AVG 9 Internet Security

Panduan Pengguna

Revisi dokumen 90.6 (14.9.2009)

Daftar Isi

1. Pendahuluan

Panduan pengguna ini berisi dokumentasi lengkap untuk **AVG 9 Internet Security**.

Selamat, Anda telah membeli AVG 9 Internet Security!

AVG 9 Internet Security adalah salah satu jajaran produk AVG peraih penghargaan yang dirancang untuk memberikan Anda ketenangan pikiran dan keamanan total untuk PC Anda. Sebagaimana dengan semua produk AVG, **AVG 9 Internet Security** 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 **AVG 9 Internet Security** baru Anda mempunyai antarmuka efektif yang dikombinasikan 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 dikembangkannya untuk melindungi aktivitas komputer dan jaringan Anda. Nikmati pengalaman perlindungan penuh dari AVG.

2. Persyaratan Instalasi AVG

2.1. Sistem Operasi yang Didukung

AVG 9 Internet Security ditujukan untuk melindungi workstation dengan sistem operasi berikut:

- Windows 2000 Professional SP4 + Update Rollup 1
- 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 2000 dan XP x64. Pada sistem operasi ini Anda dapat menginstal AVG 9 Internet Security tapi hanya tanpa komponen IDP.*

2.2. Persyaratan Perangkat Keras Minimum

Persyaratan perangkat keras minimum untuk **AVG 9 Internet Security** adalah sebagai berikut:

- Intel Pentium CPU 1,2 GHz
- ruang kosong hard drive 250 MB (untuk keperluan instalasi)
- memori RAM 256 MB

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 Anda dapat memastikan untuk menginstal versi terbaru AVG 9 Internet Security.

Kami menyarankan Anda untuk mencoba alat Pengatur Unduhan AVG kami yang baru, yang akan membantu Anda memilih file instalasi yang tepat!

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.

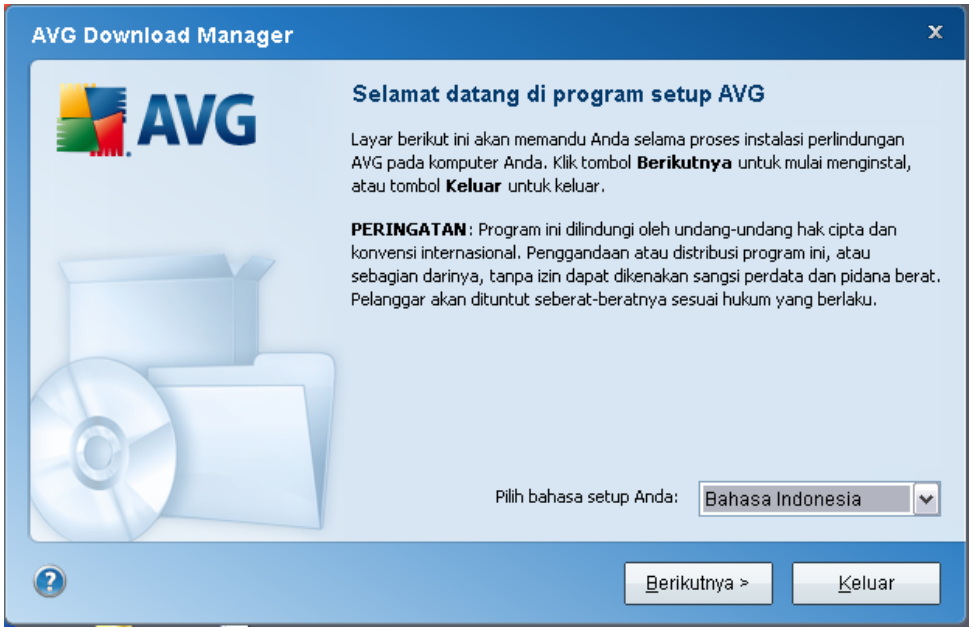
4. Pengatur Unduhan AVG

Pengatur Unduhan AVG merupakan alat sederhana yang membantu Anda memilih file instalasi yang tepat untuk produk AVG Anda. Berdasarkan data masukan Anda, manajer akan memilih produk spesifik, tipe lisensi, komponen yang diinginkan, dan bahasa. Terakhir, **Pengatur Unduhan AVG** selanjutnya akan mengunduh dan meluncurkan proses instalasi yang sesuai.

Peringatan: *Perhatikan bahwa Pengatur Unduhan AVG tidak sesuai untuk mengunduh edisi jaringan dan SBS dan hanya mendukung sistem operasi berikut: Windows 2000 (SP4 + SRP roll-up), Windows XP (SP2 dan yang lebih tinggi), Windows Vista (semua edisi).*

Pengatur Unduhan AVG tersedia untuk diunduh di situs web AVG (<% avg_websiteAVG%> . Carilah keterangan singkat masing-masing langkah yang perlu Anda lakukan dalam **Pengatur Unduhan AVG** berikut ini:

4.1. Pemilihan Bahasa

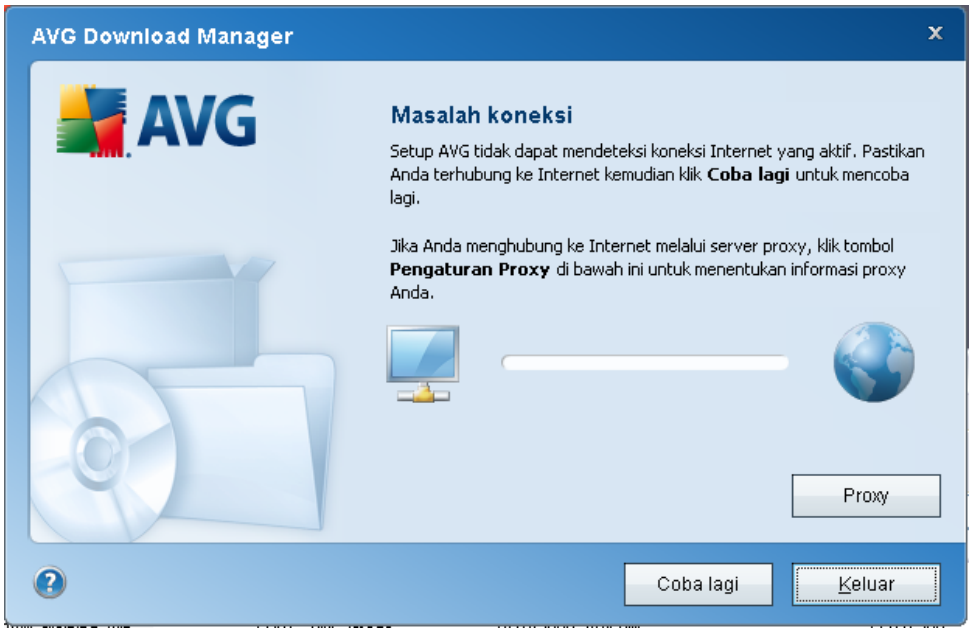


Dalam langkah pertama dari **Pengatur Unduhan AVG** ini, pilih bahasa instalasi dari menu gulir-bawah. Perhatikan, pilihan bahasa Anda hanya berlaku untuk proses instalasi; setelah instalasi, Anda akan dapat mengubah bahasanya langsung dari pengaturan program. Kemudian tekan tombol ***Berikutnya*** untuk melanjutkan.

4.2. Pemeriksaan Konektivitas

Dalam langkah berikutnya, **Pengatur Unduhan AVG** akan berusaha membuat koneksi Internet untuk mencari pembaruan. Anda tidak akan diperbolehkan untuk memajukan proses unduh hingga **Pengatur Unduhan AVG** dapat menyelesaikan tes konektivitas.

- Jika tes menunjukkan tidak ada konektivitas, pastikan Anda benar-benar telah terhubung ke Internet. Kemudian klik tombol ***Coba Lagi***



- Jika Anda menggunakan koneksi Proxy ke Internet, klik tombol ***Pengaturan Proxy*** untuk menetapkan informasi proxy Anda:

- Jika pemeriksaan berhasil, tekan tombol ***Berikutnya*** untuk melanjutkan.

4.3. Pengaturan Proxy

Jika **Pengatur Unduhan AVG** tidak dapat mengenali pengaturan Proxy, Anda harus menetapkannya secara manual. Isilah data berikut:

- ***Server*** - masukkan nama server proxy atau alamat IP yang sah
- ***Port*** - masukkan nomor port-nya
- ***Gunakan autentikasi proxy*** - jika server proxy Anda memerlukan autentikasi, tandai kotak ini.
- ***Pilih autentikasi*** - dari menu buka bawah, pilih tipe autentikasi. Kami sangat menyarankan agar Anda tetap menggunakan nilai default (*proxy server nanti akan memberitahu persyaratannya kepada Anda*). Walau demikian, jika Anda seorang pengguna mahir, Anda juga dapat memilih Dasar (*diperlukan oleh beberapa server*) atau opsi NTLM (*diperlukan oleh semua Server ISA*). Kemudian, masukkan ***Nama Pengguna*** dan ***Kata Sandi*** yang sah (opsional).

Konfirmasikan pengaturan Anda dengan menekan tombol ***Terapkan*** untuk melanjutkan ke langkah berikutnya dari **Pengatur Unduhan AVG**.

4.4. Pilih Tipe Lisensi

Dalam langkah ini Anda akan dikonfirmasi untuk memilih tipe lisensi produk yang ingin Anda unduh. Keterangan yang disediakan akan memungkinkan Anda memilih

mana yang paling cocok buat Anda:

- ***Versi lengkap*** - misalnya ***AVG Anti-Virus***, ***AVG Anti-Virus plus Firewall***, atau ***AVG Internet Security***
- ***Versi uji coba*** - memberikan Anda kesempatan menggunakan semua fitur pada produk AVG versi lengkap selama jangka waktu terbatas 30 hari
- ***Versi gratis*** - menyediakan perlindungan bebas biaya kepada pengguna rumahan, walau demikian fungsi aplikasinya terbatas! Selain itu, versi gratis hanya berisi sebagian fitur yang tersedia dalam produk berbayar.

4.5. Unduh File Untuk Diinstal

Sekarang, Anda telah memberikan semua informasi yang diperlukan bagi **Pengatur Unduhan AVG** untuk mulai mengunduh paket instalasi, dan meluncurkan proses instalasi. Selanjutnya, maju ke Proses Instalasi AVG.

5. Proses Instalasi AVG

Untuk menginstal **AVG 9 Internet Security** 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 ***Unduh***. Atau, Anda dapat menggunakan alat ***Pengatur Unduhan AVG*** kami yang baru untuk membantu Anda membuat dan mengunduh paket instalasi yang diperlukan, dan meluncurkan proses instalasi.

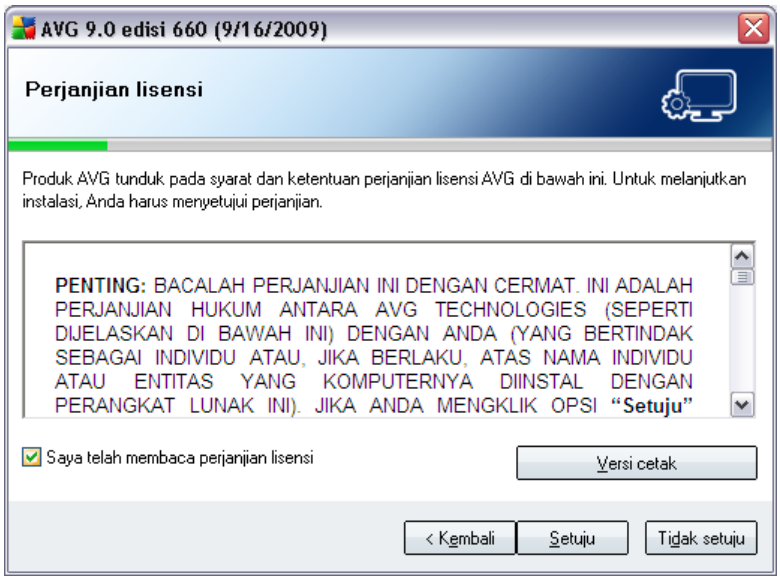
Instalasi adalah rangkaian jendela dialog berisi keterangan singkat mengenai apa yang dilakukan di setiap langkah. Berikut ini, kami menawarkan penjelasan untuk setiap jendela dialog:

5.1. Peluncuran Instalasi

Proses instalasi dimulai dengan jendela ***Selamat datang di Program Pengaturan AVG*** . Di sini Anda memilih bahasa yang digunakan untuk proses instalasi. Di bagian bawah jendela dialog, temukan item ***Pilih bahasa pengaturan Anda***, dan pilih bahasa yang diinginkan dari menu buka bawah. Kemudian tekan tombol ***Berikutnya*** untuk mengonfirmasi dan melanjutkan ke dialog berikutnya.

Perhatian: *Di sini, Anda memilih bahasa hanya untuk proses instalasi. Anda tidak memilih bahasa untuk aplikasi AVG - yang dapat ditetapkan nanti saat proses instalasi!*

5.2. Perjanjian Lisensi



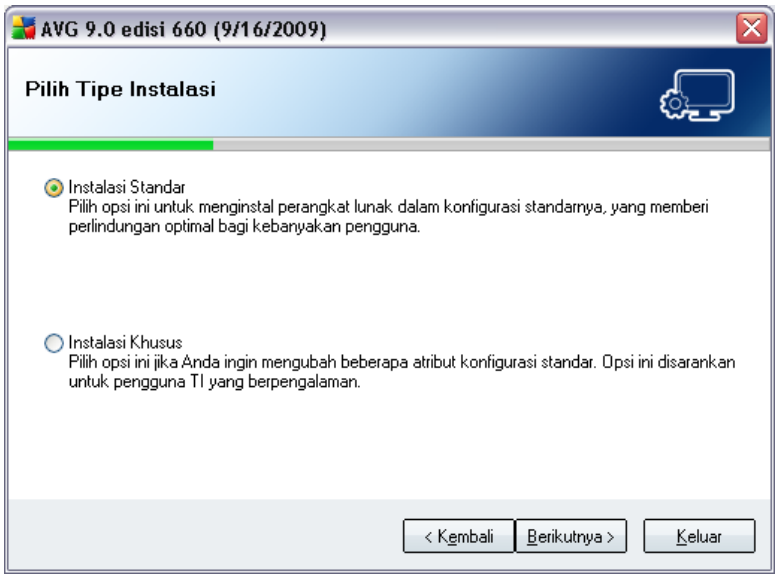
Dialog ***Perjanjian Lisensi*** menyediakan kalimat lengkap perjanjian lisensi AVG. Harap baca perjanjian ini dengan saksama dan konfirmasikan Anda telah membaca, mengerti dan menyetujui perjanjian ini dengan mencentang kotak ***Saya telah membaca perjanjian lisensi*** dan menekan tombol ***Terima***.

Jika Anda tidak setuju dengan perjanjian lisensi tersebut, tekan tombol ***Jangan terima***, maka proses instalasi akan segera diakhiri.

5.3. Memeriksa Status Sistem

Setelah mengonfirmasi perjanjian lisensi, Anda akan dialihkan ke dialog ***Memeriksa Status Sistem***. Dialog ini tidak memerlukan intervensi apa pun; sistem Anda akan diperiksa sebelum instalasi AVG dapat dimulai. Harap tunggu hingga proses selesai, kemudian lanjutkan secara otomatis ke dialog berikut.

5.4. Pilih Tipe Instalasi



Dialog ***Pilih Tipe Instalasi*** menyediakan pilihan dua opsi instalasi: instalasi ***standar*** dan ***khusus***.

Untuk sebagian besar pengguna, sangatlah disarankan untuk tetap menggunakan ***instalasi standar*** yang akan menginstal AVG dalam mode otomatis penuh bersama pengaturan yang telah ditentukan 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.

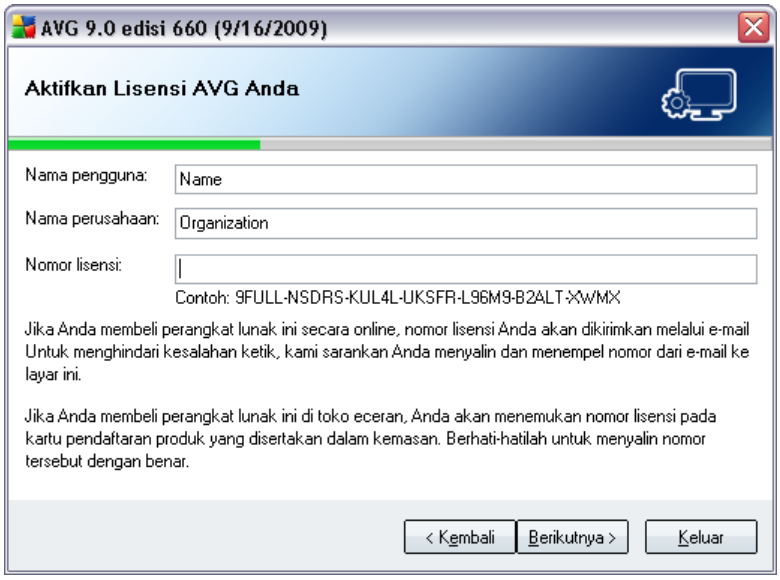
Instalasi khusus hanya boleh digunakan oleh pengguna berpengalaman dengan alasan yang sah untuk menginstal AVG dengan pengaturan non-standar. Misalnya, agar pas dengan persyaratan sistem tertentu.

5.5. Aktifkan Lisensi AVG Anda

Dalam dialog ***Aktifkan Lisensi AVG Anda***, Anda harus mengisi data pendaftaran. Ketikkan nama Anda (bidang ***Nama Pengguna***) dan nama organisasi Anda (bidang ***Nama Perusahaan***).

Kemudian masukkan nomor lisensi/nomor penjualan Anda ke dalam bidang teks ***Nomor Lisensi*** . Nomor penjualan dapat ditemukan pada kemasan CD di kotak **AVG 9 Internet Security** Anda. Nomor lisensi ada dalam email konfirmasi yang telah

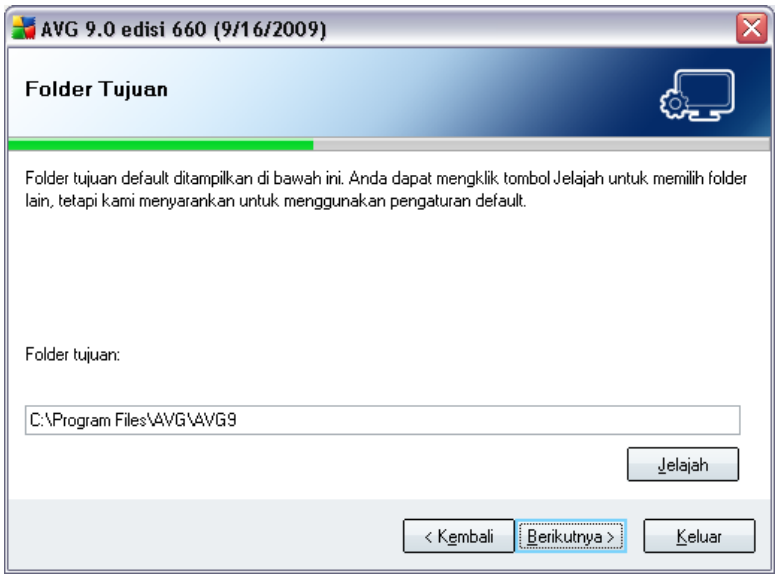
Anda terima setelah membeli **AVG 9 Internet Security** Anda secara online. Anda harus mengetikkan angkanya persis seperti yang ditampilkan. Jika tersedia bentuk digital dari nomor lisensi tersebut (*dalam email*), disarankan menggunakan metode salin dan tempel untuk memasukkannya.



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

Jika dalam langkah sebelumnya Anda telah memilih instalasi standar, Anda akan dialihkan langsung ke dialog ***AVG Security Toolbar*** . Jika telah memilih instalasi khusus, Anda akan melanjutkan dengan dialog ***Folder Tujuan***.

5.6. Instalasi Khusus - Folder Tujuan

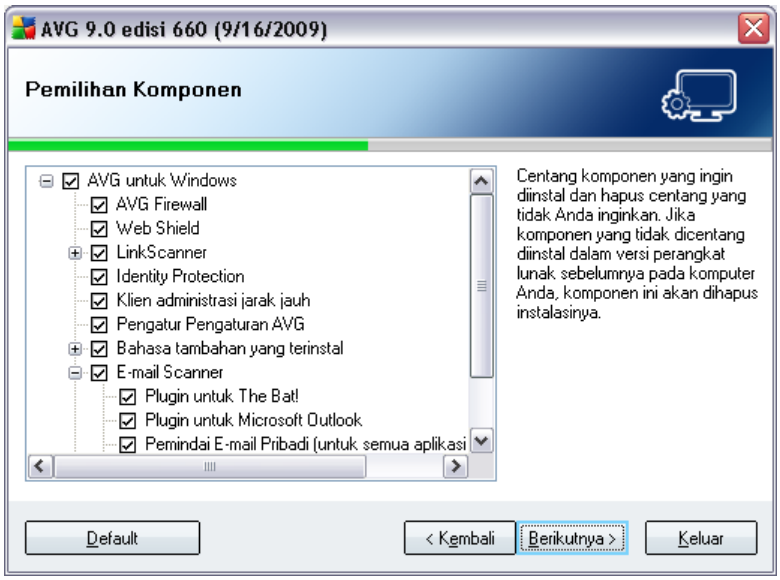


Dialog ***Folder Tujuan*** memungkinkan Anda untuk menetapkan lokasi menginstal **AVG 9 Internet Security**. Secara default, AVG akan diinstal ke folder Program Files yang berada di drive C:. Jika folder tersebut belum ada, Anda akan ditanya dalam dialog baru untuk mengonfirmasi bahwa Anda setuju AVG membuat folder tersebut sekarang.

Jika Anda ingin mengubah lokasi ini, gunakan tombol ***Jelajah*** untuk menampilkan struktur drive, dan pilih foldernya.

Tekan tombol ***Berikutnya*** untuk mengonfirmasi.

5.7. Instalasi Khusus - Pemilihan Komponen



Dialog ***Pemilihan Komponen*** **AVG 9 Internet Security**menampilkan gambaran umum mengenai semua komponen 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. Dalam dialog Pemilihan Komponen hanya ada komponen-komponen yang tersedia untuk diinstal!

- ***Pemilihan bahasa***

  Dalam daftar komponen yang akan diinstal, Anda dapat menentukan bahasa yang harus diinstal dalam AVG. Periksa item ***Bahasa tambahan yang diinstal*** kemudian pilih bahasa yang diinginkan dari menunya.

- ***Plugin Pemindai E-mail***

  Klik item ***Pemindai E-mail*** untuk membuka dan memutuskan plugin yang diinstal untuk menjamin keamanan surat elektronik Anda. Secara default, ***Plugin untuk Microsoft Outlook*** akan diinstal. Jika lisensi yang Anda beli menyertakan ***Anti-Spam***, maka ia juga akan diinstal secara otomatis. Opsi spesifik lainnya adalah ***Plugin untuk The Bat!*** Jika Anda menggunakan klien e-mail lain (*MS Exchange, Qualcomm Eudora, ...*), carilah opsi ***Pemindai E-mail Pribadi*** untuk mengamankan komunikasi e-mail Anda secara otomatis, apa pun program e-mail yang Anda jalankan.

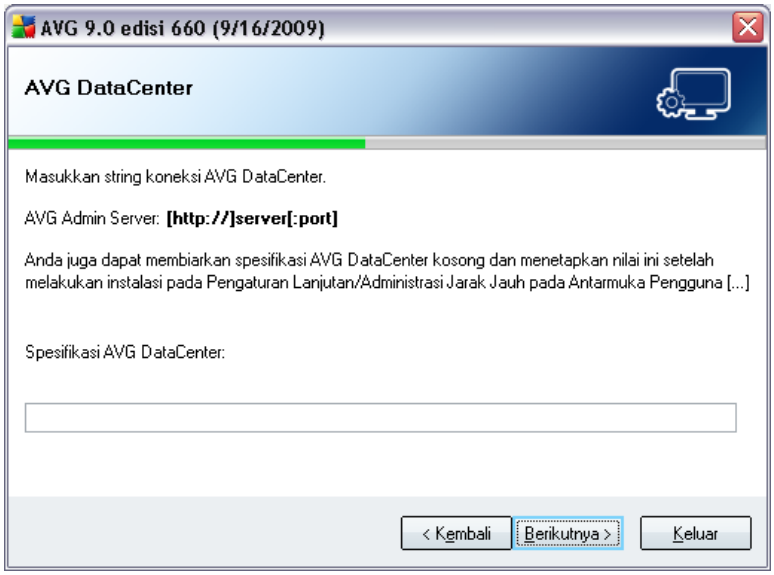
- ***Administrasi Jarak Jauh***

  Jika Anda berencana menghubungkan komputer Anda ke AVG Remote Administration nanti, tandai itemnya agar diinstal juga.

Lanjutkan dengan menekan tombol ***Berikutnya***.

5.8. AVG DataCenter

Jika dalam dialog ***Instalasi Khusus - Pemilihan Komponen*** sebelumnya Anda telah menandai item***Administrasi jarak jauh*** untuk diinstal, maka parameter ***AVG DataCenter*** perlu ditentukan:



Dalam bidang teks ***spesifikasi AVG DataCenter*** , masukkan string koneksi menuju ***AVG DataCenter*** dalam format *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***.

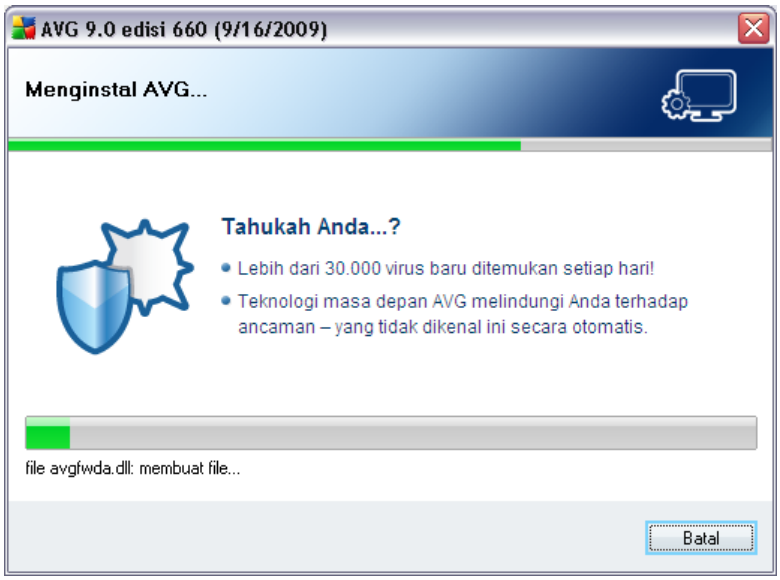
Catatan: *Untuk informasi terperinci mengenai AVG Remote administration, harap baca panduan pengguna AVG Network Edition; dapat diunduh darisitus web AVG (* *http://www.avg.com/*).

5.9. AVG Security Toolbar

Dalam dialog ***AVG Security Toolbar*** , putuskan apakah Anda ingin menginstal ***AVG Security Toolbar*** (*verifikasi hasil telusur dari mesin telusur Internet yang didukung*). Jika Anda tidak mengubah pengaturan default, komponen ini akan diinstal secara otomatis dalam peramban Internet Anda guna memberi perlindungan online menyeluruh saat menjelajahi Internet.

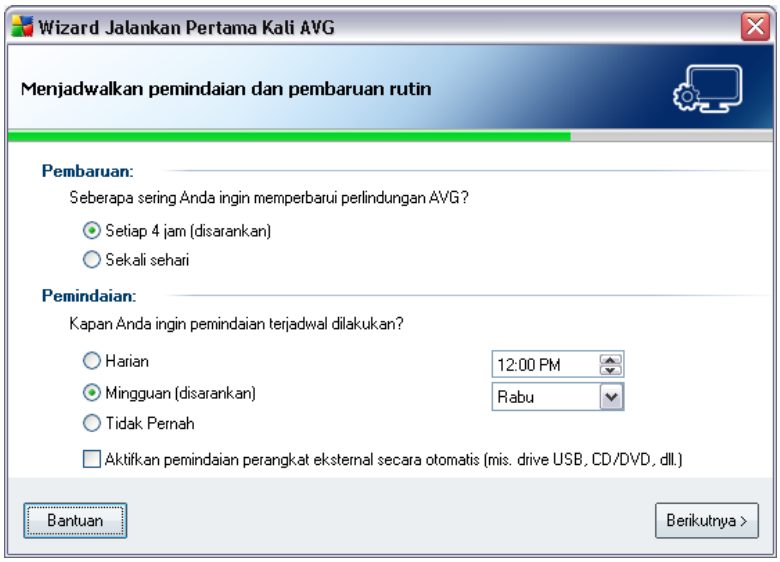
5.10. Menginstal AVG

Dialog ***Menginstal AVG*** menampilkan progres proses instalasi, dan tidak memerlukan campur-tangan:



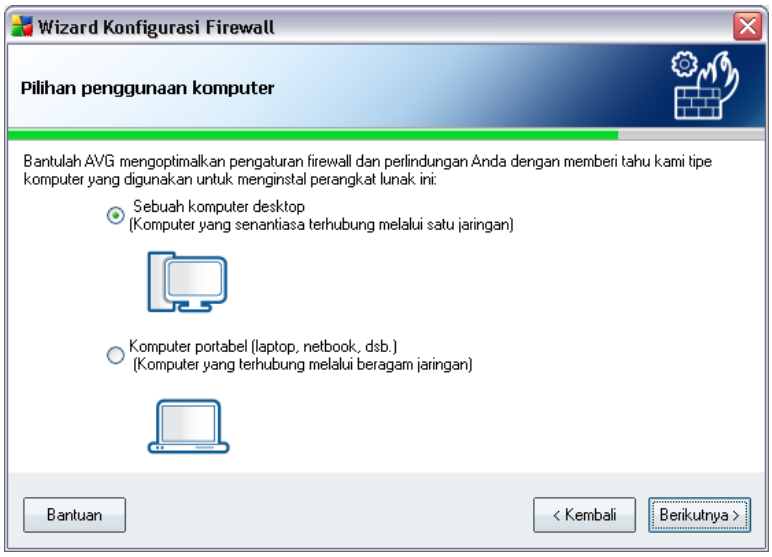
Setelah proses instalasi selesai, Anda akan dialihkan ke dialog berikutnya secara otomatis.

5.11. Menjadwalkan pemindaian dan pembaruan rutin



Dalam dialog ***Jadwalkan pemindaian dan pembaruan rutin*** aturlah interval untuk pemeriksaan aksesibilitas file pembaruan baru, dan tentukan kapan pemindaian terjadwal harus diluncurkan. Disarankan untuk mempertahankan nilai-nilai default. Tekan tombol ***Berikutnya*** untuk melanjutkan.

5.12. Pilihan penggunaan komputer



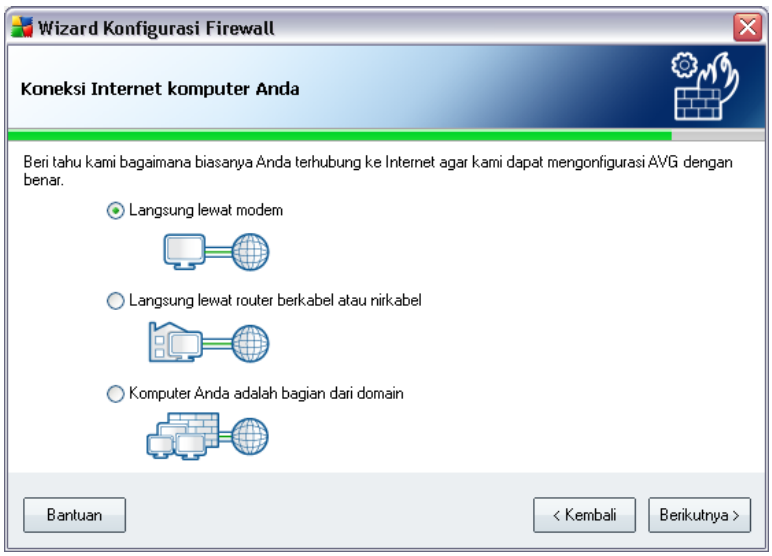
Dalam dialog ini, ***Wizard Konfigurasi Firewall*** akan menanyakan tipe komputer apa yang Anda gunakan. Sebagai contoh, notebook Anda, yang terhubung ke Internet dari banyak lokasi (*bandara, kamar hotel, dll.*) memerlukan aturan keamanan yang lebih ketat daripada komputer yang berada dalam domain (*jaringan perusahaan, dll.*). Berdasarkan tipe pemakaian komputer yang dipilih, aturan default ***Firewall*** akan ditentukan dengan tingkat keamanan berbeda.

Anda mempunyai dua opsi alternatif untuk dipilih:

- ***Komputer dekstop***
- ***Komputer portabel***

Konfirmasikan pilihan Anda dengan menekan tombol ***Berikutnya*** dan melanjutkan ke dialog berikutnya.

5.13. Desain jaringan komputer Anda



Dalam dialog ini, ***Wizard Konfigurasi Firewall*** menanyakan bagaimana komputer terhubung ke Internet. Berdasarkan tipe koneksi yang dipilih, aturan default ***Firewall*** akan ditentukan dengan tingkat keamanan berbeda.

Anda mempunyai tiga opsi alternatif untuk dipilih dari:

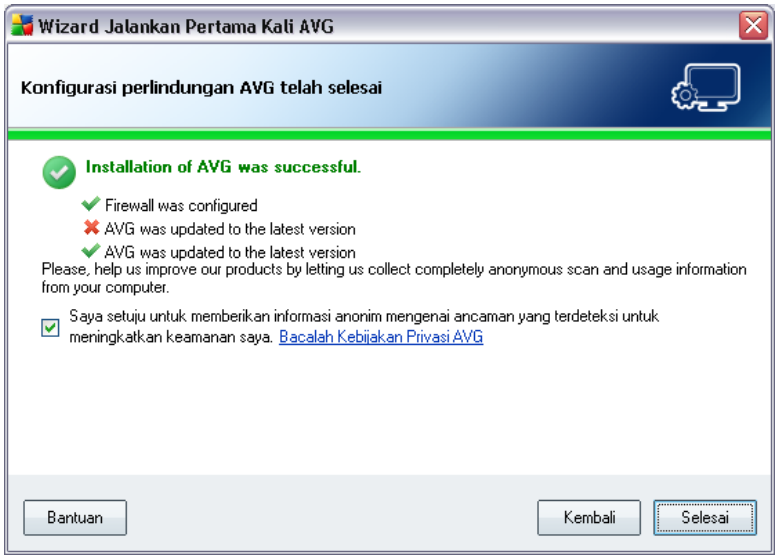
- ***Langsung ke Internet***

- ***Jaringan rumah kecil***
- ***Komputer Anda berada dalam domain***

Pilih tipe koneksi yang paling baik menerangkan koneksi internet komputer Anda.

Konfirmasikan pilihan Anda dengan menekan tombol ***Berikutnya*** dan melanjutkan ke dialog berikutnya.

5.14. Konfigurasi perlindungan AVG selesai



Sekarang **AVG 9 Internet Security** Anda telah dikonfigurasi.

Dalam dialog ini Anda perlu memutuskan apakah akan mengaktifkan opsi pelaporan anonim mengenai eksploit dan situs jahat ke lab virus AVG. Jika ya, maka centang opsi ***Saya setuju untuk memberikan informasi ANONIM tentang ancaman yang terdeteksi untuk meningkatkan keamanan saya*** .

Terakhir, tekan tombol ***Selesai***. Komputer Anda mungkin perlu dihidupkan ulang supaya Anda dapat mulai memakai AVG.

6. Setelah Instalasi

6.1. Pendaftaran Produk

Setelah menyelesaikan instalasi **AVG 9 Internet Security**, daftarkan produk Anda secara online pada situs web AVG (http://www.avg.com/), laman ***Pendaftaran*** (*ikuti petunjuk yang diberikan langsung dalam laman ini*). Setelah pendaftaran, Anda akan mendapatkan akses penuh ke Akun pengguna AVG, Berita pembaruan AVG, dan layanan lain yang disediakan khusus untuk pengguna terdaftar.

6.2. Akses ke Antarmuka Pengguna

Antarmuka Pengguna AVG dapat diakses dengan beberapa cara:

- klik dua kali ikon AVG di baki sistem
- klik dua kali ikon AVG di desktop
- dari menu ***Start/ Programs/AVG 9.0/Antarmuka Pengguna AVG***

6.3. Pemindaian seluruh komputer

Ada kemungkinan risiko bila virus komputer telah terkirim ke komputer Anda sebelum instalasi **AVG 9 Internet Security**. 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***.

6.4. Tes EICAR

Untuk mengonfirmasi apakah **AVG 9 Internet Security** telah diinstal dengan benar, Anda dapat menjalankan tes EICAR.

Tes EICAR adalah metode standar dan benar-benar aman untuk mengetes 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, ***Perisai Web*** akan bereaksi padanya dengan sebuah peringatan. Pemberitahuan ***Perisai Web*** ini menunjukkan AVG telah terinstal pada komputer Anda dengan benar.

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

6.5. Konfigurasi Default AVG

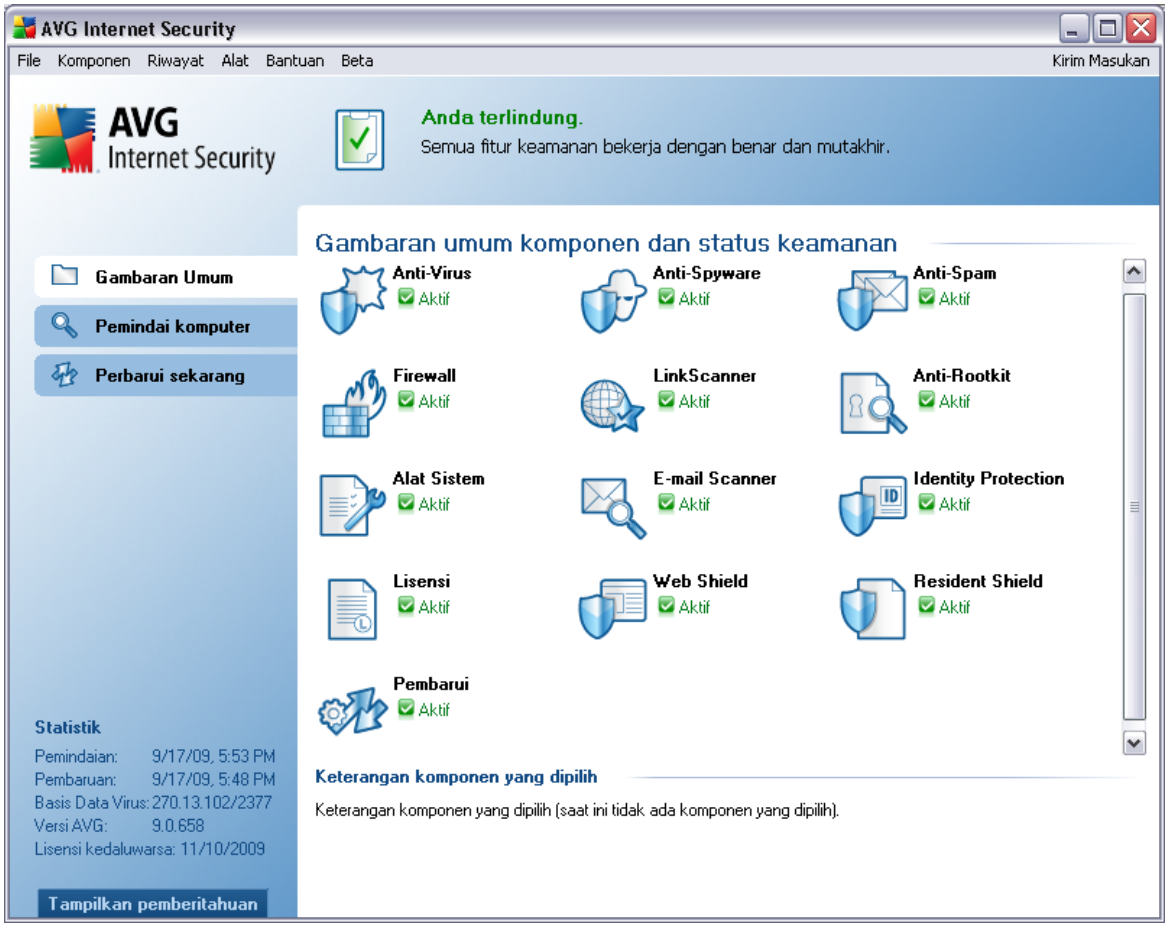
Konfigurasi default (*yakni cara aplikasi diatur tepat setelah instalasi*) **AVG 9 Internet Security** diatur melalui vendor perangkat lunak sehingga semua komponen dan fungsi telah disesuaikan untuk mencapai performa optimal.

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.

7. Antarmuka Pengguna AVG

AVG 9 Internet Security dibuka bersama 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)* menyediakan pada Anda semua data statistik menyangkut operasi program - perincian >>
- ***Ikon Baki Sistem*** *(sudut kanan bawah monitor, pada baki sistem)* menunjukkan status terkini AVG - perincian >>

7.1. Menu Sistem

Menu sistem adalah navigasi standar yang digunakan dalam semua aplikasi Windows. Ia ditempatkan secara horizontal di bagian paling atas pada jendela utama **AVG 9 Internet Security**. Gunakan menu sistem untuk mengakses komponen, fitur dan layanan AVG tertentu.

Menu sistem dibagi ke dalam lima bagian:

7.1.1. File

- ***Keluar*** - menutup antarmuka pengguna **AVG 9 Internet Security** . Walau demikian, aplikasi AVG akan terus berjalan di latar belakang dan komputer Anda tetap terlindungi!

7.1.2. Komponen

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

- ***Gambaran umum sistem*** - beralih ke dialog antarmuka pengguna default berisigambaran umum semua komponen yang terinstal dan statusnya
- ***Anti-Virus*** - membuka halaman default komponen ***Anti-Virus***
- ***Anti-Rootkit*** - membuka halaman default komponen ***Anti-Rootkit***
- ***Anti-Spyware*** - membuka halaman default komponen ***Anti-Spyware***
- ***Firewall*** - membuka halaman default komponen ***Firewall***
- ***LinkScanner*** - membuka halaman default komponen ***LinkScanner***

- ***Alat Sistem*** - membuka halaman default ***Alat Sistem***
- ***Anti-Spam*** - membuka halaman default komponen ***Anti-Spam***
- ***Pemindai E-mail*** - membuka halaman default komponen ***Pemindai E-mail***
- ***Perlindungan ID*** - membuka halaman default komponen ***Perlindungan ID***
- ***Lisensi*** - membuka halaman default komponen ***Lisensi***
- ***Perisai Web*** - membuka halaman default komponen ***Perisai Web***
- ***Perisai Tetap*** - membuka halaman default komponen ***Perisai Tetap***
- ***Pengatur Pembaruan*** - membuka halaman default komponen ***Pengatur Pembaruan***

7.1.3. 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 Perisai Web*** - membuka dialog berisi gambaran umum mengenai ancaman yang terdeteksi oleh ***Perisai Web***
- ***Gudang Virus*** - membuka antarmuka ruang karantina (***Virus Vault***) 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 berisi gambaran umum semua tindakan **AVG 9 Internet Security** yang telah tercatat dalam log.
- ***Firewall*** - membuka antarmuka pengaturan Firewall pada tab ***Log*** berisi gambaran umum terperinci mengenai semua tindakan Firewall

7.1.4. Alat

- ***Pindai komputer*** - beralih ke antarmuka pemindaian AVG dan meluncurkan pemindaian seluruh komputer
- ***Pindai folder yang dipilih*** - beralih keantarmuka pemindaian AVG dan memungkinkan Anda menentukan dalam struktur komputer Anda file dan folder mana yang harus dipindai
- ***Pindai file*** - memungkinkan Anda menjalankan tes saat-diperlukan terhadap satu file yang dipilih dari struktur pada disk Anda
- ***Perbarui*** - secara otomatis meluncurkan proses pembaruan **AVG 9 Internet Security**
- ***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 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 **AVG 9 Internet Security** . Umumnya, disarankan untuk tetap menggunakan pengaturan default aplikasi sebagaimana ditentukan oleh vendor perangkat lunak.
- ***Pengaturan Firewall*** - membuka dialog mandiri untuk konfigurasi lanjutan komponen ***Firewall***

7.1.5. Bantuan

- ***Daftar Isi*** - membuka file bantuan AVG
- ***Dapatkan Bantuan Online*** - membuka situs web AVG (http://www.avg.com/) di laman 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 laman 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.

- ***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***.

7.2. 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 terbaru dari **AVG 9 Internet Security** 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 komponen (opsi *"Abaikan status komponen" tersedia dari menu konteks dengan mengklik kanan pada ikon komponen yang bersangkutan dalam gambaran 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.

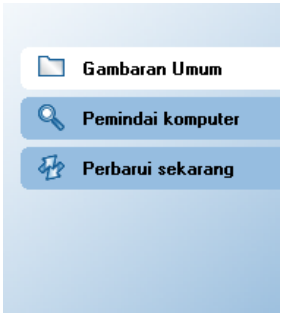
 Ikon merah menunjukkan bahwa AVG dalam status kritis! Satu atau beberapa komponen tidak berfungsi dengan benar dan AVG tidak dapat melindungi komputer Anda. Perhatikan segera untuk memperbaiki masalah yang dilaporkan. Jika Anda tidak dapat memperbaiki sendiri kesalahan tersebut, hubungi tim Dukungan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

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.*

7.3. Tautan Cepat

Tautan cepat *(di bagian kiri jendela 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 >>***
- ***Pemindai komputer*** - gunakan tautan ini untuk membuka antarmuka pemindaian AVG di mana Anda dapat menjalankan tes secara langsung, menjadwalkan pemindaian, atau mengedit parameternya - lihat bab ***Tes AVG >>***
- ***Perbarui sekarang*** - tautan ini membuka antarmuka pembaruan dan meluncurkan proses pembaruan AVG dengan 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 (*gambar 2)*.

7.4. 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

Dalam bagian **AVG 9 Internet Security** ***Gambaran 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*** memindai aplikasi Anda di latar belakang saat Anda menjalankannya - 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 >>
- ***Anti-Rootkit*** mendeteksi berbagai program dan teknologi yang mencoba menyamarkan malware - perincian >>
- ***Alat Sistem*** memberikan ringkasan terperinci mengenai lingkungan AVG - perincian >>
- ***Pemindai E-mail*** memeriksa adanya virus pada semua e-mail yang masuk dan keluar - perincian >>
- ***Perlindungan ID*** - komponen anti-malware fokus untuk mencegah pencuri

identitas mencuri harta digital pribadi Anda - perincian >>

- ***Lisensi*** menyediakan kalimat lengkap Perjanjian Lisensi AVG - perincian >>
- ***Perisai Web*** memindai semua data yang akan diunduh oleh peramban web - perincian >>
- ***Perisai Tetap*** berjalan di latar belakang dan memindai file saat disalin, dibuka atau disimpan - perincian >>
- ***Pengatur Pembaruan*** mengontrol semua pembaruan AVG - perincian >>

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 warna abu-abu pada ikon baki sistem.

7.5. Statistik

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

- ***Terakhir dipindai*** - menyediakan tanggal kapan pemindaian terakhir dilakukan
- ***Terakhir diperbarui*** - menyediakan tanggal kapan pembaruan terakhir diluncurkan
- ***DB Virus*** - memberitahu tentang versi basis data virus yang saat ini terinstal
- ***Versi AVG*** - memberitahu Anda tentang versi AVG yang terinstal *(nomornya dalam format 8.0.xx, di mana 8.0 merupakan versi lini produk, dan xx menyatakan nomor pembuatan)*
- ***Lisensi kedaluwarsa*** - menyediakan tanggal kedaluwarsa lisensi AVG Anda

7.6. Ikon Baki Sistem

Ikon Baki Sistem (*pada Windows taskbar*) menunjukkan status terkini dari **AVG 9 Internet Security** Anda. Ini selalu terlihat pada baki sistem Anda, baik jendela utama AVG Anda sedang dibuka ataupun ditutup.

Jika sepenuh warna , ***Ikon Baki Sistem*** menunjukkan bahwa semua komponen AVG aktif dan berfungsi penuh. Selain itu, ikon baki sistem AVG dapat ditampilkan dalam sepenuh warna jika AVG dalam status kesalahan namun Anda mengetahui situasi ini sepenuhnya dan sengaja memutuskan untuk ***Abaikan status komponen***.

Ikon berwarna abu-abu dengan tanda seru menunjukkan adanya masalah (*komponen 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, kejadian status kesalahan, ...*) melalui jendela sembul yang dibuka 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
- ***Perbarui*** - meluncurkan pembaruan dengan segera

8. Komponen AVG

8.1. Anti-Virus

8.1.1. 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.

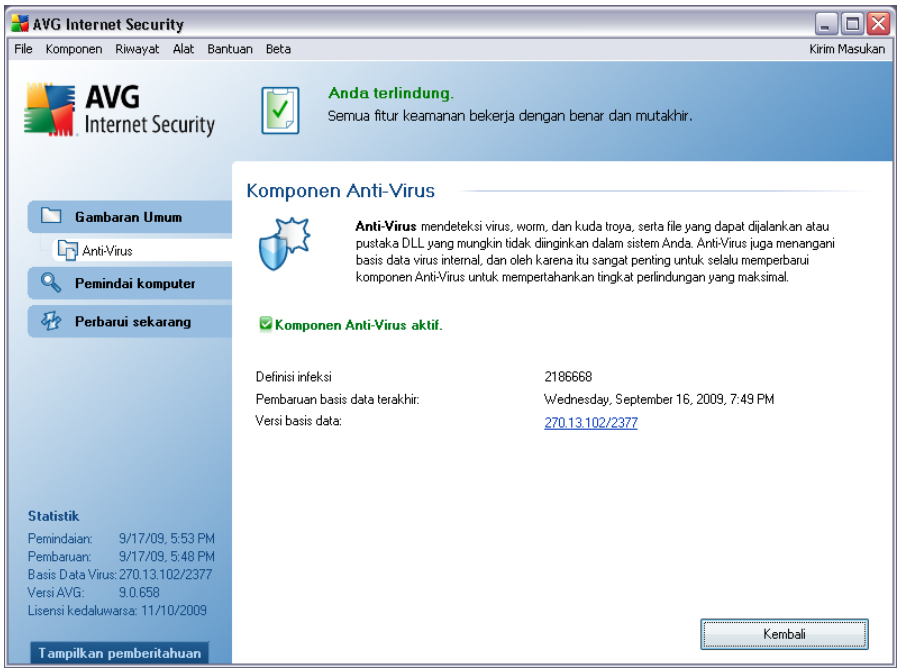
Fitur penting pada perlindungan antivirus adalah karena tidak ada virus dikenal yang dapat berjalan pada komputer!

Sementara satu teknologi mungkin gagal mendeteksi atau mengenali virus, ***Anti-Virus*** mengombinasikan 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.

8.1.2. 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*** :

- ***Definisi infeksi*** - angka yang menyediakan jumlah virus yang didefinisikan dalam versi basis data virus terbaru
- ***Pembaruan basis data terbaru*** - menentukan kapan dan pukul berapa basis data virus diperbarui
- ***Versi basis data*** - menentukan nomor versi basis data virus terbaru, dan nomor 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).

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.*

8.2. Anti-Spyware

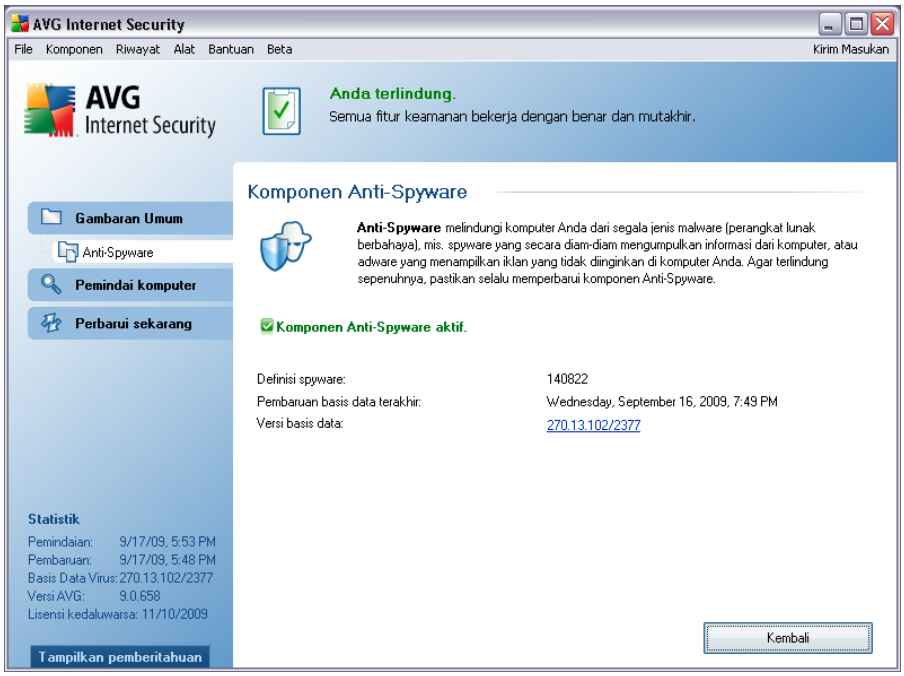
8.2.1. Prinsip-Prinsip Anti-Spyware

Spyware biasanya didefinisikan sebagai tipe malware, yaitu perangkat lunak, yang mengumpulkan informasi dari komputer pengguna tanpa sepengetahuan atau persetujuan pengguna. Beberapa aplikasi spyware mungkin juga terinstal saat pembelian dan seringkali berisi iklan, jendela yang muncul atau tipe perangkat lunak tidak menyenangkan lainnya.

Saat ini, sumber infeksi paling umum adalah situs web dengan konten yang mungkin berbahaya. Metode transmisi lainnya, seperti e-mail atau transmisi melalui worm dan virus juga lazim. Perlindungan paling penting adalah menggunakan pemindai latar belakang yang selalu aktif, ***Anti-Spyware***, yang bekerja seperti 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 **AVG 9 Internet Security** 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.

8.2.2. Antarmuka Anti-Spyware



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

- ***Definisi spyware*** - angka yang menyediakan jumlah contoh spyware yang didefinisikan dalam versi basis data spyware terbaru
- ***Pembaruan basis data terbaru*** - menentukan kapan dan pukul berapa basis data spyware diperbarui
- ***Versi basis data*** - menentukan nomor versi basis data spyware terbaru, dan nomor 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).

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.*

8.3. Anti-Spam

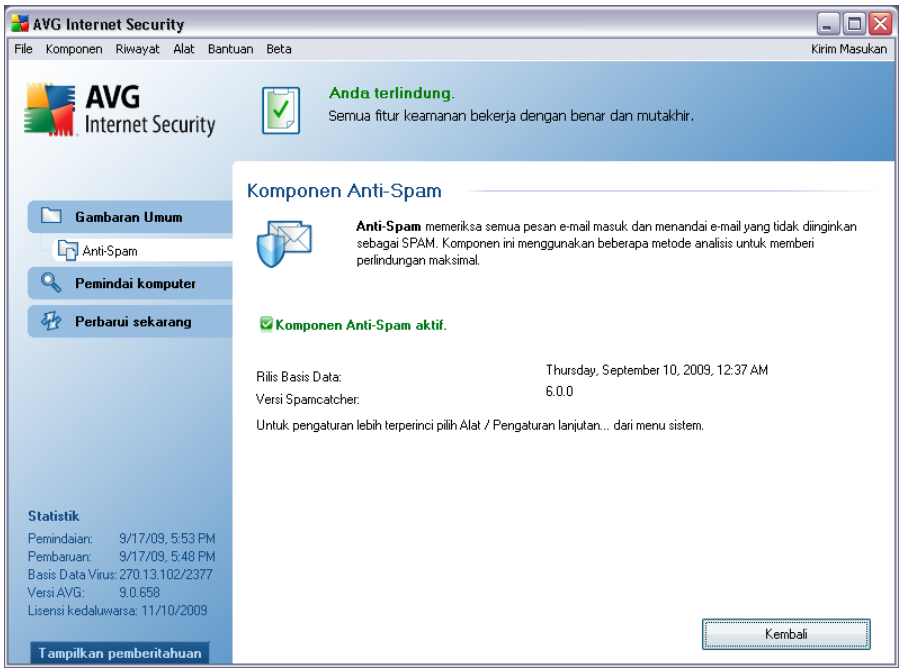
Spam adalah e-mail yang tidak diundang, hampir semuanya mengiklankan produk atau layanan yang dikirimkan massal ke sejumlah besar alamat e-mail sekaligus, memenuhi kotak surat penerima . E-mail komersial resmi yang telah disetujui oleh konsumen tidak termasuk spam. Spam tidak hanya mengganggu, tetapi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

8.3.1. Prinsip-Prinsip Anti-Spam

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 basis data umum server RBL (*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*).

8.3.2. Antarmuka Anti-Spam



Dalam dialog komponen ***Anti-Spam*** Anda akan menemukan teks singkat yang menjelaskan fungsionalitas komponen, dan informasi mengenai status terbarunya (*komponen Anti-Spam aktif.*), 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

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*).

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.*

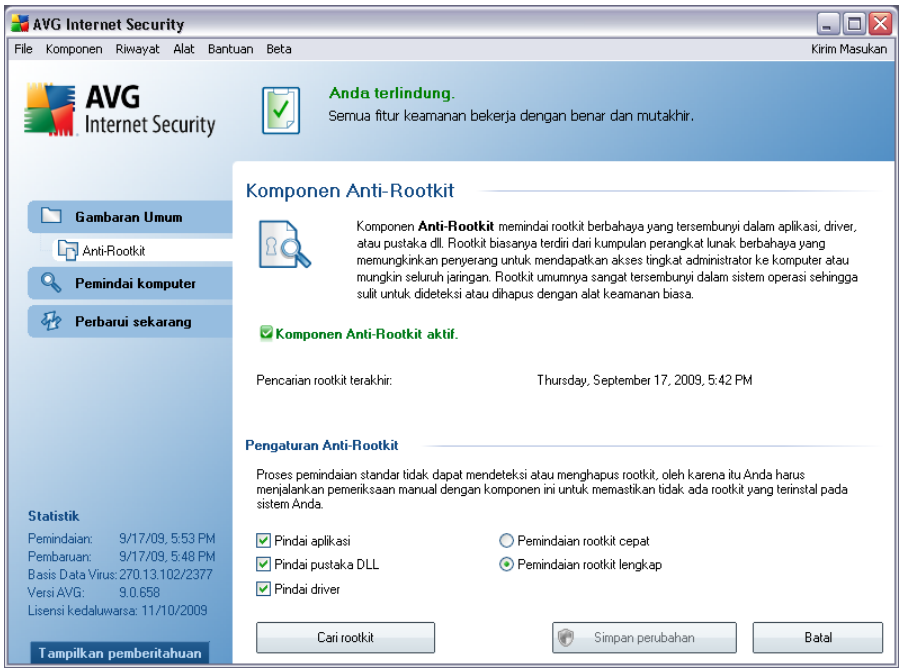
8.4. Anti-Rootkit

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.

8.4.1. 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.

8.4.2. Antarmuka Anti-Rootkit



Antarmuka pengguna ***Anti-Rootkit*** memberikan keterangan singkat mengenai fungsionalitas komponen, memberi tahu status komponen saat ini (*komponen Anti-Rootkit aktif.*) juga menampilkan informasi mengenai waktu terakhir tes ***Anti-Rootkit*** diluncurkan.

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*** - hanya memindai folder sistem (*biasanya c:\Windows*)
- ***Pemindaian rootkit lengkap*** – memindai semua disk yang dapat diakses

kecuali A: dan B:

Tersedia 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)
- ***Batalkan*** - tekan tombol ini untuk kembali ke ***antarmuka pengguna AVG*** default (gambaran umum komponen) tanpa menyimpan perubahan yang telah Anda buat

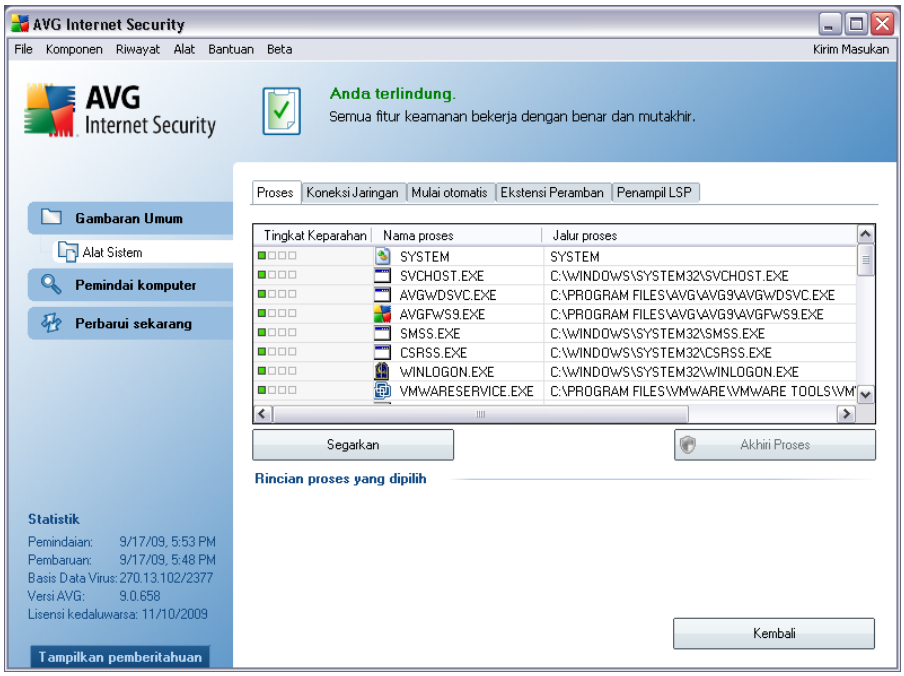
8.5. Alat Sistem

Alat Sistem merujuk pada alat yang menyediakan ringkasan terperinci mengenai lingkungan **AVG 9 Internet Security** . 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!

8.5.1. Proses



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

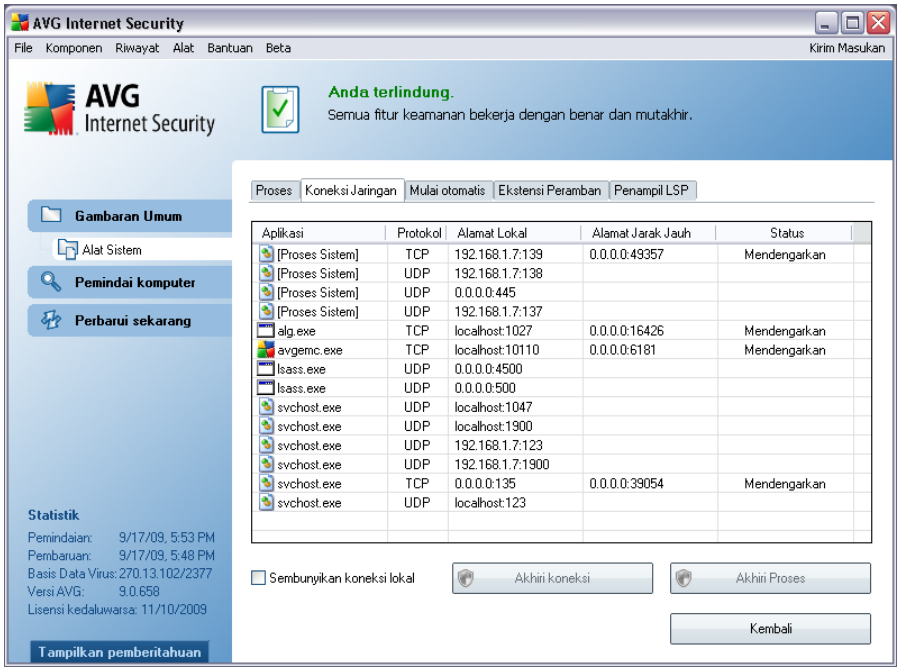
- ***Tingkat Keseriusan*** –identifikasi grafis dari keseriusan proses yang bersangkutan pada skala empat-tingkat dari kurang penting () hingga kritis ( )
- ***Nama proses*** - nama proses yang berjalan
- ***Jalur*** - jalur fisik ke proses yang berjalan
- ***Jendela*** - jika berlaku, menunjukkan nama jendela aplikasi
- ***Internet*** - menunjukkan apakah proses yang berjalan juga terhubung ke Internet (*Ya/Tidak*)
- ***Layanan*** - menunjukkan apakah proses yang berjalan adalah layanan (*Ya/Tidak*)
- ***PID*** - nomor identifikasi proses merupakan pengenal 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!***
- ***Tombol Kembali***- akan mengembalikan Anda ke ***antarmuka pengguna AVG*** default (gambaran umum komponen).

8.5.2. Koneksi Jaringan



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

- ***Aplikasi*** - nama aplikasi yang berhubungan dengan koneksi. Informasi ini hanya tersedia di Windows XP.

- ***Protokol*** - tipe protokol transmisi yang digunakan untuk koneksi:
    - TCP - protokol yang digunakan bersama dengan Internet Protocol (IP) untuk mengirim informasi melalui Internet
    - UDP - alternatif untuk protokol TCP
- ***Alamat lokal*** - alamat IP dari komputer lokal dan nomor port yang digunakan
- ***Alamat jarak jauh*** - alamat IP dari komputer jarak jauh dan nomor port yang dihubungi. Jika memungkinkan, nama host komputer jarak jauh juga akan dicari.
- ***Status*** - menunjukkan status yang paling memungkinkan saat ini (*Terhubung, Server harus menutup, Dengar, Aktif tutup selesai, Pasif tutup, Aktif tutup*)

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

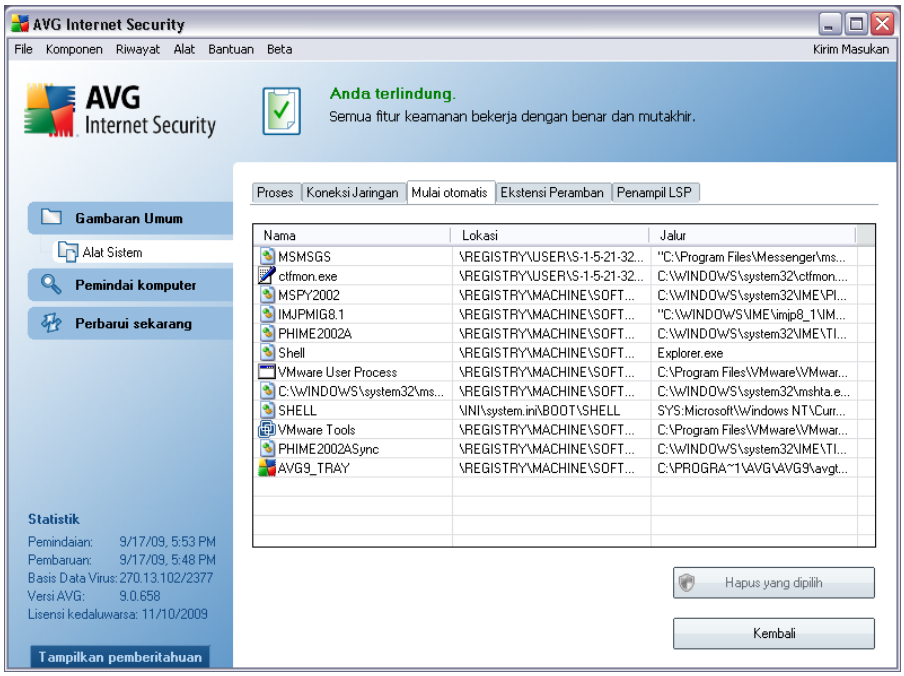
Tombol kontrol

Tombol kontrol yang tersedia adalah:

- ***Akhiri Koneksi*** - menutup satu atau beberapa koneksi yang dipilih dalam daftar
- ***Akhiri Proses*** - menutup satu atau beberapa aplikasi yang berhubungan dengan koneksi yang dipilih dalam daftar (*tombol ini hanya tersedia pada sistem yang menjalankan Windows XP*)
- ***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!

8.5.3. Mulai otomatis

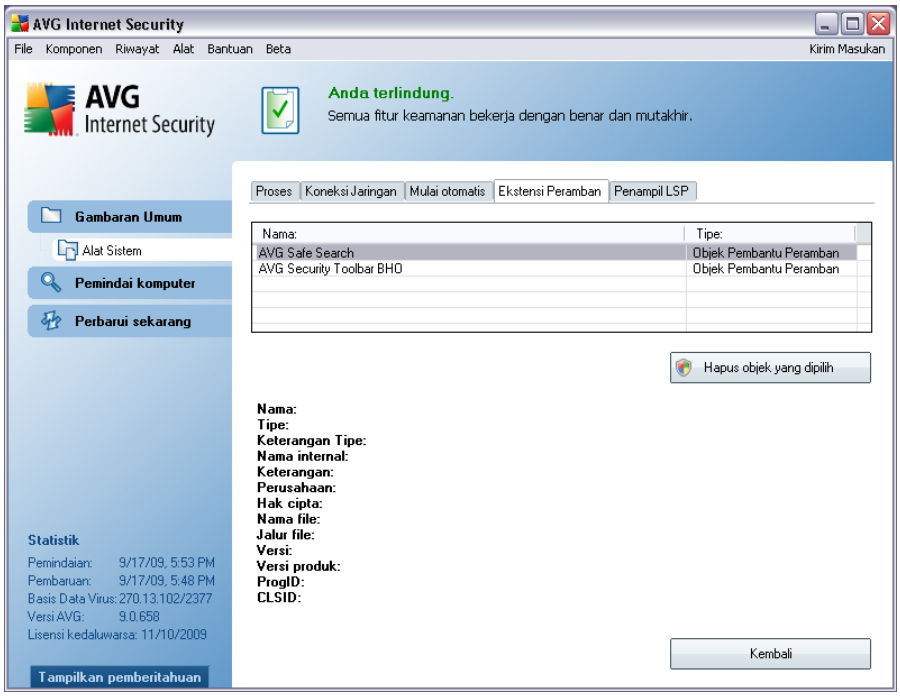


Dialog ***Mulai Otomatis*** menampilkan daftar semua aplikasi yang dijalankan selama menjalankan ulang sistem Windows. Sering sekali, beberapa aplikasi malware menambahkan diri mereka sendiri ke entri register start-up secara otomatis.

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!

8.5.4. 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.

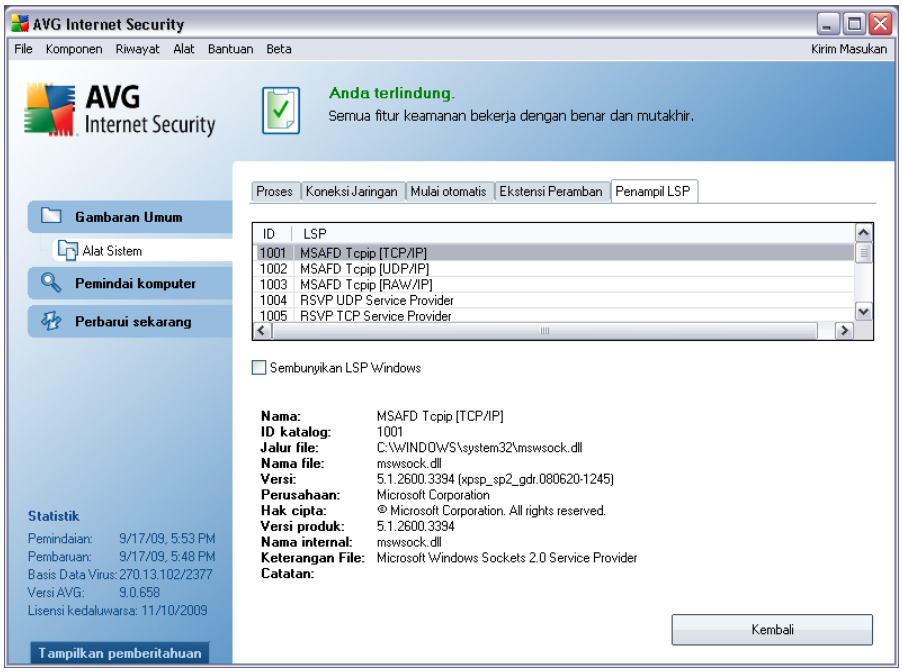
Tombol kontrol

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!***

- ***Tombol Kembali***- akan mengembalikan Anda ke ***antarmuka pengguna AVG*** default (gambaran umum komponen)

8.5.5. 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*).

8.6. 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 dikofigurasi 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.*

8.6.1. 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
- Menyimpan arsip semua profil dan pengaturan yang telah ditentukan
- Mengganti profil secara otomatis saat menghubungkan ke berbagai jaringan, atau menggunakan beberapa macam adaptor jaringan

8.6.2. 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***:
    - ***Komputer saat bepergian*** – 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.

- ***Komputer dalam 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 tunggal.

- ***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".

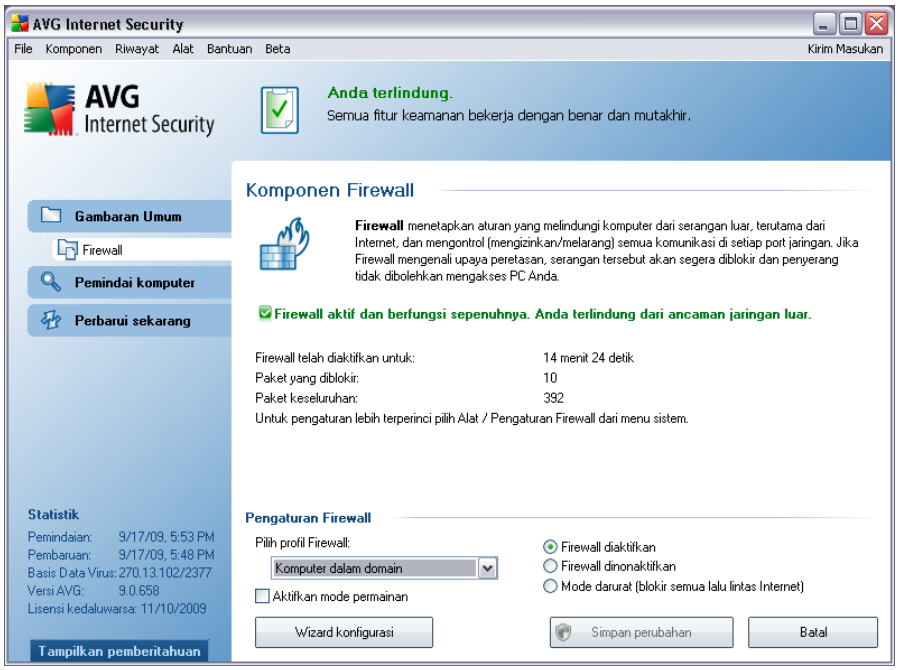
Pengalihan profil

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.

8.6.3. Antarmuka Firewall



Antarmuka ***Firewall***memberikan beberapa informasi dasar mengenai fungsionalitas komponen, dan gambaran umum singkat tentang 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

Konfigurasi komponen dasar

- ***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*** - Centang opsi ini untuk memastikan bahwa bila aplikasi layar penuh dijalankan (permainan, presentasi PowerPoint, dll.) ***Firewall*** tidak akan menampilkan dialog untuk bertanya apakah Anda ingin memperbolehkan atau memblokir komunikasi dari 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.

- ***Status Firewall***:

    - ***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 mematikan ***Firewall*** sama sekali, semua lalu lintas jaringan diperbolehkan namun tidak diperiksa!

    - ***Mode darurat (memblokir semua lalu lintas Internet)*** - pilih opsi ini untuk memblokir semua lalu lintas pada setiap port jaringan tunggal; ***Firewall*** tetap berjalan namun semua lalu lintas jaringan dihentikan

Perhatikan: *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* ***File / Pengaturan Firewall*** *dan edit konfigurasi Firewall dalam dialog* ***Pengaturan Firewall*** *yang baru dibuka.*

Tombol kontrol

- ***Wizard konfigurasi***- tekan tombol ini untuk berpindah ke dialognya (*digunakan dalam proses instalasi*) yang bernama ***Pilihan Penggunaan Komputer*** di mana Anda dapat menentukan konfigurasi komponen ***Firewall***

- ***Simpan perubahan*** - tekan tombol ini untuk menyimpan dan menerapkan semua perubahan yang dibuat dalam dialog ini

- ***Batalkan*** - tekan tombol ini untuk kembali ke gambaran umum komponen antarmuka pengguna AVG (*default*)

8.7. 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-email perusahaan dan memasang filter anti-spam, dsb, untuk mengurangi risiko tersebut.

8.7.1. Prinsip-Prinsip Pemindai E-mail

Komponen ***Pemindai E-mail*** memindai e-mail masuk/keluar secara otomatis. Anda dapat menggunakannya dengan klien e-mail yang tidak memiliki plugin sendiri dalam AVG (*misalnya Outlook Express, Mozilla, Incredimail, dll.*).

Selama instalasi AVG 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*).

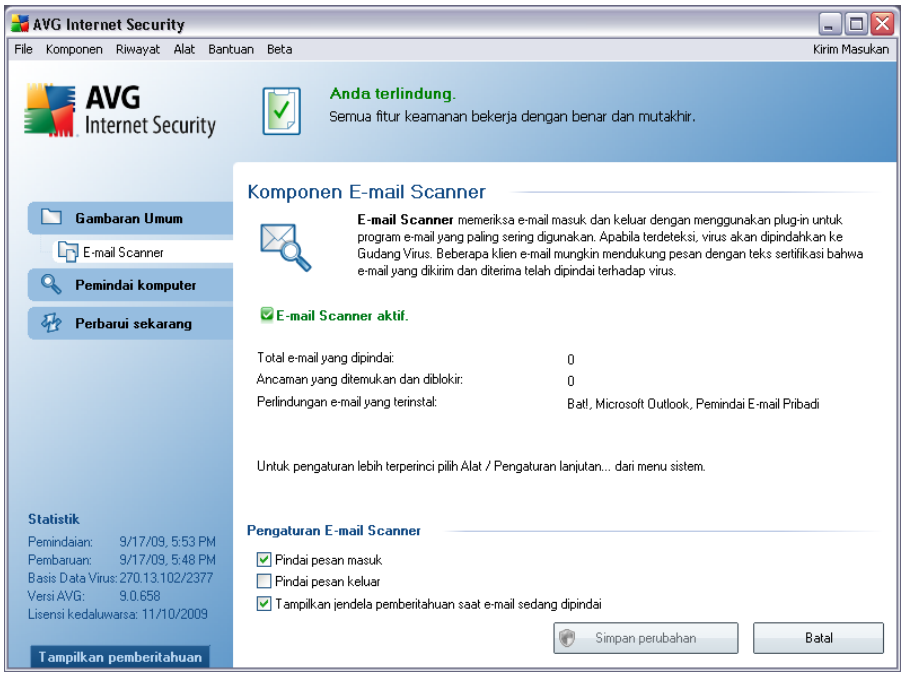
Pemindai E-mail berfungsi sebagai antarmuka antara klien e-mail dan server e-mail di Internet.

- ***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!*

8.7.2. Antarmuka Pemindai E-mail



Dalam dialog komponen ***Pemindai E-mail*** Anda dapat menemukan teks singkat yang menerangkan fungsionalitas komponen, dan informasi mengenai status terbarunya (*Pemindai E-mail aktif.*), dan statistik berikut:

- ***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

Konfigurasi komponen dasar

Di bagian bawah dialog, Anda dapat menemukan bagian bernama ***Pengaturan Pemindai E-mail*** di mana Anda dapat mengatur 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 semua e-mail yang terkirim dari akun Anda harus dipindai virusnya. Secara default, item ini tidak aktif.

- *Tampilkan ikon pemberitahuan saat e-mail sedang dipindai* - selama pemindaian, komponen ***Pemindai E-mail*** akan menampilkan dialog pemberitahuan yang memberitahukan mengenai tugas sesungguhnya yang sedang diproses oleh komponen (*menghubungkan ke server, mengunduh pesan, memindai pesan, ...*). Opsi ini diaktifkan dan tidak dapat diedit.

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

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

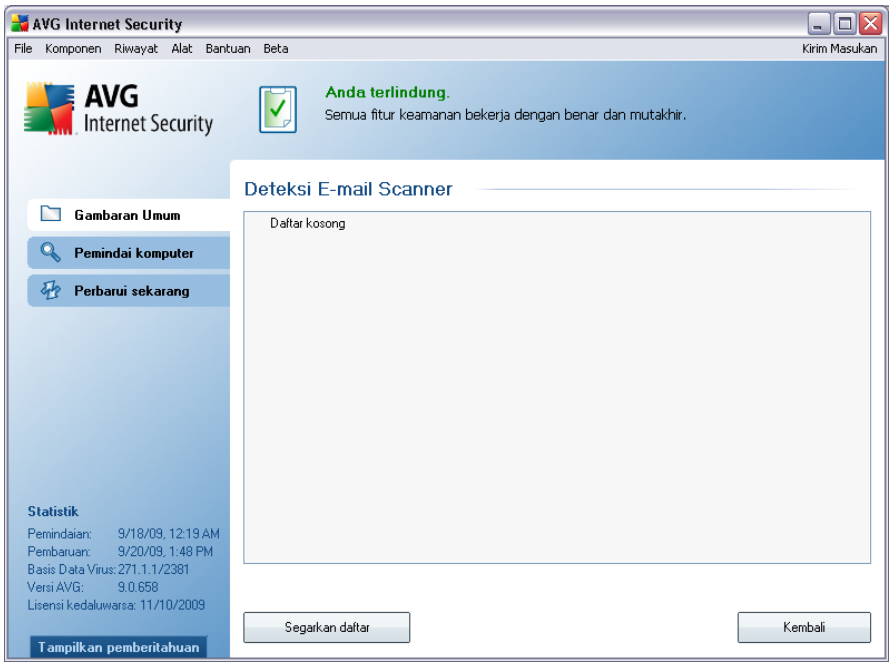
Tombol kontrol

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

- ***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)

8.7.3. Deteksi Pemindai E-mail



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

- ***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
- ***Tombol Kembali***- akan mengembalikan Anda ke ***antarmuka pengguna AVG*** default (gambaran umum komponen)

8.8. Perlindungan ID

AVG Identity Protectionadalah 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.

8.8.1. Prinsip-Prinsip Perlindungan ID

AVG Identity Protectionmerupakan 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.

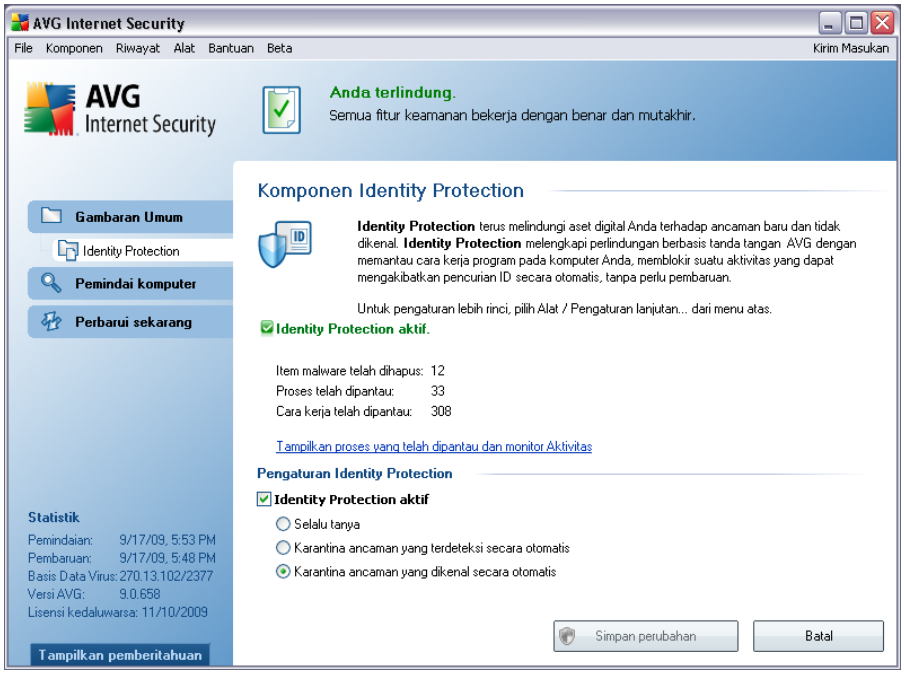
Kami sangat menyarankan agar Anda menginstal kedua aplikasi AVG Anti-Virus dan AVG Identity Protection, untuk mendapatkan perlindungan penuh bagi PC Anda.

8.8.2. Antarmuka Perlindungan ID

Antarmuka komponen ***Perlindungan Identitas***memberikan keterangan singkat mengenai fungsionalitas dasar komponen, statusnya (*AVG Identity Protection aktif dan fungsional sepenuhnya.*) 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



Konfigurasi komponen dasar

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

- ***Perlindungan Identitas aktif*** - (*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 komponen ***Perlindungan Identitas*** jika ada deteksi aktivitas yang mencurigakan:

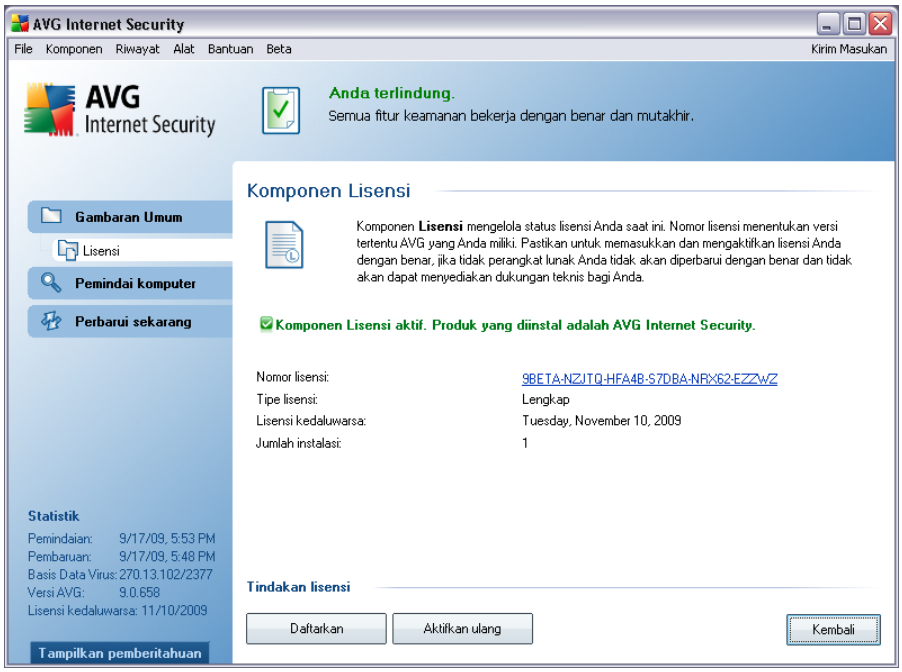
- ***Selalu tanya*** - jika aplikasi dideteksi sebagai malware, Anda akan ditanya apakah ia harus diblokir
- ***Karantina ancaman yang terdeteksi secara otomatis*** - semua aplikasi yang terdeteksi sebagai malware akan diblokir secara otomatis
- ***Karantina ancaman yang dikenal secara otomatis*** -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

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
- ***Batalkan*** - tekan tombol ini untuk kembali ke antarmuka pengguna AVG default (gambaran umum komponen)

8.9. Lisensi



Dalam antarmuka komponen***Lisensi*** Anda akan menemukan teks singkat yang menjelaskan fungsionalitas komponen, dan informasi mengenai status terbarunya(*komponen Lisensi aktif.*), dan informasiberikut:

- ***Nomor lisensi*** - menyediakan bentuk persis dari nomor lisensi Anda. 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*** - menetapkan tipe produk yang diinstal.

- ***Lisensi kedaluwarsa*** - tanggal ini menentukan masa berlaku lisensi Anda. Jika Anda ingin terus menggunakan **AVG 9 Internet Security** 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 **AVG 9 Internet Security**.

Tombol kontrol

- ***Daftar*** - menghubungkan ke laman 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*).

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

8.10. Link Scanner

8.10.1. Prinsip-Prinsip Link Scanner

Komponen ***LinkScanner***memberikan perlindungan terhadap situs web, yang dirancang untuk menginstal malware ke dalam komputer Anda melalui peramban web atau pluginnya. Teknologi ***LinkScanner*** terdiri atas dua fitur, ***AVG Search-Shield*** dan ***AVG Active Surf-Shield***:

- ***AVG Search-Shield*** berisi daftar situs web (*alamat URL*) yang diketahui berbahaya. Saat menelusuri Google, Yahoo!, MSN, atau Baidu, semua hasil telusur diperiksa sesuai dengan daftar ini dan ikon keputusan ditampilkan (*untuk hasil telusur di Yahoo! hanya ikon keputusan "situs web terinfeksi" yang ditampilkan*). Demikian pula jika Anda mengetikkan alamat langsung ke peramban, mengklik tautan pada situs web atau mis. dalam e-mail Anda, ia akan diperiksa secara otomatis dan diblokir bila perlu.

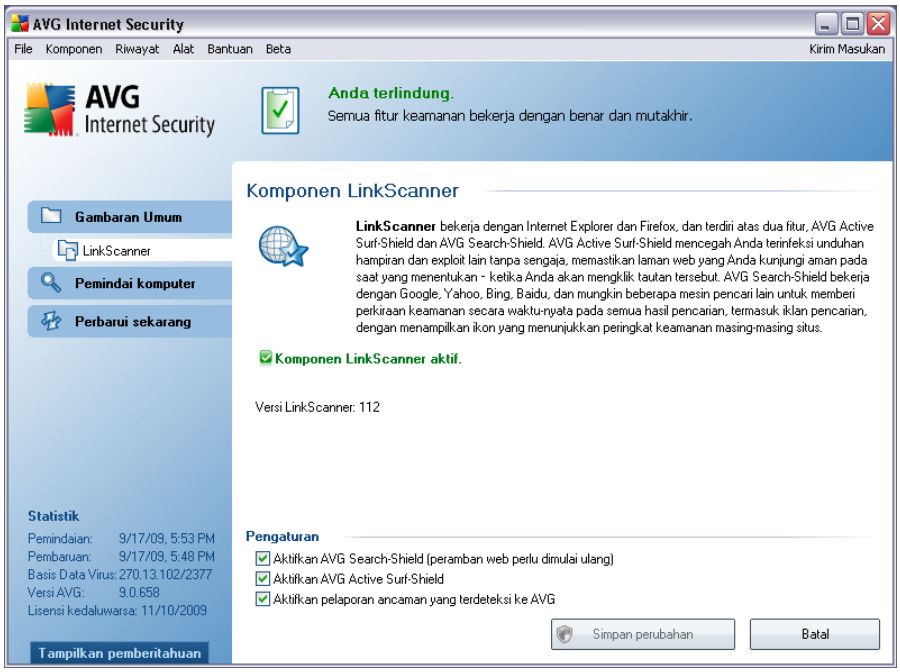
- ***AVG Active Surf-Shield*** memindai konten situs web yang Anda kunjungi, apa pun alamat situs webnya. Bahkan jika situs web tertentu tidak terdeteksi oleh ***AVG Search Shield*** (*(mis. bila situs web jahat baru dibuat, atau situs web yang sebelumnya bersih sekarang berisi malware*), akan terdeteksi dan diblokir oleh ***AVG Active Surf-Shield*** begitu Anda mencoba mengunjunginya.

Catatan: *AVG LinkScanner tidak ditujukan untuk platform server!*

8.10.2. Antarmuka Link Scanner

Komponen ***LinkScanner*** terdiri atas dua bagian yang dapat Anda aktifkan/ nonaktifkan dalam antarmuka ***komponen LinkScanner***:

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



Di bagian bawah dialog Anda dapat menemukan beberapa opsi:

- ***Aktifkan AVG Search-Shield*** - (*diaktifkan secara default*): ikon pemberitahuan saran penelusuran yang dijalankan di Google, Yahoo atau MSN setelah sebelumnya memeriksa konten situs yang dihasilkan oleh mesin telusur.

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

- ***Aktifkan pelaporan ancaman yang terdeteksi ke AVG*** - centang item ini agar dapat melaporkan kembali eksploit dan situs jahat yang ditemukan oleh pengguna melalui ***Safe Surf*** atau ***Safe Search*** untuk memasok basis data yang mengumpulkan informasi mengenai aktivitas merusak pada web.

8.10.3. AVG Search-Shield

Bila melakukan penelusuran di Internet dengan mengaktifkan ***AVG Search-Shield***, semua hasil telusur akan dihasilkan dari mesin telusur paling populer: Yahoo!, Google, MSN, dsb. akan dievaluasi untuk mengetahui adanya tautan yang berbahaya atau mencurigakan. Dengan memeriksa tautan ini dan menandainya sebagai tautan jahat, ***AVG Security Toolbar*** memperingatkan Anda sebelum mengklik tautan berbahaya atau mencurigakan tersebut, sehingga Anda bisa yakin hanya menuju ke situs web yang aman.

Saat tautan dievaluasi pada laman 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:

Laman tertaut aman (*dengan mesin telusur Yahoo! dalam AVG Security Toolbar ikon ini tidak akan ditampilkan!*).

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

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

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

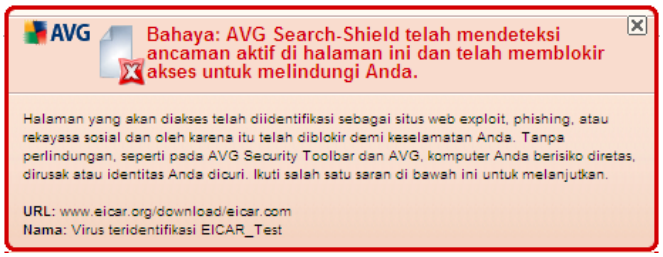
Laman tertaut tidak dapat diakses, sehingga tidak dapat dipindai.

Melayangkan kursor di atas masing-masing ikon peringkat akan menampilkan perincian tentang tautan tertentu yang meragukan. Informasi meliputi perincian tambahan mengenai ancaman (jika ada), alamat IP tautan dan waktu pemindaian laman tersebut oleh AVG:

8.10.4. AVG Active Surf-Shield

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

Jika Anda menemukan situs web jahat, dalam peramban web ***AVG Security Toolbar*** akan memperingatkan Anda dengan layar seperti ini:



Memasuki situs web seperti ini sangat berisiko dan tidak disarankan!

8.11. Perisai Web

8.11.1. Prinsip-Prinsip Perisai Web

Perisai Web adalah sebuah tipe perlindungan menetap waktu nyata; ia memindai isi laman web yang dikunjungi (dan mungkin file yang dimasukkan di dalamnya) bahkan sebelum laman ditampilkan di peramban web Anda atau diunduh ke komputer.

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

Catatan: *Perisai Web AVG tidak ditujukan untuk platform server!*

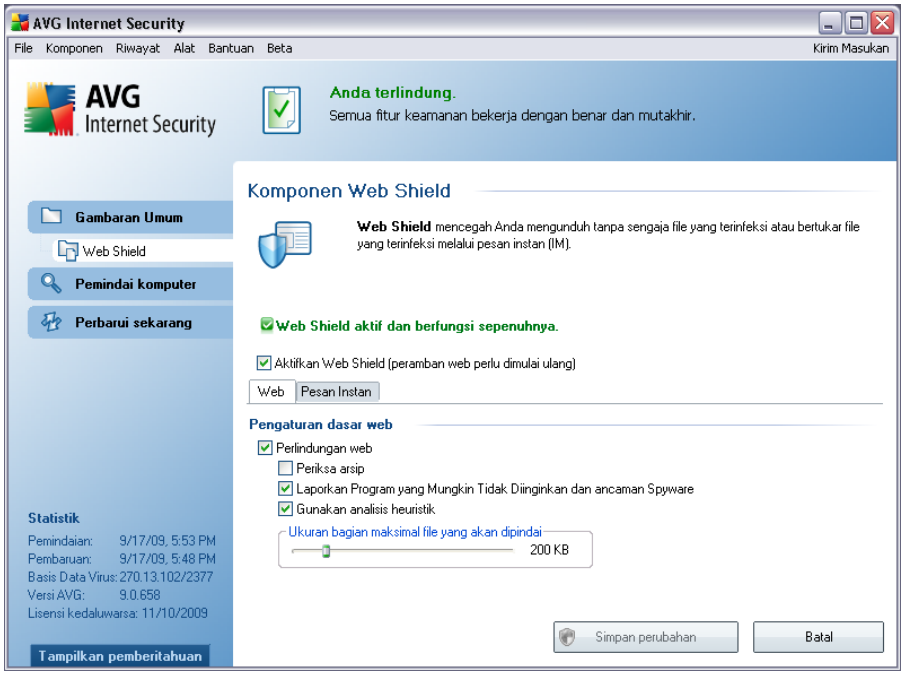
8.11.2. Antarmuka Perisai Web

Antarmuka komponen ***Perisai Web*** menerangkan cara kerja tipe perlindungan ini. Lebih jauh Anda dapat menemukan informasi tentang status terkini komponen (*Perisai Web aktif dan berfungsi penuh.*). Di bagian bawah dialog, Anda akan menemukan opsi pengeditan dasar untuk fungsionalitas komponen ini.

Konfigurasi komponen dasar

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

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

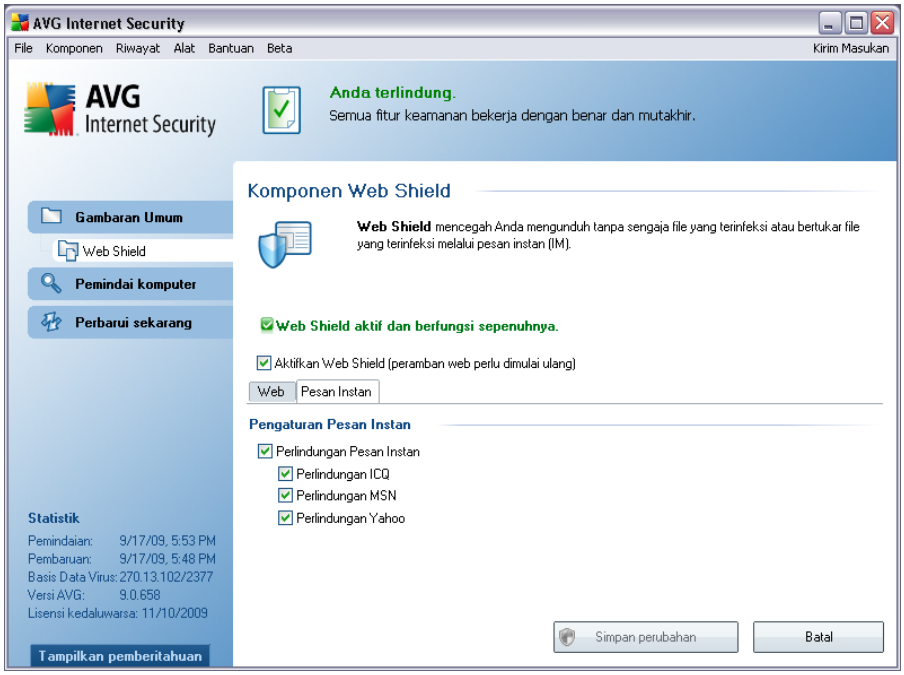


o ***Perlindungan web*** - opsi ini mengonfirmasi bahwa ***Perisai Web*** harus melakukan pemindaian isi laman www. Asalkan opsi ini diaktifkan (*secara default*), Anda dapat mengaktifkan/menonaktifkan item ini:

- ***Periksa arsip*** - memindai isi arsip yang mungkin telah dimasukkan di laman www yang akan ditampilkan.
- ***Laporkan Program yang Mungkin Tidak Diinginkan*** - memindai program yang mungkin tidak diinginkan (*program yang dapat dijalankan, yang dapat berjalan sebagai spyware atau adware*) yang dimasukkan di laman www untuk ditampilkan
- ***Gunakan analisis heuristik*** - memindai isi laman yang akan ditampilkan, menggunakan metode analisis heuristik *(emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual - lihat bab Prinsip-Prinsip Anti-Virus*)
- ***Ukuran file maksimum yang akan dipindai*** - jika file yang disertakan ada di laman yang ditampilkan, Anda juga dapat memindai isinya bahkan sebelum diunduh ke komputer Anda. Namun, pemindaian file besar akan memakan waktu lama dan laman web mungkin diunduh jauh lebih pelan. Anda dapat menggunakan bilah geser untuk menetapkan ukuran maksimum file yang masih

akan dipindai dengan ***Perisai Web***. Sekalipun file yang telah diunduh lebih besar dari yang ditetapkan, sehingga tidak akan dipindai dengan ***Perisai Web***, Anda masih terlindungi: seandainya file terinfeksi, ***Perisai Tetap*** akan segera mendeteksinya.

- ***Pesan Instan*** - memungkinkan Anda mengedit pengaturan komponen yang menyangkut pemindaian pesan instan (*misalnya ICQ, MSN Messenger, Yahoo ...*).



  - Perlindungan Pesan Instan - centang item ini jika Anda ingin agar Perisai Web memverifikasi apakah komunikasi online sudah bebas-virus. Asalkan opsi ini diaktifkan, Anda dapat menetapkan lebih jauh aplikasi pesan instan yang ingin Anda kontrol - saat ini **AVG 9 Internet Security** mendukung aplikasi ICQ, MSN, dan Yahoo.

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

Tombol kontrol

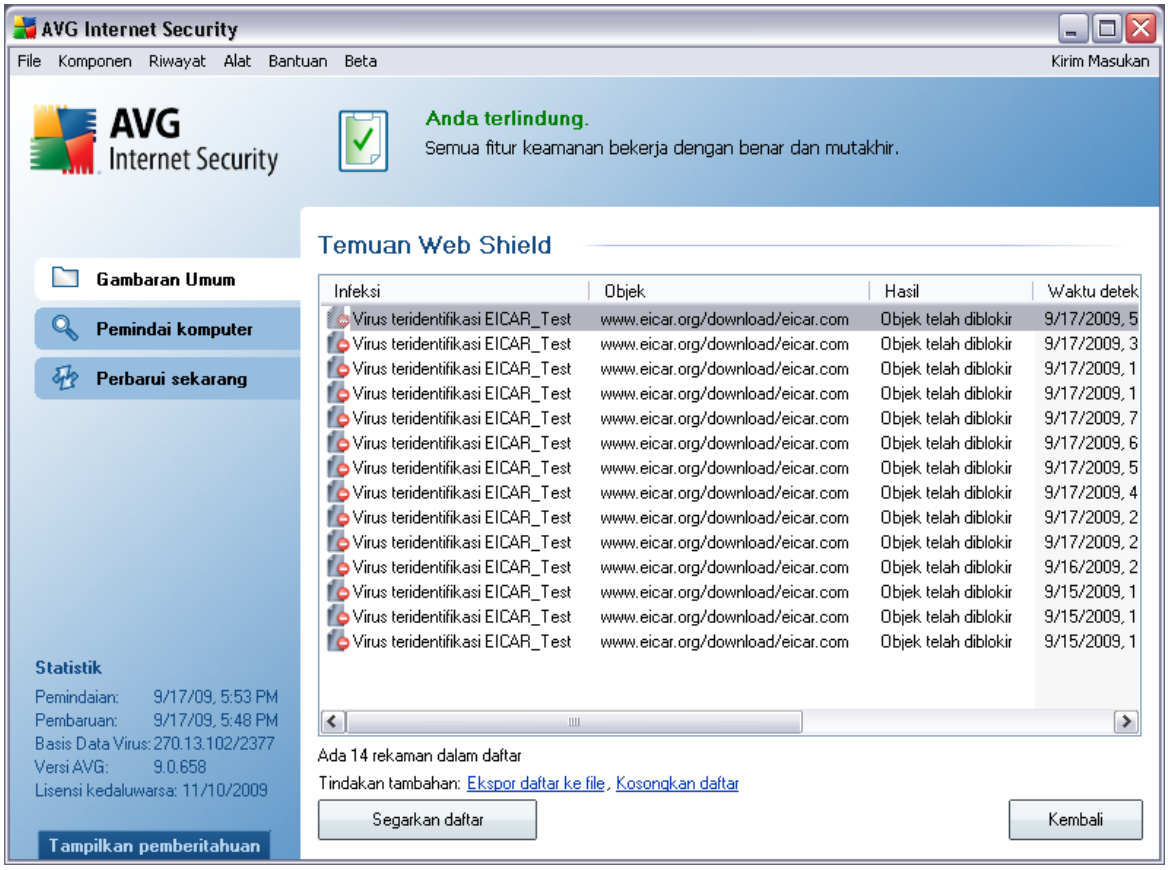
Tombol kontrol yang tersedia dalam antarmuka ***Perisai Web*** adalah sebagai berikut:

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

8.11.3. Deteksi Perisai Web

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

Halaman web yang dicurigai tidak akan dibuka dan deteksi ancaman akan direkam pada log dalam daftar ***Temuan Perisai Web*** - gambaran umum ancaman yang terdeteksi ini dapat diakses melalui menu sistem ***Riwayat / Temuan Perisai Web***.



Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Infeksi***- keterangan (*bahkan mungkin nama*) objek yang terdeteksi
- ***Objek*** - sumber objek (*laman 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 ***Perisai Web***. Tombol ***Kembali*** akan mengembalikan Anda ke ***antarmuka pengguna AVG*** default (gambaran umum komponen).

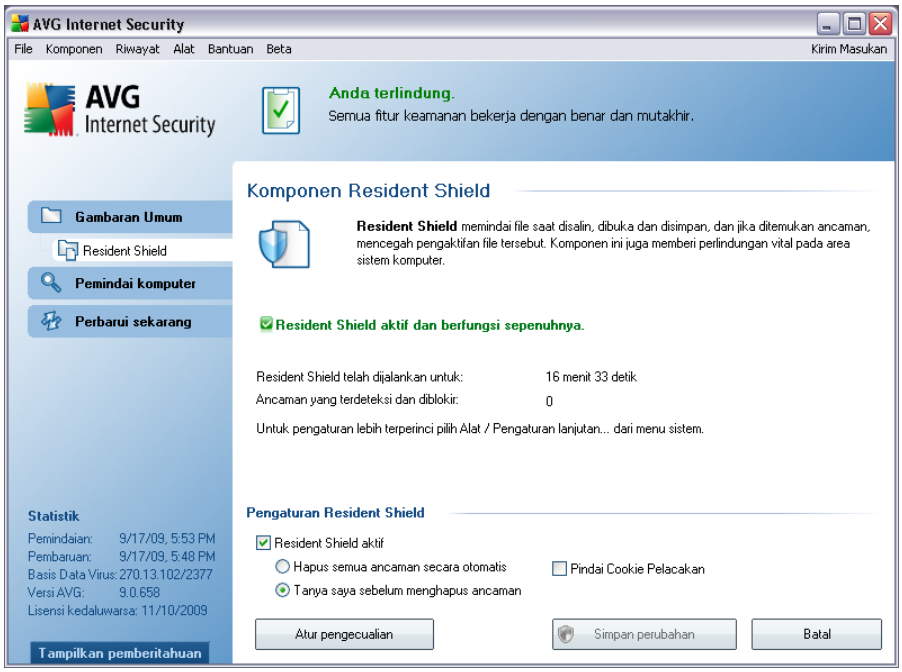
8.12. Perisai Tetap

8.12.1. 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*** sedang dimuat ke dalam memori komputer Anda selama menghidupkan ulang sistem.

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

8.12.2. Antarmuka Perisai Tetap



Di samping gambaran umum mengenai data statistik paling penting dan informasi mengenai status komponen saat ini (*Perisai Tetap aktif dan berfungsi penuh*), antarmuka ***Perisai Tetap*** juga menyediakan beberapa opsi pengaturan komponen dasar. Statistik tersebut adalah sebagai berikut:

- ***Perisai Tetap telah aktif 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*)

Konfigurasi komponen dasar

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 File/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):

- secara otomatis (***Hapus semua ancaman secara otomatis***)
- 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 ***Hapus cookie secara otomatis.*** Dalam kasus tertentu, Anda dapat mengaktifkan opsi ini untuk mencapai tingkat keamanan maksimum, walau demikian ia telah dinonaktifkan secara default. (*cookie = parsel teks dari teks yang dikirimkan oleh server ke peramban web yang kemudian dikirim kembali tanpa perubahan oleh peramban setiap kali ia mengakses server itu. Cookie HTTP digunakan untuk autentikasi, pelacakan, dan pengelolaan informasi tertentu tentang pengguna, seperti preferensi situs atau isi keranjang belanja elektronik mereka*).

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

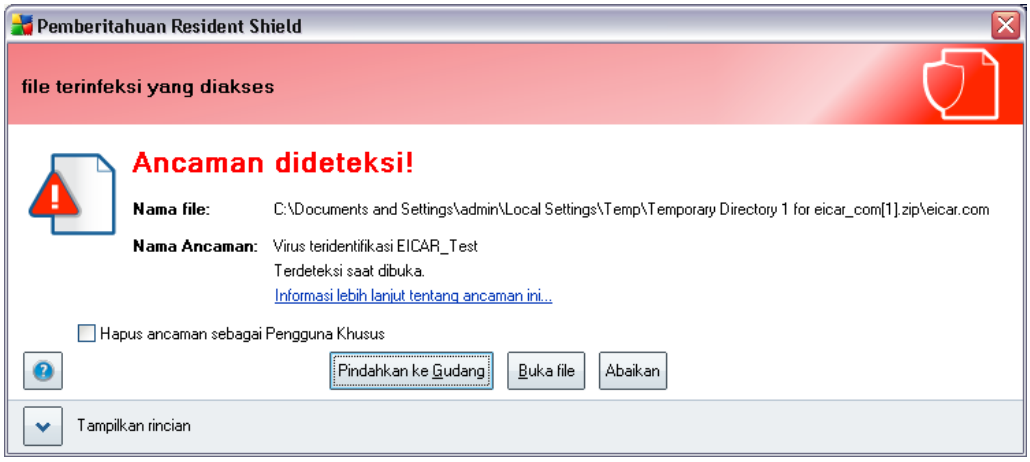
Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka ***Perisai Tetap*** adalah sebagai berikut:

- ***Atur pengecualian*** - membuka dialog ***Perisai Tetap - Pengecualian Direktori*** di mana Anda menentukan folder yang harus dibiarkan dari pemindaian ***Perisai Tetap***
- ***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)

8.12.3. Deteksi Perisai Tetap

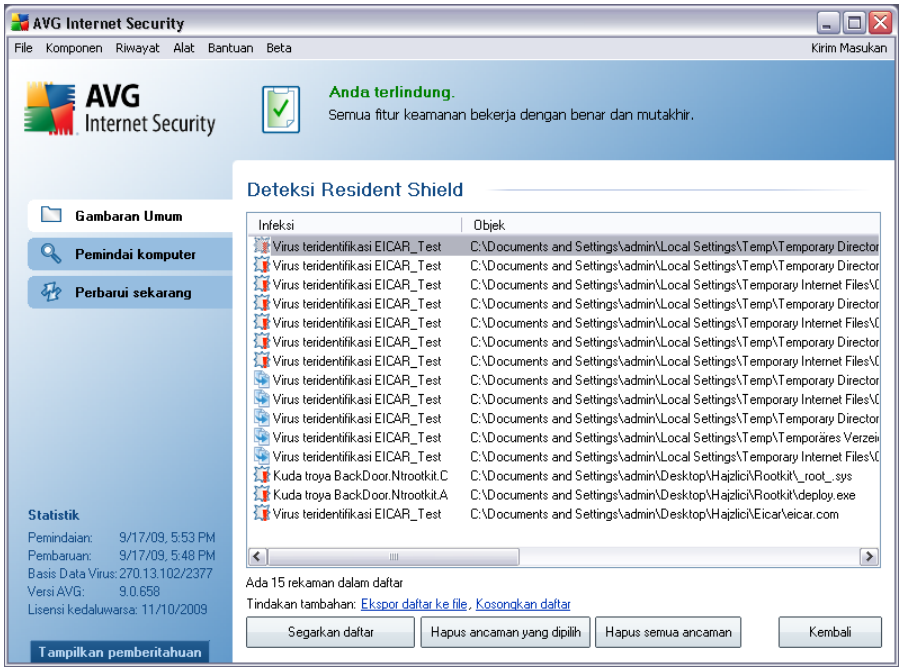
Perisai Tetap memindai file saat disalin, dibuka atau disimpan. Bila ada virus atau semacam ancaman yang terdeteksi, Anda akan segera diperingatkan melalui dialog berikut:



Dialog ini menyediakan informasi mengenai ancaman yang terdeteksi dan meminta Anda memutuskan tindakan apa yang harus diambil sekarang:

- ***Pulihkan*** - jika ada penawarnya, AVG akan memulihkan file yang terinfeksi secara otomatis; opsi ini merupakan tindakan yang disarankan
- ***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!

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 / Temuan 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).

8.13. 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!*

Pengatur Unduhan AVG adalah alat sederhana yang memberi Anda cara yang mudah untuk mengelola unduhan produk rumah AVG. Berdasarkan pilihan Anda, pengatur unduhan akan menyesuaikan pada produk, tipe lisensi dan bahasa tertentu. Keuntungan terbesar utilitas ini adalah untuk membantu mengelola unduhan produk AVG sesuai keinginan Anda. Selain itu, file instalasi terbaru selalu diunduh, sehingga program AVG terus diperbarui setelah instalasi.

Pengatur Unduhan AVG

- Selalu mengunduh file instalasi terbaru;
- Mengurangi ukuran file yang diunduh;
- Mendukung unduhan lanjutan jika unduhan putus karena suatu alasan;
- Kompatibel dengan semua edisi program AVG yang ditujukan untuk penggunaaan rumah

Catatan: *Harap ingat bahwa Pengatur Unduhan AVG tidak cocok untuk mengunduh edisi jaringan dan SBS dan hanya mendukung sistem operasi berikut: Windows 2000*

(SP4 + SRP roll-up), Windows XP (SP2 dan yang lebih tinggi), Windows Vista (semua edisi).

8.13.1. Prinsip-Prinsip Pengatur Pembaruan

Pengatur Unduhan AVG dijalankan dengan langkah berikut:

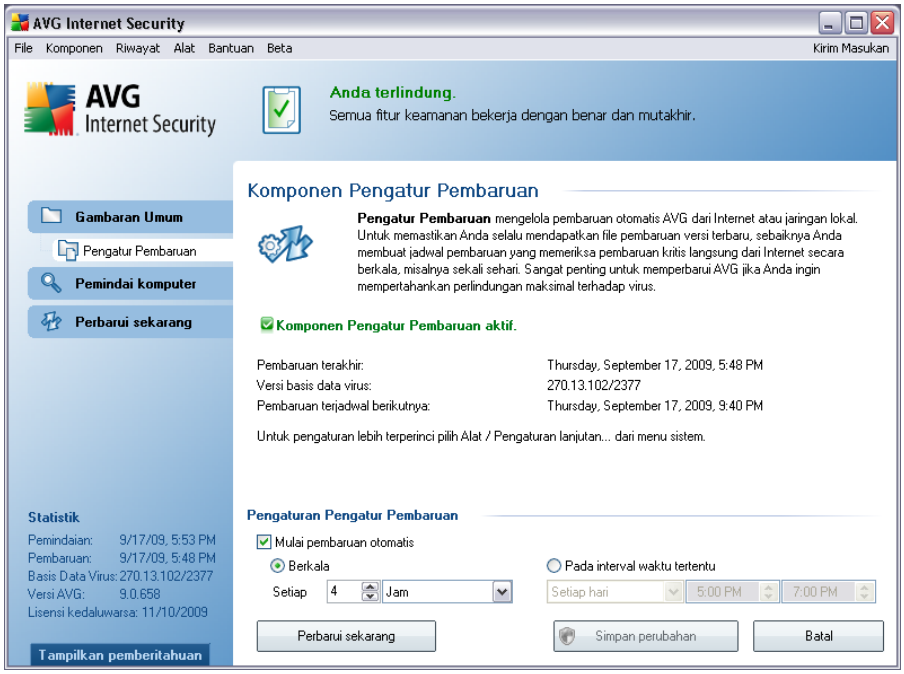
- Pertama, perlu mengunduh aplikasi ***Pengatur Unduhan AVG*** itu sendiri. Setelah diluncurkan, ***Pengatur Unduhan AVG*** meminta Anda untuk memilih bahasa proses instalasi.

- Kemudian, ***Pengatur Unduhan AVG*** berusaha untuk membuat koneksi Internet untuk menjalankan tes konektivitas. Jika tes konektivitas berhasil, Anda akan dapat memilih versi program AVG mana yang ingin Anda instal (*versi lengkap, versi uji coba, versi gratis*).

- Setelah versi program AVG dipilih, Anda akan diminta untuk memilih produk yang ingin Anda instal.

- Terakhir, semua file instalasi yang diperlukan akan diunduh. ***Pengatur Unduhan AVG*** tertutup dan instalasi AVG diluncurkan.

8.13.2. Antarmuka Pengatur Pembaruan



Antarmuka ***Pengatur Pembaruan*** menampilkan informasi tentang fungsionalitas komponen dan statusnya saat ini (*Pengatur pembaruan aktif.*), dan menyediakan data statistik yang relevan:

- ***Pembaruan terbaru*** - menetapkan kapan dan pukul berapa basis data diperbarui
- ***Versi basis data virus*** - menentukan nomor versi basis data virus terbaru; dan nomor ini bertambah setiap kali basis data virus diperbarui
- ***Pembaruan terjadwal berikutnya*** - menentukan kapan dan pukul berapa basis data dijadwalkan untuk diperbarui lagi

Konfigurasi komponen dasar

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 rutin atas file pembaruan terbaru sangatlah penting agar perangkat lunak keamanan berfungsi dengan semestinya!

Lebih lanjut, Anda dapat menentukan kapan pembaruan harus diluncurkan:

- ***Secara berkala*** - menentukan interval waktu
- ***Pada waktu tertentu*** - menentukan hari dan waktu yang pasti

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

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

Tombol kontrol

Tombol kontrol yang tersedia dalam 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)

8.14. AVG Security Toolbar

AVG Security Toolbar adalah alat baru yang bekerja bersama komponen ***Link Scanner***dan memeriksa hasil penelusuran dari mesin telusur Internet yang didukung (*Yahoo!, Google, MSN, Baidu*).

Jika Anda memilih untuk menginstal bilah alat saat instalasi **AVG 9 Internet Security**, maka ia akan ditambahkan ke dalam peramban web Anda secara otomatis.

AVG Security Toolbar dapat digunakan untuk mengontrol fungsi ***Link Scanner*** dan untuk menyesuaikan cara kerjanya, serta memperbarui **AVG 9 Internet Security** Anda jika tersedia pembaruan yang baru.

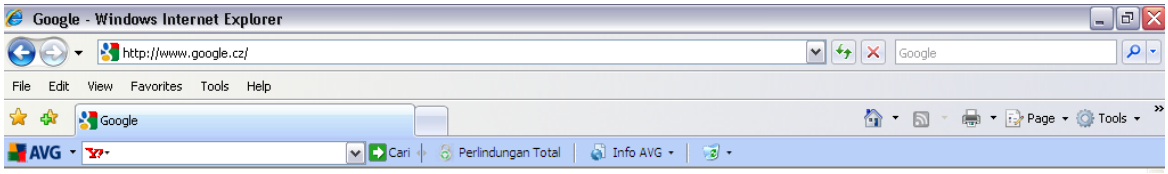
Catatan: *jika Anda menggunakan peramban Internet alternatif (mis. Avant Browser) maka Anda dapat menemui cara kerja yang tidak terduga.*

8.14.1. Antarmuka AVG Security Toolbar

AVG Security Toolbar dirancang untuk bekerja bersama ***MS Internet Explorer*** (*versi 6.0 atau yang lebih tinggi*) dan ***Mozilla Firefox*** (*versi 1.5 atau yang lebih tinggi*).

Catatan: *AVG Security Toolbar tidak ditujukan untuk platform server!*

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 terletak di peramban web Anda tepat di bawah bilah alamat:



AVG Security Toolbar terdiri dari berikut ini:

- ***Tombol logo AVG*** - menyediakan akses ke item toolbar umum. Klik tombol logo agar dialihkan ke situs web AVG (http://www.avg.com/). Mengklik pointer di sebelah ikon AVG akan membuka item berikut:
    - ***Info Toolbar*** - menautkan ke laman utama ***AVG Security Toolbar*** bersama informasi terperinci mengenai perlindungan toolbar
    - ***Luncurkan AVG 9.0*** - membuka antarmuka pengguna AVG
    - ***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 untuk *Menghapus riwayat lengkap* AVG Security Toolbar, atau untuk *Menghapus riwayat penelusuran, 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***, atau melihat perincian versi Toolbar saat ini
- ***Kotak telusur yang didukung Yahoo!*** - cara mudah dan aman untuk menelusuri web dengan menggunakan Yahoo! Search. Masukkan kata atau frasa ke dalam kotak telusur kemudian tekan ***Cari*** untuk memulai penelusuran di server Yahoo! secara langsung, apa pun laman yang ditampilkan saat itu. Kotak telusur juga menampilkan daftar riwayat penelusuran Anda. Penelusuran yang dilakukan melalui kotak telusur akan dianalisis menggunakan perlindungan ***AVG Search-Shield***.
- ***Tombol AVG Active Surf-Shield*** - tombol aktif/nonaktif yang mengontrol status perlindungan***AVG Active Surf-Shield***
- ***Tombol AVG Search-Shield*** - tombol aktif/nonaktif yang mengontrol status

perlindungan ***AVG Search-Shield***

- ***Tombol Info AVG*** - menyediakan tautan ke informasi keamanan penting yang berada di Situs web AVG (http://www.avg.com/)

8.14.2. 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 tiga bagian:

- ***Umum***

Pada tab ini Anda dapat menentukan tombol yang harus ditampilkan / disembunyikan dalam panel ***AVG Security Toolbar***:

- ***Tombol Berita AVG*** - opsi ini menampilkan tombol ***Berita AVG***. Dengan menekan tombol ini dalam panel ***AVG Security Toolbar***, Anda dapat membuka menu buka bawah yang berisi tautan menuju pernyataan pers terbaru yang berkaitan dengan AVG.

- ***Tombol Info AVG*** - tombol ***Info AVG*** tombol membuka menu berisi opsi berikut:

- *Info Bilah Alat* - membuka laman produk ***AVG Security Toolbar*** yang berisi informasi terperinci mengenai komponen ini
- *Tentang Ancaman* - membuka laman web lab virus AVG yang berisi informasi mengenai ancaman, rekomendasi penghapusan virus, daftar Tanya-Jawab, dll.
- *Berita AVG* - membuka laman web yang menyediakan pernyataan pers terbaru yang berkaitan dengan AVG
- *Tingkat Ancaman Saat Ini* - membuka laman web lab virus yang berisi tampilan grafis tingkat ancaman saat ini pada web
- *Ensiklopedia Virus* - membuka laman Ensiklopedia Virus di mana Anda dapat mencari virus tertentu berdasarkan nama dan mendapatkan informasi terperinci mengenai setiap virus

o ***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***.

- ***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:

- ***AVG Browser Security*** - centang item ini untuk mengaktifkan atau menonaktifkan ***AVG Search-Shield*** dan/atau layanan ***AVG Active Surf-Shield***
- ***Peringkat*** - pilih simbol grafis yang digunakan untuk peringkat hasil telusur oleh komponen ***AVG Search-Shield*** yang ingin Anda gunakan:
  -  laman aman
  -  laman agak mencurigakan
  -  laman berisi tautan ke laman yang dipastikan berbahaya
  -  laman berisi ancaman aktif
  -  laman 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 laman 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.***

- ***Opsi Lanjutan***

Pada tab ***Opsi Lanjutan*** , Anda dapat mengaktifkan atau menonaktifkan pengaturan ***AVG Security Toolbar*** yang lebih spesifik:

- ***Atur dan tetapkan Yahoo! sebagai penyedia layanan penelusuran untuk bilah Alamat*** - (*diaktifkan secara default*) - jika dicentang, opsi ini akan memungkinkan Anda memasukkan kata sandi penelusuran langsung ke dalam bilah alamat dalam peramban Internet dan layanan Yahoo! layanan akan digunakan secara otomatis untuk mencari situs web yang relevan.

- ***Tampilkan kotak telusur Yahoo! pada tab baru dalam peramban*** - (*diaktifkan secara default*) - jika dicentang, opsi ini akan menampilan kotak telusur Yahoo! kotak telusur dalam tiap tab peramban Internet yang baru dibuka.

- ***Biarkan AVG memberi saran mengenai kesalahan navigasi peramban (404/DNS)*** - (*diaktifkan secara default*) - jika saat melakukan penelusuran Anda menemui laman yang tidak ada, atau laman yang tidak dapat ditampilkan (*kesalahan 404*), maka ***AVG Security Toolbar*** akan secara otomatis memberikan gambaran umum mengenai laman alternatif yang berhubungan dengan topik.

- ***Atur dan tetapkan Yahoo! sebagai penyedia layanan penelusuran untuk peramban Anda*** - (*dinonaktifkan secara default*) - Yahoo!

adalah mesin telusur default bagi penelusuran web dalam ***AVG Security Toolbar***, dan dengan mengaktifkan opsi ini, Anda dapat menjadikannya mesin telusur default peramban web Anda.

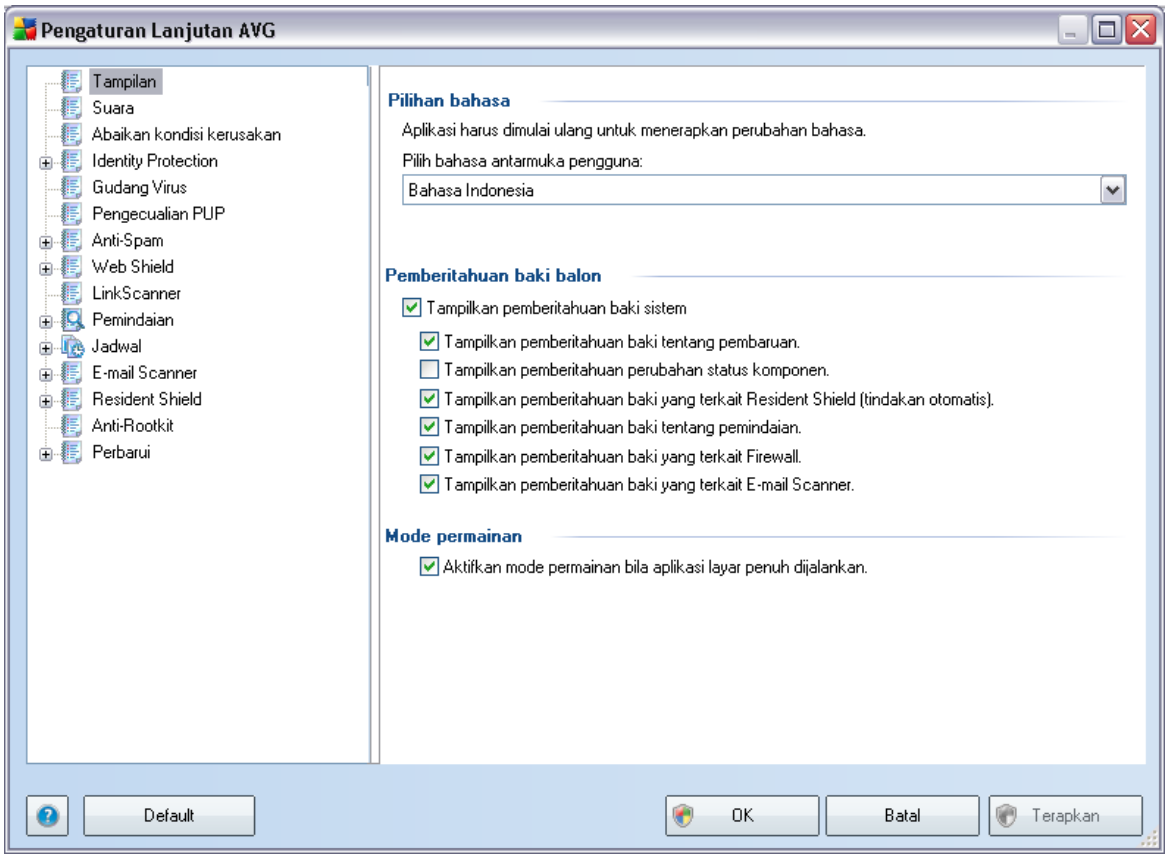
- ***Tampilkan ulang AVG Security Toolbar bila tersembunyi (mingguan)*** - (*diaktifkan secara default*) - opsi ini aktif secara default dan bila ***AVG Security Toolbar*** Anda secara tidak sengaja tersembunyi, maka ia akan ditampilkan kembali dalam jangka waktu satu minggu.

9. Pengaturan Lanjutan AVG

Dialog konfigurasi lanjutan **AVG 9 Internet Security** akan dibuka dalam 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:

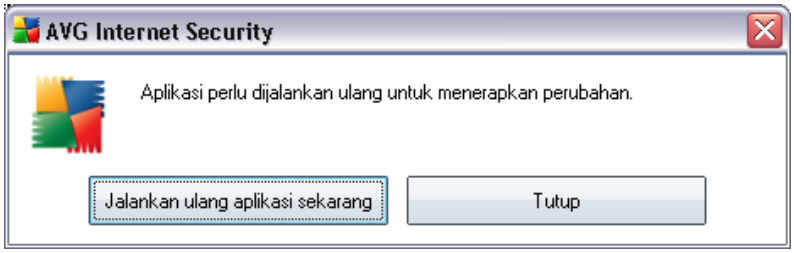


Pemilihan bahasa

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-bahasa yang telah dipilih sebelumnya untuk diinstal selama proses instalasi (lihat bab Instalasi Khusus - Pemilihan Komponen). 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 konfirmasikan pilihan Anda dengan menekan tombol ***Terapkan*** (sudut kanan bawah)
- Tekan tombol ***OK*** untuk mengonfirmasi.
- 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 memperhatikannya!

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

- ***Tampilkan pemberitahuan baki sistem*** - secara default, item ini dicentang (*diaktifkan*), dan pemberitahuan ditampilkan. Jangan centang item ini untuk menonaktifkan sama sekali tampilan semua balon pemberitahuan. Bila diaktifkan, Anda dapat memilih lebih lanjut pemberitahuan spesifik yang akan ditampilkan:

- ***Tampilkan pemberitahuan baki tentang pembaruan*** - memutuskan apakah informasi mengenai peluncuran proses pembaruan AVG, kemajuannya, dan finalisasinya harus ditampilkan;

- ***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;

- ***Tampilkan pemberitahuan baki menyangkut Perisai Tetap*** - memutuskan apakah informasi mengenai penyimpanan, penyalinan, dan proses pembukaan file harus ditampilkan atau disembunyikan;

- ***Tampilkan pemberitahuan baki tentang pemindaian*** - memutuskan apakah informasi mengenai peluncuran otomatis dari pemindaian terjadwal, kemajuannya, dan hasilnya harus ditampilkan;

- ***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;

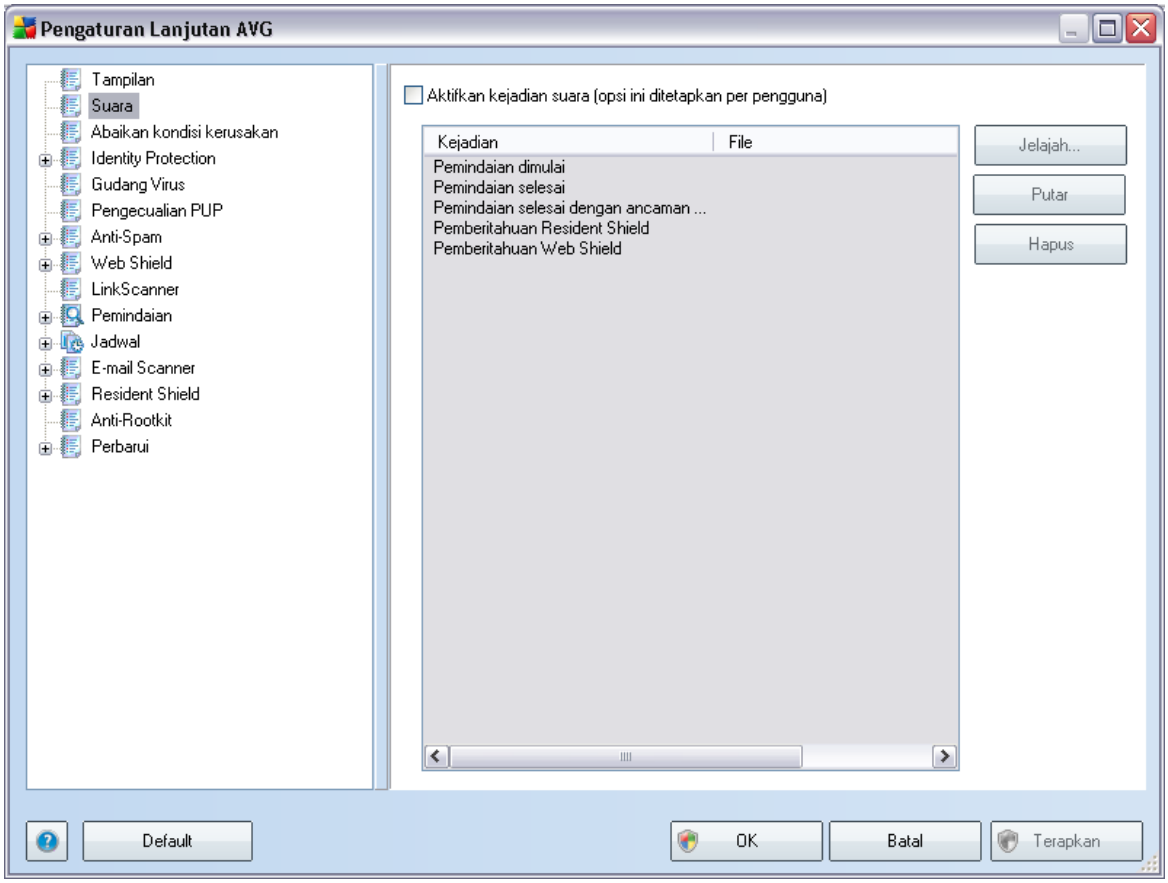
- ***Tampilkan pemberitahuan baki menyangkut Pemindai E-mail*** - memutuskan apakah informasi mengenai pemindaian semua pesan e-mail yang masuk dan keluar akan ditampilkan.

Mode permainan

Fungsi AVG ini dirancang untuk aplikasi layar penuh yang perlu berkomunikasi melalui Internet dan kemungkinan dialog pertanyaan AVG akan mempengaruhi aplikasi (*mengurangi atau merusak grafiknya*). Untuk menghindari hal ini, biarkan kotaknya dicentang 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:

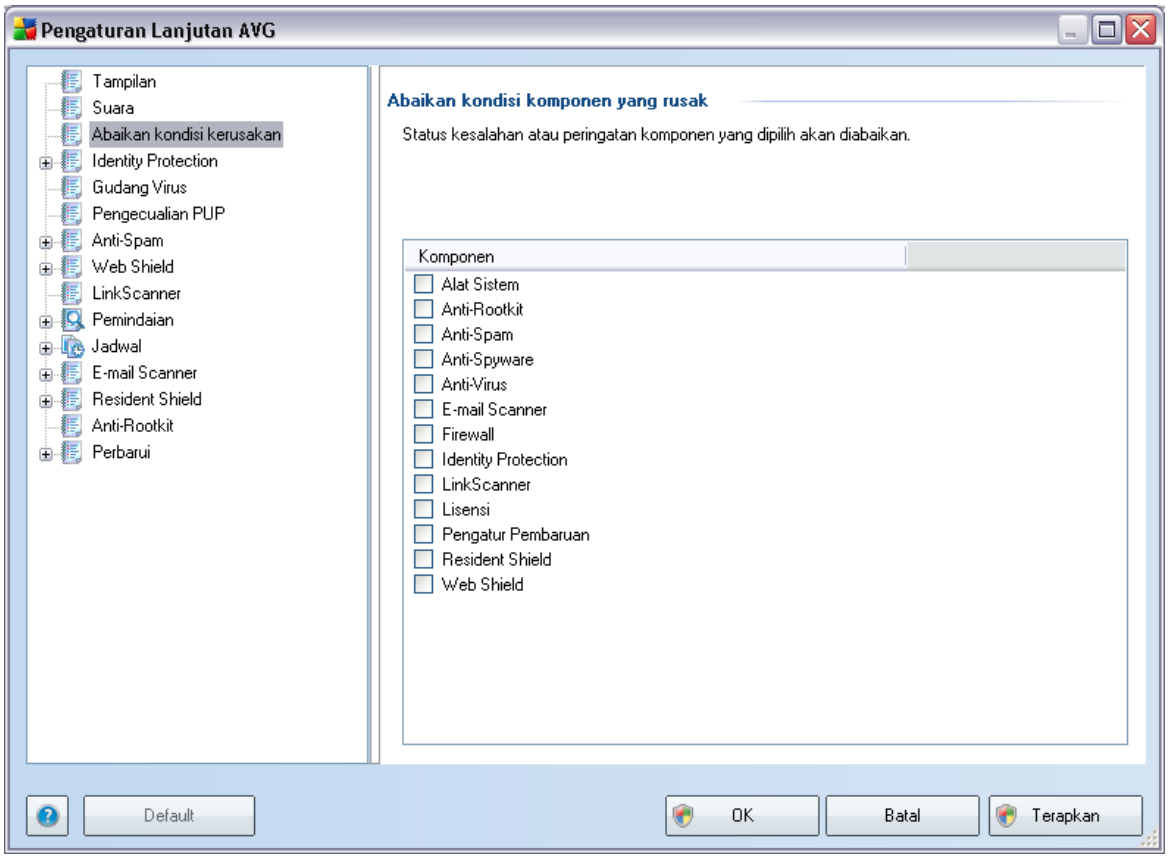


Kemudian, pilih kejadian yang terkait dari daftar dan jelajahi (***Jelajahi***) disk Anda untuk menemukan suara yang ingin Anda tetapkan untuk kejadian ini. Untuk mendengarkan suara yang dipilih, sorot kejadian dalam daftar dan tekan tombol ***Putar*** . Gunakan tombol ***Hapus*** untuk menghapus suara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

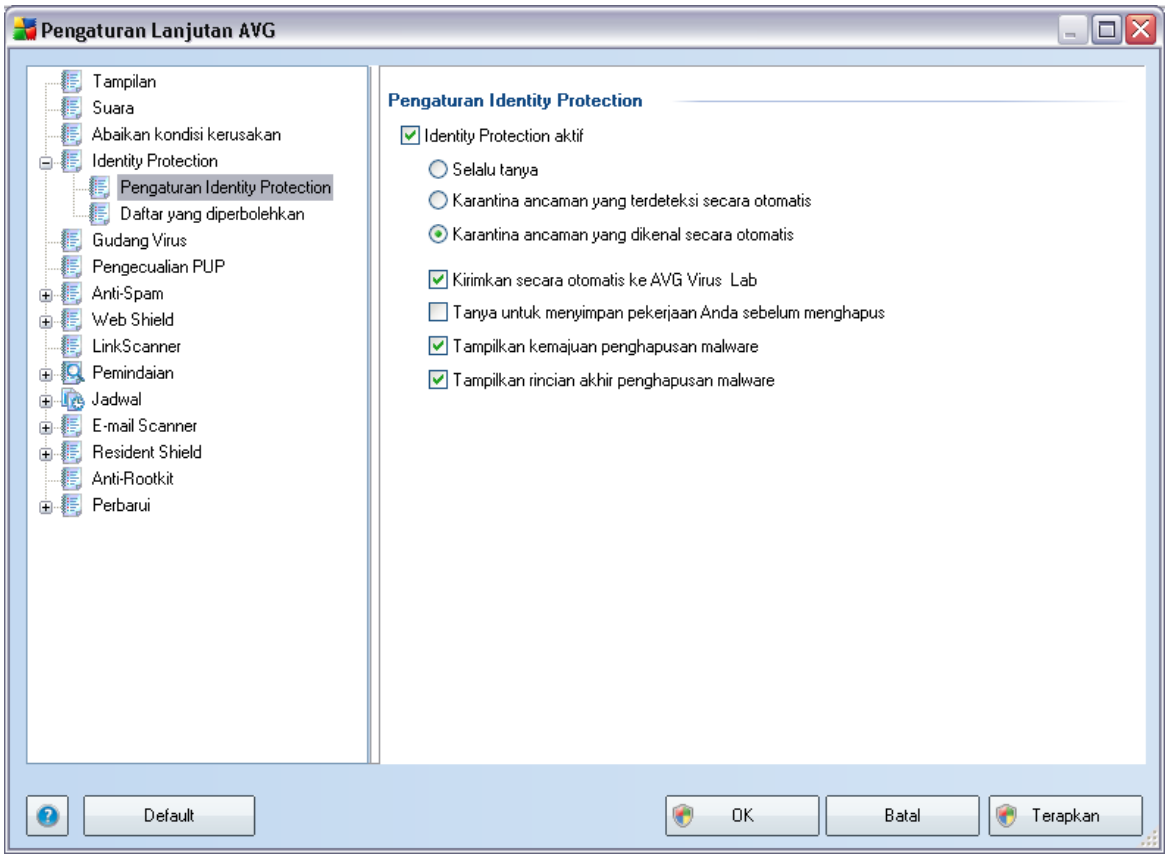
komponen untuk sementara (*hal ini tidak disarankan, Anda harus tetap mengaktifkan semua komponen selamanya dan dalam konfigurasi default, namun hal ini mungkin saja terjadi*). Dalam hal itu, ikon baki sistem secara otomatis melaporkan status kesalahan komponen tersebut. Walau demikian, dalam hal ini 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***:

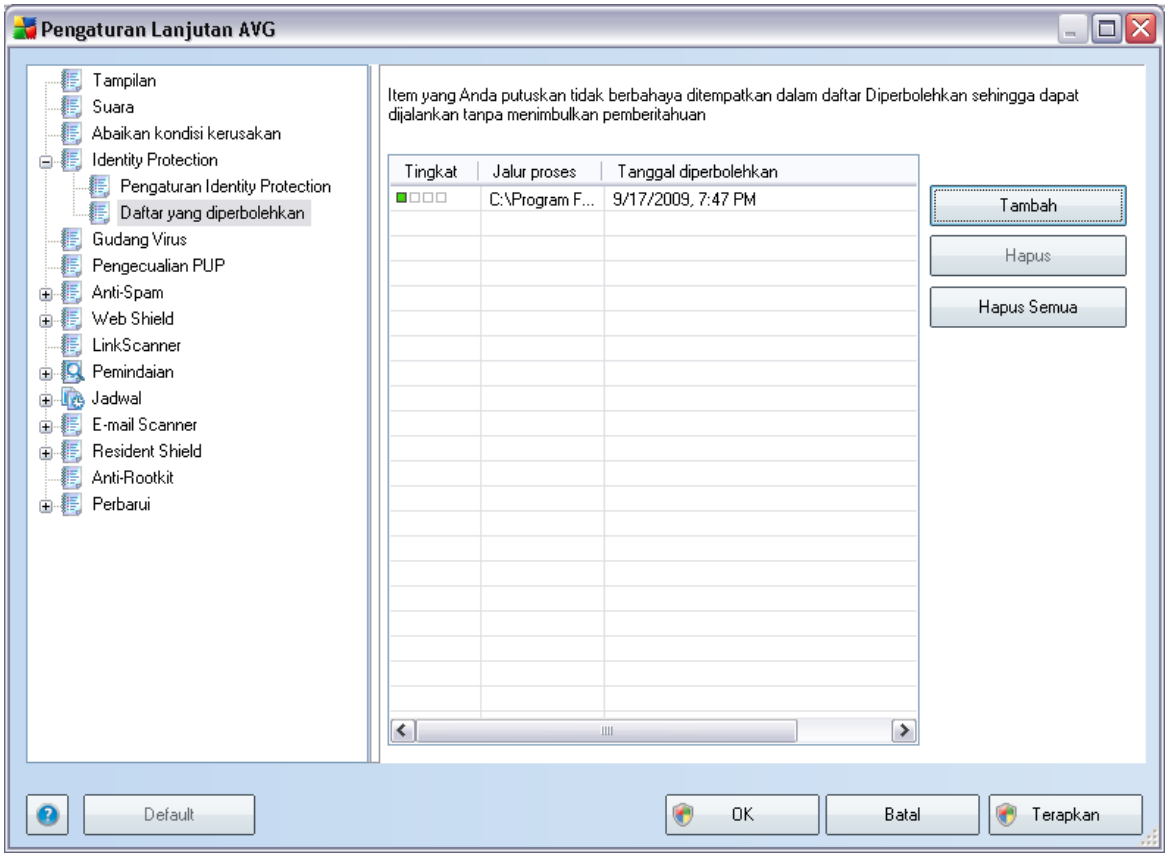


- ***Karantina ancaman yang terdeteksi secara otomatis*** - (*dinonaktifkan secara default*: centang kotak ini untuk menentukan bahwa Anda ingin semua ancaman yang mungkin terdeteksi segera dipindahkan ke ruang aman di Gudang Virus AVG. Dengan menyimpan pengaturan default, saat ancaman terdeteksi, Anda akan ditanyai apakah ia harus dipindahkan ke karantina untuk memastikan tidak terhapusnya aplikasi yang ingin Anda jalankan.

- ***Kirimkan secara otomatis ke Lab Virus AVG*** - (*diaktifkan secara default*): Tetap centang kotak ini untuk memasok basis data yang mengumpulkan informasi tentang aktivitas jahat/merusak di web dan untuk membantu kami mengenali ancaman baru.

9.4.2. Daftar yang Diperbolehkan

Jika dalam dialog ***Pengaturan Perlindungan Identitas*** Anda memutuskan untuk tidak mencentang 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***, dan ia tidak akan dilaporkan sebagai item yang mungkin berbahaya lagi:



Daftar yang diperbolehkan menyediakan informasi berikut mengenai setiap aplikasi:

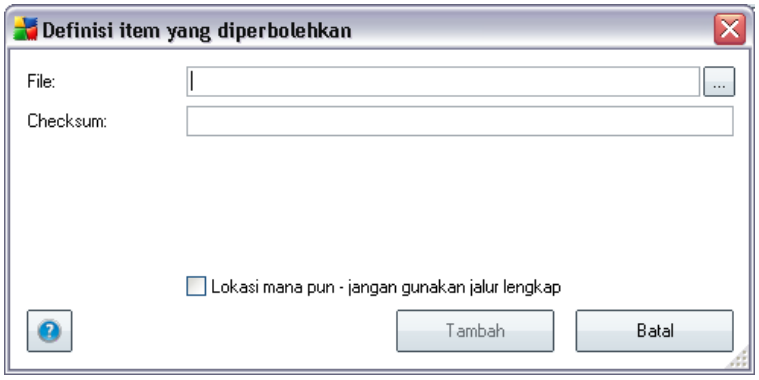
- ***Tingkat*** - identifikasi grafis dari keseriusan proses yang bersangkutan pada skala empat-tingkat dari kurang penting (■□□□) hingga kritis (■■■■)

- ***Jalur proses*** - jalur ke aplikasi (*proses*) lokasi file eksekusi
- ***Tanggal yang diperbolehkan*** - tanggal saat Anda secara manual menetapkan aplikasi sebagai aman

Tombol kontrol

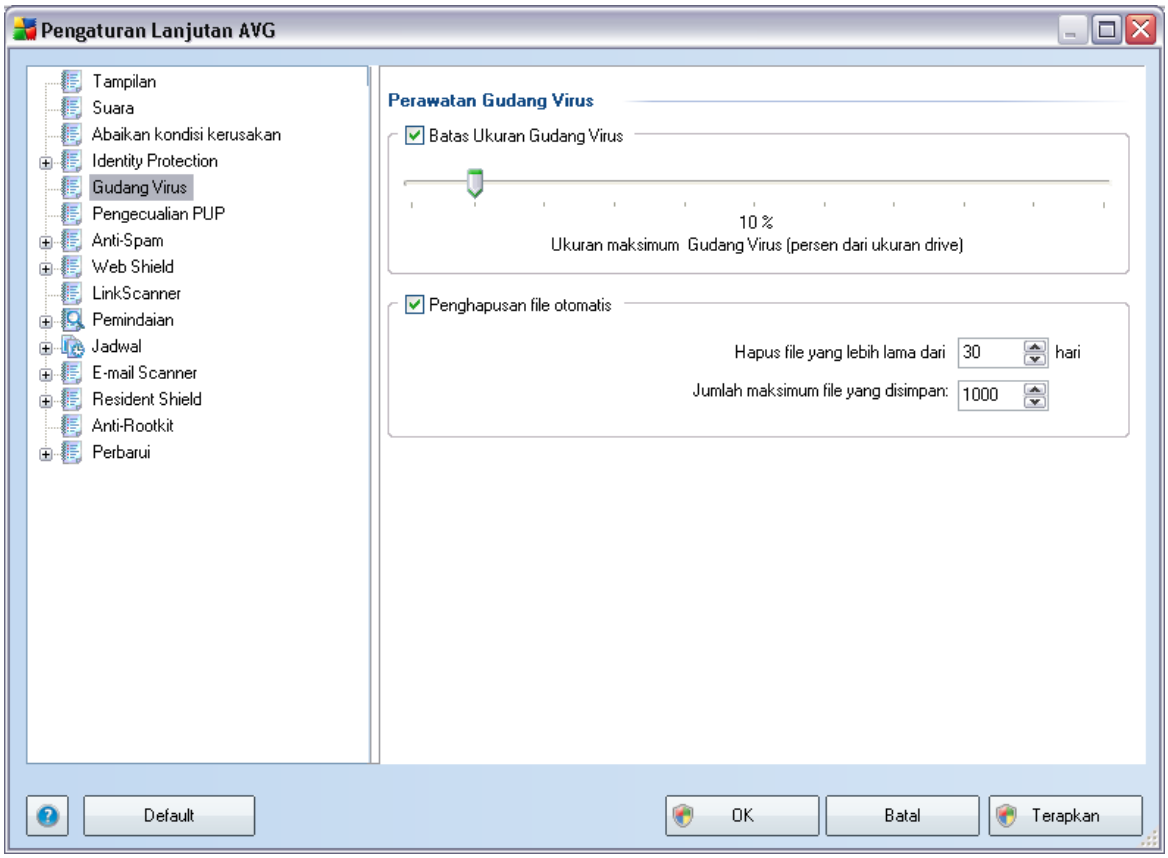
Tombol kontrol yang tersedia dalam dialog ***Daftar yang diperbolehkan*** adalah sebagai berikut:

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



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

9.5. Gudang Virus

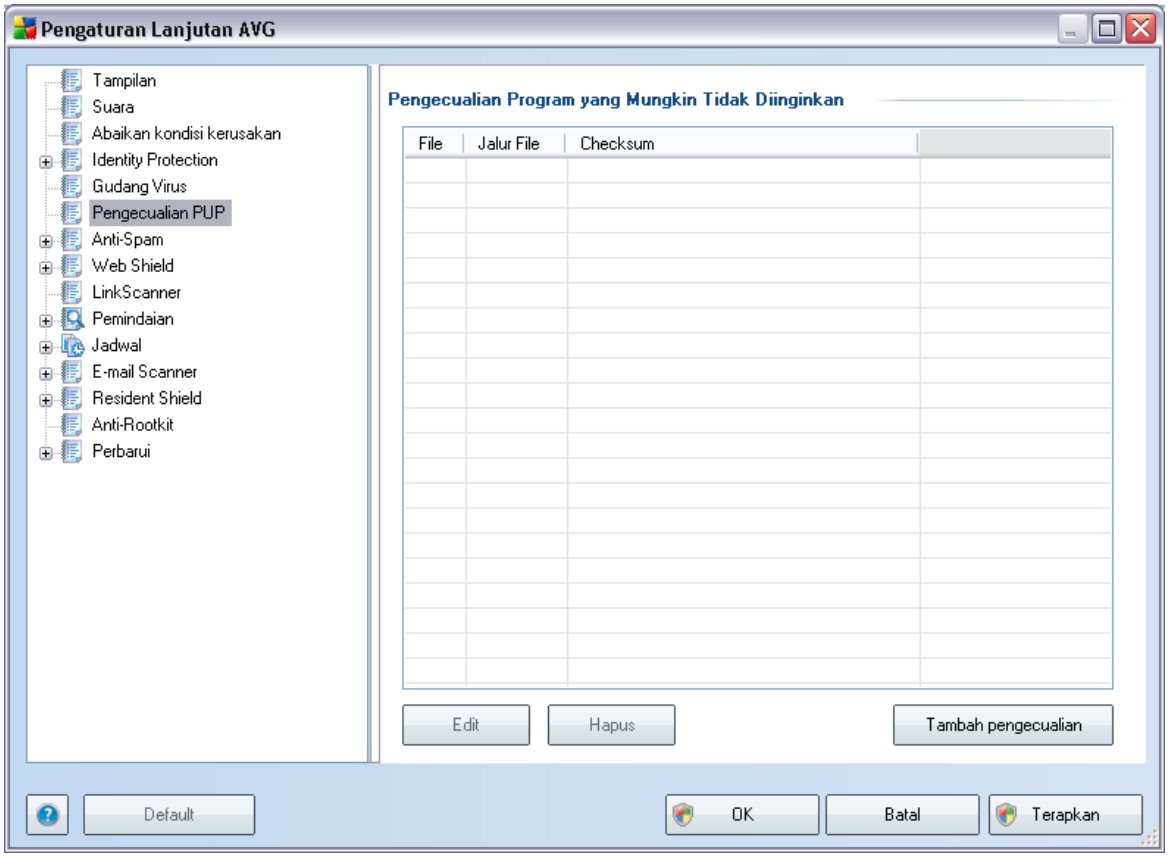


Dialog ***Perawatan Gudang Virus*** memungkinkan Anda menentukan beberapa parameter yang menyangkut administrasi berbagai objek yang tersimpan dalam ***Gudang Virus***:

- ***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

AVG 9 Internet Security dapat menganalisis dan mendeteksi aplikasi yang dapat dijalankan atau pustaka DLL yang mungkin tidak diinginkan dalam sistem. Dalam beberapa kasus, pengguna mungkin ingin membiarkan beberapa program yang tidak diinginkan di komputer (*program yang sengaja diinstal*). Beberapa program, khususnya yang gratisan, termasuk adware. Adware tersebut mungkin terdeteksi dan dilaporkan oleh AVG sebagai ***program yang mungkin tidak diinginkan***. Jika Anda ingin membiarkan program tersebut pada komputer Anda, Anda dapat menentukannya sebagai pengecualian program yang mungkin tidak diinginkan:

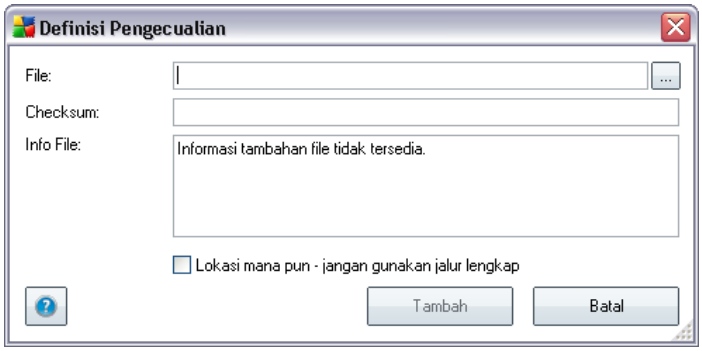


Dialog ***Pengecualian Program yang Mungkin Tidak Diinginkan*** menampilkan daftar pengecualian yang telah ditentukan dan yang saat ini sah dari program yang mungkin tidak diinginkan. Anda dapat mengedit daftar ini, menghapus item yang ada, atau menambahkan pengecualian baru. Informasi berikut dapat 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 suatu file 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 ditentukan di mana Anda dapat mengubah parameter pengecualian
- ***Hapus*** - menghapus item yang dipilih dari daftar pengecualian
- ***Tambah pengecualian*** - membuka dialog pengeditan di mana Anda dapat menentukan parameter pengecualian baru yang akan dibuat:

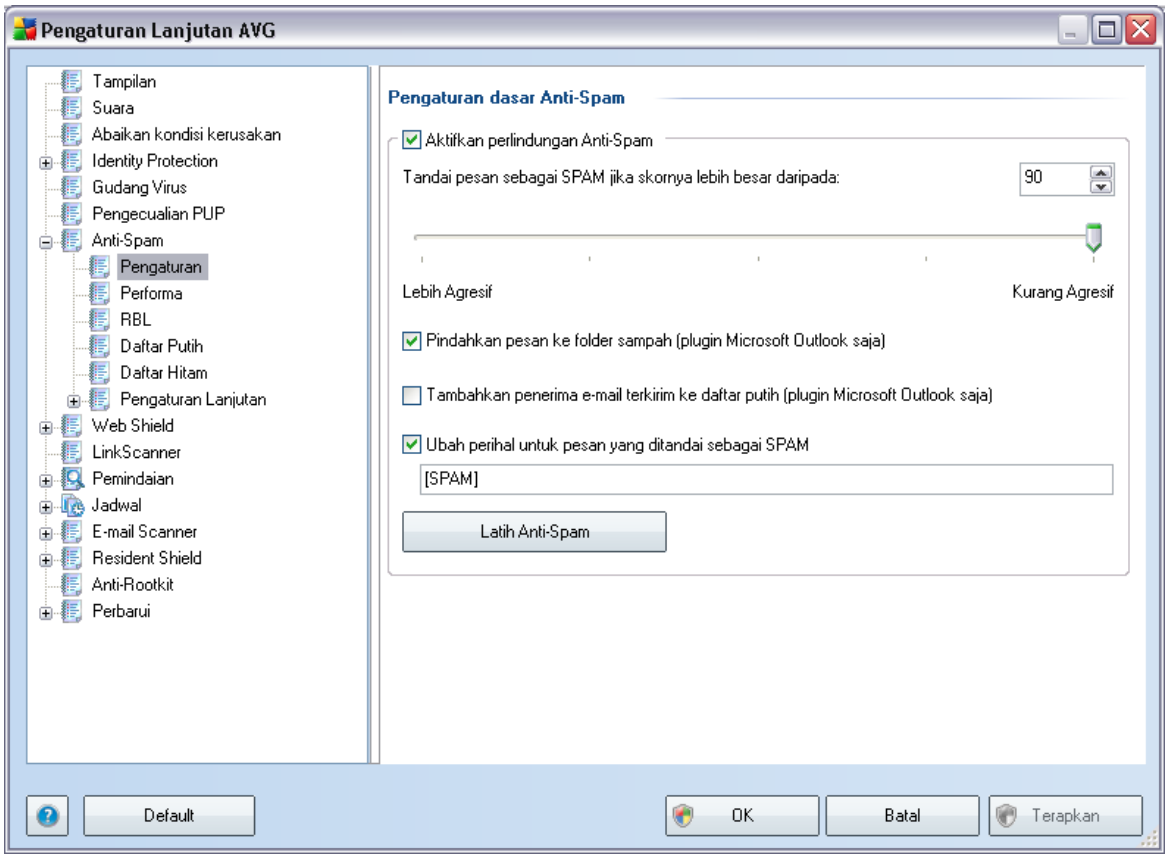


  - ***File*** - ketikkan jalur lengkap ke file yang ingin Anda tandai sebagai pengecualian
  - ***Checksum*** - menampilkan 'tanda tangan' unik atas file yang dipilih. Checksum ini adalah string karakter yang dibuat secara otomatis, yang memungkinkan AVG dengan jelas membedakan suatu file dari file lainnya. Checksum dibuat dan ditampilkan setelah penambahan file berhasil.
  - ***Info File*** - menampilkan informasi tambahan tentang file (*lisensi/ informasi versi, dll.*)

- ***Sembarang lokasi - jangan gunakan jalur lengkap*** - jika Anda ingin menentukan file ini sebagai pengecualian hanya untuk lokasi tertentu, jangan centang kotak ini

9.7. Anti-Spam

9.7.1. Pengaturan



Dalam dialog ***Pengaturan dasar Anti-Spam*** Anda dapat mencentang/ menghilangkan 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 (*0 sampai 100*) atau dengan menggerakkan bilah geser ke kiri atau ke kanan (*dengan menggunakan bilah geser, 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 90-99*** - Kebanyakan pesan e-mail masuk akan dikirim seperti biasa (tanpa ditandai sebagai spam). Spam yang paling mudah dikenali akan difilter, namun jumlah spam yang sangat besar mungkin tetap diperbolehkan masuk.

- ***Nilai 80-89*** - 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 1-59*** - Konfigurasi sangat agresif. Pesan bukan-spam hampir bisa dipastikan akan tertangkap sebagai pesan spam nyata. Kisaran ambang batas ini tidak disarankan untuk penggunaan biasa.

- ***Nilai 0*** - Dalam mode ini, Anda akan menerima pesan e-mail dari pengirim yang ada dalam ***Daftar Putih*** Anda. Pesan e-mail lain akan dianggap sebagai spam. ***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 mengonfirmasikan bahwa semua penerima e-mail terkirim dapat dipercaya, dan semua pesan e-mail yang berasal dari akun e-mail mereka dapat disampaikan;

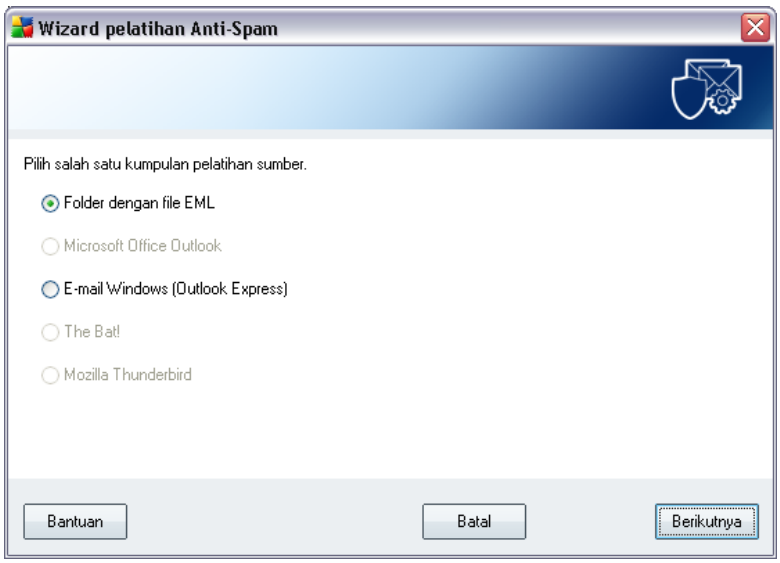
- ***Ubah perihal pesan yang ditandai sebagai SPAM*** - centang kotak ini jika

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.

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!, Mozilla Thunderbird*), 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

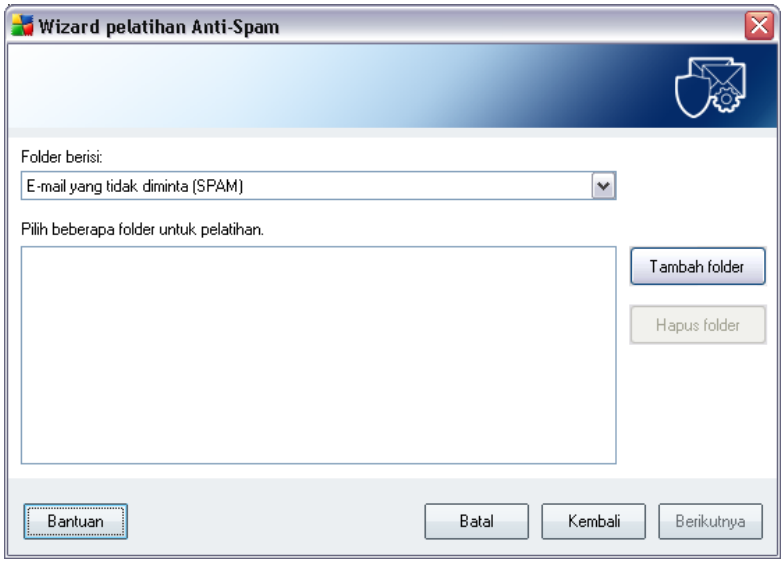
menemukan folder yang diinginkan pada langkah berikutnya

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



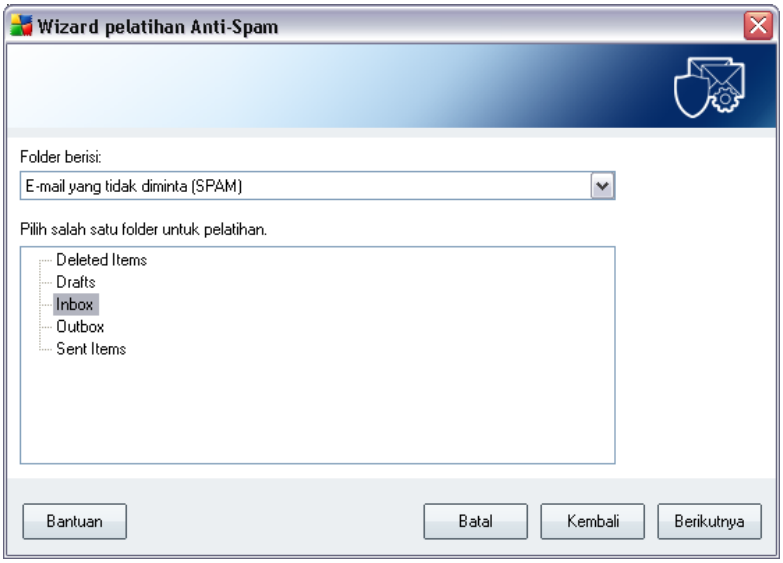
Dalam dialog ini, pilih folder dengan pesan yang ingin Anda gunakan untuk pelatihan. Tekan tombol ***Tambah folder*** untuk menemukan folder dengan file .eml (*pesan e-mail tersimpan*). Folder yang dipilih akan ditampilkan dalam dialog.

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

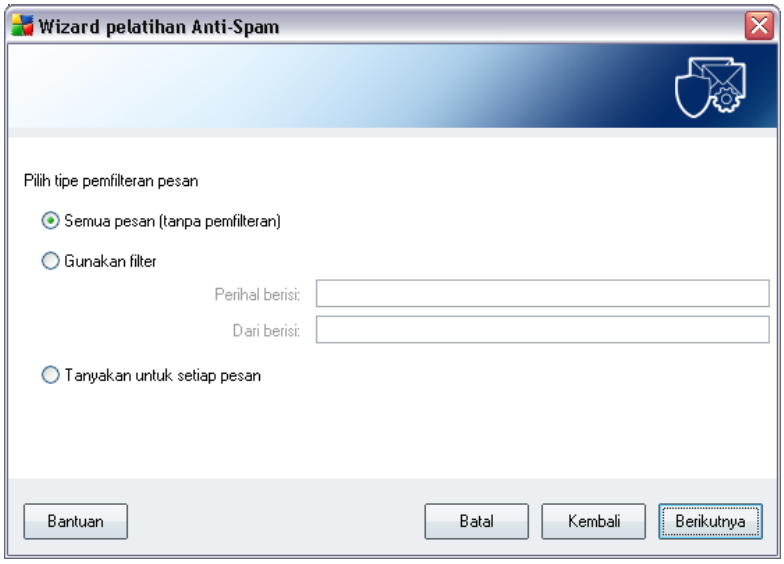
Setelah Anda mengonfirmasi salah satu opsi, dialog baru akan muncul.



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)***.

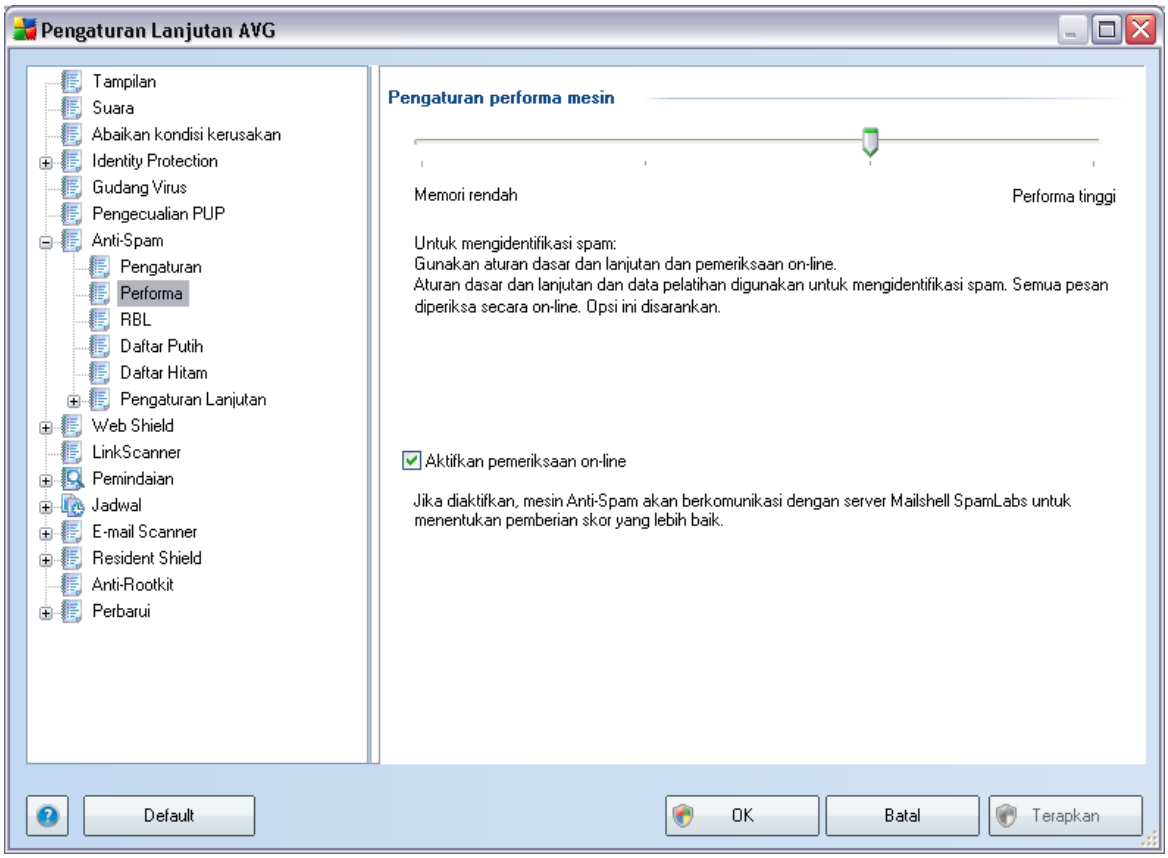
Jika Anda tidak yakin tentang pesan yang terdapat di dalam folder, dan ingin wizard menanyakan setiap pesan (sehingga Anda dapat memutuskan apakah akan digunakan untuk pelatihan atau tidak), pilih opsi ***Tanyakan untuk setiap pesan***.

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 bilah geser 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.

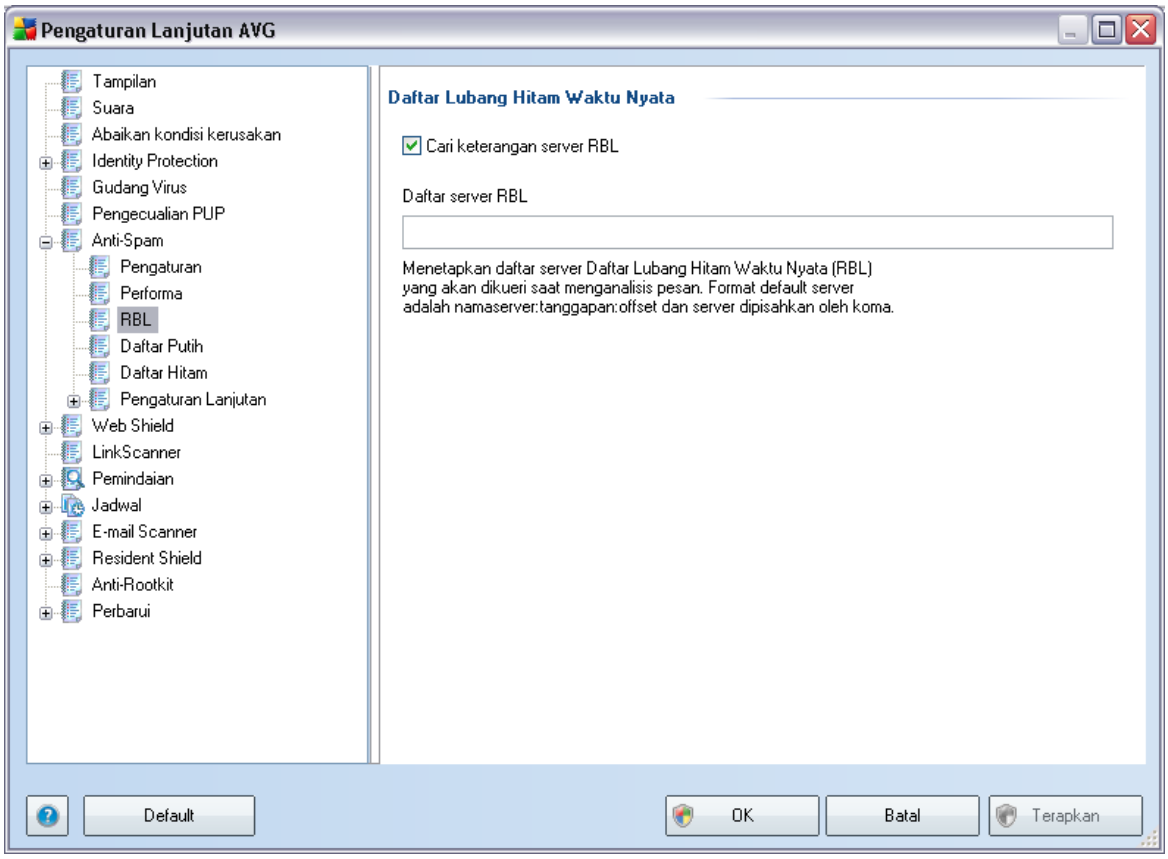
- ***Performa tinggi*** - mode ini akan menghabiskan banyak memori. Selama proses pemindaian untuk mengenali spam, fitur berikut akan digunakan: aturan dan cache basis data spam, aturan dasar dan lanjutan, basis data alamat IP dan basis data spammer.

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 sah 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.

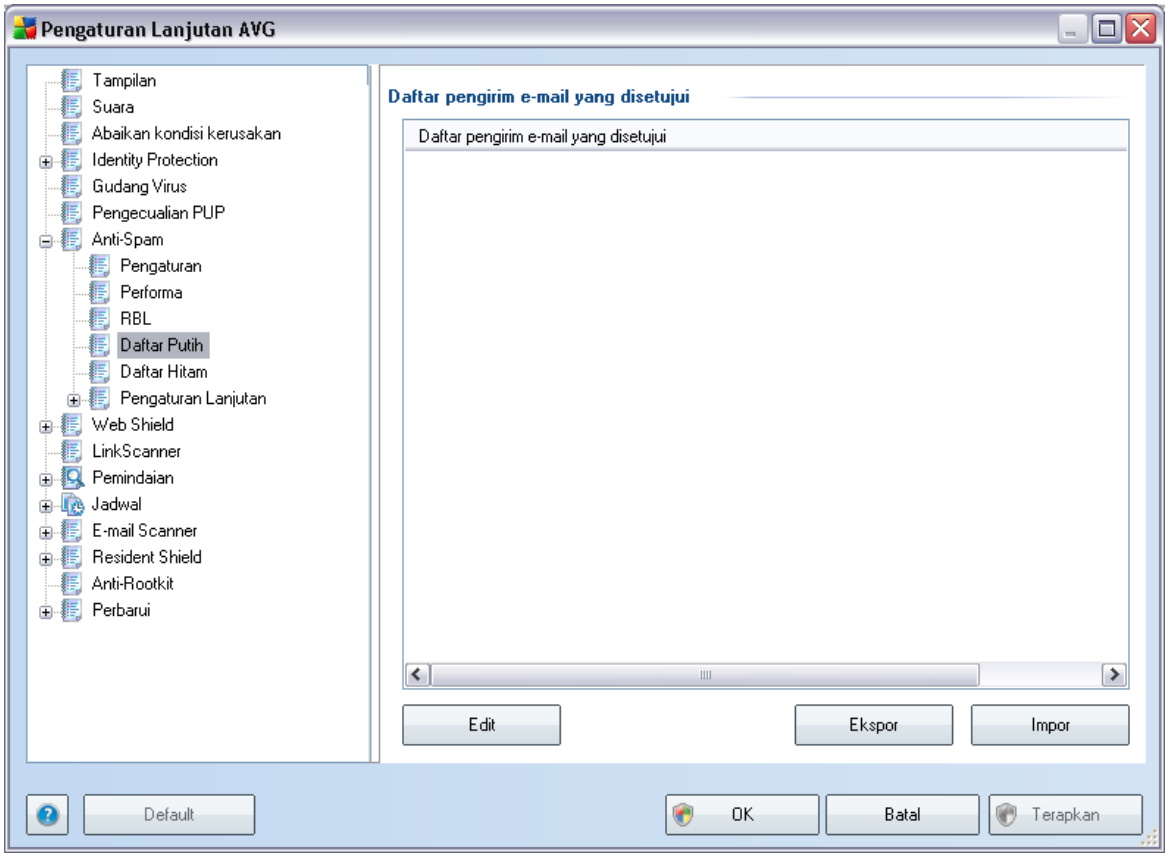
Daftar server RBL memungkinkan Anda menentukan lokasi server RBL tertentu.

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 mengirimi Anda pesan yang tidak diinginkan (spam). Anda juga dapat mengompilasi daftar nama domain lengkap (*misalnya avg.com*), yang Anda tahu tidak akan membuat pesan spam.

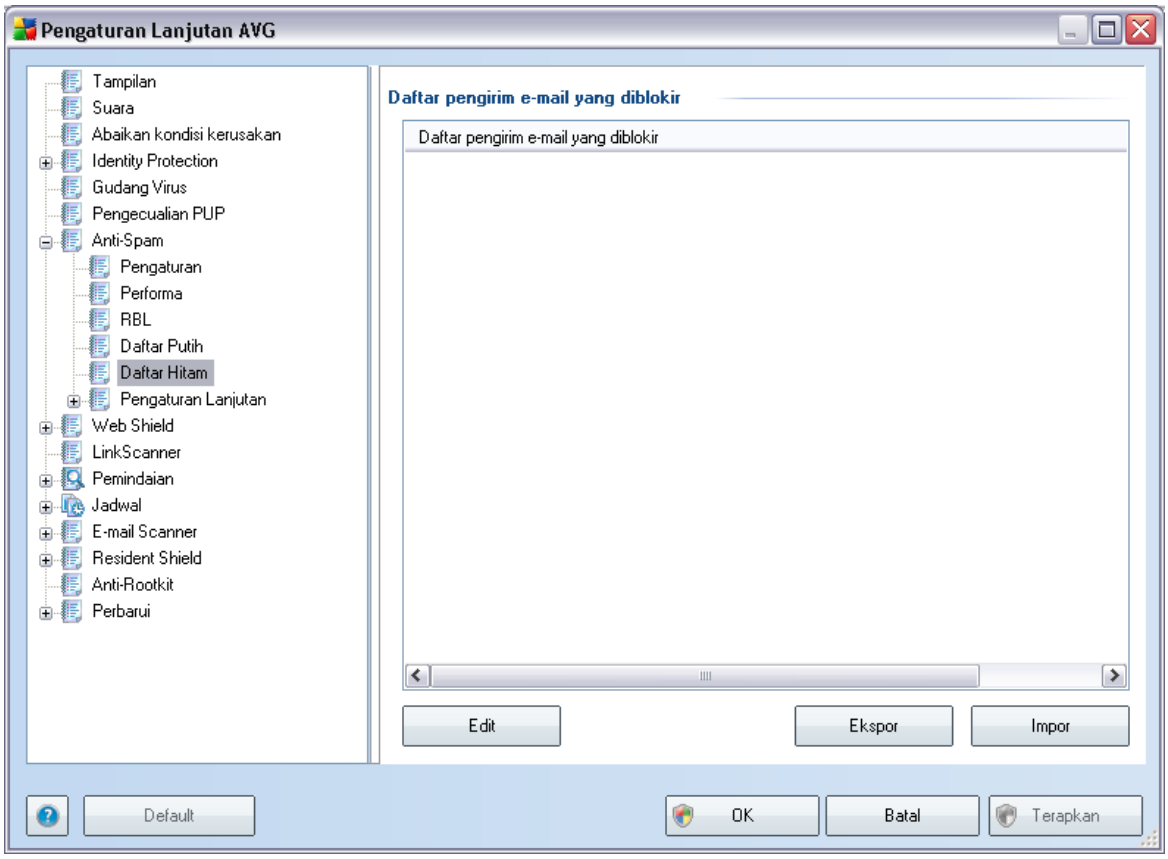
Setelah Anda membuat daftar pengirim dan/atau nama domain, Anda dapat mengisinya dengan salah satu metode berikut: dengan memasukkan langsung setiap alamat e-mail atau dengan mengimpor seluruh daftar alamat sekaligus. Tombol kontrol berikut ini tersedia:

- ***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. File masukan ini harus dalam format teks biasa, dan isinya 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 domain pengirim yang diblokir, yang pesannya selalu ditandai sebagai spam.



Dalam antarmuka pengeditan, Anda dapat mengompilasi daftar pengirim yang Anda perkirakan akan mengirimi Anda pesan yang tidak diinginkan (spam). Anda juga dapat mengompilasi daftar nama domain lengkap (*misalnya spammingcompany.com*), yang Anda perkirakan atau pernah terima pesan spam darinya. Semua e-mail dari alamat/domain yang tercantum akan dikenali sebagai spam.

Setelah Anda membuat daftar pengirim dan/atau nama domain, Anda dapat

mengisinya dengan salah satu metode berikut: dengan memasukkan langsung setiap alamat e-mail atau dengan mengimpor seluruh daftar alamat sekaligus. Tombol kontrol 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. File masukan ini harus dalam format teks biasa, dan isinya hanya boleh berisi satu item (*alamat, nama domain*) per baris.

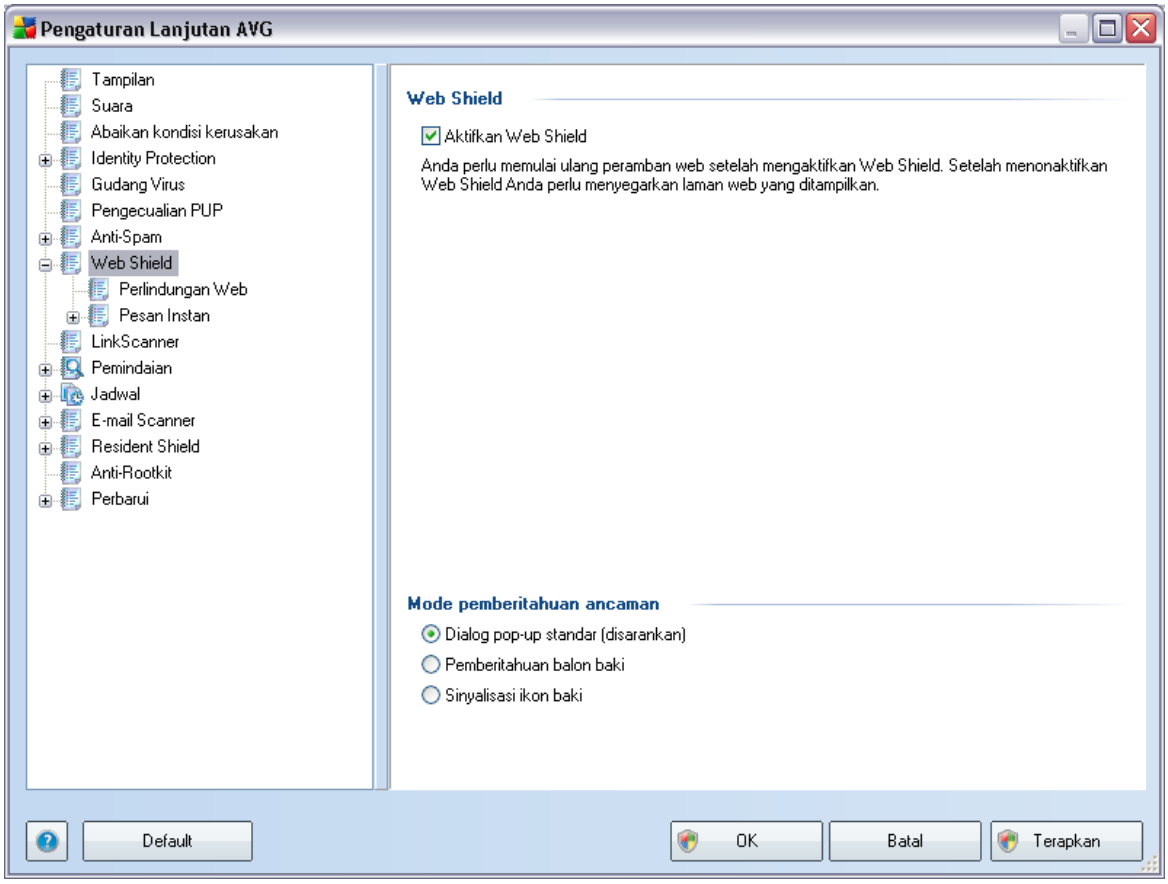
9.7.6. Pengaturan Lanjutan

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

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*** - pelatihan kata, riwayat skor, offset skor, entri kata maksimum, ambang batas pelatihan otomatis, bobot, buffer penulisan
- ***Pemfilteran*** - daftar bahasa, daftar negara, IP yang disetujui, IP yang diblokir, negara yang diblokir, charset yang diblokir, pengirim yang diperdaya
- ***RBL*** - server RBL, multihit, ambang batas, batas waktu, IP maksimum
- ***Koneksi internet*** - batas waktu

9.8. Perisai Web



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

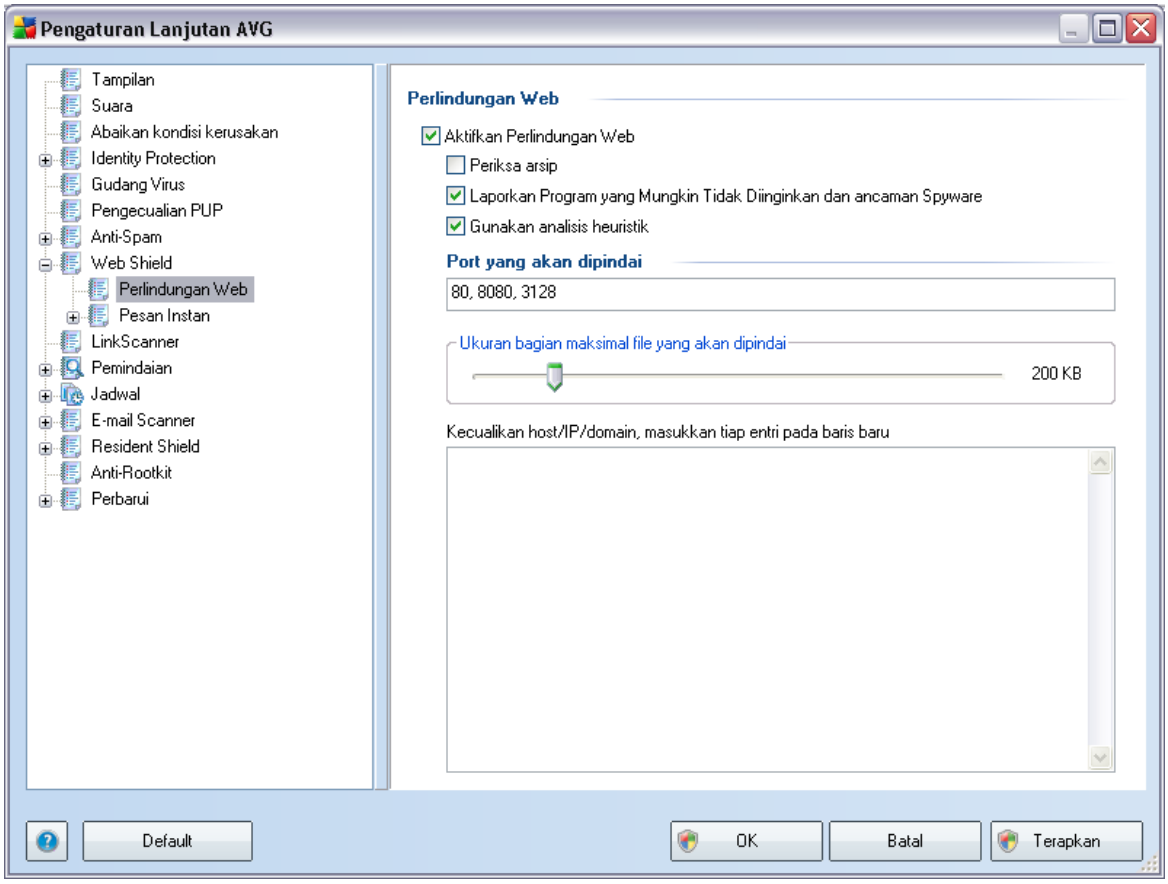
- ***Perlindungan Web***
- ***Pesan Instan***

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 ***Perisai Web*** harus melakukan pemindaian isi laman www. Asalkan opsi ini diaktifkan (*secara default*), Anda dapat mengaktifkan/menonaktifkan item ini:
    - ***Periksa arsip*** - memindai isi arsip yang mungkin telah dimasukkan di laman www yang akan ditampilkan.
    - ***Laporkan Program yang Mungkin Tidak Diinginkan dan Ancaman***

Spyware - memindai program yang mungkin tidak diinginkan (*program yang dapat dijalankan, yang dapat berjalan sebagai spyware atau adware*) yang dimasukkan di laman www untuk ditampilkan, dan infeksi spyware.

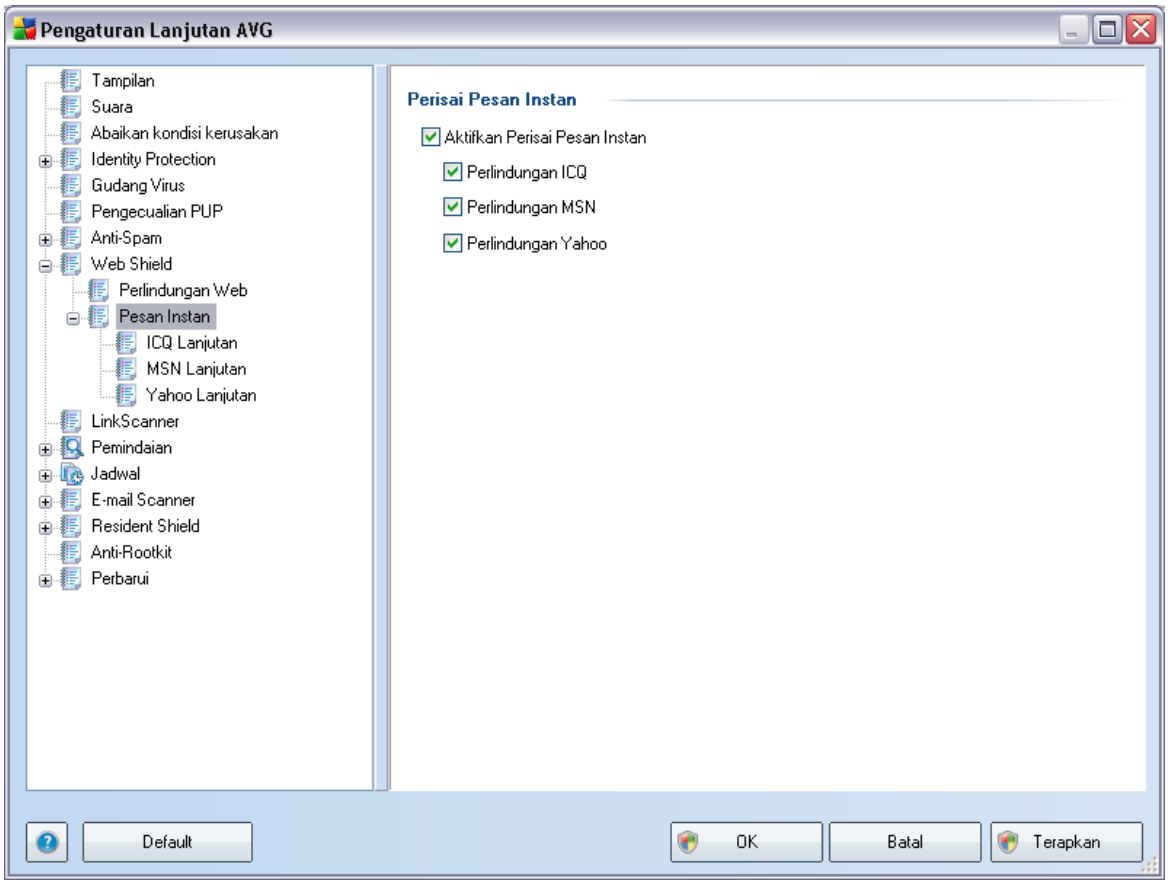
- ***Gunakan analisis heuristik*** - memindai isi laman yang akan ditampilkan, menggunakan metode analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*).

- ***Port yang akan dipindai*** - bidang ini mencantumkan daftar nomor port komunikasi http standar. Jika konfigurasi komputer Anda berbeda, Anda dapat mengubah nomor port, bila perlu.

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

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

9.8.2. Pesan Instan

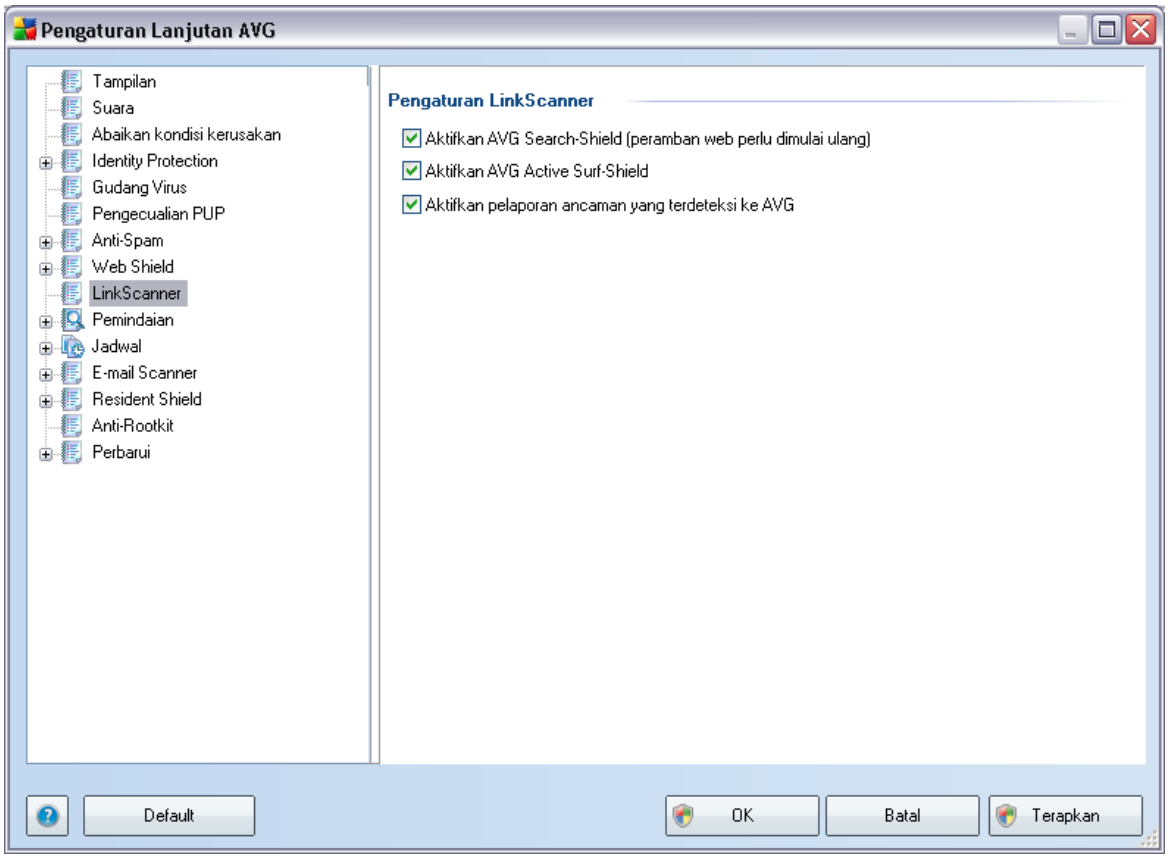


Dalam dialog ***Perisai Pesan Instan*** Anda dapat mengedit pengaturan komponen ***Perisai Web*** yang mengacu pada pemindaian pesan instan. Saat ini, mendukung tiga program pesan instan berikut: ***ICQ***, ***MSN***, dan ***Yahoo*** - centang item terkait untuk setiap item jika Anda ingin ***Perisai Web*** 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 AVG Search-Shield*** - (*diaktifkan secara default*): ikon pemberitahuan saran penelusuran yang dijalankan di Google, Yahoo, MSN, atau Baidu setelah sebelumnya memeriksa konten situs yang dihasilkan oleh mesin telusur.

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

- ***Aktifkan pelaporan ancaman yang terdeteksi ke AVG*** - (*diaktifkan secara*

default): centang item ini untuk memungkinkan pelaporan eksploit dan situs jahat yang ditemukan pengguna melalui ***AVG Active Surf-Shield*** atau ***AVG Search-Shield*** untuk memasok basis data yang mengumpulkan informasi mengenai aktivitas merusak pada web.

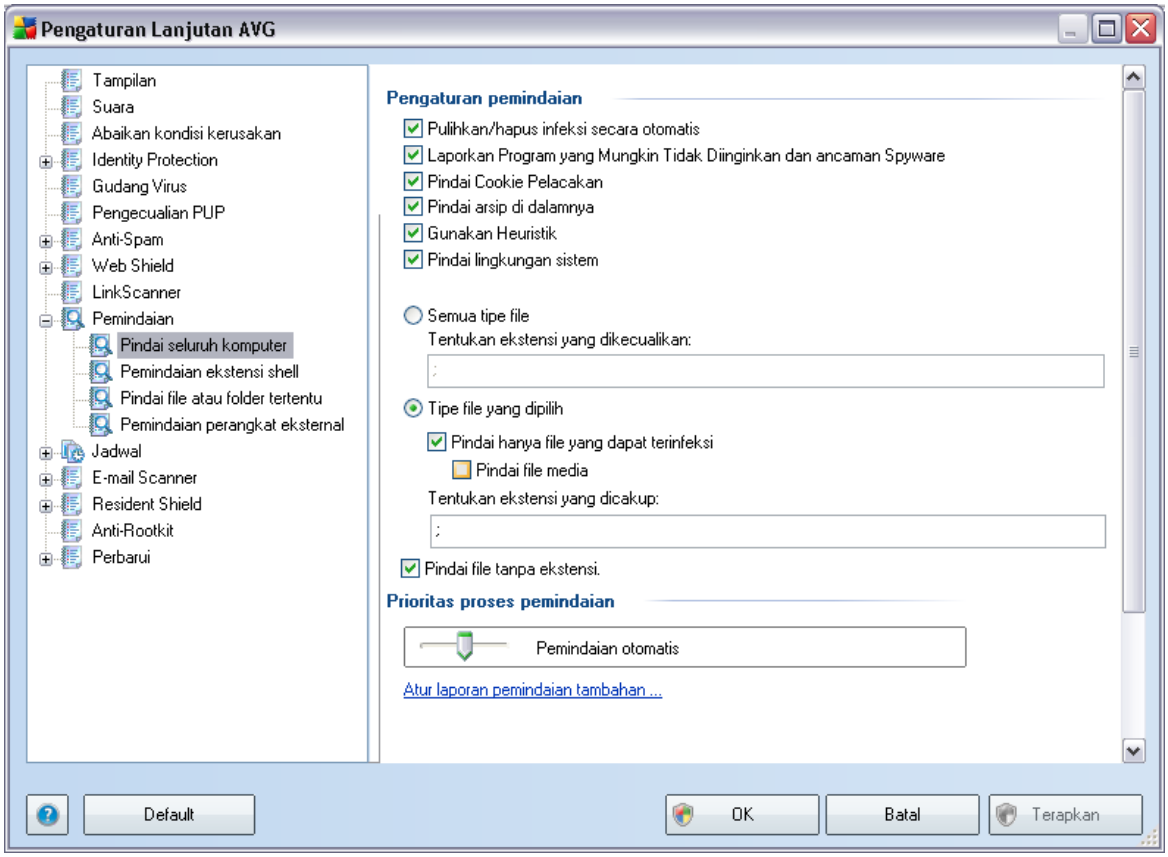
9.10. Pemindaian

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

- ***Pindai Seluruh Komputer*** - pemindaian standar yang ditentukan atas 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 Seluruh Komputer

Opsi ***Pindai seluruh komputer***memungkinkan Anda mengedit parameter salah satu pemindaian yang telah ditentukan oleh vendor perangkat lunak, ***Pindai seluruh komputer***:



Pengaturan pindai

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

- ***Pulihkan/hapus infeksi secara otomatis*** - jika ada virus teridentifikasi selama pemindaian, ia dapat dipulihkan otomatis jika penawarnya tersedia. Jika 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. Metode yang disarankan adalah menghapus file yang terinfeksi ke Gudang Virus.

- ***Laporkan Program Yang Mungkin Tidak Diinginkan dan Ancaman Spyware*** - parameter ini mengontrol fungsionalitas ***Anti-Virus*** yang memungkinkan deteksi terhadap program yang mungkin tidak diinginkan (*file*

yang dapat dijalankan sebagai spyware atau adware) dan semua ini kemudian diblokir atau dihapus;

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

- ***Pindai di dalam arsip*** - parameter ini menentukan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut tersimpan dalam arsip, misalnya, ZIP, RAR, ...

- ***Gunakan Heuristik*** - 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*** - pemindaian juga akan memeriksa area sistem komputer Anda.

Selanjutnya, Anda harus menentukan apakah Anda ingin memindai

- ***Semua tipe file*** yang menyertakan kemungkinan penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisahkan koma yang tidak harus dipindai; atau

- ***Tipe file yang dipilih*** - Anda dapat menetapkan 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 dicentang, 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 menetapkan file mana yang harus selalu dipindai berdasarkan ekstensinya.

- 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.

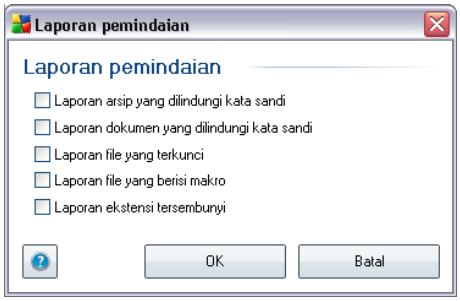
Prioritas proses pindai

Di bagian ***Prioritas proses pindai*** Anda dapat menetapkan lebih jauh kecepatan

pemindaian sesuai dengan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke penggunaan sumber daya secara otomatis tingkat sedang. 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.

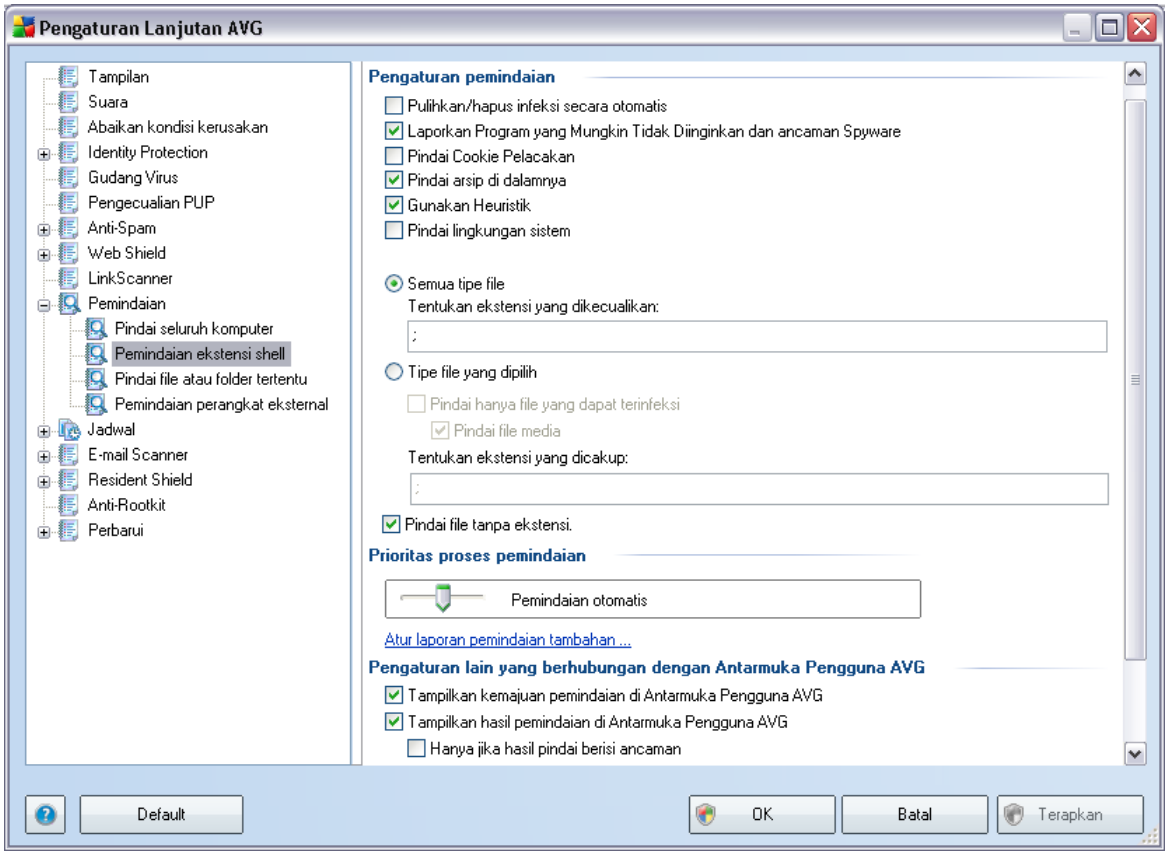
Atur laporan pindai tambahan...

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



9.10.2. Pemindaian Ekstensi Shell

Seperti pada item ***Pindai seluruh komputer*** sebelumnya, item 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***:

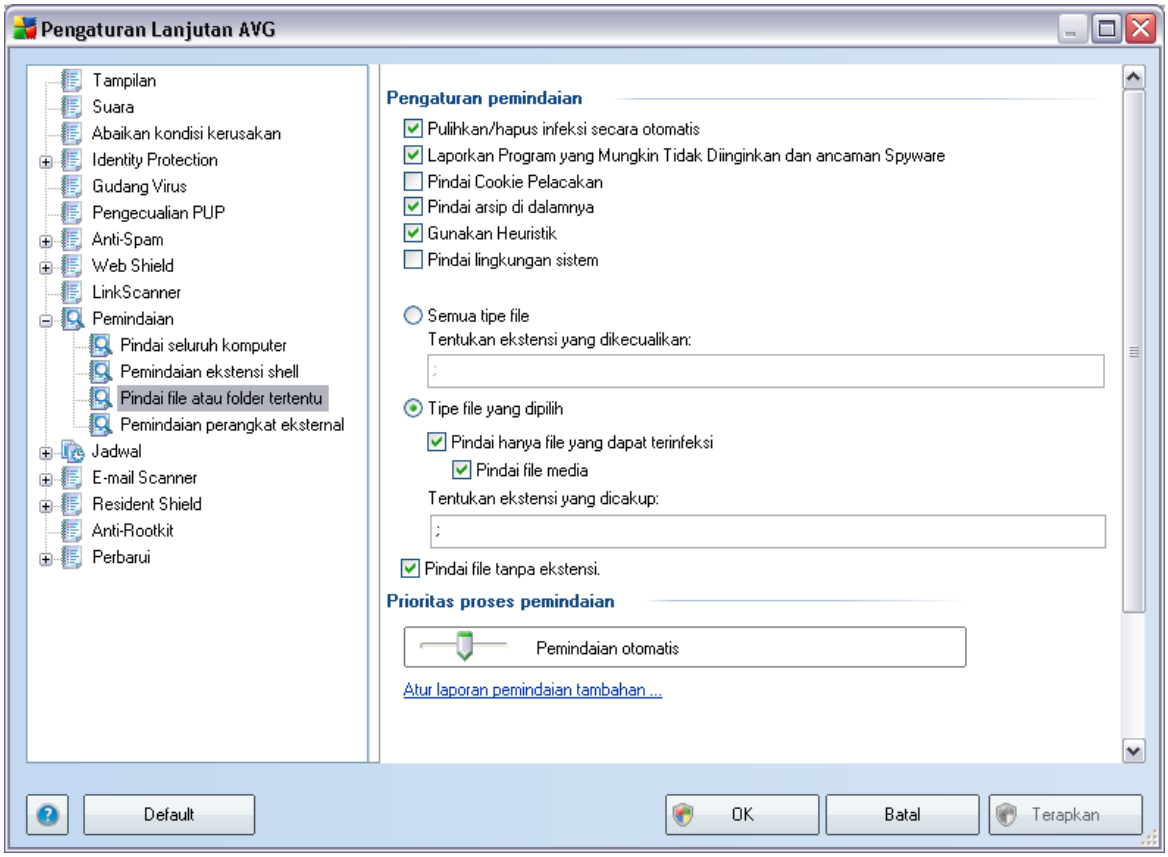


Daftar parameter identik dengan yang tersedia untuk ***Pindai seluruh komputer***. Walau demikian, pengaturan default berbeda: pada ***Pemindaian Seluruh Komputer*** sebagian besar parameter dipilih sedangkan untuk ***Pemindaian ekstensi shell*** (***Pemindaian di Windows Explorer***) hanya parameter yang relevan yang diaktifkan.

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

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***:

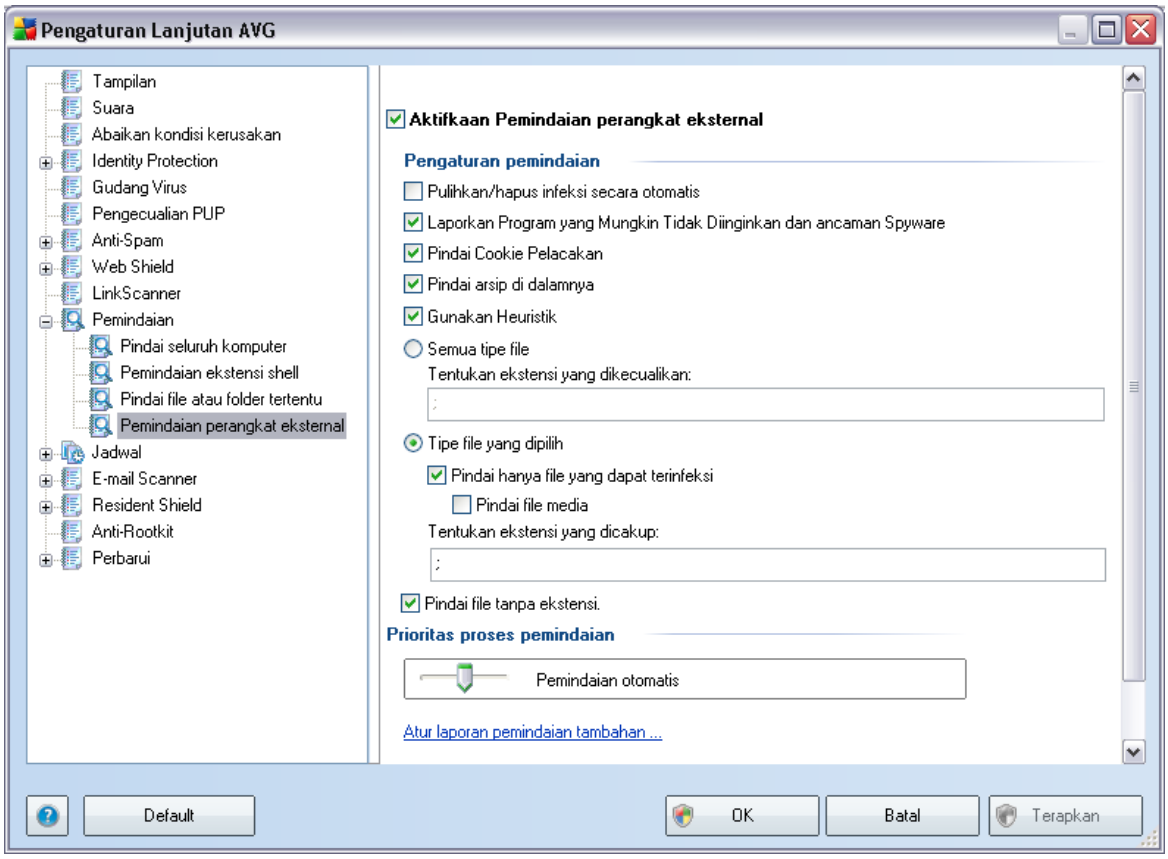


Semua parameter yang diatur dalam dialog konfigurasi ini hanya berlaku untuk area yang dipilih bagi pemindaian dengan ***Pindai file atau folder tertentu***! Jika Anda menandai opsi ***Pindai rootkit*** dalam dialog konfigurasi ini, hanya tes rootkit cepat yang akan dilakukan, yakni pemindaian rootkit pada area yang dipilih saja.

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***.

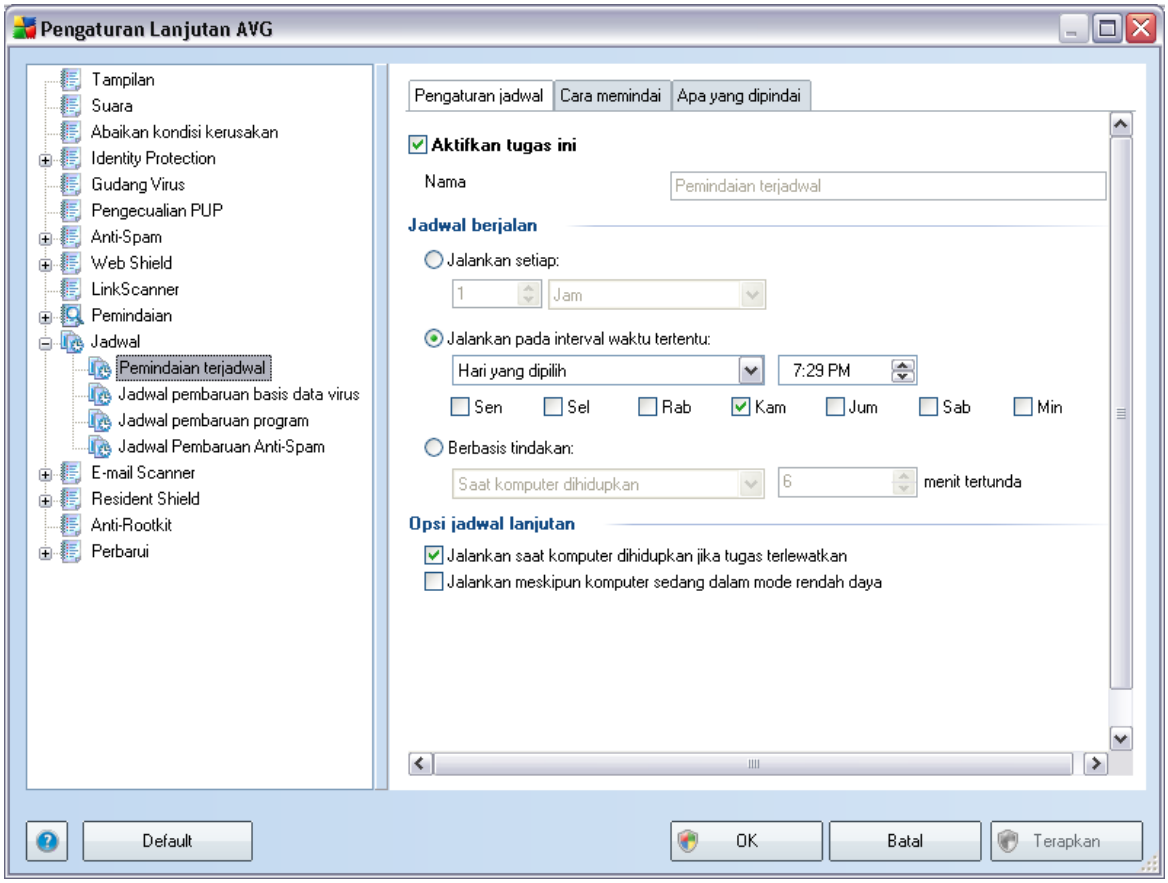
9.11. Jadwal

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

- Jadwal pemindaian seluruh komputer
- Jadwal pembaruan basis data virus
- Jadwal pembaruan program
- Jadwal pembaruan Anti-Spam

9.11.1. Pemindaian Terjadwal

Parameter pemindaian yang telah dijadwalkan dapat diedit (*atau jadwal baru yang telah diatur*) pada ketiga tab:



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, dalam bidang teks ***Nama*** (*menonaktifkan 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

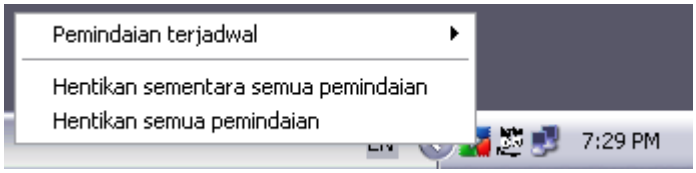
Di sini, Anda dapat menetapkan interval waktu untuk peluncuran pemindaian yang baru dijadwalkan. Penentuan waktu dapat ditentukan dengan pengulangan peluncuran pemindaian setelah periode waktu tertentu (***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada interval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

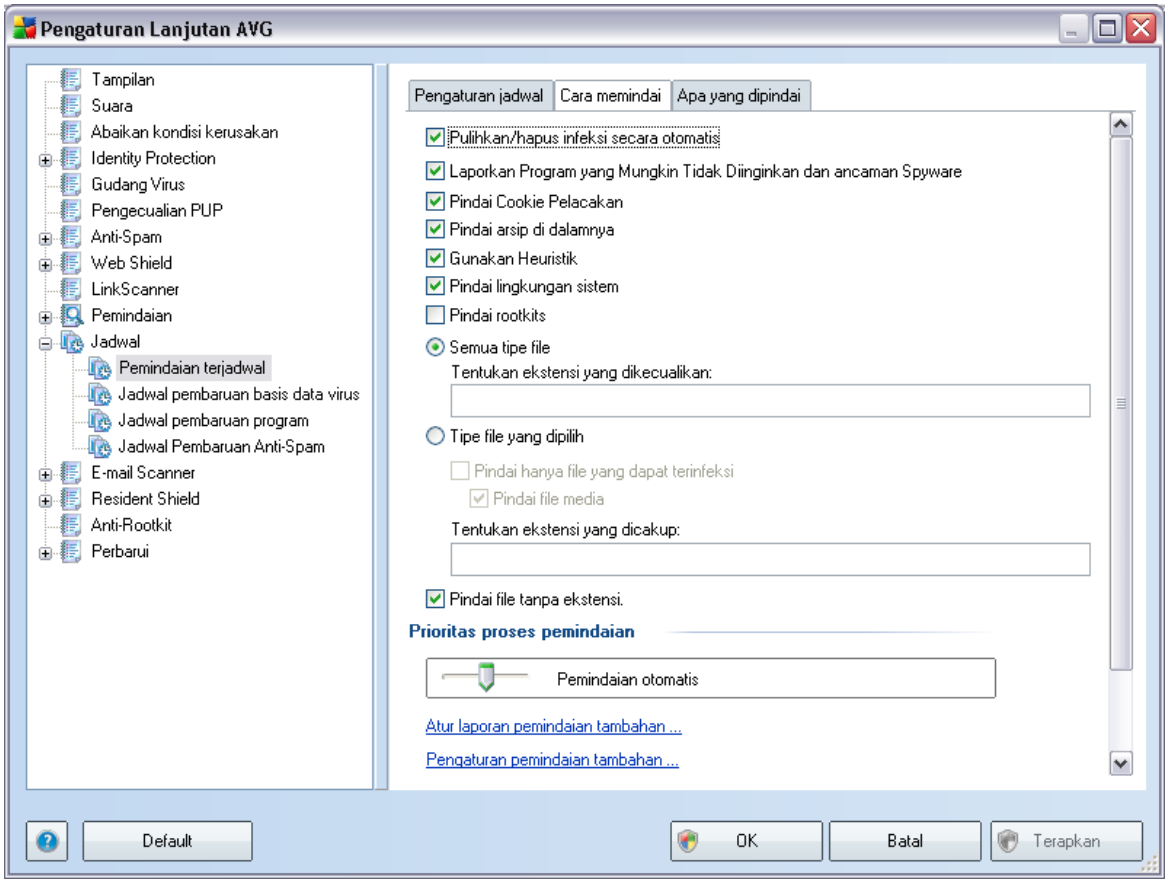
Opsi jadwal lanjutan

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

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 baru kemudian muncul (*dengan penuh warna bersama panah putih - lihat gambar di atas*) memberi tahu adanya pemindaian terjadwal yang sedang dijalankan. Klik kanan pada ikon pemindaian AVG yang sedang berjalan untuk membuka menu konteks di mana Anda dapat memutuskan untuk menghentikannya sementara atau bahkan menghentikan sama sekali pemindaian yang sedang berjalan tersebut:





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 sah untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditentukan:

- ***Pulihkan/hapus infeksi secara otomatis*** - (*telah diaktifkan, secara default*): jika ada virus terdeteksi selama pemindaian, ia dapat dipulihkan otomatis jika penawarnya tersedia. Jika 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*** - (*telah diaktifkan, secara default*): parameter ini mengontrol fungsionalitas Anti-Virus yang memungkinkan deteksi terhadap program yang mungkin tidak diinginkan (*file eksekusi yang dapat dijalankan sebagai spyware atau adware*) dan semua ini kemudian diblokir atau dihapus;

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

- ***Pindai di dalam arsip*** - (*telah diaktifkan, secara default*): parameter ini menentukan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut tersimpan dalam arsip, seperti ZIP, RAR, ...

- ***Gunakan Heuristik*** - (*telah 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*** - (*telah diaktifkan, secara default*): pemindaian juga akan memeriksa area sistem komputer Anda;

- ***Pindai rootkit*** - tandai item ini jika Anda ingin menyertakan deteksi rootkit ke pemindaian seluruh komputer. Deteksi rootkit juga tersedia pada komponen ***Anti-Rootkit*** sendiri;

Selanjutnya, Anda harus menentukan apakah Anda ingin memindai

- ***Semua tipe file*** dengan kemungkinan menentukan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang tidak boleh dipindai yang dipisahkan dengan koma; atau

- ***Tipe file yang dipilih*** - Anda dapat menetapkan 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*

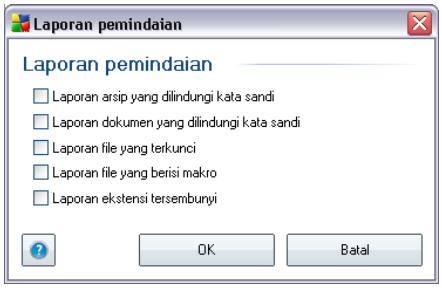
kemungkinannya untuk terinfeksi virus). Sekali lagi, Anda dapat menetapkan ekstensi file yang harus selalu dipindai.

- 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.

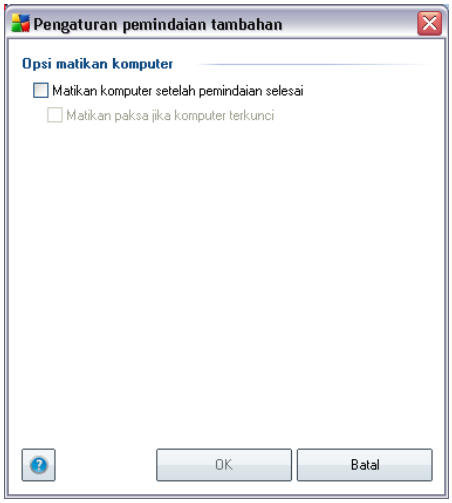
Prioritas proses pemindaian

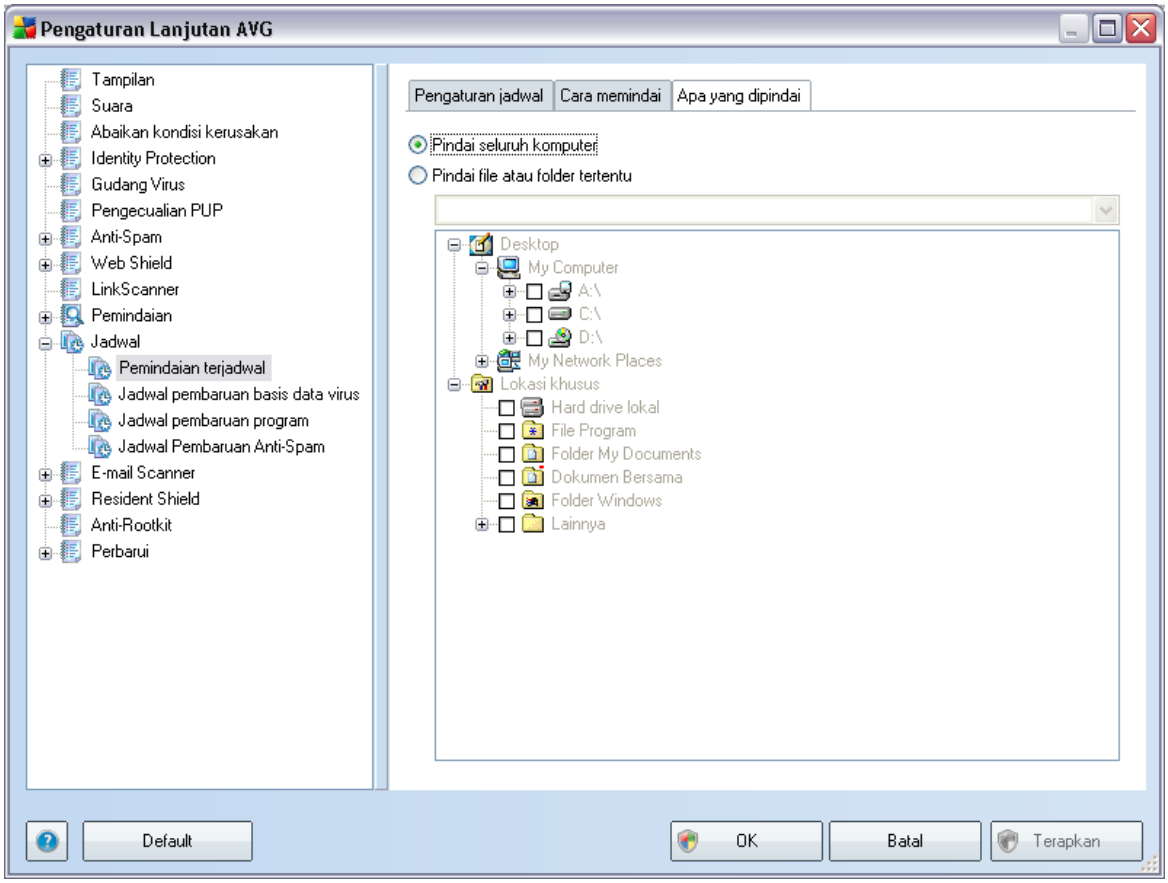
Di bagian ***Prioritas proses pemindaian*** Anda dapat menetapkan lebih lanjut kecepatan pemindaian menurut penggunaan sumber daya sistem. Secara default, opsi ini diatur ke penggunaan sumber daya secara otomatis tingkat sedang. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu 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.

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



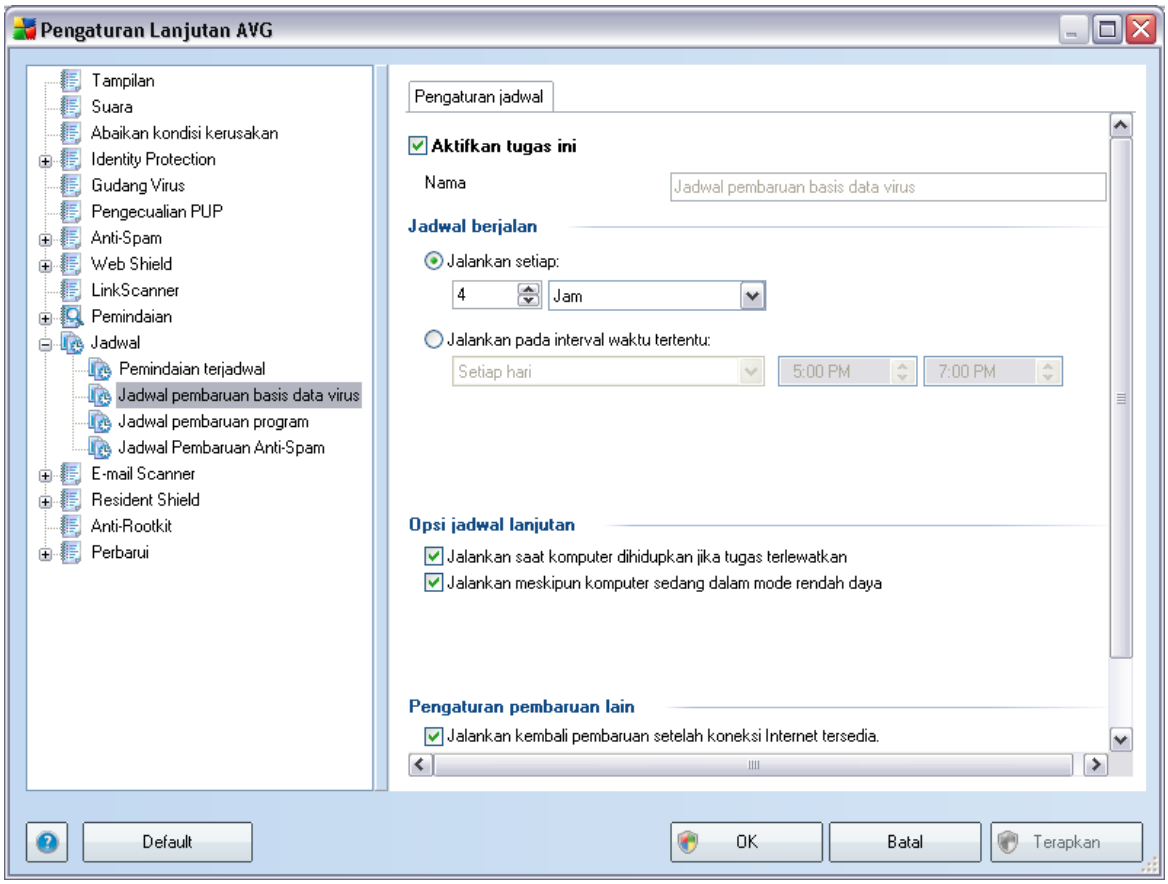
Klik ***Pengaturan pemindaian tambahan ...*** untuk membuka dialog baru ***Opsi matikan komputer*** di mana Anda dapat memutuskan apakah komputer harus dimatikan secara otomatis setelah proses pemindaian selesai. Dengan mengonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah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


Pengaturan pemindaian tambahan
Opsi matikan komputer
Matikan komputer setelah pemindaian selesai
Matikan paksa jika komputer terkunci
OK
Batal



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



Pada tab ***Pengaturan jadwal*** Anda dapat mencentang/tidak mencentang item ***Aktifkan tugas ini*** terlebih dahulu untuk menonaktifkan pembaruan basis data virus yang telah dijadwalkan untuk sementara, dan mengaktifkannya lagi saat diperlukan.

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*** (*menonaktifkan 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* ***Jadwal pembaruan basis data virus*** *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 yang singkat dan deskriptif bagi jadwal Anda agar nanti lebih mudah mengenalinya.

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

Opsi jadwal lanjutan

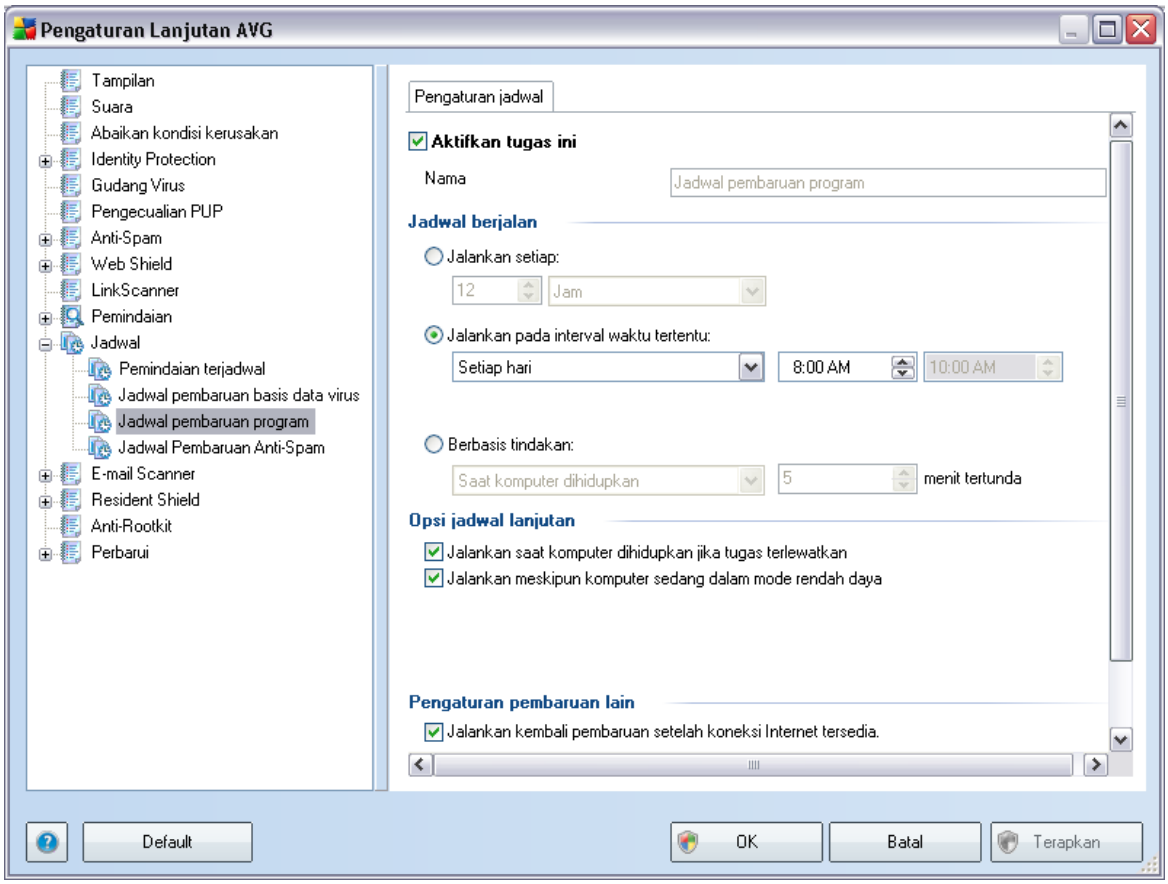
Di bagian ini Anda dapat menentukan dalam kondisi apa pembaruan basis data virus harus/tidak harus diluncurkan jika komputer dalam mode daya rendah atau dimatikan sama sekali.

Pengaturan pembaruan lain

Akhirnya, centang opsi ***Jalankan lagi pembaruan begitu koneksi Internet tersedia*** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan gagal, ia 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 sembul 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



Pada tab ***Pengaturan jadwal*** Anda dapat mencentang/tidak mencentang item ***Aktifkan tugas ini*** terlebih dahulu untuk menonaktifkan pembaruan program yang telah dijadwalkan untuk sementara, dan mengaktifkannya lagi saat diperlukan.

Dalam bidang teks ***Nama*** (*menonaktifkan semua jadwal default*) terdapat nama yang ditetapkan ke jadwal ini oleh vendor program . Untuk jadwal yang baru ditambahkan (*Anda dapat menambahkan jadwal baru dengan mengklik-kanan mouse di atas item* ***Jadwal pembaruan program*** *di struktur navigasi kiri*) Anda dapat menetapkan nama Anda sendiri, dan dalam hal ini bidang teks akan dibuka untuk pengeditan. Cobalah selalu gunakan nama yang singkat dan deskriptif bagi jadwal Anda agar nanti lebih mudah mengenalinya.

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 mengaitkan peluncuran pembaruan dengan (***Tindakan berdasar pengaktifan komputer***).

Opsi jadwal lanjutan

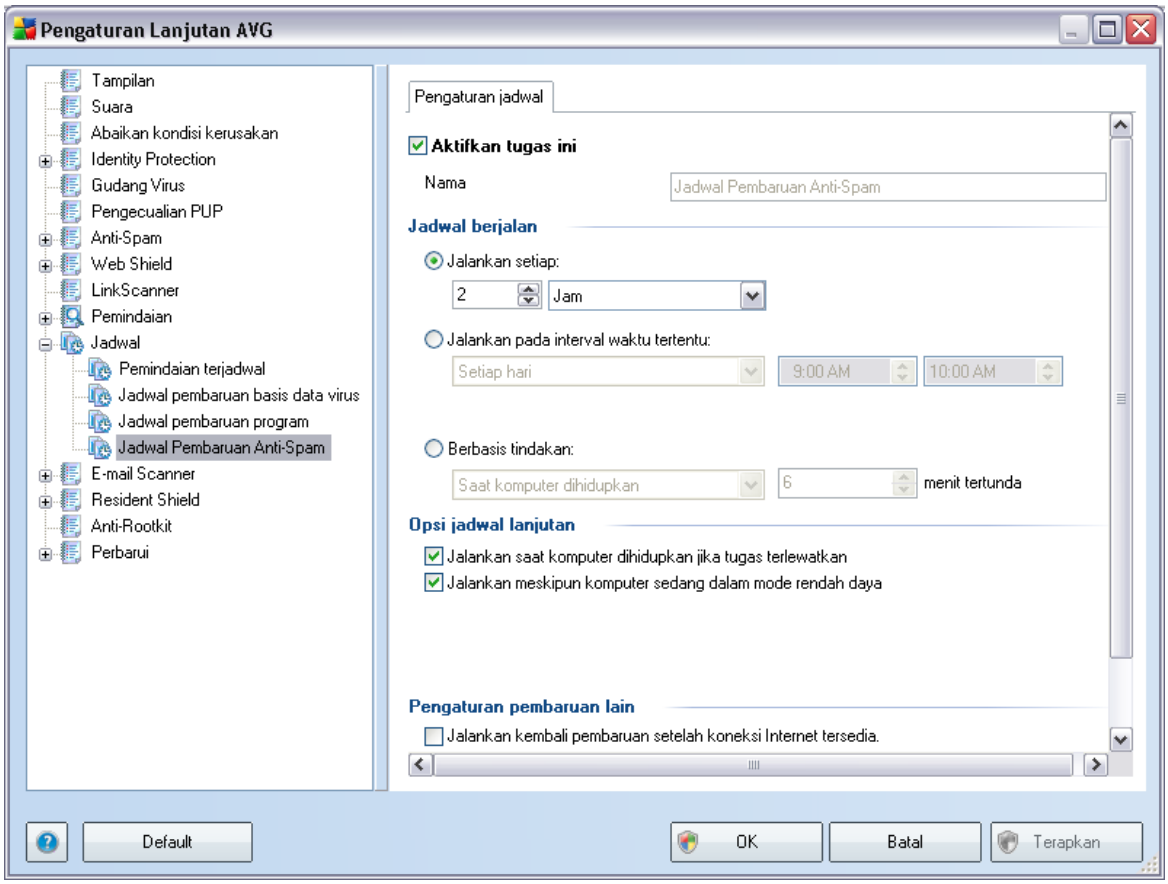
Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan program boleh/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

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 sembul yang muncul di atas ikon baki sistem AVG (*asalkan Anda telah membiarkan konfigurasi default pada dialog* ***Pengaturan Lanjutan/Tampilan***).

9.11.4. Jadwal Pembaruan Anti-Spam



Pada tab ***Pengaturan jadwal*** Anda dapat mencentang/tidak mencentang item ***Aktifkan tugas ini*** terlebih dahulu untuk menonaktifkan pembaruan ***Anti-Spam*** yang telah dijadwalkan untuk sementara, dan mengaktifkannya kembali bila perlu.

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*** (*menonaktifkan semua jadwal default*) terdapat nama yang ditetapkan ke jadwal ini oleh vendor program . Untuk jadwal yang baru ditambahkan (*Anda dapat menambahkan jadwal baru dengan mengklik kanan mouse pada item* ***Jadwal pembaruan Anti-Spam*** *di struktur navigasi kiri*) Anda dapat menetapkan nama Anda sendiri, dan untuk itu bidang teks akan dibuka untuk pengeditan. Cobalah selalu menggunakan nama yang singkat dan deskriptif bagi jadwal Anda agar nanti lebih mudah mengenalinya.

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 untuk mengaitkan peluncuran pembaruan dengan (***Tindakan berdasar pengaktifan komputer***).

Opsi jadwal lanjutan

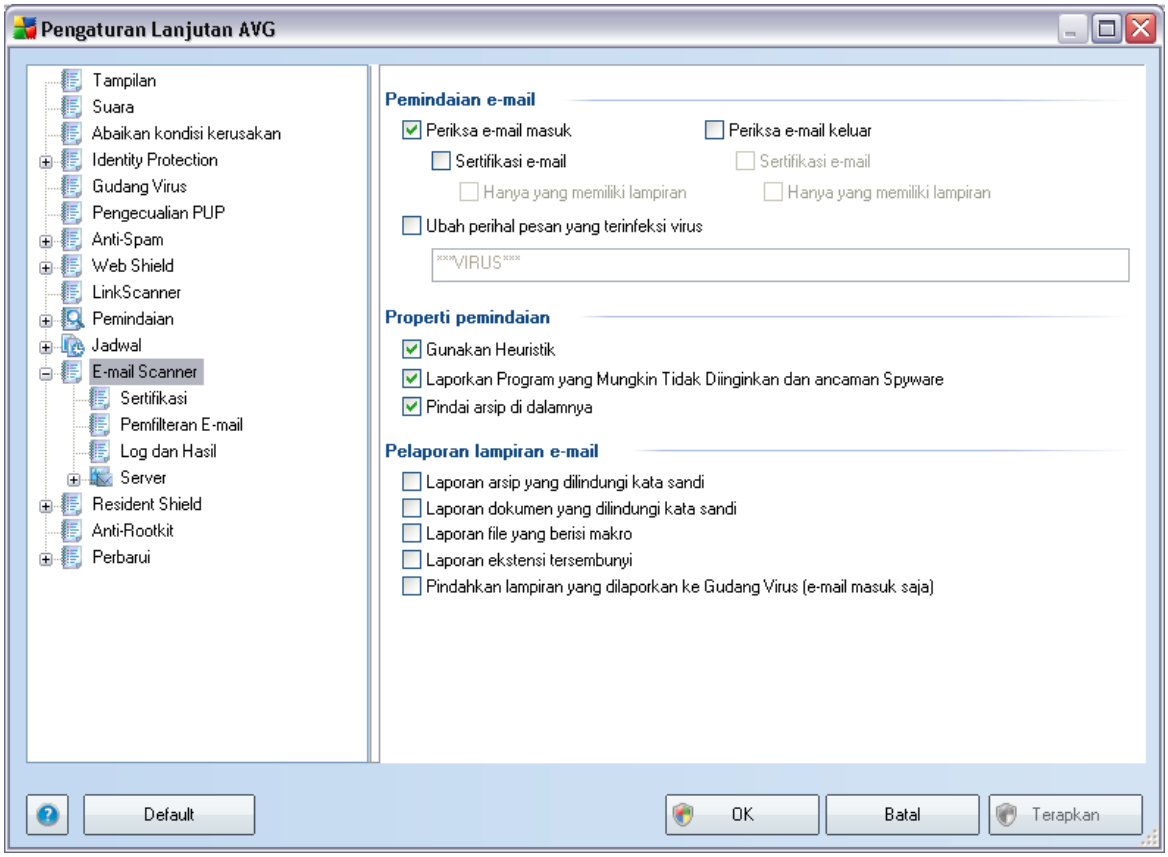
Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan ***Anti-Spam*** harus/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sama sekali.

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 diberi tahu mengenai hal ini melalui jendela sembul yang muncul di atas ikon baki sistem AVG (*asalkan Anda telah membiarkan konfigurasi default pada dialog* ***Pengaturan Lanjutan/Tampilan***).

9.12. Pemindai E-mail



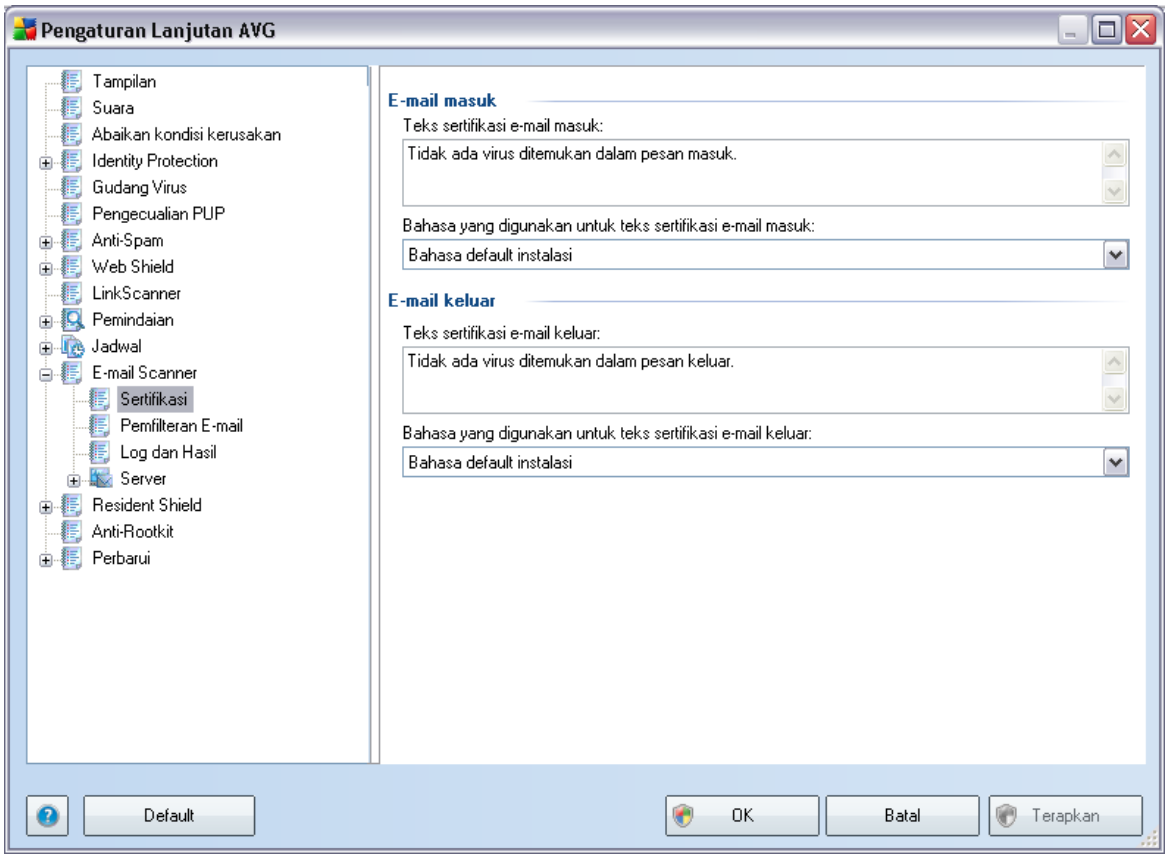
Dialog ***Pemindai E-mail*** terbagi ke dalam tiga bagian:

- ***Pemindaian e-mail*** - di bagian ini, pilih apakah Anda ingin memindai pesan e-mail masuk/keluar dan apakah semua e-mail harus disertifikasi atau hanya e-mail yang berisi lampiran (sertifikasi e-*mail bebas-virus tidak didukung dalam format HTML/RTF*). Selain itu, Anda dapat memilih jika ingin AVG mengubah perihal untuk pesan yang kemungkinan berisi virus. Centang kotak ***Ubah perihal pesan yang terinfeksi virus*** dan ubah pula teksnya (*nilai defaultnya* ****VIRUS****).

- ***Properti pemindaian*** - menetapkan apakah metode analisis heuristik harus digunakan saat memindai (***Gunakan heuristik***), apakah Anda ingin memeriksa adanya program yang mungkin tidak diinginkan (***Laporkan Program Yang Mungkin Tidak Diinginkan dan Ancaman Spyware***), dan apakah arsip harus dipindai juga (***Pindai di dalam arsip***).

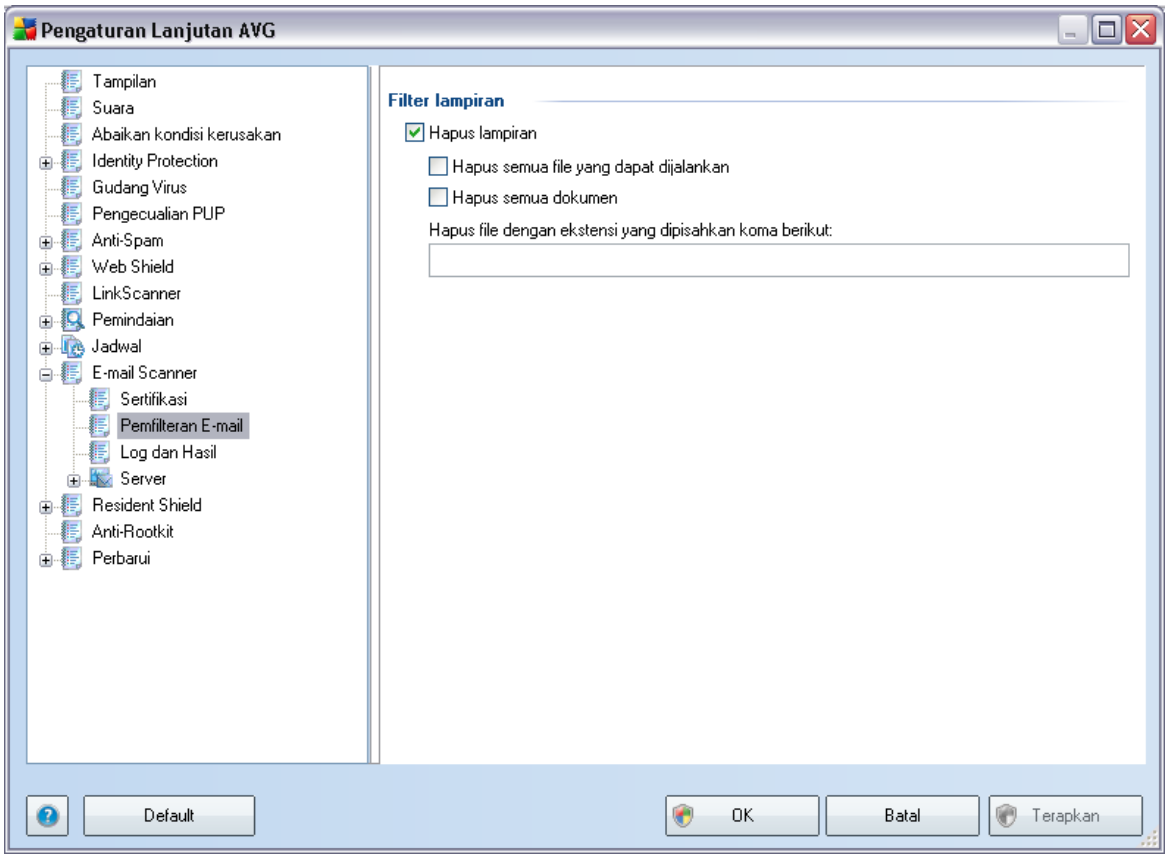
- ***Pelaporan lampiran e-mail*** - menetapkan apakah Anda ingin diberi tahu melalui e-mail tentang arsip yang dilindungi kata sandi, dokumen yang dilindungi kata sandi, file berisi makro dan/atau file dengan ekstensi tersembunyi yang terdeteksi sebagai lampiran pada pesan e-mail yang dipindai. Jika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

9.12.1. Sertifikasi



Dalam dialog ***Sertifikasi*** Anda dapat menetapkan secara persis teks apa yang akan dimuat dalam sertifikasi, dan bahasanya. Hal ini harus ditetapkan secara terpisah untuk ***E-mail masuk***dan ***E-mail keluar***.

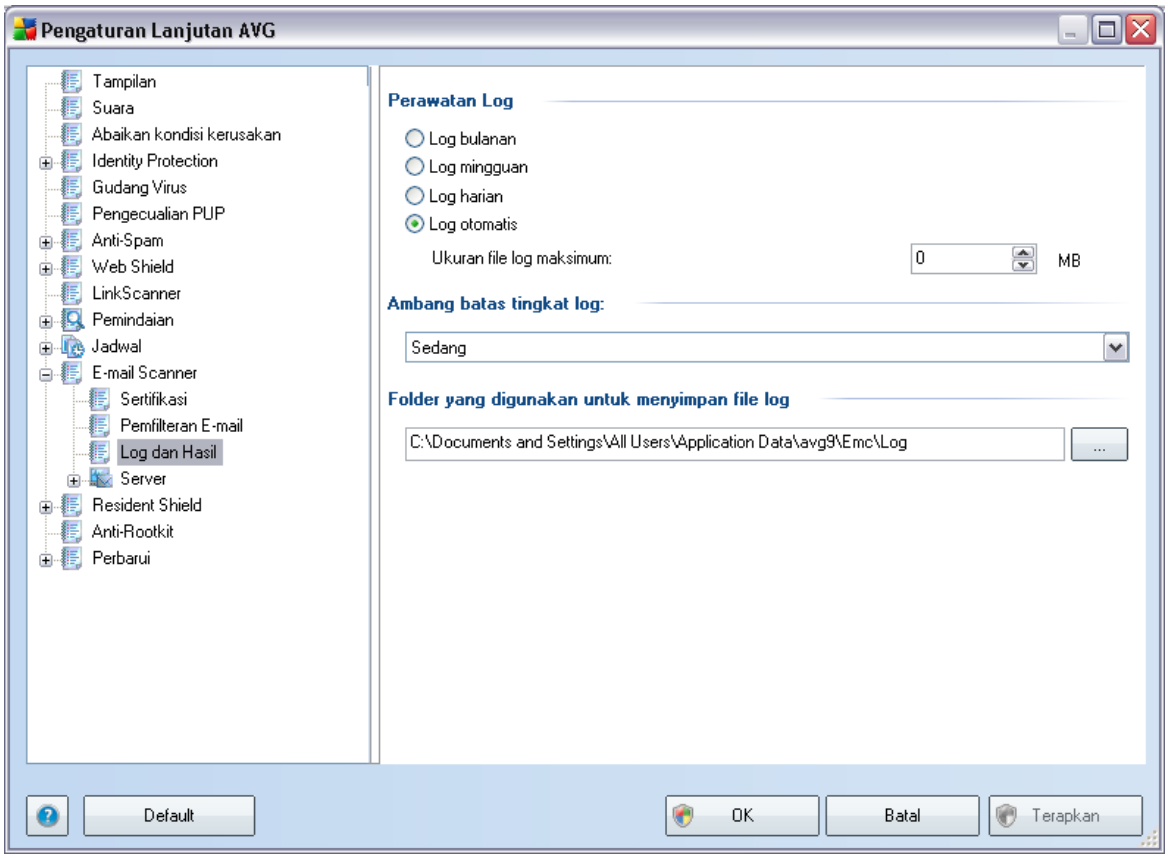
9.12.2. Pemfilteran E-mail



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 menentukan 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 akan dihapus
- ***Hapus file dengan ekstensi yang dipisahkan koma ini*** - akan menghapus semua file dengan ekstensi yang ditentukan

9.12.3. Log dan Hasil

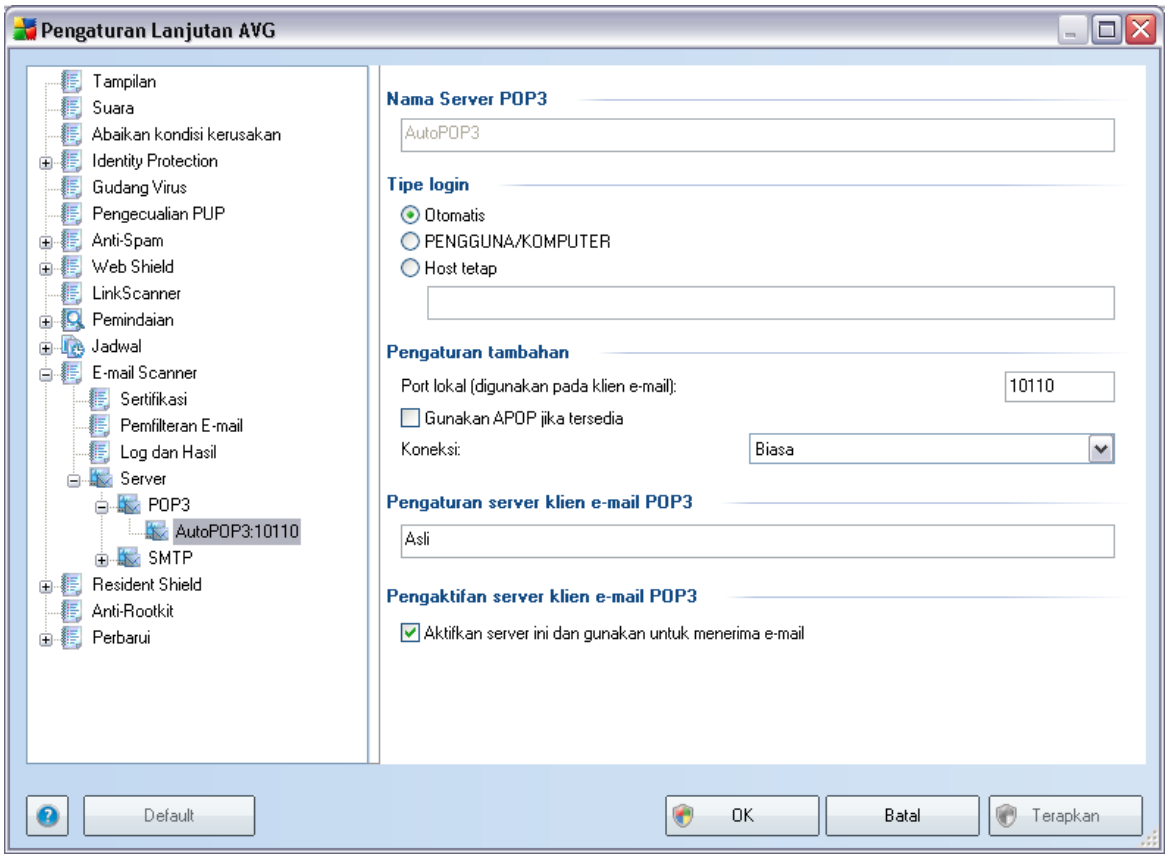


Dialog dibuka melalui item navigasi ***Log dan Hasil*** memungkinkan Anda menetapkan parameter bagi pemeliharaan hasil pemindaian e-mail. Dialog dibagi ke dalam beberapa bagian:

- ***Pemeliharaan Log*** - menentukan apakah Anda ingin merekam informasi pemindaian e-mail secara harian, mingguan, bulanan, ... ; juga menetapkan ukuran maksimum file log (*dalam MB*)
- ***Ambang batas tingkat log*** - tingkat sedang telah diatur secara default - Anda dapat memilih tingkat yang lebih rendah (*merekam informasi koneksi dasar ke dalam log*) atau tingkat yang lebih tinggi (*merekam semua lalu lintas ke dalam log*)
- ***Folder yang digunakan untuk menyimpan file log*** - menentukan tempat penyimpanan file log

9.12.4. 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 E-mail*** dengan menggunakan protokol POP3 untuk e-mail masuk:

- ***Nama Server POP3*** - ketikkan nama server atau biarkan nama default AutoPOP3
- ***Tipe login*** - menentukan metode untuk menentukan server e-mail yang digunakan bagi e-mail masuk:
    - ***Otomatis*** - Login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda.

- ***PENGGUNA/KOMPUTER*** - metode paling sederhana dan paling banyak digunakan untuk menentukan server email tujuan adalah metode proxy. Untuk menggunakan metode ini, tetapkan nama atau alamat (atau juga port) sebagai bagian dari nama pengguna login untuk server e-mail tersebut, yang dipisahkan dengan karakter /. Sebagai contoh, untuk akun pengguna1 pada server pop.acme.com dan port 8200 Anda akan menggunakan pengguna1/pop.acme.com:8200 sebagai nama login.

- ***Host tetap*** - Dalam kasus ini, program akan selalu menggunakan server yang ditetapkan 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) atau alamat IP (misalnya, 123.45.67.89). Jika server e-mail menggunakan port non-standar, Anda dapat menetapkan 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*** - menetapkan parameter yang lebih terperinci:

  - ***Port lokal*** - menetapkan port yang akan dicari oleh aplikasi e-mail Anda untuk berkomunikasi. Anda kemudian harus menetapkan port ini sebagai port untuk komunikasi POP3 dalam aplikasi e-mail Anda.

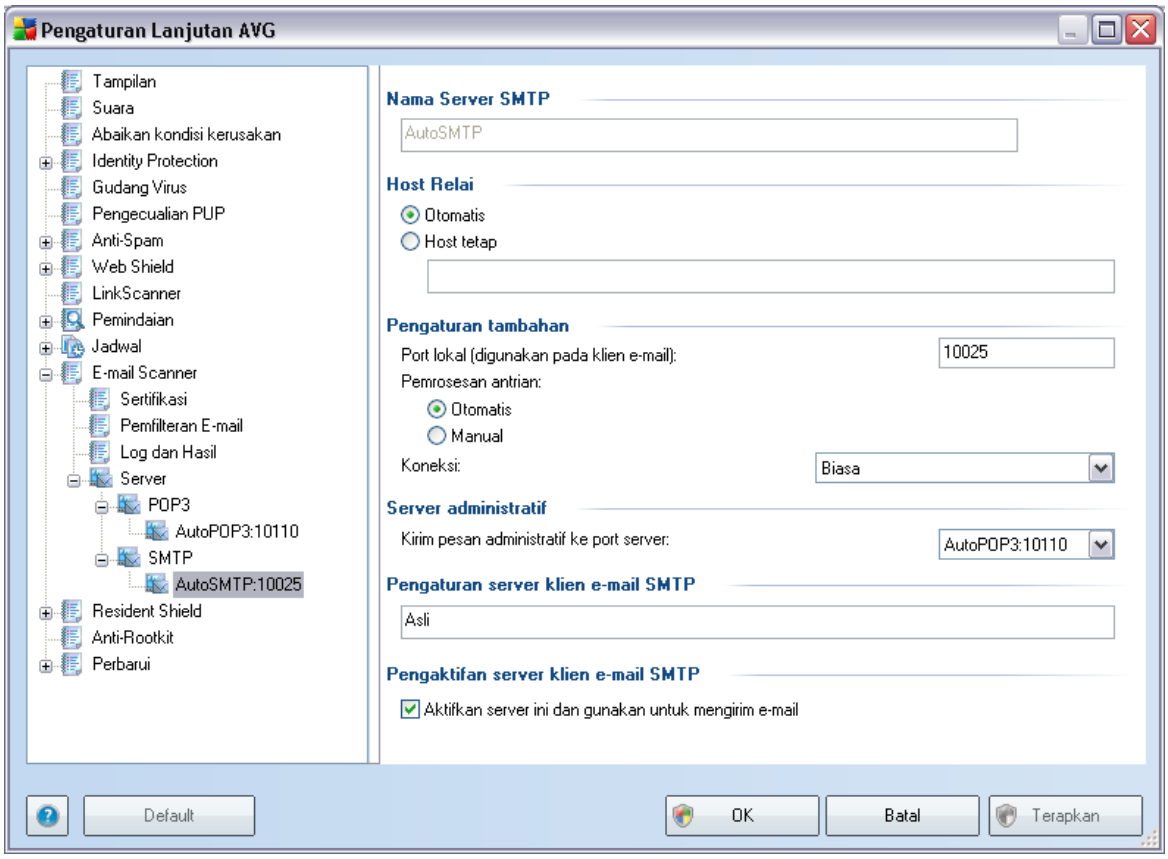
  - ***Gunakan APOP bila tersedia*** - opsi ini menyediakan login server e-mail yang lebih aman. Ini memastikan ***Pemindai E-mail*** menggunakan metode alternatif untuk meneruskan kata sandi akun pengguna untuk login, mengirimkan kata sandi tersebut ke server tidak dalam keadaan terbuka melainkan dalam format terenkripsi dengan menggunakan rantai variabel yang diterima dari server. Tentu saja, fitur ini hanya tersedia bila server e-mail tujuan mendukungnya.

  - ***Koneksi*** - dalam menu buka bawah, Anda dapat menetapkan 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*** - menyediakan informasi singkat mengenai pengaturan konfigurasi yang diperlukan untuk mengonfigurasi klien e-mail Anda dengan benar (sehingga ***Pemindai E-mail*** akan memeriksa semua e-mail masuk). Ringkasan ini didasarkan pada parameter yang terkait yang ditetapkan dalam dialog ini dan dialog lain yang terkait.

- ***Aktivasi server POP3 klien e-mail*** - centang/hapus centang pada item ini

untuk mengaktifkan atau menonaktifkan server POP3 yang ditetapkan



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

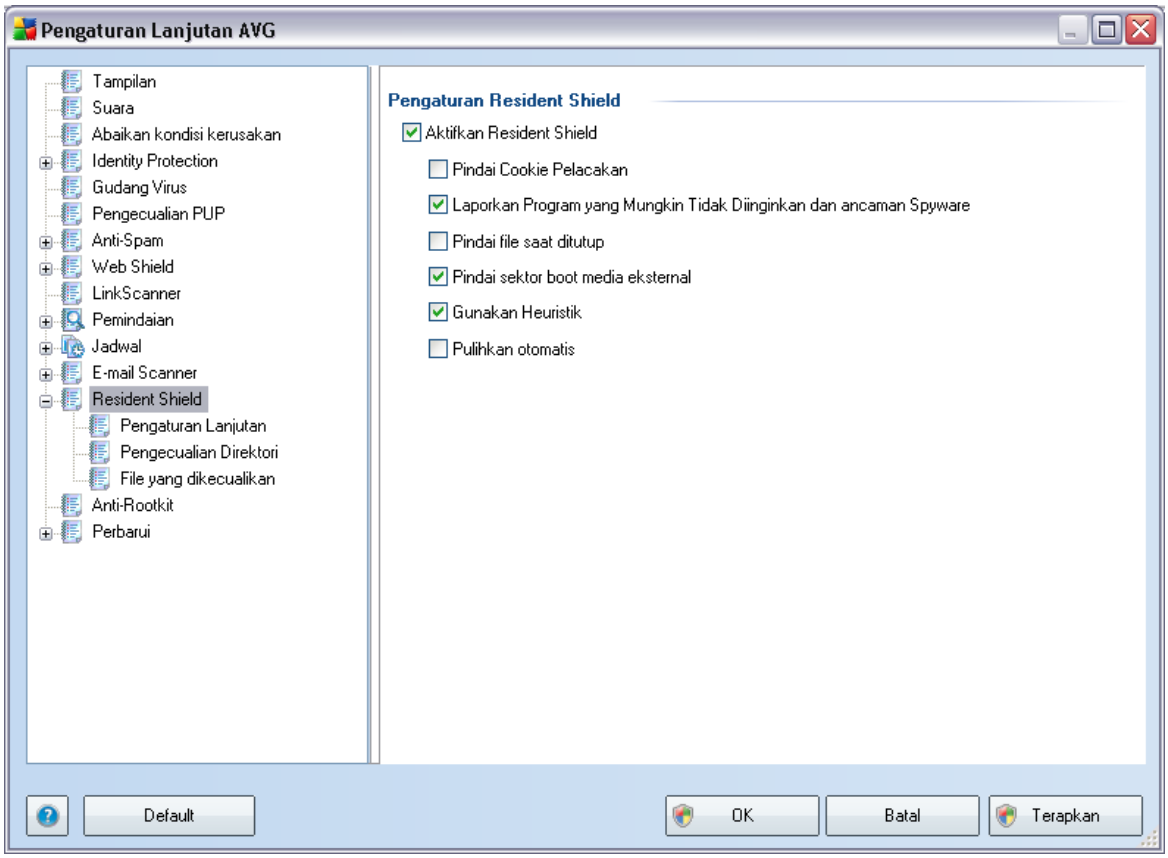
- ***Nama Server SMTP*** - ketikkan nama server atau biarkan nama default AutoSMTP
- ***Host Relai*** - menentukan metode untuk menentukan server e-mail yang digunakan untuk e-mail keluar:
  - ***Otomatis*** - login akan dilakukan secara otomatis, sesuai pengaturan klien e-mail Anda
  - ***Host tetap*** - Dalam kasus ini, program akan selalu menggunakan server yang ditetapkan 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 e-mail menggunakan port non-standar, Anda dapat menetapkan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (misalnya, pop.acme.com:8200). Port standar untuk komunikasi SMTP adalah 25.

- ***Pengaturan tambahan*** - menetapkan parameter yang lebih terperinci:
  - ***Port lokal*** - menetapkan port yang akan dicari oleh aplikasi e-mail Anda untuk berkomunikasi. Anda kemudian harus menetapkan port ini sebagai port untuk komunikasi SMTP dalam aplikasi e-mail Anda.
  - ***Pemrosesan antrean*** - menentukan cara kerja ***Pemindai E-mail*** saat memproses persyaratan untuk mengirim pesan e-mail:
    - Otomatis - e-mail keluar langsung dikirim ke server e-mail tujuan
    - Manual - pesan dimasukkan ke dalam antrean pesan keluar untuk dikirim kemudian
  - ***Koneksi*** - dalam menu buka bawah ini, Anda dapat menetapkan 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.
- ***Server administrasi*** - menampilkan nomor port server yang akan digunakan untuk pengiriman kembali laporan administrasi. Pesan ini dibuat, misalnya, bila server e-mail tujuan menolak pesan keluar atau bila server e-mail ini tidak tersedia.
- ***Pengaturan server SMTP klien e-mail*** - menyediakan informasi tentang cara mengonfigurasi aplikasi e-mail agar pesan e-mail keluar diperiksa menggunakan server yang sedang diubah untuk memeriksa pesan keluar. Ringkasan ini didasarkan pada parameter yang terkait yang ditetapkan dalam dialog ini dan dialog lain yang terkait.

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 menandai/tidak menandai item ***Aktifkan Perisai Tetap*** (*opsi ini telah diaktifkan secara default*). Selain itu, Anda dapat memilih fitur ***Perisai Tetap*** yang harus diaktifkan:

- ***Pindai Cookie Pelacak*** - 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*) memindai program yang mungkin tidak

diinginkan (*aplikasi yang dapat dijalankan, yang bisa berupa aneka tipe spyware atau adware*)

- ***Pindai file saat ditutup*** - 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

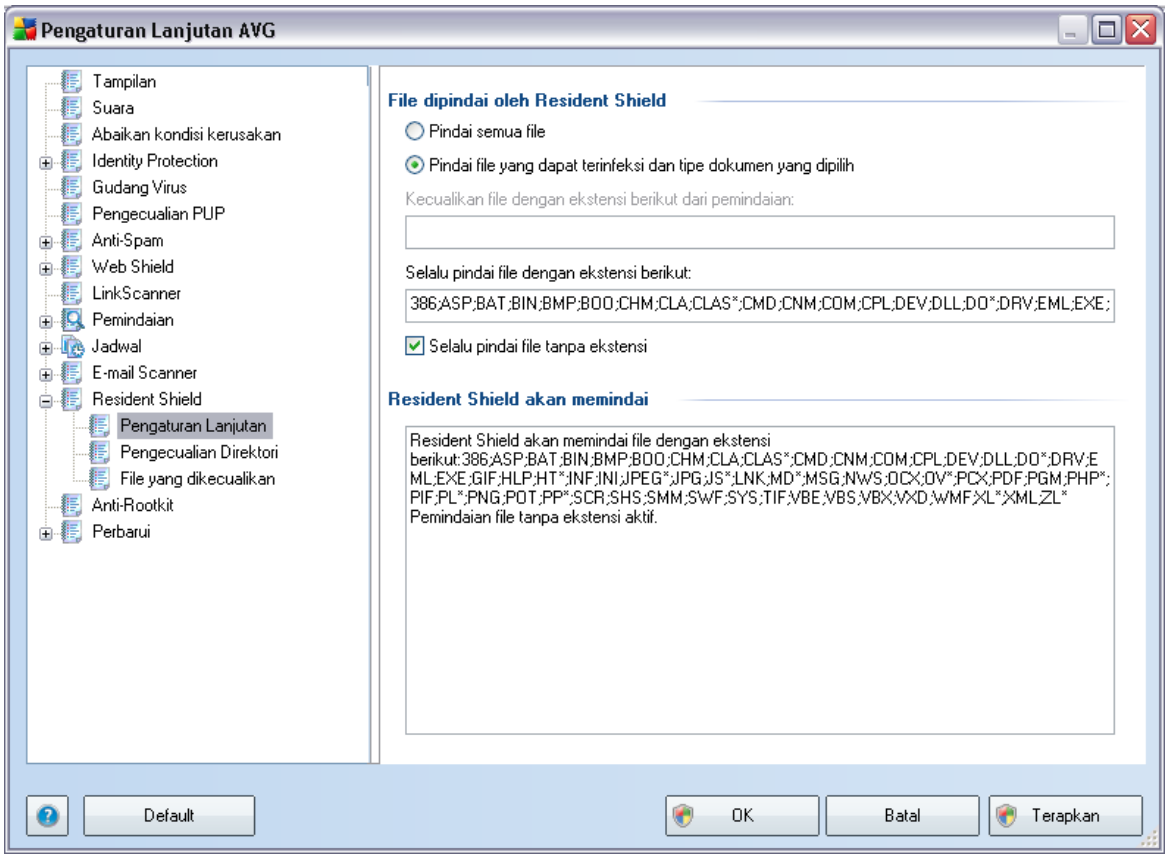
- ***Pindai sektor boot media eksternal*** - (*telah diaktifkan secara default*)

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

- ***Pulihkan otomatis*** - infeksi yang terdeteksi akan dipulihkan secara otomatis jika ada penawarnya

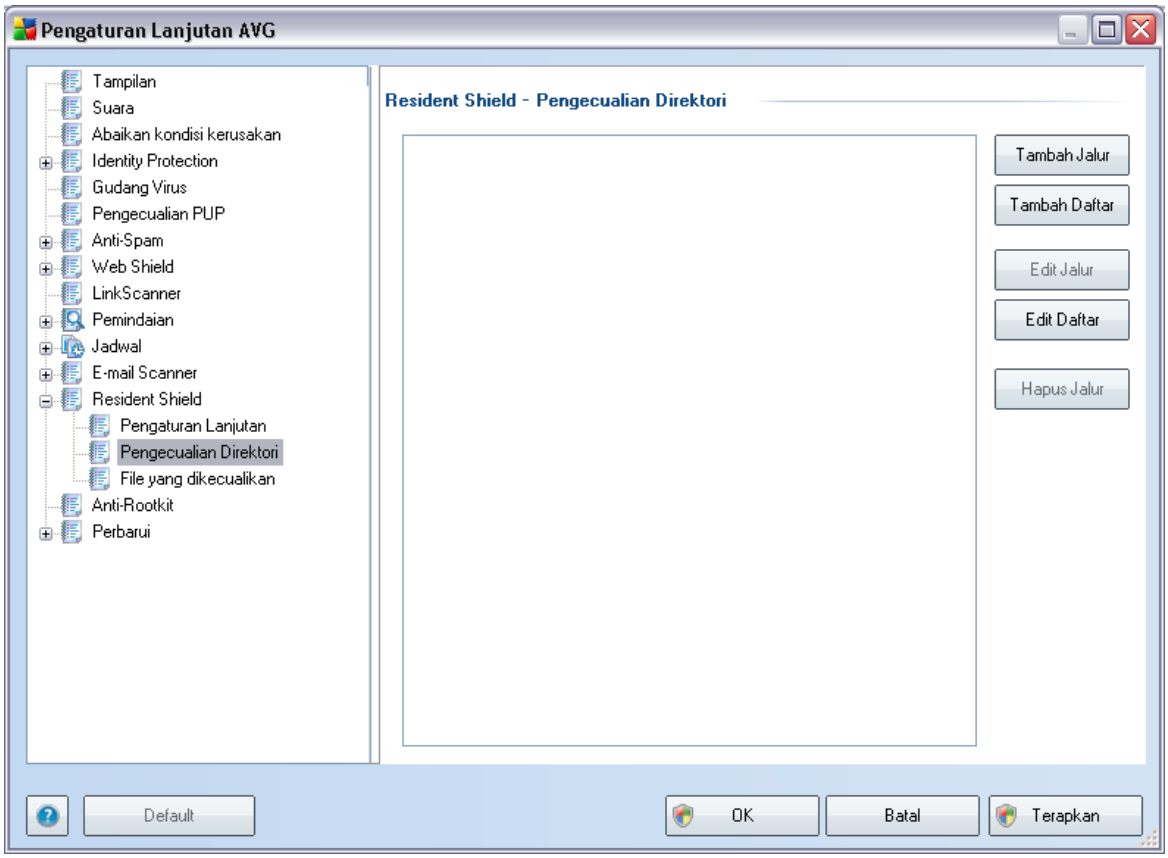
9.13.1. Pengaturan Lanjutan

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.

9.13.2. Pengecualian Direktori



Dialog ***Perisai Tetap - Pengecualian Direktori*** menyediakan kemungkinan untuk menentukan folder yang harus dikecualikan dari pemindaian ***Perisai Tetap.***

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

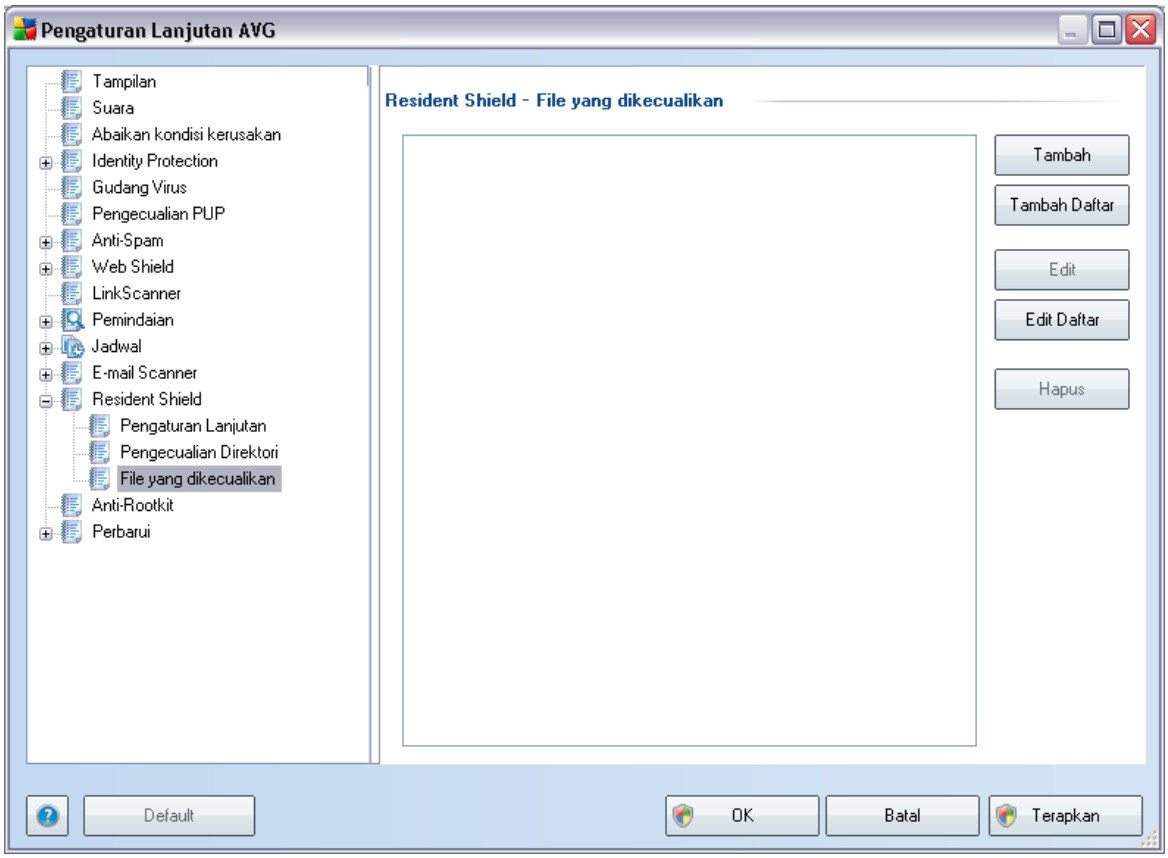
Dialog ini menyediakan tombol kontrol berikut:

- ***Tambah jalur*** – menetapkan direktori yang akan dikecualikan dari pemindaian dengan memilihnya satu per satu dari struktur navigasi disk lokal
- ***Tambah daftar*** – memungkinkan Anda memasukkan seluruh daftar direktori untuk dikecualikan dari pemindaian ***Perisai Tetap***
- ***Edit jalur*** – memungkinkan Anda mengedit jalur yang ditetapkan ke folder

yang dipilih

- ***Edit daftar*** – memungkinkan Anda mengedit daftar folder
- ***Hapus jalur*** – memungkinkan Anda menghapus jalur ke folder yang dipilih dari daftar

9.13.3. File yang Dikecualikan



Dialog ***Perisai Tetap - File yang dikecualikan*** bekerja persis seperti ***Perisai Tetap - Pengecualian Direktori*** yang telah diterangkan sebelumnya, tetapi sebagai ganti folder Anda sekarang dapat menetapkan file tertentu yang harus dikecualikan dari pemindaian ***Perisai Tetap***.

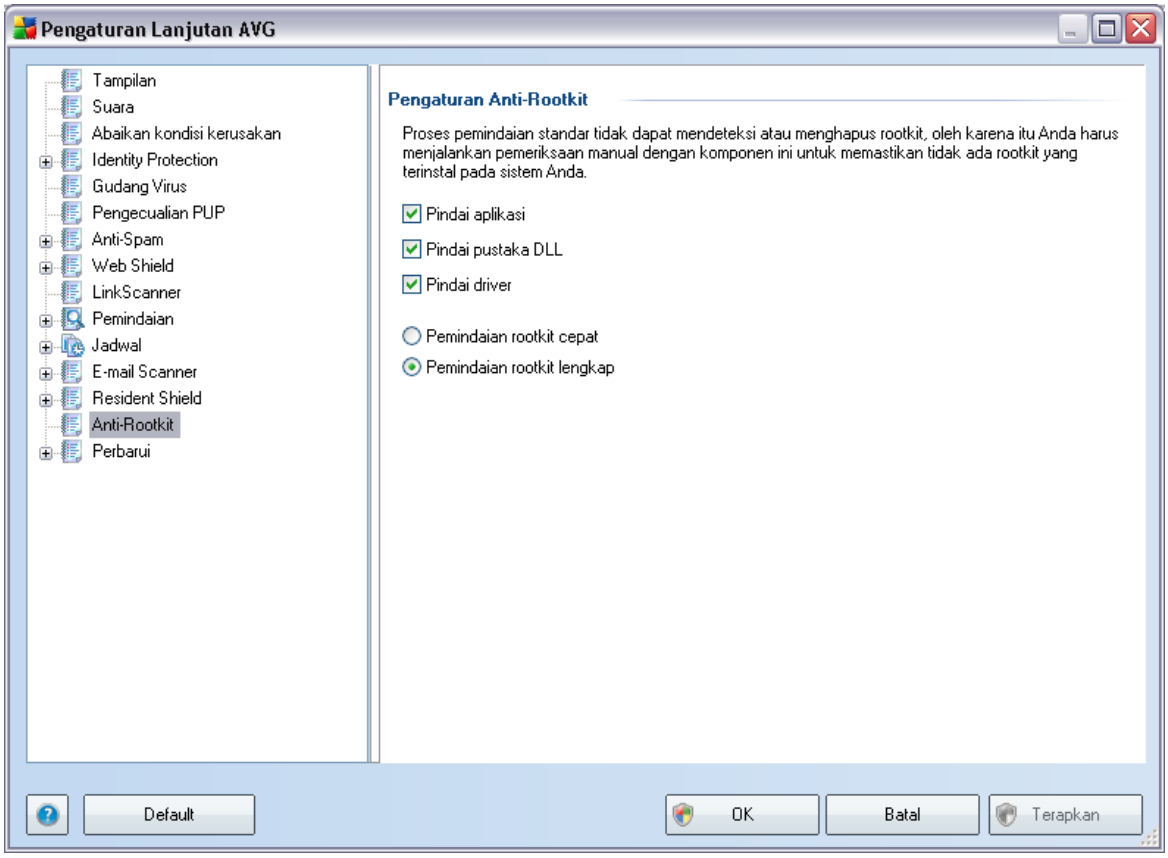
Jika hal ini tidak penting, kami sangat menyarankan untuk tidak mengecualikan file apa pun!

Dialog ini menyediakan tombol kontrol berikut:

- ***Tambah*** – menetapkan direktori yang akan dikecualikan dari pemindaian dengan memilihnya satu per satu dari struktur navigasi disk lokal
- ***Tambah daftar*** – memungkinkan Anda memasukkan seluruh daftar direktori untuk dikecualikan dari pemindaian ***Perisai Tetap***
- ***Edit*** – memungkinkan Anda mengedit jalur yang ditetapkan ke folder yang dipilih
- ***Edit daftar*** – memungkinkan Anda mengedit daftar folder
- ***Hapus*** – memungkinkan Anda menghapus jalur ke folder yang dipilih dari daftar

9.14. 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***.

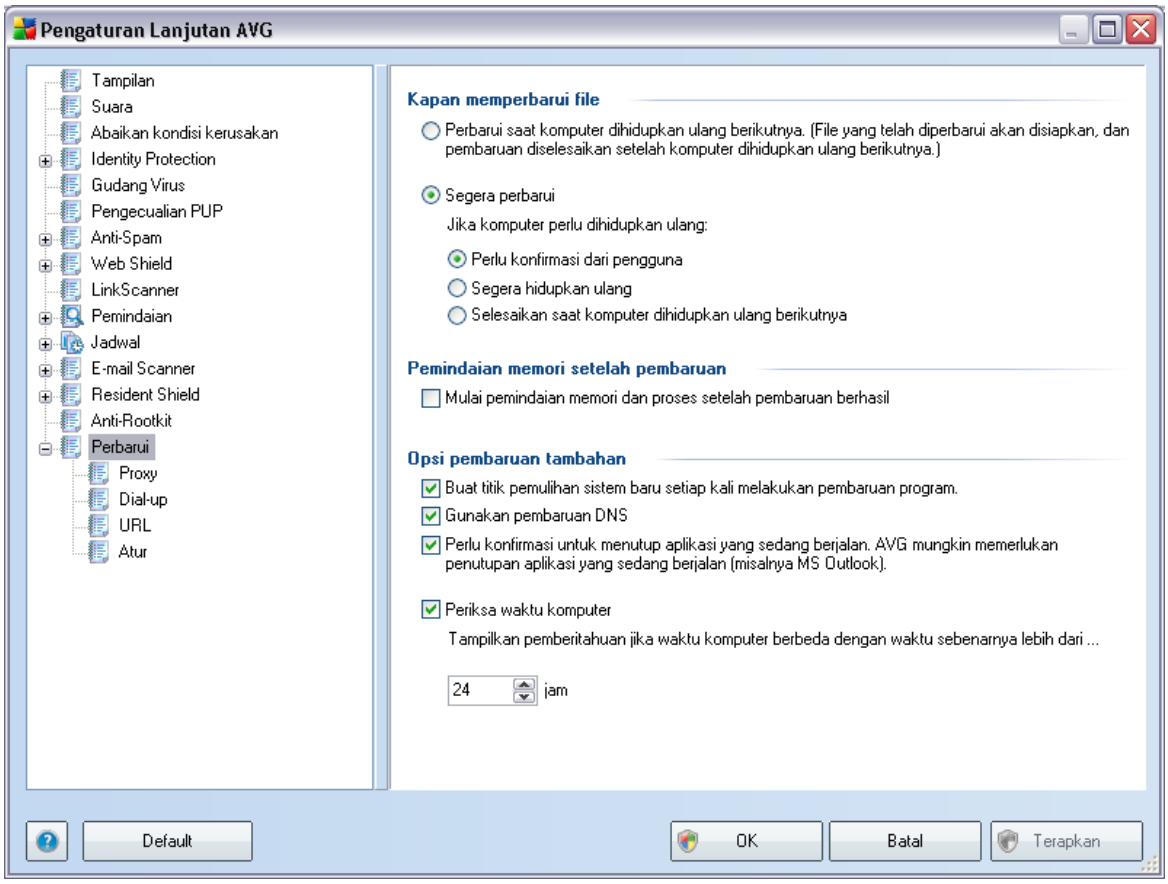
Tandai kotaknya untuk menentukan objek yang harus dipindai:

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

Selanjutnya Anda dapat memilih mode pemindaian rootkit:

- ***Pemindaian rootkit cepat*** - hanya memindai folder sistem (*biasanya c:\Windows*)
- ***Pemindaian rootkit lengkap*** – memindai semua disk yang dapat diakses kecuali A: dan B:

9.15. 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 antara dua opsi alternatif: pembaruan dapat dijadwalkan untuk saat menghidupkan PC berikutnya atau Anda dapat meluncurkan

pembaruan dengan segera. Secara default, opsi pembaruan segera dipilih karena dengan cara ini AVG dapat mengamankan pada tingkat keamanan maksimum. Menjadwalkan pembaruan di saat berikutnya menghidupkan ulang PC hanya disarankan jika Anda yakin komputer akan dihidupkan ulang secara rutin, sedikitnya setiap hari.

Jika Anda memutuskan untuk mempertahankan konfigurasi default dan meluncurkan proses pembaruan dengan segera, Anda dapat menetapkan kondisi untuk menghidupkan ulang bila diperlukan:

- ***Minta konfirmasi dari pengguna*** - 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*** - finalisasi proses pembaruan akan ditunda hingga saat berikutnya komputer dihidupkan ulang - sekali lagi, ingatlah bahwa opsi ini hanya disarankan jika Anda yakin komputer akan dihidupkan ulang secara rutin, sedikitnya setiap hari

Pemindaian memori setelah pembaruan

Beri centang pada 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

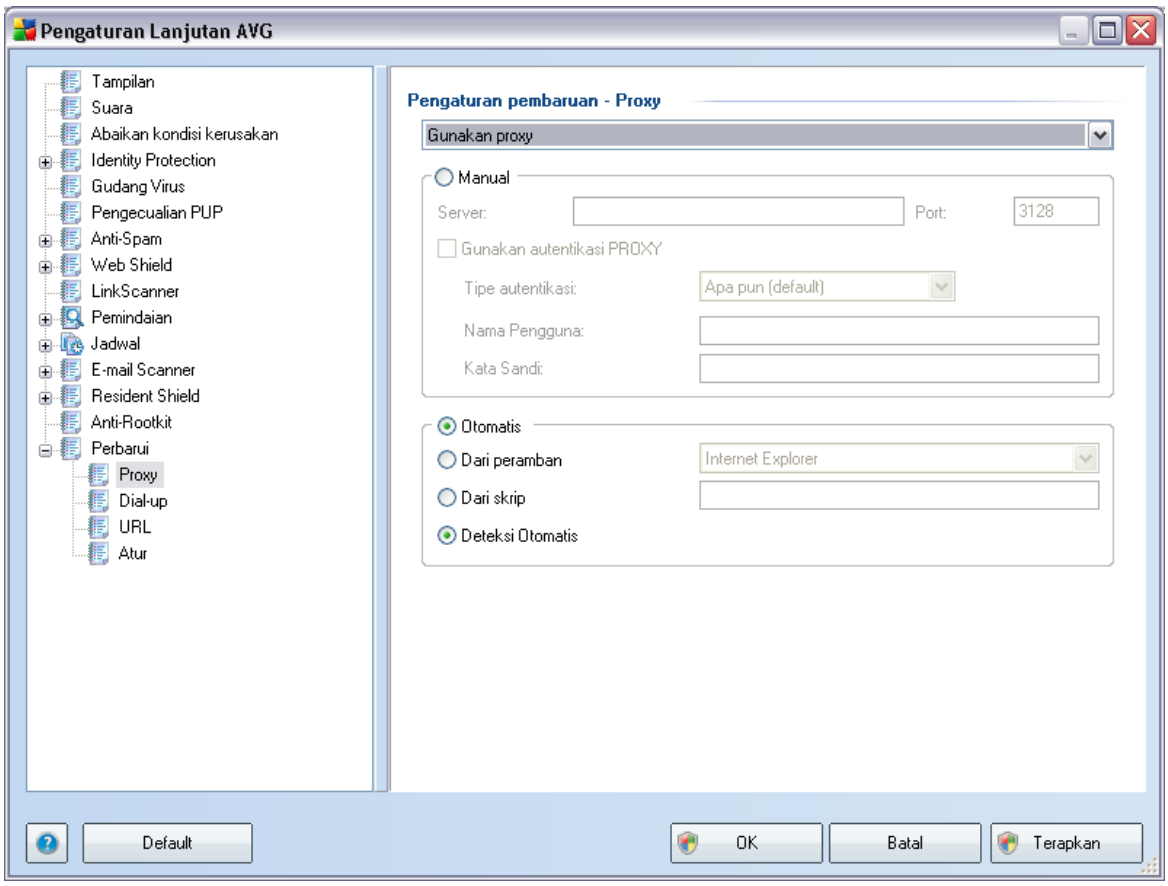
- ***Buat titik pemulihan sistem baru setiap kali melakukan pembaruan program*** - sebelum setiap peluncuran pembaruan program AVG, akan dibuat titik pemulihan sistem. Seandainya proses pembaruan gagal dan sistem operasi crash, Anda dapat memulihkan OS ke konfigurasi aslinya dari titik ini. Opsi ini 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*** - centang kotak ini untuk untuk mengonfirmasi

bahwa Anda ingin menggunakan metode deteksi file pembaruan yang mengurangi jumlah data yang ditransfer antara server pembaruan dan klien AVG;

- ***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.

9.15.1. Proxy



Server proxy adalah server mandiri atau layanan yang berjalan pada PC, yang menjamin koneksi ke Internet lebih aman. Sesuai aturan jaringan yang ditetapkan, 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***
- ***Cobalah koneksi menggunakan proxy dan jika gagal, hubungkan langsung*** - pengaturan default

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

Konfigurasi manual

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

- ***Server*** – menetapkan alamat IP server atau nama server
- ***Port*** – menetapkan 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, centang opsi ***Gunakan autentikasi PROXY*** untuk memverifikasi apakah nama pengguna dan kata sandi Anda sudah sah untuk menghubungkan ke Internet melalui server proxy.

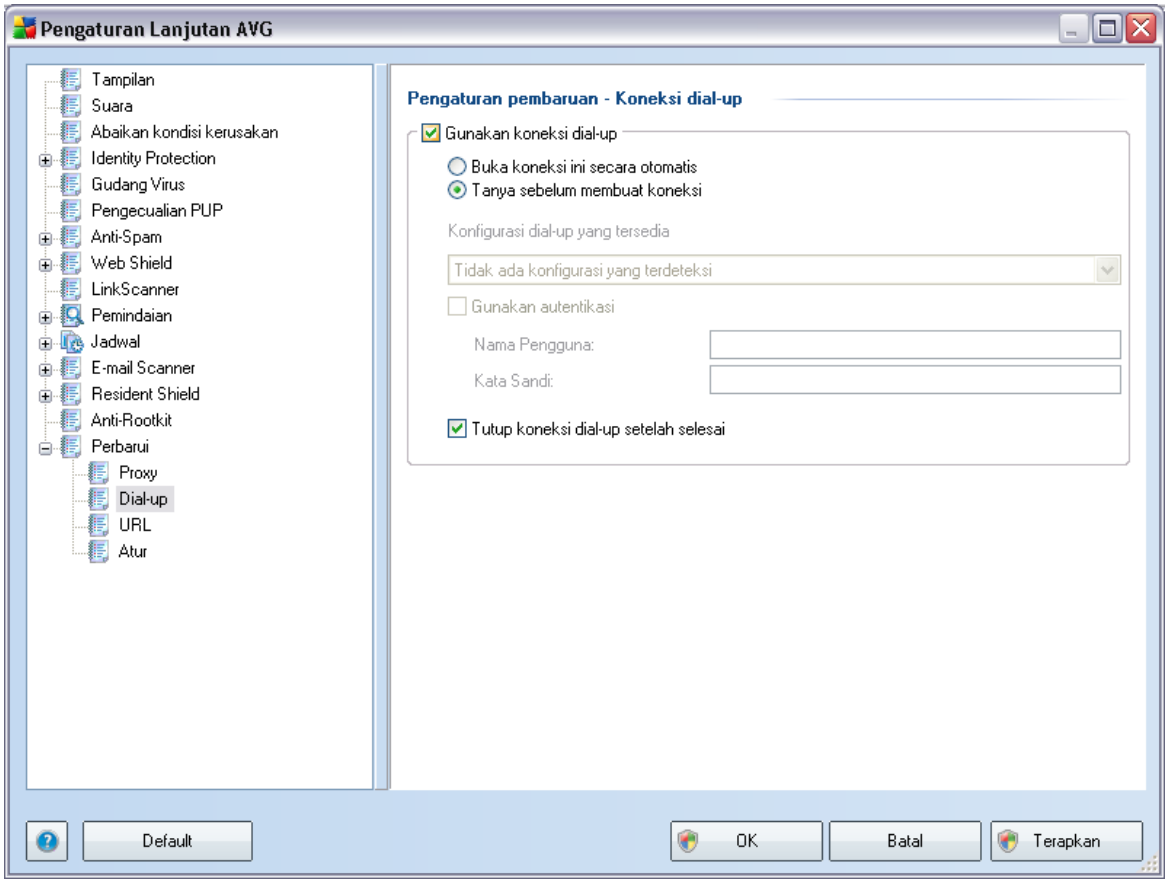
Konfigurasi otomatis

Jika Anda memilih konfigurasi otomatis (*tandai opsi* ***Auto*** *untuk mengaktifkan bagian dialognya*) maka pilih dari mana konfigurasi 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

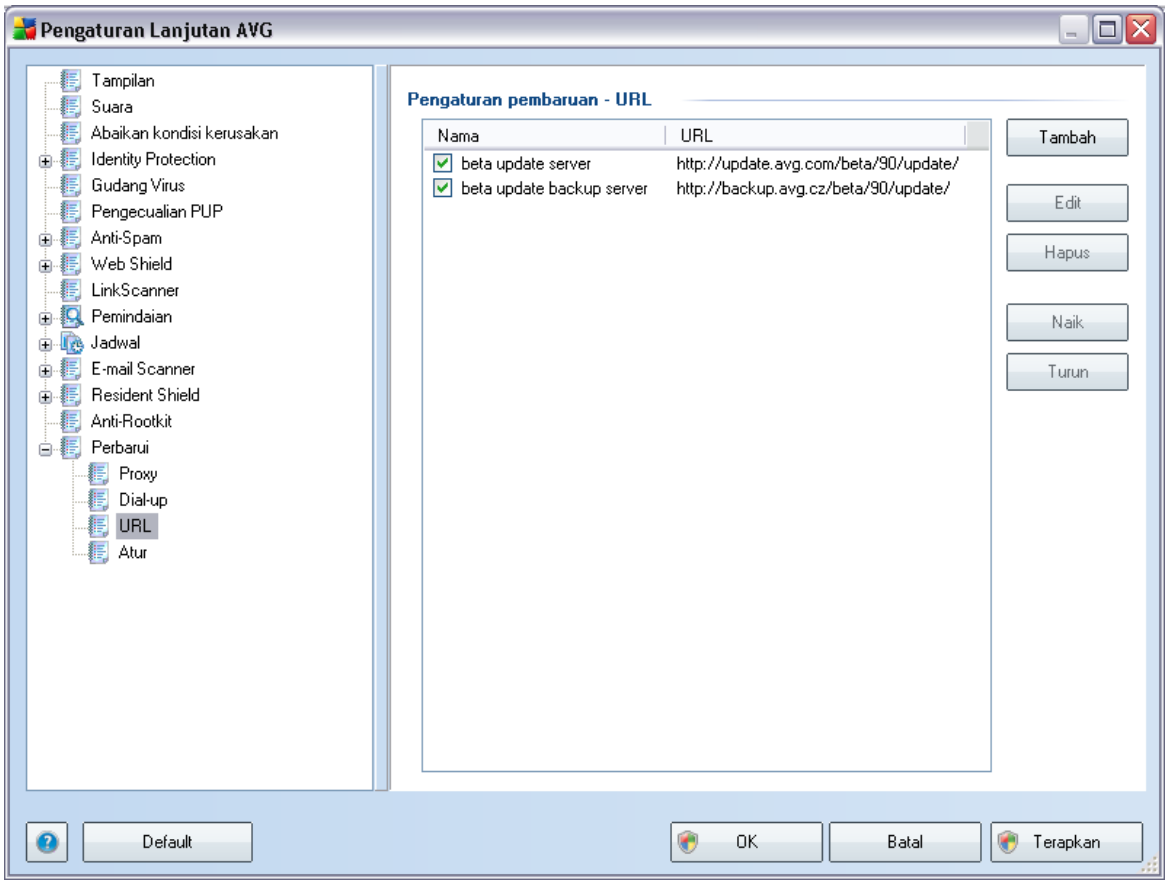
9.15.2. Dial-up



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***).

9.15.3. URL



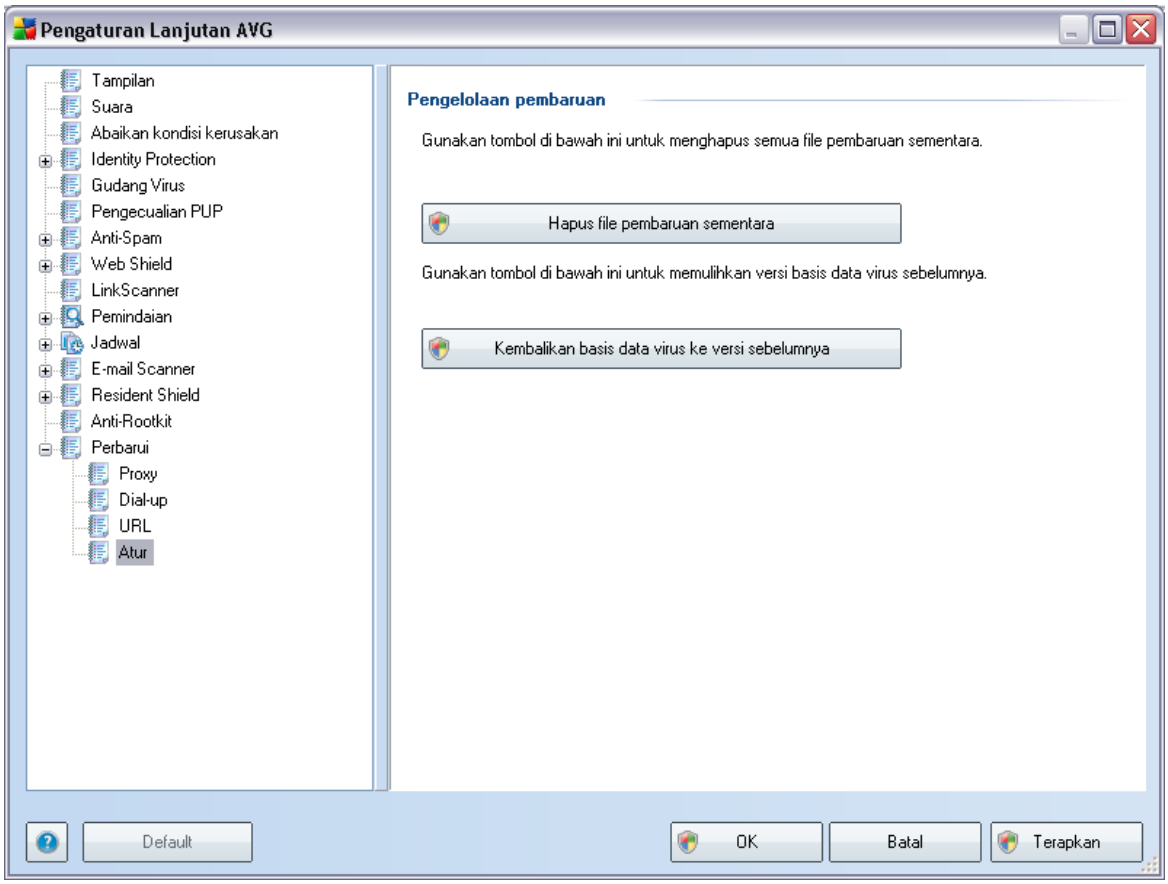
Dialog ***URL*** menyediakan daftar alamat Internet dari mana Anda dapat mengunduh file pembaruan. Daftar ini dan itemnya dapat diubah dengan menggunakan tombol kontrol berikut:

- ***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

9.15.4. Atur

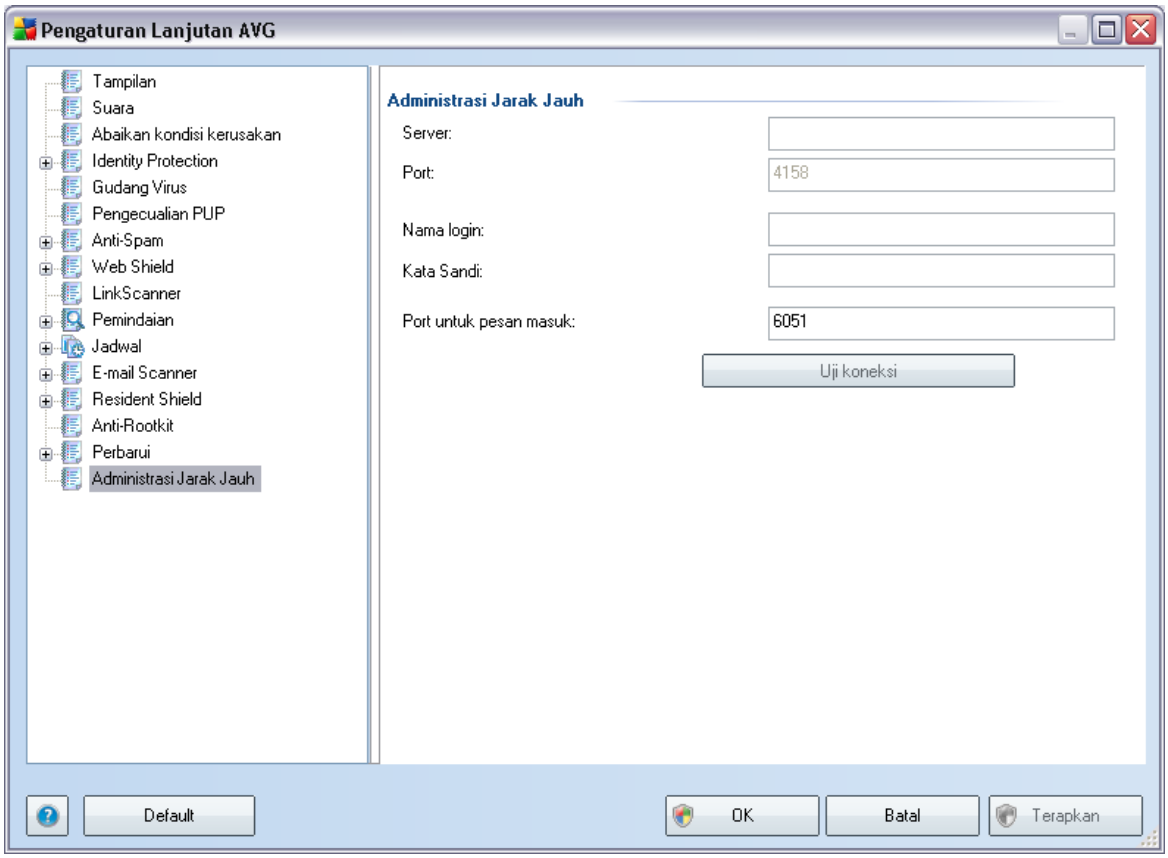
Dialog ***Atur*** menyediakan dua opsi yang dapat diakses melalui dua tombol:



- ***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*)

9.16. Administrasi Jarak Jauh



Pengaturan ***Administrasi Jarak Jauh*** merujuk pada koneksi stasiun klien AVG ke sistem administrasi jarak jauh. Jika Anda berencana menghubungkan stasiun yang bersangkutan ke administrasi jarak jauh, tetapkan parameter berikut:

- ***Server*** - nama server (atau alamat IP server) di mana AVG Admin Server diinstal
- ***Port*** - masukkan nomor port yang digunakan klien AVG untuk berkomunikasi dengan AVG Admin Server (*nomor port 4158 dianggap sebagai default - jika Anda menggunakan nomor port ini, Anda tidak perlu menetapkannya secara eksplisit*)
- ***Login*** - jika komunikasi antara klien AVG dan AVG Admin Server telah dipastikan aman, masukkan nama pengguna Anda ...

- ***Kata Sandi*** - ... dan kata sandi Anda
- ***Port pesan masuk*** - nomor port yang digunakan klien AVG untuk menerima pesan masuk dari AVG Admin Server

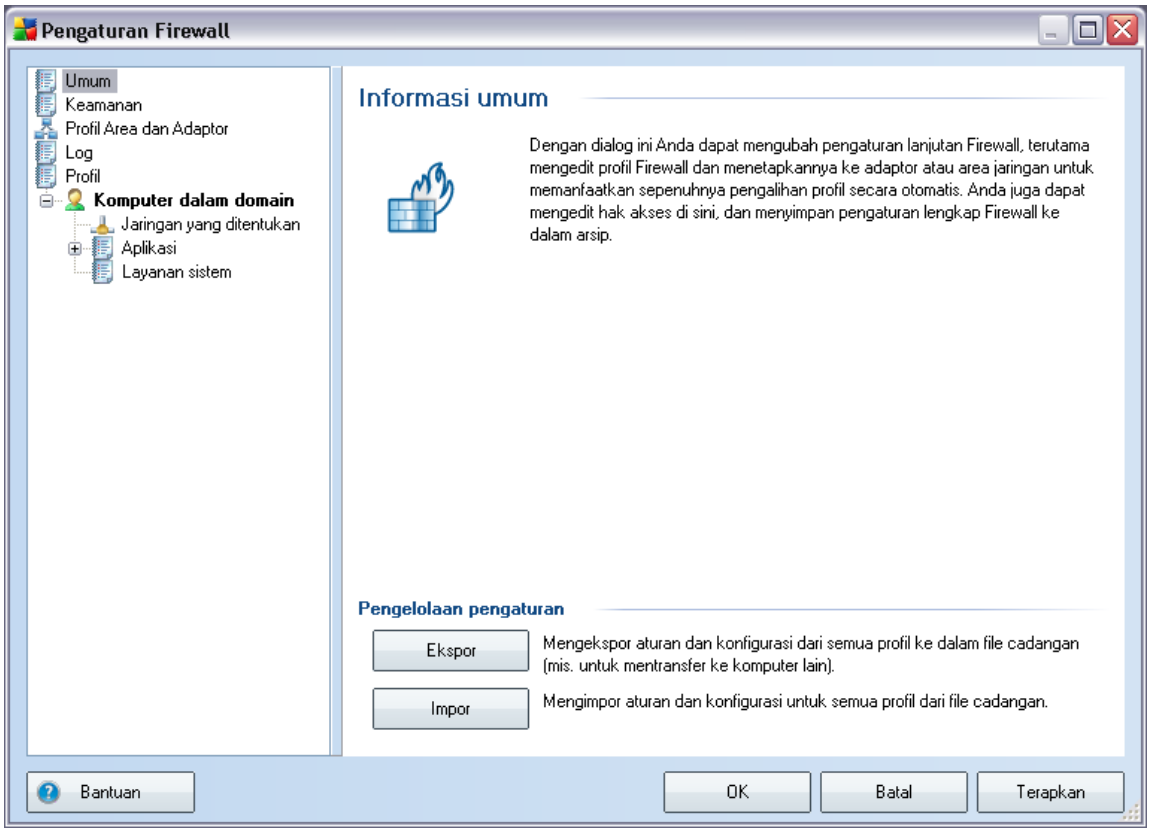
Tombol ***Uji koneksi*** membantu Anda memverifikasi apakah semua data yang tercantum di atas sudah sah dan dapat digunakan untuk keberhasilan menghubungkan ke DataCenter.

Catatan: *Untuk keterangan terperinci mengenai administrasi jarak jauh bacalah dokumentasi AVG Network Edition.*

10. Pengaturan Firewall

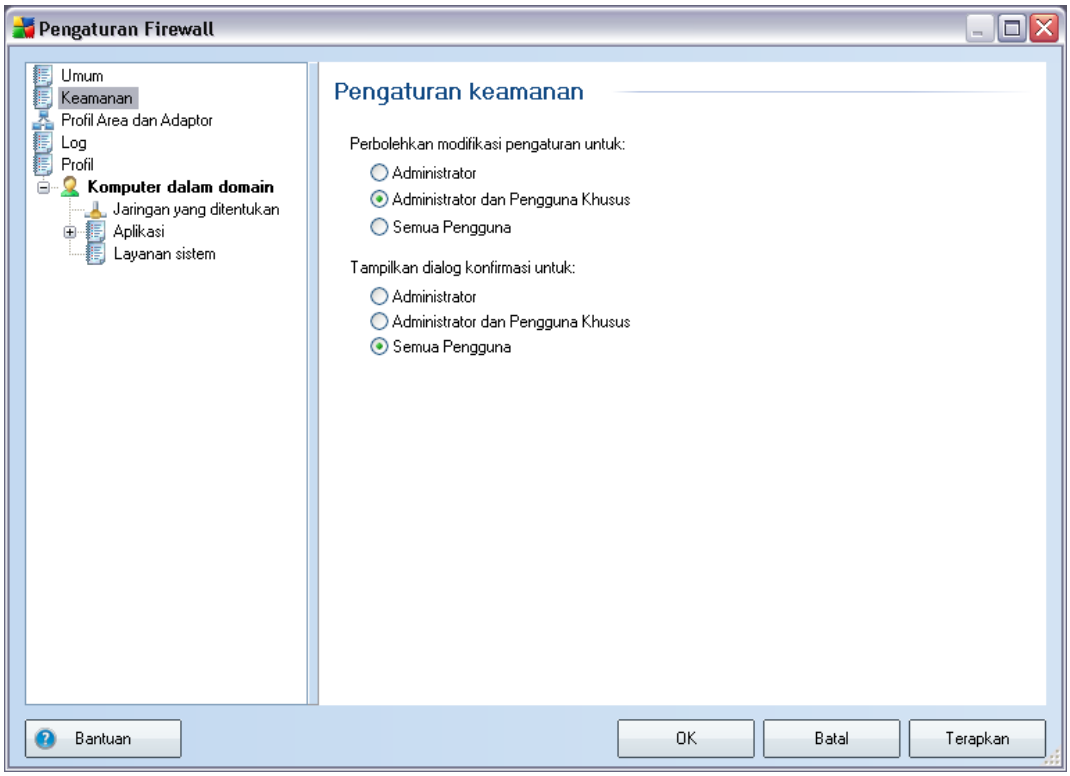
Konfigurasi ***Firewall*** akan dibuka dalam jendela baru berisi sejumlah dialog di mana Anda dapat mengatur parameter lebih lanjut dari komponen tersebut. ***Walau demikian, pengeditan konfigurasi lanjutan hanya ditujukan bagi para pengguna berpengalaman dan ahli.***

10.1. Umum



Dalam ***Informasi umum*** Anda dapat melakukan ***Ekspor*** / ***Impor*** ***konfigurasi Firewall***; misalnya mengekspor aturan dan pengaturan ***Firewall*** yang telah ditentukan untuk mencadangkan file, atau sebaliknya 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

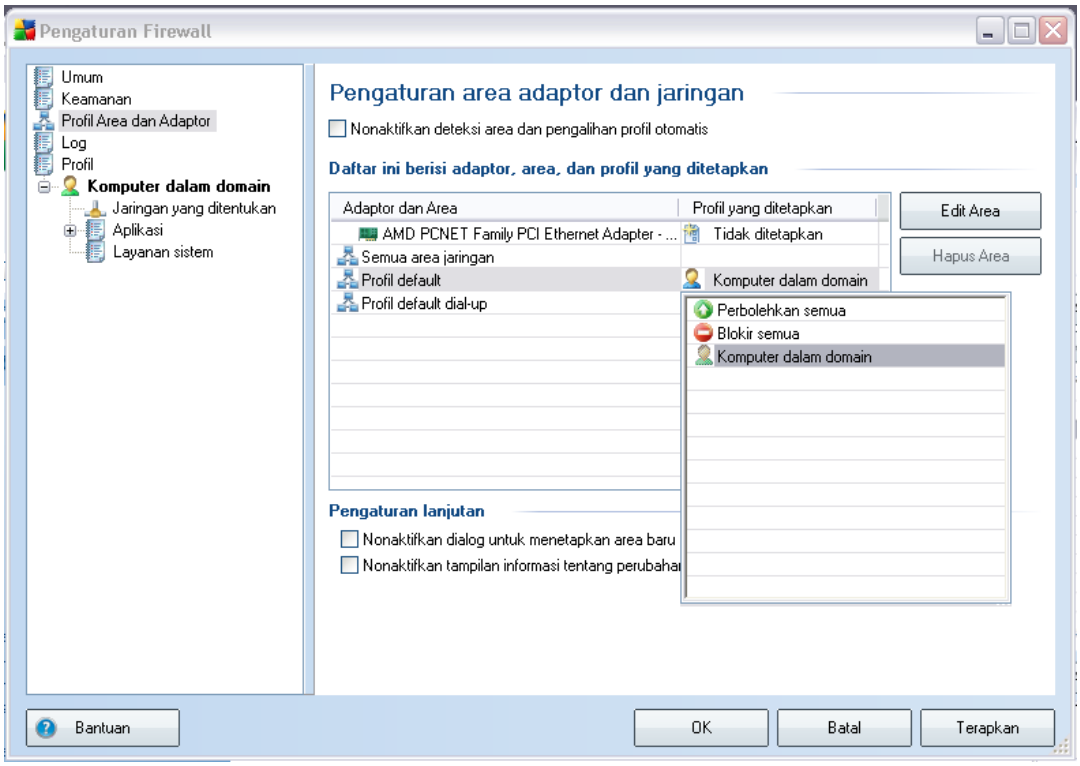
Pada kedua kasus, Anda dapat menetapkan hak tertentu ke salah satu dari beberapa grup pengguna berikut:

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

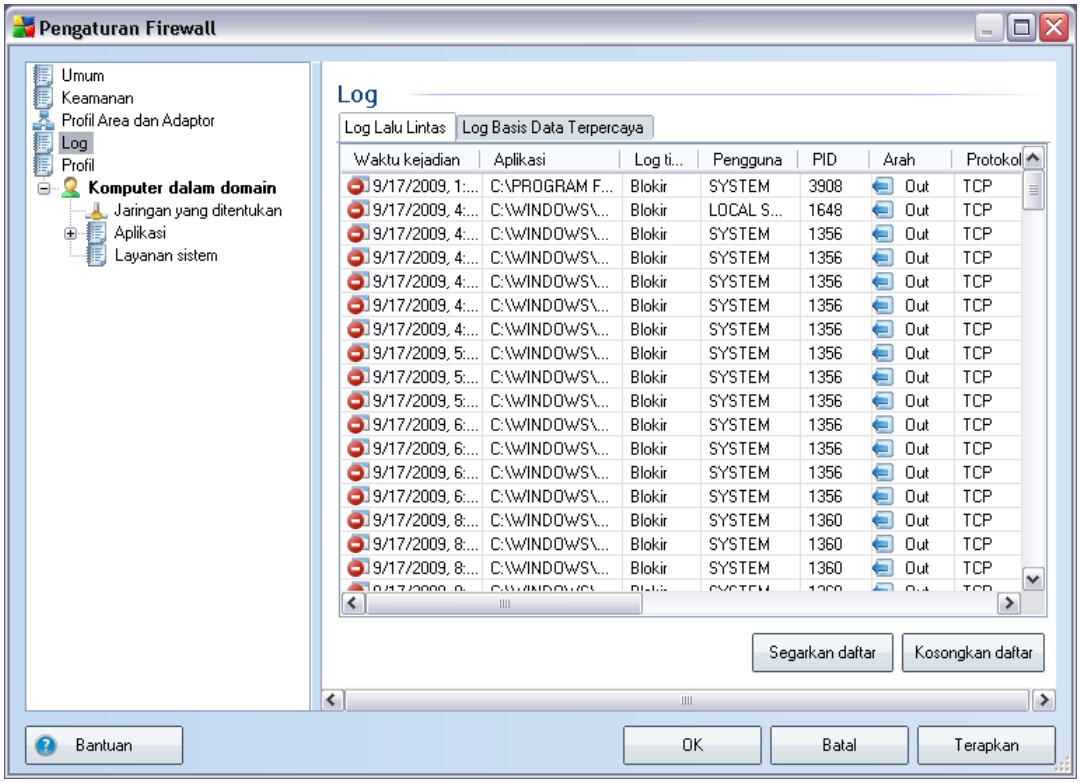
- ***Nonaktifkan deteksi area dan alih profil otomatis*** - salah satu profil yang ditentukan dapat diberikan ke setiap tipe antarmuka jaringan, sesuai masing-masing area. Jika Anda tidak ingin menentukan profil spesifik, maka satu profil umum yang ditentukan berdasarkan pilihan penggunaan komputer dan desain jaringan komputer saat ***Proses Instalasi*** akan digunakan. Walau demikian, jika Anda memutuskan untuk membedakan berbagai profil dan menetapkannya ke berbagai adapter dan area spesifik, dan kemudian - karena beberapa alasan - Anda ingin mengubah pengaturan ini untuk

sementara, centang opsi ***Nonaktifkan deteksi area dan alih profil otomatis***.

- ***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*** - menandai opsi terkait akan menonaktifkan fitur untuk menampilkan pesan informasi.

10.4. 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 dua 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.

Tombol kontrol

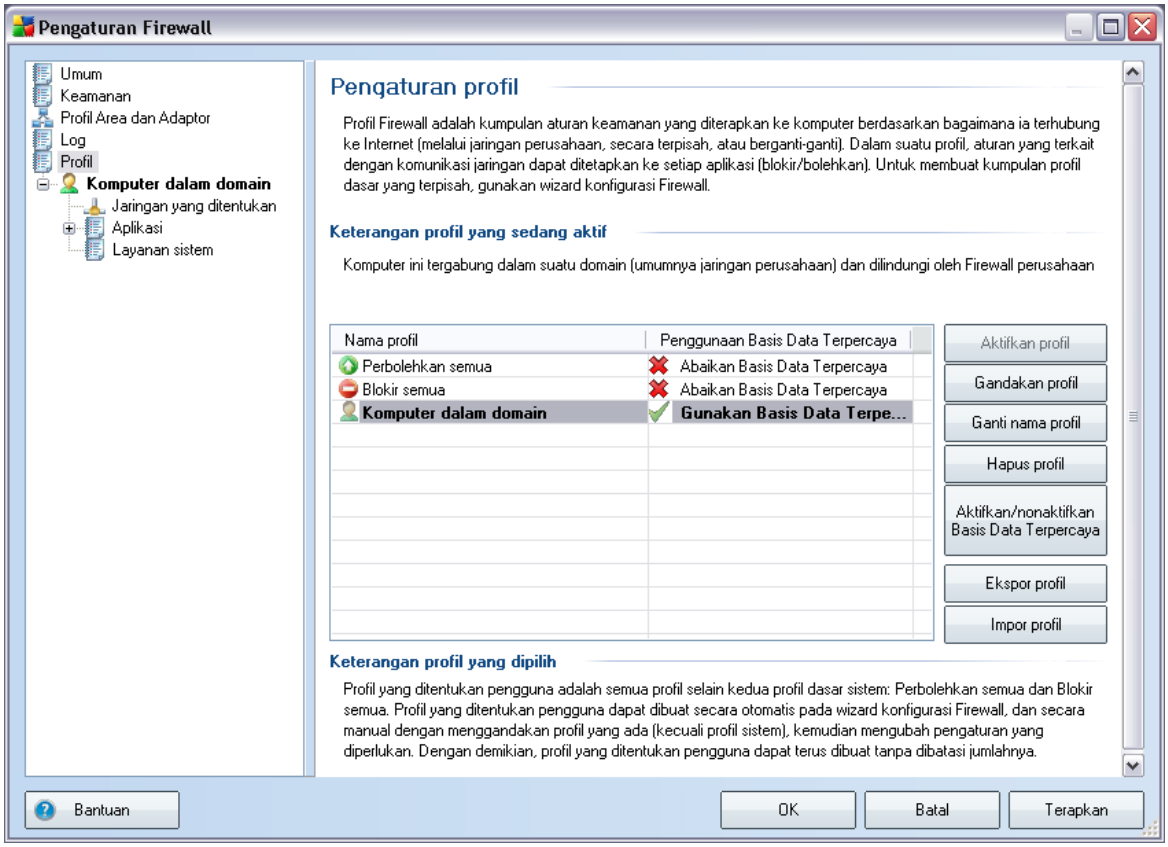
- ***Bantuan*** - membuka file bantuan yang terkait dengan dialog.

- ***Segarkan daftar*** - semua parameter yang terekam dalam log dapat disusun menurut atribut yang dipilih: secara kronologis (*tanggal*) atau secara 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.

10.5. 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:

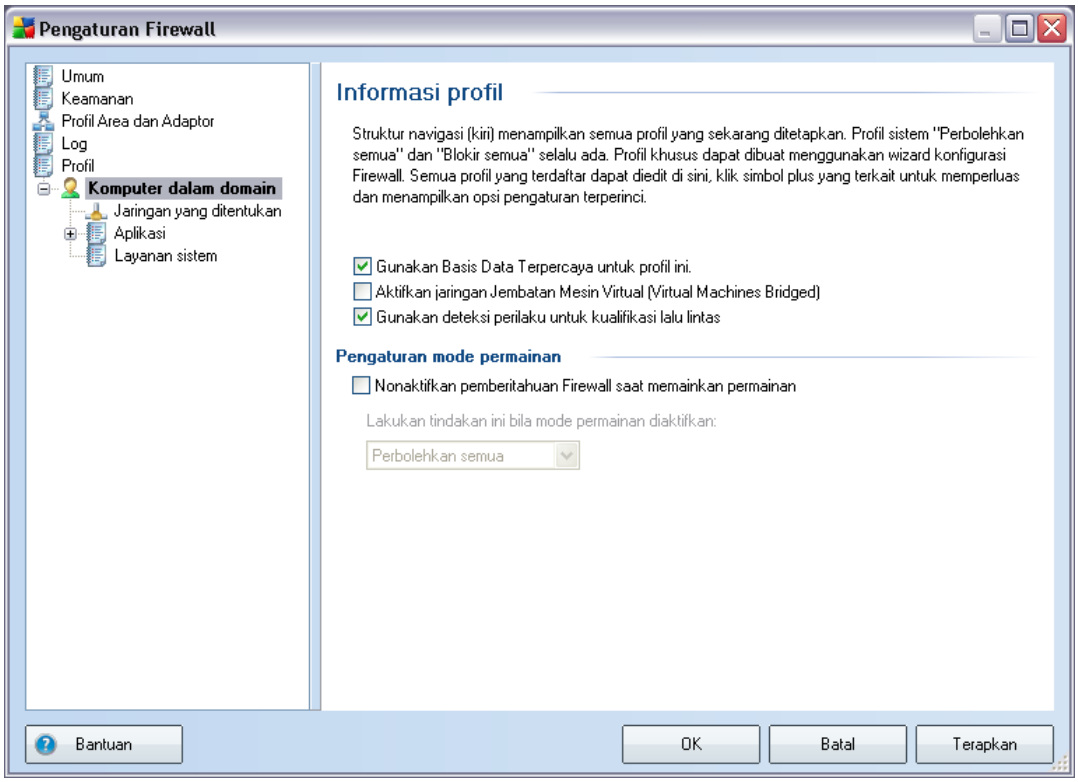
- ***Aktifkan profil*** - tombol ini akan mengaktifkan profil yang dipilih, yang berarti konfigurasi profil yang dipilih akan digunakan oleh ***Firewall*** untuk mengontrol lalu lintas jaringan
- ***Gandakan profil*** - membuat salinan identik dari profil yang dipilih; nanti Anda dapat mengedit dan mengganti 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
- ***Bantuan*** - membuka file bantuan yang terkait dengan dialog

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*):

10.5.1. Informasi Profil



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

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

- ***Aktifkan Jaringan Berpenghubung Mesin Virtual*** - (*dinonaktifkan secara default*) centang item ini untuk memperbolehkan mesin virtual di WMware

menghubungkan langsung ke jaringan

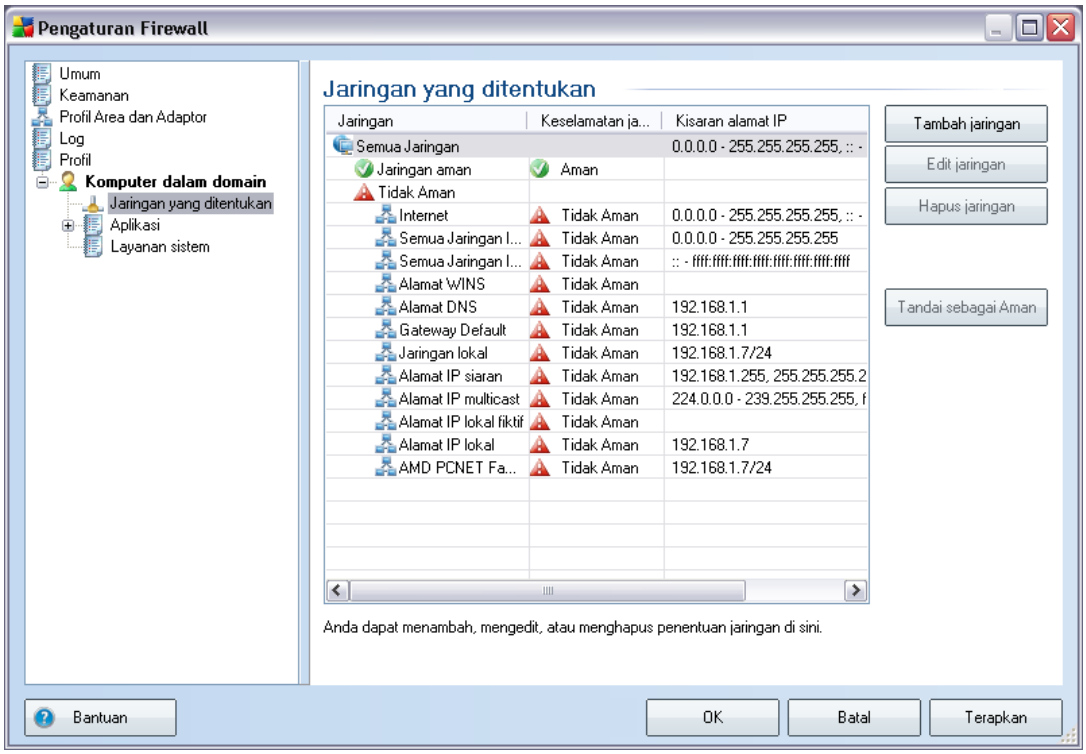
- ***Gunakan deteksi perilaku untuk kualifikasi lalu lintas*** - (*diaktifkan secara default*) centang opsi ini untuk memperbolehkan ***Firewall*** menggunakan fungsionalitas ***LinkScanner*** saat mengevaluasi aplikasi - ***LinkScanner*** dapat memberi tahu apakah aplikasi menunjukkan perilaku mencurigakan,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

Pengaturan mode permainan

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

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

10.5.2. Jaringan Yang Ditentukan

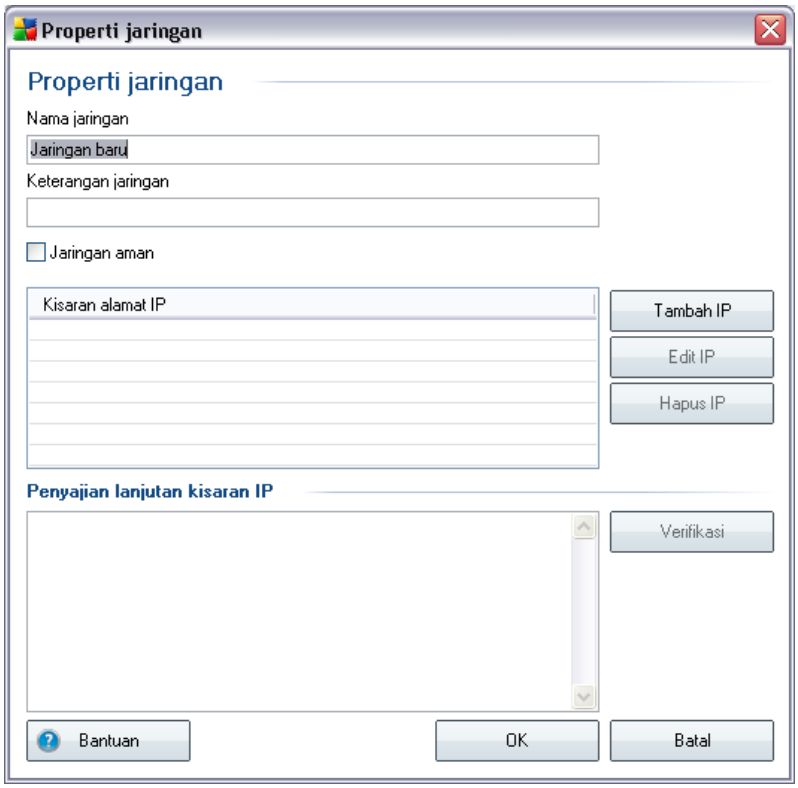


Dialog ***Jaringan yang ditentukan*** menyediakan daftar semua jaringan yang terhubung ke komputer Anda. Informasi berikut ini tersedia untuk setiap jaringan yang terdeteksi:

- ***Jaringan*** - daftar nama semua jaringan ke mana komputer terhubung
- ***Keamanan jaringan*** - secara default, semua adaptor dianggap tidak aman, dan hanya jika Anda yakin suatu jaringan aman, Anda dapat menetapkannya demikian (*klik item daftar yang merujuk ke jaringan tersebut dan pilih Aman dari menu konteks*) - semua jaringan aman akan dimasukkan ke dalam suatu kelompok yang dapat digunakan aplikasi untuk berkomunikasi dengan kumpulan aturan aplikasi yang diatur ke ***Perbolehkan aman***
- ***Kisaran alamat IP*** - setiap jaringan akan dideteksi secara otomatis dan ditetapkan dalam bentuk kisaran alamat IP

Tombol kontrol

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



Dalam dialog ini, Anda dapat menetapkan ***Nama jaringan***, memberikan ***Keterangan jaringan*** dan mungkin dapat menetapkan jaringan sebagai aman. Jaringan baru tersebut dapat ditentukan secara manual dalam dialog tersendiri yang dibuka melalui tombol ***Tambah IP*** (atau ***Edit IP*** / ***Hapus IP***), dalam dialog ini Anda dapat menetapkan jaringan dengan memberikan kisaran IP atau maskernya.

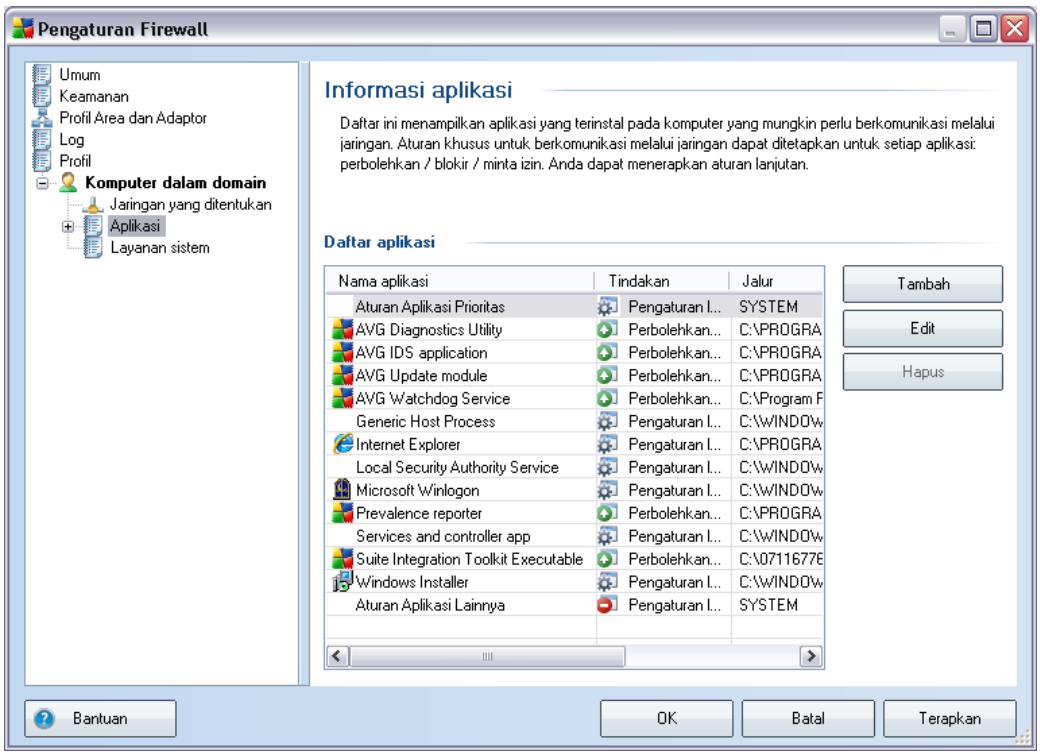
Untuk jaringan dalam jumlah besar yang harus ditentukan sebagai bagian dari jaringan yang baru dibuat, Anda dapat menggunakan opsi ***Representasi kisaran IP lanjutan***: Masukkan daftar semua jaringan ke dalam bidang teksnya (*semua format standar didukung*), dan tekan tombol ***Verifikasi*** untuk memastikan bahwa format ini dapat dikenali. Kemudian tekan ***OK*** untuk mengonfirmasi dan menyimpan data.

- ***Edit jaringan*** - membuka jendela dialog ***Properti jaringan*** (*lihat di atas*) di mana Anda dapat mengedit berbagai parameter jaringan yang sudah

ditentukan (*dialognya sama dengan dialog untuk menambah jaringan baru, lihat keterangan dalam paragraf sebelumnya*)

- ***Hapus jaringan*** - menghapus catatan jaringan yang dipilih dari daftar jaringan
- ***Tandai aman*** - secara default, semua jaringan dianggap tidak aman, dan hanya jika Anda yakin jaringan tersebut memang aman, Anda dapat menggunakan tombol ini untuk menetapkannya demikian
- ***Bantuan*** - membuka file bantuan yang terkait dengan dialog

10.5.3. Aplikasi

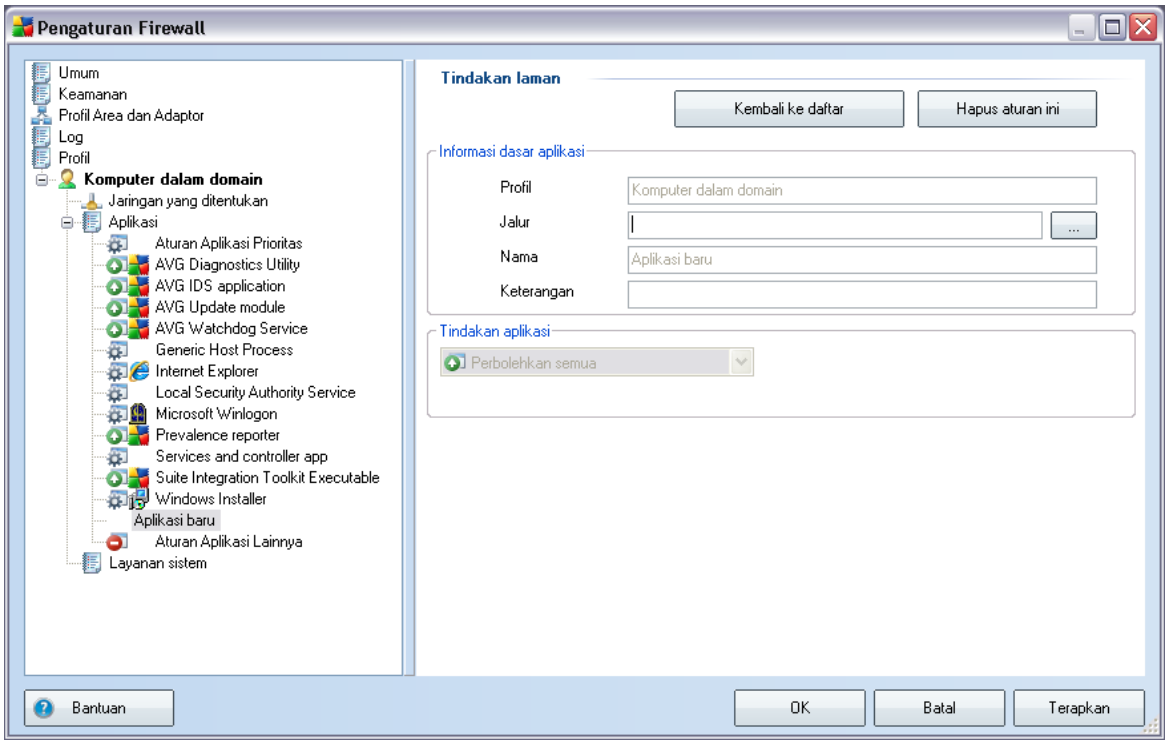


Dalam dialog ***Informasi aplikasi***, Anda dapat menemukan gambaran umum atas semua aplikasi yang berkomunikasi melalui jaringan. Daftar ini dapat diedit menggunakan tombol kontrol berikut:

- ***Tambah*** - membuka dialog untuk yang menentukan kumpulan aturan aplikasi baru

- ***Edit*** - membuka dialog untuk mengedit kumpulan aturan aplikasi yang ada
- ***Hapus*** - menghapus aplikasi yang dipilih dari daftar
- ***Bantuan*** - membuka file bantuan yang terkait dengan dialog

Dialog untuk menetapkan kumpulan aturan aplikasi baru akan terbuka menggunakan tombol ***Tambah*** dari dialog ***Aplikasi*** dalam ***Pengaturan Firewall***:



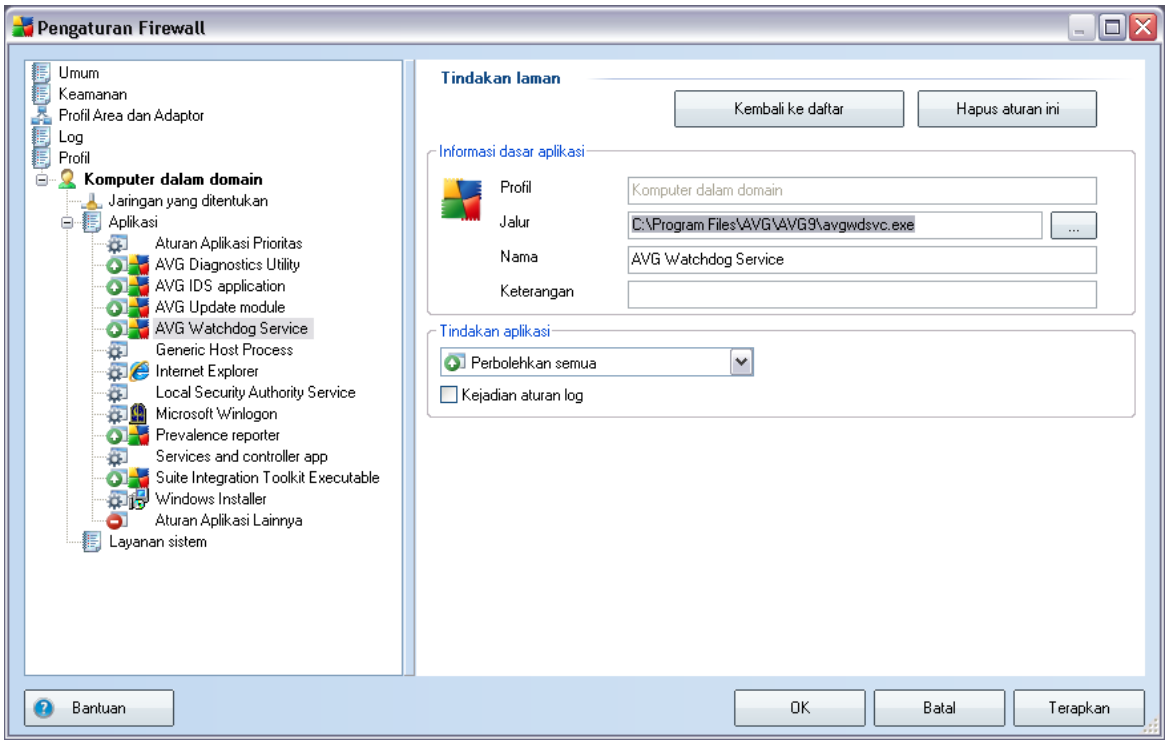
Dalam dialog ini Anda dapat menentukan:

- ***Informasi dasar aplikasi*** - nama aplikasi, keterangan singkatnya dan jalur lokasinya pada disk
- ***Tindakan aplikasi*** - dari menu buka bawah pilih aturan yang akan diterapkan pada cara kerja aplikasi:
  - ***Pengaturan lanjutan -*** opsi ini memungkinkan Anda mengedit kumpulan aturan secara terperinci di bagian bawah dialog ini; *untuk*

*keterangan mengenai bagian ini, lihat bab **Edit Aplikasi***

- ***Perbolehkan semua -*** akan memperbolehkan upaya komunikasi apa pun dari aplikasi
- ***Perbolehkan untuk aman -*** aplikasi hanya akan diperbolehkan berkomunikasi melalui jaringan aman (*sebagai contoh, komunikasi ke jaringan perusahaan yang telah terlindungi akan diperbolehkan walaupun komunikasi ke Internet diblokir*); untuk gambaran umum dan keterangan mengenai jaringan aman, lihat dialog ***Jaringan***
- ***Tanya -*** kapan pun aplikasi berusaha berkomunikasi melalui jaringan, Anda akan diminta untuk memutuskan apakah komunikasi harus diperbolehkan atau diblokir
- ***Blokir -*** semua upaya komunikasi dari aplikasi akan diblokir

Dialog untuk mengedit kumpulan aturan aplikasi yang ada akan terbuka dengan menggunakan tombol ***Edit*** dari dialog ***Aplikasi*** dalam ***Pengaturan Firewall***:

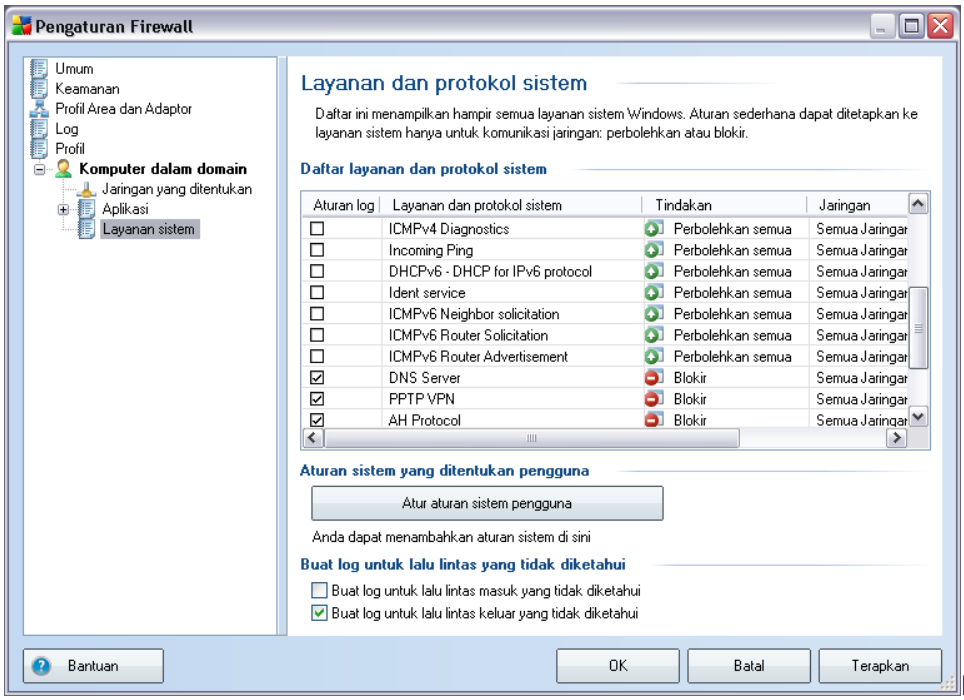


Dalam dialog ini Anda dapat mengedit semua parameter aplikasi:

- ***Informasi dasar aplikasi*** - nama aplikasi, keterangan singkatnya dan jalur lokasinya pada disk
- ***Tindakan aplikasi*** - dari menu buka bawah pilih aturan yang akan diterapkan pada cara kerja aplikasi:
  - ***Pengaturan lanjutan -*** opsi ini memungkinkan Anda mengedit kumpulan aturan secara terperinci di bagian bawah dialog ini
  - ***Perbolehkan semua -*** akan memperbolehkan upaya komunikasi apa pun dari aplikasi
  - ***Perbolehkan untuk aman -*** aplikasi hanya akan diperbolehkan berkomunikasi melalui jaringan aman (*sebagai contoh, komunikasi ke jaringan perusahaan yang telah terlindungi akan diperbolehkan walaupun komunikasi ke Internet diblokir*); untuk gambaran umum dan keterangan mengenai jaringan aman, lihat dialog ***Jaringan***
  - ***Tanya -*** kapan pun aplikasi berusaha berkomunikasi melalui jaringan, Anda akan diminta untuk memutuskan apakah komunikasi harus diperbolehkan atau diblokir
  - ***Blokir -*** semua upaya komunikasi dari aplikasi akan diblokir
- ***Kejadian aturan log*** - tandai opsi ini untuk mengonfirmasi bahwa Anda ingin merekam semua tindakan ***Firewall*** yang menyangkut aplikasi yang telah Anda konfigurasi kumpulan aturannya. Masing-masing entri log dapat ditemukan dalam dialog ***Log***.

10.5.4. Layanan Sistem

Segala pengeditan dalam dialog Layanan dan protokol standar sistem ditujukan untuk pengguna berpengalaman SAJA!



Dialog ***Layanan dan protokol standar sistem*** membuka gambaran umum atas layanan dan protokol sistem yang berkomunikasi melalui jaringan. Di bawah daftar, Anda dapat menemukan dua opsi: centang/jangan centang untuk mengonfirmasi bahwa Anda ingin merekam dalam log semua lalu lintas yang tidak dikenal dalam dua arah (*masuk atau keluar*).

Tombol kontrol

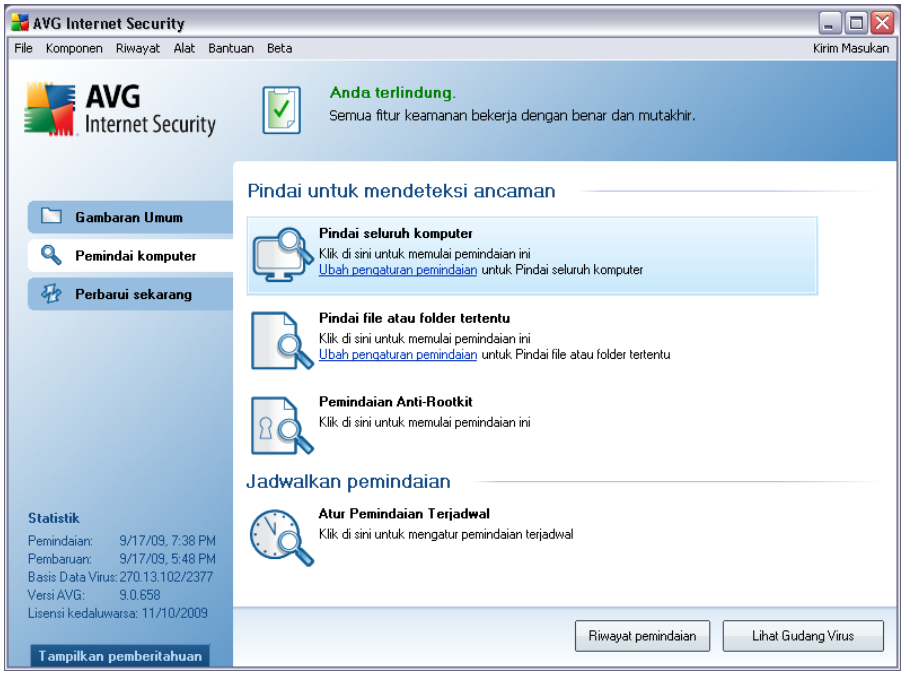
- ***Tambah/Edit*** - kedua tombol akan membuka dialog yang sama di mana Anda dapat mengedit parameter layanan sistem. Tombol ***Tambah*** membuka dialog kosong dan dalam mode dasar (*tidak ada bagian pengaturan lanjutan; namun bagian ini dapat dibuka dengan memilih pengaturan lanjutan untuk tindakan aplikasi*); tombol ***Edit*** membuka dialog yang sama dengan data yang sudah terisi yang merujuk pada layanan sistem yang dipilih.

Segala pengeditan dalam dialog Layanan dan protokol standar sistem ditujukan untuk pengguna berpengalaman SAJA!

11. Pemindaian AVG

Pemindaian adalah bagian krusial pada fungsionalitas **AVG 9 Internet Security**. Anda dapat menjalankan tes seperlunya atau menjadwalkannya untuk dijalankan secara berkala pada waktu yang diinginkan.

11.1. Antarmuka Pemindaian



Antarmuka pemindaian AVG dapat diakses melalui tautan cepat ***Pemindai Komputer***. 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:
    - ***Pindai seluruh komputer***
    - ***Pindai file atau folder tertentu***
    - ***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 indeksi yang terdeteksi dikarantina

11.2. Pemindaian Yang Ditentukan

Salah satu fitur utama **AVG 9 Internet Security** 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.

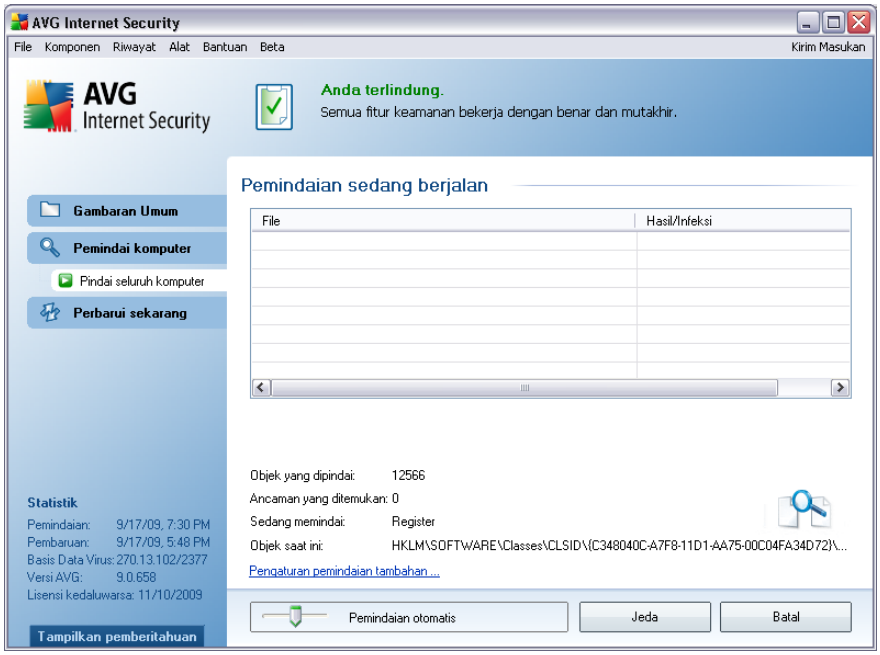
Dalam **AVG 9 Internet Security** Anda akan menemukan dua tipe pemindaian yang sudah ditentukan oleh vendor perangkat lunak:

11.2.1. Pindai Seluruh Komputer

Pindai seluruh komputer - memindai seluruh 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 menghapus infeksi yang terdeteksi ke ***Gudang Virus***. Pemindaian seluruh komputer Anda harus dijadwalkan pada workstation sedikitnya sekali seminggu.

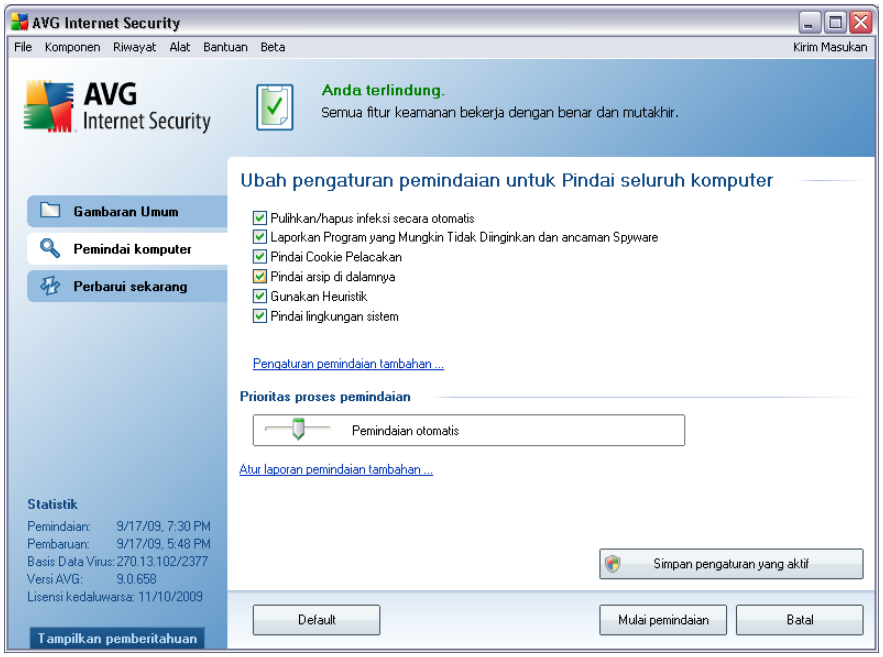
Peluncuran pindai

Pindai seluruh komputerdapat 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.



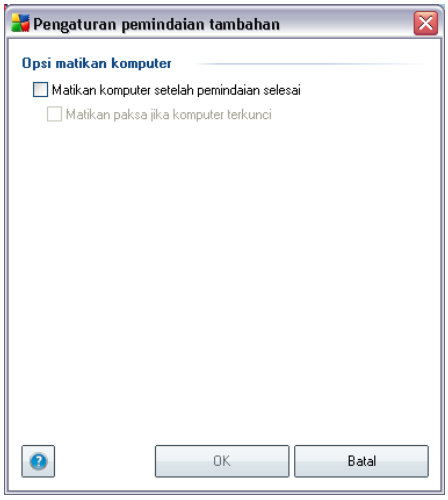
Mengedit konfigurasi pindai

Anda mempunyai opsi untuk mengedit pengaturan default yang telah ditentukan pada ***Pindai seluruh komputer***. Tekan tombol ***Ubah pengaturan pindai***untuk masuk ke dialog ***Ubah pengaturan pindai untuk Pindai seluruh 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. Secara default, hampir semua parameter diaktifkan dan ini akan digunakan secara otomatis selama pemindaian.

- ***Pengaturan pindai tambahan*** - tautan ini membuka dialog ***Pengaturan pindai tambahan*** yang baru di mana Anda dapat menetapkan parameter berikut:



- ***Opsi matikan komputer*** - putuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengonfirmasi 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***).

- ***Tentukan tipe file untuk pemindaian*** - selanjutnya Anda harus memutuskan Anda ingin memindai:

  - ***Semua tipe file*** yang menyertakan kemungkinan penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisahkan koma yang tidak harus dipindai; atau

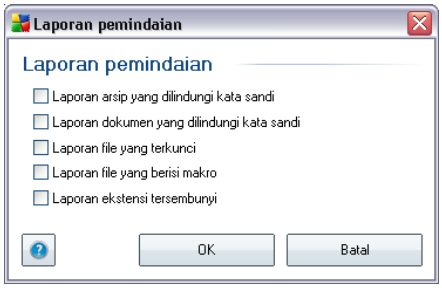
  - ***Tipe file yang dipilih*** - Anda dapat menetapkan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video,audio - jika Anda membiarkan kotak ini tidak dicentang, 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 menetapkan file mana yang harus selalu dipindai berdasarkan ekstensinya.

  - 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, prioritas diatur ke tingkat sedang (*Pindai otomatis*) yang mengoptimalkan kecepatan proses pemindaian dan penggunaan sumber daya sistem. 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 ditentukan - seperti diterangkan dalam bab* ***Pemindaian AVG / Menjadwalkan pemindaian/ Cara Memindai****. Seandainya Anda harus memutuskan untuk mengubah konfigurasi default* ***Pindai seluruh komputer*** *maka Anda dapat menyimpan pengaturan baru sebagai konfigurasi default untuk digunakan bagi semua pemindaian seluruh komputer selanjutnya.*

11.2.2. Pindai File atau Folder Tertentu

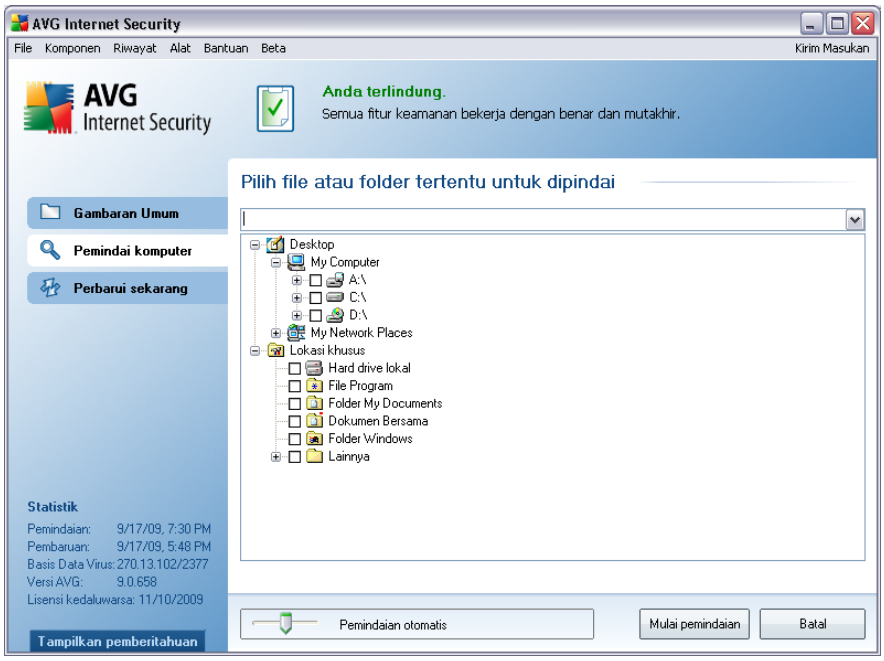
Pindai file atau folder tertentu - hanya memindai area komputer Anda yang telah dipilih untuk dipindai (*folder, hard disk, disket floppy, atau CD yang dipilih, dll.*). Progres pemindaian jika terdeteksi virus dan penyembuhannya sama dengan pindai seluruh komputer: virus yang ditemukan akan dipulihkan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

Peluncuran pindai

Pindai file atau folder tertentudapat 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.

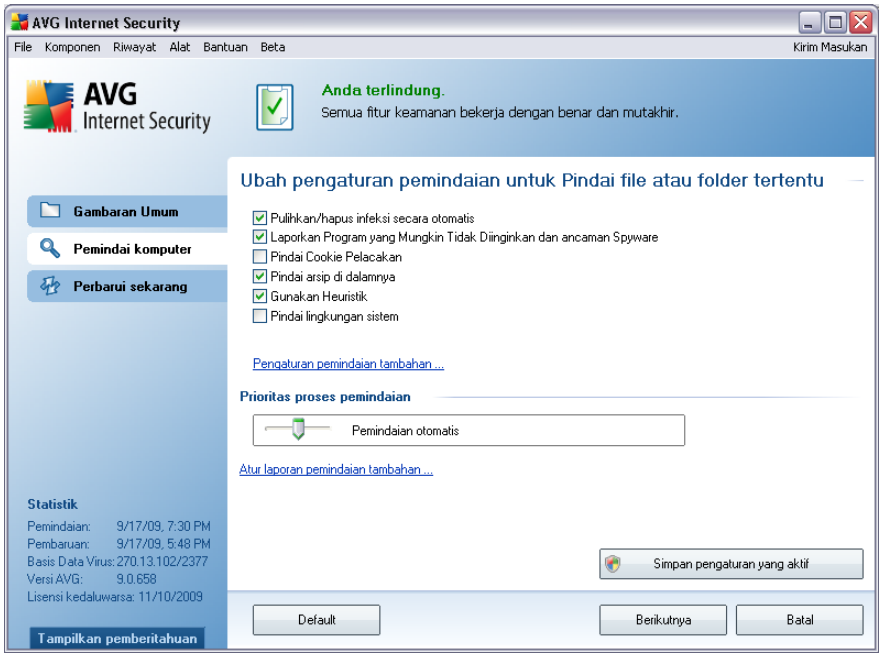
Juga ada kemungkinan pada folder tertentu yang dipindai sementara semua subfoldernya telah dikecualikan dari pemindaian ini; untuk melakukannya ketikkan tanda kurang "**-**" di depan jalur yang telah dibuat secara otomatis (*lihat cuplikan layar*). Untuk mengecualikan seluruh folder dari pemindaian,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

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



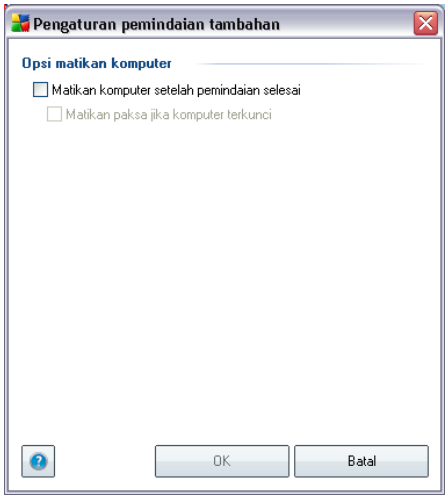
Mengedit konfigurasi pindai

Anda mempunyai opsi untuk mengedit pengaturan default yang telah ditentukan pada ***Pindai file atau folder tertentu***. Tekan tombol ***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 (*untuk keterangan terperinci mengenai pengaturan ini bacalah bab Pengaturan Lanjutan AVG / Pemindaian / Pindai File atau Folder Tertentu*).

- ***Pengaturan pindai tambahan*** - tautan ini membuka dialog Pengaturan pindai tambahan yang baru di mana Anda dapat menetapkan parameter berikut:



- ***Opsi matikan komputer*** - memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengonfirmasi 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***).

- ***Tentukan tipe file untuk pemindaian*** - selanjutnya Anda harus memutuskan Anda ingin memindai:

  - ***Semua tipe file*** yang menyertakan kemungkinan penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisahkan koma yang tidak harus dipindai; atau

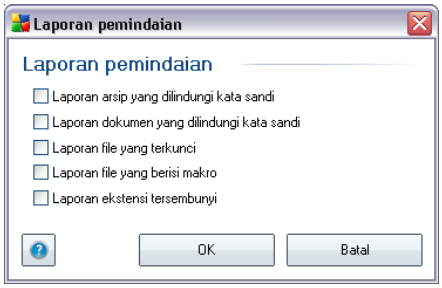
  - ***Tipe file yang dipilih*** - Anda dapat menetapkan bahwa Anda hanya ingin memindai file yang mungkin terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video,audio - jika Anda membiarkan kotak ini tidak dicentang, 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 menetapkan file mana yang harus selalu dipindai berdasarkan ekstensinya.

  - 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, prioritas diatur ke tingkat sedang (*Pindai otomatis*) yang mengoptimalkan kecepatan proses pemindaian dan penggunaan sumber daya sistem. 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:



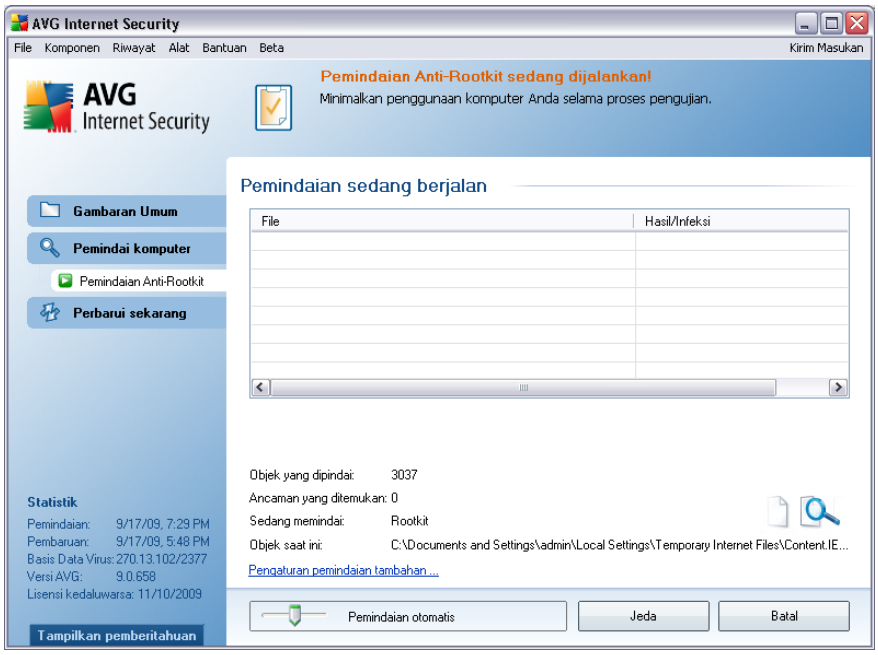
Peringatan: *Pengaturan pindai ini sama dengan parameter pemindaian yang baru ditentukan - seperti diterangkan dalam bab* ***Pemindaian AVG / Menjadwalkan pemindaian/ Cara Memindai****. Seandainya Anda harus memutuskan untuk mengubah konfigurasi default* ***Pindai file atau folder tertentu*** *maka Anda 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

Pemindaian Anti-Rootkit 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.

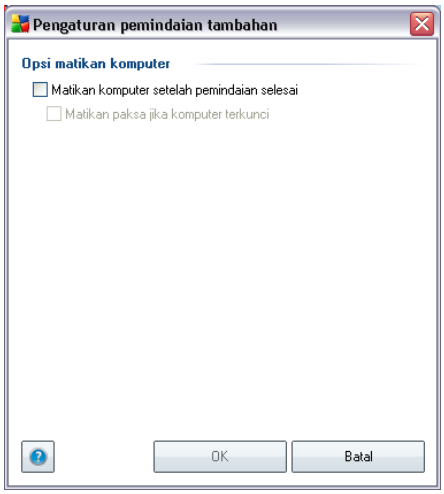


Mengedit konfigurasi pemindaian

Pemindaian Anti-Rootkit selalu diluncurkan di pengaturan default, dan mengedit parameter pemindaian hanya dapat diakses dalam dialog ***Pengaturan Lanjutan AVG/Anti-Rootkit***. Dalam antarmuka pemindaian, hanya tersedia konfigurasi berikut:

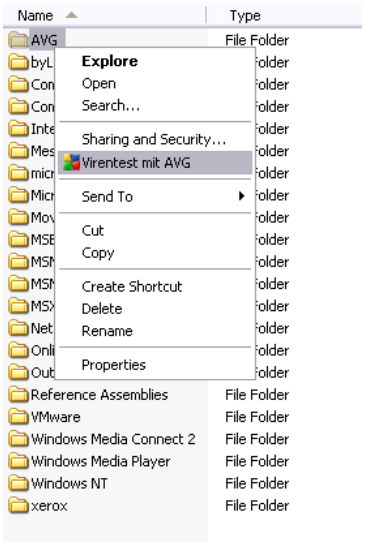
- ***Pindai otomatis*** - Anda dapat menggunakan penggeser untuk mengganti prioritas proses pemindaian. Secara default, prioritas diatur ke tingkat sedang (*Pindai otomatis*) yang mengoptimalkan kecepatan proses pemindaian dan penggunaan sumber daya sistem. Sebagai alternatif, Anda dapat menjalankan 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*).

- ***Pengaturan pindai tambahan*** - link ini membuka dialog baru ***Pengaturan pindai tambahan*** di mana Anda dapat menentukan kondisi yang memungkinkan untuk mematikan komputer sehubungan dengan ***Pemindaian Anti-Rootkit*** (***Matikan komputer setelah pemindaian selesai***, *atau mungkin* ***Matikan paksa jika komputer terkunci***):



11.3. Memindai dalam Windows Explorer

Di samping pemindaian yang telah ditentukan, yang diluncurkan untuk seluruh komputer atau area yang dipilih, **AVG 9 Internet Security** 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 **AVG 9 Internet Security** terdapat 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 seluruh 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 komputer yang akan dipindai, maka Anda harus memberikan jalur yang persis ke bagian yang dipilih tersebut), nilai-nilainya dipisah dengan koma, sebagai contoh: ***avgscanx /scan=C:\,D:***

Parameter pemindaian

Untuk menampilkan gambaran umum seluruh parameter yang tersedia, ketikkan perintah tersebut dengan paramater /? atau /HELP (mis. ***avgscanx /?***). Satu-satunya parameter wajib adalah /SCAN untuk menetapkan 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, juga memungkinkan untuk meluncurkan pemindaian baris perintah dari antarmuka pengguna grafis. Pemindaiannya sendiri akan diluncurkan dari baris perintah, dialog ***Penyusun Baris Perintah*** hanya memungkinkan Anda menetapkan 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 (e.g. /

SCAN=C:\;D:\)

- ***/COMP*** Pindai 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

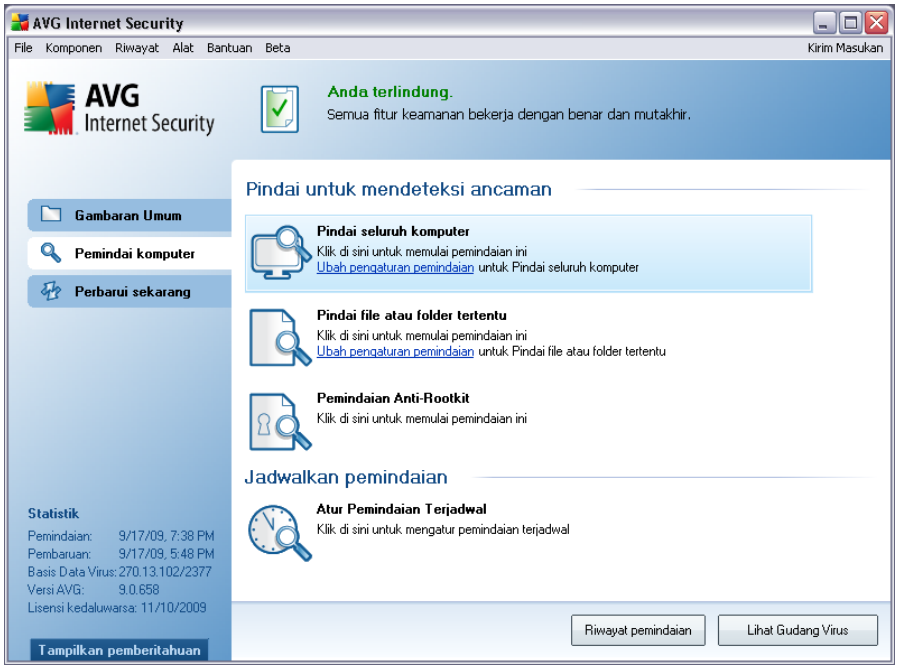
- ***/?*** Tampilkan bantuan untuk topik ini
- ***/HELP*** Tampilkan bantuan untuk topik ini
- ***/PRIORITY*** Atur prioritas pindai /Low, Auto, High/ (lihat Pengaturan lanjutan / Pemindaian)
- ***/SHUTDOWN*** Matikan komputer setelah pemindaian selesai
- ***/FORCESHUTDOWN*** Matikan paksa komputer setelah pemindaian selesai
- ***/ADS*** Pindai Aliran Data Alternatif (hanya NTFS)

11.5. Penjadwalan Pemindaian

Dengan **AVG 9 Internet Security** 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 jika dan kapan meluncurkan pemindaian.

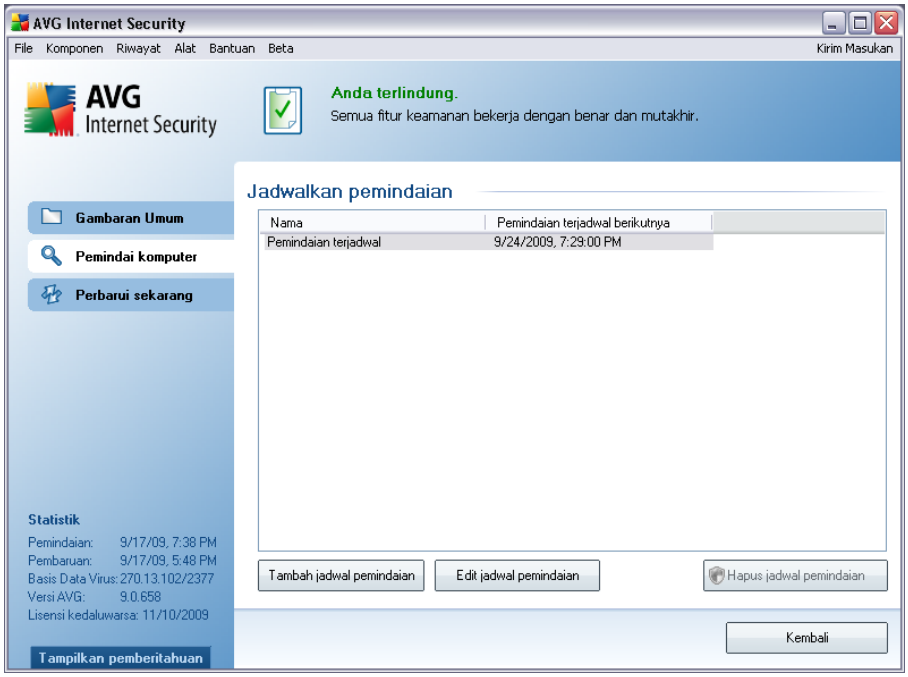
Anda harus meluncurkan ***Pindai seluruh komputer*** secara rutin, sedikitnya sekali seminggu. Walau demikian, jika memungkinkan, luncurkan pemindaian seluruh komputer Anda setiap hari - sebagaimana diatur dalam konfigurasi default jadwal pemindaian. Jika komputer "selalu dihidupkan" maka Anda dapat 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 menetapkan parameter tes yang baru ditentukan.

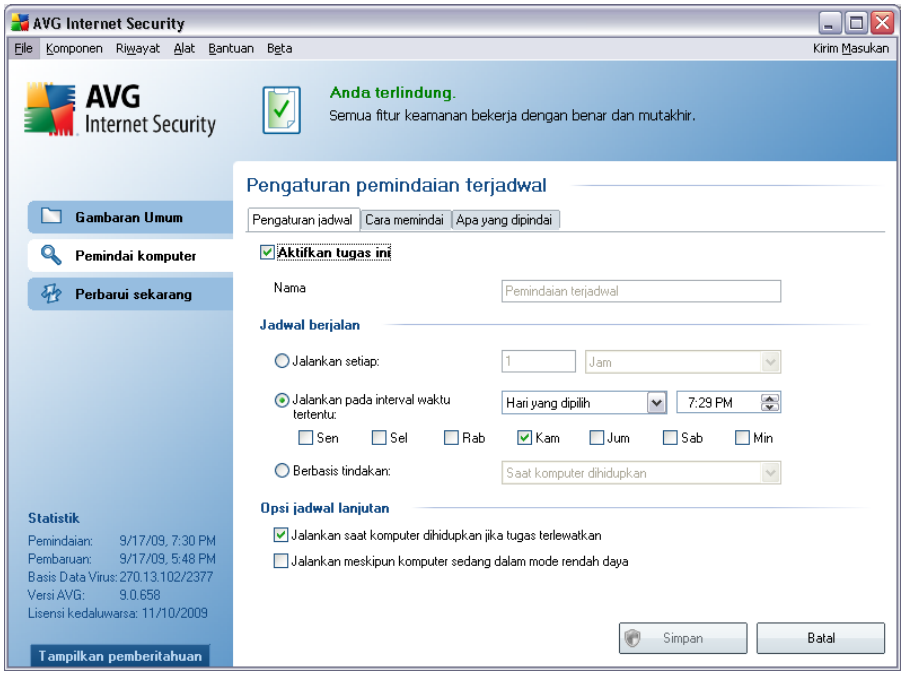
- ***Edit jadwal pemindaian*** - tombol ini hanya digunakan jika sebelumnya Anda telah memilih tes yang ada dari daftar pemindaian terjadwal. Jika tombol muncul sebagai aktif maka Anda dapat mengkliknya untuk beralih ke dialog ***Pengaturan pemindaian terjadwal*** , tab ***Pengaturan jadwal***. Parameter tes yang dipilih sudah ditetapkan di sini dan dapat diedit.

- ***Hapus jadwal pemindaian*** - tombol ini juga aktif jika sebelumnya Anda telah memilih tes yang ada dari daftar pemindaian terjadwal. Tes ini nanti dapat dihapus dari daftar dengan menekan tombol kontrol. Walau demikian, Anda hanya dapat menghapus tes Anda sendiri; ***Jadwal pemindaian seluruh komputer***yang telah ditentukan 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, masuklah ke dialog ***Pengaturan tes terjadwal*** (*klik tombol* ***Tambah jadwal pemindaian*** *dalam dialog* ***Jadwalkan pemindaian***). Dialog ini terbagi ke dalam tiga: ***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.

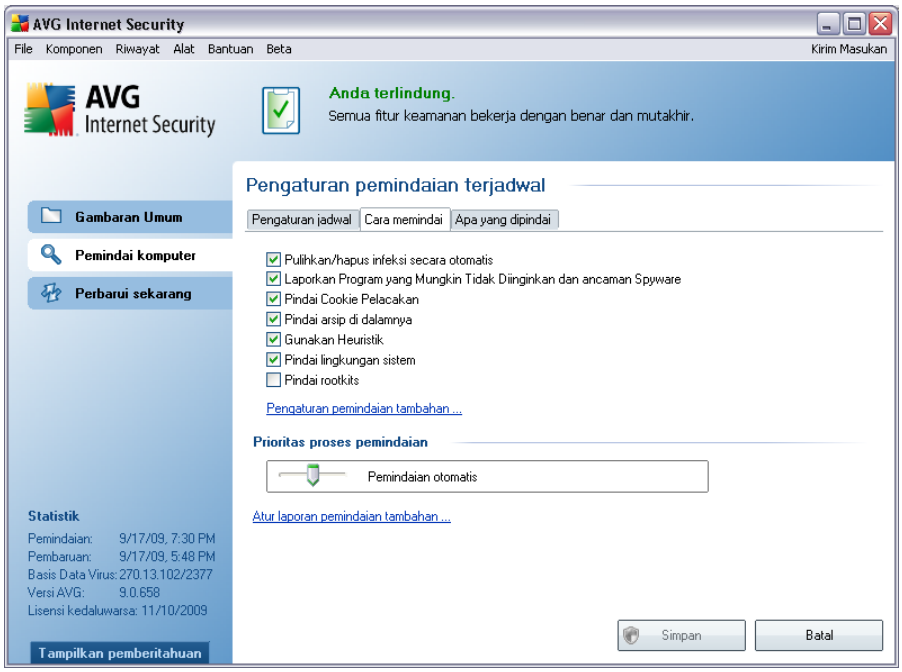
Tombol kontrol pada dialog Pengaturan pemindaian terjadwal

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 menetapkan semua persyaratan.

- ***Batalkan*** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG.

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 sah untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditentukan:

- ***Pulihkan/hapus infeksi secara otomatis*** - (*telah diaktifkan, secara default*): jika ada virus terdeteksi 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*** - (*telah diaktifkan secara default*): parameter ini mengontrol fungsionalitas ***Anti-Virus*** yang memungkinkan deteksi terhadap program yang mungkin tidak diinginkan (*file eksekusi yang dapat dijalankan sebagai spyware atau adware*) dan semua ini kemudian diblokir atau dihapus;

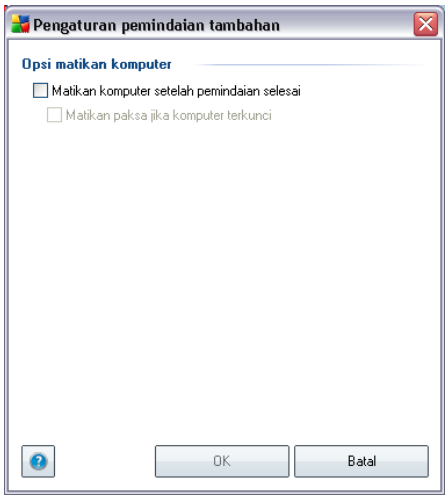
- ***Pindai Cookie Pelacak*** - (*telah diaktifkan, secara default*): parameter

komponen ***Anti-Spyware*** ini menentukan bahwa cookie harus terdeteksi selama pemindaian (*cookie HTTP digunakan untuk mengotentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*);

- ***Pindai di dalam arsip*** - (*telah diaktifkan, secara default*: parameter ini menentukan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut dikemas di dalam suatu tipe arsip, misalnya, ZIP, RAR, ...
- ***Gunakan Heuristik*** - (*telah 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*** - (*telah diaktifkan, secara default*): pemindaian juga akan memeriksa area sistem komputer Anda;
- ***Pindai rootkit*** - centang item ini jika Anda ingin menyertakan deteksi rootkit ke pemindaian seluruh komputer. Deteksi rootkit juga tersedia pada komponen ***Anti-Rootkit*** sendiri;

Kemudian, Anda dapat mengubah konfigurasi pemindaian seperti berikut:

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



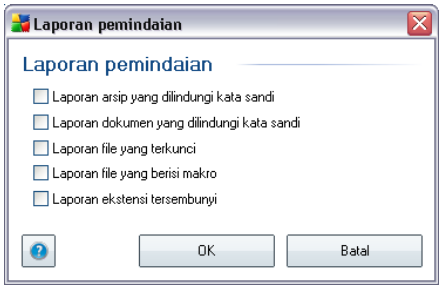
o ***Opsi matikan komputer*** - putuskan apakah komputer akan dimatikan

secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengonfirmasi 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***).

- ***Tentukan tipe file yang akan dipindai*** - selanjutnya Anda dapat memutuskan apakah Anda ingin memindai:
  - ***Semua tipe file*** yang menyertakan kemungkinan penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisahkan koma yang tidak harus dipindai; atau
  - ***Tipe file yang dipilih*** - Anda dapat menetapkan 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 dicentang, 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 menetapkan file mana yang harus selalu dipindai berdasarkan ekstensinya.
  - 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, prioritas diatur ke tingkat sedang (*Pindai otomatis*) yang mengoptimalkan kecepatan proses pemindaian dan penggunaan sumber daya sistem. 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 sah untuk mengubah pengaturan pemindaian, sangatlah disarankan untuk tetap menggunakan konfigurasi yang sudah ditentukan. 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****.*

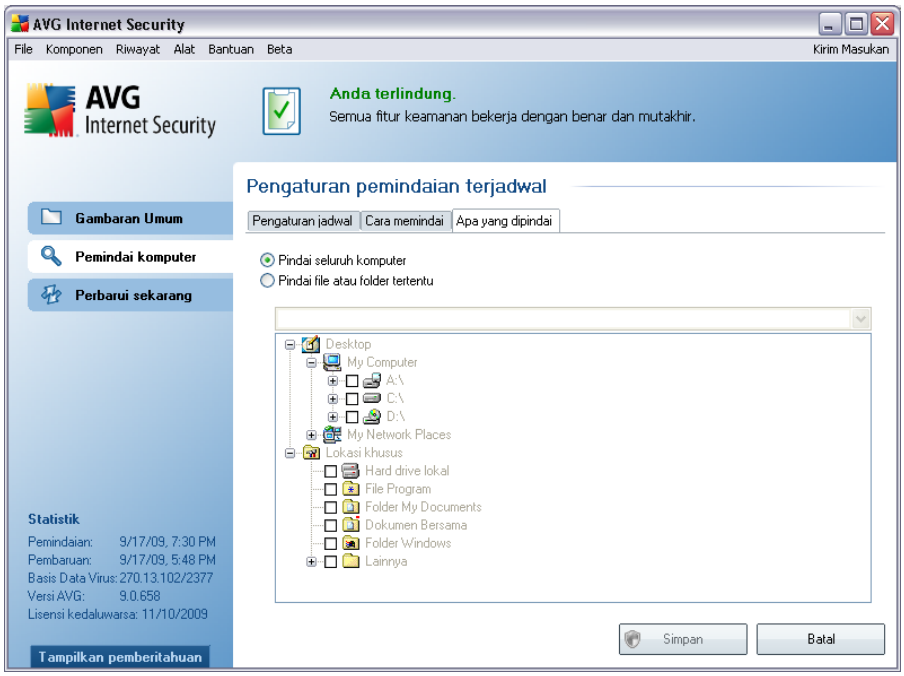
Tombol kontrol

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 menetapkan semua persyaratan.

- ***Batalkan*** - membatalkan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG.

11.5.3. Apa yang Dipindai



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.

Tombol kontrol pada dialog Pengaturan pemindaian terjadwal

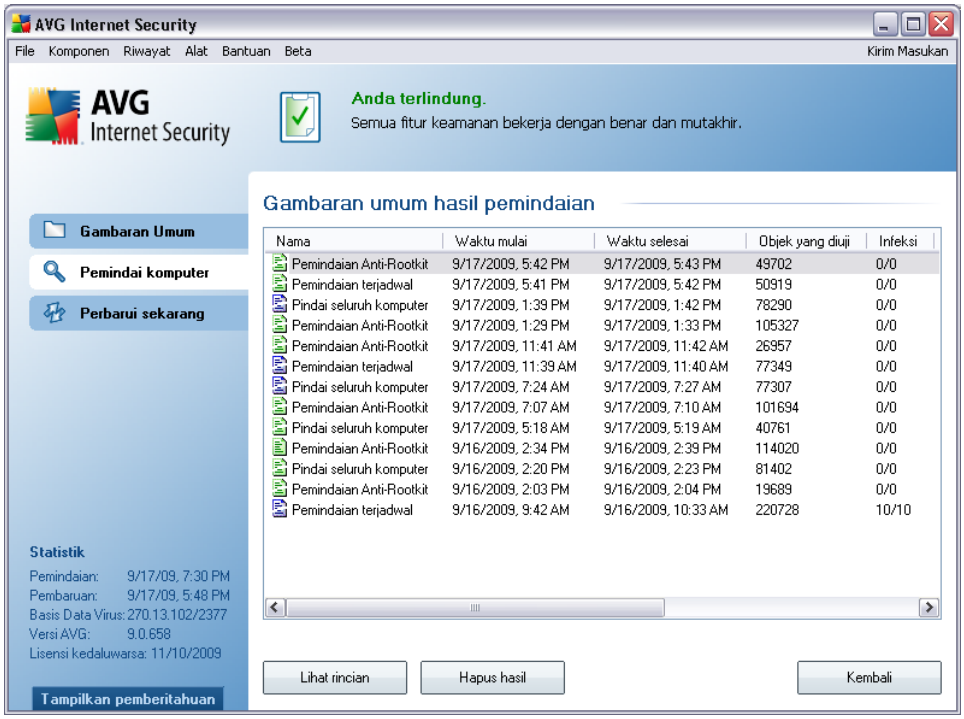
Ada dua tombol kontrol yang tersedia pada ketiga tab di dialog ***Pengaturan pemindaian terjadwal*** (***Pengaturan jadwal***, ***Cara memindai*** dan ***Apa yang dipindai***) dan semua ini mempunyai fungsionalitas yang sama, di tab apa pun saat itu Anda berada:

- ***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 menetapkan semua persyaratan.

- ***Batalkan*** - membatalkan semua perubahan yang telah dilakukan pada tab ini

atau tab lain pada dialog ini dan kembali ke dialog default antarmuka pemindaian AVG.

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
- ***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*** - tombol ini hanya aktif jika pemindaian tertentu dipilih dalam gambaran umum di atas; tekan ini untuk beralih ke dialog ***Hasil pemindaian*** untuk melihat data terperinci mengenai pemindaian yang dipilih
- ***Hapus hasil*** - tombol ini hanya aktif jika pemindaian tertentu dipilih dalam gambaran umum di atas; tekan ini untuk menghapus item yang dipilih dari gambaran umum hasil pemindaian
- ***Kembali*** - mengembalikan ke dialog default antarmuka pemindaian AVG

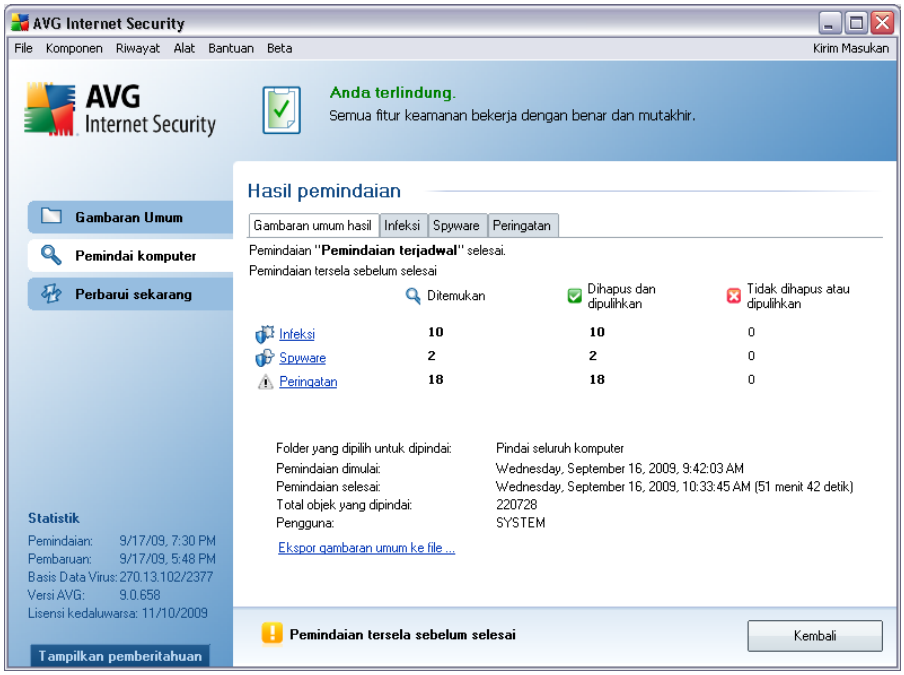
11.7. Perincian Hasil Pemindaian

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 hanya ditampilkan jika beberapa objek yang tidak dapat dipindai telah terdeteksi selama pemindaian
- ***Rootkit*** - tab ini hanya ditampilkan jika rootkit telah terdeteksi selama pemindaian
- ***Informasi*** **-** tab ini hanya ditampilkan jika beberapa kemungkinan ancaman telah terdeteksi namun tidak dapat dimasukkan sebagai salah satu dari kategori di atas; maka tab ini akan menyediakan pesan peringatan mengenai temuan tersebut

11.7.1. Tab Gambaran Umum Hasil



Pada tab ***Hasil pemindaian*** Anda dapat menemukan statistik terperinci berisi

informasi mengenai:

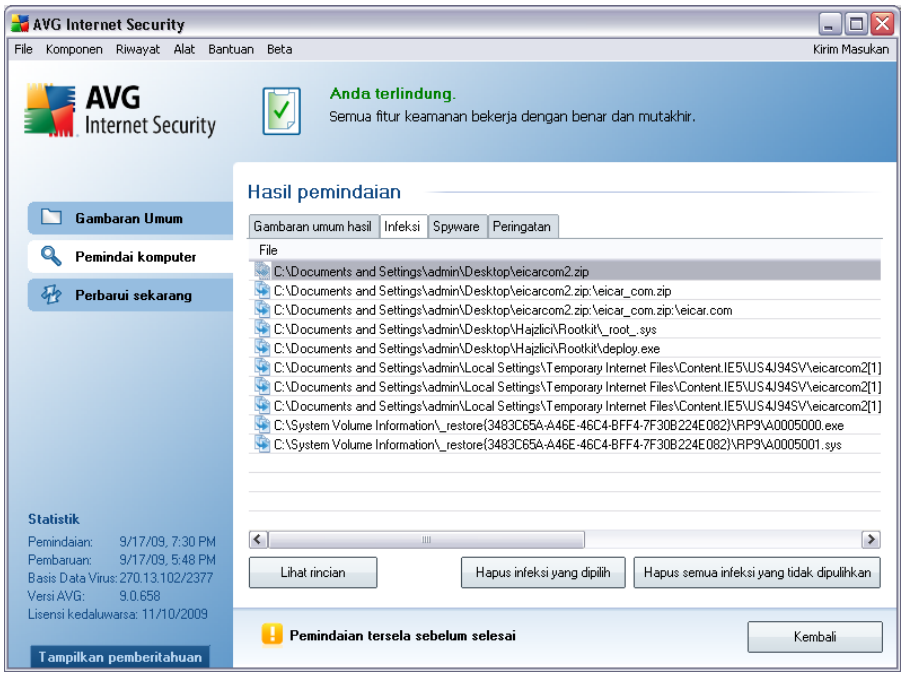
- infeksi virus / spyware yang terdeteksi
- infeksi virus / spyware yang dihapus
- jumlah infeksi virus / spyware yang tidak dapat dihapus atau dipulihkan

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



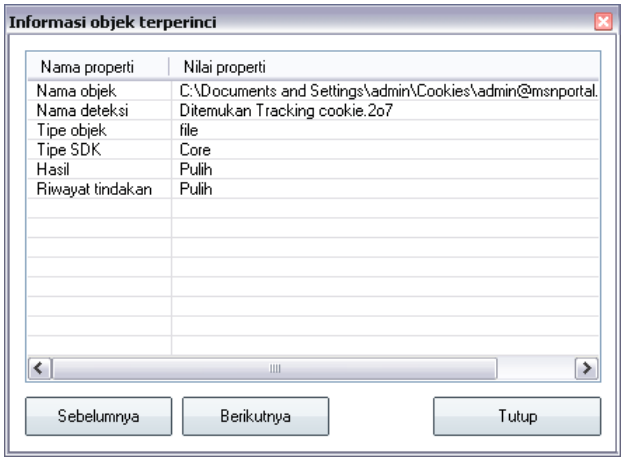
Tab ***Infeksi*** hanya ditampilkan dalam dialog ***Hasil pemindaian*** jika infeksi virus terdeteksi selama pemindaian. Tab ini terdiri dari tiga bagian yang memberikan informasi berikut:

- ***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:
    - ***Terinfeksi*** - objek terinfeksi yang terdeteksi dan dibiarkan di lokasi aslinya (*misalnya, jika Anda telah menonaktifkan opsi pemulihan otomatis dalam pengaturan pemindaian tertentu*)
    - ***Dipulihkan***- objek terinfeksi yang dipulihkan secara otomatis dan dibiarkan di lokasi aslinya
    - ***Dipindahkan ke Gudang Virus*** - objek yang terinfeksi telah dipindahkan ke karantina ***Gudang Virus***
    - ***Dihapus*** - objek yang terinfeksi dihapus
    - ***Ditambahkan ke pengecualian PUP*** - temuan telah dievaluasi sebagai pengecualian dan telah ditambahkan ke daftar pengecualian PUP (*dikonfigurasi dalam dialog* ***Pengecualian PUP*** *pada pengaturan lanjutan*)
    - ***File terkunci - belum dites*** - objek yang bersangkutan telah dikunci sehingga AVG tidak dapat memindainya
    - ***Objek yang mungkin berbahaya*** - objek telah terdeteksi sebagai objek yang mungkin berbahaya namun tidak terinfeksi *ia bisa berisi makro, misalnya*; informasi harus diartikan sebagai peringatan saja
    - ***Boot ulang diperlukan untuk menyelesaikan tindakan*** objek yang terinfeksi tidak dapat dihapus, untuk menghapusnya Anda harus menghidupkan ulang komputer Anda

Tombol kontrol

Ada tiga tombol kontrol yang tersedia dalam dialog ini:

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



Dalam dialog ini Anda dapat menemukan informasi lokasi objek terinfeksi yang terdeteksi (***Nama properti***). Dengan menggunakan tombol ***Sebelumnya*** / ***Berikutnya*** Anda dapat melihat informasi mengenai temuan tertentu. Gunakan tombol ***Tutup*** untuk menutup dialog ini.

- ***Hapus infeksi yang dipilih*** - gunakan tombol ini untuk memindahkan temuan yang dipilih ke ***Gudang Virus***
- ***Hapus semua infeksi 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 rincian mengenai virus tertentu, lihatlah* ***Ensiklopedia Virus*** *online*)
- ***Hasil*** - menentukan status terkini dari objek yang terdeteksi selama pemindaian:
    - ***Terinfeksi*** - objek terinfeksi yang terdeteksi dan dibiarkan di lokasi

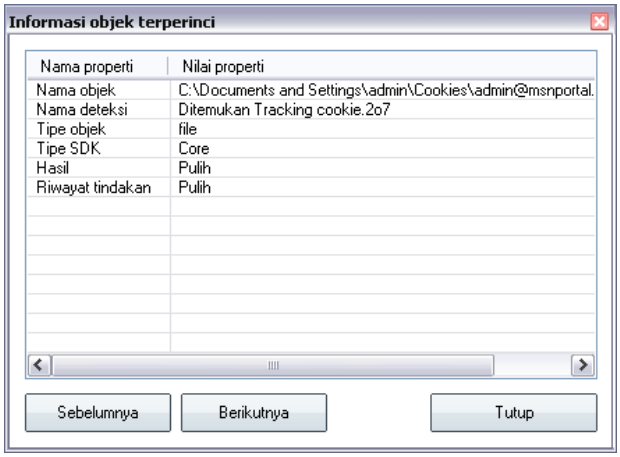
aslinya (misalnya, jika Anda telah menonaktifkan opsi pemulihan otomatis dalam pengaturan pemindaian tertentu)

- ***Dipulihkan*** - objek terinfeksi yang dipulihkan secara otomatis dan dibiarkan di lokasi aslinya
- ***Dipindahkan ke Gudang Virus*** - objek yang terinfeksi telah dipindahkan ke karantina ***Gudang Virus***
- ***Dihapus*** - objek yang terinfeksi dihapus
- ***Ditambahkan ke pengecualian PUP*** - temuan telah dievaluasi sebagai pengecualian dan telah ditambahkan ke daftar pengecualian PUP (*dikonfigurasi dalam dialog* ***Pengecualian PUP*** *pada pengaturan lanjutan*)
- ***File terkunci - belum dites*** - objek yang bersangkutan telah dikunci sehingga AVG tidak dapat memindainya
- ***Objek yang mungkin berbahaya*** - objek telah terdeteksi sebagai objek yang mungkin berbahaya namun tidak terinfeksi (ia bisa berisi makro, misalnya); informasi ini peringatan saja
- ***Boot ulang diperlukan untuk menyelesaikan tindakan*** objek yang terinfeksi tidak dapat dihapus, untuk menghapusnya Anda harus menghidupkan ulang komputer Anda

Tombol kontrol

Ada tiga tombol kontrol yang tersedia dalam dialog ini:

- ***Lihat rincian*** - tombol ini membuka jendela dialog baru bernama ***Rincian informasi hasil pemindaian***:

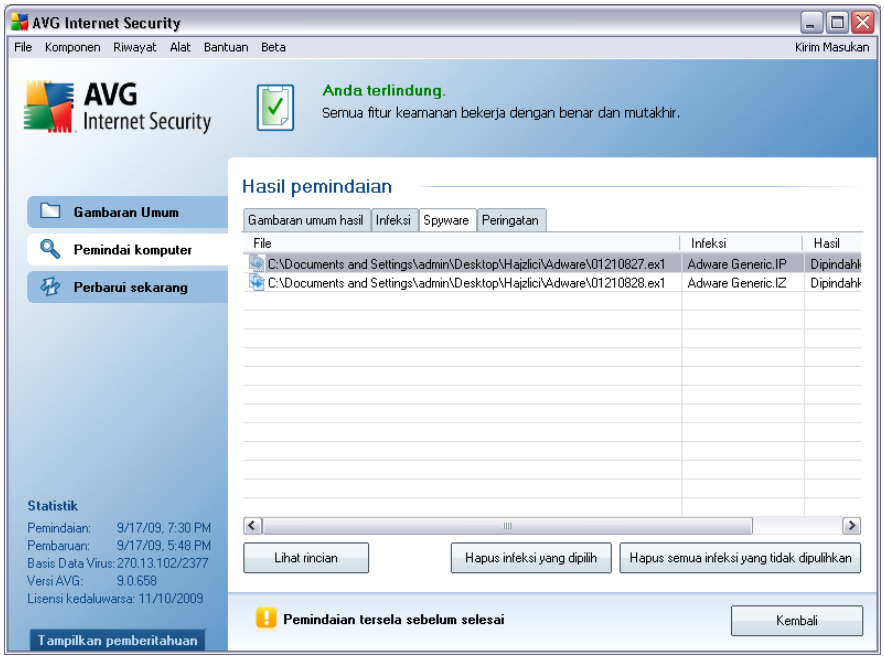


Dalam dialog ini Anda dapat menemukan informasi lokasi objek terinfeksi yang terdeteksi (***Nama properti***). Dengan menggunakan tombol ***Sebelumnya*** / ***Berikutnya*** Anda dapat melihat informasi mengenai temuan tertentu. Gunakan tombol ***Tutup*** untuk meninggalkan dialog ini.

- ***Hapus infeksi yang dipilih*** - gunakan tombol ini untuk memindahkan temuan yang dipilih ke ***Gudang Virus***
- ***Hapus semua infeksi 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***, atau secara manual menambahkan opsi pemindaian anti-rootkit ke dalam ***Pemindaian seluruh komputer*** (*opsi ini dinonaktifkan secara default*).

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***.

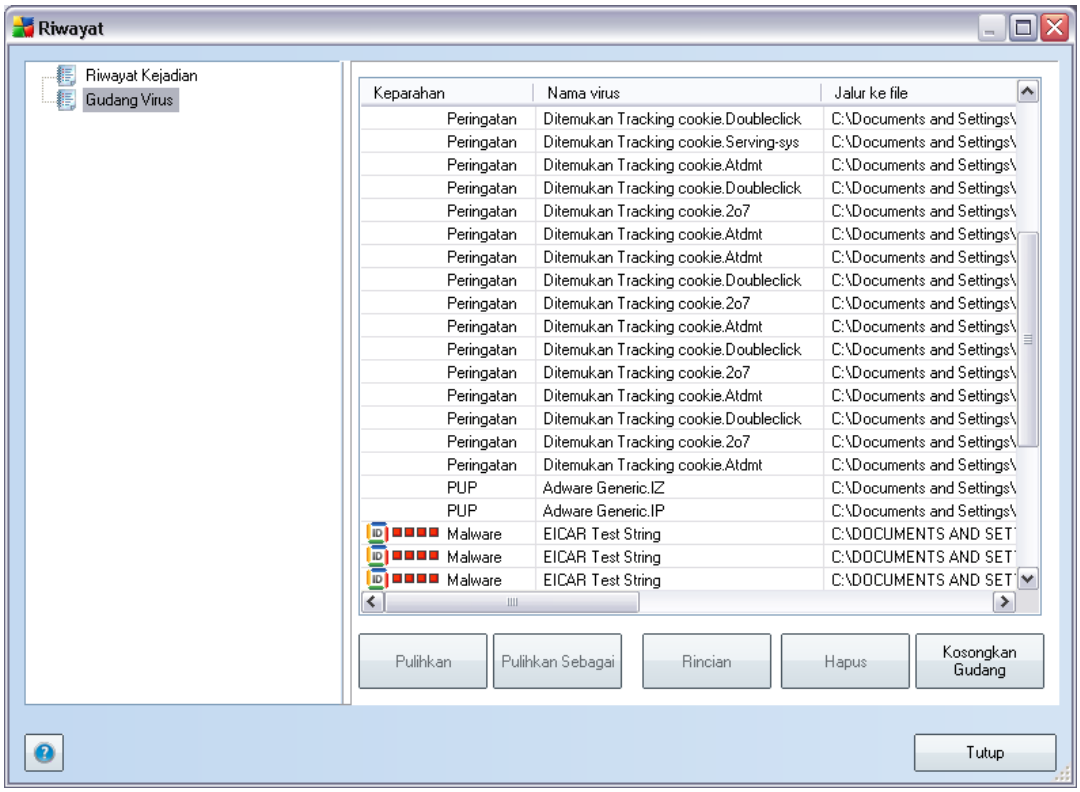
Informasi keseriusandapat dilaporkan untuk salah satu alasan berikut:

- ***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.

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

- ***Keseriusan*** - memberikan identifikasi grafis dari keseriusan temuan yang terkait pada skala empat-tingkat dari dapat diterima (■□□□) hingga sangat berbahaya (■■■■)
- ***Tipe infeksi*** - membedakan tipe temuan berdasarkan tingkat infeksi (*semua objek yang tercantum bisa jadi kemungkinan atau positif telah 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*** - seandainya Anda memutuskan untuk memindah objek terinfeksi yang terdeteksi dari ***Gudang Virus*** ke folder yang dipilih, gunakan tombol ini. Objek mencurigakan dan terdeteksi akan disimpan dengan nama aslinya. Jika nama aslinya tidak dikenal, maka nama standar yang akan digunakan.
- ***Hapus*** - menghapus sama sekali file yang terinfeksi dari ***Gudang Virus***
- ***Kosongkan Gudang*** - menghapus sama sekali semua isi ***Gudang Virus***

12. Pembaruan AVG

Menjaga AVG Anda selalu terbarui 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. Memeriksa setiap 4 jam akan menjamin bahwa basis Virus AVG Anda akan selalui terbarui sepanjang hari.

12.1. Tingkat Pembaruan

AVG menyediakan dua tingkat pembaruan untuk dipilih dari:

- ***Pembaruan definisi*** berisi perubahan yang diperlukan agar perlindungan anti-virus, anti-spam dan anti-malware tetap bisa diandalkan. Biasanya, ini tidak termasuk segala perubahan pada kode dan hanya memperbarui basis data definisi. Pembaruan ini akan diterapkan begitu tersedia.

- ***Pembaruan program*** berisi beragam perubahan program, perbaikan dan peningkatan.

Saat menjadwalkan pembaruan, Anda dapat memilih tingkat prioritas yang akan diunduh dan diterapkan.

12.2. Tipe Pembaruan

Anda dapat membedakan dua jenis 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 ditetapkan, ia akan diunduh langsung dari Internet atau dari direktori jaringan. Bila tidak tersedia pembaruan baru, maka tidak terjadi apa-apa.

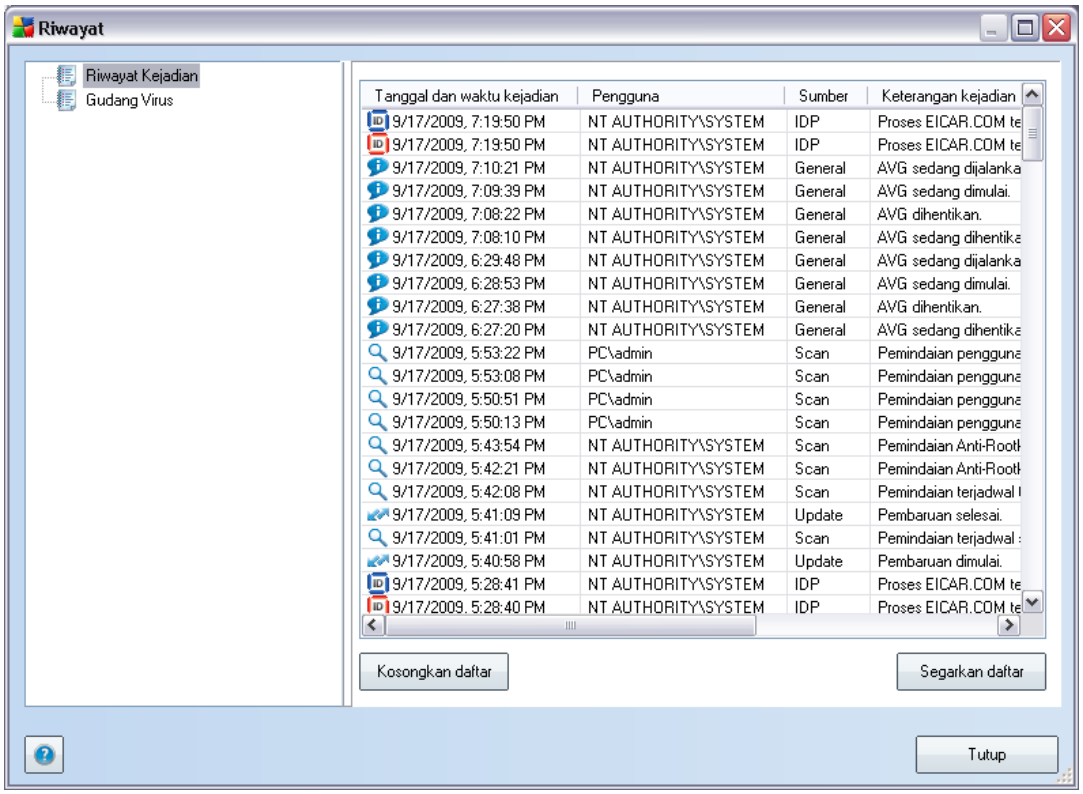
12.3. Proses Pembaruan

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. Hanya disarankan untuk pengguna yang berpengalaman!*

13. Riwayat Kejadian



Dialog ***Riwayat Kejadian*** dapat diakses dari menu sistem melalui item ***Riwayat/ Log Riwayat Kejadian***. Dalam dialog ini Anda dapat menemukan ringkasan kejadian penting yang terjadi selama operasi **AVG 9 Internet Security**. ***Riwayat Kejadian*** merekam tipe kejadian berikut:

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

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***dari situs web AVG (http://www.avg.com/).

Jika Anda tidak 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***.