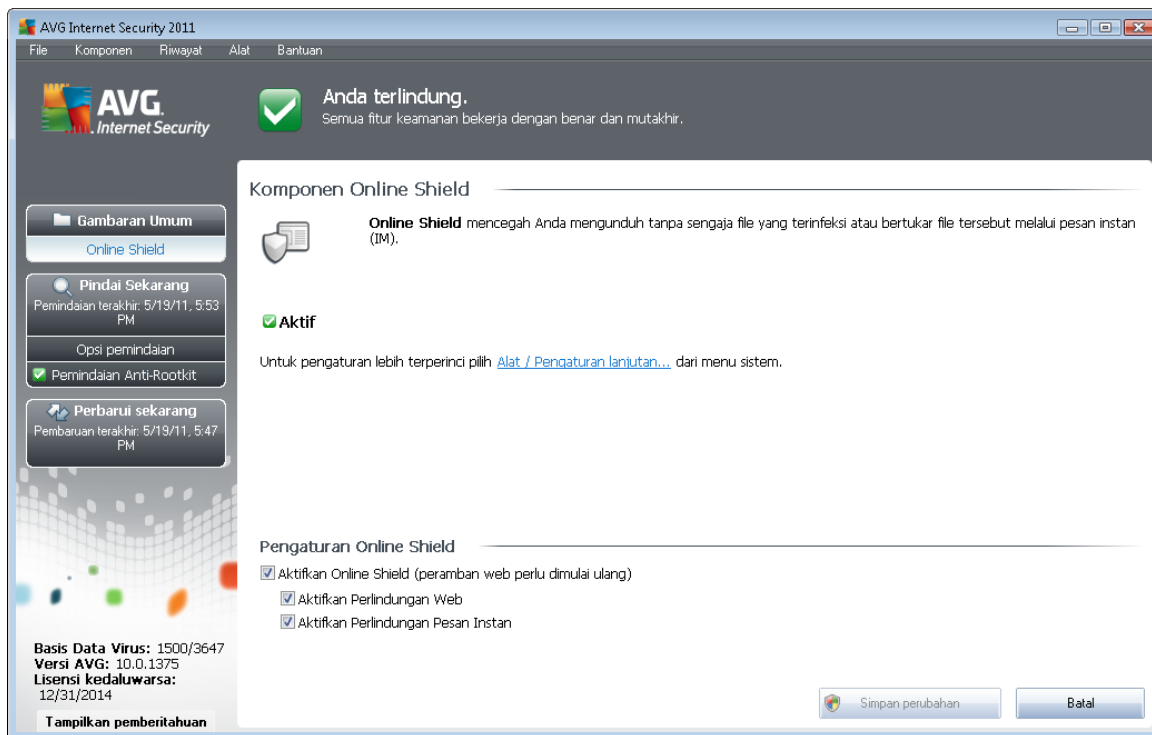
Online Shield adalah sebuah tipe perlindungan menetap secara waktu nyata yang memindai isi halaman web yang dikunjungi (*dan file yang mungkin termasuk di dalamnya*) bahkan sebelum halaman ditampilkan di peramban web Anda atau diunduh ke komputer.

Online Shield mendeteksi apakah halaman yang akan Anda kunjungi berisi javascript berbahaya dan mencegah halaman tersebut untuk ditampilkan. Selain itu, ia akan mengenali malware yang dimasukkan dalam sebuah halaman dan segera menghentikan unduhannya agar jangan sampai masuk ke komputer Anda.

Catatan: AVG Online Shield tidak ditujukan untuk platform server!

7.13.2. Antarmuka Online Shield

Antarmuka komponen **Online Shield** menerangkan cara kerja tipe perlindungan ini. Selanjutnya Anda dapat menemukan informasi tentang status saat ini. Di bagian bawah dialog, Anda akan menemukan opsi pengeditan dasar untuk fungsionalitas komponen ini:



Pengaturan Online Shield

Pertama-tama, Anda punya opsi untuk segera mengaktifkan/menonaktifkan **Online Shield** dengan mencentang item **Aktifkan Online Shield**. Opsi ini telah diaktifkan secara default, dan komponen **Online Shield** aktif. Walau demikian, jika Anda tidak mempunyai alasan yang kuat untuk mengubah pengaturan ini, kami menyarankan untuk tetap membiarkan komponen ini aktif. Jika item ini dicentang, dan **Online Shield** sedang berjalan, dua opsi konfigurasi lainnya akan diaktifkan:

- **Aktifkan Perlindungan Web**- opsi ini mengkonfirmasi bahwa **Online Shield** harus melakukan pemindaian atas isi situs Web.
- **Aktifkan perlindungan Pesan Instan** - tandai item ini jika Anda ingin **Online Shield** memverifikasi bahwa komunikasi pesan instan (*misalnya ICQ, MSN Messenger, ...*) bebas virus.

Perhatikan: Penjual 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 antarmuka **Online Shield** adalah sebagai berikut:



- **Simpan perubahan** - tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini
- **Batalan** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG](#) default (gambaran umum komponen)

7.13.3. Deteksi Online Shield

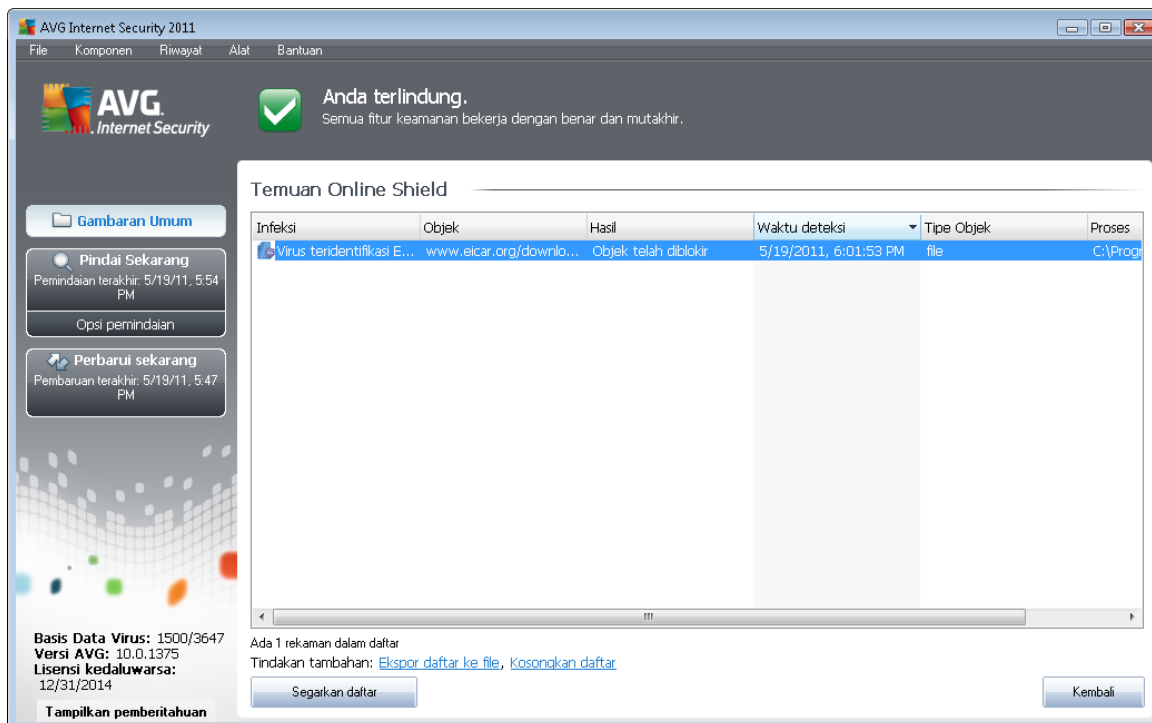
Online Shield memindai isi halaman web yang dikunjungi dan mungkin file yang dimasukkan di dalamnya bahkan sebelum halaman ditampilkan di peramban web Anda atau diunduh ke komputer. Bila ada ancaman yang terdeteksi, Anda akan segera diperingatkan dengan dialog berikut:



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 diketahui*). 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** - gambaran 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 **Segarkan daftar** akan memperbarui daftar temuan yang terdeteksi oleh **Online Shield**. Tombol **Kembali** akan mengembalikan Anda ke [antarmuka pengguna AVG](#) default (*gambaran umum komponen*).

7.14. Anti-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

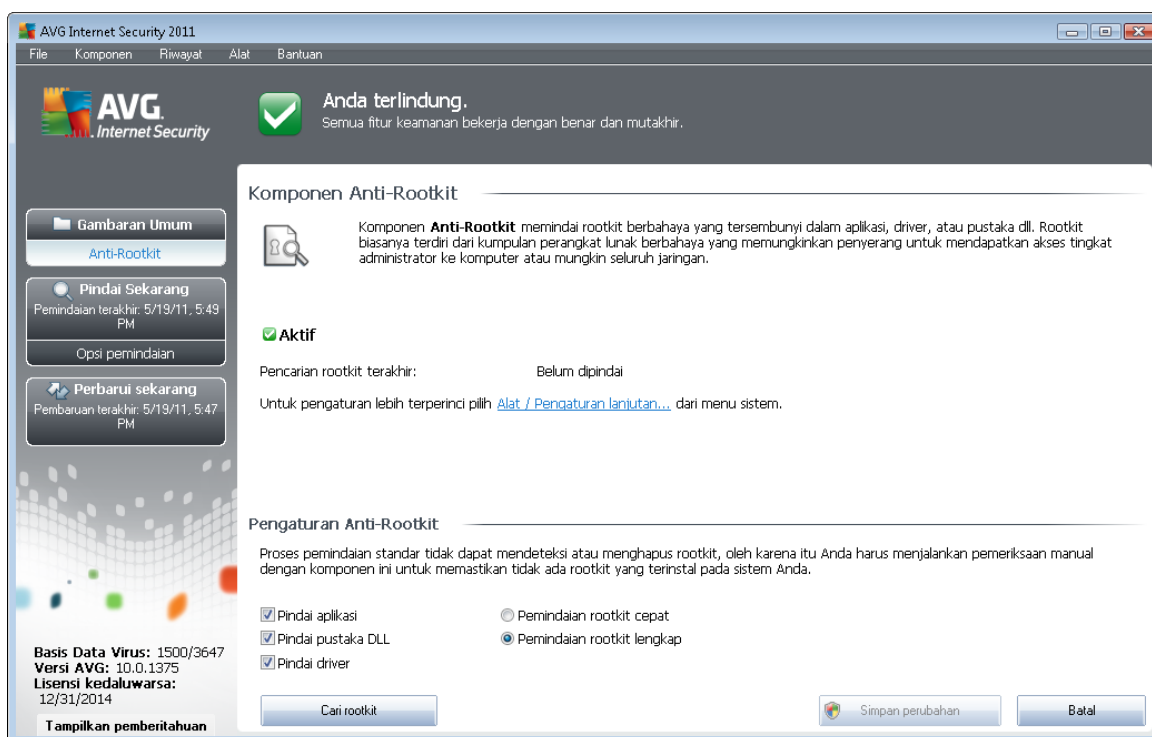


perangkat keras tersebut. Biasanya, rootkit mengaburkan kehadirannya pada sistem dengan menyusup ke atau mengelakkan mekanisme keamanan sistem operasi standar. Seringkali, mereka juga berupa Trojan, yang memperdaya pengguna agar menganggapnya aman dijalankan pada sistem mereka. Berbagai teknik digunakan untuk melakukan hal ini termasuk merahasiakan proses yang sedang berjalan dari program pemantau, atau menyembunyikan file atau data sistem dari sistem operasi.

7.14.1. Prinsip-Prinsip Anti-Rootkit

AVG 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. **AVG Anti-Rootkit** mampu mendeteksi rootkit berdasarkan seperangkat aturan yang ditentukan. Perhatikan, semua rootkit dideteksi (*tidak hanya yang terinfeksi*). Jika **AVG Anti-Rootkit** menemukan rootkit, tidak berarti komputer tersebut terinfeksi. Kadang, rootkit digunakan sebagai driver atau bagian dari aplikasi yang benar.

7.14.2. Antarmuka Anti-Rootkit



Antarmuka pengguna **Anti-Rootkit** memberikan gambaran singkat fungsionalitas komponen, menginformasikan status komponen saat ini, dan juga membawa informasi tentang terakhir kali tes **Anti-Rootkit** diluncurkan (**Pencarian rootkit terakhir**). Dialog **Anti-Rootkit** selanjutnya memberikan tautan [Alat/Pengaturan Lanjutan](#). Gunakan tautan untuk diarahkan kembali ke lingkungan konfigurasi lanjutan komponen **Anti-Rootkit**.

Perhatikan: Penjual 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 Anti-Rootkit

Di bagian bawah dialog, Anda dapat menemukan bagian **Pengaturan Anti-Rootkit** di mana Anda dapat mengatur beberapa fungsi dasar dari pemindaian kehadiran rootkit. Pertama, tandai kotaknya untuk menetapkan objek yang harus dipindai:

- **Pindai aplikasi**
- **Pindai pustaka DLL**
- **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 floppy-disk/drive CD*)

Tombol kontrol

- **Cari rootkit** - karena pemindaian rootkit bukan bagian implisit dari [Pindai seluruh 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 [antarmuka pengguna AVG default](#) (*gambaran umum komponen*)
- **Batalan** - tekan tombol ini untuk kembali ke [antarmuka pengguna AVG default](#) (*gambaran umum komponen*) tanpa menyimpan perubahan yang telah Anda buat

7.15. Alat Sistem

Alat Sistem merujuk pada alat yang menyediakan ringkasan terperinci mengenai lingkungan dan sistem operasi **Keamanan Internet AVG 2011**. 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

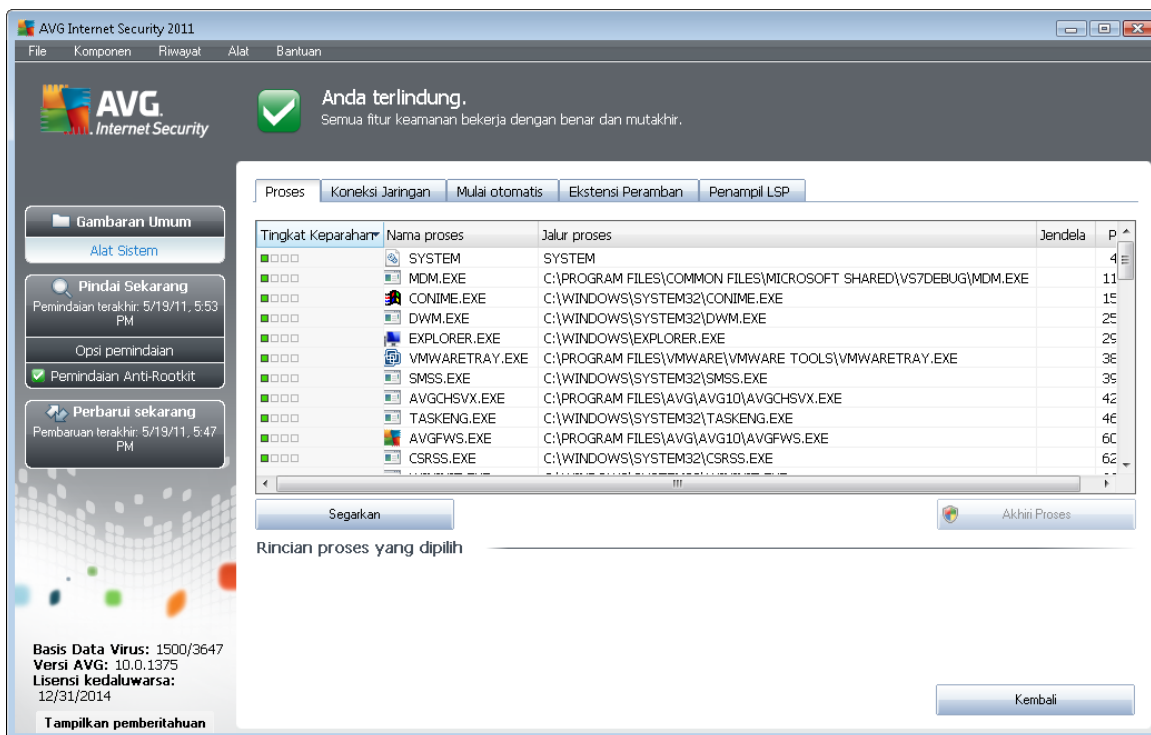


Internet Anda

- [Penampil LSP](#) - daftar Layered Service Provider (LSP)

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

7.15.1. 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 pengenalan proses internal Windows

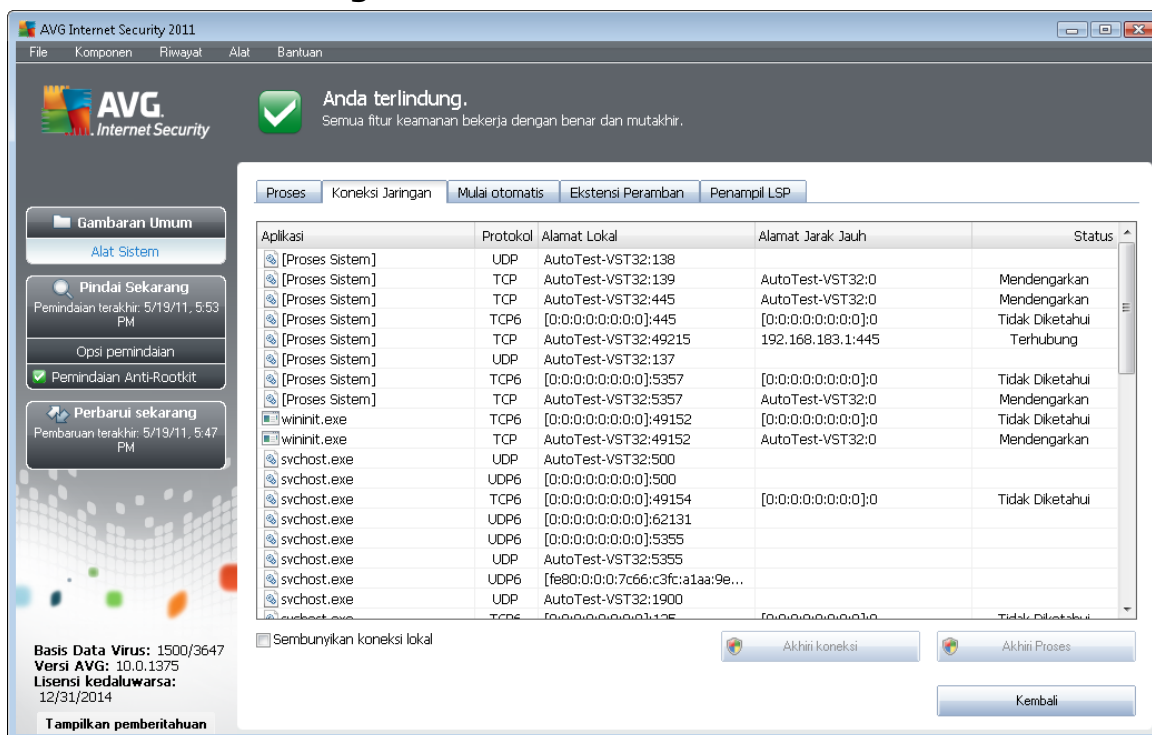
Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka **Alat Sistem** 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** - akan mengembalikan Anda ke [antarmuka pengguna AVG](#) default (gambaran umum komponen)

7.15.2. 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:
 - o TCP - protokol yang digunakan bersama dengan Internet Protocol (IP) untuk mengirim informasi melalui Internet
 - o 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.

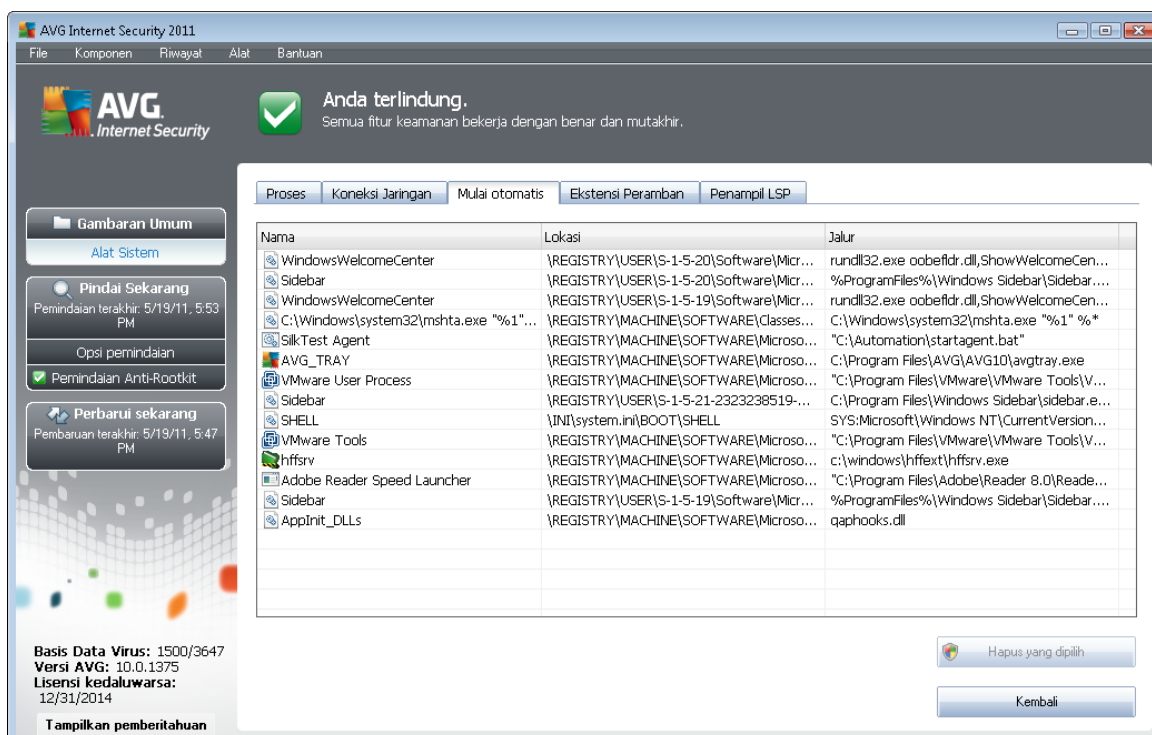
Tombol kontrol

Tombol kontrol yang tersedia adalah:

- **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 [antarmuka pengguna AVG](#) default (gambaran 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!

7.15.3. Mulai otomatis



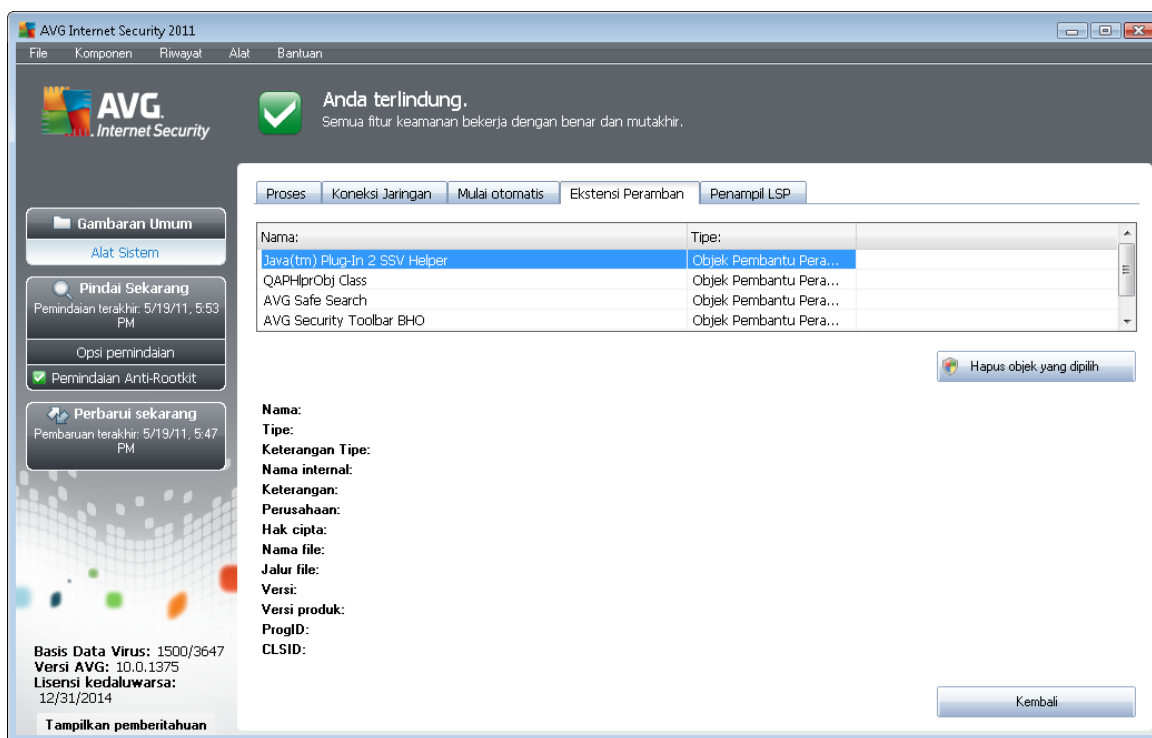


Dialog **Mulai Otomatis** menampilkan daftar semua aplikasi yang dijalankan selama menjalankan ulang sistem Windows. Sering sekali, beberapa aplikasi malware menambahkan diri mereka sendiri ke entri register start-up secara otomatis.

Anda dapat menghapus satu atau beberapa entri dengan memilihnya dan menekan tombol **Hapus yang dipilih**. Tombol **Kembali** akan mengembalikan Anda ke [antarmuka pengguna AVG](#) default (gambaran 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!

7.15.4. 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

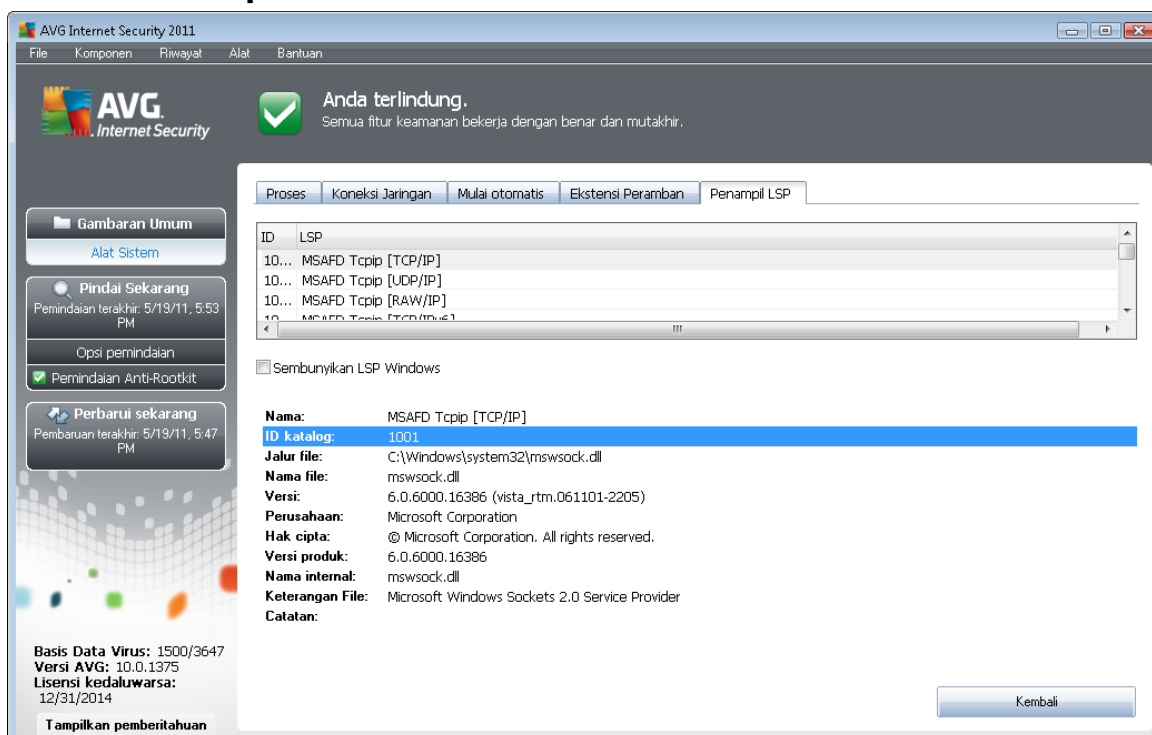
Tombol kontrol yang tersedia pada tab **Ekstensi Peramban** adalah:

- **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** - akan mengembalikan Anda ke [antarmuka pengguna AVG](#) default (gambaran umum komponen)

7.15.5. Penampil LSP



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

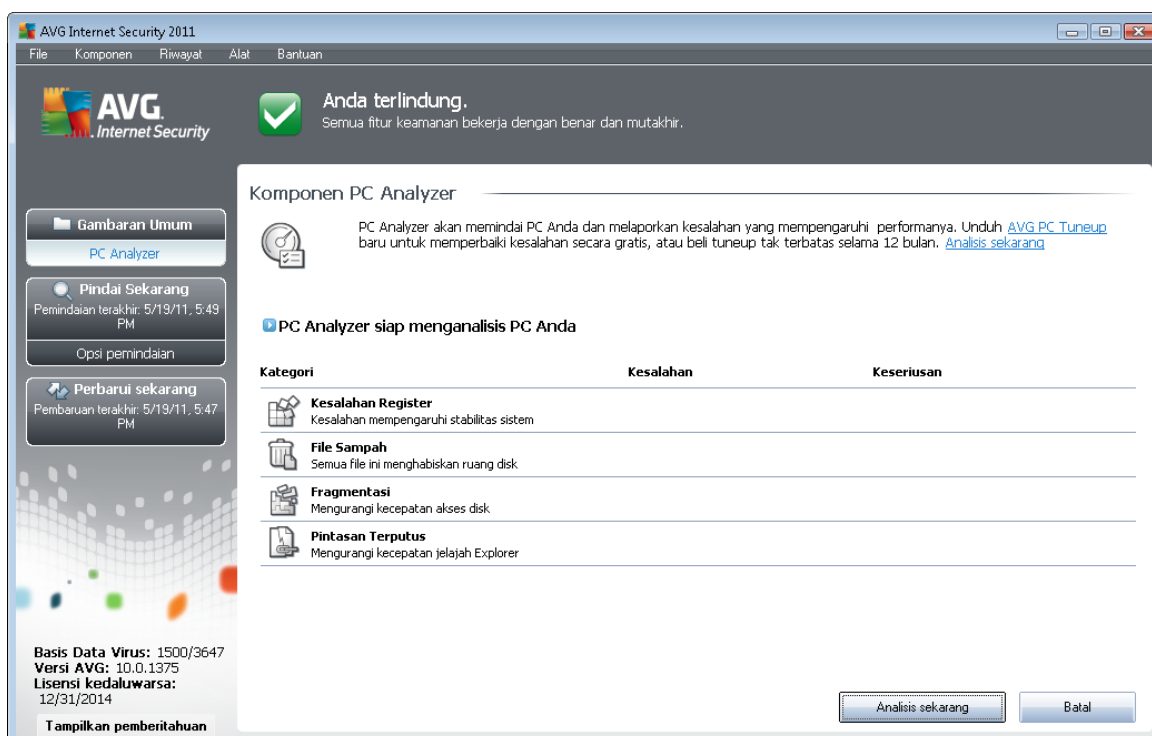
Layered Service Provider (LSP) adalah driver sistem yang tertaut dengan layanan jaringan sistem operasi Windows. Di sini Anda dapat mengakses semua data yang masuk dan keluar komputer, termasuk mengubah data ini. Beberapa LSP diperlukan agar Windows dapat menghubungkan Anda ke komputer lain, termasuk 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.

Untuk memasukkan LSP Windows ke dalam daftar, hapus centang di kotak **Sembunyikan LSP Windows**. Tombol **Kembali** akan mengembalikan Anda ke [antarmuka pengguna AVG](#) default (gambaran umum komponen).

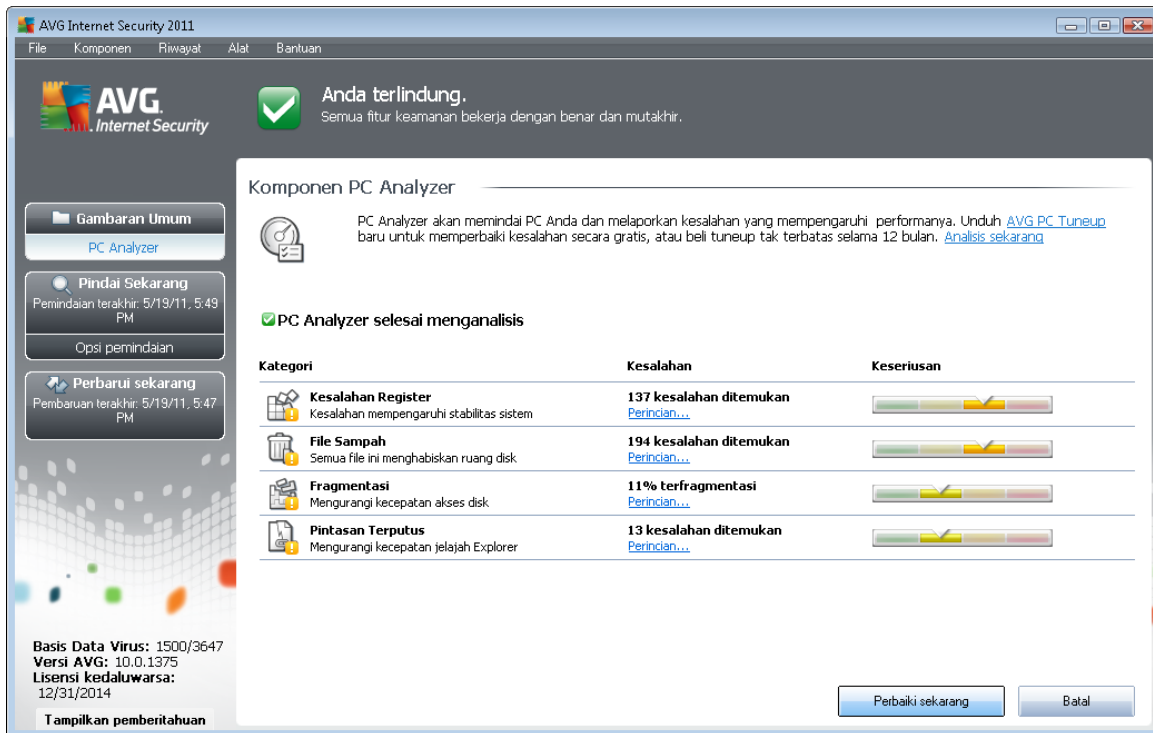
7.16. PC Analyzer

Komponen **PC Analyzer** dapat melakukan pemindaian masalah sistem pada komputer Anda, dan memberi Anda gambaran 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 harddisk yang difragmentasi, 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:



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

Tombol kontrol

- **Analisis sekarang** (ditampilkan sebelum analisis dimulai) - tekan tombol ini untuk segera meluncurkan analisis 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**
- **Batalkan** - tekan tombol ini untuk menghentikan analisis yang sedang berjalan, atau kembali ke komponen default [antarmuka pengguna AVG](#) (gambaran umum) setelah analisis selesai

7.17. Perlindungan ID

AVG Identity Protection adalah produk anti-malware yang fokus untuk mencegah pencuri identitas mencuri kata sandi, perincian rekening bank, nomor kartu kredit, dan harta digital pribadi lainnya dari semua jenis perangkat lunak jahat (*malware*) yang menarget PC Anda. AVG Identity Protection memastikan semua program yang berjalan pada PC Anda beroperasi dengan benar. **AVG Identity Protection** menemukan dan memblokir perilaku mencurigakan secara terus-menerus dan melindungi komputer Anda dari semua malware baru.

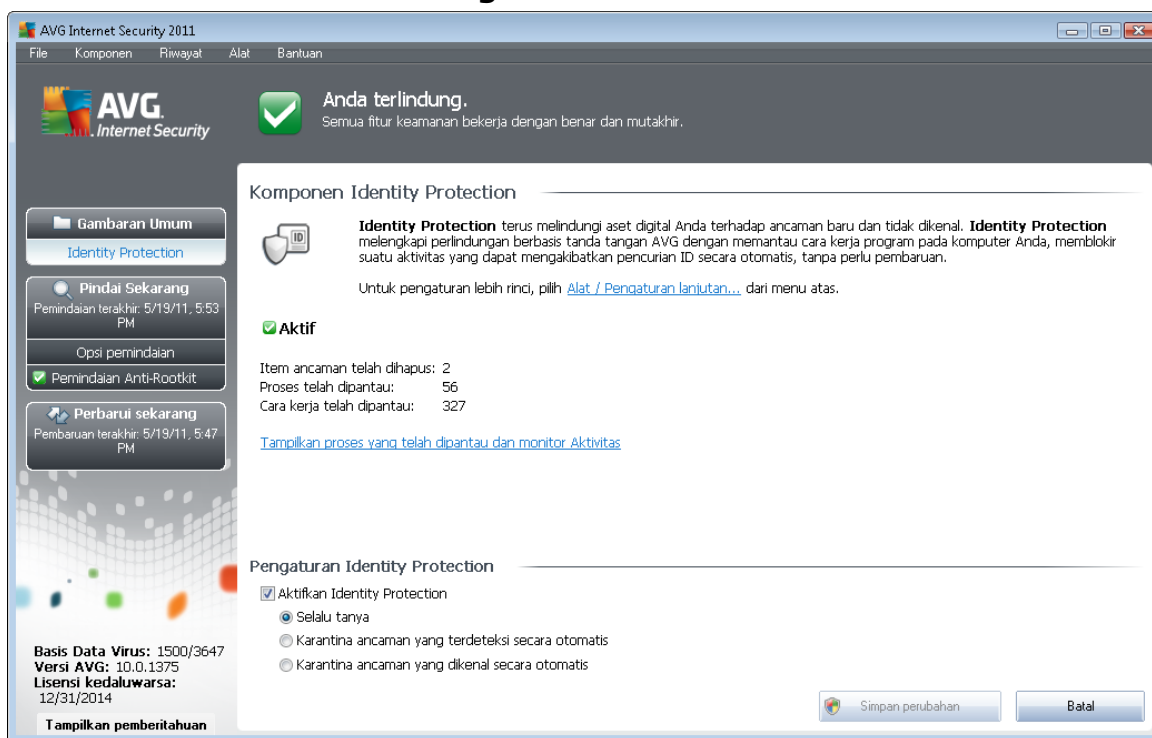


7.17.1. Prinsip-Prinsip Perlindungan ID

AVG Identity Protection merupakan komponen anti-malware yang melindungi Anda dari semua jenis malware (*spyware, bot, pencuri identitas, ...*) menggunakan teknologi perilaku dan memberikan perlindungan setiap hari dari virus baru. Saat malware menjadi semakin canggih dan masuk dalam bentuk program biasa yang dapat membuka PC Anda untuk penyusup luar yang mencuri identitas, **AVG Identity Protection** mengamankan Anda dari program baru berbasis malware ini. Ini adalah perlindungan pelengkap untuk **AVG Anti-Virus** yang melindungi Anda dari virus berbasis file dan yang telah dikenal menggunakan mekanisme tanda tangan dan pemindaian.

*Kami sangat menyarankan agar Anda menginstal kedua aplikasi **AVG Anti-Virus** dan **AVG Identity Protection**, untuk mendapatkan perlindungan penuh bagi PC Anda.*

7.17.2. Antarmuka Perlindungan ID



Antarmuka komponen **Perlindungan Identitas** memberikan gambaran singkat tentang fungsionalitas dasar komponen, status dan beberapa data statistik:

- **Item malware 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 gambaran terperinci tentang seluruh proses yang diawasi.

Pengaturan Perlindungan Identitas

Di bagian bawah dialog, Anda akan melihat bagian **Pengaturan Perlindungan Identitas** di mana Anda dapat mengedit beberapa fitur dasar fungsionalitas komponen:

- **Aktifkan Perlindungan Identitas** - (*diaktifkan secara default*): centang untuk mengaktifkan komponen IDP, dan untuk membuka opsi pengeditan lebih lanjut.

Dalam beberapa kasus, **Perlindungan Identitas** mungkin melaporkan bahwa beberapa file yang sah bersifat mencurigakan atau berbahaya. Karena **Perlindungan Identitas** 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 **Perlindungan Identitas** jika ada deteksi aktivitas yang mencurigakan:

- o **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*)
- o **Karantina ancaman yang terdeteksi secara otomatis** - semua aplikasi yang terdeteksi sebagai malware akan diblokir secara otomatis
- o **Karantina ancaman yang dikenal secara otomatis** - hanya aplikasi yang benar-benar pasti terdeteksi sebagai malware yang akan diblokir

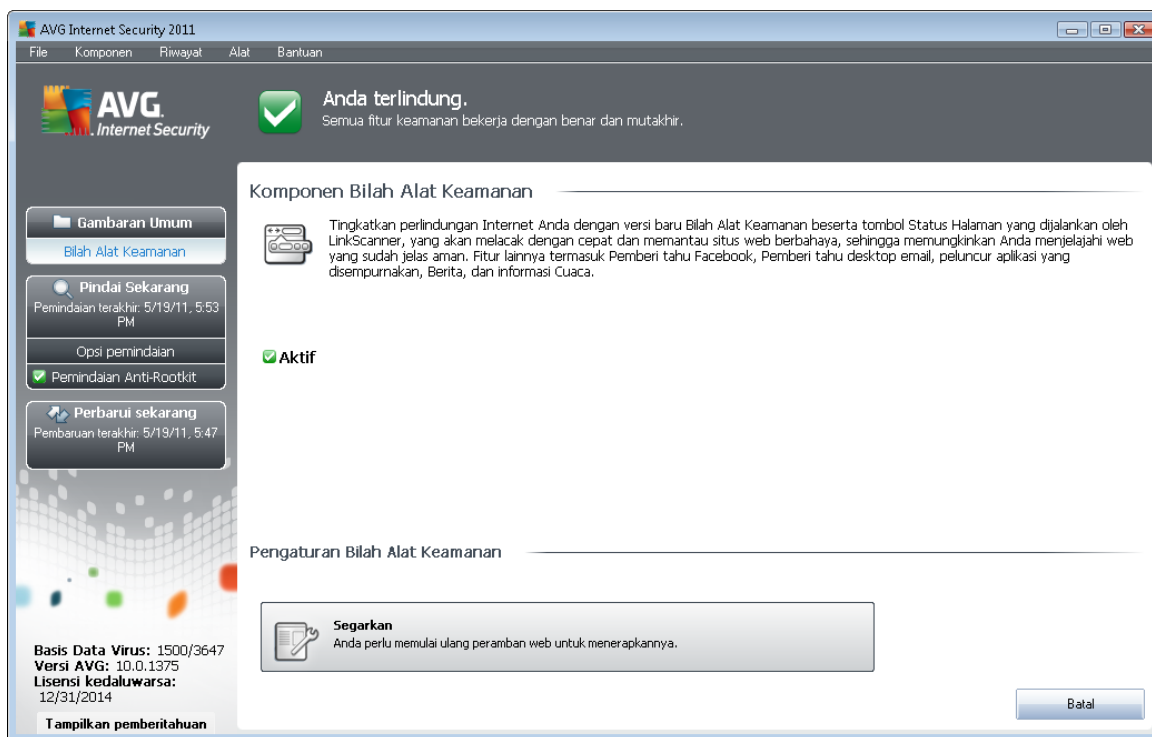
Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka **Perlindungan Identitas** 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 [antarmuka pengguna AVG](#) default (*gambaran umum komponen*)

7.18. Security Toolbar

Security Toolbar adalah bilah alat peramban Web opsional, yang menawarkan perlindungan AVG yang ditingkatkan dan berbagai fitur serta alat berguna saat menjelajahi Web. Saat ini, **Security Toolbar** didukung oleh peramban Internet Explorer (6.0 atau yang lebih tinggi), dan Mozilla Firefox (3.0 atau yang lebih tinggi):



Semua pengaturan komponen **Security Toolbar** dapat diakses langsung dalam [Security Toolbar](#) dalam peramban Web Anda.



8. AVG Security Toolbar

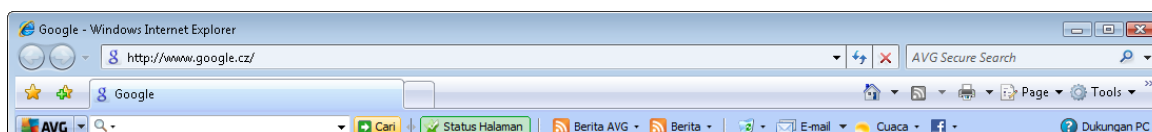
AVG Security Toolbar adalah alat baru yang bekerja sama dengan komponen [LinkScanner](#). **AVG Security Toolbar** dapat digunakan untuk mengontrol fungsi komponen [LinkScanner](#) dan untuk menyesuaikan perilakunya.

Jika Anda memilih untuk menginstal bilah alat saat instalasi **Keamanan Internet AVG 2011**, maka bilah akan ditambahkan ke peramban web Anda (*Internet Explorer 6.0 atau yang lebih baru, dan Mozilla Firefox 3.0 atau yang lebih baru*) secara otomatis. Peramban internet lain untuk saat ini tidak didukung.

Catatan: Jika Anda menggunakan peramban Internet alternatif (mis. Avant Browser) maka Anda dapat menemui cara kerja yang tidak terduga.

8.1. Antarmuka AVG Security Toolbar

AVG Security Toolbar dirancang untuk bekerja bersama dengan **MS Internet Explorer** (versi 6.0 atau yang lebih tinggi) dan **Mozilla Firefox** (versi 3.0 atau yang lebih tinggi). Setelah Anda memutuskan untuk menginstal **AVG Security Toolbar** (selama [proses instalasi AVG](#) Anda akan diminta untuk memutuskan apakah Anda ingin menginstal komponen ini atau tidak), komponen ini akan diletakkan di peramban web Anda tepat di bawah bilah alamat:



AVG Security Toolbar terdiri dari berikut ini:

8.1.1. Tombol logo AVG

Tombol ini memberikan akses ke item bilah alat umum. Klik tombol logo agar dialihkan ke [situs Web AVG](#). Mengklik pointer di sebelah ikon AVG akan membuka item berikut:

- **Info Toolbar** - menautkan ke halaman utama **AVG Security Toolbar** bersama informasi terperinci mengenai perlindungan toolbar
- **Luncurkan AVG** - membuka **Keamanan Internet AVG 2011** [antarmuka pengguna AVG](#)
- **Info AVG** - membuka menu konteks dengan tautan berikut tentang informasi keamanan penting terkait dengan **Keamanan Internet AVG 2011**:
 - o *Tentang Ancaman* - membuka [situs web AVG](#) pada halaman yang menampilkan data paling penting tentang ancaman teratas, rekomendasi penghapusan virus, pembaruan AVG, akses ke [basis data Virus](#) dan info yang lebih relevan
 - o *Berita AVG* - membuka halaman web yang menyediakan pernyataan pers terbaru yang berkaitan dengan AVG

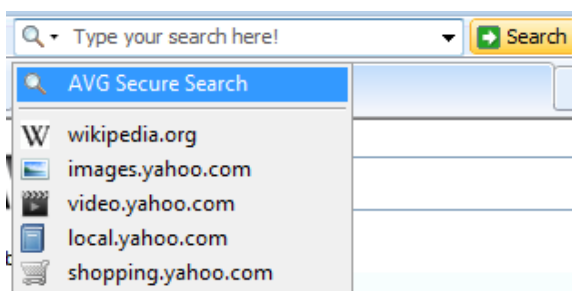


- o *Tingkat Ancaman Saat Ini* - membuka halaman Web lab virus yang berisi tampilan grafis mengenai tingkat ancaman saat ini di Web
- o *Lab Ancaman AVG* - membuka situs web [Laporan Situs AVG](#) tempat Anda dapat mencari ancaman tertentu berdasarkan nama dan mendapatkan informasi terperinci untuk masing-masing ancaman
- **Opsi** - membuka dialog konfigurasi di mana Anda dapat menyesuaikan pengaturan **AVG Security Toolbar** untuk memenuhi kebutuhan Anda - lihat bab berikut [Opsi AVG Security Toolbar](#)
- **Hapus Riwayat** - memungkinkan Anda dalam **AVG Security Toolbar** menghapus riwayat lengkap, atau secara terpisah menghapus riwayat penelusuran, menghapus riwayat peramban, menghapus riwayat unduhan dan menghapus cookie.
- **Perbarui** - akan memeriksa pembaruan baru bagi **AVG Security Toolbar Anda**
- **Bantuan** - menyediakan opsi untuk membuka file bantuan, menghubungi [dukungan teknis AVG](#), mengirimkan masukan terkait produk atau melihat perincian versi Toolbar saat ini

8.1.2. Kotak telusur yang didukung AVG Secure Search (powered by Google)

Kotak **AVG Secure Search (powered by Google)** adalah cara mudah dan aman untuk menelusuri Web menggunakan AVG Secure Search (powered by Google). Masukkan kata atau frasa ke dalam kotak telusur kemudian tekan tombol **Telusuri**, atau tombol **Enter**, untuk mulai menelusuri langsung pada server AVG Secure Search (powered by Google), halaman apa pun yang saat ini sedang ditampilkan. Kotak telusur juga menampilkan daftar riwayat penelusuran Anda. Penelusuran yang dilakukan melalui kotak telusur akan dianalisis menggunakan perlindungan [Search-Shield](#).

Cara lainnya, dengan bidang penelusuran, Anda dapat beralih ke Wikipedia atau beberapa layanan penelusuran lainnya - lihat gambar:



8.1.3. Status Halaman

Langsung pada bilah alat, tombol ini menampilkan evaluasi halaman web yang sedang ditampilkan berdasarkan kriteria komponen [Surf-Shield](#):

- - Halaman tertaut aman
- - Halaman agak mencurigakan.

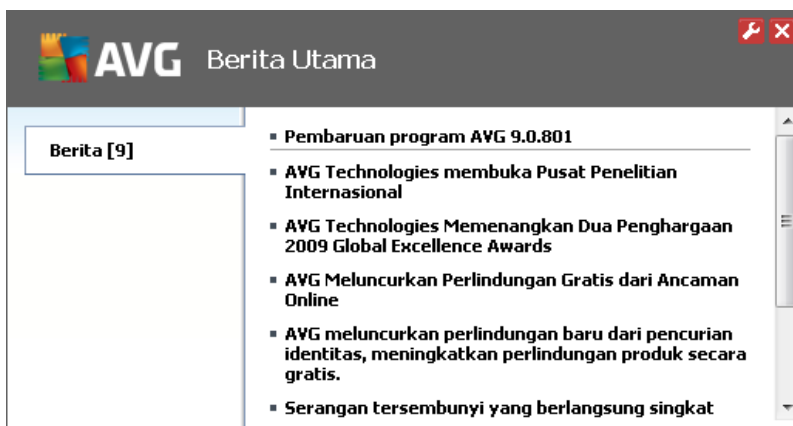


-  - Halaman berisi tautan ke halaman yang dipastikan berbahaya.
-  - Halaman tertaut berisi ancaman yang aktif! Demi keamanan, Anda tidak akan diperbolehkan mengunjungi halaman ini.
-  - Halaman tidak dapat diakses, sehingga tidak dapat dipindai.

Klik tombol ini untuk membuka panel informasi yang berisi data terperinci mengenai halaman web tertentu.

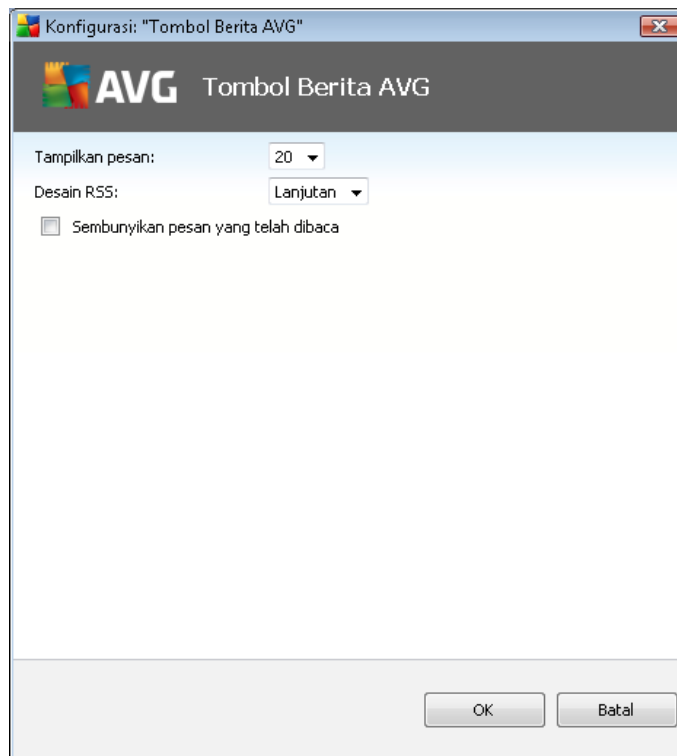
8.1.4. Berita AVG

Langsung dari **AVG Security Toolbar**, tombol ini membuka gambaran umum terbaru **Judul berita utam**aterkait AVG, baik berita dari pers maupun rilis pers perusahaan:



Di pojok kanan atas, Anda dapat melihat dua tombol kontrol merah:

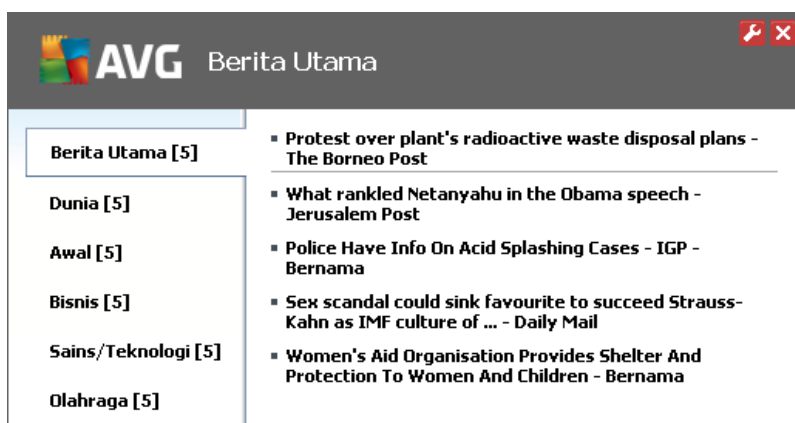
-  - tombol membuka dialog pengeditan tempat Anda dapat menentukan parameter untuk tombol **Berita AVG** yang ditampilkan dalam **AVG Security Toolbar**:



- o **Pesan yang ditampilkan** - mengubah jumlah pesan yang ingin ditampilkan pada satu waktu
- o **Rancangan RSS** - pilih antara mode Lanjutan/Dasar dari tampilan gambaran umum berita saat ini (*secara default, mode Lanjutan yang dipilih - lihat gambar di bawah*)
- o **Sembunyikan pesan yang sudah dibaca** - tandai pilihan ini untuk mengonfirmasi bahwa setiap pesan yang telah dibaca tidak perlu ditampilkan lagi, sehingga pesan baru dapat ditampilkan
-  - klik tombol ini untuk menutup gambaran umum berita yang sedang terbuka.

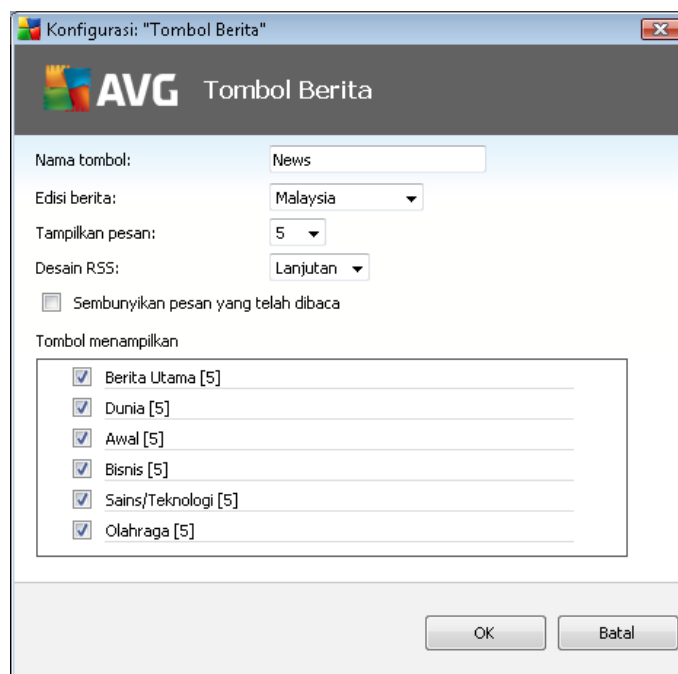
8.1.5. Berita

Demikian pula, langsung dari **AVG Security Toolbar**, tombol ini membuka gambaran umum berita terakhir dari media terpilih yang dibagi dalam beberapa bagian:



Di pojok kanan atas, Anda dapat melihat dua tombol kontrol merah:

-  - tombol ini membuka dialog pengeditan tempat Anda dapat menentukan parameter tombol **Berita** yang ditampilkan dalam **AVG Security Toolbar**:



- o **Nama tombol** - Anda memiliki opsi untuk mengubah nama tombol yang akan ditampilkan pada **AVG Security Toolbar**
- o **Edisi berita** - pilih negara dari daftar untuk menampilkan berita dari wilayah yang dipilih
- o **Pesan yang ditampilkan** - menentukan jumlah pesan yang ingin ditampilkan pada saat bersamaan



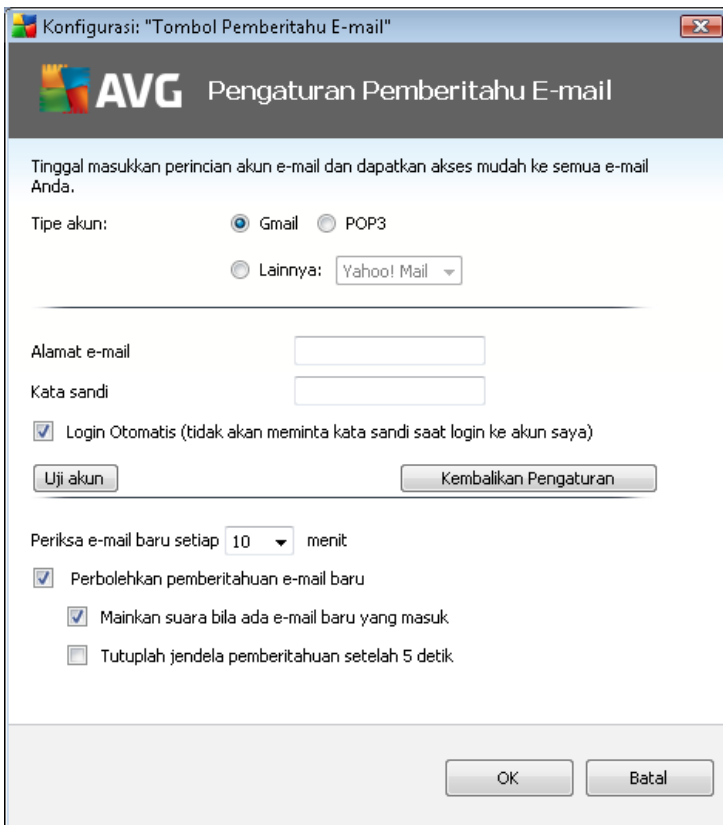
- o **Rancangan RSS** - beralih dari opsi Dasar/Lanjutan untuk memilih rancangan gambaran umum berita (*rancangan lanjutan ditentukan secara default, lihat gambar di atas*)
- o **Sembunyikan pesan yang sudah dibaca** - tandai pilihan ini untuk mengonfirmasi bahwa pesan yang sudah dibaca tidak perlu ditampilkan pada gambaran umum berita lagi dan harus diganti dengan judul berita baru
- o **Tombol yang ditampilkan** - pada bidang ini Anda dapat menentukan berita apa saja yang akan ditampilkan pada gambaran umum berita **AVG Security Toolbar**
 -  - klik tombol ini untuk menutup gambaran umum berita yang sedang terbuka.

8.1.6. Hapus Riwayat

Tombol ini dapat Anda gunakan untuk menghapus riwayat peramban sama seperti melalui opsi **logo AVG -> Hapus riwayat**.

8.1.7. Pemberitahu E-mail

Tombol **Pemberi Tahu Email** memungkinkan Anda mengaktifkan opsi untuk diberi tahu tentang masuknya pesan email baru langsung di antarmuka [AVG Security Toolbar](#). Tombol ini membuka dialog pengeditan berikut tempat Anda dapat menentukan parameter akun email dan aturan tampilan email Anda. Harap ikuti instruksi dalam dialog:



- **Jenis akun** - Menentukan jenis protokol yang digunakan akun email Anda. Anda dapat memilih dari alternatif berikut: *Gmail*, *POP3*, atau pilih nama server dari menu buka bawah dalam pilihan *Lainnya* (*saat ini, Anda dapat menggunakan opsi ini jika akun Anda adalah akun Yahoo! JP Mail atau Hotmail*). Jika Anda tidak yakin jenis server email yang



digunakan akun Anda, coba temukan informasi tersebut dari penyedia layanan email Anda atau penyedia layanan Internet Anda.

- **Login** - Di bagian login, berikan bentuk persis dari *alamat e-mail* Anda dan *kata sandinya*. Biarkan opsi *Login Otomatis* ditandai sehingga Anda tidak perlu memasukkan data berulang-ulang.
- **Uji akun** - Gunakan tombol ini untuk menguji perincian yang dimasukkan.
- **Kembalikan Pengaturan** - Dengan cepat menghapus perincian alamat e-mail yang dimasukkan di atas.
- **Periksa email baru setiap ... menit** - Tentukan interval waktu yang digunakan untuk memeriksa pesan e-mail baru (*dalam kisaran 5-120 menit*), dan tentukan apakah Anda ingin untuk diberi tahu tentang adanya pesan baru dan cara memberitahukannya.
- **Perbolehkan pemberitahuan e-mail baru** - Jangan tandai ini untuk menonaktifkan pemberitahuan visual mengenai pesan e-mail yang baru masuk.
 - o **Mainkan suara bila ada e-mail baru yang masuk** - Jangan tandai ini untuk menonaktifkan pemberitahuan suara mengenai pesan e-mail yang baru masuk.
 - o **Tutup jendela pemberitahuan setelah 5 detik** - Tandai ini untuk menutup jendela pemberitahuan visual atas pesan e-mail yang baru masuk setelah 5 detik secara otomatis.

8.1.8. Info Cuaca

Tombol **Cuaca** menampilkan informasi suhu saat ini (*diperbarui setiap 3-6 jam*) di tujuan yang Anda pilih langsung melalui antarmuka **AVG Security Toolbar**. Klik tombol tersebut untuk membuka panel info baru dengan gambaran cuaca terperinci:

Brno, CZ
[[ubah lokasi](#)]

25° C

Kecepatan angin: 14,48 km/j
Matahari Terbit: 05:04
Matahari Terbenam: 20:34

JUM	SAB
Tinggi: 24 °C Rendah: 14 °C	Tinggi: 25 °C Rendah: 14 °C

Diperbarui 05/20/2011 14:03:57 **YAHOO! NEWS** [Prakiraan Lengkap >](#)

Berikut temukan opsi pengeditan:



- **Ubah lokasi** - klik teks **Ubah lokasi** untuk menampilkan dialog baru yang disebut **Cari lokasi Anda**. Masukkan nama lokasi yang Anda inginkan ke bidang teks, dan konfirmasi dengan mengklik tombol **Cari**. Berikutnya, dalam daftar semua lokasi dengan nama yang sama, pilih tujuan yang Anda cari. Terakhir, panel info akan ditampilkan kembali dengan menyajikan informasi cuaca untuk lokasi yang dipilih.
- **Konversi Fahrenheit / Celsius** - pada pojok kanan atas panel info, Anda dapat memilih antara skala Fahrenheit dan Celsius. Berdasarkan pilihan Anda, informasi temperatur selanjutnya akan disediakan dalam skala yang dipilih.
- **Prakiraan Lengkap** - jika tertarik pada prakiraan lengkap dan terperinci, gunakan tautan **Prakiraan Lengkap** untuk membuka situs Web khusus cuaca.

8.1.9. Facebook

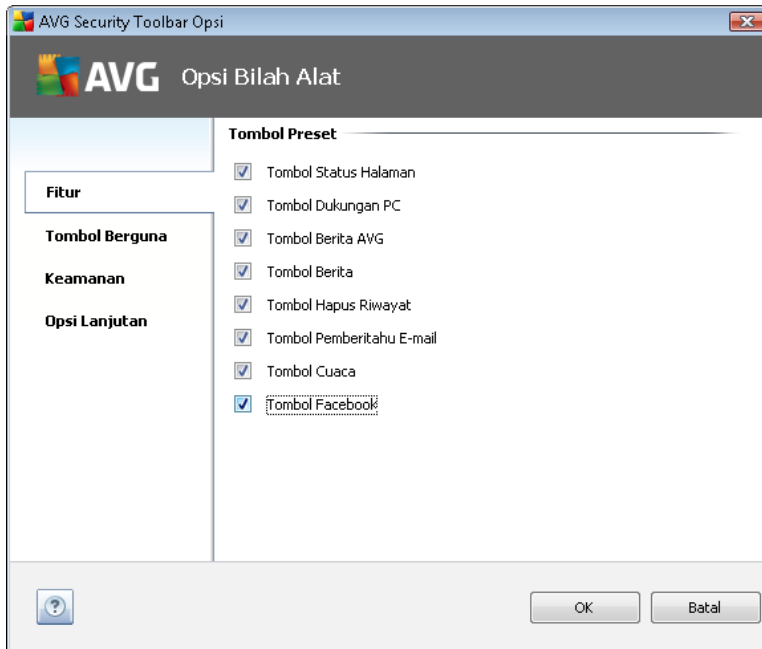
Tombol **Facebook** memungkinkan Anda terhubung ke jejaring sosial [Facebook](#) dari **AVG Security Toolbar** secara langsung. Klik tombol dan akan muncul undangan untuk login; klik lagi untuk membuka dialog **login Facebook**. Berikan data akses Anda, dan tekan tombol **Hubungkan**. Jika Anda belum memiliki akun [Facebook](#), Anda dapat langsung membuatnya menggunakan tautan **Daftar Facebook**.

Setelah Anda melakukan proses pendaftaran [Facebook](#), Anda akan diundang untuk memperbolehkan aplikasi **Ekstensi Sosial AVG**. Fungsionalitas aplikasi ini penting untuk bilah alat - koneksi [Facebook](#), oleh karena itu direkomendasikan untuk mengizinkan aplikasi ini berfungsi, dengan demikian pastikan Anda membolehkannya. Kemudian koneksi [Facebook](#) akan diaktifkan dan tombol **Facebook** dalam **AVG Security Toolbar** sekarang menawarkan opsi menu [Facebook](#) standar.

8.2. Opsi AVG Security Toolbar

Semua konfigurasi parameter **AVG Security Toolbar** dapat diakses langsung dalam panel **AVG Security Toolbar**. Antarmuka pengeditan terbuka melalui item menu bilah alat AVG / **Opsi** dalam dialog baru bernama **Opsi Bilah Alat** yang terbagi ke dalam empat bagian:

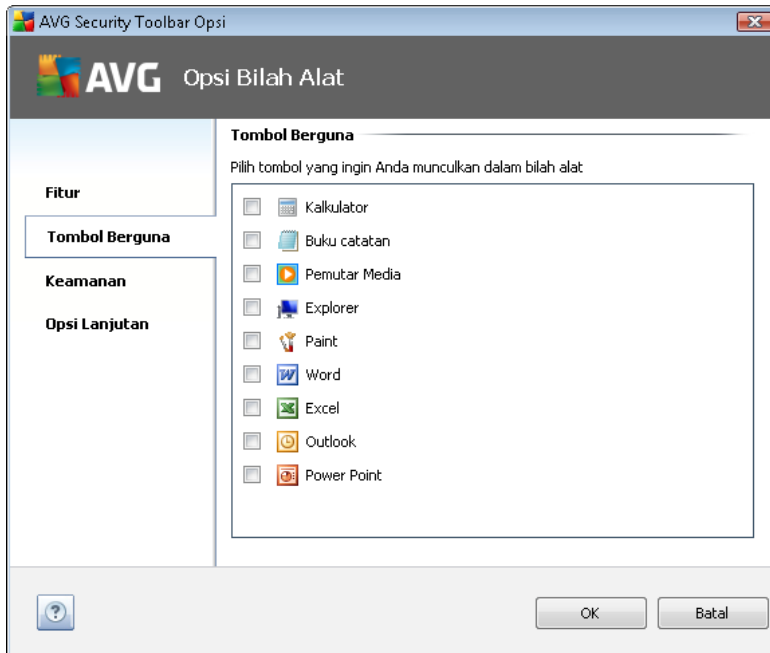
8.2.1. Tab Umum



Pada tab ini Anda dapat menentukan tombol kontrol bilah alat yang harus ditampilkan atau disembunyikan dalam panel **AVG Security Toolbar**. Tandai opsi untuk tombol yang ingin Anda tampilkan. Selanjutnya temukan keterangan tentang fungsionalitas tiap tombol bilah alat:

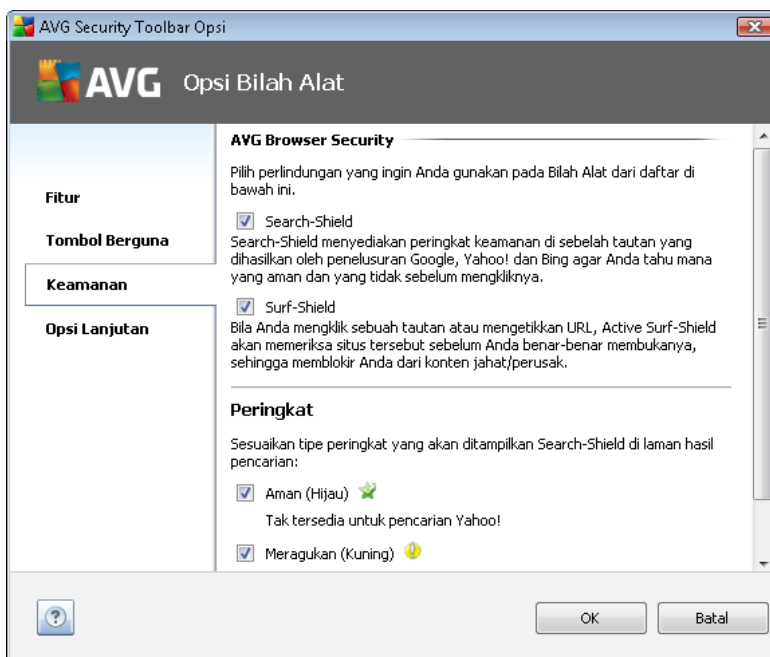
- **Tombol Status Halaman** - tombol ini menawarkan kemungkinan untuk menampilkan informasi tentang status keamanan halaman yang baru dibuka dalam **AVG Security Toolbar**
- **Tombol Berita AVG** - tombol ini membuka halaman web yang menyediakan pernyataan pers terbaru yang berkaitan dengan AVG
- **Tombol Berita** - tombol ini menyediakan gambaran umum terstruktur mengenai berita terbaru dari berita harian
- **Tombol Hapus Riwayat** - tombol ini memungkinkan Anda memilih opsi Hapus riwayat lengkap, atau Hapus riwayat penelusuran, Hapus riwayat peramban, Hapus riwayat unduhan, atau Hapus cookie langsung dari panel AVG Security Toolbar
- **Tombol Pemberitahu Email** - tombol ini memungkinkan Anda menampilkan pesan email yang baru diterima dalam antarmuka **AVG Security Toolbar**
- **Tombol Cuaca** - tombol ini memberikan informasi langsung tentang kondisi cuaca di lokasi terpilih.
- **Tombol Facebook** - tombol menawarkan hubungan langsung ke jejaring sosial [Facebook](https://www.facebook.com/AVG)

8.2.2. Tab Tombol yang Berguna



Tab ***Tombol yang Berguna*** memungkinkan Anda memilih aplikasi dari daftar dan menampilkan ikonnya dalam antarmuka bilah alat. Ikon tersebut kemudian berfungsi sebagai tautan cepat yang memungkinkan peluncuran aplikasi terkait dengan segera.

8.2.3. Tab Keamanan



Tab ***Keamanan*** terbagi ke dalam dua bagian, ***AVG Browser Security*** dan ***Peringkat***, di mana Anda

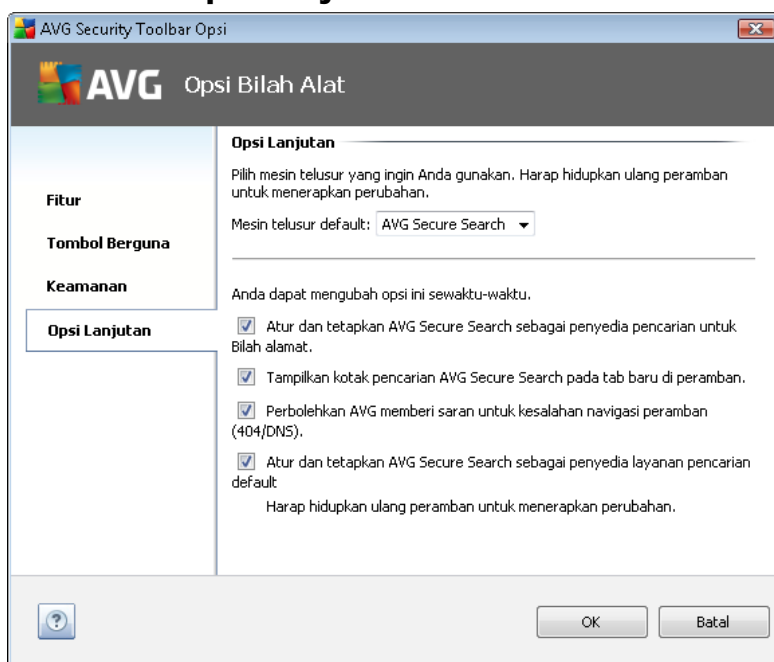


dapat mencentang kotak tertentu untuk menetapkan fungsionalitas **AVG Security Toolbar** yang ingin Anda pakai:

- **Browser Security** - centang item ini untuk mengaktifkan atau menonaktifkan [AVG Search-Shield](#) dan/atau layanan [Surf-Shield](#)
- **Peringkat** - pilih simbol grafis yang digunakan untuk peringkat hasil telusur oleh komponen [Search-Shield](#) yang ingin Anda gunakan:
 - o  halaman aman
 - o  halaman agak mencurigakan
 - o  halaman berisi tautan ke halaman yang dipastikan berbahaya
 - o  halaman berisi ancaman aktif
 - o  halaman tidak dapat diakses, sehingga tidak dapat dipindai

Centang opsi terkait untuk mengonfirmasikan bahwa Anda ingin diberi tahu tentang tingkat ancaman spesifik ini. Namun, tampilan tanda merah yang ditetapkan untuk halaman yang berisi ancaman aktif dan berbahaya tidak dapat dinonaktifkan. ***Sekali lagi, disarankan untuk membiarkan konfigurasi default yang diatur oleh vendor program kecuali Anda memiliki alasan kuat untuk mengubahnya.***

8.2.4. Tab Opsi Lanjutan





Pada tab **Opsi Lanjutan** pilih terlebih dahulu mesin telusur yang ingin Anda gunakan secara default. Anda punya pilihan **AVG Secure Search (powered by Google)**, **Baidu**, **WebHledani**, **Yandex** dan **Yahoo! JP**. Setelah mengubah mesin telusur default, jalankan ulang peramban Internet Anda agar perubahan tersebut diterapkan.

Lebih jauh, Anda dapat mengaktifkan atau menonaktifkan pengaturan lebih spesifik pada **AVG Security Toolbar** (keterangan yang tercantum di bawah merujuk pada pengaturan default **AVG Secure Search (powered by Google)**):

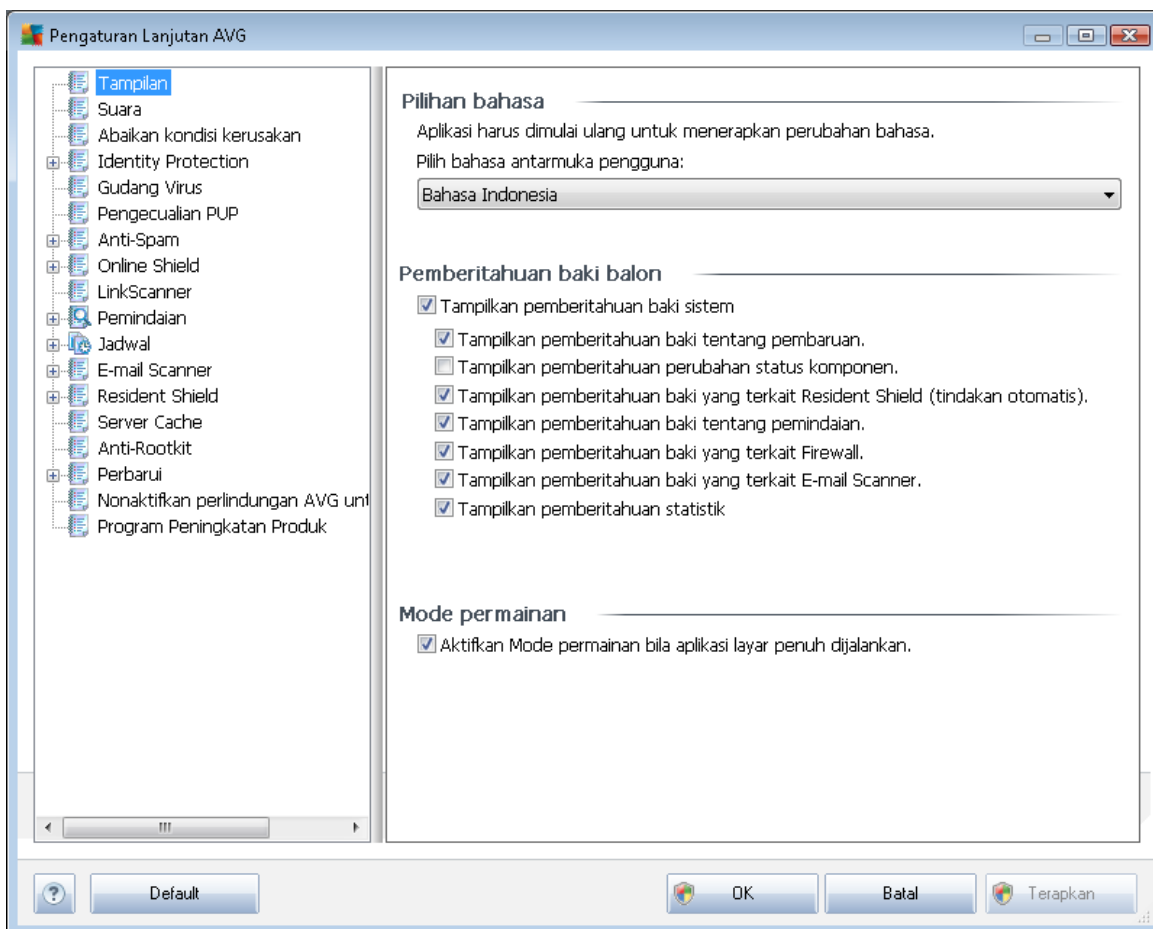
- **Atur dan pertahankan AVG Secure Search (powered by Google) sebagai penyedia penelusuran untuk bilah Alamat** - jika ditandai, opsi ini akan memungkinkan Anda mengetikkan langsung kata kunci penelusuran ke dalam bilah alamat di peramban Internet Anda dan layanan Google akan digunakan untuk menelusuri secara otomatis situs Web terkait.
- **Biarkan AVG memberi saran mengenai kesalahan navigasi peramban (404/DNS)** - jika saat melakukan penelusuran Anda menemukan halaman yang tidak ada, atau halaman yang tidak dapat ditampilkan (kesalahan 404), maka secara otomatis Anda akan diarahkan kembali ke halaman Web yang memungkinkan Anda memilih dari gambaran umum halaman alternatif yang berhubungan dengan topik.
- **Atur dan pertahankan AVG Secure Search (powered by Google) sebagai penyedia penelusuran default** - Google adalah mesin telusur default untuk penelusuran Web dalam **AVG Security Toolbar**, dan mengaktifkan opsi ini juga akan menjadikannya mesin telusur default untuk peramban Web Anda.

9. Pengaturan Lanjutan AVG

Dialog konfigurasi lanjutan **Keamanan Internet AVG 2011** 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.

9.1. Tampilan

Item pertama pada struktur navigasi, **Tampilan**, mengacu pada pengaturan umum [antarmuka pengguna AVG](#) dan beberapa opsi dasar pada cara kerja aplikasi:

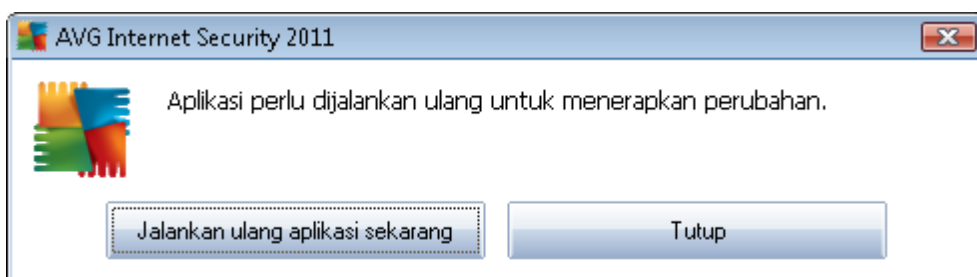


Pemilihan bahasa

Di bagian **Pemilihan bahasa** Anda dapat memilih bahasa yang diinginkan dari menu buka-bawah; bahasa tersebut kemudian akan digunakan untuk seluruh [antarmuka pengguna AVG](#). Menu buka-bawah hanya menawarkan bahasa yang sebelumnya telah Anda pilih untuk diinstal pada [proses instalasi](#) (*lihat bab [Opsi Khusus](#)*) ditambah bahasa Inggris (*yang diinstal secara default*). Walau demikian, untuk menyelesaikan peralihan aplikasi ke bahasa lain, Anda harus menjalankan ulang

antarmuka pengguna; ikuti langkah-langkah ini:

- Pilih bahasa yang diinginkan untuk aplikasi dan konfirmasi pilihan Anda dengan menekan tombol **Terapkan** (sudut kanan bawah)
- Tekan tombol **OK** untuk mengkonfirmasi
- Jendela dialog baru muncul memberi tahu Anda bahwa perubahan bahasa pada antarmuka pengguna AVG mengharuskan aplikasi dijalankan ulang:



Pemberitahuan baki balon

Dalam bagian ini, Anda dapat menyembunyikan tampilan balon pemberitahuan baki sistem mengenai status aplikasi. Secara default, balon pemberitahuan diperbolehkan untuk ditampilkan dan disarankan untuk mempertahankan konfigurasi ini! Biasanya balon pemberitahuan memberitahukan perubahan status beberapa komponen AVG dan Anda harus memerhatikannya!

Walau demikian, jika karena beberapa alasan Anda tidak menginginkan pemberitahuan ini ditampilkan, atau Anda hanya ingin menampilkan pemberitahuan tertentu (berhubungan dengan komponen AVG tertentu), Anda dapat menetapkan dan menentukan preferensi Anda dengan menandai/tidak menandai opsi berikut:

- **Tampilkan pemberitahuan baki sistem** - secara default, item ini ditandai (*diaktifkan*), dan pemberitahuan ditampilkan. Jangan tandai item ini untuk menonaktifkan sama sekali tampilan semua balon pemberitahuan. Bila diaktifkan, Anda dapat memilih lebih lanjut pemberitahuan spesifik yang akan ditampilkan:
 - o **Tampilkan pemberitahuan baki tentang pembaruan** - memutuskan apakah informasi mengenai peluncuran proses pembaruan AVG, kemajuannya, dan finalisasinya harus ditampilkan;
 - o **Tampilkan pemberitahuan perubahan status komponen** - 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 (perubahan warna) yang melaporkan masalah dalam komponen AVG;
 - o **Tampilkan pemberitahuan baki menyangkut Perisai Tetap** (tindakan otomatis) - memutuskan apakah informasi mengenai penyimpanan, penyalinan, dan proses pembukaannya harus ditampilkan atau disembunyikan (*konfigurasi ini hanya*



menunjukkan apakah opsi [Pulih otomatis](#) pada Perisai Tetap telah diaktifkan);

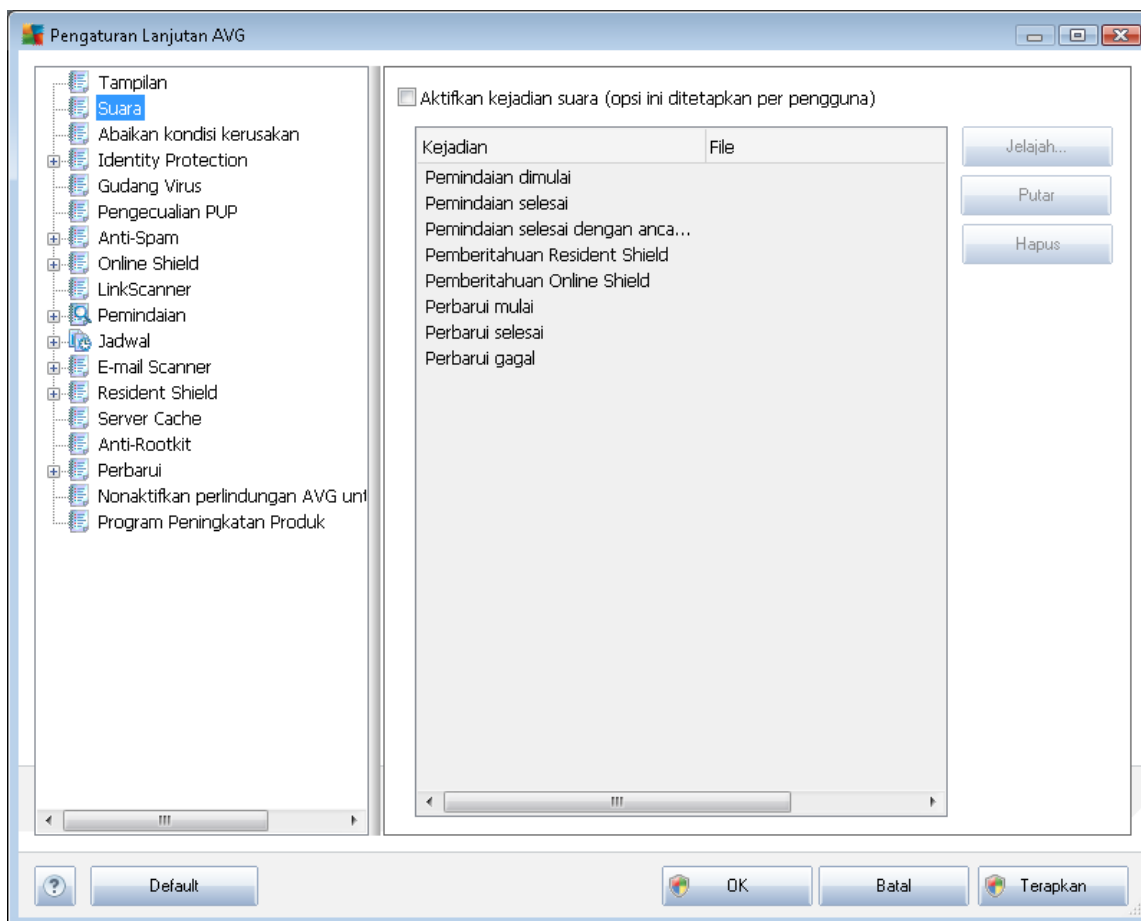
- o **Tampilkan pemberitahuan baki tentang [pemindaian](#)** - memutuskan apakah informasi mengenai peluncuran otomatis dari pemindaian terjadwal, kemajuannya, dan hasilnya harus ditampilkan;
- o **Tampilkan pemberitahuan baki menyangkut [Firewall](#)** - memutuskan apakah informasi mengenai status dan proses Firewall, misalnya peringatan aktivasi/deaktivasi komponen, kemungkinan pemblokiran lalu lintas, dsb. harus ditampilkan;
- o **Tampilkan pemberitahuan baki menyangkut [Pemindai E-mail](#)** - memutuskan apakah informasi mengenai pemindaian semua pesan e-mail yang masuk dan keluar akan ditampilkan.
- o **Tampilkan pemberitahuan statistik** - biarkan opsi ini ditandai untuk memungkinkan pemberitahuan peninjauan statistik secara rutin ditampilkan di baki sistem.

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).

9.2. Suara

Dalam dialog **Suara** Anda dapat menetapkan apakah Anda ingin diberi tahu tentang tindakan AVG tertentu dengan pemberitahuan suara. Jika ya, centang opsi **Aktifkan kejadian suara** (dinonaktifkan secara default) untuk mengaktifkan daftar tindakan AVG:

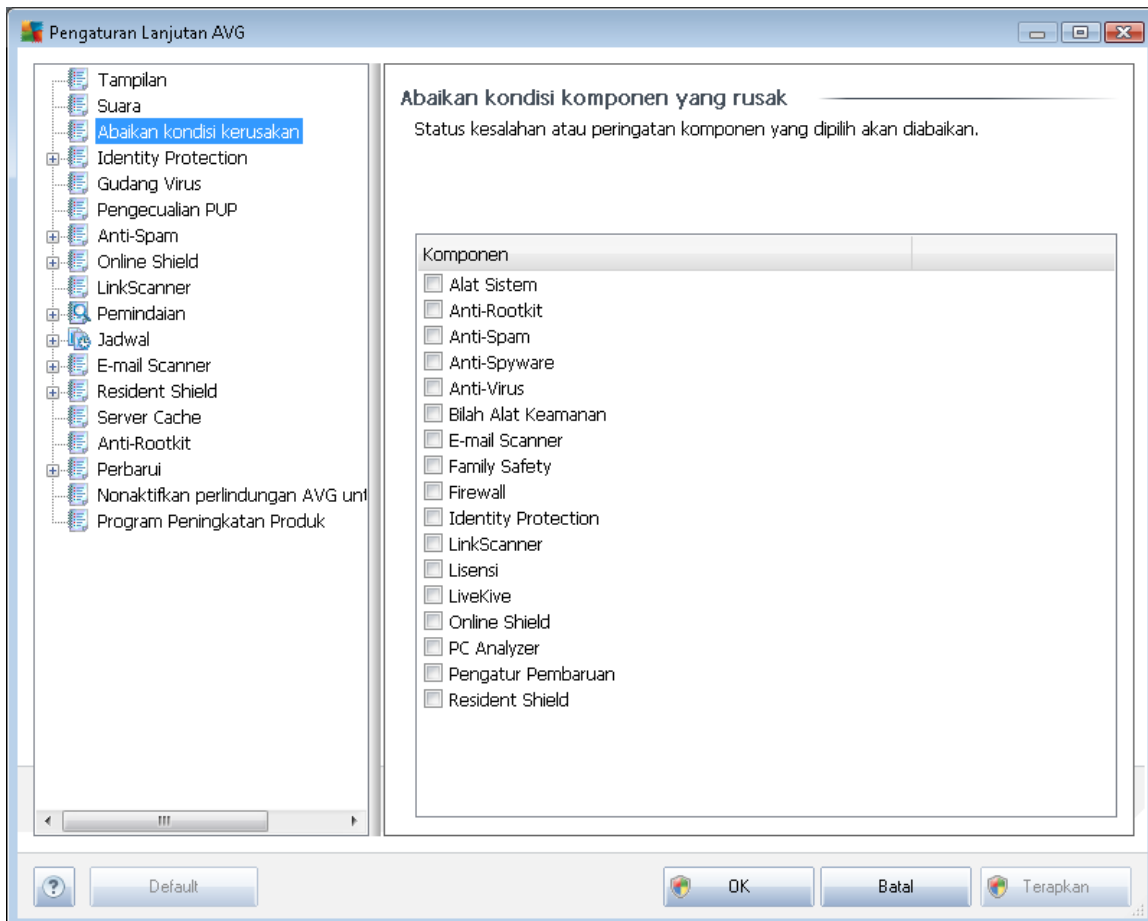


Kemudian, pilih kejadian yang terkait dari daftar dan jelajahi (**Jelajahi**) disk Anda untuk menemukan suara yang ingin Anda tetapkan untuk kejadian ini. Untuk mendengarkan suara yang dipilih, sorot kejadian dalam daftar dan tekan tombol **Putar** . Gunakan tombol **Hapus** untuk menghapus suara yang ditetapkan untuk kejadian tertentu.

Catatan: Hanya suara *.wav yang didukung!

9.3. Abaikan Kondisi Kerusakan

Dalam dialog **Abaikan kondisi kerusakan komponen**, 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



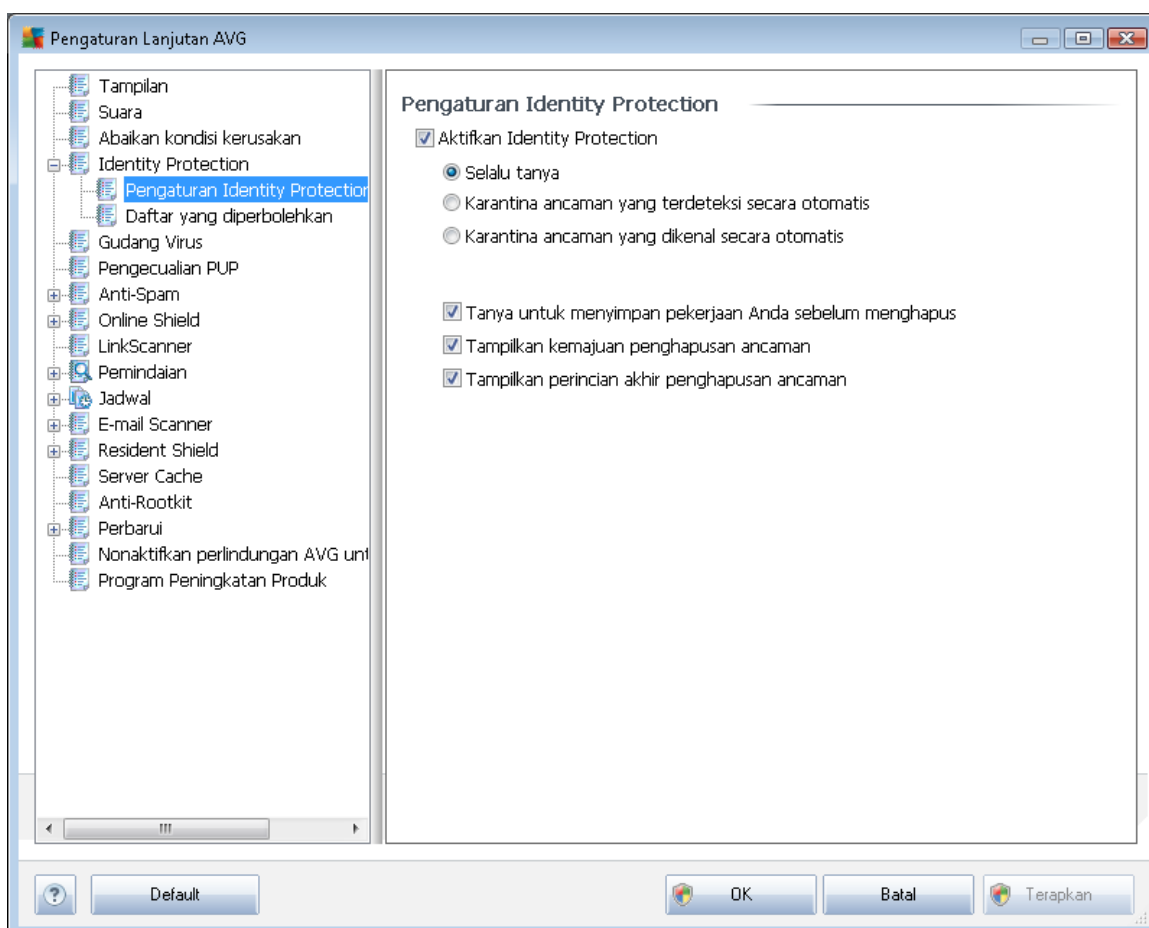
abu-abu, ikon tersebut tidak dapat melaporkan dengan sebenarnya segala kemungkinan kesalahan lebih lanjut yang mungkin muncul.

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 untuk **Mengabaikan status komponen** juga tersedia secara langsung untuk beberapa komponen tertentu dari [gambaran umum komponen dalam jendela utama AVG](#).

9.4. Perlindungan Identitas

9.4.1. Pengaturan Perlindungan Identitas

Dialog [Pengaturan Perlindungan Identitas](#) memungkinkan Anda mengaktifkan atau menonaktifkan fitur dasar komponen [Perlindungan Identitas](#):



Aktifkan Perlindungan Identitas (*diaktifkan secara default*) – jangan centang untuk menonaktifkan komponen [Perlindungan Identitas](#).

Kami sangat menyarankan agar Anda tidak melakukannya jika tidak perlu!



Bila [Perlindungan Identitas](#) diaktifkan, Anda dapat menetapkan apa yang dilakukan bila ancaman terdeteksi:

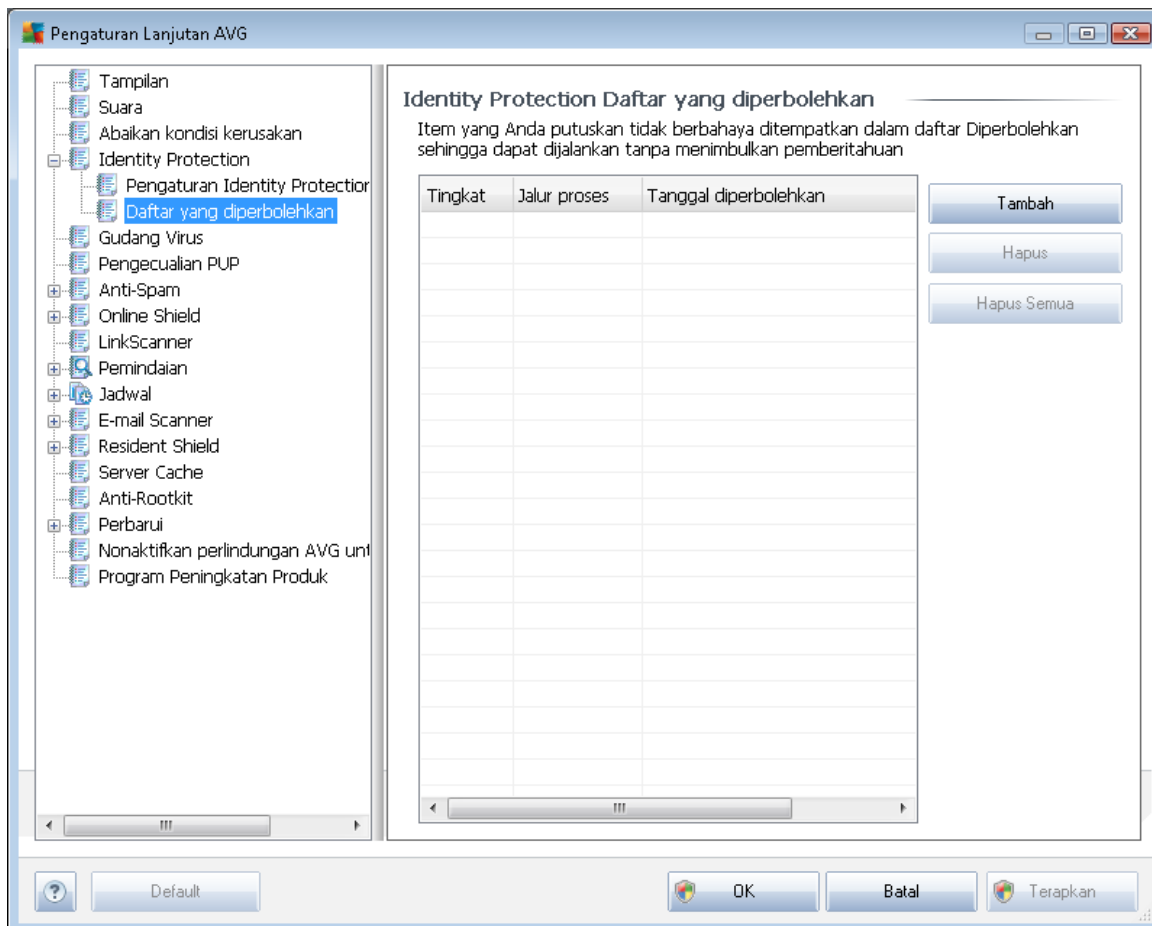
- **Selalu tanya** (*diaktifkan secara default*) - saat ancaman terdeteksi, Anda akan ditanyai apakah ia harus dipindahkan ke karantina untuk memastikan tidak terhapusnya aplikasi yang ingin Anda jalankan.
- **Karantina ancaman yang terdeteksi secara otomatis** - centang kotak ini untuk menentukan bahwa Anda ingin semua ancaman yang mungkin terdeteksi segera dipindahkan ke ruang aman di [Gudang Virus AVG](#). 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 AVG](#).

Lebih lanjut Anda dapat menetapkan item tertentu untuk mengaktifkan fungsionalitas [Perlindungan Identitas](#) 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 malware** - (*diaktifkan secara default*) - dengan aktifnya item ini, **Perlindungan Identitas** menampilkan informasi terperinci mengenai setiap objek yang dipindahkan ke karantina (*tingkat keseriusan, lokasi, dll.*).

9.4.2. Daftar yang Diperbolehkan

Jika dalam dialog **Pengaturan Perlindungan Identitas** 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 mengonfirmasinya agar tetap disimpan di komputer Anda, aplikasi ini akan ditambahkan ke **Daftar yang Diperbolehkan Perlindungan Identitas**, dan tidak akan dilaporkan lagi sebagai item yang mungkin berbahaya:



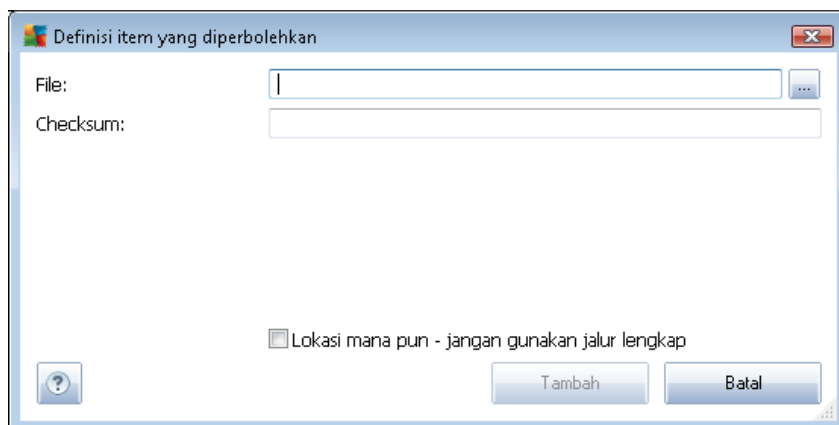
Daftar yang Diperbolehkan Perlindungan Identitas menyediakan informasi berikut mengenai setiap aplikasi:

- **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

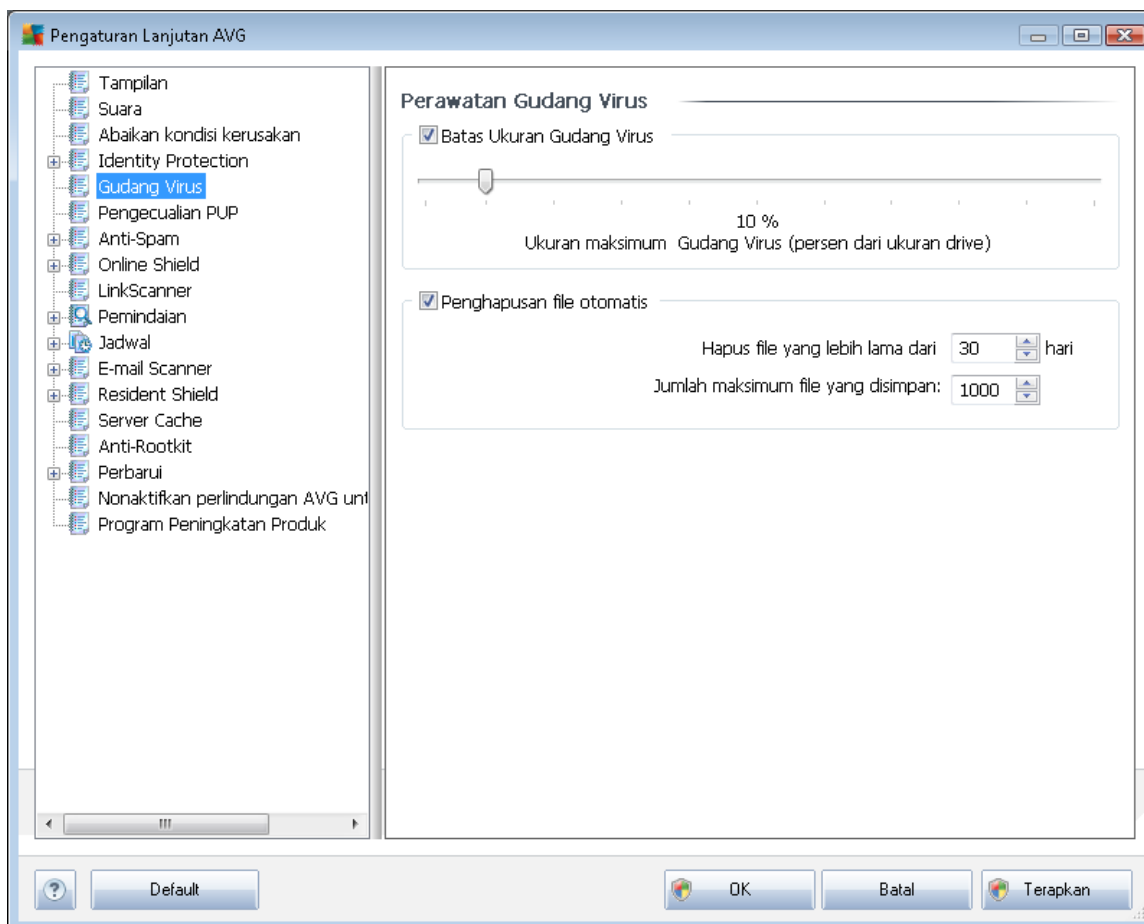
Tombol kontrol yang tersedia dalam dialog **Daftar yang diperbolehkan Perlindungan Identitas** adalah sebagai berikut:

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



- o **File** - ketikkan jalur lengkap ke file (*aplikasi*) yang ingin Anda tandai sebagai pengecualian
- o **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.
- o **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

9.5. Gudang Virus



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

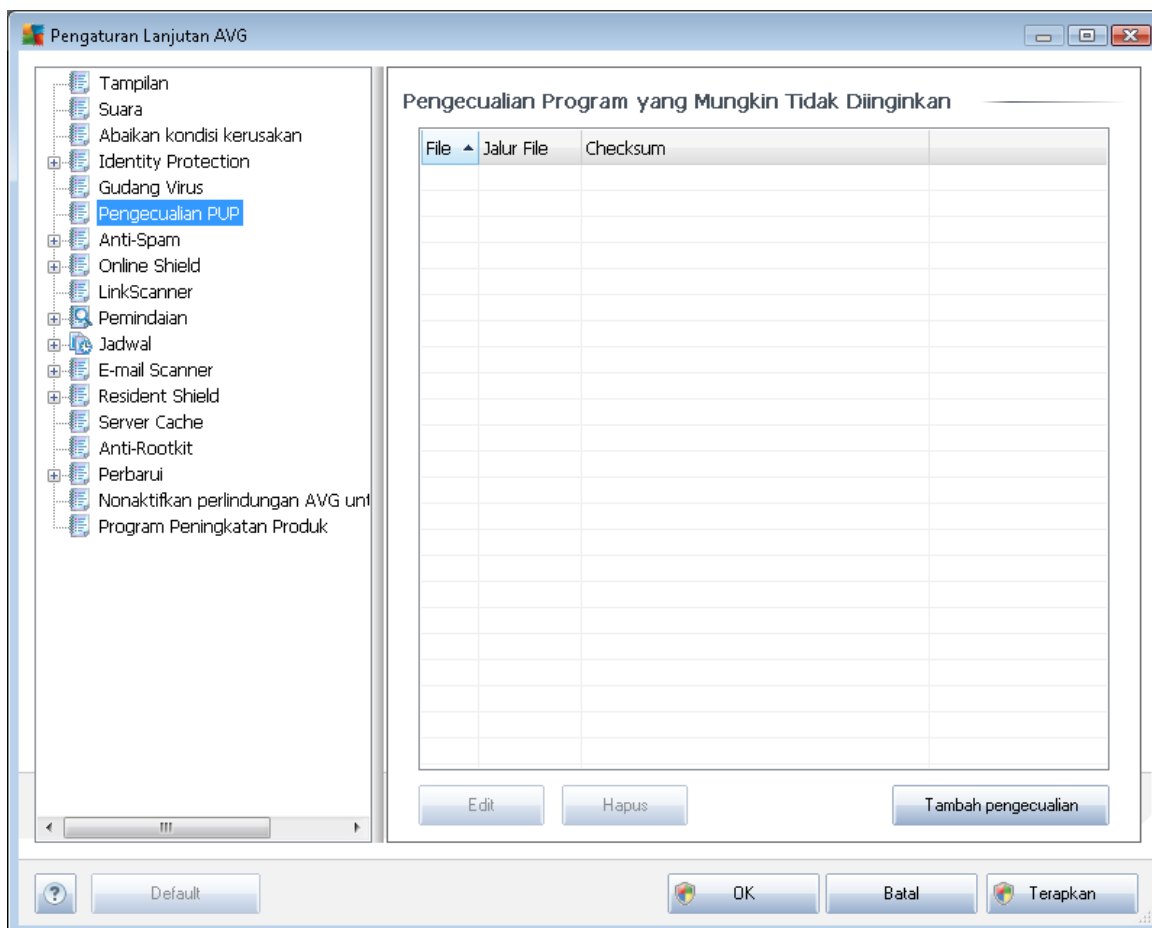
- **Batasi ukuran Gudang Virus** - gunakan penggeser untuk mengatur ukuran maksimum **Gudang Virus**. Ukuran ditetapkan secara proporsional, dibandingkan dengan ukuran disk lokal Anda.
- **Penghapusan file otomatis** - di bagian ini, tentukan lama maksimum untuk menyimpan objek dalam **Gudang Virus** (**Hapus file yang lebih lama dari ... hari**), dan jumlah maksimum file yang disimpan dalam **Gudang Virus** (**Jumlah maksimum file yang disimpan**)

9.6. Pengecualian PUP

Keamanan Internet AVG 2011 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 gratis, termasuk adware. Adware tersebut mungkin terdeteksi dan dilaporkan oleh AVG sebagai **program yang mungkin tidak diinginkan**.



Jika Anda ingin membiarkan program tersebut pada komputer Anda, Anda dapat menetakannya 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:

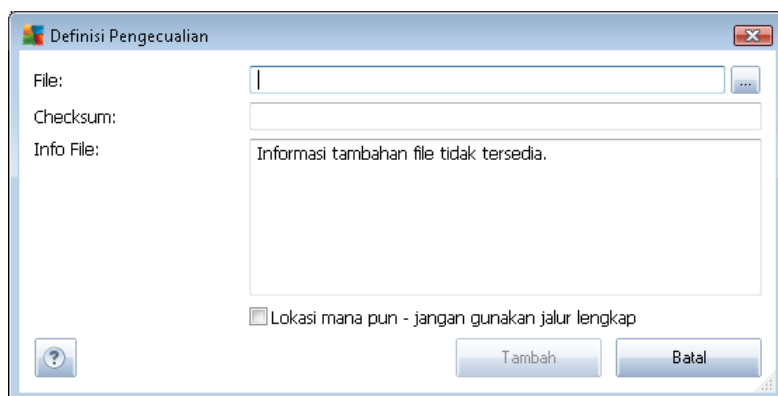
- **File** - memberikan nama aplikasi yang bersangkutan
- **Jalur File** - menunjukkan jalur menuju lokasi aplikasi.
- **Checksum** - menampilkan 'tanda tangan' unik atas file yang dipilih. Checksum ini adalah string karakter yang dibuat secara otomatis, yang memungkinkan AVG dengan jelas membedakan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

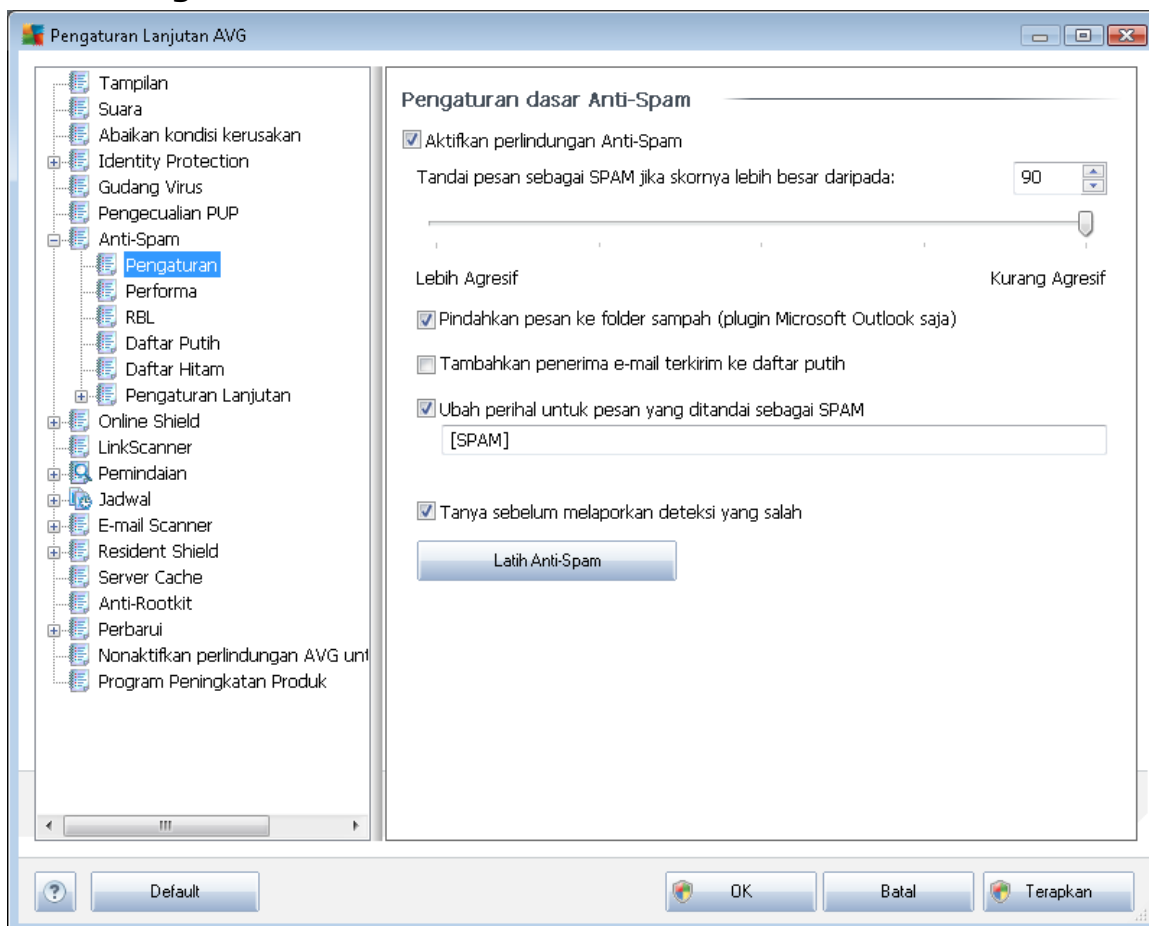
- **Hapus** - menghapus item yang dipilih dari daftar pengecualian
- **Tambah pengecualian** - membuka dialog pengeditan di mana Anda dapat menetapkan parameter pengecualian baru yang akan dibuat:



- o **File** - ketikkan jalur lengkap ke file yang ingin Anda tandai sebagai pengecualian
- o **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.
- o **Info File** - menampilkan informasi tambahan tentang file (*lisensi/informasi versi, dll.*)
- o **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 (*akan tetapi, bagaimana pun juga Anda harus mengisi jalur lengkap file tersebut, file kemudian akan digunakan sebagai contoh unik untuk kemungkinan dua file dengan nama yang sama muncul di sistem Anda*).

9.7. Anti-Spam

9.7.1. Pengaturan



Dalam dialog **Pengaturan dasar Anti-Spam** Anda dapat mencentang/menghapus centang pada 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 gambaran 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 bukan-spam hampir bisa dipastikan akan tertangkap sebagai pesan [spam](#) nyata. Kisaran ambang batas ini tidak disarankan untuk penggunaan biasa.

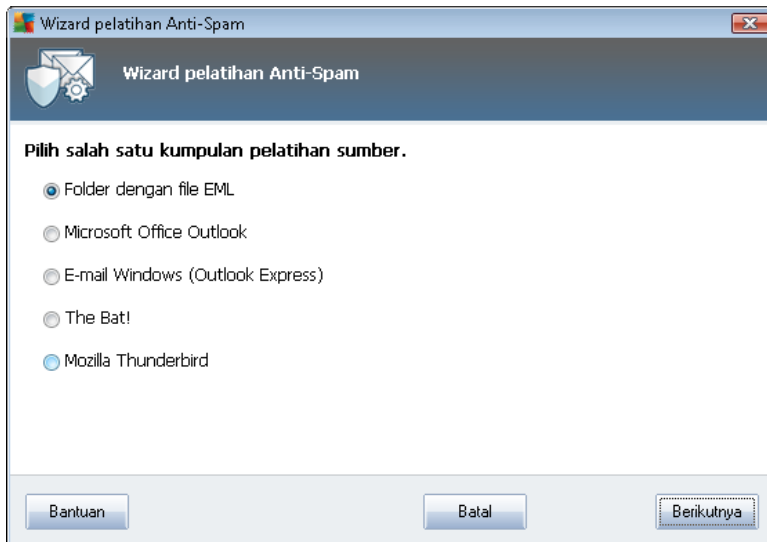
Dalam dialog **Pengaturan dasar Anti-Spam** Anda dapat menentukan lebih jauh bagaimana seharusnya memperlakukan pesan e-mail [spam](#) yang terdeteksi:

- **Pindahkan pesan ke folder sampah** - centang kotak ini untuk menetapkan bahwa setiap pesan spam yang terdeteksi secara otomatis harus dipindahkan ke folder sampah tertentu dalam klien e-mail Anda;
- **Tambahkan penerima e-mail terkirim ke [daftar-putih](#)** - centang kotak ini untuk mengonfirmasi bahwa semua penerima e-mail terkirim dapat dipercaya, dan semua pesan e-mail yang berasal dari akun e-mail 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 e-mail; teks yang diinginkan dapat diketikkan dalam bidang teks yang telah diaktifkan.
- **Tanyakan sebelum melaporkan deteksi kesalahan** - apabila 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 mencentang 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:

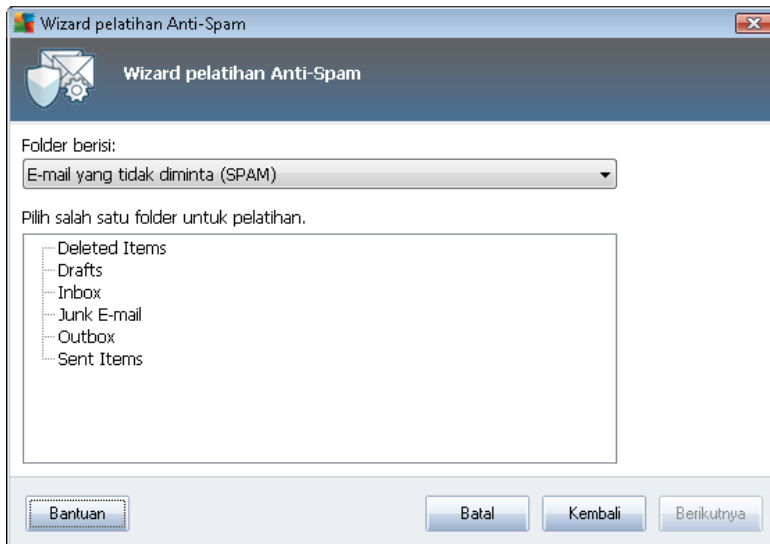
- **Klien e-mail tertentu** - jika Anda menggunakan salah satu klien e-mail yang tercantum (*MS Outlook, Outlook Express, The Bat!*), tinggal pilih opsi yang terkait
- **Folder dengan file EML** - jika Anda menggunakan program e-mail lain, Anda harus menyimpan pesan ke folder tertentu (*dalam format .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



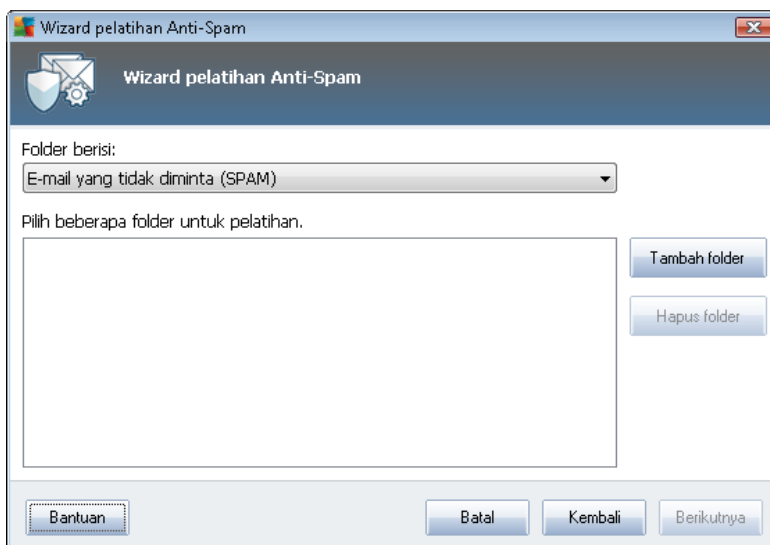
Dalam dialog ini, pilih folder dengan pesan yang ingin Anda gunakan untuk pelatihan. Tekan tombol **Tambah folder** untuk menemukan folder dengan file .eml (*pesan e-mail tersimpan*). Folder yang dipilih akan ditampilkan dalam dialog.

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.

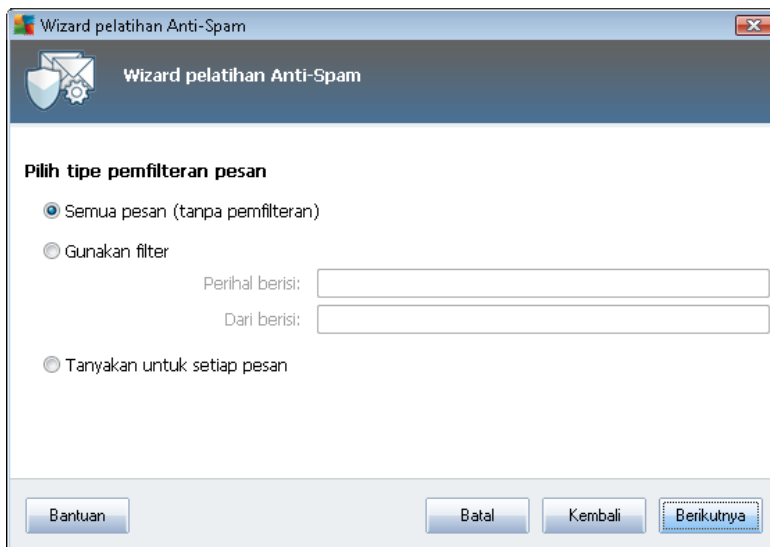




Catatan: Untuk Microsoft Office Outlook, Anda akan dikonfirmasi untuk memilih profil MS Office Outlook terlebih dahulu.

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.

Jika Anda yakin folder yang dipilih hanya berisi pesan yang akan digunakan untuk pelatihan, pilih opsi **Semua pesan (tanpa pemfilteran)**.

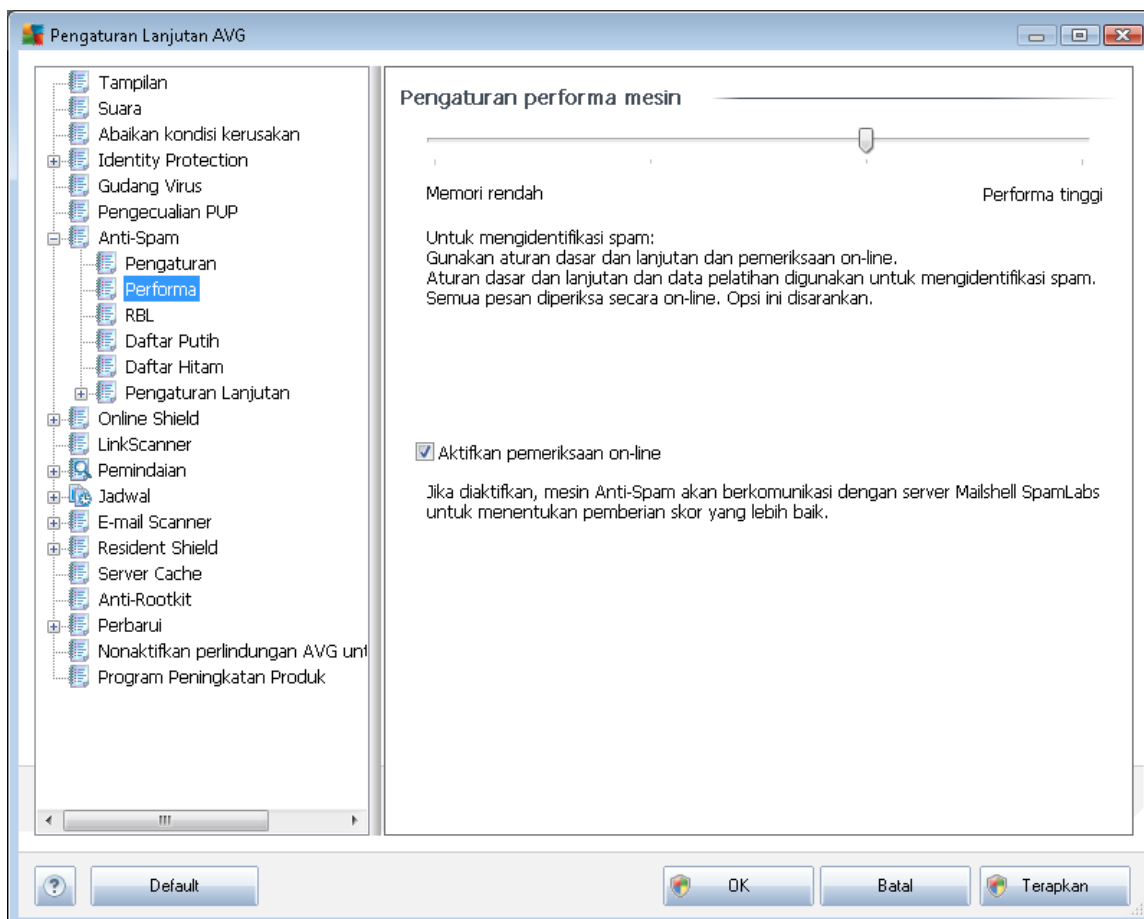
Jika Anda tidak yakin tentang pesan yang terdapat di dalam folder, dan ingin wizard menanyakan setiap pesan (sehingga Anda dapat memutuskan apakah akan digunakan untuk pelatihan atau tidak), pilih opsi **Tanyakan untuk setiap pesan**.

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.

Perhatian! Bila Anda mengisi kedua bidang teks, alamat yang hanya cocok dengan salah satu dari kedua ketentuan tersebut juga akan digunakan!

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.

9.7.2. Performa



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.

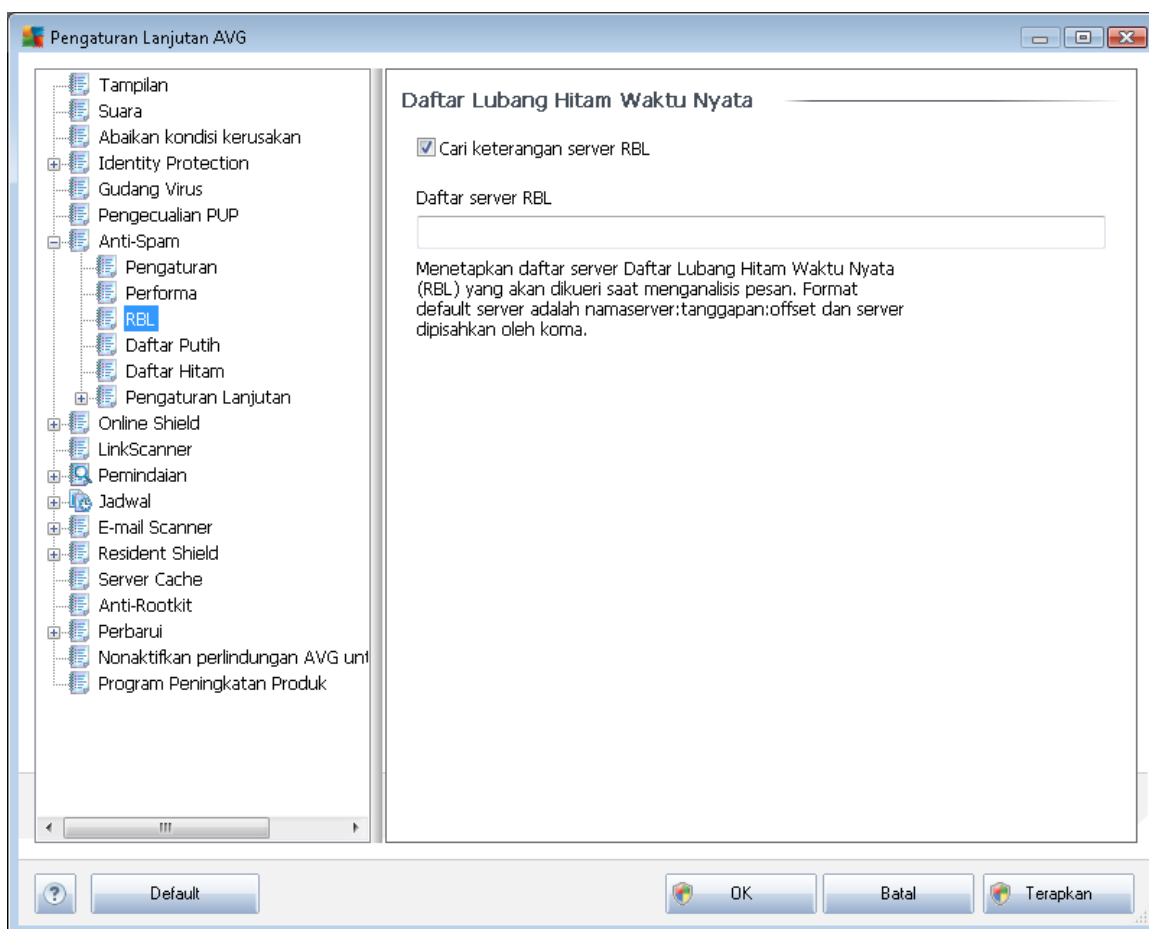
Item **Aktifkan pemeriksaan online** diaktifkan secara default. Ini menghasilkan deteksi [spam](#) yang lebih akurat melalui komunikasi dengan server [Mailshell](#), yakni data yang telah dipindai akan dibandingkan dengan basis data online [Mailshell](#).

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!

9.7.3. RBL

Item **RBL** membuka dialog pengeditan bernama **Daftar Lubang Hitam Waktu Nyata**:



Dalam dialog ini, Anda dapat mengaktifkan/menonaktifkan fungsi **Tanya server RBL**.

RBL (**Daftar Lubang Hitam Waktu Nyata**) 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](#).

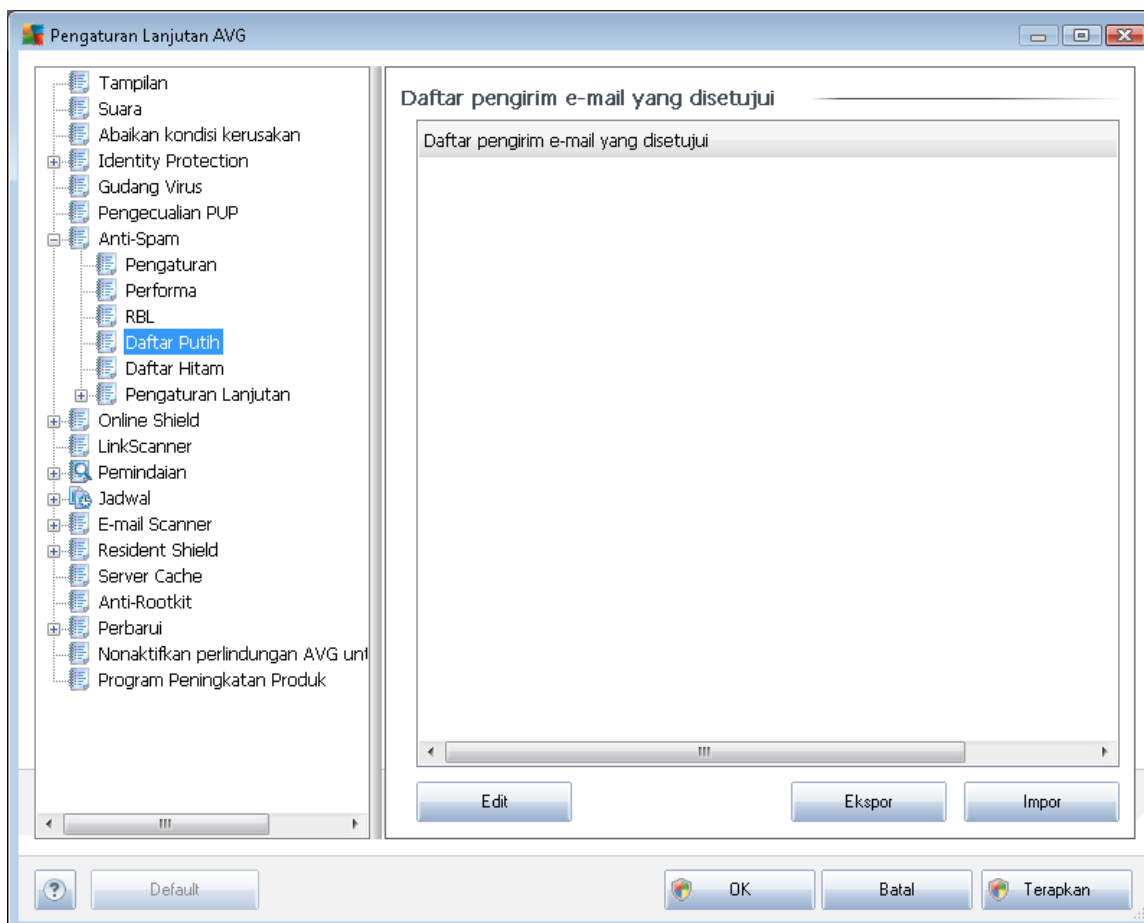
Daftar server RBL memungkinkan Anda menentukan lokasi server RBL tertentu.

Catatan: Mengaktifkan fitur ini mungkin, pada beberapa sistem dan konfigurasi, memperlambat proses penerimaan e-mail, karena setiap pesan harus diverifikasi terhadap basis data server RBL.

Tidak ada data pribadi yang dikirim ke server!

9.7.4. Daftar Putih

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 mengirim 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 berikut ini tersedia:

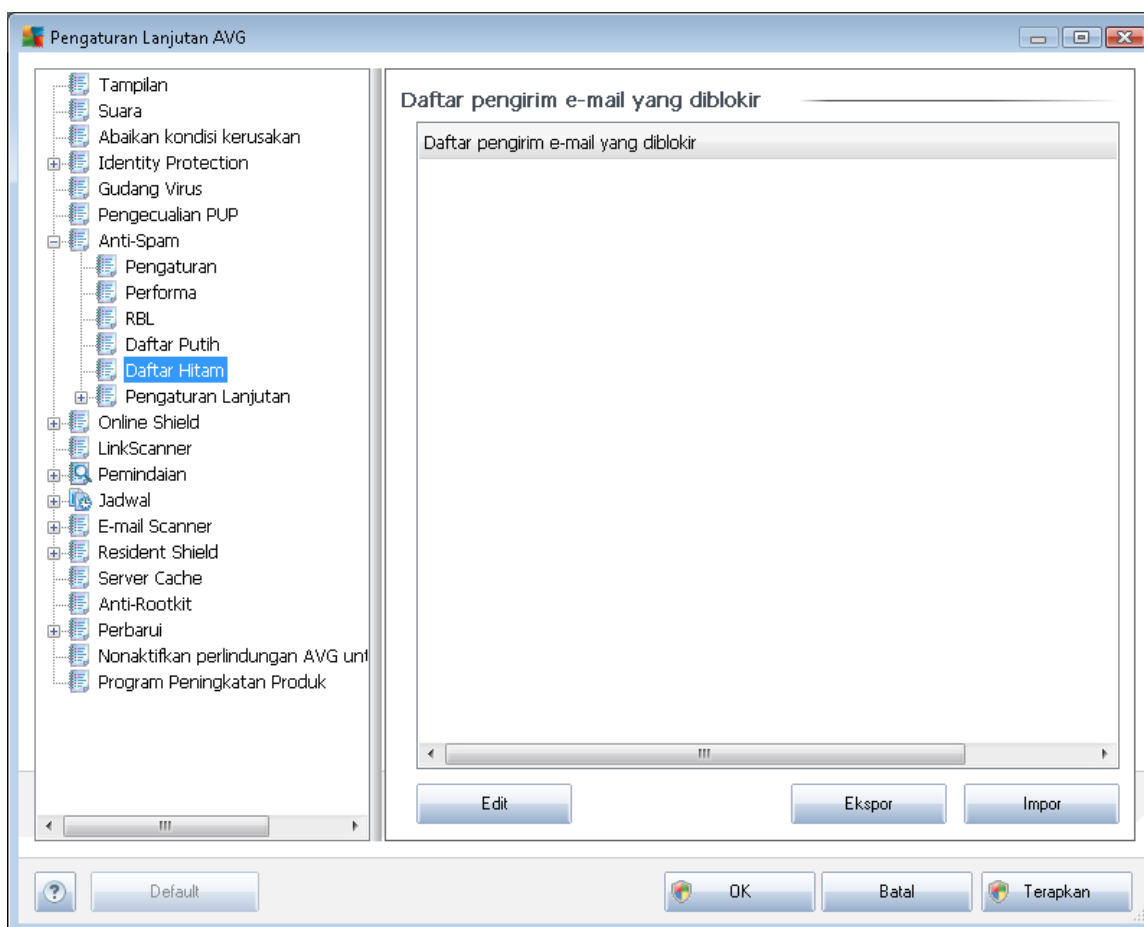
- **Edit** - tekan tombol ini untuk membuka dialog, di mana Anda dapat memasukkan daftar alamat secara manual (*Anda juga dapat menggunakan salin dan tempel*). Masukkan satu item (*pengirim, nama domain*) per baris.
- **Ekspor** - jika Anda memutuskan untuk mengeksport record karena suatu tujuan, Anda 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.

9.7.5. Daftar Hitam

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 mengirimkan 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 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.

9.7.6. Pengaturan Lanjutan

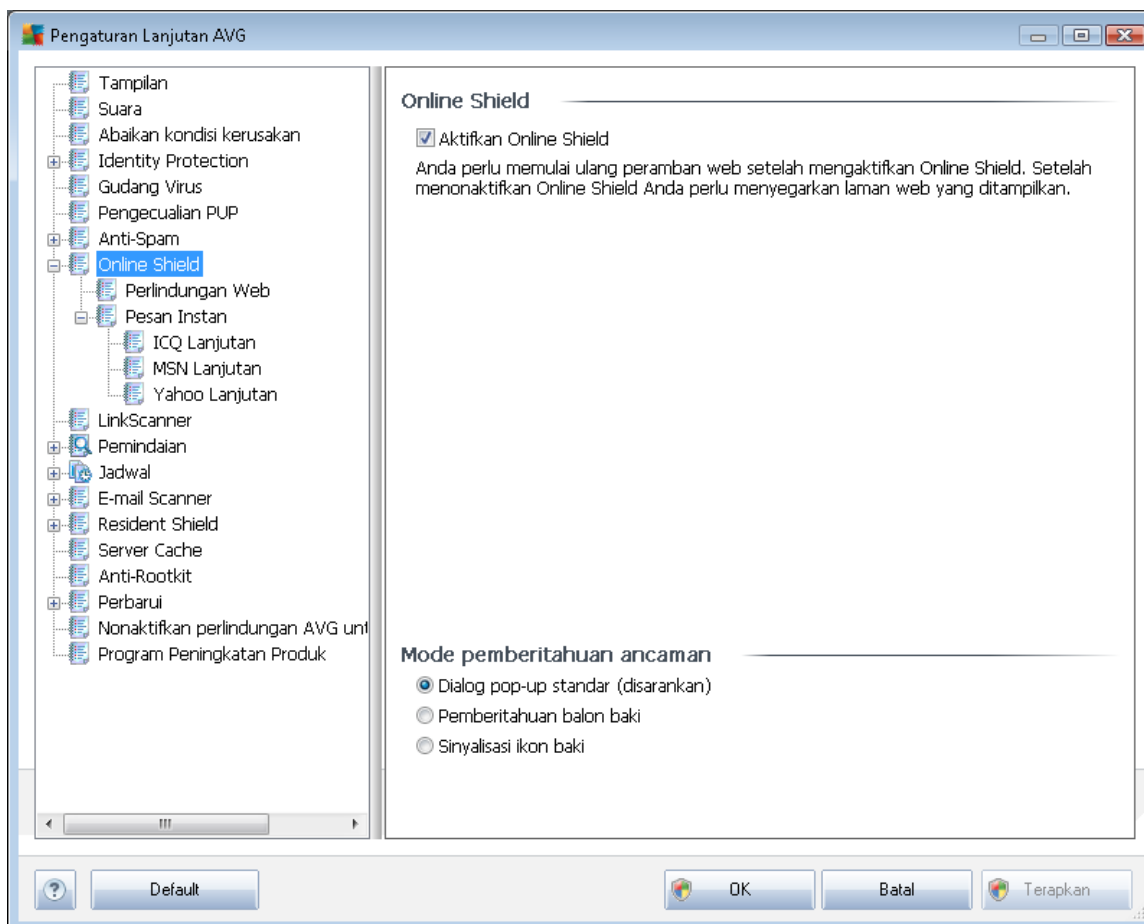
Cabang Pengaturan Lanjutan berisi opsi pengaturan lengkap untuk komponen Anti-Spam. Pengaturan ini ditujukan untuk pengguna berpengalaman, umumnya administrator jaringan yang perlu mengkonfigurasi perlindungan anti-spam secara terperinci untuk perlindungan terbaik server e-mail. Oleh karena itu, tidak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

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

9.8. Online Shield



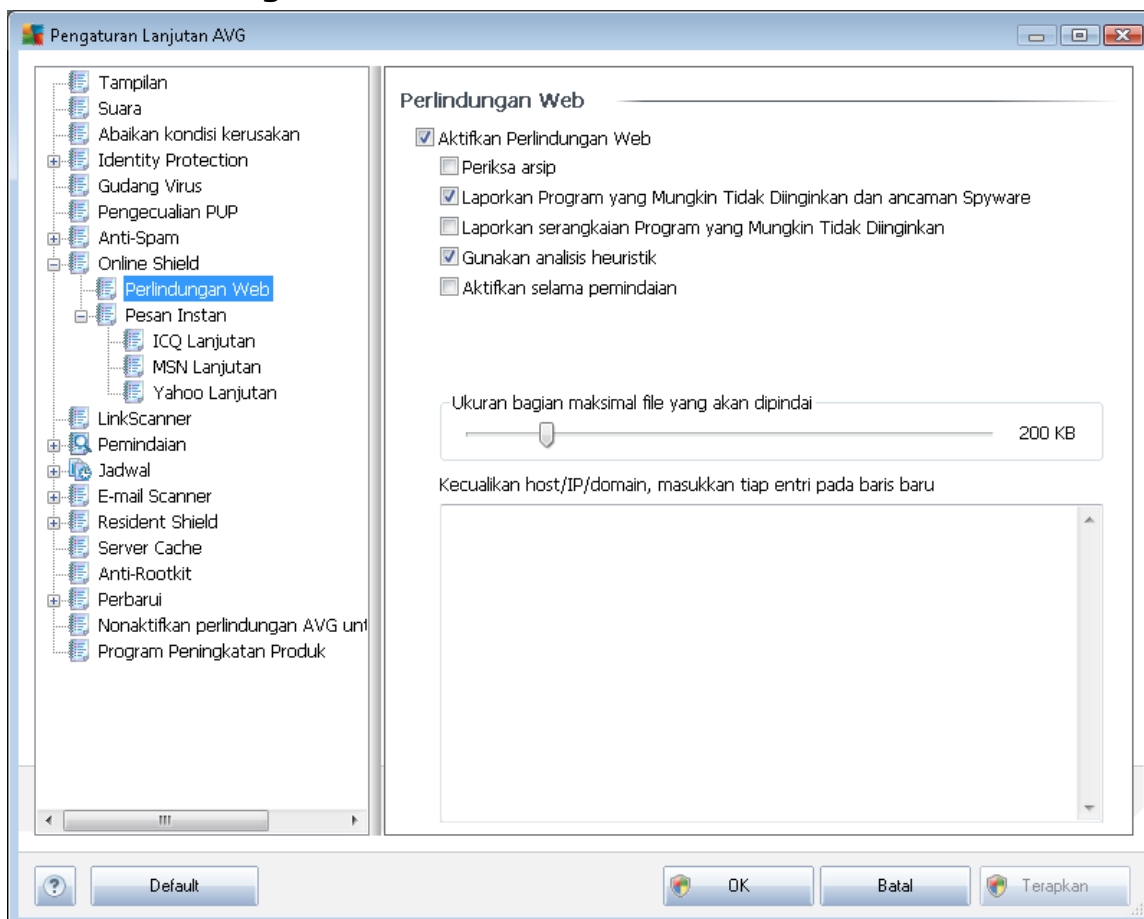
Dialog **Online Shield** memungkinkan Anda untuk mengaktifkan/menonaktifkan seluruh komponen **Online Shield** melalui opsi **Aktifkan Online Shield** (*diaktifkan secara default*). Untuk pengaturan lanjutan atas komponen ini, lanjutkan ke dialog berikutnya sebagaimana tercantum dalam navigasi struktur:

- [Perlindungan Web](#)
- [Pesan Instan](#)

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.

9.8.1. Perlindungan Web



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

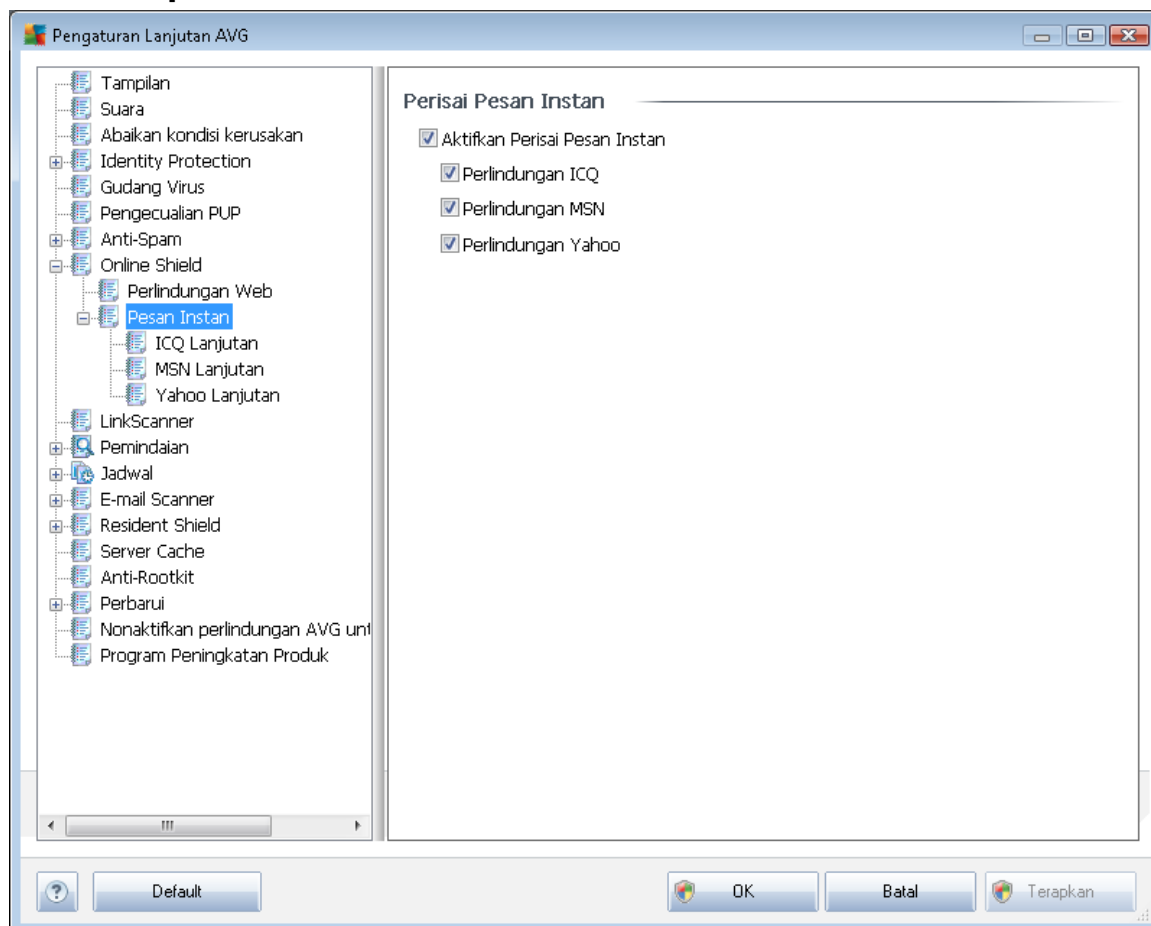
- **Aktifkan Perlindungan Web** - opsi ini mengonfirmasi bahwa [Online Shield](#) harus melakukan pemindaian atas isi halaman www. Asalkan opsi ini diaktifkan (*secara default*), Anda dapat mengaktifkan/menonaktifkan item ini:
 - o **Periksa arsip** - (*dinonaktifkan secara default*): memindai isi arsip yang mungkin telah dimasukkan di halaman www yang akan ditampilkan.
 - o **Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware** - (*diaktifkan secara default*): centang 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.
 - o **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.

- o **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).
- o **Aktifkan pemindaian menyeluruh** (dininaktifkan 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.
- o **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, [Perisai Tetap](#) akan segera mendeteksinya.
- o **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.

9.8.2. Perpesanan Instan

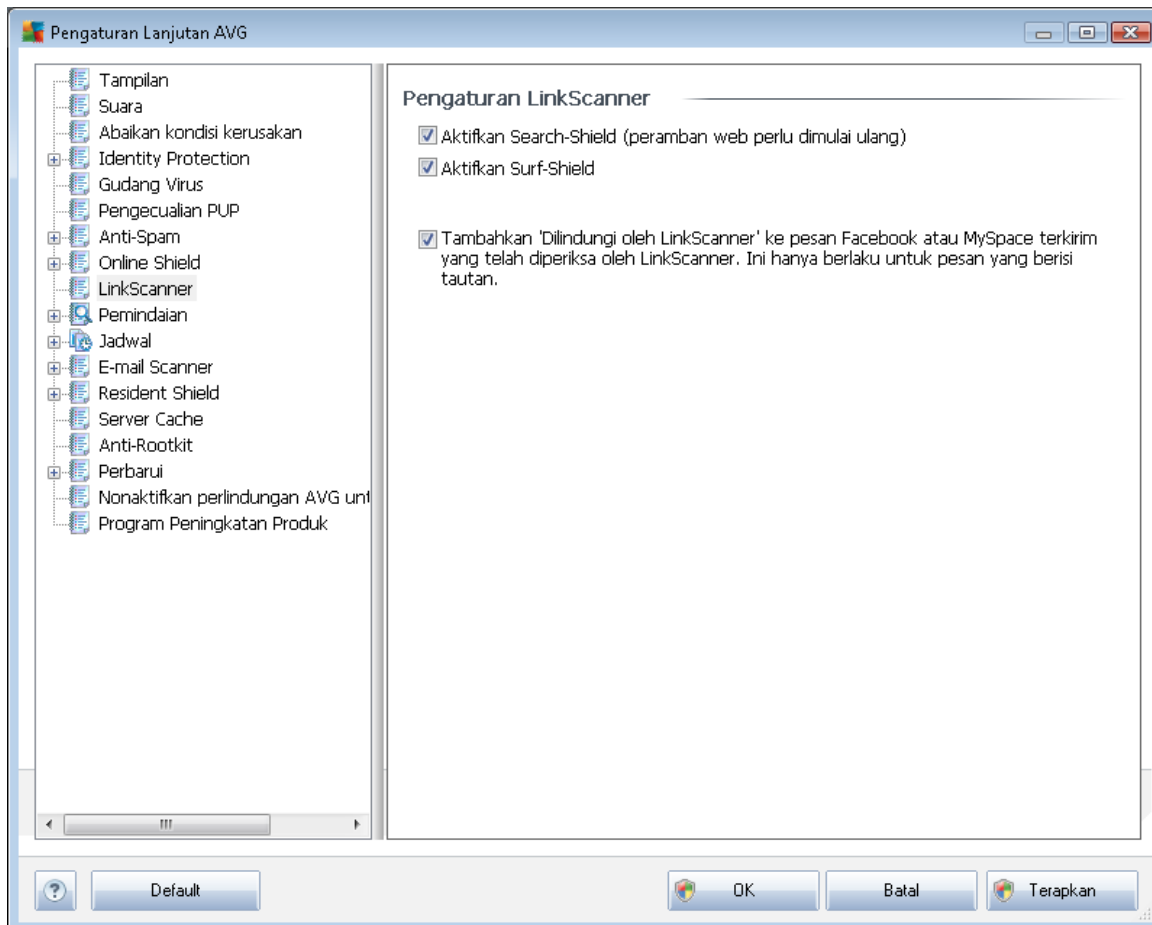


Dalam dialog **Perisai Pesan Instan** Anda dapat mengedit pengaturan komponen **Online Shield** yang mengacu pada pemindaian pesan instan. Saat ini, mendukung tiga program pesan instan berikut: **ICQ**, **MSN**, dan **Yahoo** - centang item terkait untuk setiap item jika Anda ingin **Online Shield** memverifikasi komunikasi online bebas virus.

Untuk spesifikasi lebih lanjut mengenai pengguna yang diperbolehkan/diblokir, Anda dapat melihat dan mengedit dialog terkait (**ICQ Lanjutan**, **MSN Lanjutan**, **Yahoo Lanjutan**) dan menetapkan **Daftar Putih** (daftar pengguna yang akan diperbolehkan berkomunikasi dengan Anda) dan **Daftar Hitam** (pengguna yang harus diblokir).

9.9. Link Scanner

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 eksploitatif saat mengaksesnya. Koneksi situs jahat yang telah dikenal dan konten eksploitatifnya diblokir begitu ia diakses oleh pengguna melalui peramban web (*atau aplikasi lain yang menggunakan HTTP*).
- **Tambahkan 'Dilindungi oleh LinkScanner' ...** - tandai pilihan ini untuk mengonfirmasi Anda ingin memasukkan keterangan sertifikasi pemeriksaan [Link Scanner](#) di semua pesan yang mengandung hyperlink aktif, yang dikirim dari jejaring sosial Facebook dan MySpace.

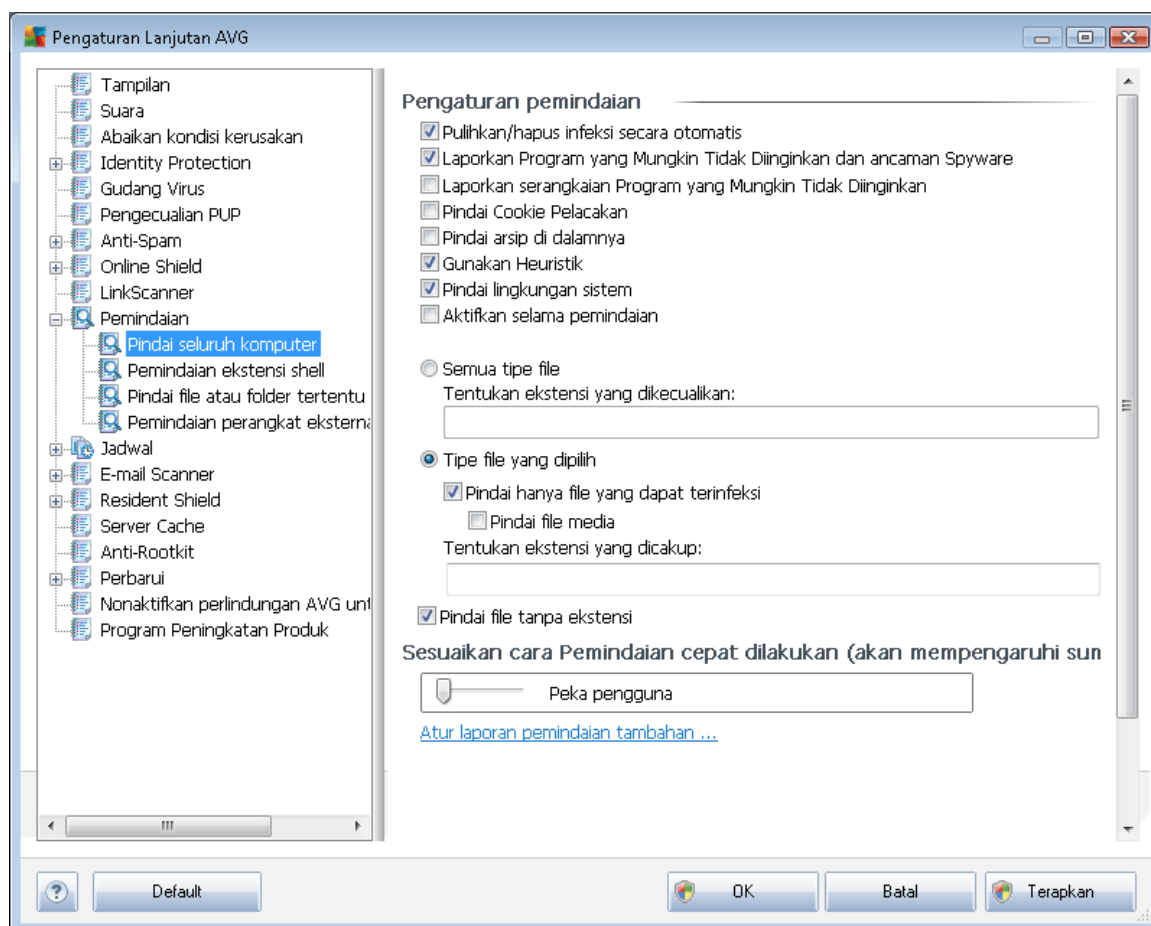
9.10. Pemindaian

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
- [Pindai File atau Folder Tertentu](#) - pemindaian standar yang ditentukan atas area yang dipilih pada komputer Anda
- [Pemindaian Perangkat Eksternal](#) - pemindaian tertentu atas perangkat eksternal yang dipasang pada komputer Anda

9.10.1. Pindai 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 secara otomatis** (*diaktifkan secara default*) - jika ada virus teridentifikasi selama pemindaian, ia dapat dipulihkan 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 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 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.

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;

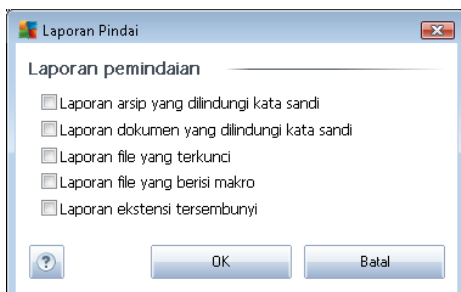
- **Tipe file yang dipilih** - Anda dapat menentukan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio - jika 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.

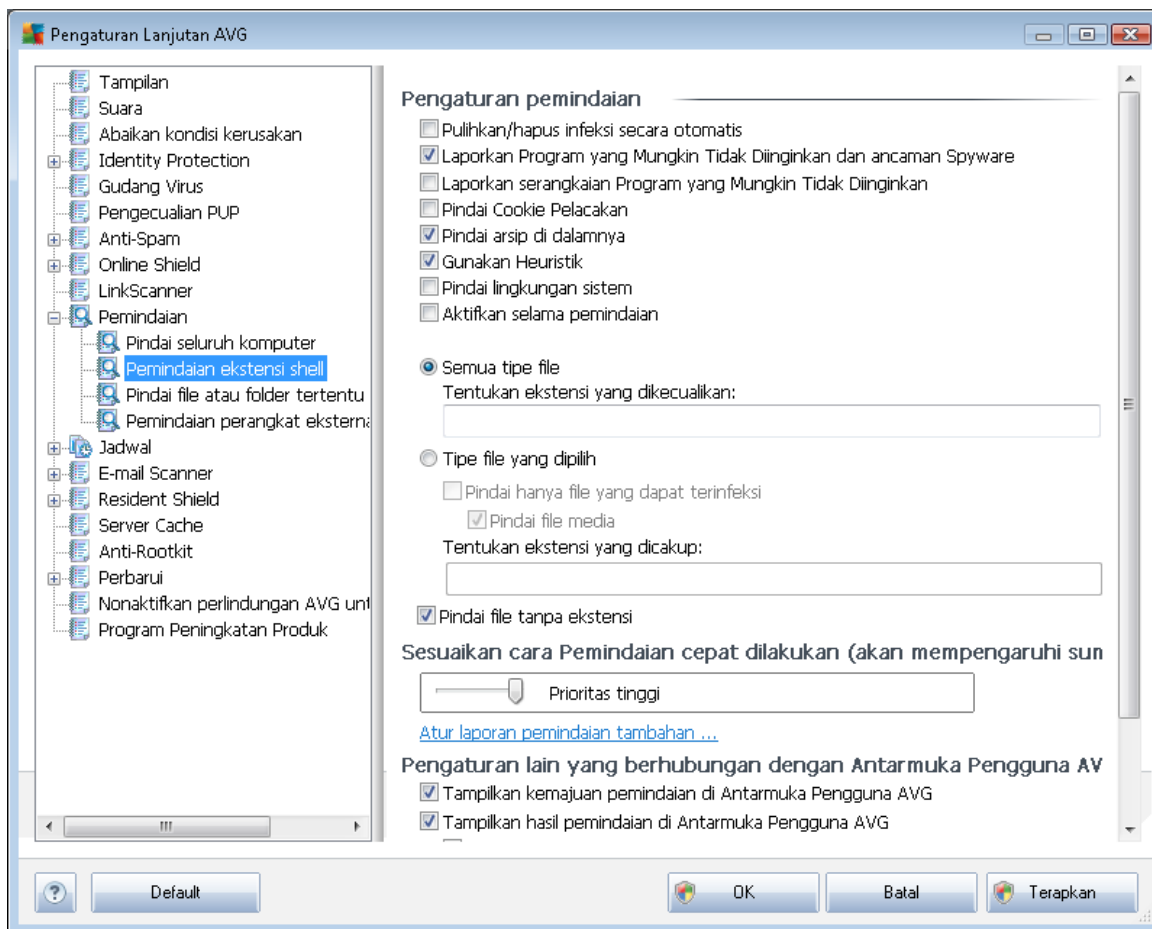
Atur laporan pemindaian tambahan ...

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:



9.10.2. Pemindaian Ekstensi Shell

Seperti pada fungsi [Pindai seluruh komputer](#) sebelumnya, fungsi yang dinamai **Pemindaian ekstensi shell** ini juga menawarkan beberapa opsi untuk mengedit pemindaian yang 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](#).



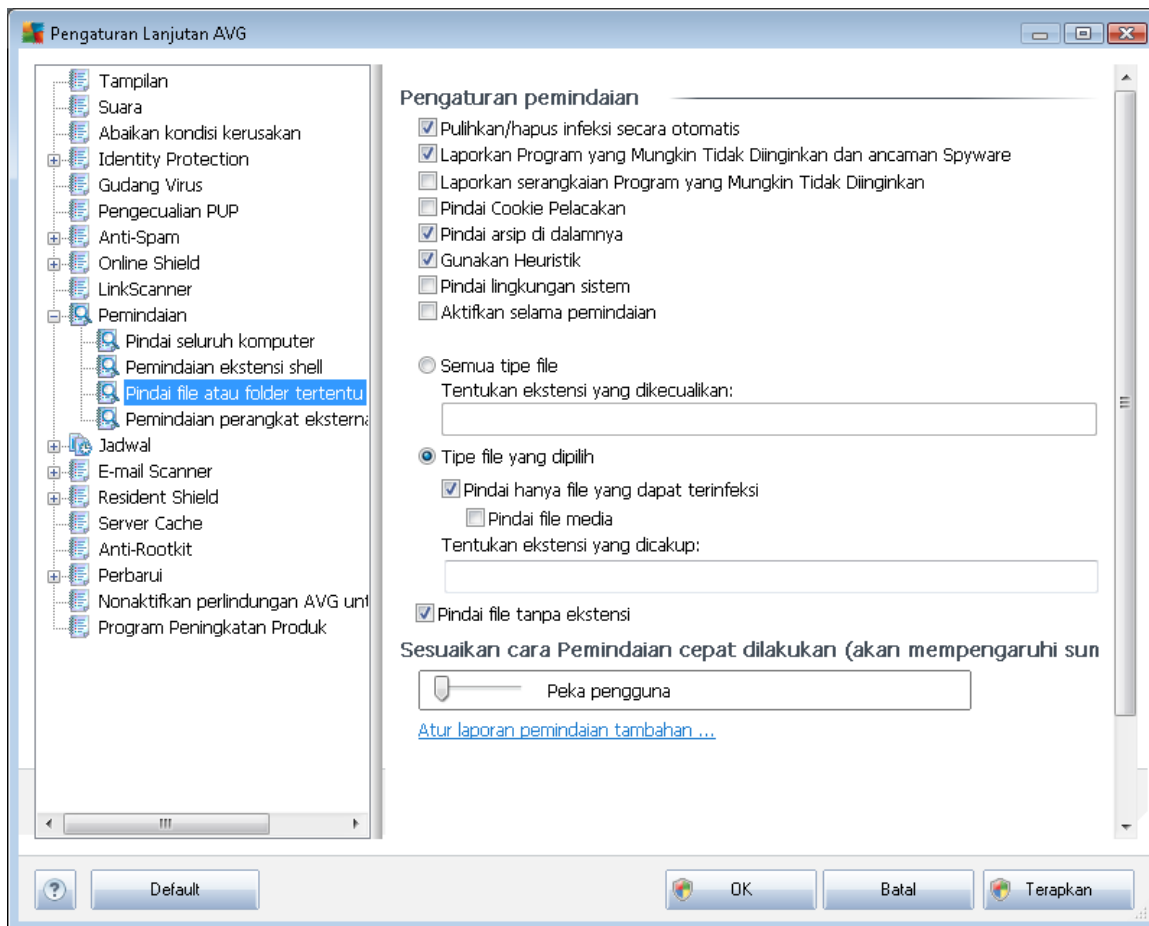
Daftar parameter identik dengan yang tersedia untuk [Pindai seluruh komputer](#). Akan tetapi, pengaturan default berbeda misalnya, *Pindai Seluruh Komputer secara default tidak memeriksa arsip tetapi memindai lingkungan sistem; sementara Pemindaian Ekstensi Shell melakukan sebaliknya*).

Catatan: Untuk keterangan mengenai parameter tertentu, bacalah bab [Pengaturan Lanjutan AVG / Pemindaian / Pindai Seluruh Komputer](#).

Dibandingkan dengan dialog [Pindai seluruh komputer](#), dialog [Pemindaian ekstensi shell](#) juga mencakup bagian yang disebut **Pengaturan lainnya terkait dengan antarmuka pengguna AVG**, tempat Anda dapat menentukan apakah Anda ingin kemajuan dan hasil pemindaian dapat diakses dari antarmuka pengguna. Juga, Anda dapat menentukan bahwa hasil pemindaian seharusnya hanya ditampilkan jika ada infeksi yang terdeteksi selama pemindaian.

9.10.3. Pindai File atau Folder Tertentu

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](#):

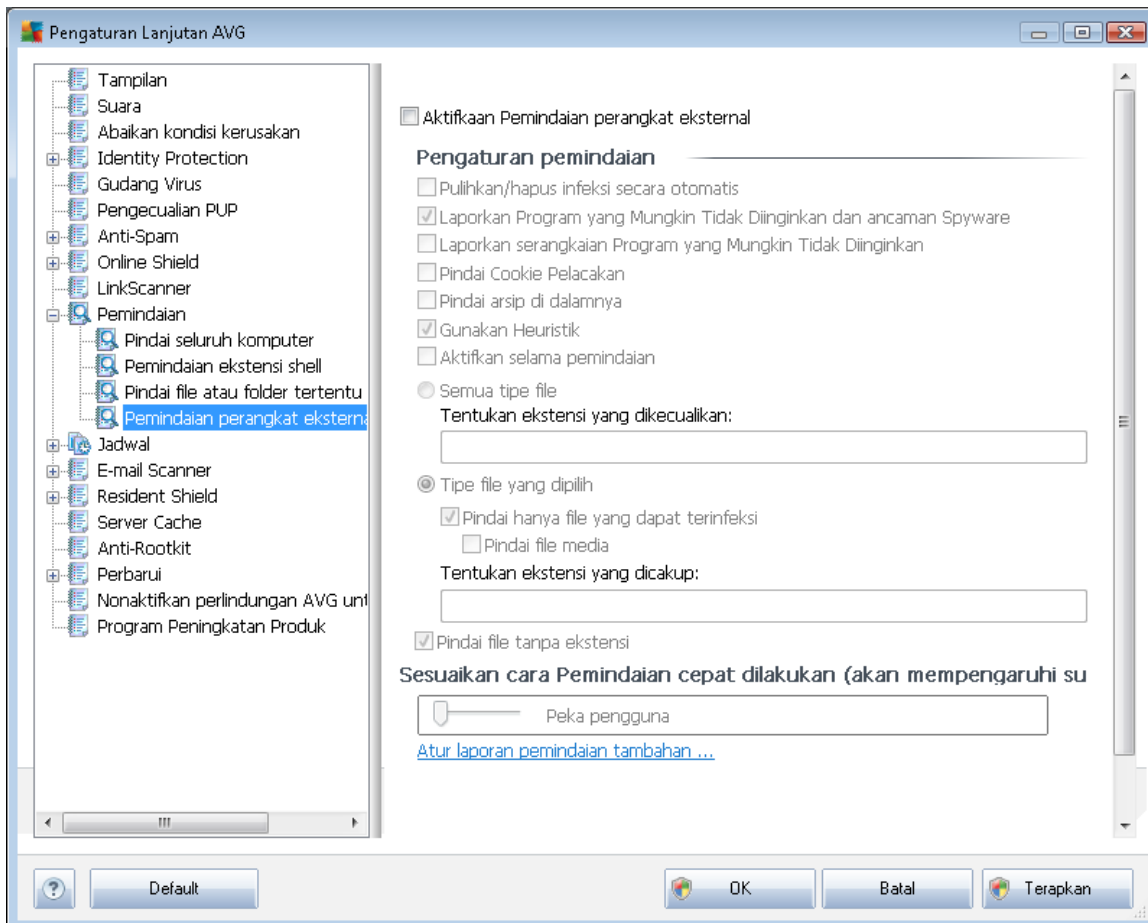


Semua parameter yang diatur dalam dialog konfigurasi ini hanya berlaku untuk area yang dipilih bagi pemindaian dengan **Pindai file atau folder tertentu!**

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

9.10.4. 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](#).

9.11. Jadwal

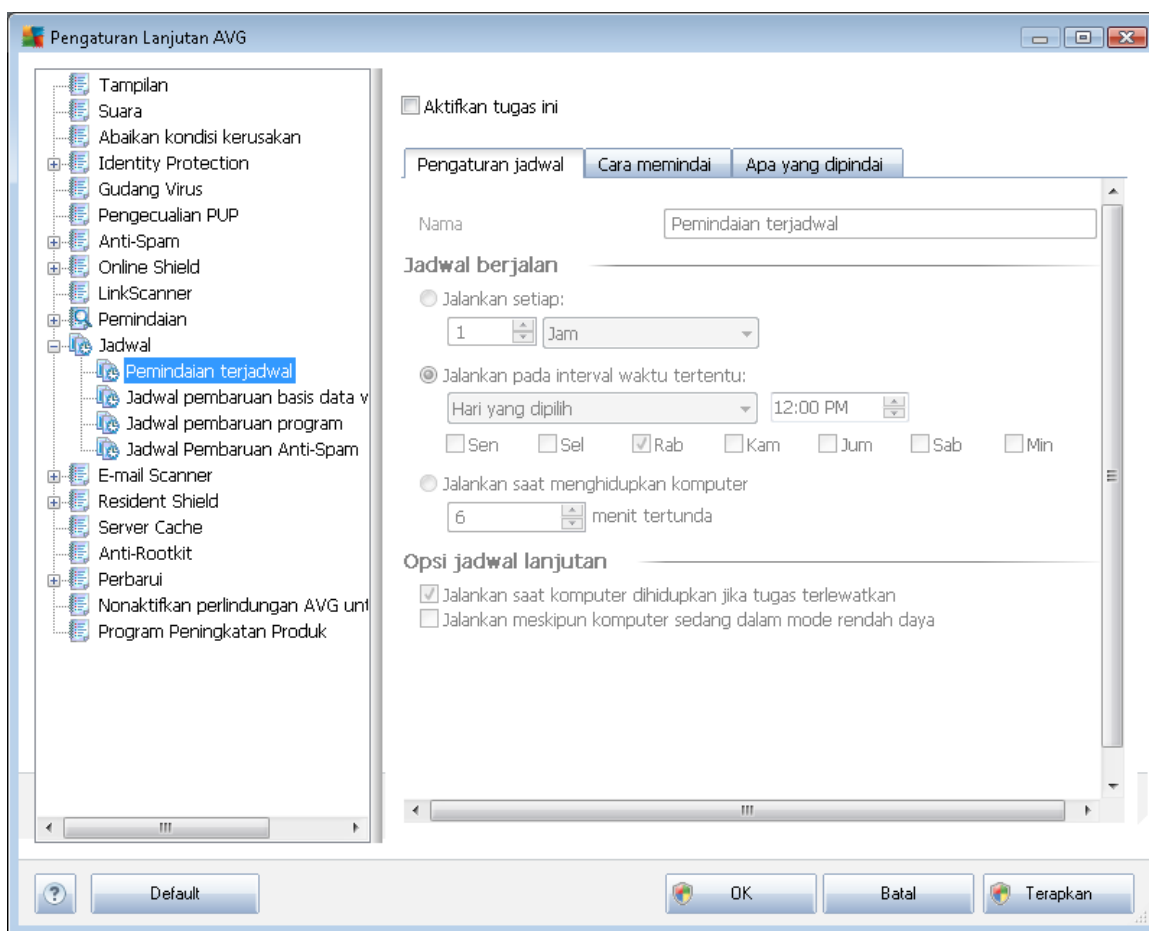
Di bagian **Jadwal** Anda dapat mengedit pengaturan default:

- [Pemindaian terjadwal](#)
- [Jadwal pembaruan basis data virus](#)

- [Jadwal pembaruan program](#)
- [Jadwal pembaruan Anti-Spam](#)

9.11.1. 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:

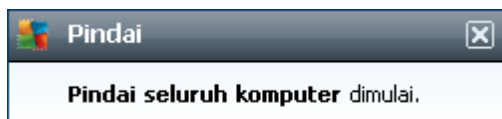
Jadwal berjalan

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 (**Tindakan berdasar menghidupkan komputer**).

Opsi jadwal lanjutan

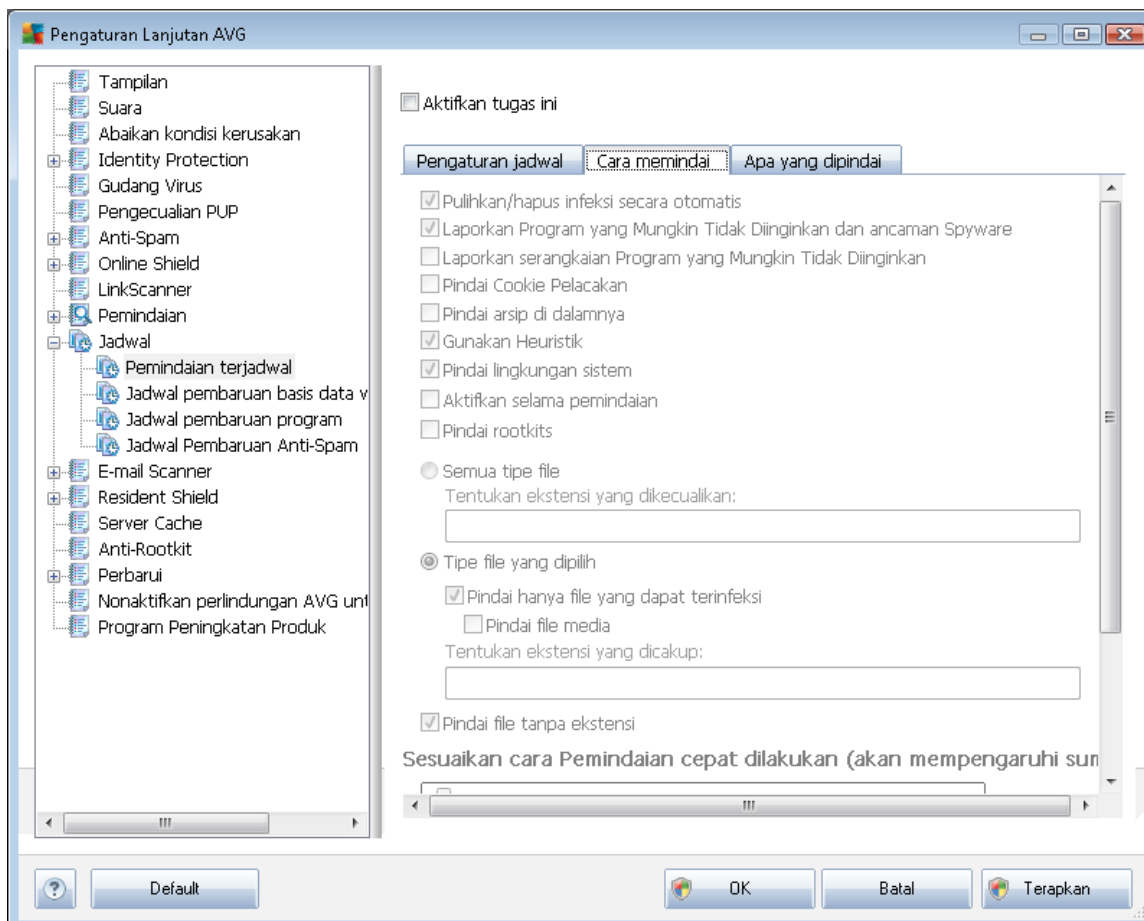
Di bagian ini Anda dapat menentukan dalam kondisi apa pemindaian harus/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sama sekali.

Setelah pemindaian terjadwal diluncurkan pada waktu yang ditetapkan, Anda akan diberi tahu mengenai hal ini melalui jendela sembul yang dibuka lewat [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 secara otomatis** (diaktifkan secara default): jika ada virus teridentifikasi selama pemindaian, file dapat dipulihkan 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 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 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 (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** (dinonaktifkan secara default): tandai item ini jika Anda ingin menyertakan deteksi rootkit ke pemindaian seisi komputer. Deteksi rootkit juga tersedia pada komponen [Anti-Rootkit](#) sendiri;

Selanjutnya, Anda harus menentukan apakah Anda ingin memindai

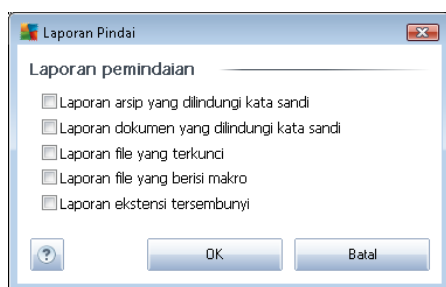
- **Semua tipe file** dengan memungkinkan penetapan pengecualian dari pemindaian dengan memberikan daftar file ekstensi yang dipisah koma (setelah disimpan, koma akan berganti menjadi titik koma) untuk file yang tidak boleh dipindai;
- **Tipe file yang dipilih** - Anda dapat menentukan bahwa Anda hanya 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.

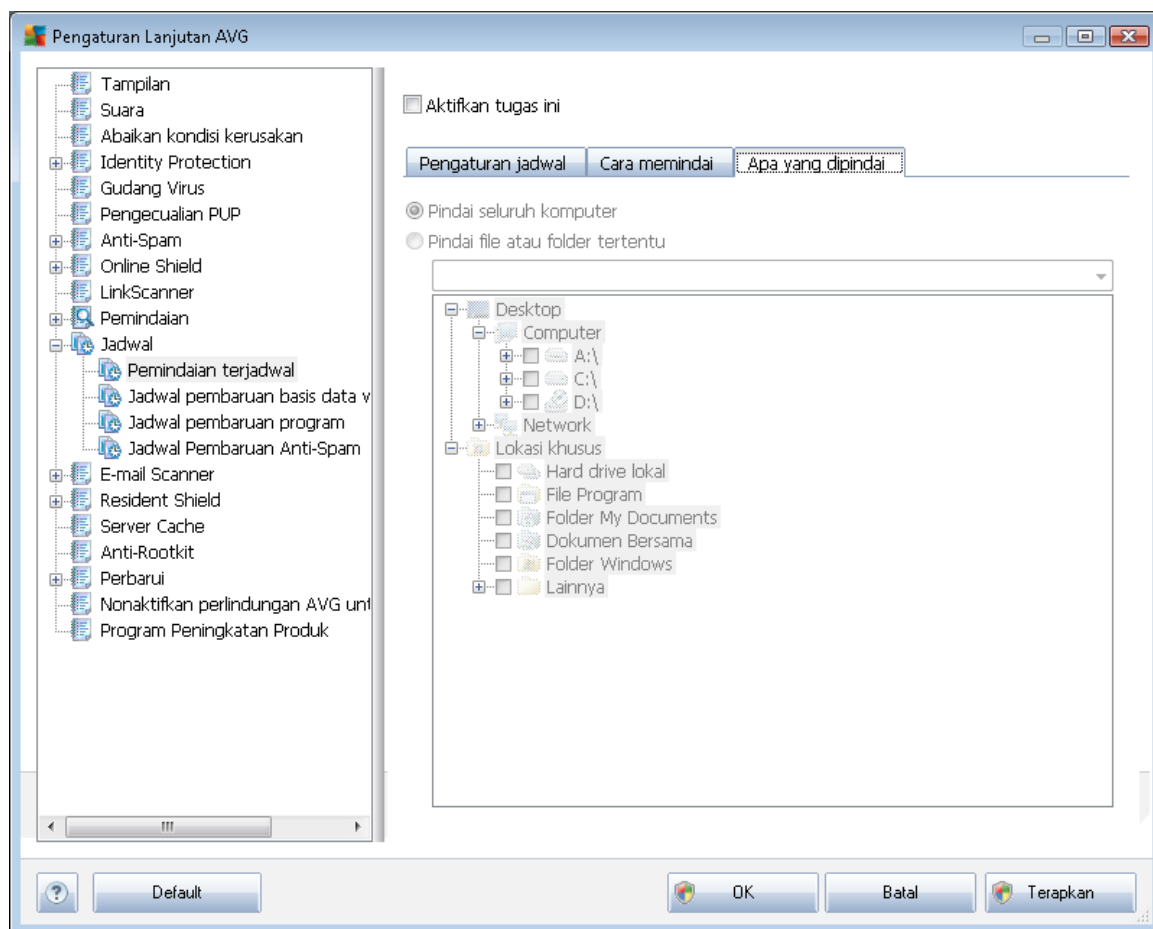
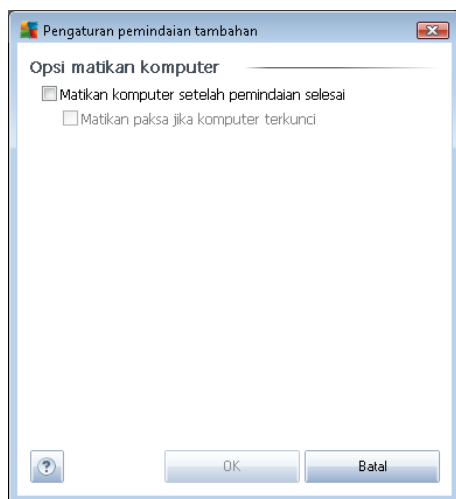
Atur laporan pemindaian tambahan

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**).

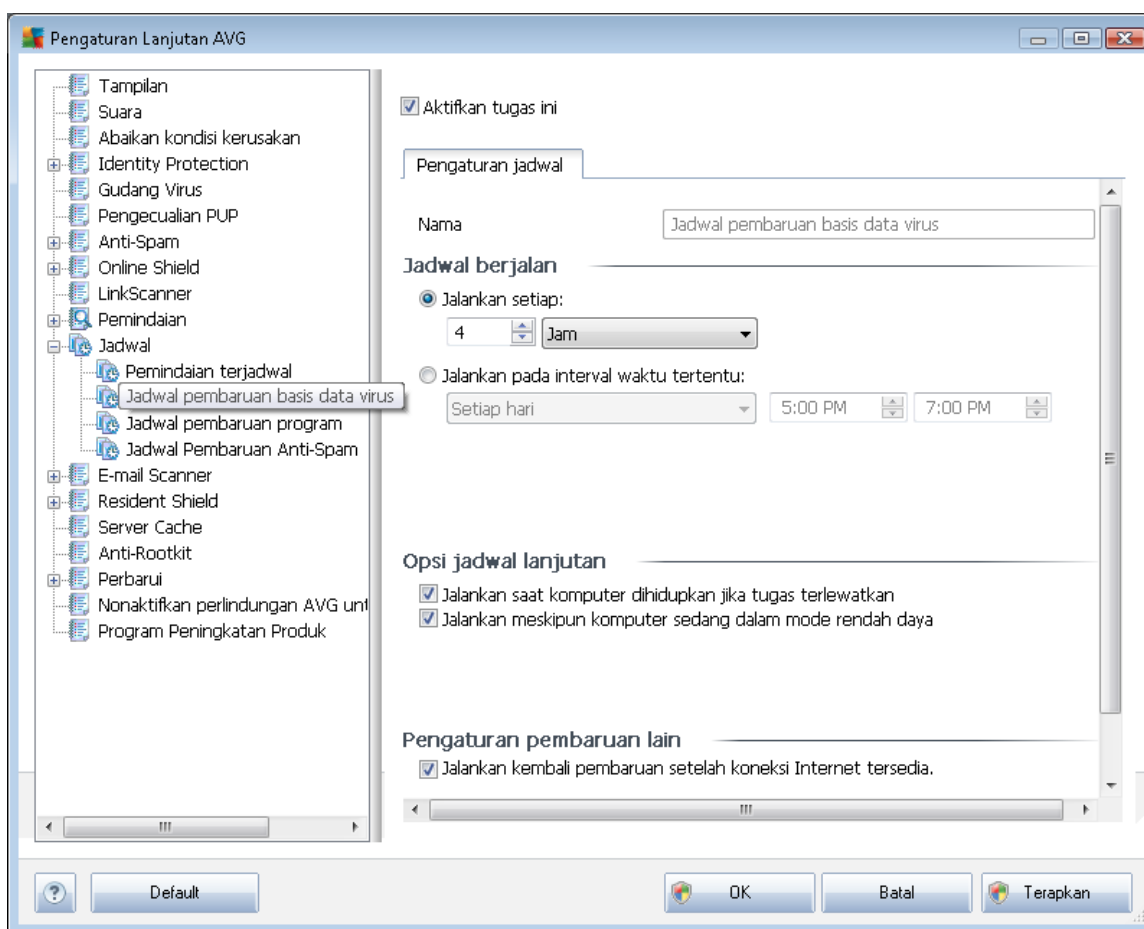


Pada tab ***Apa yang dipindai*** Anda dapat menentukan apakah Anda ingin menjadwalkan [pemindaian seluruh komputer](#) atau [pemindaian file atau folder tertentu](#). Jika Anda memilih pemindaian file atau folder tertentu, di bagian bawah dialog ini akan diaktifkan struktur yang

ditampilkan dan Anda dapat menetapkan folder yang akan dipindai.

9.11.2. Jadwal Pembaruan Basis Data Virus

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



Penjadwalan pembaruan basis data virus dasar telah tercakup dalam komponen [Pengatur Pembaruan](#). Dalam dialog ini, Anda dapat mengatur beberapa parameter terperinci atas jadwal pembaruan basis data virus. Dalam bidang teks **Nama** (*dinonaktifkan untuk semua jadwal default*) ada nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Dalam bagian ini, tetapkan interval waktu untuk peluncuran pembaruan basis data virus 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

Di bagian ini Anda dapat menentukan dalam kondisi apa pembaruan basis data virus harus/tidak harus diluncurkan jika komputer dalam mode daya rendah atau dimatikan sama sekali.

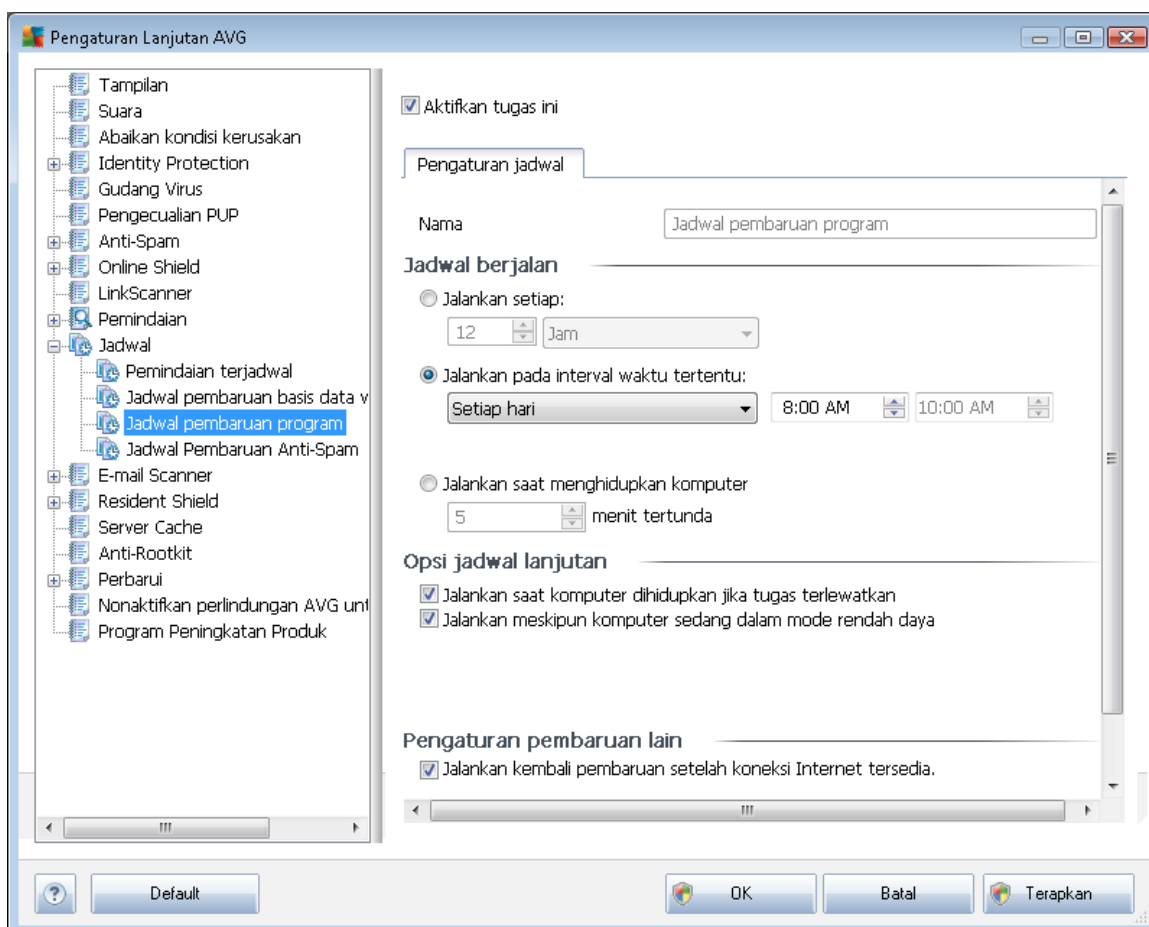
Pengaturan pembaruan lain

Akhirnya, centang 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](#)).

9.11.3. 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

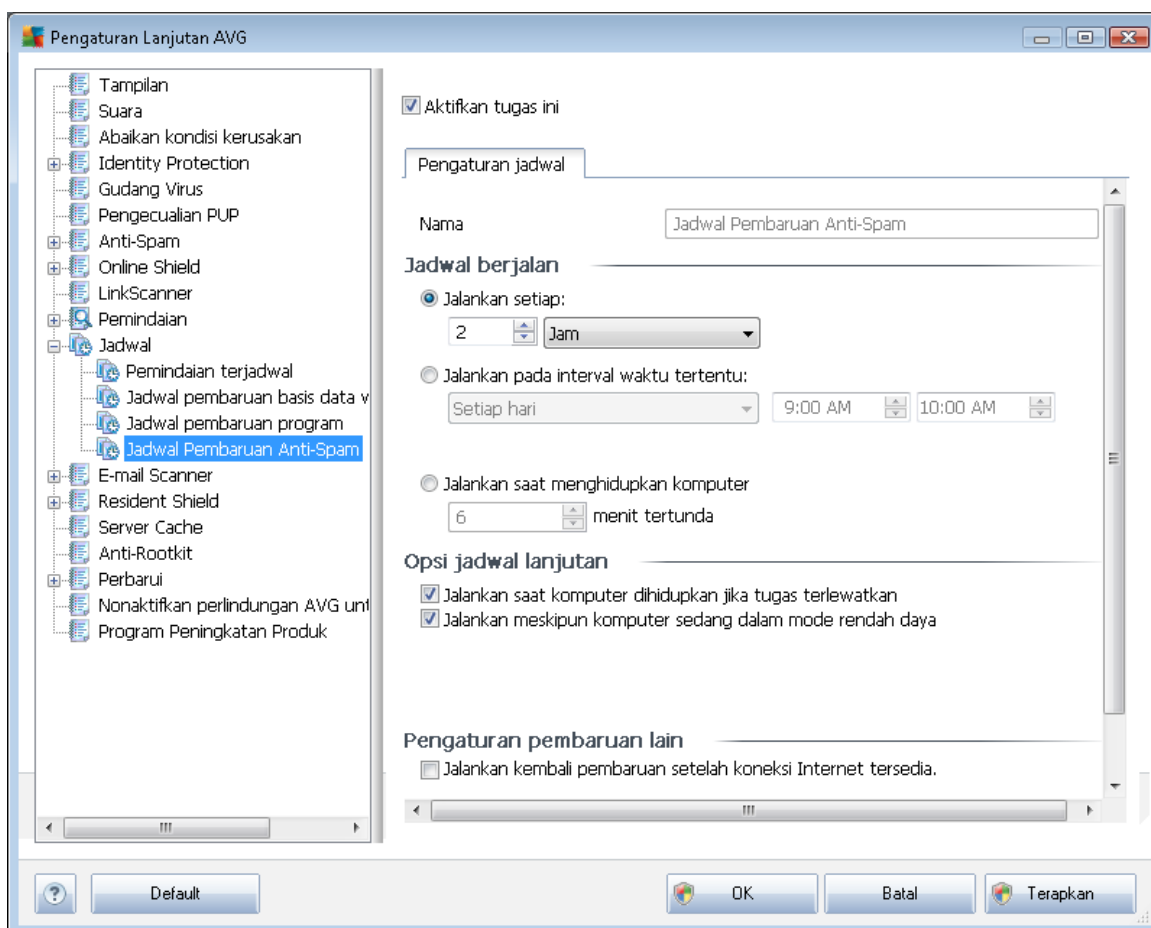
Centang opsi **Jalankan pembaruan lagi segera setelah koneksi Internet tersedia** untuk memastikan bahwa jika koneksi Internet rusak dan proses pembaruan gagal, maka ia akan diluncurkan lagi segera setelah koneksi Internet pulih.

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.

9.11.4. 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:



Penjadwalan pembaruan **Anti-Spam** dasar telah tercakup dalam komponen **Pengatur Pembaruan**. Dalam dialog ini Anda dapat mengatur beberapa parameter terperinci pada 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 dengan pengulangan peluncuran pembaruan **Anti-Spam** 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 pengaktifan 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 sama sekali.

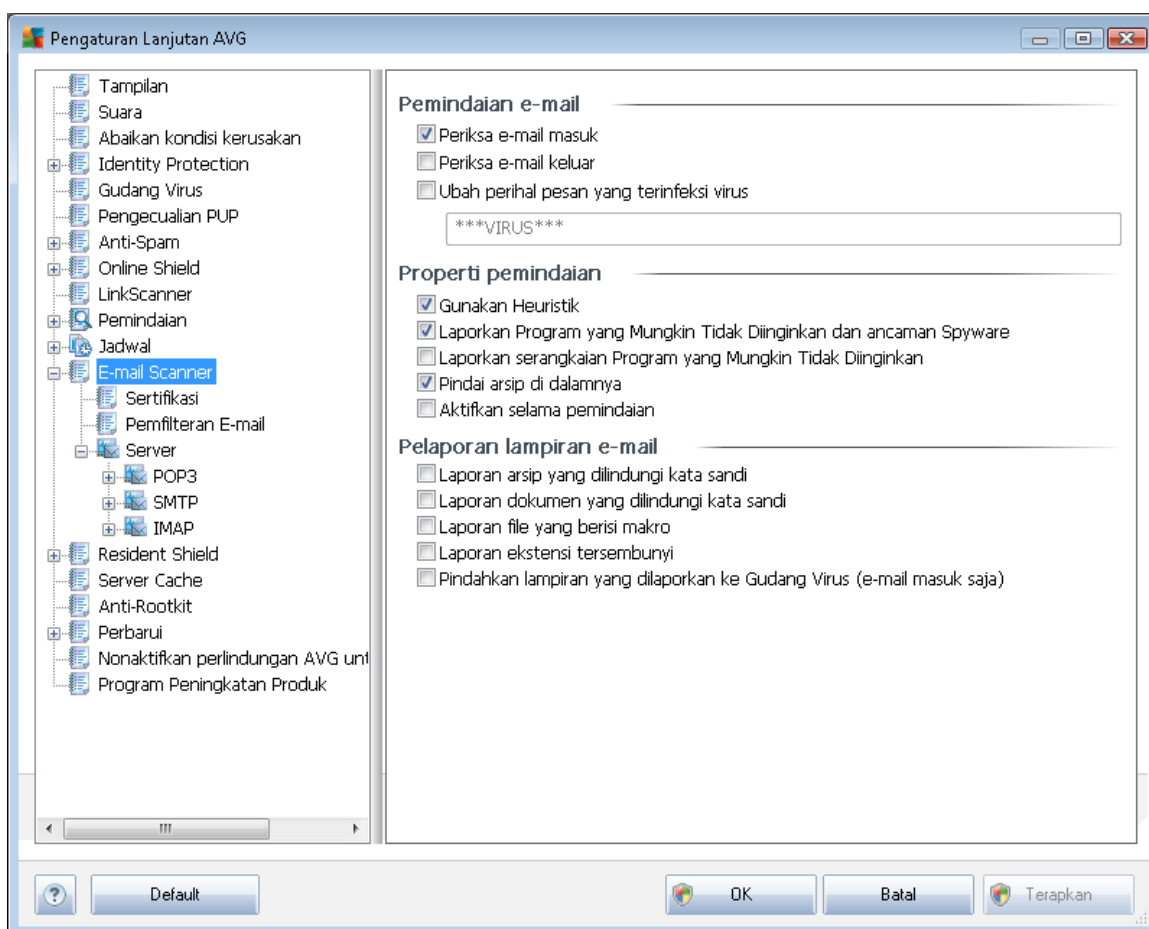
Pengaturan pembaruan lain

Centang 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 diberitahu mengenai hal ini melalui jendela yang muncul di atas [ikon baki sistem AVG](#) (asalkan Anda telah membiarkan konfigurasi default pada dialog [Pengaturan Lanjutan/Tampilan](#)).

9.12. Pemindai E-mail

Dialog **Pemindai E-mail** 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



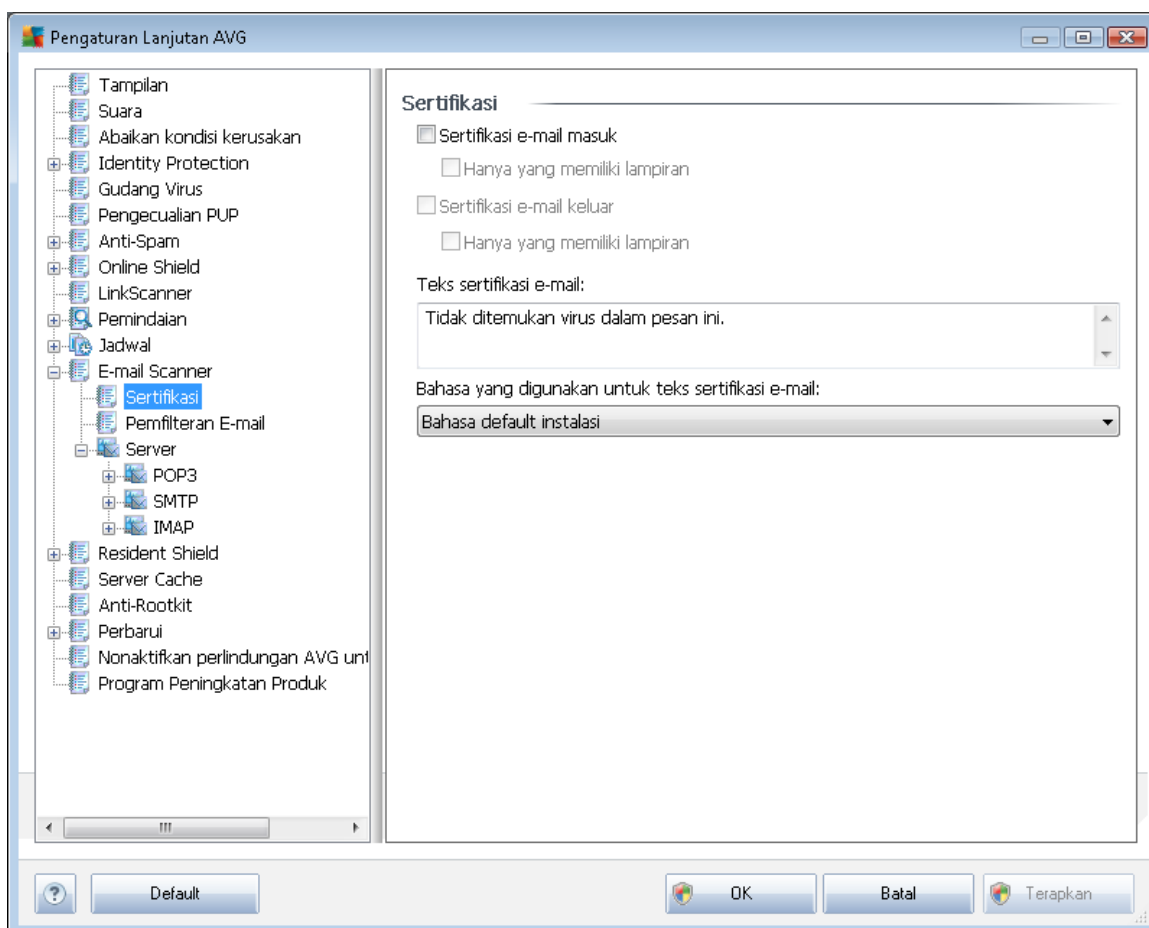
Di bagian ini, Anda dapat mengatur laporan tambahan tentang file yang mungkin membahayakan atau mencurigakan. Perhatikan bahwa tidak ada dialog peringatan yang ditampilkan, hanya teks sertifikasi yang akan ditambahkan di akhir pesan e-mail, dan semua laporan tersebut akan terdaftar dalam dialog [Deteksi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

- **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](#).



9.12.1. Sertifikasi

Pada dialog **Sertifikasi** Anda dapat menentukan teks dan bahasa sertifikasi untuk pesan masuk dan keluar:



Teks sertifikasi terdiri atas dua bagian, bagian pengguna dan bagian sistem - lihat contoh berikut: baris pertama menggambarkan bagian pengguna, sisanya dibuat secara otomatis:

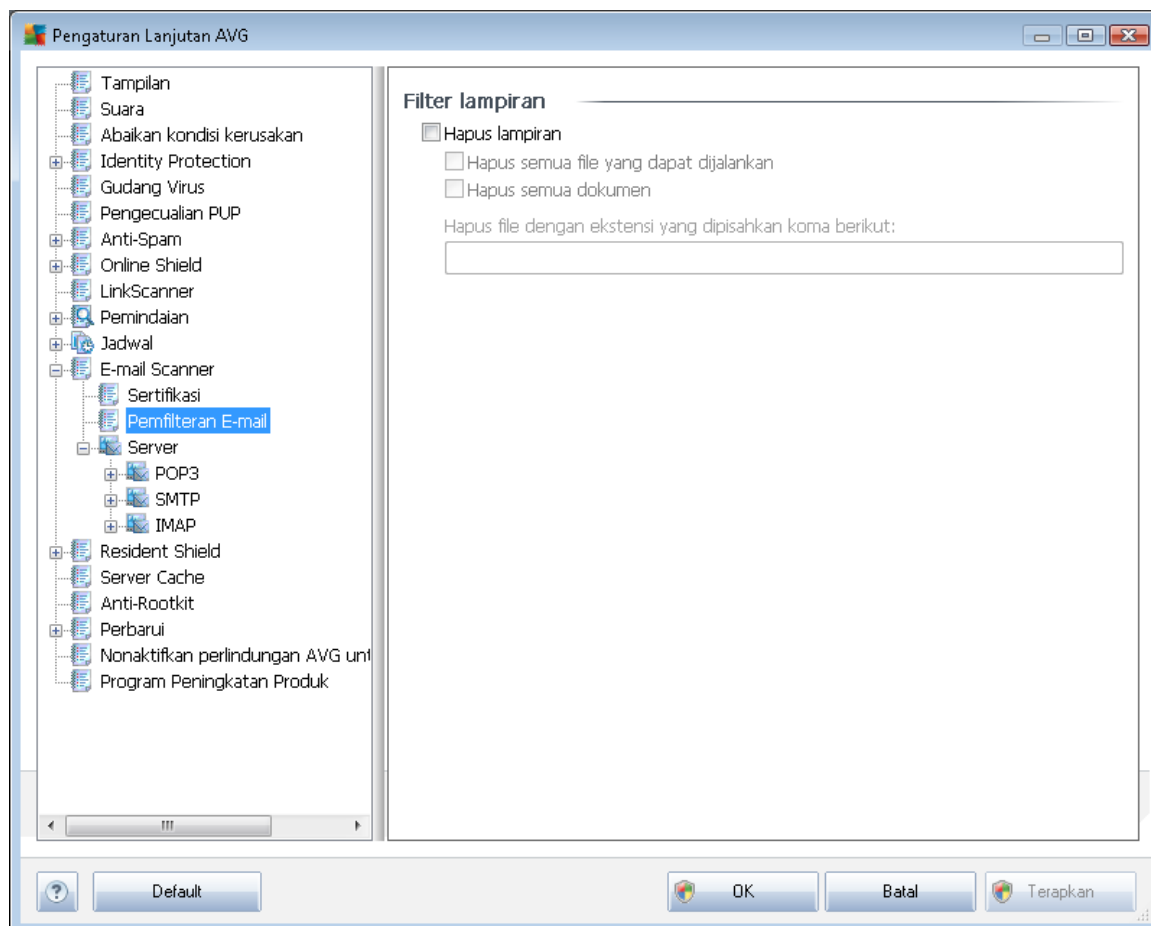
Tidak ditemukan virus dalam pesan ini.

Telah diperiksa oleh AVG.

Versi: x.y.zz / Basis Data Virus: xx.y.z - Tanggal Rilis: 12/9/2010

Jika Anda memutuskan untuk menggunakan sertifikasi untuk pesan email masuk atau keluar, selanjutnya dalam dialog ini Anda dapat menentukan kata-kata dalam bagian pengguna teks sertifikasi (**Teks sertifikasi email**), dan memilih bahasa apa yang digunakan untuk bagian sistem sertifikasi yang dibuat secara otomatis (**Bahasa yang digunakan untuk teks sertifikasi email.**).

9.12.2. Pemfilteran E-mail

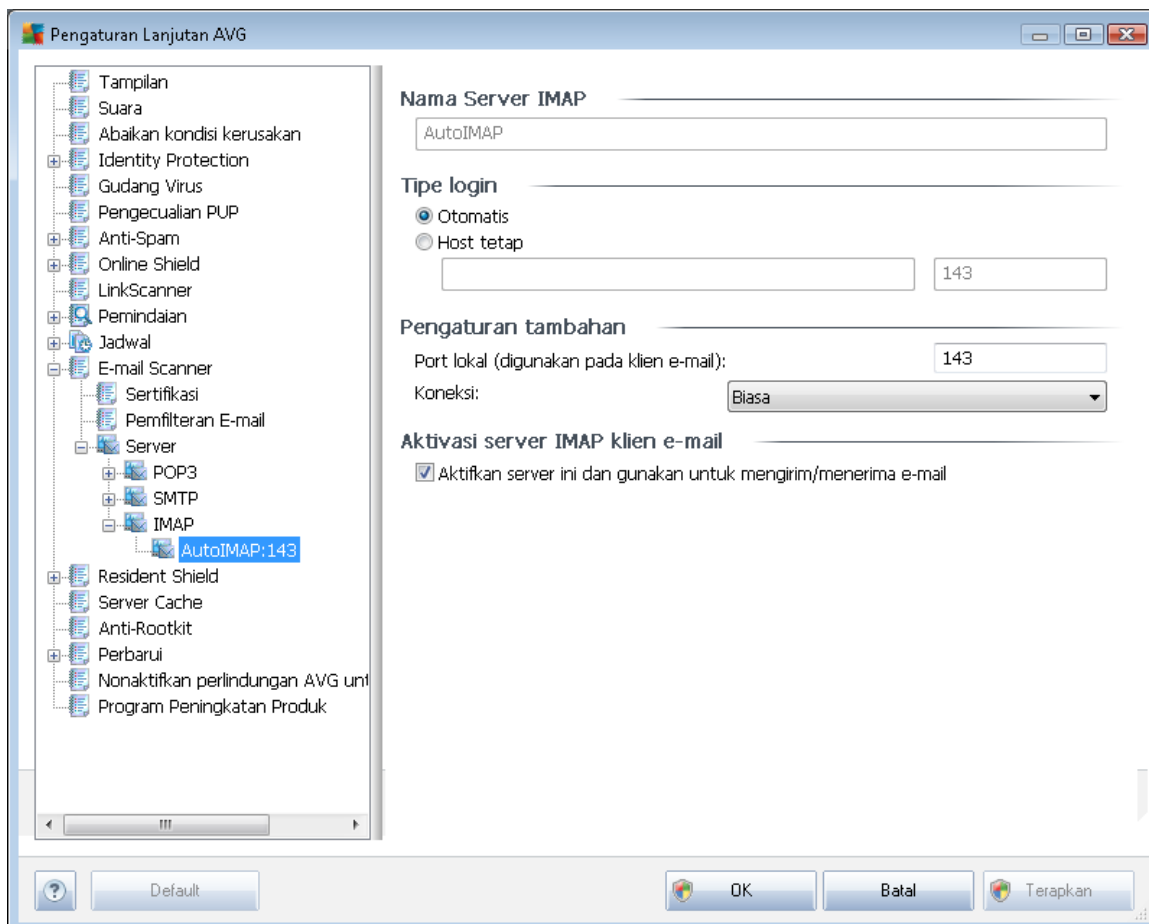


Dialog **Filter lampiran** memungkinkan Anda mengatur parameter untuk pemindaian lampiran pesan e-mail. Secara default, opsi **Hapus lampiran** dinonaktifkan. Jika Anda memutuskan untuk mengaktifkannya, semua pesan e-mail yang terdeteksi sebagai infeksi atau mungkin berbahaya akan dihapus secara otomatis.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

9.12.3. Server

Di bagian **Server** Anda dapat mengedit parameter server komponen **Pemindai E-mail** atau membuat server baru dengan menggunakan tombol **Tambah server baru**.

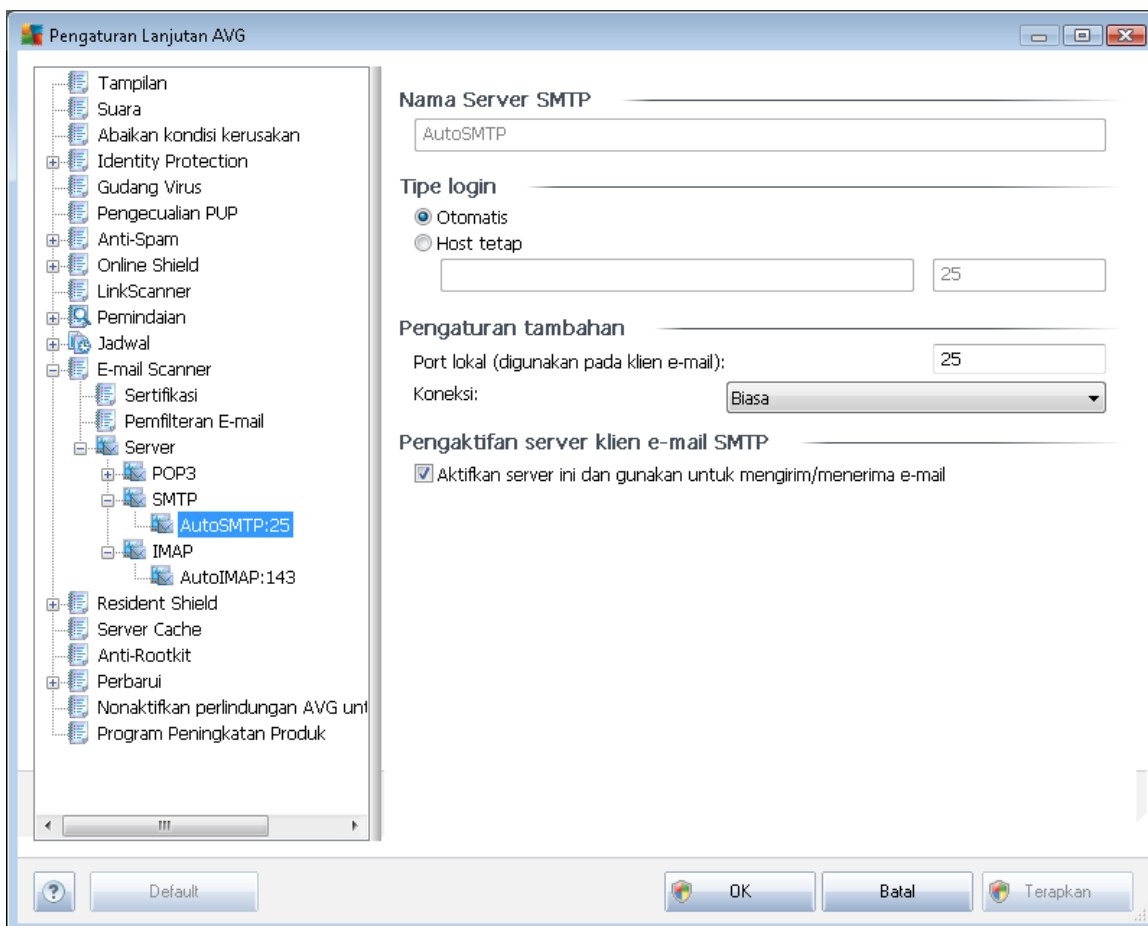


Dalam dialog ini (*dibuka melalui **Server / POP3***) Anda dapat mengatur server baru **Pemindai Email** dengan menggunakan protokol POP3 untuk email masuk:

- **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:
 - o **Otomatis** - Login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda.
 - o **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:
 - o **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.
 - o **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



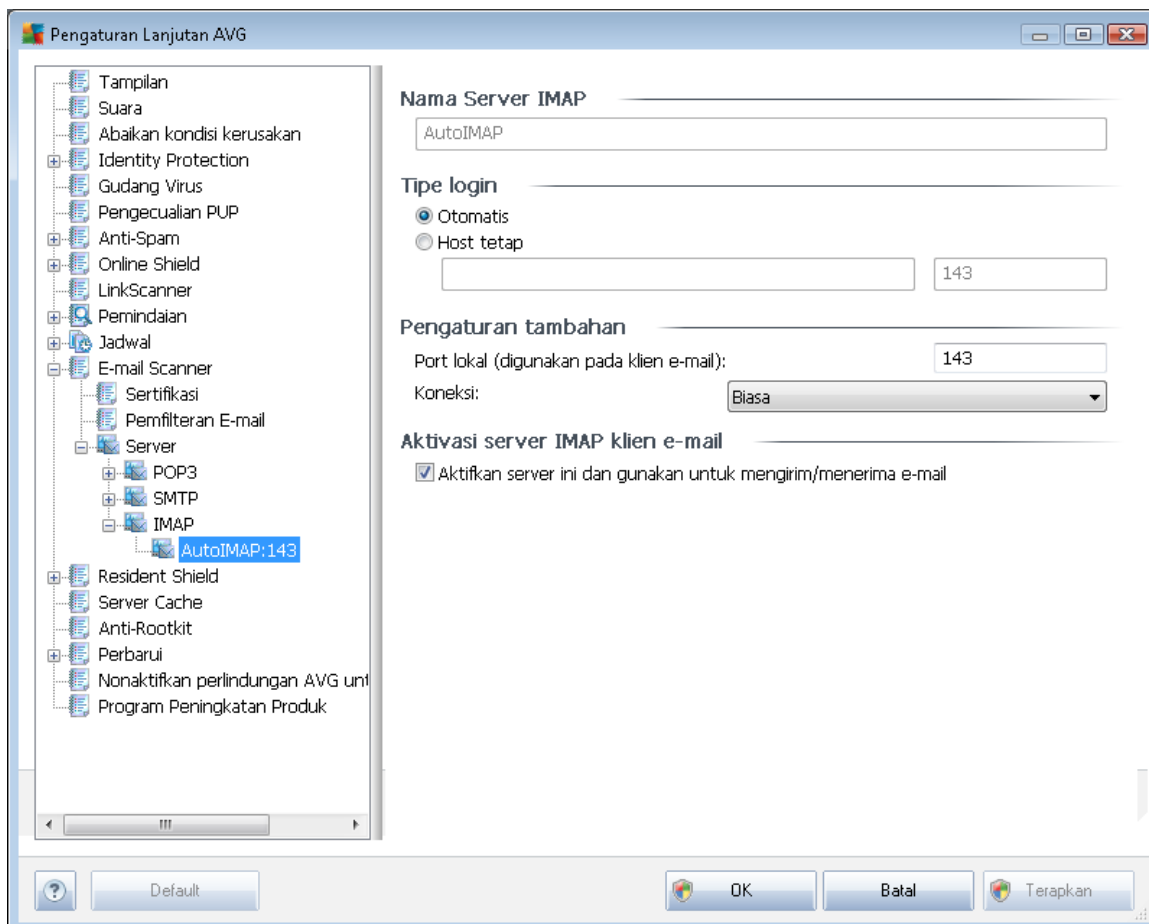
Dalam dialog ini (*dibuka melalui **Server / SMTP***) Anda dapat mengatur server baru **Pemindai Email** dengan menggunakan protokol SMTP untuk email keluar:

- **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:
 - o **Otomatis** - login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda
 - o **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:
 - o **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.
 - o **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 **Pemindai Email** dengan menggunakan protokol IMAP untuk Email keluar:

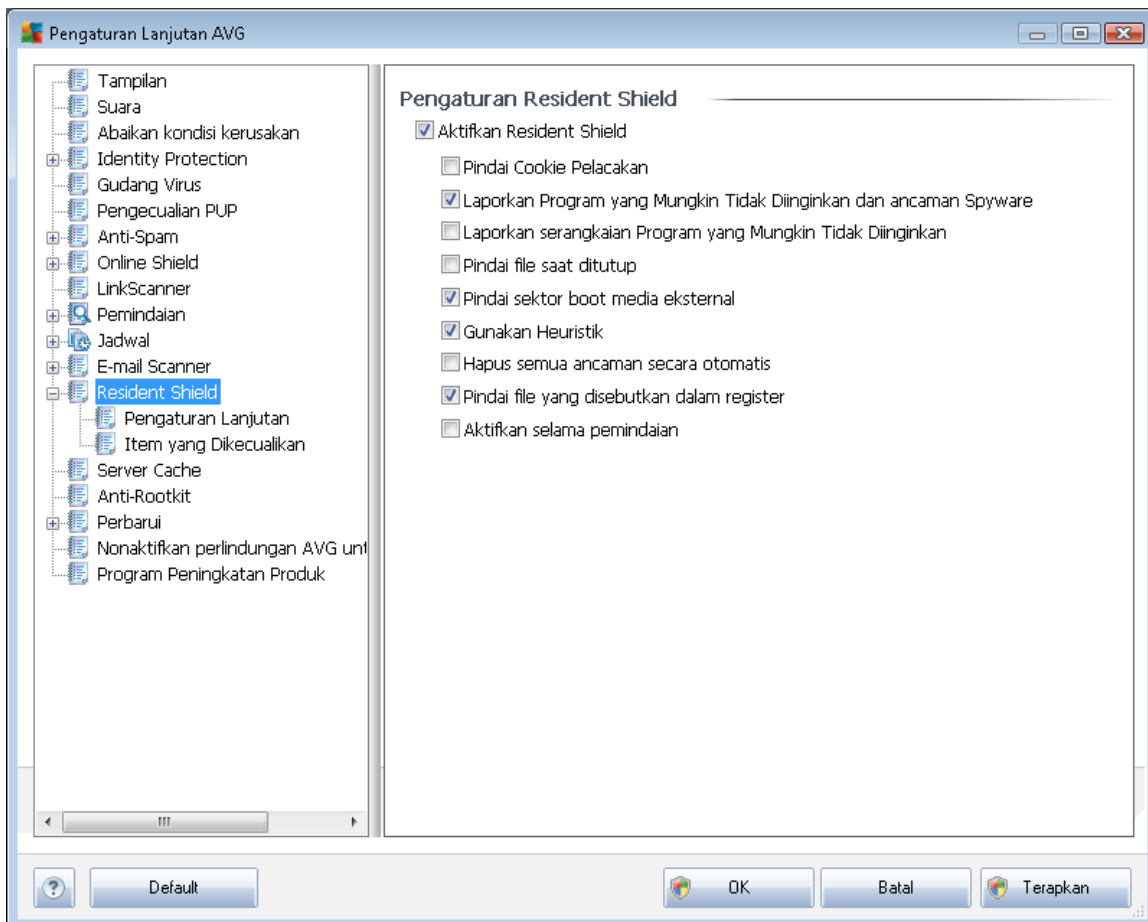
- **Nama Server IMAP** - di bidang ini Anda dapat menentukan nama server yang baru ditambahkan (*untuk menambah server IMAP, klik tombol kanan mouse di atas item IMAP pada menu navigasi kiri*). Untuk membuat server "AutoIMAP" secara otomatis, bidang ini dinonaktifkan
- **Tipe login** - menetapkan metode untuk menentukan server email yang digunakan bagi email keluar:
 - o **Otomatis** - login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda
 - o **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:
 - o **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.
 - o **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

9.13. Perisai Tetap

Komponen Perisai Tetap melakukan perlindungan langsung atas file dan folder terhadap virus, spyware dan malware lainnya.



Dalam dialog **Pengaturan Perisai Tetap** , Anda dapat mengaktifkan atau menonaktifkan



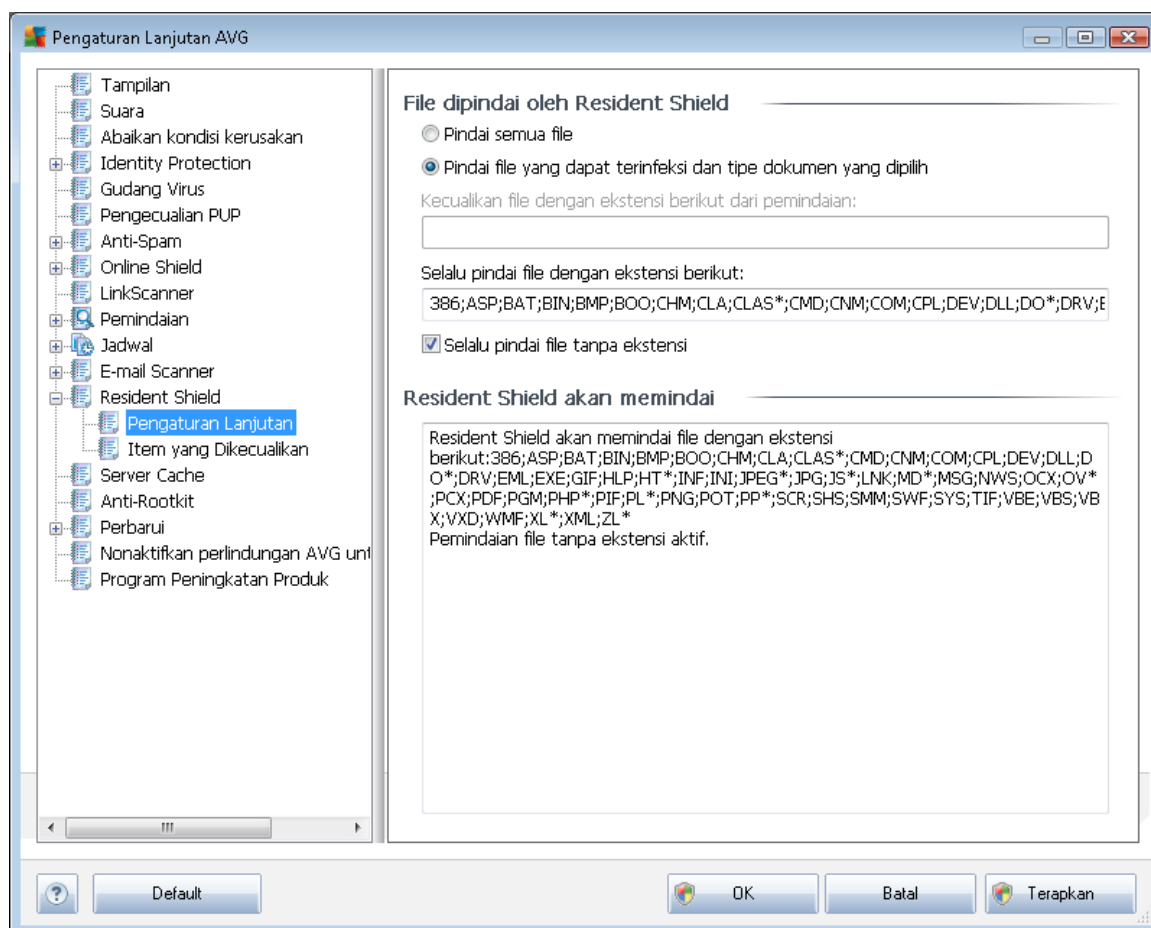
sepenuhnya perlindungan [Perisai Tetap](#) dengan mencentang /tidak mencentang item **Aktifkan Perisai Tetap** (opsi ini telah diaktifkan secara default). Selain itu, Anda dapat memilih fitur [Perisai Tetap](#) yang harus diaktifkan:

- **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): centang 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 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)
- **Hapus semua ancaman secara otomatis** (dinonaktifkan secara default) - setiap infeksi yang terdeteksi akan dipulihkan secara otomatis jika tersedia penawarnya, dan semua infeksi yang tidak dapat dipulihkan akan dihapus.
- **Pindai file yang dirujuk di register** (diaktifkan secara default) - parameter ini menentukan AVG akan memindai semua file yang dapat dijalankan yang ditambahkan ke register startup untuk menghindari infeksi yang dikenal dijalankan saat komputer dinyalakan berikutnya.
- **Aktifkan pemindaian menyeluruh** (dinonaktifkan secara default) - dalam kondisi tertentu (dalam keadaan sangat darurat) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma yang paling menyeluruh yang akan memeriksa semua objek yang mungkin mengancam secara mendalam. Tetapi harap diingat bahwa metode ini memakan waktu lama.



9.13.1. Pengaturan Lanjutan

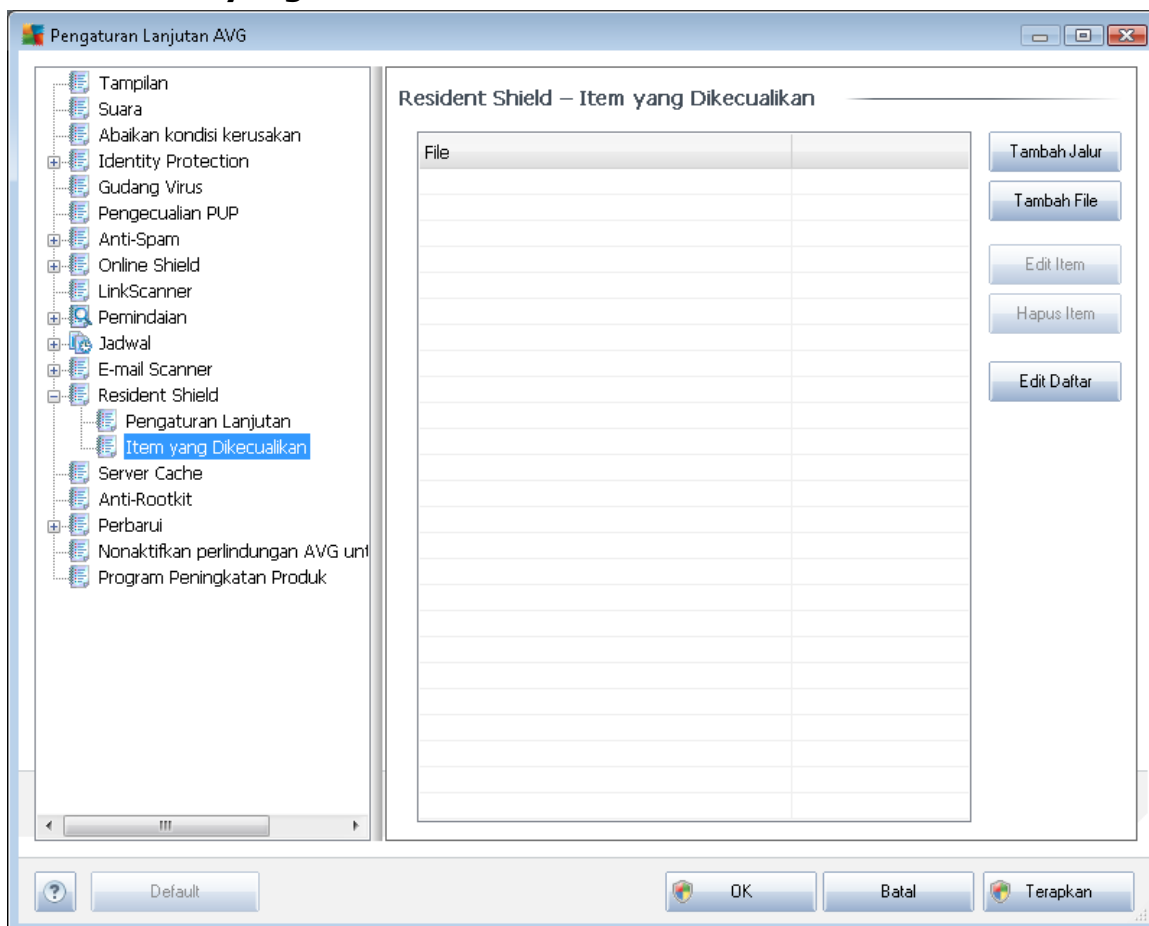
Dalam dialog **File dipindai oleh Perisai Tetap** Anda dapat mengonfigurasi file yang akan dipindai (menurut ekstensi tertentu):



Putuskan apakah Anda ingin agar semua file dipindai atau cuma file terinfeksi - jika demikian, Anda dapat menetapkan lebih lanjut suatu daftar ekstensi file yang menentukan file apa saja yang akan dikecualikan dari pemindaian, juga daftar ekstensi file yang harus dipindai pada semua keadaan.

Bagian di bawah ini yang disebut **Perisai Tetap akan memindai** selanjutnya meringkas pengaturan yang aktif, menampilkan gambaran umum terperinci tentang apa yang akan dipindai oleh [Perisai Tetap](#).

9.13.2. Item yang dikecualikan



Dialog **Perisai Tetap - Item yang Dikecualikan** menyediakan kemungkinan untuk menentukan file dan/atau folder yang harus dikecualikan dari pemindaian [Perisai Tetap](#).

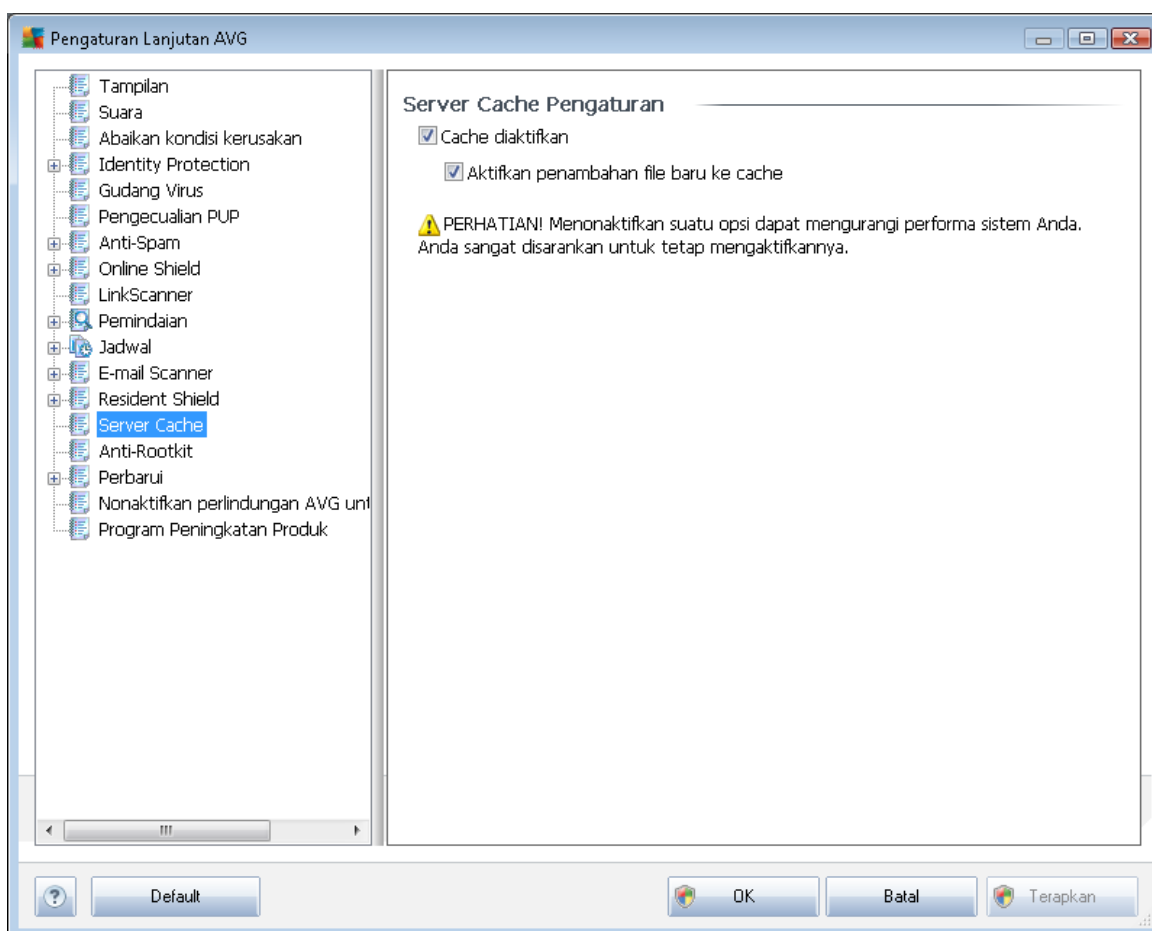
Jika hal ini tidak penting, kami sangat menyarankan untuk tidak mengecualikan file apa pun!

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

9.14. Server Cache

Server Cache adalah proses yang dirancang untuk mempercepat pemindaian (*pemindaian saat dibutuhkan, pemindaian terjadwal seisi komputer, pemindaian [Perisai Tetap](#)*). Ia mengumpulkan dan menyimpan informasi atas file terpercaya (*file sistem yang berisi tanda tangan digital, dsb.*): Semua file ini dianggap aman, dan selama pemindaian akan dilewati.

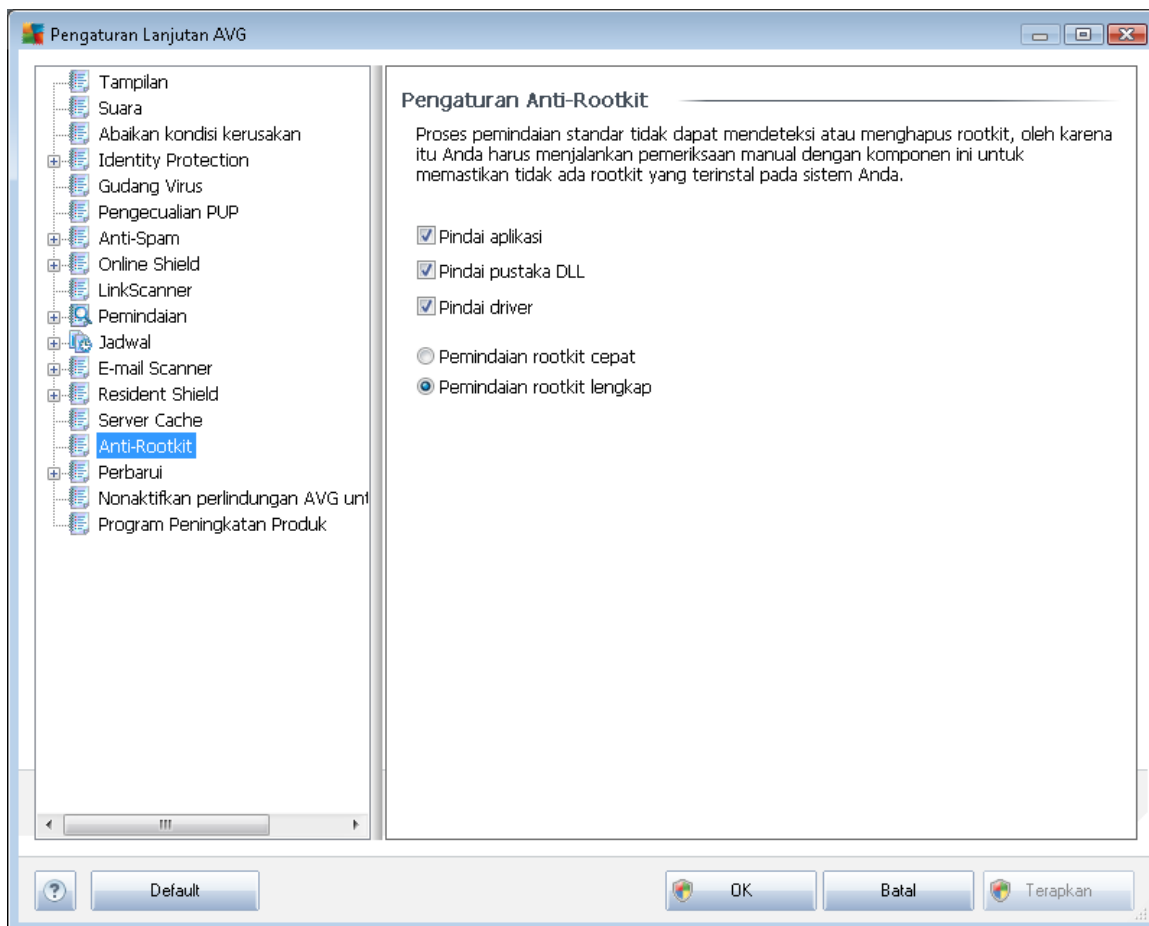


Dialog pengaturan menawarkan dua opsi:

- **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.

9.15. Anti-Rootkit

Dalam dialog ini, Anda dapat mengedit konfigurasi komponen [Anti-Rootkit](#):



Pengeditan semua fungsi komponen [Anti-Rootkit](#) yang diberikan dalam dialog ini juga dapat diakses langsung dari [antarmuka komponen Anti-Rootkit](#).

Centang kotaknya untuk menentukan objek yang harus dipindai:

- ***Pindai aplikasi***
- ***Pindai pustaka DLL***
- ***Pindai driver***

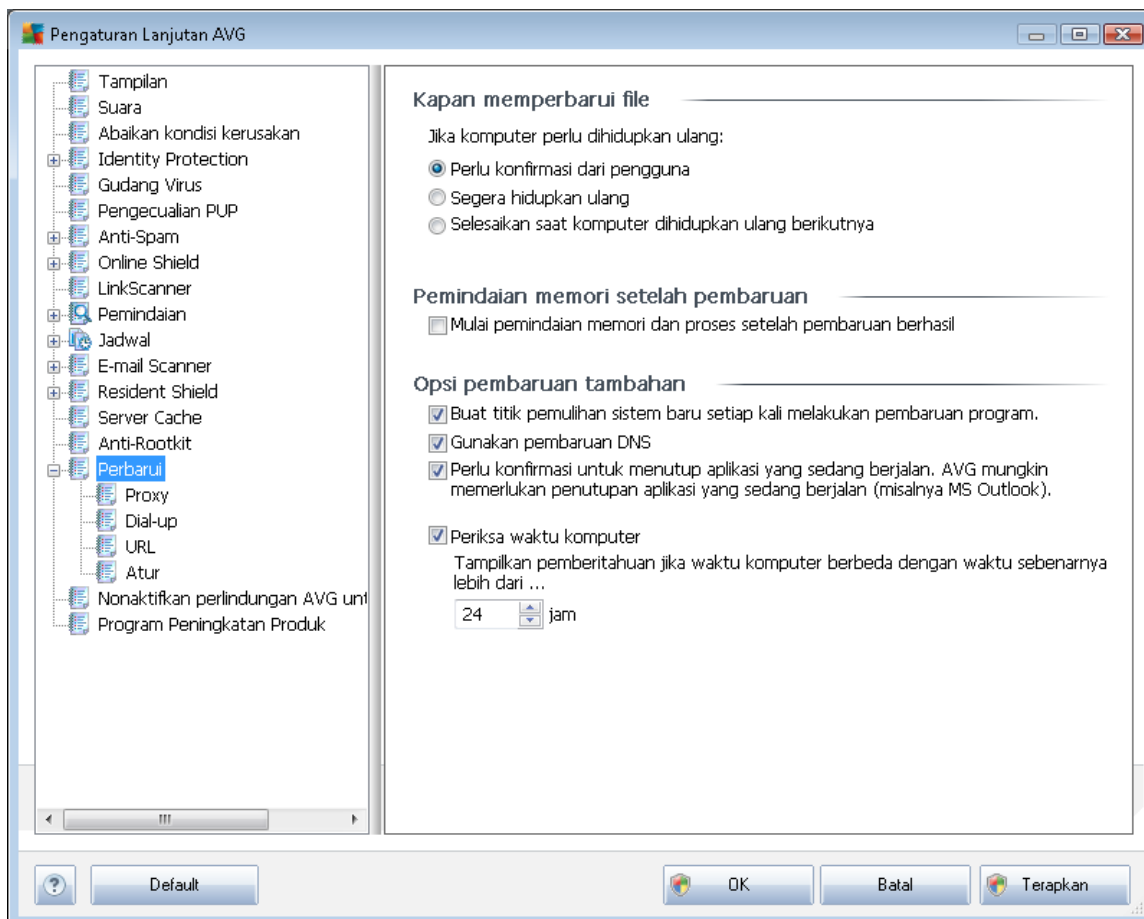
Selanjutnya Anda dapat memilih mode pemindaian rootkit:

- ***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 floppy-disk/drive CD*)

9.16. 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 untuk 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!

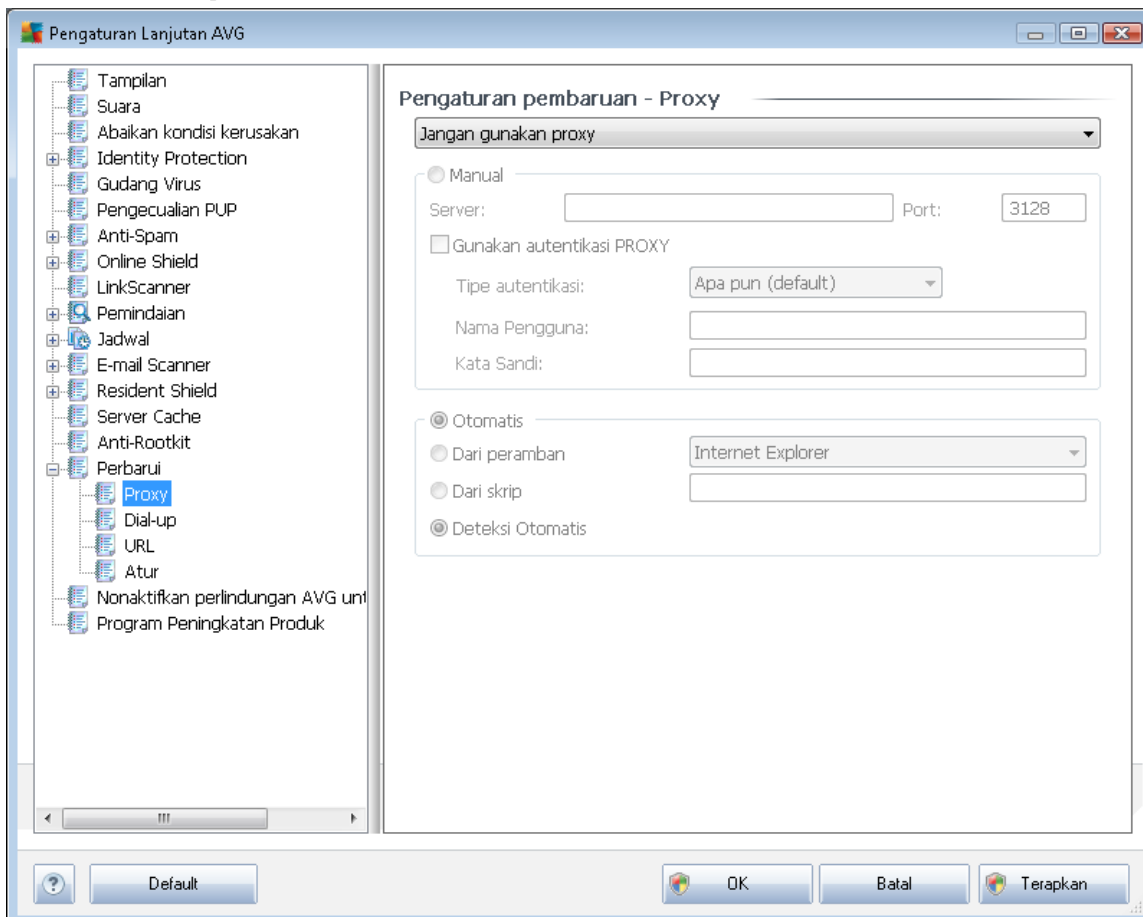
Pemindaian memori setelah pembaruan

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 Internet AVG 2011** 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.

9.16.1. 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 server 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*)

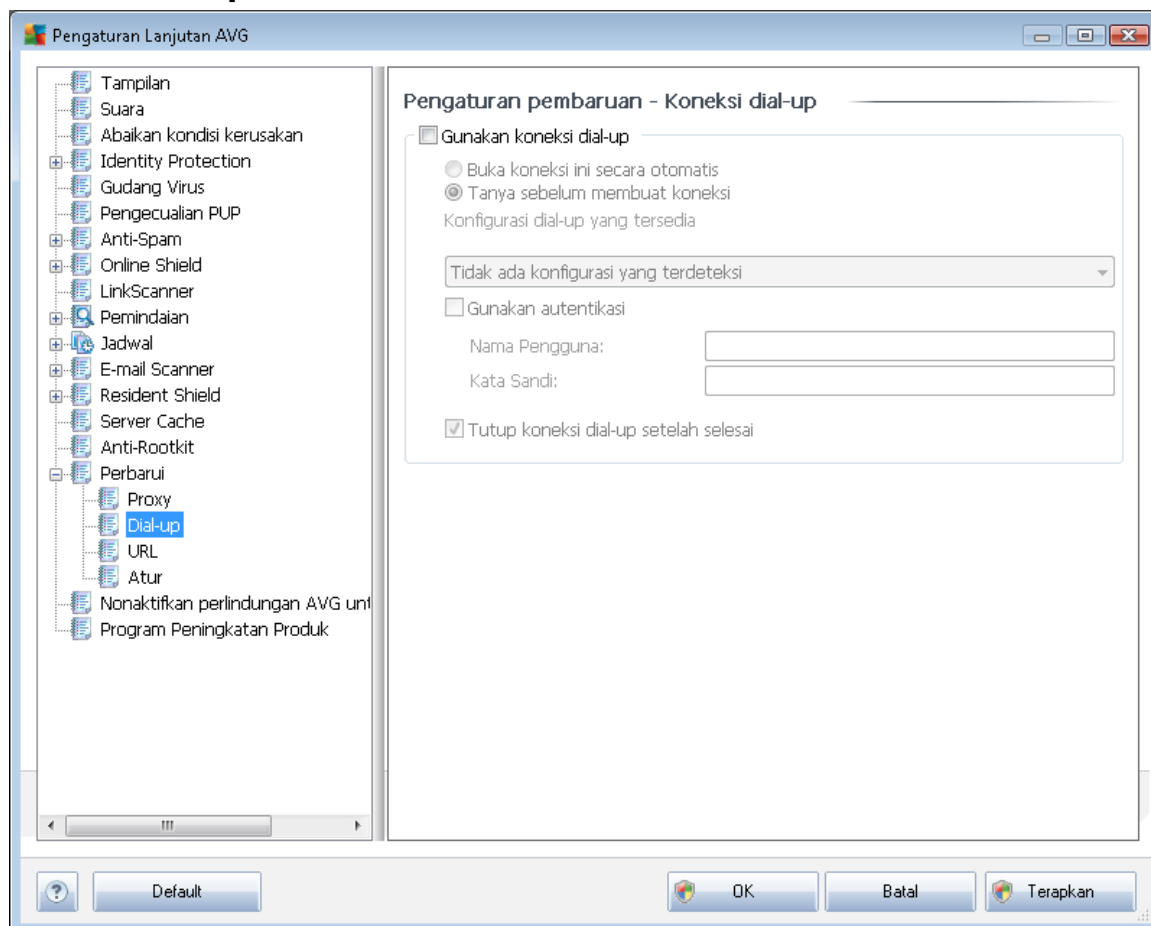
Server proxy juga dapat dikonfigurasi dengan aturan tertentu untuk setiap pengguna. Jika server proxy Anda telah diatur dengan cara ini, tandai opsi **Gunakan autentikasi PROXY** untuk memverifikasi bahwa nama pengguna dan kata sandi Anda sudah sah untuk menghubungkan ke Internet melalui server proxy.

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

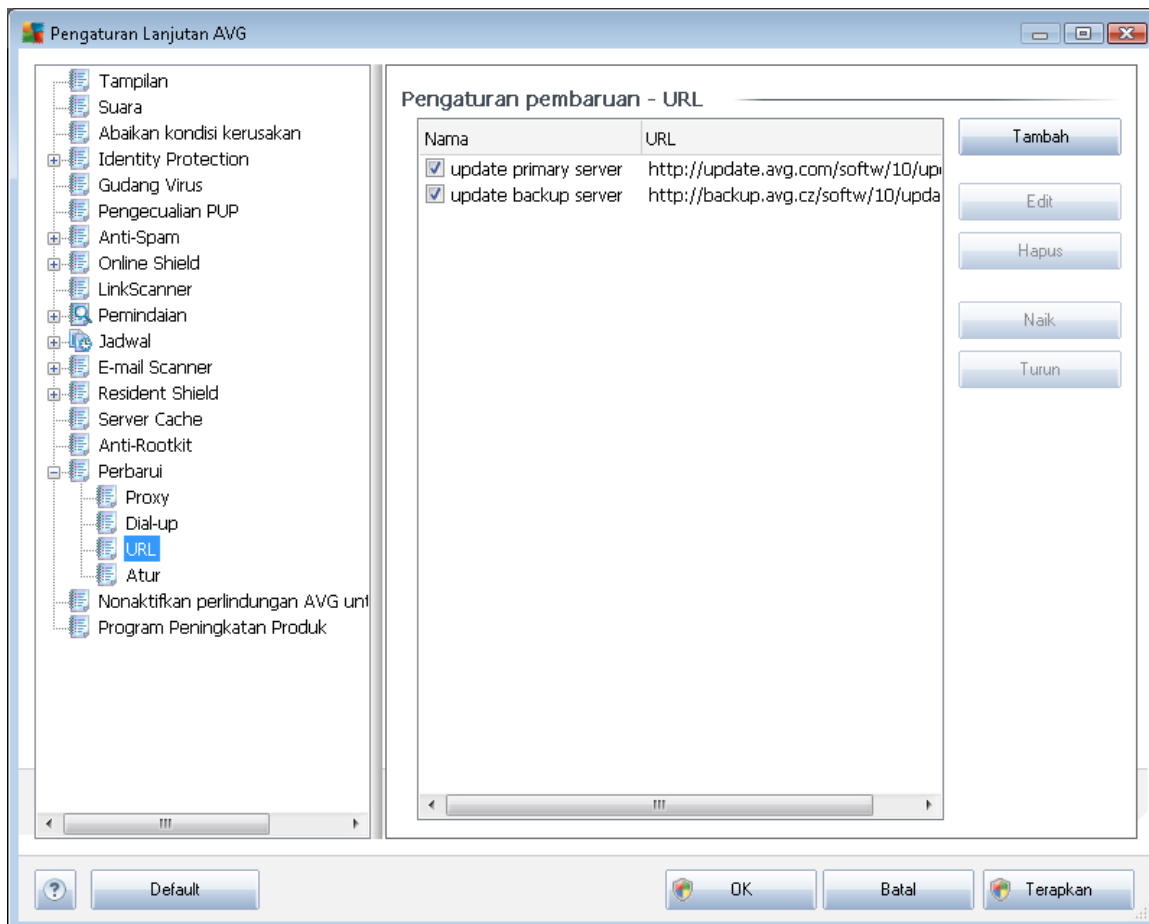
9.16.2. Dial-up



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**).

9.16.3. URL

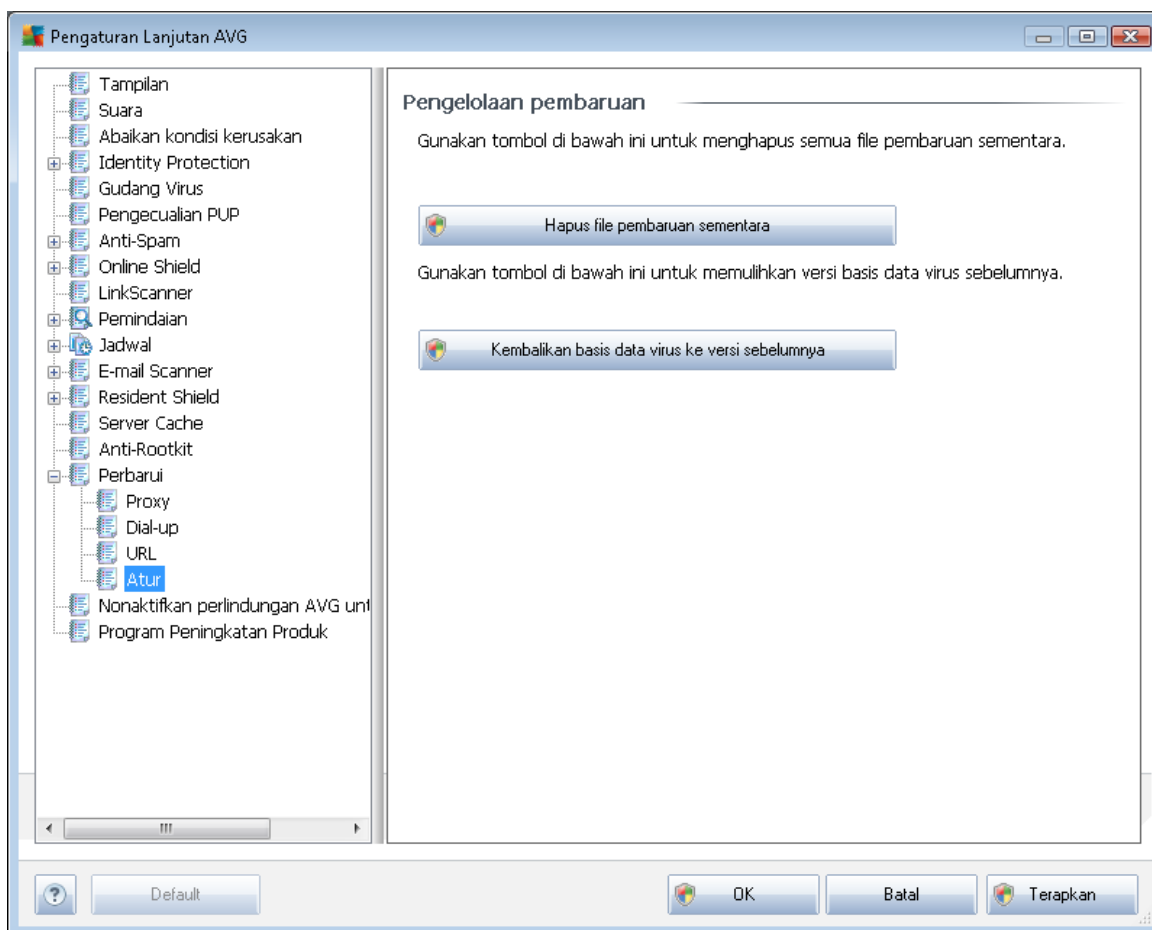


Dialog **URL** menyediakan daftar alamat Internet dari mana Anda dapat mengunduh file pembaruan. Daftar ini dan itemnya dapat diubah dengan menggunakan tombol kontrol berikut:

- **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

9.16.4. Atur

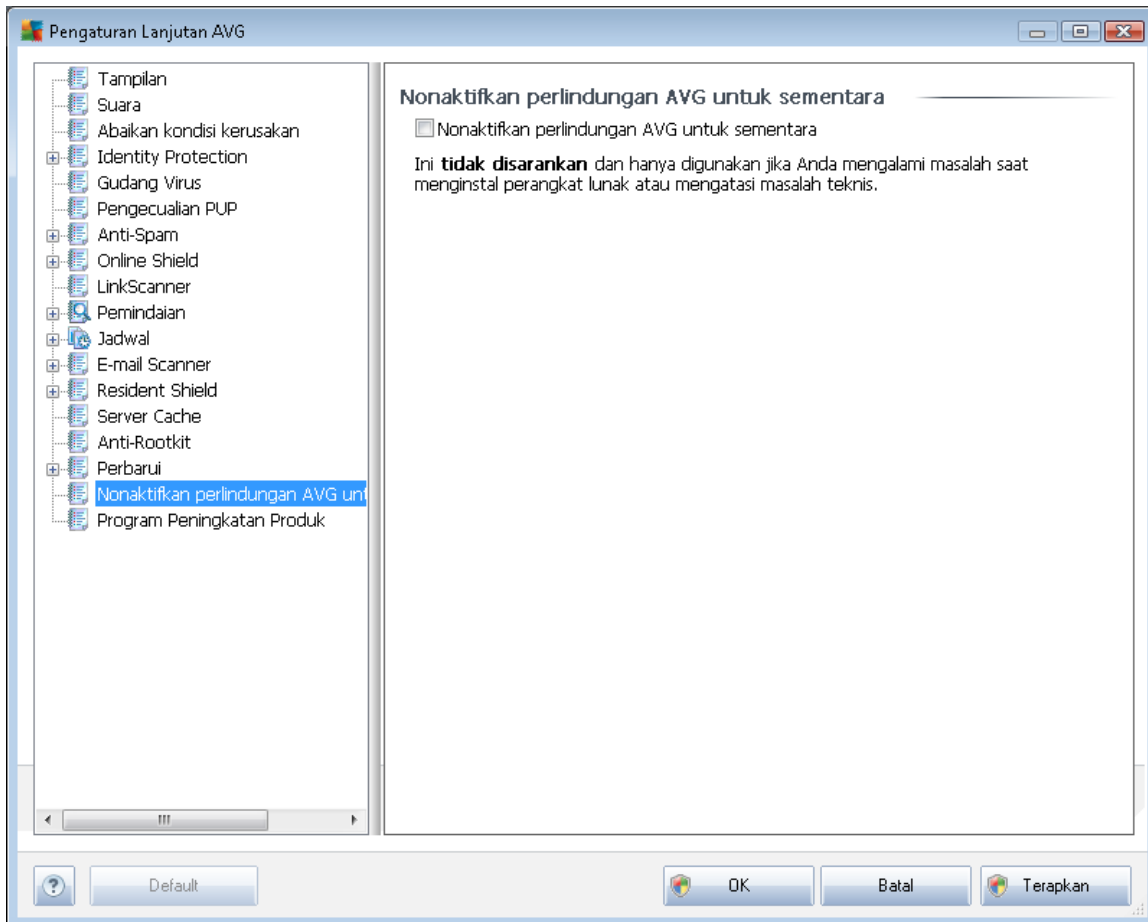
Dialog **Atur** menyediakan dua opsi yang dapat diakses melalui dua tombol:



- **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*)



9.17. Menonaktifkan perlindungan AVG untuk sementara



Dalam dialog **Nonaktifkan perlindungan AVG untuk sementara** Anda mempunyai opsi untuk menonaktifkan seluruh perlindungan yang diberikan oleh **Keamanan Internet AVG 2011** sekaligus.

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

Dalam kebanyakan kondisi, tidak diperlukan untuk menonaktifkan AVG sebelum menginstal perangkat lunak atau 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 ternyata mengalami masalah selama instalasi, coba nonaktifkan komponen **Perisai Tetap** terlebih dahulu. Jika Anda harus menonaktifkan AVG untuk sementara, Anda harus segera mengaktifkannya setelah Anda selesai. Jika Anda terhubung dengan Internet atau jaringan selama perangkat lunak antivirus Anda dinonaktifkan, komputer Anda rentan terhadap serangan.

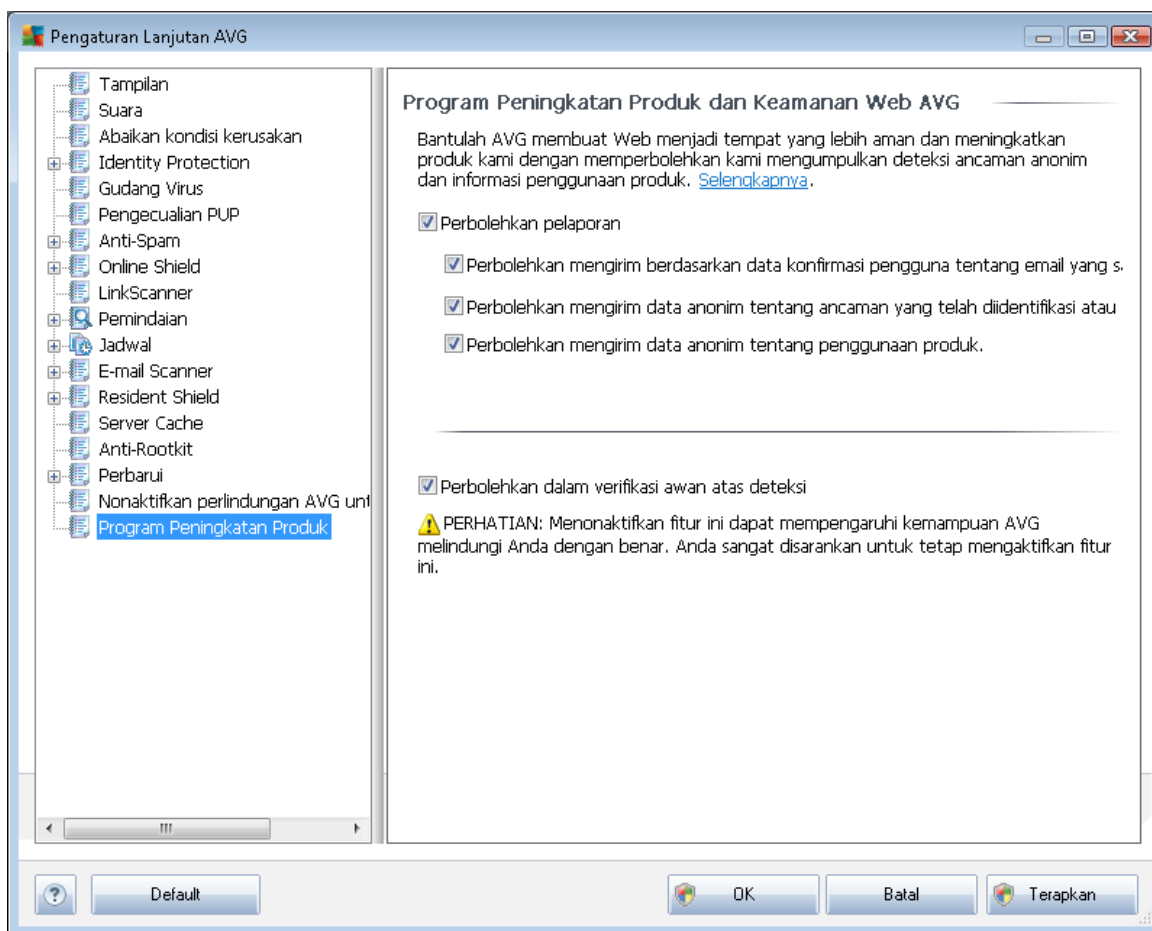
9.18. Program Peningkatan Produk

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. Tandai opsi **Izinkan pelaporan** untuk memungkinkan pelaporan



ancaman yang terdeteksi kepada 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, dan tidak ada data pribadi yang disertakan dalam laporan tersebut. Pelaporan ancaman yang terdeteksi adalah opsional, namun, kami mengharapkan Anda juga mengaktifkan fitur ini, karena dapat membantu kami menyempurnakan perlindungan bagi Anda dan pengguna AVG lainnya.



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/perusak yang menyalin dan menyebarkan diri, sering tanpa diketahui sampai kerusakan telah terjadi. 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 kerusakan.



- **Worm** adalah subkategori virus yang, tidak seperti virus normal, tidak memerlukan objek "pembawa" untuk ditemplei; 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, AVG dilengkapi dengan komponen khusus berikut:

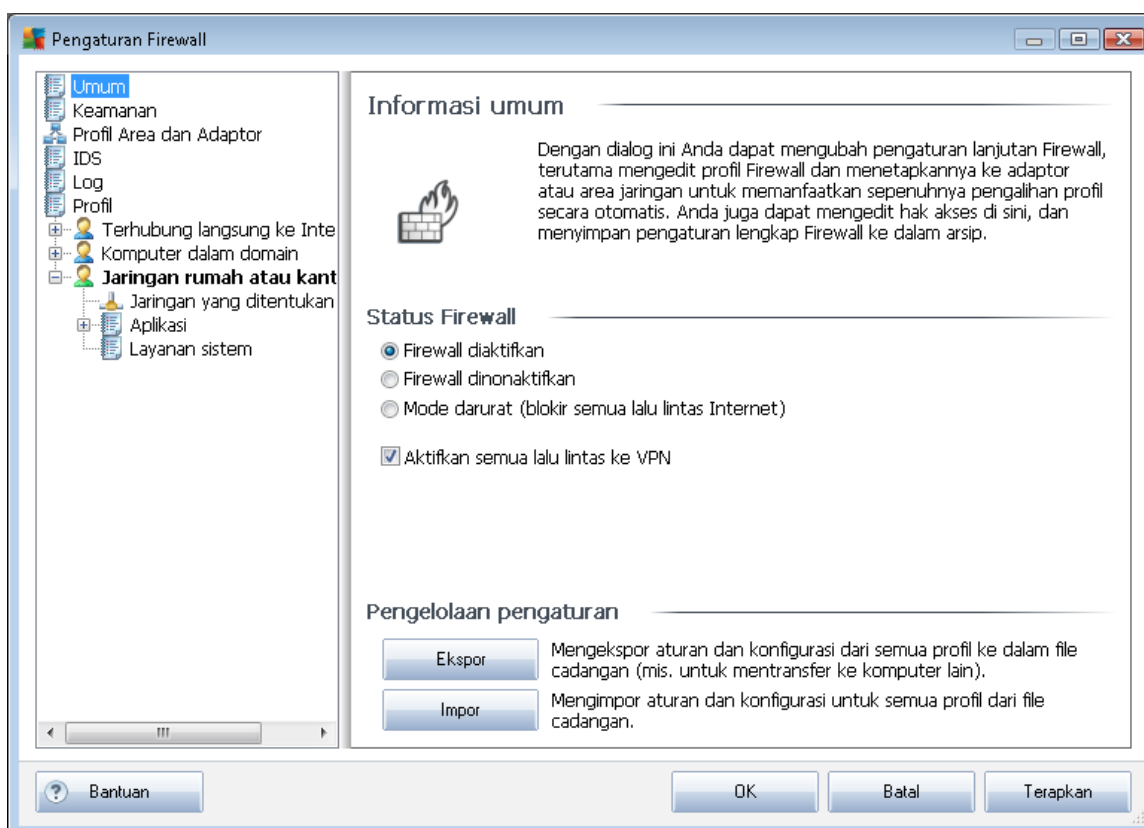
- **[Anti-Virus](#)** untuk melindungi komputer Anda dari virus,
- **[Anti-Spyware](#)** untuk melindungi komputer Anda dari spyware,
- **[Online Shield](#)** untuk melindungi Anda dari virus dan spyware saat meramban Internet,
- **[LinkScanner](#)** untuk melindungi Anda dari ancaman online lainnya yang diuraikan dalam bab ini.

10. 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, pengeditan konfigurasi lanjutan hanya ditujukan bagi para pengguna berpengalaman dan ahli.***

10.1. 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

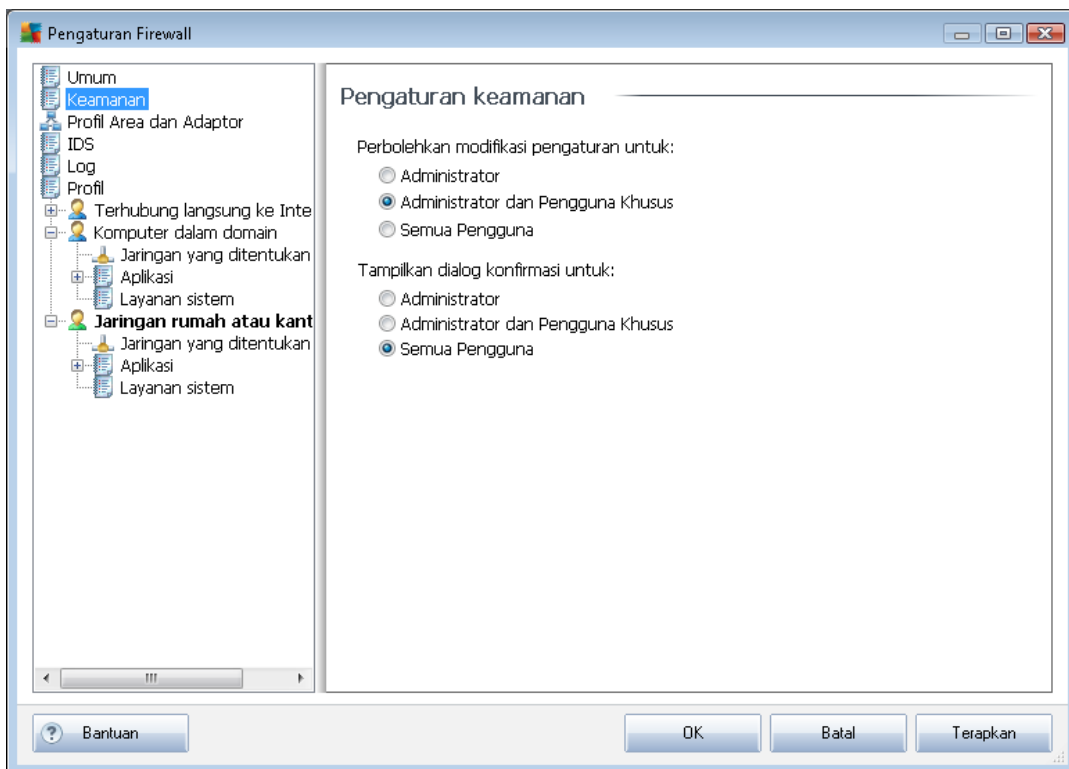
- **Aktifkan semua lalu lintas ke VPN** – jika Anda menggunakan koneksi VPN (*Virtual Private Network*), misalnya untuk menghubungkan ke kantor dari rumah, kami sarankan menandai kotak ini. **AVG Firewall** secara otomatis akan mencari ke seluruh adapter jaringan Anda, menemukan adapter yang digunakan 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

Dalam bagian **Manajemen pengaturan**, Anda dapat melakukan **Ekspor/Impor** konfigurasi **Firewall**; misalnya mengekspor aturan dan pengaturan **Firewall** yang telah ditentukan ke file cadangan, atau dengan kata lain mengimpor seluruh file cadangan.

10.2. Keamanan



Dalam dialog **Pengaturan keamanan** Anda dapat menentukan aturan umum cara kerja **Firewall**, apa pun profil yang dipilih:



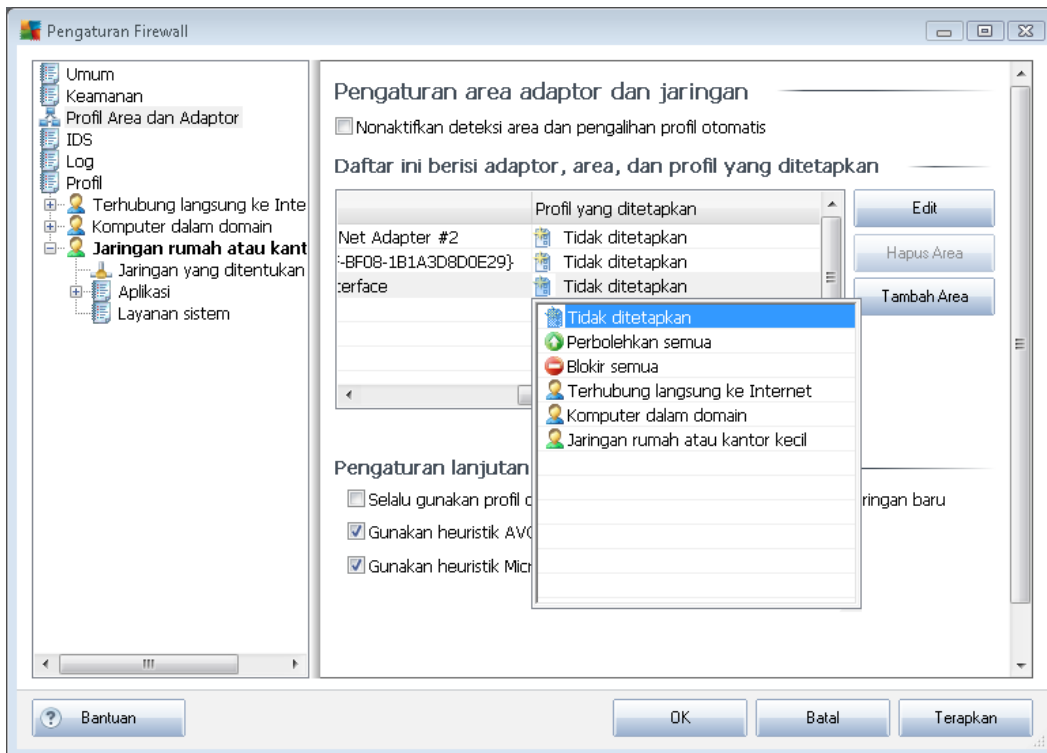
- **Izinkan modifikasi pengaturan pada** - menetapkan siapa yang diperbolehkan mengubah konfigurasi [Firewall](#)
- **Tampilkan dialog konfirmasi untuk** - menetapkan kepada siapa dialog konfirmasi (*dialog yang menanyakan keputusan dalam situasi yang tidak tercakup oleh aturan [Firewall](#) yang telah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

Pada 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

10.3. Profil Area dan Adaptor

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





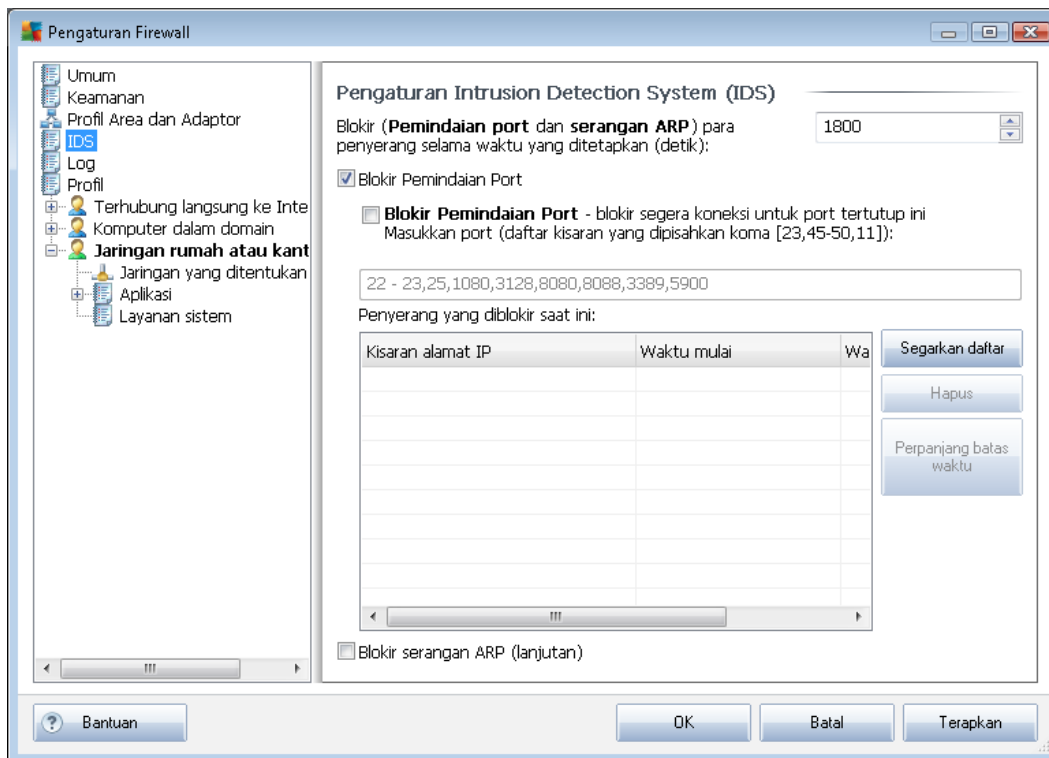
- **Nonaktifkan deteksi area dan alih profil otomatis** - salah satu profil yang ditentukan dapat diberikan ke setiap tipe antarmuka jaringan, sesuai masing-masing area. Jika Anda tidak ingin menentukan profil tertentu, akan digunakan satu profil umum. Walau demikian, jika Anda memutuskan untuk membedakan berbagai profil dan menetapkan 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**.
- **Daftar adapter, area dan profil yang ditetapkan** - dalam daftar ini Anda dapat menemukan gambaran 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 item yang bersangkutan dalam daftar adapter dan pilih profilnya.

Pengaturan lanjutan

- o **Selalu gunakan profil default dan jangan menampilkan dialog deteksi jaringan yang baru** – setiap kali komputer Anda terhubung ke jaringan baru, [Firewall](#) akan mengingatkan Anda dan menampilkan dialog yang meminta Anda memilih tipe koneksi jaringan, dan menentukan [profil Firewall](#). Jika Anda tidak ingin dialog tersebut ditampilkan, centang kotak ini.
- o **Gunakan heuristik AVG untuk deteksi jaringan baru** - memungkinkan pengumpulan informasi tentang jaringan yang baru terdeteksi dengan mekanisme AVG sendiri (*walaupun demikian, opsi ini hanya tersedia pada OS VISTA, dan yang lebih tinggi*).
- o **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*).

10.4. IDS

Intrusion Detection System adalah fitur analisis perilaku khusus yang dirancang untuk mengidentifikasi dan memblokir upaya komunikasi mencurigakan yang mencoba menggunakan port tertentu pada komputer Anda. Anda dapat mengonfigurasi parameter IDS dalam antarmuka berikut:



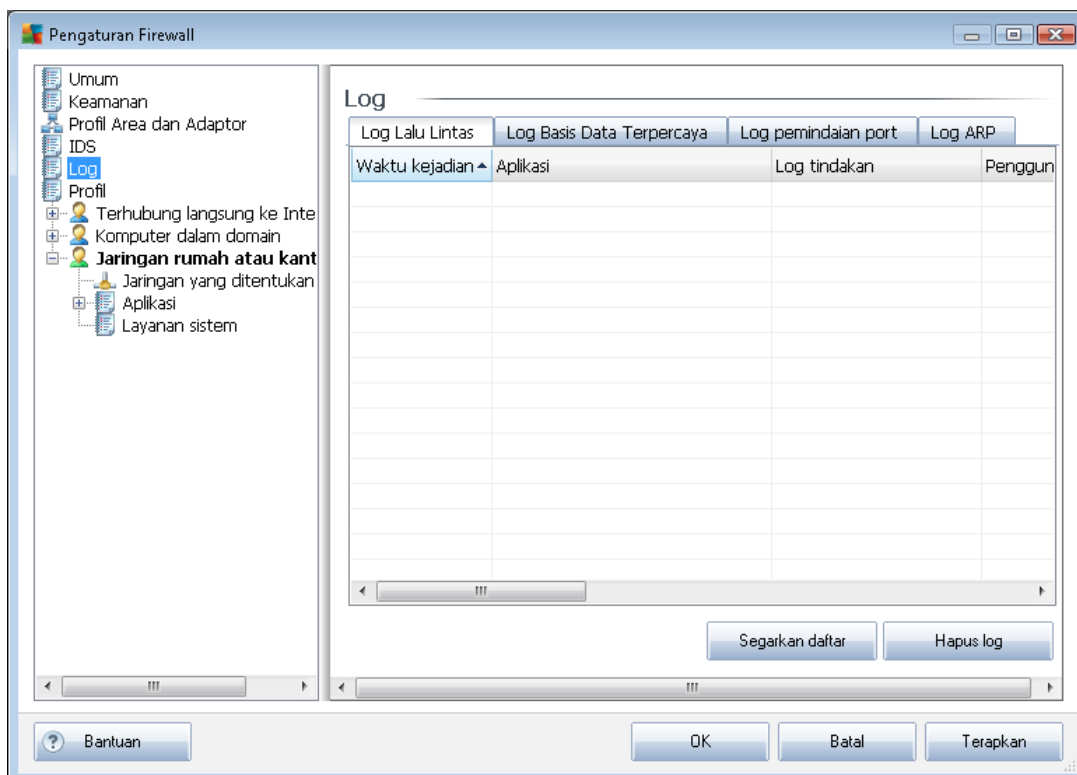
Dialog pengaturan **Intrusion Detection System (IDS)** menawarkan opsi konfigurasi berikut:

- **Blokir penyerang selama waktu yang ditetapkan** - memungkinkan Anda mengatur berapa detik suatu port akan diblokir, setiap kali upaya komunikasi mencurigakan terdeteksi pada port tersebut. Secara default, interval waktu ditentukan pada 1800 detik (30 menit).
- **Blokir Pemindaian Port** – centang kotak 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.
 - o **Blokir Pemindaian Port** – centang kotak 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.
 - o **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** mengaktifkan pemblokiran 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.

10.5. 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.

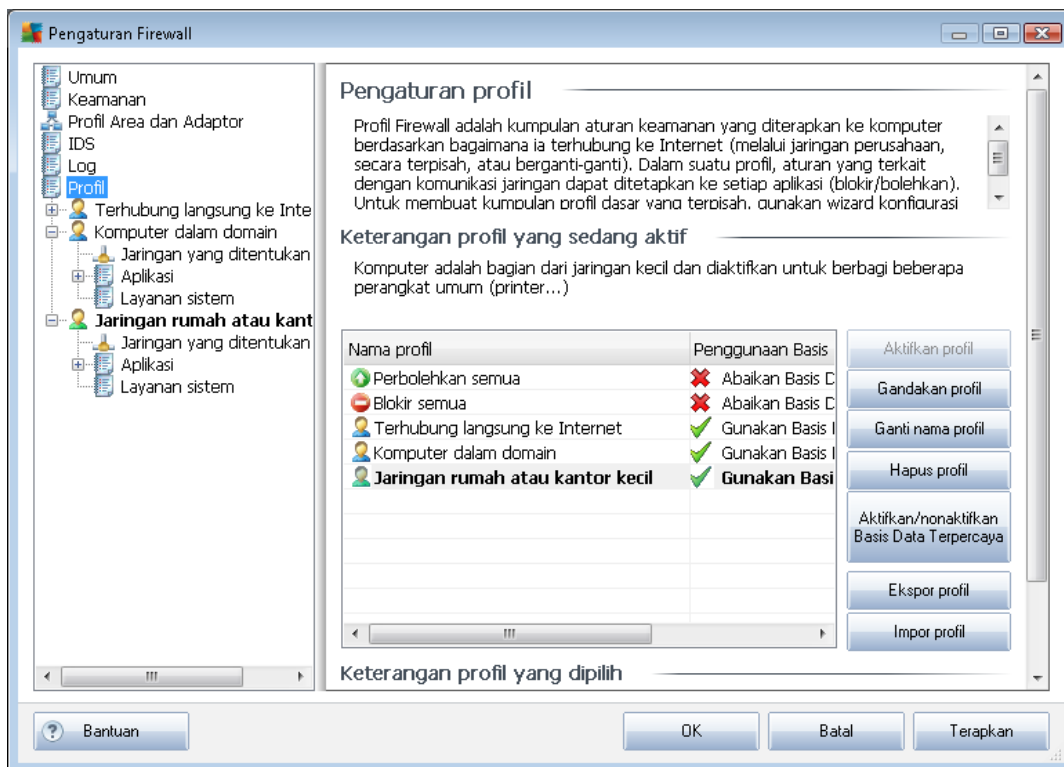
- **Log pemindaian port** - merekam semua aktivitas [Intrusion Detection System \(Sistem Deteksi Pengganggu\)](#) .
- **Log ARP** - merekam info mengenai pemblokiran upaya komunikasi khusus di dalam jaringan lokal ([opsi Blokir serangan ARP](#)) yang terdeteksi oleh [Intrusion Detection System](#) sebagai 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.
- **Kosongkan daftar** - menghapus semua entri dalam diagram.

10.6. Profil

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



Semua selain [profil](#) sistem dapat diedit dalam dialog ini dengan 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** - mengonfigurasi pengaturan profil yang dipilih berdasarkan data yang diekspor dari file konfigurasi

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

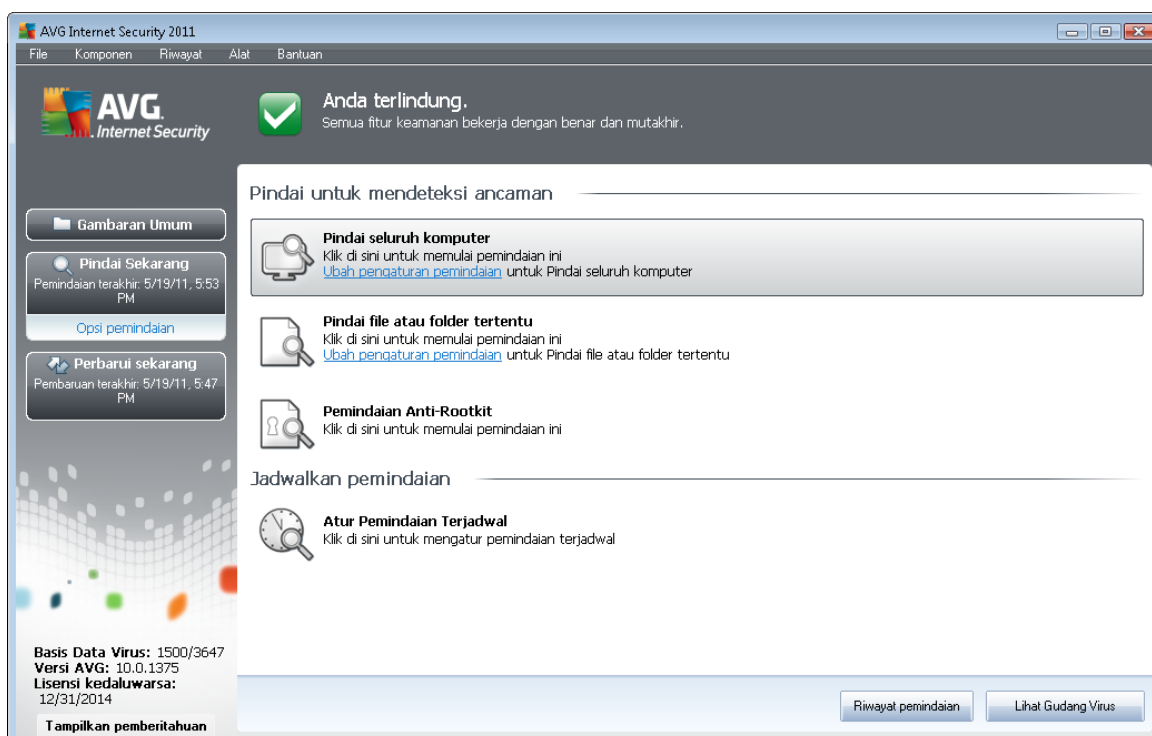
Berdasarkan jumlah profil yang ditentukan, yang telah disebutkan dalam daftar di dalam dialog **Profil**, struktur menu navigasi kiri akan turut berubah. Setiap profil yang telah ditentukan akan membuat cabang tertentu di bawah item **Profil**. Beberapa profil tertentu nanti dapat diedit dalam dialog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



11. Pemindaian AVG

Pemindaian merupakan bagian penting pada fungsionalitas **Keamanan Internet AVG 2011**. Anda dapat menjalankan tes sesuai keperluan atau [menjadwalkannya untuk dijalankan secara berkala](#) pada waktu yang diinginkan.

11.1. 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:
 - o [Pemindaian seluruh komputer](#)
 - o [Pindai file atau folder tertentu](#)
 - o [Pemindaian Anti-Rootkit](#)
- [bagian jadwal 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 infeksi yang terdeteksi dikarantina

11.2. Pemindaian Yang Ditetapkan

Salah satu fitur utama **Keamanan Internet AVG 2011** 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.

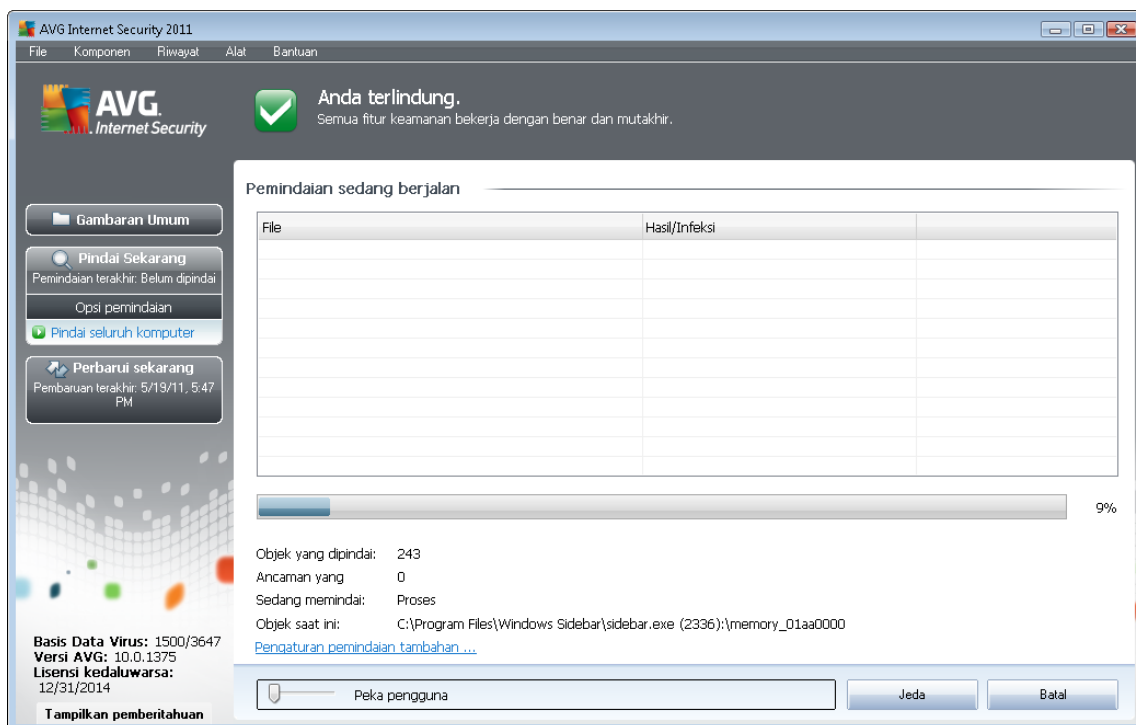
Dalam **Keamanan Internet AVG 2011** Anda akan menemukan tipe pemindaian yang sudah ditetapkan oleh vendor perangkat lunak:

11.2.1. 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.

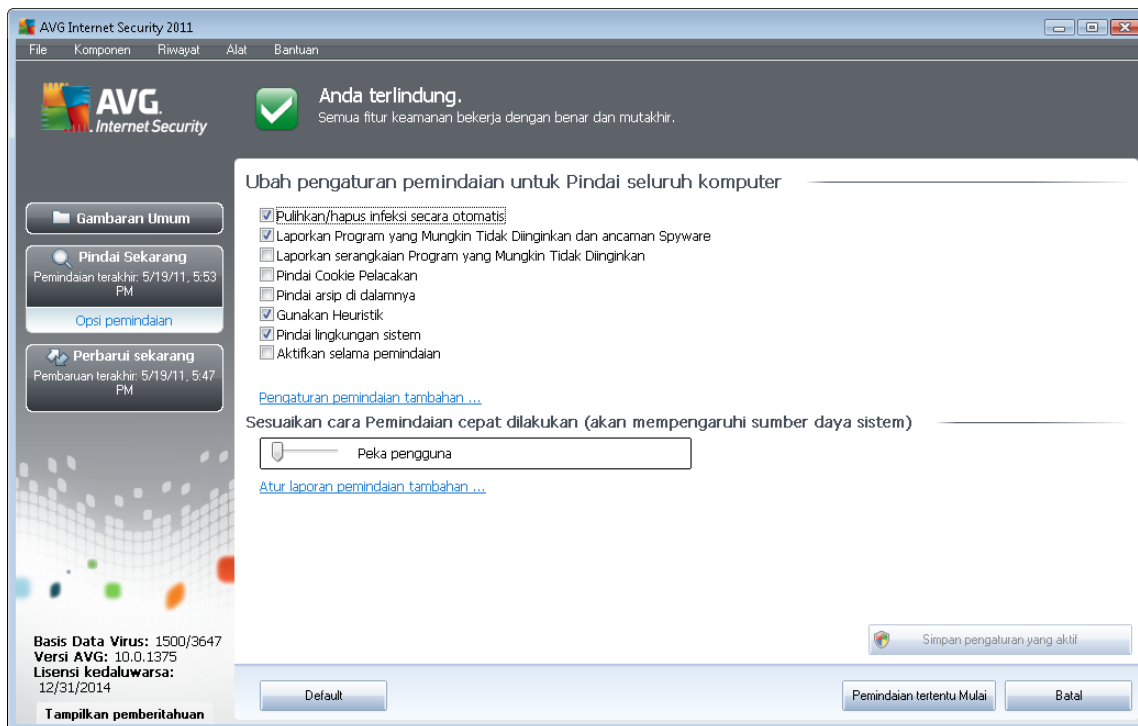
Peluncuran pemindaian

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.



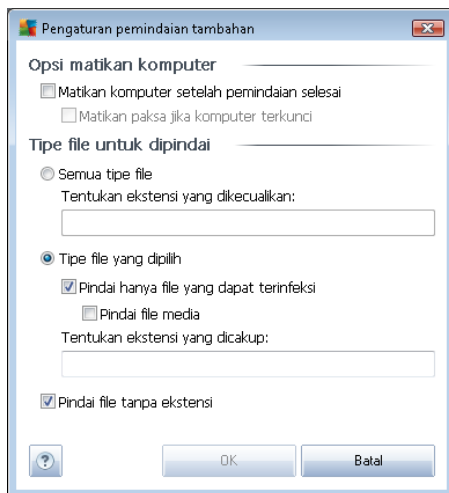
Mengedit konfigurasi pemindaian

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:
 - o **Pulihkan/hapus infeksi secara otomatis** - (*diaktifkan secara default*): jika ada virus teridentifikasi selama pemindaian, ia dapat dipulihkan otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke [Gudang Virus](#).
 - o **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.
 - o **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.
 - o **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*).

- o **Pindai di dalam arsip** (*dinonaktifkan secara default*) - parameter ini menetapkan bahwa pemindaian harus memeriksa semua file yang tersimpan dalam arsip, misalnya, ZIP, RAR, ...
- o **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.
- o **Pindai lingkungan sistem** (*diaktifkan secara default*) - pemindaian juga akan memeriksa area sistem komputer Anda.
- o **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:

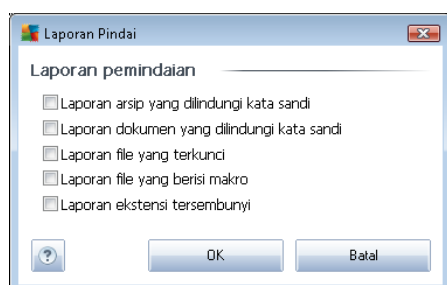


- o **Opsi matikan komputer** - memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini (**Matikan komputer setelah pemindaian selesai**), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun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

- **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.

11.2.2. Pindai File atau Folder Tertentu

Pindai file atau folder tertentu - hanya memindai area komputer Anda yang telah dipilih untuk dipindai (*folder, hard disk, disket 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 tertentu dapat digunakan untuk mengatur tes Anda sendiri dan menjadwalkannya berdasarkan kebutuhan.

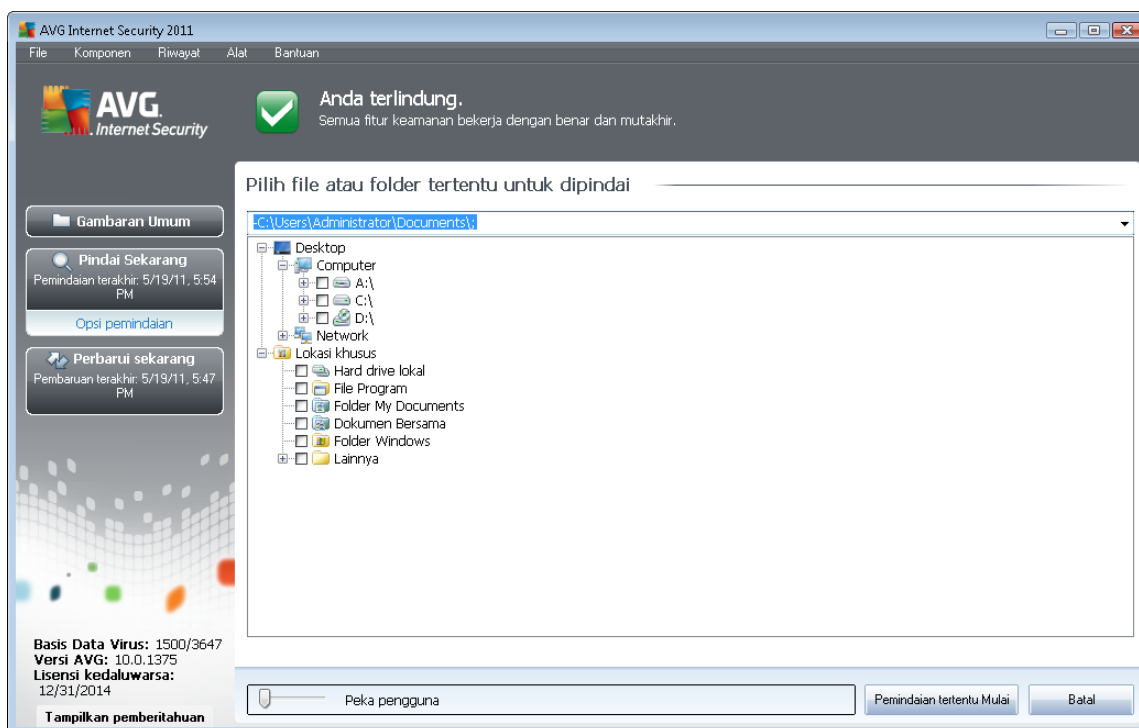
Peluncuran pemindaian



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.

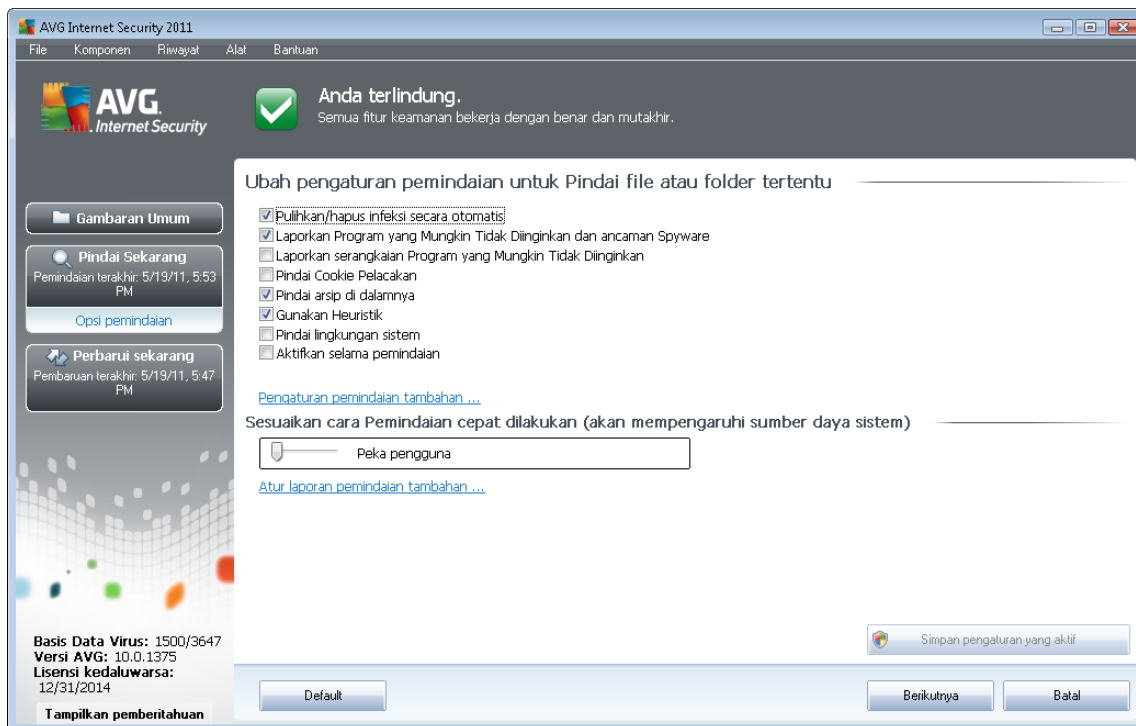
Juga ada kemungkinan untuk memindai folder tertentu sementara semua subfoldernya dikecualikan dari pemindaian ini; untuk melakukannya ketikkan tanda kurang "-" di depan jalur yang telah dibuat secara otomatis (*lihat cuplikan layar*). Untuk mengecualikan seluruh folder dari pemindaian, gunakan tanda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

Terakhir, untuk meluncurkan pemindaian, tekan tombol **Mulai pindai** ; proses pemindaian sendiri pada dasarnya sama dengan [Pemindaian seisi komputer](#).



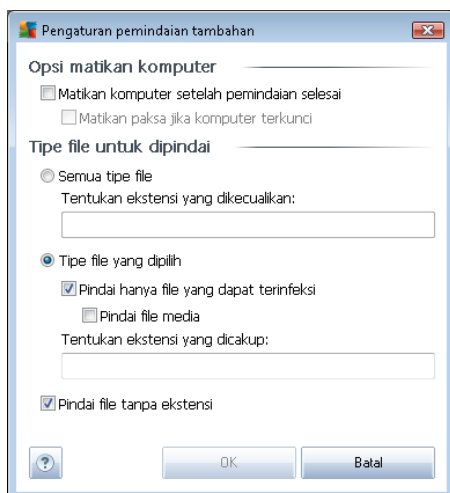
Mengedit konfigurasi pindai

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:
 - o **Pulihkan/hapus infeksi secara otomatis** - (*diaktifkan secara default*): jika ada virus teridentifikasi selama pemindaian, ia dapat dipulihkan otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke [Gudang Virus](#).
 - o **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.
 - o **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.
 - o **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*).

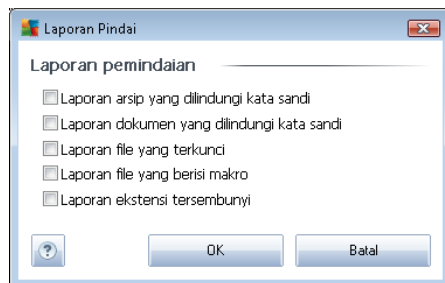
- o **Pindai di dalam arsip** (*diaktifkan secara default*) - parameter ini menetapkan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut tersimpan dalam arsip, misalnya, ZIP, RAR, ...
- o **Gunakan Heuristik** (*dinonaktifkan secara default*) - analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- o **Pindai lingkungan sistem** (*dinonaktifkan secara default*) - pemindaian juga akan memeriksa area sistem komputer Anda.
- o **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:



- o **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**).
- o **Tentukan 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 tertentu 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](#)).

11.2.3. Pemindaian Anti-Rootkit

Pemindaian Anti-Rootkit mencari kemungkinan rootkit di komputer (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.

Peluncuran pemindaian

The screenshot shows the AVG Internet Security 2011 application window. At the top, there's a menu bar with "File", "Komponen", "Riwayat", "Alat", and "Bantuan". Below the menu, the AVG logo and "Internet Security" are visible. A yellow warning icon indicates that an "Anti-Rootkit" scan is running, advising to minimize computer usage during the process.

On the left sidebar, there are several buttons: "Gambaran Umum", "Pindai Sekarang" (with a timestamp of 5/19/11, 5:43 PM), "Opsi pemindaian", "Pemindaian Anti-Rootkit" (highlighted in green), "Perbarui sekarang" (with a timestamp of 5/19/11, 5:47 PM), and "Versi".

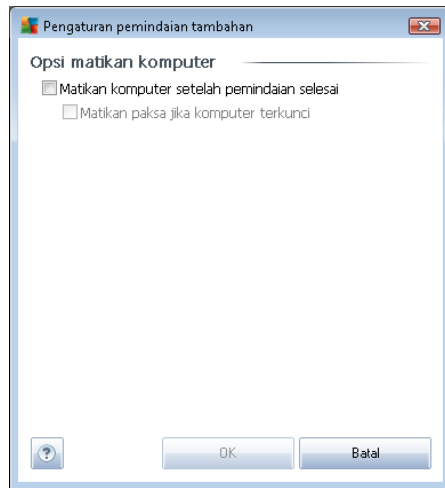
The main area displays the title "Pemindaian sedang berjalan" (Scan in progress). It contains a table with two columns: "File" and "Hasil/Infeksi". The table is currently empty. Below the table, a progress bar shows 11% completion. Further down, statistics are listed:

- Objek yang dipindai: 482
- Ancaman yang: 0
- Sedang memindai: Rootkit
- Objek saat ini: \Driver\HidUsb

At the bottom left, virus database information is shown: "Basis Data Virus: 1500/3647", "Versi AVG: 10.0.1375", and "Lisensi kedaluwarsa: 12/31/2014". A button labeled "Tampilkan pemberitahuan" is at the bottom left.

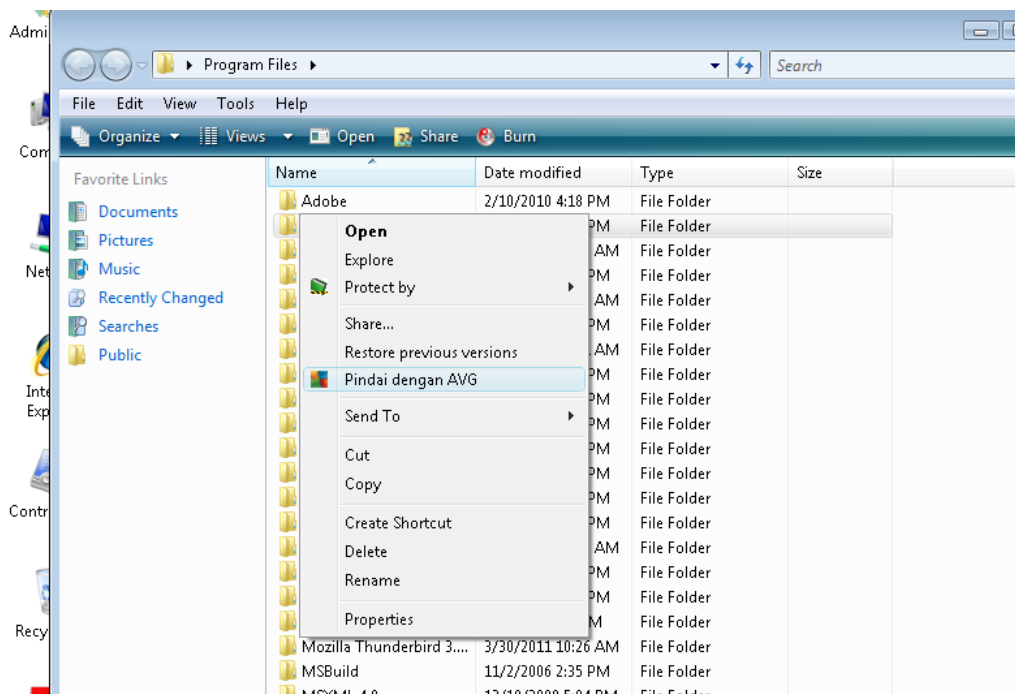
At the bottom right, there are three buttons: "Jeda" (Pause), "Batal" (Cancel), and a checkbox labeled "Peka pengguna" (User sensitive) which is currently unchecked.

Pemindaian Anti-Rootkit selalu diluncurkan di pengaturan default, dan mengedit parameter pemindaian hanya dapat diakses dalam dialog [Pengaturan Lanjutan AVG/Anti-Rootkit](#). Pada antarmuka pemindaian, konfigurasi berikut tersedia tetapi hanya ketika pemindaian sedang berjalan:



11.3. Memindai dalam Windows Explorer

Di samping pemindaian yang telah ditetapkan, yang diluncurkan untuk seisi komputer atau area yang dipilih, **Keamanan Internet AVG 2011** 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 AVG

11.4. Pemindaian Baris Perintah

Dalam **Keamanan Internet AVG 2011** 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 gambaran 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 [gambaran 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. Pemindaian 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.

11.4.1. 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
- **/MACROW** Laporkan makro
- **/PWDW** Laporkan file yang dilindungi kata sandi
- **/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](#)"
- **/REG** Pindai register



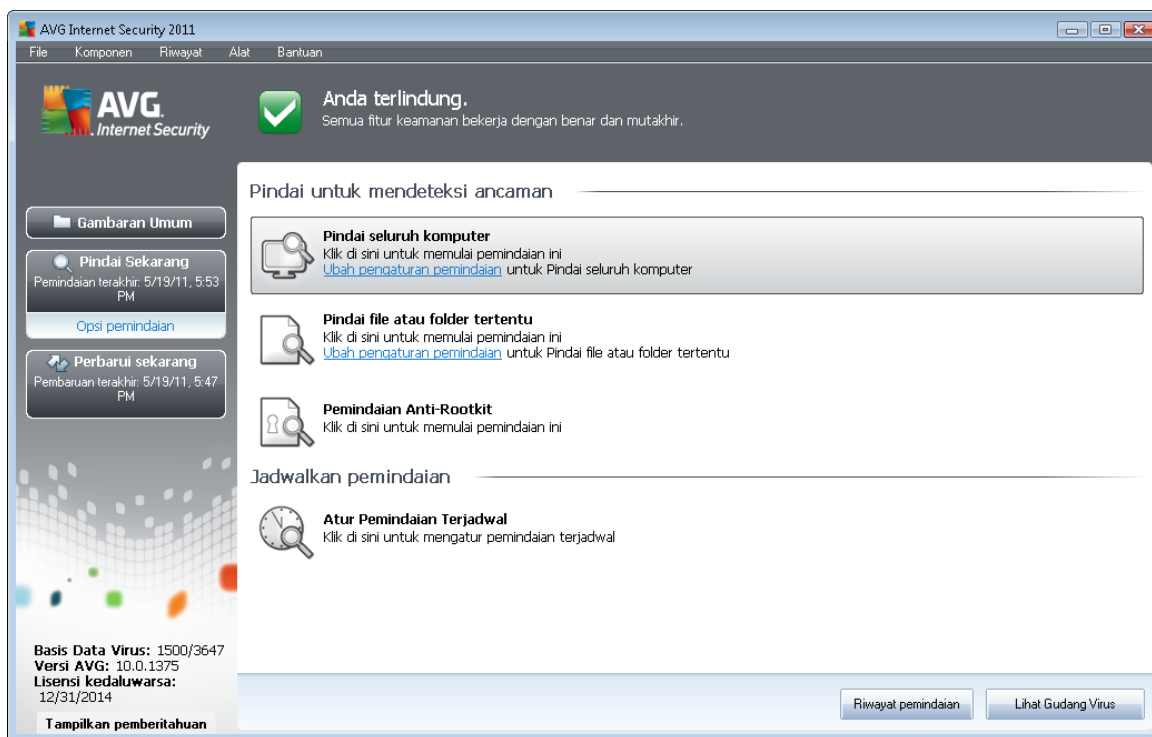
- **/COO** Pindai cookie
- **/?** Tampilkan bantuan untuk topik ini
- **/HELP** Tampilkan bantuan untuk topik ini
- **/PRIORITY** Atur prioritas pindai /Rendah, Otomatis, Tinggi/ (lihat [Pengaturan lanjutan / Pemindaian](#))
- **/SHUTDOWN** Matikan komputer setelah pemindaian selesai
- **/FORCESHUTDOWN** Matikan paksa komputer setelah pemindaian selesai
- **/ADS** Pindai Aliran Data Alternatif (hanya NTFS)
- **/ARCBOMBSW** Laporkan file arsip yang dikompres ulang

11.5. Penjadwalan Pemindaian

Dengan **Keamanan Internet AVG 2011** 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.

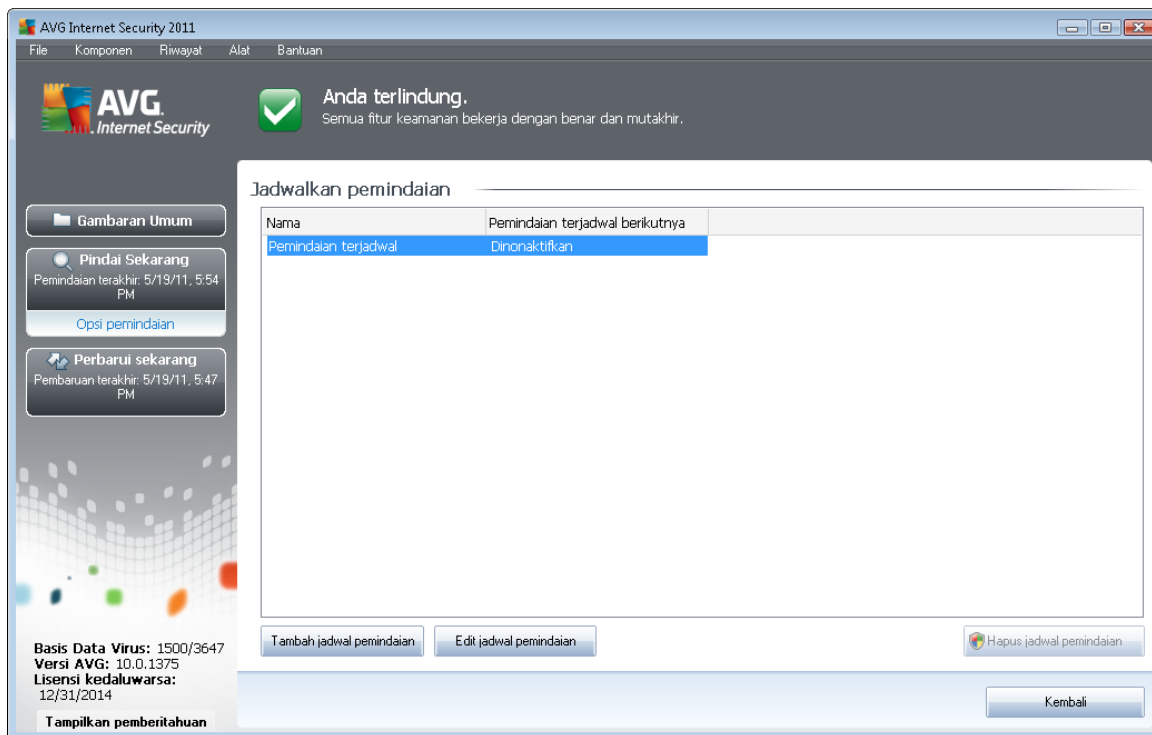
Anda harus meluncurkan [Pemindaian Seisi Komputer](#) secara rutin, sedikitnya sekali seminggu. Walau demikian, jika memungkinkan, luncurkan pemindaian seisi komputer Anda setiap hari - sebagaimana diatur dalam konfigurasi default jadwal pemindaian. Jika komputer "selalu dihidupkan" maka Anda dapat menjadwalkan pemindaian di luar jam kerja. Jika komputer kadang dimatikan, maka pemindaian yang dijadwalkan 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 dalam bagian **Jadwalkan pemindaian** untuk membuka dialog **Jadwalkan pemindaian** baru di mana Anda dapat menemukan daftar semua pemindaian terjadwal saat ini:

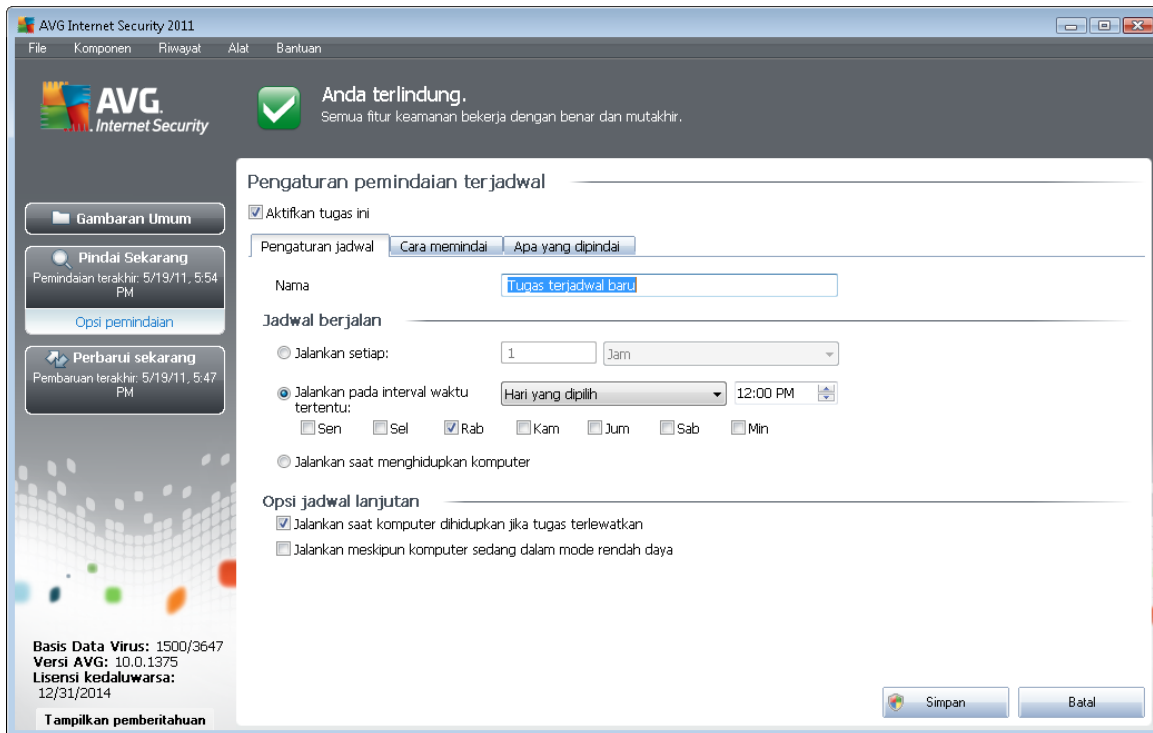


Anda dapat mengedit / menambahkan pemindaian menggunakan tombol kontrol berikut:

- **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](#)

11.5.1. 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 yang akan ditampilkan 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.

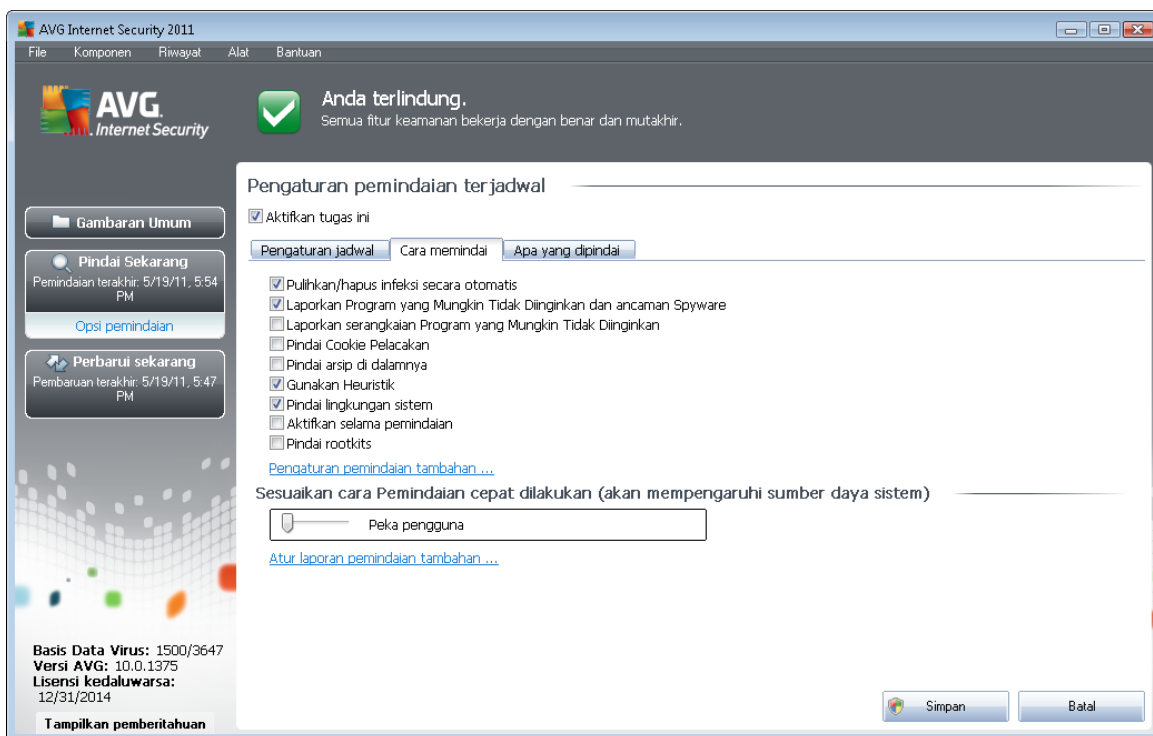


Tombol kontrol pada dialog Pengaturan pemindaian terjadwal

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.
- **Batal** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke [dialog default antarmuka pemindaian AVG](#).

11.5.2. 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 secara otomatis (diaktifkan secara default)**: jika ada virus teridentifikasi selama pemindaian, ia dapat dipulihkan 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

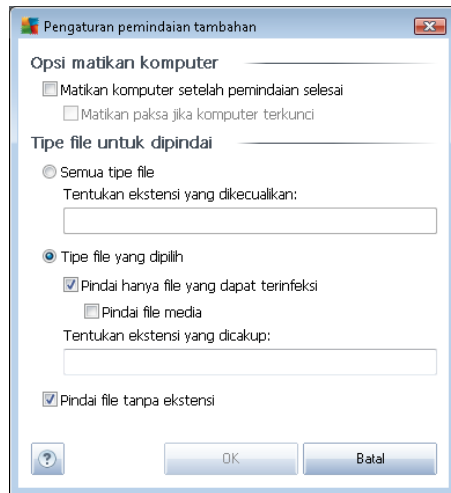


harus memutuskan apa yang akan dilakukan dengan infeksi yang terdeteksi. Tindakan yang disarankan adalah menghapus file yang terinfeksi ke [Gudang Virus](#).

- **Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware** (diaktifkan secara default): centang 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 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.

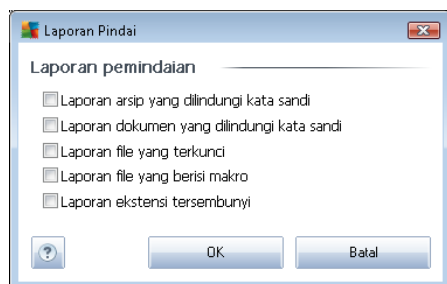
Kemudian, Anda dapat mengubah konfigurasi pemindaian seperti berikut:

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



- o **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**).
- o **Tentukan tipe file yang akan dipindai** - selanjutnya Anda dapat 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.
- **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:



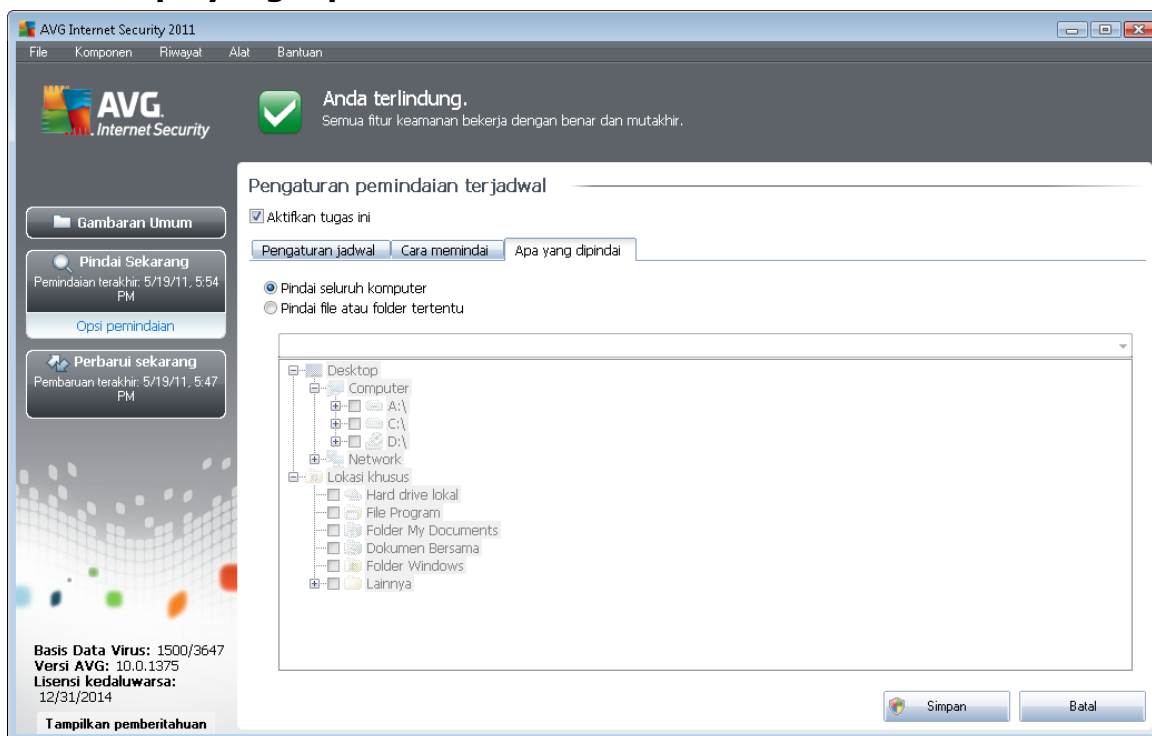
Catatan: Secara default, konfigurasi pemindaian telah diatur untuk performa optimal. Kecuali Anda mempunyai alasan yang kuat untuk mengubah pengaturan pemindaian, sangatlah disarankan untuk tetap menggunakan konfigurasi yang sudah ditetapkan. Semua perubahan konfigurasi hanya boleh dilakukan oleh pengguna berpengalaman. Untuk opsi konfigurasi pemindaian lebih lanjut, lihat dialog [Pengaturan lanjutan](#) yang dapat diakses melalui item menu sistem **File / Pengaturan lanjutan**.

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.
- **Batal** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke [dialog default antarmuka pemindaian AVG](#).

11.5.3. Apa yang Dipindai



Pada tab ***Apa yang dipindai*** Anda dapat menetapkan apakah Anda ingin menjadwalkan [pemindaian seisi komputer](#) atau [pemindaian file atau folder tertentu](#).

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***
 - o C:\Program Files\
 - o dalam versi 64-bit C:\Program Files (x86)
- ***Folder My Documents***



o untuk Win XP: C:\Documents and Settings\Default User\My Documents\

o untuk Windows Vista/7: C:\Users\user\Documents\

- **Dokumen Bersama**

o untuk Win XP: C:\Documents and Settings\All Users\Documents\

o untuk Windows Vista/7: C:\Users\Public\Documents\

- **Folder Windows** - C:\Windows\

- **Lainnya**

o Drive sistem – hard drive tempat menginstal sistem operasi Anda (biasanya C:)

o Folder sistem - C:\Windows\System32\

o Folder File Sementara - C:\Documents and Settings\User\Local\ (Windows XP); atau C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)

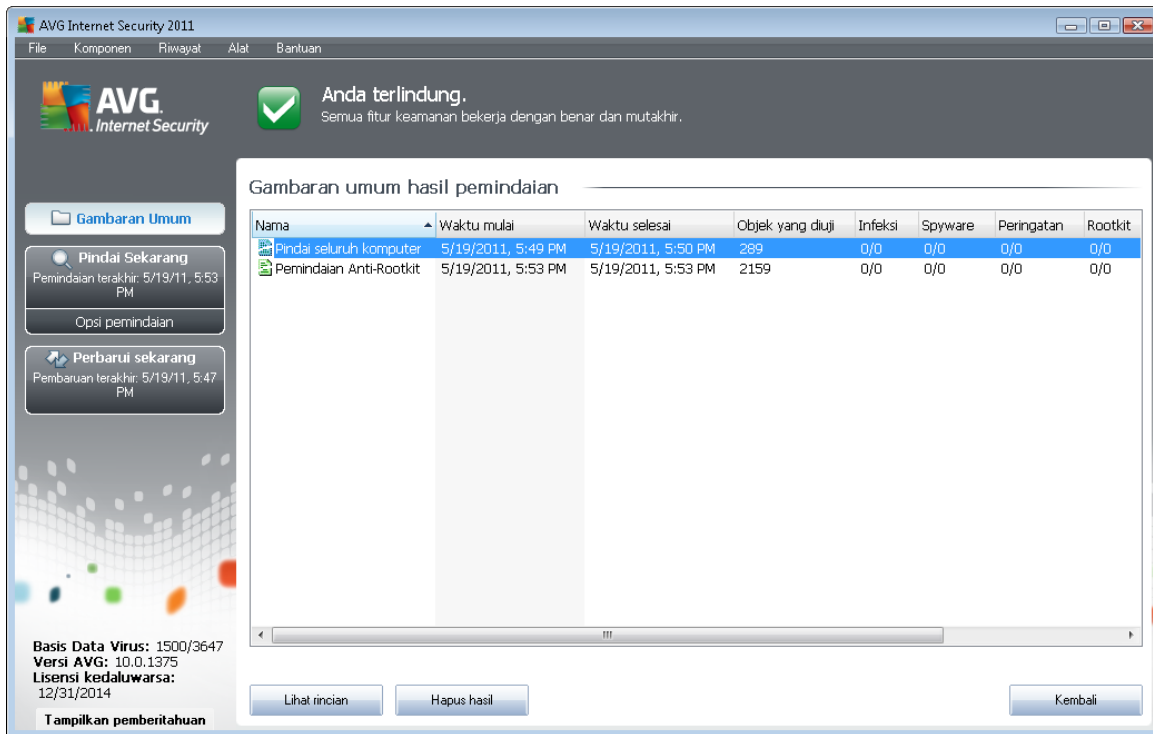
o File Internet Sementara - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); atau C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

Tombol kontrol 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.
- **Batal** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke [dialog default antarmuka pemindaian AVG](#).

11.6. Gambaran 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](#)

11.7. Perincian Hasil Pemindaian

Jika dalam dialog [Gambaran 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.

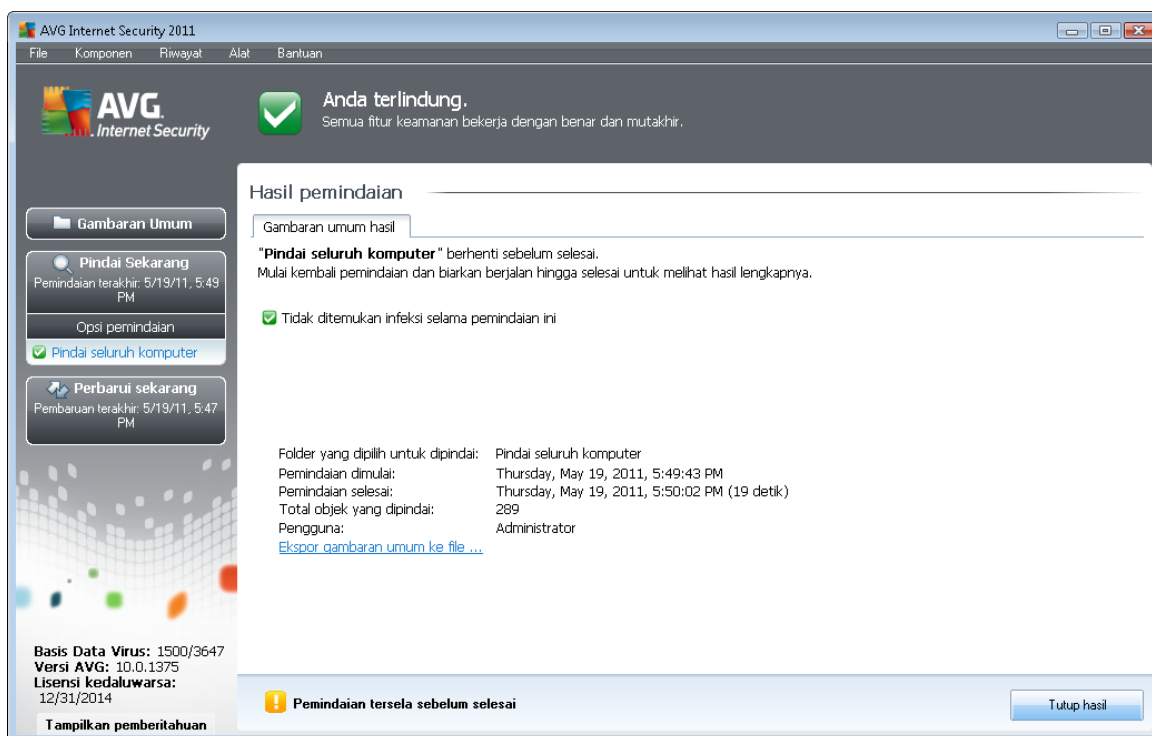
Dialog dibagi ke dalam beberapa tab:

- **Gambaran 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 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).

11.7.1. Tab Gambaran Umum Hasil



Pada tab **Hasil pemindaian** Anda dapat menemukan statistik terperinci berisi informasi mengenai:

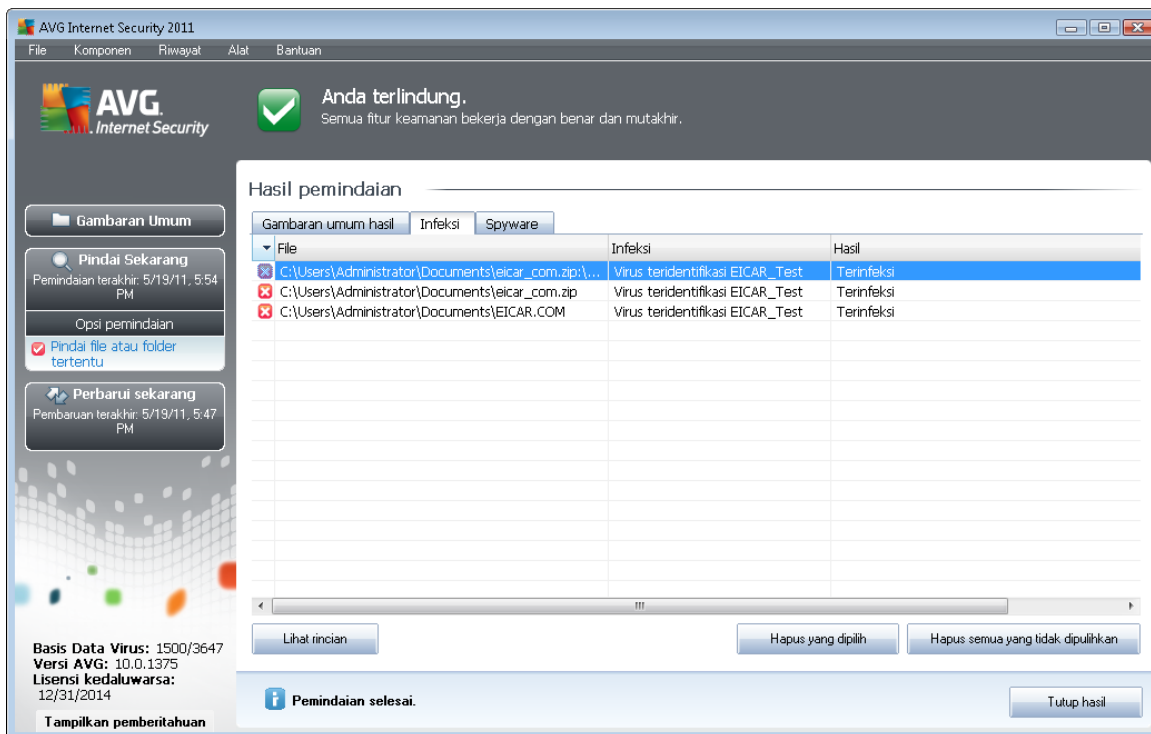
- [infeksi virus](#) / [spyware yang terdeteksi](#)
- [infeksi virus](#) / [spyware yang dihapus](#)
- jumlah [infeksi virus](#) / [spyware](#) yang tidak dapat dihapus atau dipulihkan

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 [Gambaran umum hasil pemindaian](#).

11.7.2. 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:

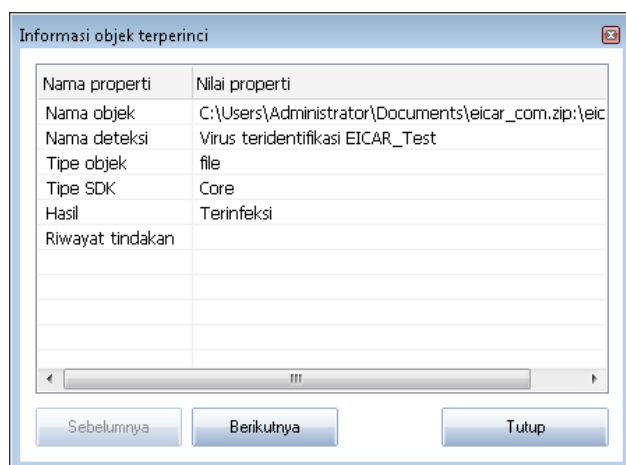
- **File** - jalur lengkap ke lokasi asli dari objek yang terinfeksi
- **Infeksi** - nama [virus](#) yang terdeteksi (*untuk perincian mengenai virus tertentu, lihatlah [Ensiklopedia Virus](#) online*)
- **Hasil** - menentukan status terkini dari objek terinfeksi yang terdeteksi selama pemindaian:
 - o **Terinfeksi** - objek terinfeksi terdeteksi dan dibiarkan di lokasi aslinya (*misalnya, jika Anda telah [menonaktifkan opsi pemulihan otomatis](#) dalam pengaturan pemindaian tertentu*)
 - o **Dipulihkan** - objek terinfeksi dipulihkan secara otomatis dan dibiarkan di lokasi aslinya
 - o **Dipindahkan ke Gudang Virus** - objek yang terinfeksi telah dipindahkan ke karantina [Gudang Virus](#)
 - o **Dihapus** - objek yang terinfeksi dihapus
 - o **Ditambahkan ke pengecualian PUP** - temuan telah dievaluasi sebagai pengecualian dan telah ditambahkan ke daftar pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian PUP](#) pada pengaturan lanjutan*)

- o **File terkunci - belum diuji** - objek yang bersangkutan telah dikunci sehingga AVG tidak dapat memindainya
- o **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
- o **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:

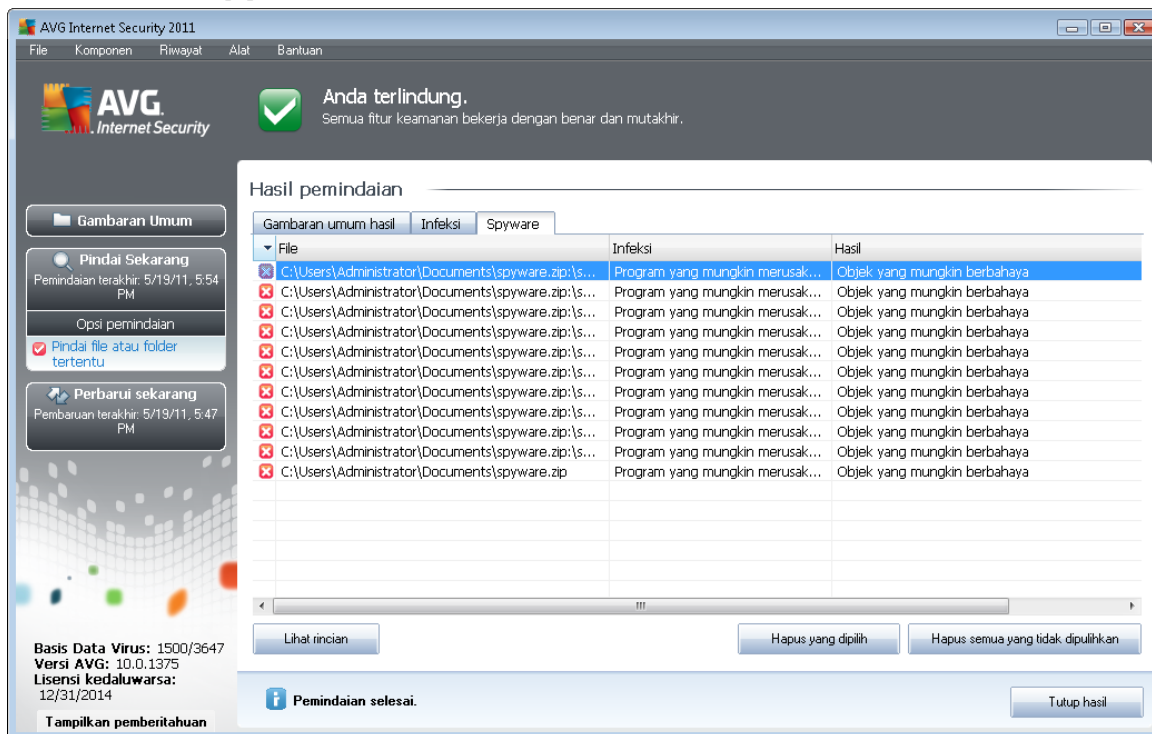
- **Lihat perincian** - tombol ini membuka jendela dialog baru bernama **Perincian informasi objek**:



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](#)

11.7.3. 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:

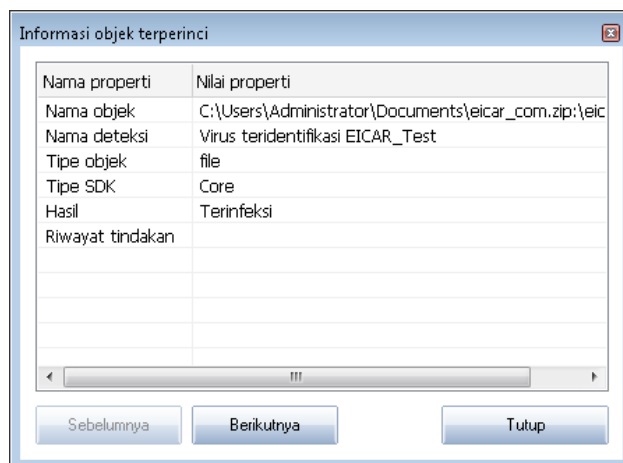
- **File** - jalur lengkap ke lokasi asli dari objek yang terinfeksi
- **Infeksi** - nama **spyware** yang terdeteksi (*untuk perincian mengenai virus tertentu, harap lihat [Ensiklopedia Virus](#) online*)
- **Hasil** - menentukan status terkini dari objek yang terdeteksi selama pemindaian:
 - o **Terinfeksi** - objek terinfeksi yang terdeteksi dan dibiarkan di lokasi aslinya (misalnya, jika Anda telah [menonaktifkan opsi pemulihan otomatis](#) dalam pengaturan pemindaian tertentu)
 - o **Dipulihkan** - objek terinfeksi yang dipulihkan secara otomatis dan dibiarkan di lokasi aslinya
 - o **Dipindahkan ke Gudang Virus** - objek yang terinfeksi telah dipindahkan ke karantina [Gudang Virus](#)
 - o **Dihapus** - objek yang terinfeksi dihapus
 - o **Ditambahkan ke pengecualian PUP** - temuan telah dievaluasi sebagai pengecualian dan telah ditambahkan ke daftar pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian PUP](#) pada pengaturan lanjutan*)

- o **File terkunci - belum dites** - objek yang bersangkutan telah dikunci sehingga AVG tidak dapat memindainya
- o **Objek yang mungkin berbahaya** - objek telah terdeteksi sebagai objek yang mungkin berbahaya namun tidak terinfeksi (ia bisa berisi makro, misalnya); informasi ini peringatan saja
- o **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 gambaran umum informasi terperinci dan mengembalikan ke dialog [Gambaran umum hasil pemindaian](#)



11.7.4. Tab Peringatan

Tab **Peringatan** menampilkan informasi mengenai objek "dicurigai" (*biasanya berupa file*) yang terdeteksi selama pemindaian. Bila terdeteksi oleh [Perisai Tetap](#), 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 yang terdeteksi oleh pengujian AVG hanya Peringatan, tidak diperlukan tindakan apa pun.

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 AVG Anda melaporkan file tersembunyi yang Anda curigai berbahaya, Anda dapat memindahkannya ke [Gudang Virus AVG](#) Anda.
- **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, dll.
- **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.

11.7.5. Tab Rootkit

Tab **Rootkit** menampilkan informasi tentang rootkit yang terdeteksi selama pemindaian jika Anda telah meluncurkan [Pemindaian Anti-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.

Struktur tab ini pada dasarnya sama seperti [Tab Infeksi](#) atau [Tab Spyware](#).

11.7.6. 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 AVG dapat mendeteksi file yang mungkin tidak terinfeksi, tetapi mencurigakan. File-file ini dilaporkan sebagai [Peringatan](#), atau sebagai **Informasi**.

Informasi keseriusan dapat dilaporkan untuk salah satu alasan berikut:

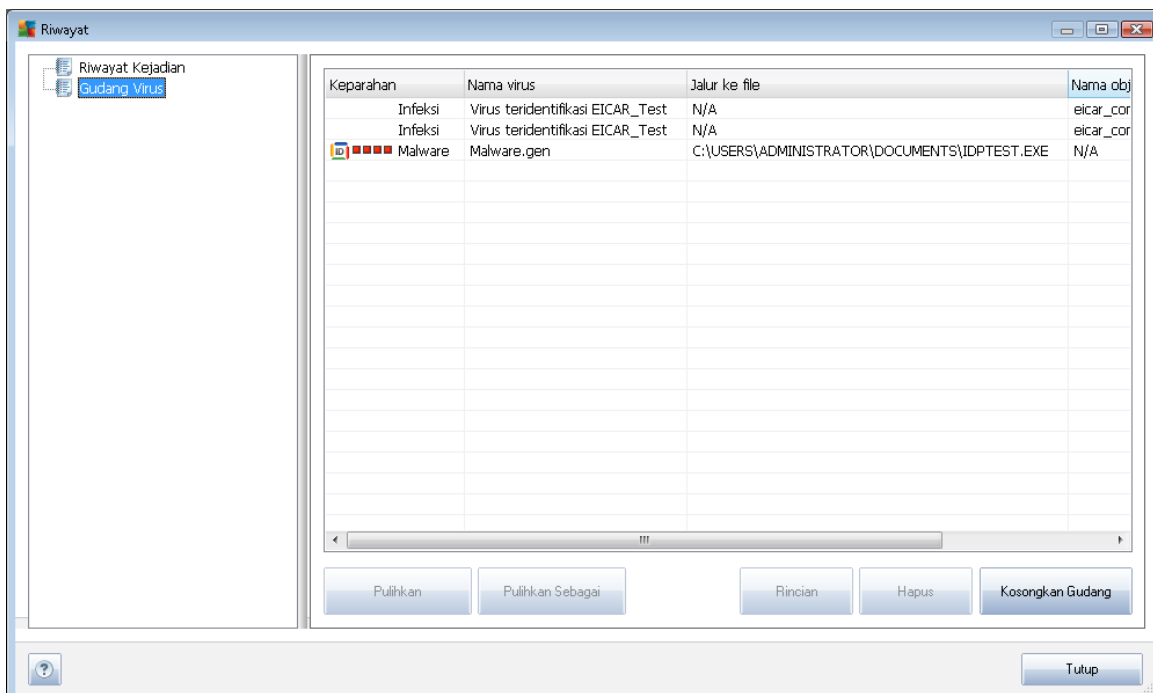
- **Kemasan run-time**- File dikemas dengan salah satu pengemas run-time yang tidak umum,



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 AVG (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 yang kedua tidak terlihat pada Windows secara default, dan AVG melaporkan file tersebut untuk mencegah 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*), AVG 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 AVG. Hal ini biasanya berarti bahwa beberapa file terus-menerus digunakan oleh sistem (mis. *file swap*).

11.8. 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.

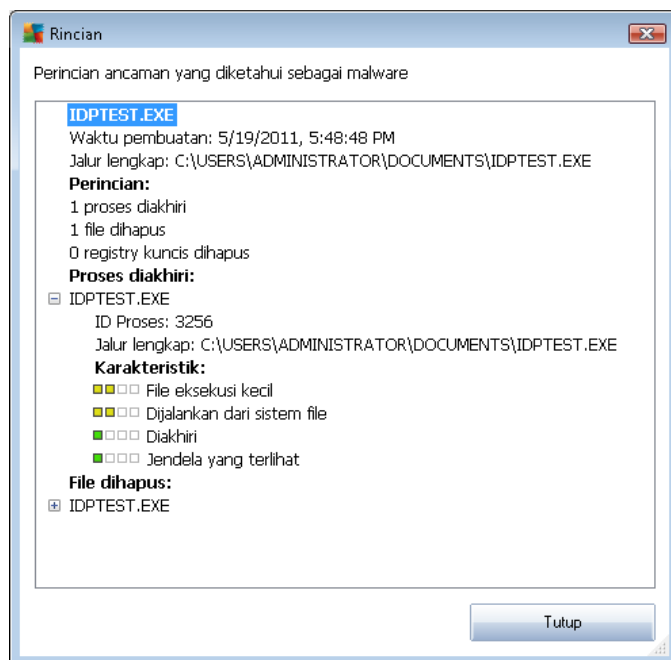
Antarmuka **Gudang Virus** membuka jendela tersendiri dan menyediakan gambaran umum informasi mengenai objek terinfeksi yang telah dikarantina:

- **Keseriusan** - jika Anda memutuskan untuk menginstal komponen [Perlindungan Identitas](#) dalam **Keamanan Internet AVG 2011** 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** - menetapkan nama infeksi yang terdeteksi ke [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 [Perlindungan Identitas](#). 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*).



12. Pembaruan AVG

Menjaga AVG Anda selalu terbaru sangatlah penting untuk memastikan bahwa semua virus yang baru ditemukan akan terdeteksi secepatnya.

Karena pembaruan AVG tidak dirilis berdasarkan jadwal tetap, tapi disesuaikan dengan reaksi terhadap jumlah dan keseriusan ancaman baru, maka disarankan agar Anda memeriksa pembaruan sedikitnya sekali setiap harinya. Hanya dengan cara ini Anda dapat memastikan **Keamanan Internet AVG 2011** tetap terkini sepanjang hari.

12.1. Tingkat Pembaruan

AVG menyediakan dua tingkat pembaruan untuk dipilih dari:

- **Pembaruan definisi** berisi perubahan yang diperlukan agar perlindungan anti-virus 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 memilih tingkat prioritas yang akan diunduh dan diterapkan.

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

12.2. Tipe Pembaruan

Anda dapat membedakan dua tipe pembaruan:

- **Pembaruan bila diperlukan** adalah pembaruan AVG tingkat menengah yang dapat dilakukan kapan saja bila diperlukan.
- **Pembaruan terjadwal** - dalam AVG juga memungkinkan untuk [mengatur rencana pembaruan](#). Pembaruan yang direncanakan akan dilaksanakan secara berkala sesuai dengan konfigurasi pengaturan. Bila file pembaruan baru sudah ada pada lokasi yang ditentukan, file akan diunduh langsung dari Internet atau dari direktori jaringan. Bila tidak tersedia pembaruan baru, maka tidak terjadi apa-apa.

12.3. Proses Pembaruan

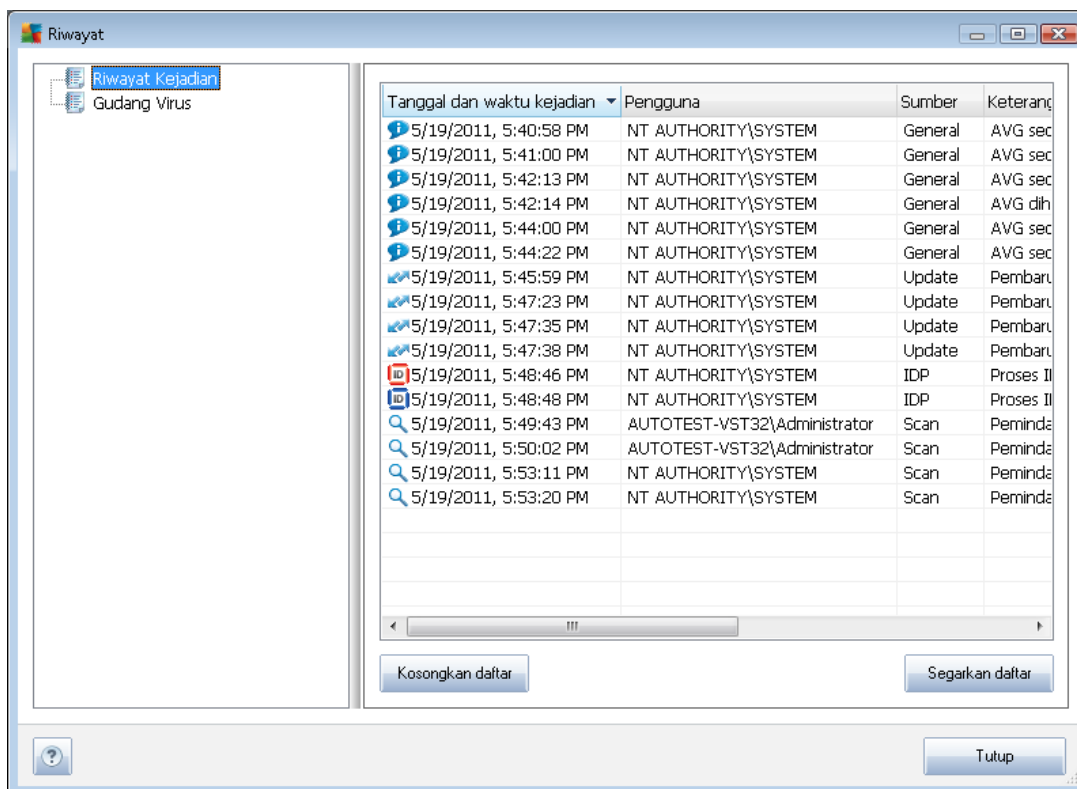
Proses pembaruan dapat diluncurkan dengan segera begitu diperlukan melalui [tautan cepat Perbarui sekarang](#). Tautan ini selalu tersedia dari dialog [antarmuka pengguna AVG](#) mana saja. Walau demikian, tetap sangat disarankan untuk melakukan pembaruan rutin sebagaimana disebutkan dalam jadwal pembaruan yang dapat diedit dalam komponen [Pengatur pembaruan](#).

Begitu Anda memulai pembaruan, AVG akan memverifikasi terlebih dahulu apakah ada file pembaruan baru yang tersedia. Jika ya, AVG akan mulai mengunduhnya dan meluncurkan proses pembaruannya. Selama proses pembaruan, Anda akan dialihkan ke antarmuka **Perbarui** di mana 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 dapat memulihkan OS ke konfigurasi aslinya dari titik ini. Opsi ini dapat diakses melalui Start / All Programs / Accessories / System tools / System Restore. Disarankan untuk pengguna yang berpengalaman saja!

13. 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 Internet AVG 2011**. **Riwayat** merekam tipe kejadian berikut:

- Informasi tentang pembaruan aplikasi AVG
- Pemindaian dimulai, selesai atau berhenti (*termasuk tes yang dilakukan secara otomatis*)
- Kejadian yang berhubungan dengan deteksi virus (oleh [Perisai Tetap](#) atau [pemindaian](#)) termasuk lokasi kejadian
- Kejadian penting lainnya

Untuk setiap kejadian, tercantum informasi berikut:

- **Tanggal dan waktu kejadian** menunjukkan tanggal dan waktu persis terjadinya kejadian
- **Pengguna** menyatakan siapa yang memulai kejadian tersebut
- **Sumber memberikan komponen sumber atau bagian lain dari sistem yang memicu kejadian tersebut**



- ***Keterangan kejadian*** berisi ringkasan apa yang sebenarnya terjadi

Tombol kontrol

- ***Kosongkan daftar*** - menghapus semua entri dalam daftar kejadian
- ***Segarkan daftar*** - memperbarui semua entri dalam daftar kejadian



14. Tanya-Jawab dan Dukungan Teknis

Jika Anda memiliki masalah dengan AVG Anda, baik dalam hal bisnis atau teknis, baca bagian [Tanya-Jawab](http://www.avg.com/) dari situs web AVG (<http://www.avg.com/>).

Jika Anda tidak berhasil mendapatkan bantuan dengan cara ini, hubungi bagian dukungan teknis melalui e-mail. Gunakan formulir kontak yang dapat diakses dari menu sistem lewat **Bantuan / Dapatkan bantuan online**.