



AVG 9 Internet Security

Manual Pengguna

Semakan dokumen 90.21 (3.2.2010)

Hak cipta AVG Technologies CZ, s.r.o. Semua hak terpelihara.
Semua tanda dagangan lain adalah hak milik pemilik masing-masing.

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

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

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

Produk ini menggunakan perpustakaan penekanan libbzip2, Hak Cipta (c) 1996-2002 Julian R. Seward.

Kandungan

1. Pengenalan	8
2. Keperluan Pemasangan AVG	9
2.1 Sistem Pengendalian yang Disokong	9
2.2 Keperluan Minimum & Disyorkan HW	9
3. Opsyen Pemasangan AVG	11
4. AVG Download Manager	12
4.1 Pemilihan Bahasa	12
4.2 Semakan Kesambungan	13
4.3 Tetapan Proksi	14
4.4 Muat Turun Fail Untuk Dipasang	15
5. Proses Pemasangan AVG	16
5.1 Lancarkan Pemasangan	16
5.2 Perjanjian Lesen	17
5.3 Memeriksa Status Sistem	17
5.4 Pilih Jenis Pemasangan	18
5.5 Aktifkan Lesen AVG anda	18
5.6 Pemasangan Tersuai - Folder destinasi	20
5.7 Pemasangan Tersuai - Pemilihan Komponen	21
5.8 PusatData AVG	22
5.9 AVG Security Toolbar	23
5.10 Tutup aplikasi terbuka	24
5.11 Memasang AVG	25
5.12 Jadualkan imbasan dan kemas kini yang tetap	26
5.13 Pemilihan penggunaan komputer	26
5.14 Sambungan Internet komputer anda	27
5.15 Konfigurasi perlindungan AVF selesai	28
6. Selepas Pemasangan	29
6.1 Pengoptimuman imbasan	29
6.2 Pendaftaran Produk	29
6.3 Akses ke Antara Muka Pengguna	29
6.4 Mengimbas seluruh komputer	30

6.5 Ujian Eicar	30
6.6 Konfigurasi Lalai AVG	31
7. Antara Muka Pengguna AVG	32
7.1 Menu Sistem	33
7.1.1 Fail	33
7.1.2 Komponen	33
7.1.3 Sejarah	33
7.1.4 Alat	33
7.1.5 Bantuan	33
7.2 Maklumat Status Keselamatan	36
7.3 Pautan Pantas	37
7.4 Gambaran keseluruhan Komponen	38
7.5 Statistik	39
7.6 Ikon Dulang Sistem	40
8. Komponen AVG	41
8.1 AntiVirus	41
8.1.1 Prinsip AntiVirus	41
8.1.2 Antara Muka AntiVirus	41
8.2 AntiPerisian Pengintip	43
8.2.1 Prinsip AntiPerisian Pengintip	43
8.2.2 Antara Muka AntiPerisian Pengintip	43
8.3 AntiSpam	45
8.3.1 Prinsip AntiSpam	45
8.3.2 Antara Muka AntiSpam	45
8.4 AntiRootkit	47
8.4.1 Prinsip AntiRootkit	47
8.4.2 Antara Muka AntiRootkit	47
8.5 Alatan Sistem	49
8.5.1 Proses	49
8.5.2 Sambungan Rangkaian	49
8.5.3 Automula	49
8.5.4 Sambungan Pelayar	49
8.5.5 Pemandang LSP	49
8.6 Firewall	56
8.6.1 Prinsip Firewall	56
8.6.2 Profil Firewall	56

8.6.3 Antara Muka Firewall	56
8.7 Pengimbas E-mel	61
8.7.1 Prinsip Pengimbas E-mel	61
8.7.2 Antara Muka Pengimbas E-mel	61
8.7.3 Pengesanan Pengimbas E-mel	61
8.8 Perlindungan ID	65
8.8.1 Prinsip Perlindungan ID	65
8.8.2 Antara Muka Perlindungan ID	65
8.9 Lesen	68
8.10 Pengimbas Pautan	69
8.10.1 Prinsip Pengimbas Pautan	69
8.10.2 Antara Muka Pengimbas Pautan	69
8.10.3 AVG Search-Shield	69
8.10.4 AVG Active Surf-Shield	69
8.11 Perisai Dalam Talian	73
8.11.1 Prinsip Perisai Dalam Talian	73
8.11.2 Antara Muka Perisai Dalam Talian	73
8.11.3 Pengesanan Perisai Dalam Talian	73
8.12 Resident Shield	79
8.12.1 Resident Shield Prinsip	79
8.12.2 Antara Muka Perisai Residen	79
8.12.3 Pengesanan Perisai Residen	79
8.13 Pengurus Kemas Kini	84
8.13.1 Kemas Kini Prinsip Pengurus	84
8.13.2 Kemas Kini Antara Muka Pengurus	84
9. AVG Security Toolbar	87
9.1 AVG Security Toolbar Antara muka	87
9.2 Opsyen AVG Security Toolbar	89
9.2.1 Tab Umum	89
9.2.2 Tab Butang Berguna	89
9.2.3 Tab Keselamatan	89
9.2.4 Tab Pilihan Lanjutan	89
10. Tetapan Lanjutan AVG	94
10.1 Penampilan	94
10.2 Bunyi	96
10.3 Abaikan Keadaan Rosak	98

10.4 Perlindungan Identiti	99
10.4.1 Tetap Perlindungan Identiti	99
10.4.2 Senarai dibenarkan	99
10.5 Bilik Kebal Virus	104
10.6 Pengecualian PUP	105
10.7 AntiSpam	107
10.7.1 Tetap	107
10.7.2 Pencapaian	107
10.7.3 RBL	107
10.7.4 Senarai putih	107
10.7.5 Senarai hitam	107
10.7.6 Tetap Lanjutan	107
10.8 Perisai Dalam Talian	119
10.8.1 Perlindungan Web	119
10.8.2 Pemesejan Segera	119
10.9 Pengimbas Pautan	123
10.10 Imbasan	124
10.10.1 Imbas Seluruh Komputer	124
10.10.2 Imbas Sambungan Kerangka	124
10.10.3 Imbas Fail atau Folder Tertentu	124
10.10.4 Imbasan Peranti Boleh Dialih	124
10.11 Jadual	131
10.11.1 Imbasan yang Dijadualkan	131
10.11.2 Jadual Kemas Kini Pangkalan Data Virus	131
10.11.3 Jadual Kemas Kini AntiSpam	131
10.12 Pengimbas E-mel	144
10.12.1 Perakuan	144
10.12.2 Penapisan Mel	144
10.12.3 Log dan Keputusan	144
10.12.4 Pelayan	144
10.13 Perisai Residen	154
10.13.1 Tetap Lanjutan	154
10.13.2 Direktori Tidak Termasuk	154
10.13.3 Fail yang Dikeluarkan	154
10.14 Pelayan Cache	159
10.15 AntiRootkit	160
10.16 Kemas kini	161
10.16.1 Proksi	161

10.16.2	<i>Dailan</i>	161
10.16.3	<i>URL</i>	161
10.16.4	<i>Uruskan</i>	161
10.17	<i>Pentadbiran Jauh</i>	169
11.	Tetapan Firewall	171
11.1	<i>Umum</i>	171
11.2	<i>Keselamatan</i>	172
11.3	<i>Profil Kawasan dan Penyesuai</i>	173
11.4	<i>Log</i>	174
11.5	<i>Profil</i>	176
11.5.1	<i>Maklumat Profil</i>	176
11.5.2	<i>Rangkaian yang Ditentukan</i>	176
11.5.3	<i>Aplikasi</i>	176
11.5.4	<i>Perkhidmatan Sistem</i>	176
12.	Pengimbasan AVG	189
12.1	<i>Antara Muka Pengimbasan</i>	189
12.2	<i>Imbasan Pratakrif</i>	190
12.2.1	<i>Imbas Seluruh Komputer</i>	190
12.2.2	<i>Imbas Fail atau Folder Tertentu</i>	190
12.2.3	<i>Imbasan AntiRootkit</i>	190
12.3	<i>Pengimbasan dalam Windows Explorer</i>	200
12.4	<i>Pengimbasan Garis Perintah</i>	201
12.4.1	<i>Parameter Imbasan CMD</i>	201
12.5	<i>Penjadualan Imbasan</i>	203
12.5.1	<i>Tetapan Jadual</i>	203
12.5.2	<i>Bagaimana untuk Mengimbas</i>	203
12.5.3	<i>Apa untuk Diimbas</i>	203
12.6	<i>Gambaran Keseluruhan Keputusan Imbasan</i>	214
12.7	<i>Keputusan Imbasan Butiran</i>	215
12.7.1	<i>Tab Gambaran Keseluruhan Keputusan</i>	215
12.7.2	<i>Tab Jangkitan</i>	215
12.7.3	<i>Tab Perisian Pengintip</i>	215
12.7.4	<i>Tab Amaran</i>	215
12.7.5	<i>Tab Rootkit</i>	215
12.7.6	<i>Tab Maklumat</i>	215
12.8	<i>Bilik Kebal Virus</i>	224

13. Kemas kini AVG	227
13.1 Tahap Kemas kini	227
13.2 Jenis Kemas Kini	227
13.3 Kemas Kini Proses	228
14. Sejarah Acara	229
15. Soalan Lazim dan Sokongan Teknikal	231



1. Pengenalan

Manual pengguna ini memberikan dokumentasi menyeluruh untuk **AVG 9 Internet Security**.

Tahniah bagi pembelian AVG 9 Internet Security anda!

AVG 9 Internet Security adalah salah satu rangkaian produk AVG yang memenangi anugerah yang direka bentuk untuk memberikan anda ketenangan minda dan keselamatan menyeluruh untuk PC anda. Sama seperti semua produk AVG **AVG 9 Internet Security** telah direka bentuk semula sepenuhnya, daripada asas, untuk memberikan perlindungan keselamatan AVG yang terkenal dan diiktiraf yang baru, lebih mesra pengguna dan berkesan.

Produk **AVG 9 Internet Security** baru anda mempunyai antara muka yang digaris arus digabungkan dengan pengimbasan yang lebih agresif dan cepat. Lebih banyak ciri keselamatan yang telah diautomasi untuk kesenangan anda dan opsyen pengguna 'bijak' yang baru telah dimasukkan supaya anda boleh menyesuaikan ciri keselamatan kami dengan gaya hidup anda. Tiada lagi penggunaan yang menimbulkan curiga untuk keselamatan!

AVG telah direka dan dibangunkan untuk melindungi aktiviti pengkomputeran dan perangkaan anda. Nikmati pengalaman perlindungan penuh dari AVG.



2. Keperluan Pemasangan AVG

2.1. Sistem Pengendalian yang Disokong

AVG 9 Internet Security adalah bertujuan untuk melindungi stesen kerja dengan sistem pengendalian berikut:

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edisi SP1
- Windows Vista (x86 dan x64, semua edisi)
- Windows 7 (x86 dan x64, semua edisi)

(dan berkemungkinan pek perkhidmatan lebih tinggi untuk sistem pengendalian khusus)

Nota: Komponen [Perlindungan ID](#) tidak disokong pada Windows 2000 dan XP x64. Pada sistem pengendalian ini, anda boleh memasang AVG 9 Internet Security tetapi hanya tanpa komponen IDP.

2.2. Keperluan Minimum & Disyorkan HW

Keperluan perkakasan minimum untuk **AVG 9 Internet Security**:

- Intel Pentium CPU 1,5 GHz
- 512 MB memori RAM
- 390 MB ruang pemacu keras yang kosong (untuk tujuan pemasangan)

Keperluan perkakasan disyorkan untuk **AVG 9 Internet Security**:

- Intel Pentium CPU 1,8 GHz
- 512 MB memori RAM



- 510 MB ruang pemacu keras yang kosong (untuk tujuan pemasangan)



3. Opsyen Pemasangan AVG

AVG boleh dipasang sama ada dari fail pemasangan yang tersedia pada CD pemasangan anda atau anda boleh memuat turun fail pemasangan terkini dari tapak web AVG (<http://www.avg.com/>).

Sebelum anda mula memasang AVG, kami amat menyarankan anda mengunjungi tapak web AVG (<http://www.avg.com/>) untuk menyemak fail pemasangan baru. Dengan cara ini, anda boleh memastikan untuk memasang versi tersedia terkini bagi AVG 9 Internet Security.

Kami mengesyorkan anda mencuba alat [Pengurus Muat Turun AVG](#) baru kami yang akan membantu anda menyediakan fail pemasangan dalam bahasa yang anda perlukan!

Sewaktu proses pemasangan, anda akan diminta nombor lesen/jualan. Sila pastikan anda mempunyainya sebelum memulakan pemasangan. Nombor jualan boleh ditemui pada pembungkusan CD. Jika anda sudah membeli salinan AVG dalam talian, nombor lesen anda akan dihantar kepada anda melalui e-mel.

4. AVG Download Manager

AVG Download Manager adalah alat mudah yang membantu anda memiliki fail pemasangan yang betul untuk versi percubaan bagi produk AVG anda. Berdasarkan pada data input anda, pengurus akan memilih produk tertentu, jenis lesen, komponen yang dikehendaki dan bahasa. Akhir sekali, **AVG Download Manager** akan pergi ke muat turun dan pelancaran [proses pemasangan](#) yang sesuai.

Amaran: Sila maklum bahawa Pengurus Muat Turun AVG tidak sesuai untuk memuat turun rangkaian dan edisi SBS dan hanya sistem pengendalian berikut disokong: Windows 2000 (SP4 + SRP gulung atas), Windows XP, Windows Vista a Windows 7.

AVG Download Manager tersedia untuk muat turun di tapak web AVG (<http://www.avg.com/>). Berikut, sila dapatkan penerangan ringkas mengenai setiap langkah tunggal yang anda perlu bawa dalam **AVG Download Manager**:

4.1. Pemilihan Bahasa

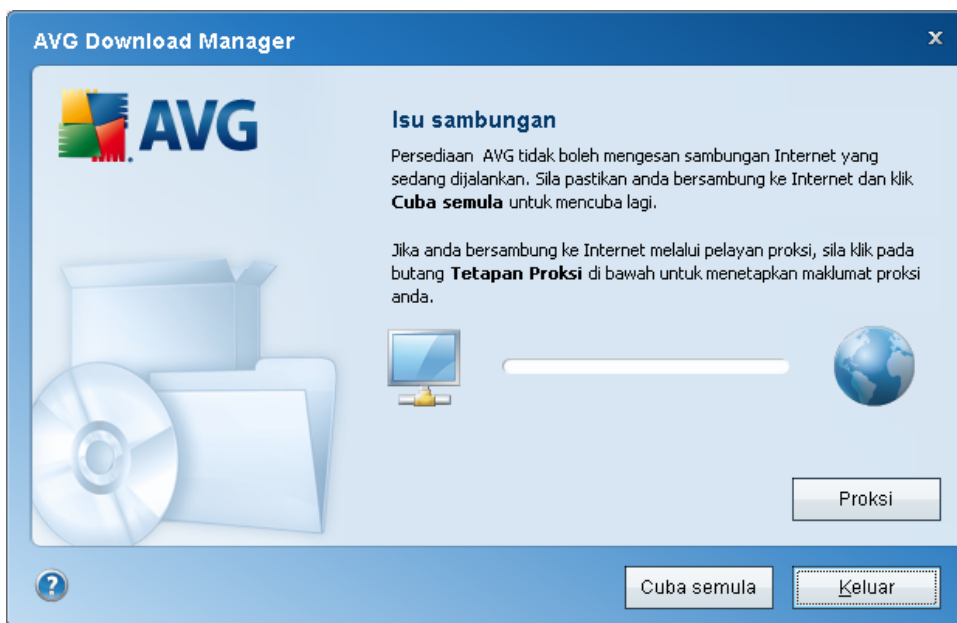


Dalam langkah pertama bagi **AVG Download Manager** pilih bahasa pemasangan daripada menu gulung bawah. Harap maklum bahawa pilihan bahasa digunakan untuk proses pemasangan sahaja; selepas pemasangan anda boleh menukar bahasa secara terus dari tetapan atur cara. Kemudian, tekan butang **Berikutnya** untuk teruskan.

4.2. Semakan Kesambungan

Dalam langkah seterusnya, **AVG Download Manager** akan cuba mewujudkan sambungan Internet supaya kemas kini boleh ditemui. Anda tidak dibenarkan untuk mendahului proses muat turun sehingga **AVG Download Manager** boleh melengkapkan ujian kesambungan.

- Jika ujian menunjukkan tiada kesambungan, pastikan anda benar-benar bersambung kepada Internet. Kemudian, klik butang **Cuba Semula**



- Jika anda menggunakan sambungan Proksi kepada Internet, klik butang **Tetapan Proksi** untuk menentukan [maklumat proksi](#) anda:
- Jika semakan telah berjaya, tekan butang **Berikutnya** untuk teruskan.

4.3. Tetapan Proksi

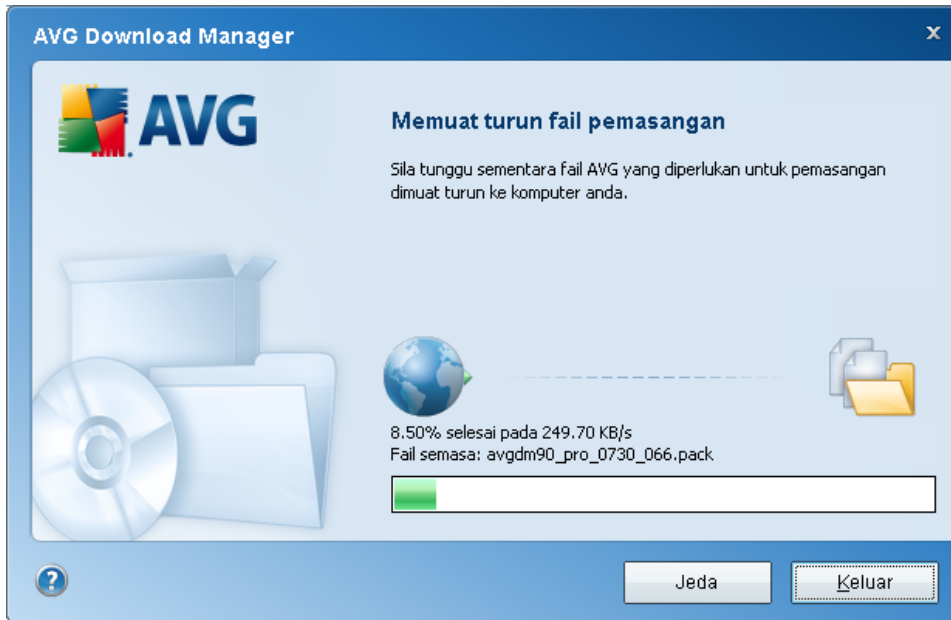


Jika **AVG Download Manager** tidak dapat mengenal pasti tetapan Proksi anda, anda perlu menentukannya secara manual. Sila isikan data berikut:

- **Pelayan** - masukkan nama pelayan atau alamat IP yang sah
- **Port** - memberikan nombor port masing-masing
- **Guna pengesahan proksi** - jika pelayan proksi anda memerlukan pengesahan, tandakan rait kotak semakan ini.
- **Pilih pengesahan** - dari menu jatuh bawah, pilih jenis pengesahan. Kami amat mengesyorkan anda mengekalkan nilai lalai (*kemudian, pelayan proksi akan mematuhi keperluannya kepada anda secara automatik*). Walau bagaimanapun, jika anda adalah pengguna yang berkemahiran, anda juga boleh memilih opsiyen Basic (*diperlukan oleh sesetengah pelayan*) atau NTLM (*diperlukan oleh semua ISA Servers*). Kemudian, masukkan **Nama pengguna** dan **Kata laluan** (secara pilihan).

Sahkan tetapan anda dengan menekan butang **Guna** untuk mengikuti langkah seterusnya bagi **AVG Download Manager**.

4.4. Muat Turun Fail Untuk Dipasang



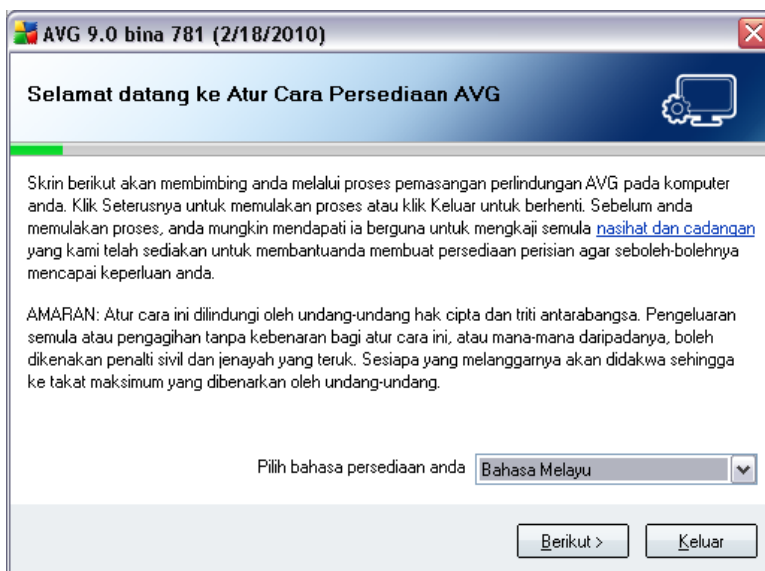
Kini, anda telah berikan semua maklumat yang diperlukan untuk **AVG Download Manager** untuk memulakan muat turun pakej pemasangan, dan melancarkan proses pemasangan. Seterusnya, lanjutkan kepada [Proses Pemasangan AVG](#).

5. Proses Pemasangan AVG

Untuk memasang **AVG 9 Internet Security** pada komputer anda, anda perlu mendapatkan fail pemasangan terkini. Anda boleh menggunakan fail pemasangan dari CD yang merupakan sebahagian daripada edisi kotak anda tetapi fail ini mungkin telah tamat tempoh. Oleh itu, kami menyarankan untuk mendapatkan fail pemasangan terkini dalam talian. Anda boleh memuat turun fail dari tapak web AVG (<http://www.avg.com/>), bahagian **Pusat Sokongan / Muat Turun**. Atau, anda boleh menggunakan alat **Pengurus Muat Turun AVG** baru yang membantu anda membuat dan memuat turun pakej pemasangan yang anda perlukan dan melancarkan proses pemasangan.

Pemasangan adalah jujukan tettingkap dialog dengan penerangan ringkas mengenai apa yang perlu dilakukan pada setiap langkah. Dalam yang berikut, kami menawarkan penerangan untuk setiap tettingkap dialog.

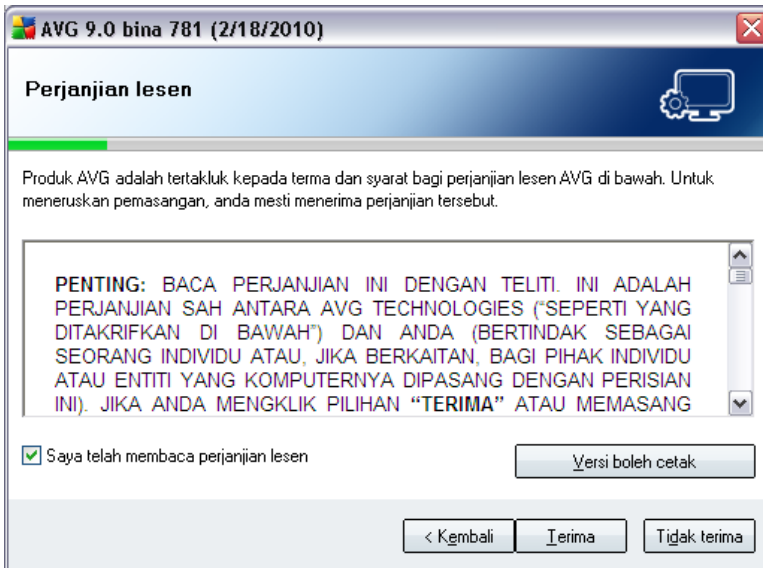
5.1. Lancarkan Pemasangan



Proses pemasangan bermula dengan tettingkap **Selamat Datang ke Atur Cara Persediaan AVG**. Di sini, anda pilih bahasa yang digunakan untuk proses pemasangan. Dalam bahagian bawah tettingkap dialog, cari item **Pilih bahasa persediaan anda**, dan pilih bahasa yang dikehendaki dari menu jatuh bawah. Kemudian, tekan butang **Berikutnya** untuk mengesahkan dan meneruskan ke dialog berikutnya.

Perhatian: Di sini, anda memilih bahasa untuk proses pemasangan sahaja. Anda tidak memilih bahasa untuk aplikasi AVG - yang boleh ditentukan kemudian sewaktu proses pemasangan!

5.2. Perjanjian Lesen



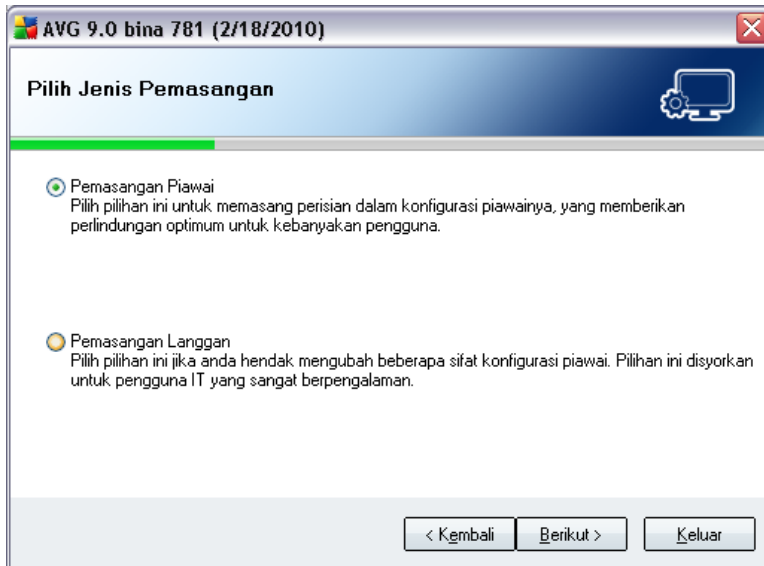
Dialog **Perjanjian Lesen** memberikan kata-kata penuh mengenai perjanjian lesen AVG. Sila bacanya dengan berhati-hati dan sahkan bahawa anda membaca, memahami dan menerima perjanjian dengan menandakan kotak semakan **Saya telah membaca perjanjian lesen** dan menekan butang **Terima**.

Jika anda tidak bersetuju dengan perjanjian lesen, tekan butang **Tidak terima**, dan proses pemasangan akan ditamatkan serta-merta.

5.3. Memeriksa Status Sistem

Dengan perjanjian lesen disahkan, anda akan diarahkan semula ke dialog **Menyemak Status Sistem**. Dialog ini tidak memerlukan sebarang campur tangan; sistem anda sedang disemak sebelum pemasangan AVG boleh bermula. Sila tunggu sehingga proses selesai, kemudian, teruskan secara automatik dengan dialog berikut.

5.4. Pilih Jenis Pemasangan



Dialog **Pilih Jenis Pemasangan** menawarkan pilihan dua opsyen pemasangan: pemasangan **standard** dan **tersuai**.

Untuk kebanyakan pengguna, ia amat disyorkan untuk mengekalkan **pemasangan standard** yang memasang AVG dalam mod automatik sepenuhnya dengan tetapan yang dipraktikkan oleh vendor atur cara. Konfigurasi ini memberikan keselamatan maksimum yang digabungkan dengan penggunaan optimum sumber. Di masa hadapan, jika perlu untuk mengubah konfigurasi, anda sentiasa mempunyai kemungkinan untuk melakukannya secara terus dalam aplikasi AVG.

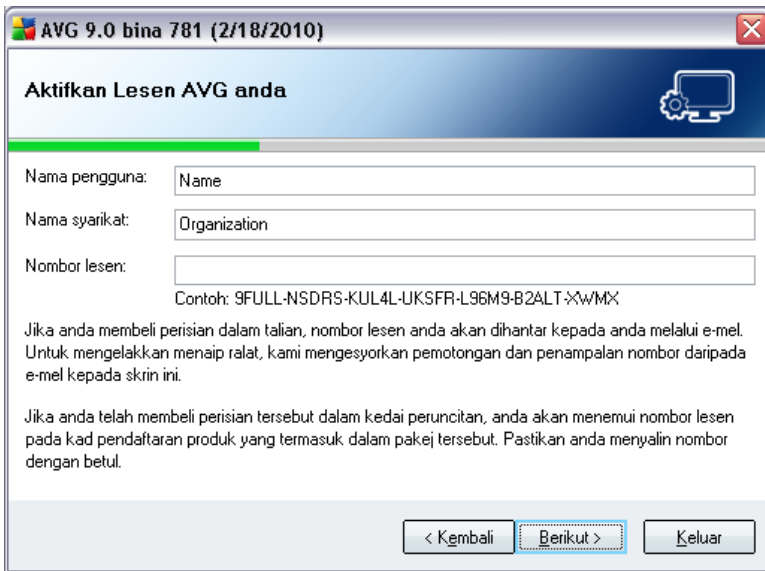
Pemasangan tersuai hanya patut digunakan oleh pengguna berpengalaman yang mempunyai sebab yang sah untuk memasang AVG dengan tetapan bukan piawai. Cth. untuk memenuhi keperluan sistem khusus.

5.5. Aktifkan Lesen AVG anda

Dalam dialog **Aktifkan AVG License anda** anda perlu mengisi data pendaftaran anda. Taipkan nama anda (medan **Nama pengguna**) dan nama organisasi anda (medan **Nama Syarikat**).

Kemudian, masukkan nombor lesen/jualan ke dalam medan teks **Nombor Lesen**. Nombor jualan boleh ditemui pada pembungkusan CD dalam kotak **AVG 9 Internet Security** anda. Nombor lesen akan berada dalam e-mel pengesahan yang anda terima

selepas membeli **AVG 9 Internet Security** anda dalam talian. Anda mesti menaip nombor betul-betul seperti yang ditunjukkan. Jika bentuk digital nombor lesen tersedia (*dalam e-mel*), ia disyorkan untuk menggunakan kaedah salin dan tampal untuk memasukkannya.



AVG 9.0 bina 781 (2/18/2010)

Aktifkan Lesen AVG anda

Nama pengguna:

Nama syarikat:

Nombor lesen:

Contoh: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX

Jika anda membeli perisian dalam talian, nombor lesen anda akan dihantar kepada anda melalui e-mel. Untuk mengelakkan menaip ralat, kami mengesyorkan pemotongan dan penampalan nombor daripada e-mel kepada skrin ini.

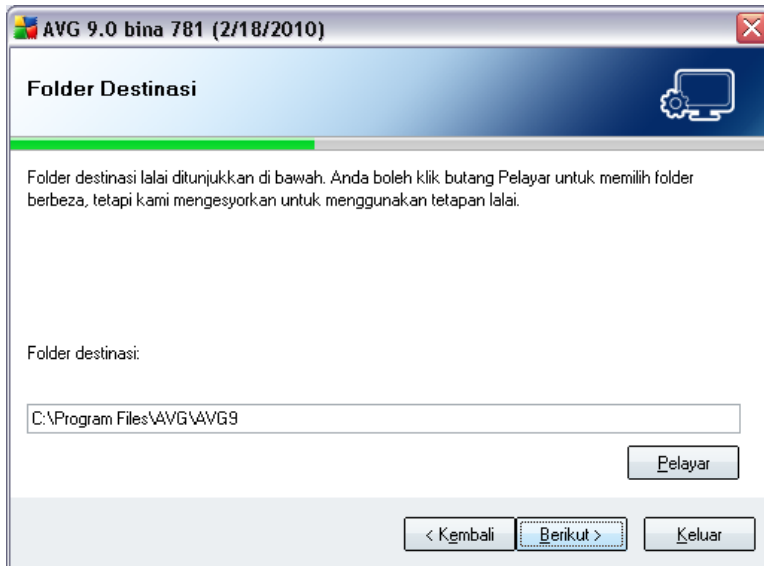
Jika anda telah membeli perisian tersebut dalam kedai peruncitan, anda akan menemui nombor lesen pada kad pendaftaran produk yang termasuk dalam pakej tersebut. Pastikan anda menyalin nombor dengan betul.

< Kembali **Berikut >** Keluar

Tekan butang ***Berikutnya*** untuk meneruskan proses pemasangan.

Jika dalam langkah sebelumnya, anda telah memilih pemasangan standard, anda akan diarahkan semula secara terus ke dialog ***Bar Alat Keselamatan AVG***. Jika pemasangan tersuai dipilih, anda akan meneruskan dengan dialog ***Folder Destinasi***.

5.6. Pemasangan Tersuai - - Folder destinasi

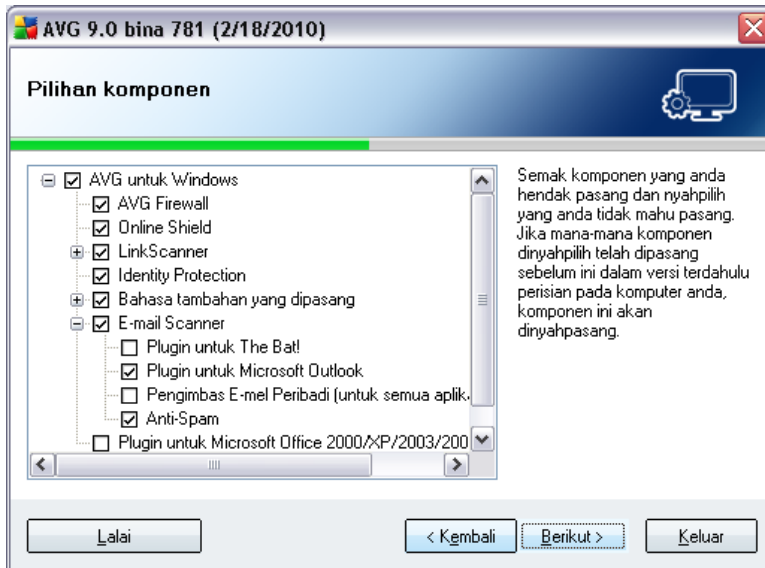


Dialog **Folder Destinasi** membenarkan anda menentukan lokasi di mana **AVG 9 Internet Security** harus dipasang. Secara lalai, AVG akan dipasang ke folder fail atur cara yang terletak pada pemacu C:. Jika folder tidak wujud lagi, anda akan diminta dalam dialog baru untuk mengesahkan anda bersetuju AVG membuat folder ini sekarang.

Jika anda hendak mengubah lokasi ini, gunakan butang **Semak Imbas** untuk memaparkan struktur pemacu dan pilih folder masing-masing.

Tekan butang **Berikutnya** untuk mengesahkan.

5.7. Pemasangan Tersuai - Pemilihan Komponen



Dialog **Pemilihan Komponen** memaparkan gambaran keseluruhan bagi semua komponen **AVG 9 Internet Security** yang boleh dipasang. Jika tetapan lalai tidak sesuai dengan anda, anda boleh membuang/menambah komponen tertentu.

Walau bagaimanapun, anda boleh memilih dari komponen yang termasuk dalam edisi AVG yang dibeli. Hanya komponen tersebut akan ditawarkan untuk dipasang dalam dialog Pemilihan Komponen!

• Pemilihan bahasa

Dalam senarai komponen untuk dipasang, anda boleh mentakrifkan bahasa mana yang AVG harus dipasang. Tandakan item **Bahasa tambahan yang dipasang** dan kemudian, pilih bahasa yang dikehendaki dari menu masing-masing.

• Plug-in Pengimbas E-mel

Klik item **Pengimbas E-mel** untuk membuka dan menentukan plug-in apa yang perlu dipasang untuk menjamin keselamatan mel elektronik. Secara lalai, **Plugin untuk Microsoft Outlook** akan dipasang. Jika anda membeli lesen yang termasuk **AntiSpam**, ia akan dipasang secara automatik. Pilihan khusus lain adalah **Plugin untuk The Bat!** Jika anda menggunakan klien e-mel lain (*MS Exchange, Qualcomm Eudora, ...*), pilih opsi **Pengimbas E-mel Peribadi** untuk melindungi komunikasi e-mel anda secara automatik tidak kira atur cara e-mel apa yang anda jalankan.

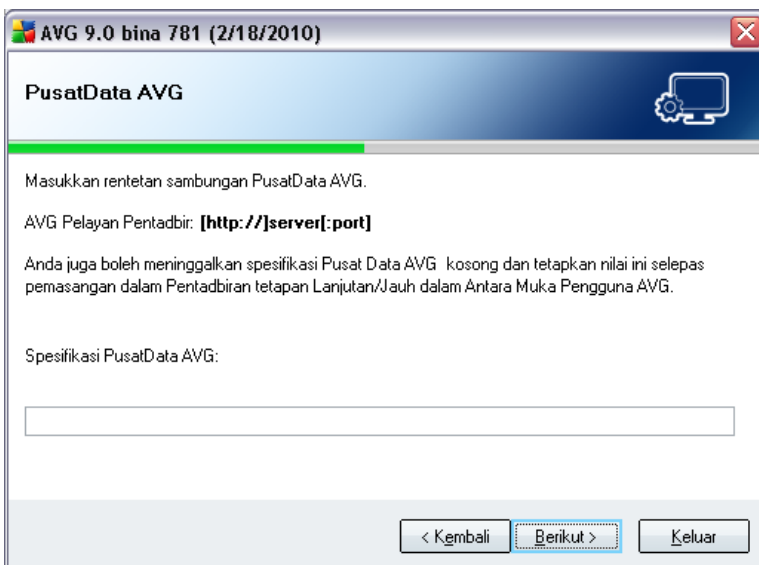
- **Pentadbiran Jauh**

Jika anda merancang untuk menyambungkan komputer anda ke Pentadbiran Jauh AVG kemudian, sila tandakan item masing-masing untuk dipasang juga.

Teruskan dengan menekan butang **Berikutnya** .

5.8. PusatData AVG

Jika menggunakan lesen rangkaian AVG dan jika sebelum ini dialog **Pemasangan Tersuai - Pemilihan Komponen** anda telah tandakan item **Pentadbiran jauh** untuk dipasang, adalah perlu untuk menentukan parameter **AVG DataCenter**:



Dalam medan teks **spesifikasi AVG DataCenter** sila berikan rentetan sambungan kepada **AVG DataCenter** dalam bentuk *pelayan:port*. Jika maklumat tidak tersedia buat sementara waktu, biarkan medan kosong dan anda boleh menetapkan konfigurasi kemudian dalam dialog **Tetapan Lanjutan / Pentadbiran Jauh**.

Nota: Untuk maklumat terperinci mengenai AVG Remote administration, sila rujuk manual pengguna AVG Network Edition; untuk dimuat turun dari tapak web AVG (<http://www.avg.com/>).

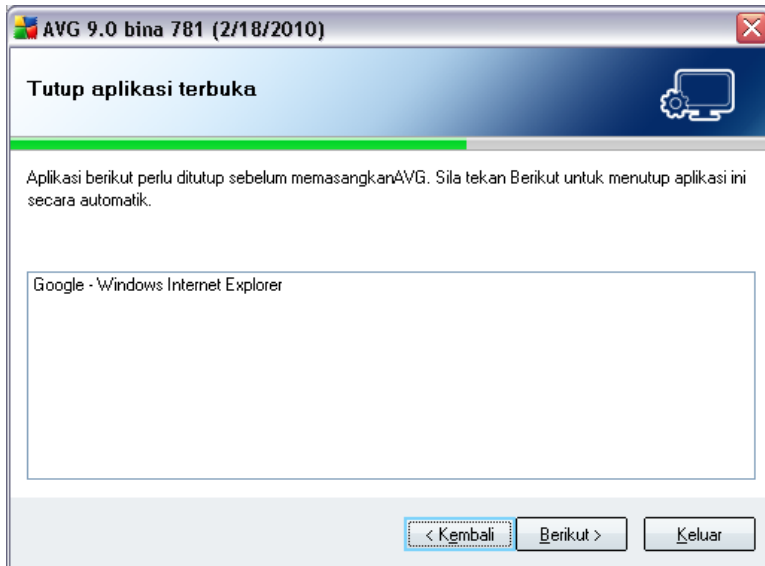
5.9. AVG Security Toolbar



Dalam dialog **AVG Security Toolbar**, tentukan sama ada anda hendak memasang **AVG Security Toolbar** (pengesahan bagi keputusan carian bagi enjin carian Internet yang disokong). Jika anda tidak mengubah tetapan lalai, komponen ini akan dipasang secara automatik ke dalam penyemak imbas Internet anda (penyemak imbas yang disokong buat masa ini adalah Microsoft Internet Explorer v. 6.0 atau lebih tinggi, dan Mozilla Firefox v. 2.0 atau lebih tinggi) untuk memberikan anda perlindungan dalam talian menyeluruh semasa melayari Internet.

Serta, anda mempunyai pilihan untuk memutuskan sama ada anda hendak memilih Yahoo! sebagai pembekal carian lalai anda. Jika sedemikian, sila tandakan kotak semakan masing-masing.

5.10. Tutup aplikasi terbuka



Dialog **Tutup aplikasi terbuka** muncul sewaktu proses pemasangan hanya jika terdapat beberapa atur cara bertembung yang berjalan pada komputer buat masa itu. Kemudian, senarai atur cara yang perlu ditutup untuk berjaya menyelesaikan proses pemasangan akan diberikan. Tekan butang **Seterusnya** untuk mengesahkan bahawa anda bersetuju untuk menutup aplikasi masing-masing dan untuk meneruskan ke langkah seterusnya.

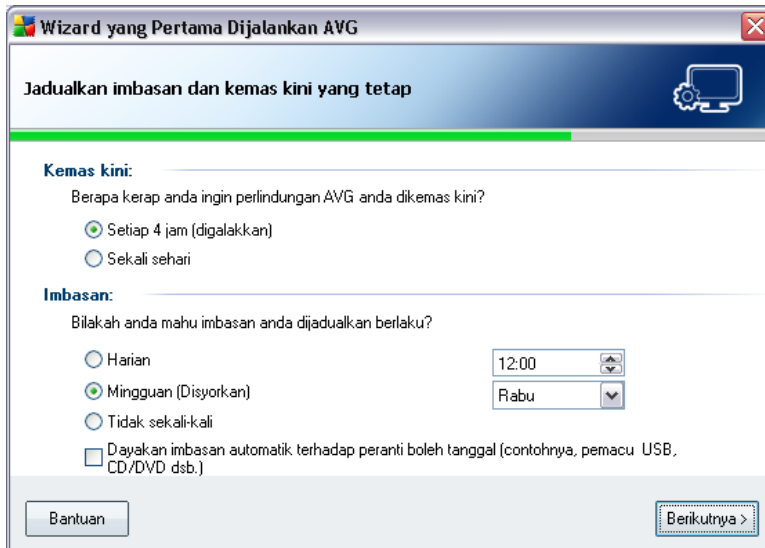
5.11. Memasang AVG

Dialog **Memasang AVG** menunjukkan perkembangan proses pemasangan dan tidak memerlukan sebarang campur tangan:



Selepas proses pemasangan selesai, anda akan diarah semula ke dialog seterusnya secara automatik.

5.12. Jadualkan imbasan dan kemas kini yang tetap



Dalam dialog **Jadualkan imbasan dan kemas kini tetap** sediakan selang untuk semakan akses fail kemas kini baru dan tentukan masa bila [imbasan yang dijadualkan](#) harus dilancarkan. Ia disarankan untuk mengekalkan nilai lalai. Tekan butang **Berikutnya** untuk meneruskan.

5.13. Pemilihan penggunaan komputer



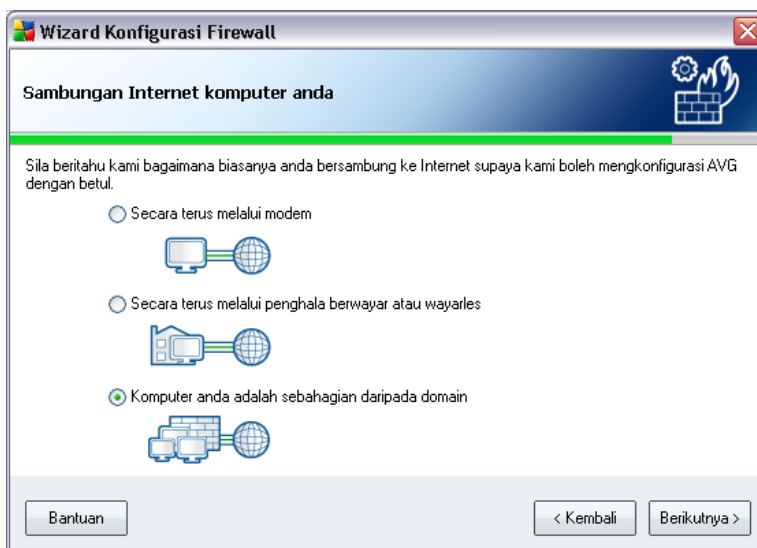
Dalam dialog ini, **Wizard Konfigurasi Firewall** menanyakan jenis komputer yang anda gunakan. Contohnya, komputer bimbit anda yang menyambungkan Internet dari banyak lokasi berbeza (*lapangan terbang, bilik hotel, dll.*) memerlukan peraturan keselamatan yang lebih ketat daripada komputer dalam domain (*rangkaian komputer, dll.*). Berdasarkan pada jenis penggunaan komputer yang dipilih, peraturan lalai **Firewall** akan ditentukan dengan tahap keselamatan berbeza.

Anda mempunyai dua opsi alternatif untuk dipilih daripada:

- **Komputer desktop**
- **Komputer yang boleh dialihkan**

Sahkan pilihan anda dengan menekan butang **Berikutnya** dan teruskan dengan dialog berikutnya.

5.14. Sambungan Internet komputer anda



Dalam dialog ini, **Wizard Konfigurasi Firewall** menanyakan bagaimana komputer anda disambungkan kepada Internet. Berdasarkan pada jenis sambungan yang dipilih, peraturan lalai **Firewall** akan ditentukan dengan tahap keselamatan berbeza.

Anda mempunyai tiga opsi alternatif untuk dipilih daripada:

- **Secara terus melalui modem**

- **Secara terus melalui penghala berwayar atau wayarles**
- **Komputer anda adalah sebahagian daripada domain**

Pilih jenis sambungan yang terbaik menerangkan sambungan komputer anda kepada Internet.

Sahkan pilihan anda dengan menekan butang **Berikutnya** dan teruskan dengan dialog berikutnya.

5.15. Konfigurasi perlindungan AVF selesai



Kini, **AVG 9 Internet Security** telah dikonfigurasi.

Dalam dialog ini, anda putuskan sama ada anda hendak mengaktifkan pilihan tanpa nama melaporkan eksploitasi dan tapak jahat kepada makmal virus AVG. Jika sedemikian, sila tandakan opsyen **Saya bersetuju untuk memberikan maklumat TANPA NAMA mengenai ancaman yang dikesan untuk mempertingkatkan keselamatan saya**.

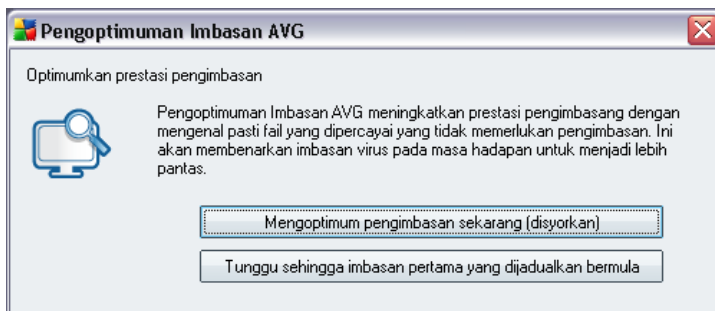
Akhir sekali, tekan butang **Selesai**. Mula semula komputer anda mungkin diperlukan supaya anda boleh mula bekerja dengan AVG.

6. Selepas Pemasangan

6.1. Pengoptimuman imbasan

Pengoptimuman pengimbasan mencari *Windows* dan folder *Atur Cara* di mana ia mengesan fail sesuai (*buat masa ini adalah fail *.exe, *.dll dan *.sys*) dan menyimpan maklumat pada fail ini. Dengan akses seterusnya, fail ini tidak akan diimbas semula dan ini mengurangkan masa pengimbasan secara signifikan.

Sebaik sahaja proses pemasangan tamat, anda akan dijemput melalui tetingkap dialog baru untuk mengoptimumkan imbasan:



Kami mengesyorkan untuk menggunakan pilihan ini dan menjalankan proses pengoptimuman pengimbasan dengan menekan butang ***Optimumkan pengimbasan sekarang***.

6.2. Pendaftaran Produk

Menyelesaikan pemasangan **AVG 9 Internet Security**, sila daftarkan produk anda dalam talian pada tapak web AVG (<http://www.avg.com/>), halaman **Pendaftaran** (*diikuti arahan yang diberikan secara terus dalam halaman*). Selepas pendaftaran, anda boleh mendapatkan akses penuh ke akaun Pengguna AVG anda, surat berita Kemas Kini AVG dan perkhidmatan lain yang disediakan secara eksklusif untuk pengguna yang berdaftar.

6.3. Akses ke Antara Muka Pengguna

Antara Muka Pengguna AVG boleh diakses dalam beberapa cara:

- klik dua kali ikon AVG pada dulang sistem



- klik dua kali ikon AVG pada desktop
- dari menu **Start/ Programs/AVG 9.0/AVG User Interface**

6.4. Mengimbas seluruh komputer

Terdapat kemungkinan risiko bahawa virus komputer telah dihantar ke komputer anda sebelum pemasangan **AVG 9 Internet Security**. Atas sebab itu, anda harus menjalankan [Imbas seluruh komputer](#) untuk memastikan tiada jangkitan pada PC anda.

Untuk arahan bagi menjalankan [Imbas seluruh komputer](#) sila rujuk bab [Pengimbasan AVG](#).

6.5. Ujian Eicar

Untuk mengesahkan bahawa **AVG 9 Internet Security** telah dipasang dengan betul, anda boleh melakukan ujian EICAR.

Ujian EICAR adalah kaedah yang sememangnya selamat digunakan untuk menguji kefungsi sistem antivirus. Ia selamat untuk diagihkan kerana ia bukan virus sebenar dan tidak termasuk sebarang pecahan kod virus. Kebanyakan produk bertindak balas kepadanya seperti ia adalah virus (*walaupun biasanya ia melaporkannya dengan nama yang biasa seperti "EICAR-AV-Test"*). Anda boleh memuat turun virus EICAR dari tapak web EICAR di www.eicar.com, dan anda juga boleh menemui semula maklumat ujian EICAR di situ.

Cuba muat turun fail **eicar.com** dan simpannya pada cakera tempatan anda. Serta-merta selepas anda mengesahkan muat turun fail ujian, [Perisai Dalam Talian](#) akan bertindak balas kepadanya dengan amaran. Notis ini menunjukkan bahawa AVG dipasang dengan betul pada komputer anda.



Dari tapak web <http://www.eicar.com>, anda juga boleh memuat turun versi yang dimampatkan bagi 'virus' EICAR (*cth. dalam bentuk eicar_com.zip*). **Perisai Dalam Talian** membenarkan anda untuk memuat turun fail ini dan menyimpannya pada cakera tempatan anda tetapi, kemudian, **Perisai Residen** mengesan 'virus' apabila anda cuba mengeluarkannya. **Jika AVG gagal mengenal pasti fail ujian EICAR sebagai virus, anda harus menyemak konfigurasi atur cara semula!**

6.6. Konfigurasi Lalai AVG

Konfigurasi lalai (*iaitu bagaimana aplikasi disediakan betul-betul selepas pemasangan*) bagi **AVG 9 Internet Security** disediakan oleh vendor perisian supaya semua komponen dan fungsi ditiun untuk mencapai prestasi optimum.

Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG! Perubahan kepada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja.

Beberapa pengeditan minor bagi tetapan [komponen AVG](#) boleh diakses secara terus daripada antara muka pengguna komponen khusus. Jika anda rasa anda perlu mengubah konfigurasi AVG untuk lebih sesuai dengan keperluan anda, pergi ke **Tetapan Lanjutan AVG**: pilih item menu sistem **tetapan Alat/Lanjutan** dan edit konfigurasi AVG dalam dialog **Tetapan Lanjutan AVG** yang baru dibuka.

7. Antara Muka Pengguna AVG

AVG 9 Internet Security terbuka dengan tettingkap utama:



Tetingkap utama dibahagikan kepada beberapa bahagian:

- **Menu Sistem** (*baris sistem atas dalam tettingkap*) adalah navigasi standard yang membenarkan anda mengakses semua komponen, perkhidmatan dan ciri AVG - [butiran >>](#)
- **Maklumat Status Keselamatan** (*bahagian atas tettingkap*) memberikan anda maklumat pada status semasa bagi atur cara AVG anda - [butiran>>](#)
- **Pautan Pantas** (*bahagian kiri tettingkap*) membenarkan anda untuk mengakses dengan pantas kepada tugas AVG yang paling penting dan paling kerap



digunakan - [butiran >>](#)

- **Gambaran Keseluruhan Komponen** (*bahagian tengah tetingkap*) menawarkan gambaran keseluruhan komponen AVG yang dipasang - [butiran >>](#)
- **Statistik** (*bahagian bawah kiri tetingkap*) memberikan anda semua data statistik berkenaan operasi atur cara - [butiran >>](#)
- **Ikon Dulang Sistem** (*penjuru kanan bawah monitor, pada dulang sistem*) menunjukkan status semasa AVG - [butiran >>](#)

7.1. Menu Sistem

Menu sistem adalah navigasi standard yang digunakan dalam semua aplikasi Windows. Ia terletak secara mendatar pada bahagian paling atas bagi tetingkap utama **AVG 9 Internet Security**. Gunakan menu sistem untuk mengakses komponen, ciri dan perkhidmatan AVG tertentu.

Menu sistem dibahagikan dalam lima bahagian utama:

7.1.1. Fail

- **Keluar** - menutup antara muka pengguna **AVG 9 Internet Security**. Walau bagaimanapun, aplikasi AVG akan terus dijalankan di latar belakang dan komputer anda masih akan dilindungi!

7.1.2. Komponen

Item **Komponen** bagi menu sistem memasukkan pautan kepada semua komponen AVG yang dipasang, membuka halaman dialog lalainya dalam antara muka pengguna:

- **Gambaran keseluruhan sistem** - beralih ke dialog antara muka pengguna lalai dengan [gambaran keseluruhan semua komponen yang dipasang dan statusnya](#)
- **AntiVirus** - membuka halaman lalai bagi komponen [AntiVirus](#)
- **Anti-Rootkit** - membuka halaman lalai bagi komponen [Anti-Rootkit](#)
- **AntiPerisian Pengintip** - membuka halaman lalai bagi komponen [AntiPerisian Pengintip](#)
- **Firewall** - membuka halaman lalai bagi komponen [Firewall](#)
- **Pengimbas Pautan** - membuka halaman lalai bagi komponen [Pengimbas Pautan](#)

- **Alat Sistem** - membuka halaman lalai bagi [Alat Sistem](#)
- **Anti-Spam** - membuka halaman lalai bagi komponen [Anti-Spam](#)
- **Pengimbas E-mel** - membuka halaman lalai bagi komponen [Pengimbas E-mel](#)
- **Perlindungan ID** - membuka halaman lalai bagi komponen [Perlindungan ID](#)
- **Lesen** - membuka halaman lalai bagi komponen [Lesen](#)
- **Perisai Dalam Talian** - membuka halaman lalai bagi komponen [Perisai Dalam Talian](#)
- **Perisai Residen** - membuka halaman lalai bagi komponen [Perisai Residen](#)
- **Pengurus Kemas Kini** - membuka halaman lalai bagi komponen [Pengurus Kemas Kini](#)

7.1.3. Sejarah

- **Imbas keputusan** - beralih ke antara muka pengujian AVG, secara khusus kepada dialog [Gambaran Keseluruhan Keputusan Imbasan](#)
- **Pengesanan Perisai Residen** - membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh [Perisai Residen](#)
- **Pengesanan Pengimbas E-mel** - membuka dialog dengan gambaran keseluruhan lampiran mesej mel yang dikesan sebagai berbahaya oleh komponen [Pengimbas E-mel](#)
- **Penemuan Perisai Dalam Talian** - membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh [Perisai Dalam Talian](#)
- **Bilik Kebal Virus** - membuka antara muka ruang kuarantin ([Bilik Kebal Virus](#)) ke mana AVG membuang semua jangkitan yang dikesan yang tidak boleh dipulihkan secara automatik atas sebab tertentu. Di dalam kuarantin ini, fail yang dijangkiti dipencilkan dan keselamatan komputer dijamin dan pada masa yang sama, fail yang dijangkiti disimpan untuk kemungkinan pembaikan di masa hadapan.
- **Log Sejarah Acara** - membuka antara muka log sejarah dengan gambaran keseluruhan bagi semua tindakan **AVG 9 Internet Security** yang dilog.
- **Firewall** - membuka antara muka tetapan Firewall pada tab [Log](#) tab dengan gambaran keseluruhan semua tindakan Firewall

7.1.4. Alat

- **Imbas komputer** - mengalihkan ke [antara muka imbasan AVG](#) dan melancarkan imbasan seluruh komputer
- **Imbas folder yang dipilih** - mengalihkan ke [antara muka pengimbasan AVG](#) dan membenarkan anda mentakrif dalam struktur pepohon komputer anda bagi fail dan folder masa yang harus diimbas
- **Imbas fail** - membenarkan anda menjalankan ujian dengan permintaan pada fail tunggal yang dipilih daripada struktur pepohon bagi cakera anda
- **Kemas kini** - melancarkan proses kemas kini secara automatik **AVG 9 Internet Security**
- **Kemas kini dari direktori** - menjalankan proses kemas kini dari fail kemas kini yang terletak dalam folder tertentu pada cakera tempatan anda. Walau bagaimanapun, opsyen ini hanya disyorkan sebagai kecemasan, cth. dalam situasi di mana tiada sambungan Internet (*contohnya, komputer anda dijangkiti dan dinyahsambung dari Internet; komputer anda disambungkan ke rangkaian dengan tiada akses kepada Internet, dll.*). Dalam tettingkap yang baru dibuka, pilih folder di mana anda telah meletakkan fail kemas kini sebelum ini dan melancarkan proses kemas kini.
- **Tetapan lanjutan** - membuka dialog **tetapan lanjutan AVG** di mana anda boleh mengedit konfigurasi **AVG 9 Internet Security**. Secara umum, ia disyorkan untuk mengekalkan tetapan lalai bagi aplikasi seperti yang ditakrifkan oleh vendor perisian.
- **Tetapan Firewall** - membuka dialog tersendiri untuk konfigurasi lanjutan bagi komponen **Firewall**

7.1.5. Bantuan

- **Kandungan** - membuka fail bantuan AVG
- **Dapatkan Bantuan Dalam Talian** - membuka tapak web AVG (<http://www.avg.com/>) di halaman pusat sokongan pelanggan
- **Web AVG anda** - membuka tapak web AVG (<http://www.avg.com/>)
- **Mengenai Virus dan Ancaman** - membuka **Ensiklopedia Virus** dalam talian di mana anda boleh mendapatkan maklumat terperinci mengenai virus yang dikenal pasti

- **Aktifkan semula** - membuka dialog **Aktifkan AVG** dengan data yang anda telah masukkan dalam dialog **Peribadikan AVG** bagi proses pemasangan. Dalam dialog ini, anda boleh memasukkan nombor lesen anda dengan sama ada menggantikan nombor jualan (*nombor yang anda telah pasangkan AVG*), atau untuk menggantikan nombor lesen lama (*cth. semasa menaik taraf ke produk AVG baru*).
- **Daftar sekarang** - menyambung kepada halaman pendaftaran bagi tapak web AVG (<http://www.avg.com/>). Sila isikan data pendaftaran anda; hanya pelanggan yang mendaftarkan produk AVG mereka boleh menerima sokongan teknikal percuma.

Perhatian: Jika menggunakan versi percubaan **AVG 9 Internet Security**, dua item kedua muncul sebagai **Beli sekarang** dan **Aktifkan**, membenarkan anda membeli versi penuh atur cara dengan serta-merta. Untuk **AVG 9 Internet Security** yang dipasang dengan nombor jualan, item dipaparkan sebagai **Daftar** dan **Aktifkan**. Untuk maklumat lanjut, sila rujuk bahagian Lesen bagi dokumentasi ini.

- **Mengenai AVG** - membuka dialog **Maklumat** dengan lima tab memberikan data pada nama atur cara, atur cara dan versi pangkalan data virus, maklumat sistem, perjanjian lesen dan maklumat hubungan bagi **AVG Technologies CZ**.

7.2. Maklumat Status Keselamatan

Bahagian **Maklumat Status Keselamatan** terletak di bahagian atas tettingkap utama AVG. Dalam bahagian ini, anda akan sentiasa mendapatkan maklumat mengenai status keselamatan terkini bagi **AVG 9 Internet Security** anda. Sila lihat gambaran keseluruhan ikon yang berkemungkinan bertindih dalam bahagian ini dan maksudnya:



Ikon hijau menunjukkan bahawa AVG anda berfungsi sepenuhnya. Komputer anda dilindungi sepenuhnya, terkini dan semua komponen dipasang berfungsi dengan betul.



Ikon jingga memberi amaran bahawa satu atau lebih komponen dikonfigurasi dengan salah dan anda harus memberi perhatian kepada sifat/tetapannya. Tiada masalah kritikal dalam AVG dan anda berkemungkinan telah memutuskan untuk mematikan beberapa komponen atas sebab tertentu. Anda masih dilindungi oleh AVG. Walau bagaimanapun, sila berikan perhatian kepada masalah tetapan komponen! Namanya akan diberikan dalam bahagian **Maklumat Status Keselamatan**.

Ikon ini juga muncul jika atas beberapa sebab anda telah memutuskan untuk [mengabaikan status ralat komponen](#) (pilihan "Abaikan keadaan komponen" tersedia dari menu konteks yang dibuka dengan mengklik kanan pada ikon komponen masing-masing dalam gambaran keseluruhan komponen bagi tettingkap utama AVG). Anda mungkin perlu menggunakan opsi ini dalam situasi tertentu tetapi amat disyorkan untuk mematikan opsi "Abaikan keadaan komponen" secepat mungkin.



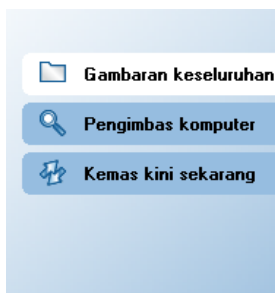
Ikon merah menunjukkan bahawa AVG berada dalam status kritikal ! Satu atau lebih komponen tidak berfungsi dengan betul dan AVG tidak dapat melindungi komputer anda. Sila berikan perhatian serta-merta untuk menyelesaikan masalah yang dilaporkan. Jika anda tidak dapat membetulkan ralat dengan sendiri, hubungi pasukan [sokongan teknikal AVG](#).

Adalah amat disyorkan supaya anda memberikan perhatian kepada Maklumat Status Keselamatan dan jika laporan menunjukkan sebarang masalah, teruskan dan cuba menyelesaikannya dengan serta-merta. Jika tidak, komputer anda berisiko!

Nota: maklumat status AVG boleh diperoleh pada bila-bila masa dari [ikon dulang sistem](#).

7.3. Pautan Pantas

Pautan pantas (dalam bahagian sebelah kiri [Antara Muka Pengguna AVG](#)) membenarkan anda untuk mengakses ciri AVG yang paling penting dan paling kerap digunakan:



- **Gambaran keseluruhan** - gunakan pautan ini untuk beralih dari sebarang antara muka AVG yang sedang terbuka ke lalai dengan gambaran keseluruhan semua komponen yang dipasang - lihat bab [Gambaran Keseluruhan Komponen >>](#)

- **Pengimbas komputer** - gunakan pautan ini untuk membuka antara muka pengimbasan AVG di mana anda boleh menjalankan ujian secara terus, menjadualkan imbasan atau mengedit parameter mereka - lihat bab [Pengimbasan AVG >>](#)
- **Kemas kini sekarang** - pautan ini membuka kemas kini antara muka dan melancarkan proses kemas kini AVG dengan serta-merta - lihat bab [Kemas Kini AVG >>](#)

Pautan ini boleh diakses dari antara muka pengguna pada setiap masa. Apabila anda menggunakan pautan pantas untuk menjalankan proses tertentu, GUI akan beralih ke dialog baru tetapi pautan pantas masih tersedia. Tambahan pula, proses yang sedang dijalankan selanjutnya digambarkan secara grafik.

7.4. Gambaran keseluruhan Komponen

Bahagian **Gambaran Keseluruhan Komponen** terletak di bahagian tengah [Antara Muka Pengguna AVG](#). Bahagian tersebut dibahagikan kepada dua bahagian:

- Gambaran keseluruhan bagi komponen yang dipasang terdiri daripada panel dengan ikon komponen dan maklumat sama ada komponen masing-masing adalah aktif atau tidak aktif
- Penerangan bagi komponen yang dipilih

Dalam **AVG 9 Internet Security** bahagian **Gambaran Keseluruhan Komponen** mengandungi maklumat mengenai komponen berikut:

- **AntiVirus** memastikan komputer anda dilindungi daripada virus yang cuba memasuki komputer anda- [butiran >>](#)
- **AntiPerisian Pengintip** mengimbas aplikasi anda di latar belakang daripada virus yang cuba memasuki komputer anda - [butiran >>](#)
- **AntiSpam** memeriksa semua mesej masuk dan menandakan e-mel yang tidak diingini sebagai SPAM - [butiran >>](#)
- **Firewall** mengawal bagaimana komputer anda menukar data dengan komputer lain pada Internet atau rangkaian tempatan- [butiran >>](#)
- **Pengimbas Pautan** memeriksa keputusan carian yang dipaparkan dalam pelayar internet anda - [butiran >>](#)
- **AntiRootkit** mengesan atur cara dan teknologi yang cuba menyamar malware

- [butiran >>](#)

- **Alat Sistem** menawarkan ringkasan terperinci bagi persekitaran AVG dan maklumat sistem pengendalian - [butiran >>](#)
- **Pengimbas E-mel** memeriksa semua mel masuk dan keluar bagi virus - [butiran >>](#)
- **Perlindungan ID** - komponen antimalware memberi fokus pada pencegahan pencuri identiti daripada mencuri barang digital peribadi anda yang bernilai - [butiran >>](#)
- **Lesen** memaparkan nombor lesen, jenis dan tarikh tamat tempoh - [butiran >>](#)
- **Perisai Dalam Talian** mengimbas semua data yang dimuat turun oleh penyemak imbas web - [butiran >>](#)
- **Perisai Residen** berjalan di latar belakang dan mengimbas fail semasa ia disalin, dibuka atau disimpan - [butiran >>](#)
- **Pengurus Kemas Kini** mengawal semua kemas kini AVG - [butiran >>](#)

Klik sekali pada mana-mana ikon komponen untuk menyerlahkannya dalam gambaran keseluruhan komponen. Dalam masa yang sama, penerangan kefungsi asas komponen muncul di bahagian bawah antara muka pengguna. Klik dua kali pada ikon untuk membuka antara muka komponen itu sendiri dengan senarai data statistik asas.

Klik kanan tetikus anda pada ikon komponen untuk mengembangkan menu konteks: selain daripada membuka antara muka grafik komponen, anda juga boleh memilih untuk **Abai keadaan komponen**. Pilih pilihan ini untuk menyatakan bahawa anda menyedari [keadaan ralat komponen](#) tetapi atas sebab tertentu anda hendak mengekalkan AVG anda seperti itu dan tidak mahu diberi amaran oleh [ikon dulang sistem](#).

7.5. Statistik

Bahagian **Statistik** terletak di bahagian bawah [Antara Muka Pengguna AVG](#). Ia menawarkan senarai maklumat berkenaan operasi atur cara:

- **Imbasan terakhir** - memberikan tarikh bila imbasan terakhir dilakukan
- **Kemas kini terakhir** - memberikan tarikh bila kemas kini terakhir dilancarkan
- **Virus DB** - memberitahu anda mengenai versi yang baru dipasang bagi pangkalan data virus



- **Versi LS** - memberitahu anda mengenai versi AVG yang dipasang (*nombor adalah dalam bentuk 9.0.xx, di mana 9.0 adalah versi baris produk dan xx adalah untuk nombor binaan*)
- **Lesen tamat tempoh** - memberikan tarikh tamat tempoh lesen AVG anda

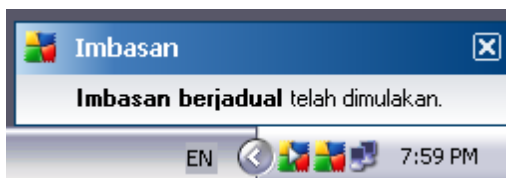
7.6. Ikon Dulang Sistem

Ikon Dulang Sistem (pada bar tugas Windows anda) menunjukkan status terkini bagi **AVG 9 Internet Security** anda. Ia boleh dilihat setiap masa ada dulang sistem anda, tidak kira sama ada tettingkap utama AVG anda dibuka atau ditutup.

Jika dalam warna penuh , **Ikon Dulang Sistem** menunjukkan bahawa semua komponen AVG adalah aktif dan berfungsi sepenuhnya. Serta, ikon dulang sistem boleh dipaparkan dalam warna penuh jika AVG berada dalam keadaan ralat tetapi anda betul-betul menyedari mengenai situasi ini dan memutuskan dengan segera untuk [Abaikan keadaan komponen](#).

Ikon dengan tanda seru  menunjukkan masalah (*komponen tidak aktif, status ralat, dll.*). Klik dua kali pada **Ikon Dulang Sistem** untuk membuka tettingkap utama dan mengedit komponen.

Ikon dulang sistem seterusnya memberitahu mengenai aktiviti AVG dan kemungkinan perubahan status dalam atur cara (*cth, pelancaran automatik bagi imbasan atau kemas kini yang dijadualkan, Peralihan profil firewall perubahan status komponen, perulangan status ralat, ...*) melalui tettingkap pop timbul yang dibuka dari ikon dulang sistem AVG:



Ikon Dulang Sistem juga boleh digunakan sebagai pautan pantas untuk mengakses tettingkap utama AVG pada bila-bila masa - klik dua kali pada ikon. Dengan mengklik kanan pada **Ikon Dulang Sistem** anda membuka menu konteks ringkas dengan opsi berikut:

- **Buka Antara Muka Pengguna AVG** - klik untuk membuka [Antara Muka Pengguna AVG](#)
- **Kemas Kini** - melancarkan kemas kini [segera](#)



8. Komponen AVG

8.1. AntiVirus

8.1.1. Prinsip AntiVirus

Enjin pengimbasan perisian antivirus mengimbas semua fail dan aktiviti fail (membuka/ menutup fail, dll.) bagi virus yang diketahui. Sebarang virus yang dikesan akan disekat daripada melakukan sebarang tindakan dan kemudian, akan dibersihkan atau dikuarantin. Kebanyakan perisian antivirus juga menggunakan pengimbasan heuristik di mana fail diimbas untuk ciri virus biasa yang dipanggil tandatangan virus. Ini bermaksud bahawa pengimbas antivirus boleh mengesan virus yang baru dan tidak diketahui jika virus baru yang mengandungi beberapa ciri biasa bagi virus sedia ada.

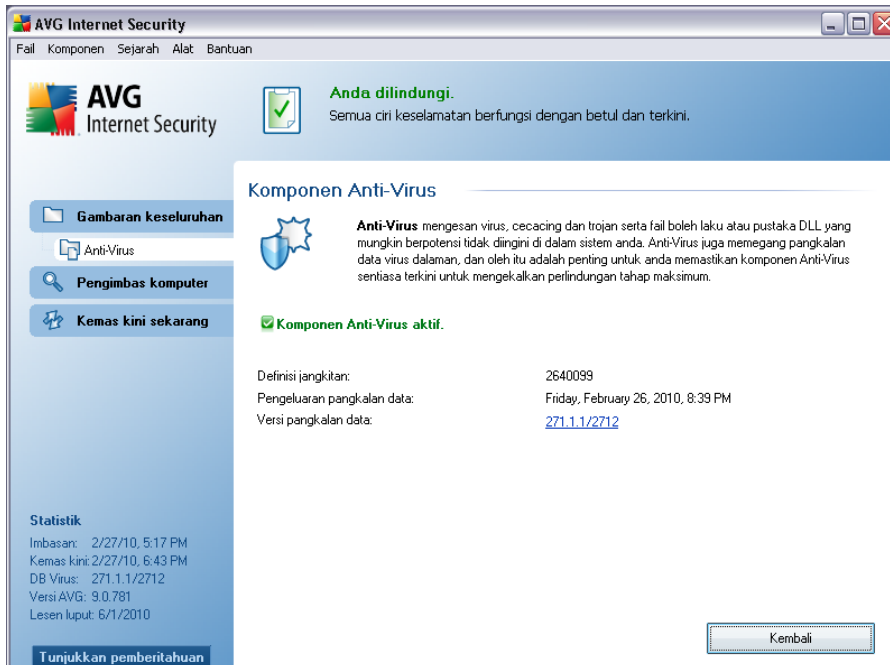
Ciri penting bagi perlindungan antivirus adalah tiada virus yang diketahui boleh dijalankan pada komputer!

Di mana hanya satu teknologi tunggal boleh kekurangan pengesanan atau pengenalpastian virus, **AntiVirus** menggabungkan beberapa teknologi untuk memastikan komputer anda dilindungi daripada virus:

- Pengimbasan - mencari rentetan aksara yang merupakan ciri bagi virus tertentu
- Analisis Heuristik - perlagakan dinamik objek yang diimbas' arahan dalam persekitaran komputer maya
- Pengesanan generik - pengesanan arahan ciri bagi virus/kumpulan virus yang ditetapkan

AVG juga boleh menganalisis dan mengesan aplikasi boleh laku atau pustaka DLL yang berpotensi tidak dikehendaki dalam sistem. Kami memanggil ancaman seperti ini sebagai Atur Cara Yang Berkemungkinan Tidak Diperlukan (pelbagai jenis perisian pengintip, adware, dsb.). Tambahan pula, AVG mengimbas pendaftaran sistem anda bagi entri yang mencurigakan, fail Internet sementara dan kuki penjejakan dan membolehkan anda memperlakukan semua item berpotensi berbahaya dengan cara yang sama seperti sebarang jangkitan lain.

8.1.2. Antara Muka AntiVirus



Antara muka komponen **AntiVirus** memberikan beberapa maklumat asas mengenai kefungsiannya, maklumat pada status semasa komponen (*komponen AntiVirus adalah aktif.*), dan gambaran keseluruhan ringkas statistik **AntiVirus** :

- **Definisi jangkitan** - bilangan memberikan kiraan virus yang ditakrifkan dalam versi terkini pangkalan data virus
- **Kemas kini pangkalan data terkini** - menentukan bila dan pada masa bila pangkalan data kali terakhir dikemas kini
- **Versi pangkalan data** - mentakrifkan bilangan versi pangkalan data virus terkini; dan nombor ini meningkat dengan setiap kemas kini asas virus

Terdapat hanya satu butang operasi yang tersedia dalam antara muka komponen ini (**Undur**) - tekan butang tersebut untuk kembali ke [antara muka pengguna AVG](#) (gambaran keseluruhan komponen).

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu



*mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetap lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.*

8.2. AntiPerisian Pengintip

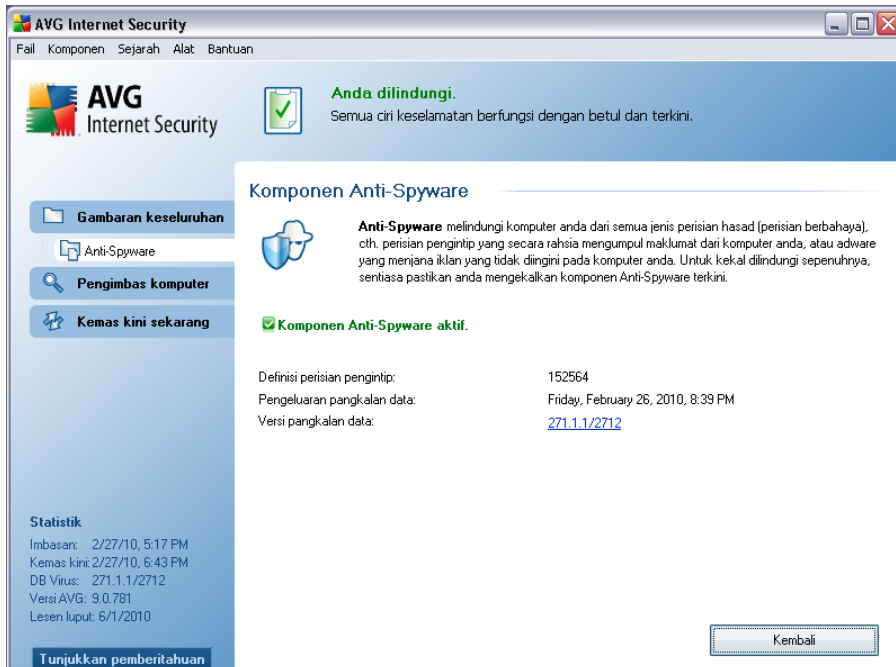
8.2.1. Prinsip AntiPerisian Pengintip

Perisian pengintip biasanya ditakrifkan sebagai sejenis malware, cth. perisian yang mengumpulkan maklumat dari komputer pengguna tanpa pengetahuan atau persetujuan pengguna. Sesetengah aplikasi perisian pengintip juga boleh dipasang secara tidak sengaja dan biasanya mengandungi iklan, pop muncul tettingkap atau perisian berlainan jenis yang tidak disenangi.

Pada masa ini, sumber jangkitan yang paling lazim adalah laman web yang mempunyai kandungan yang mungkin berbahaya. Kaedah pemindahan lain seperti melalui e-mel atau pemindahan melalui cecacing dan virus juga tersebar luas. Perlindungan paling penting adalah untuk menggunakan pengimbas di latar belakang yang sentiasa dipasang, **AntiPerisian Pengintip**, yang berfungsi seperti perisai residen dan mengimbas aplikasi anda di latar belakang apabila anda menjalankannya.

Terdapat juga kemungkinan risiko yang malware telah dihantar ke komputer anda sebelum pemasangan AVG atau anda telah mengabaikan untuk memastikan **AVG 9 Internet Security** anda terkini dengan [pangkalan data dan kemas kini atur cara terkini](#). Atas sebab ini, AVG membolehkan anda mengimbas komputer anda sepenuhnya untuk menapis malware/perisian pengintip dengan menggunakan ciri pengimbasan. Ia juga mengesan malware yang tidur dan tidak aktif, cth. malware yang telah dimuat turun tetapi belum lagi diaktifkan.

8.2.2. Antara Muka AntiPerisian Pengintip



Antara muka komponen **AntiPerisian Pengintip** memberikan gambaran keseluruhan yang ringkas mengenai kefungsiian komponen, maklumat pada status terkini komponen (komponen **AntiPerisian Pengintip** adalah aktif.), dan beberapa statistik **AntiPerisian Pengintip** :

- **Definisi perisian pengintip** - bilangan memberikan kiraan sampel perisian pengintip yang ditakrifkan dalam versi pangkalan data perisian pengintip terkini
- **Kemas kini pangkalan data terkini** - menentukan bila dan pada masa bila pangkalan data perisian pengintip dikemas kini
- **Versi pangkalan data terkini** - menentukan bilangan versi pangkalan data perisian pengintip terkini; dan nombor ini meningkat dengan setiap kemas kini pangkalan virus

Terdapat hanya satu butang operasi yang tersedia dalam antara muka komponen ini (**Undur**) - tekan butang tersebut untuk kembali ke [antara muka pengguna AVG](#) (gambaran keseluruhan komponen).

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk

melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

8.3. AntiSpam

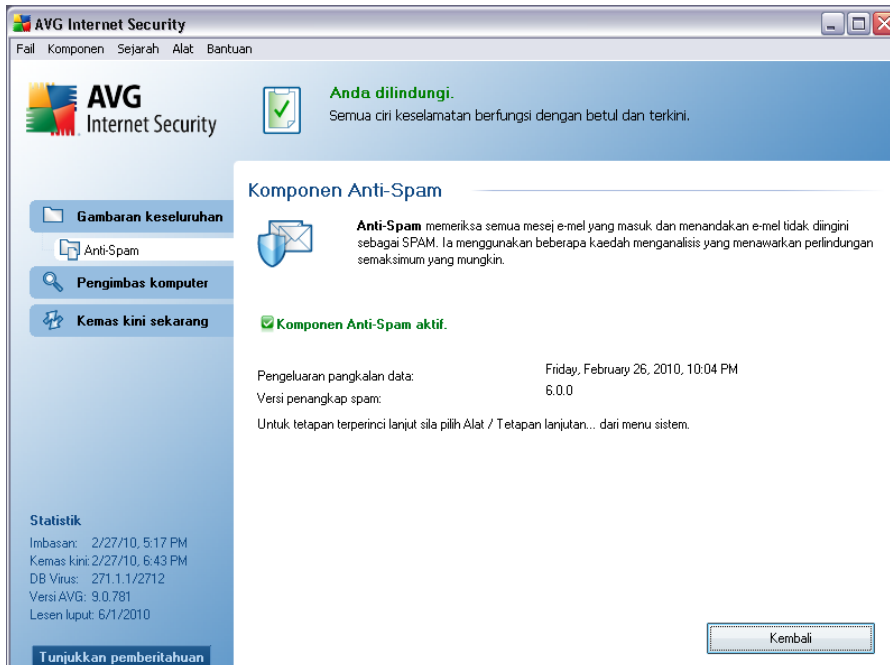
Spam merujuk kepada e-mel yang tidak diminta, kebanyakannya mengiklankan produk atau perkhidmatan yang dimel dengan banyak kepada sebilangan besar alamat e-mel pada satu masa, mengisi kotak mel' penerima. Spam tidak merujuk kepada e-mel komersial sah yang mana telah mendapat kebenaran pengguna. Spam bukan sahaja mengganggu, tetapi juga selalunya adalah sumber penipuan, virus dan kandungan mengganggu.

8.3.1. Prinsip AntiSpam

AVG Anti-spam memeriksa semua mesej e-mel masuk dan menandakan e-mel yang tidak diingini sebagai SPAM. **AVG Anti-Spam** boleh mengubah suai subjek e-mel (*yang telah dikenal pasti sebagai spam*) dengan menambah rentetan teks khas. Kemudian, anda boleh menapis e-mel anda dalam klien e-mel anda dengan mudah.

AVG Anti-Spam komponen menggunakan beberapa kaedah analisis untuk memproses setiap mesej e-mel, menawarkan kemungkinan perlindungan maksimum terhadap mesej e-mel. **AVG Anti-Spam** menggunakan pangkalan data yang biasa dikemas kini untuk pengesanan spam. Adalah berkemungkinan untuk menggunakan pangkalan data umum [pelayan RBL](#) (*bagi alamat e-mel "spammer diketahui"*) dan untuk menambah alamat e-mel secara manual ke [Senarai Putih](#) anda (*jangan tandakan sebagai spam*) dan [Senarai Hitam](#) (*sentiasa tandakan sebagai spam*).

8.3.2. Antara Muka AntiSpam



Dalam dialog komponen **AntiSpam** anda akan menemui teks ringkas yang menerangkan kefungsiian komponen, maklumat pada status terkini (*komponen AntiSpam masih aktif.*), dan statistik berikut:

- **Pengeluaran pangkalan data** - menentukan bila dan dalam masa bila pangkalan data spam dikemas kini dan diterbitkan.
- **Versi penangkap spam** - menentukan bilangan versi terkini bagi enjin antispam

Terdapat hanya satu butang operasi yang tersedia dalam antara muka komponen ini (**Undur**) - tekan butang untuk kembali ke [antara muka pengguna AVG](#) lalai (*gambaran keseluruhan komponen*).

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

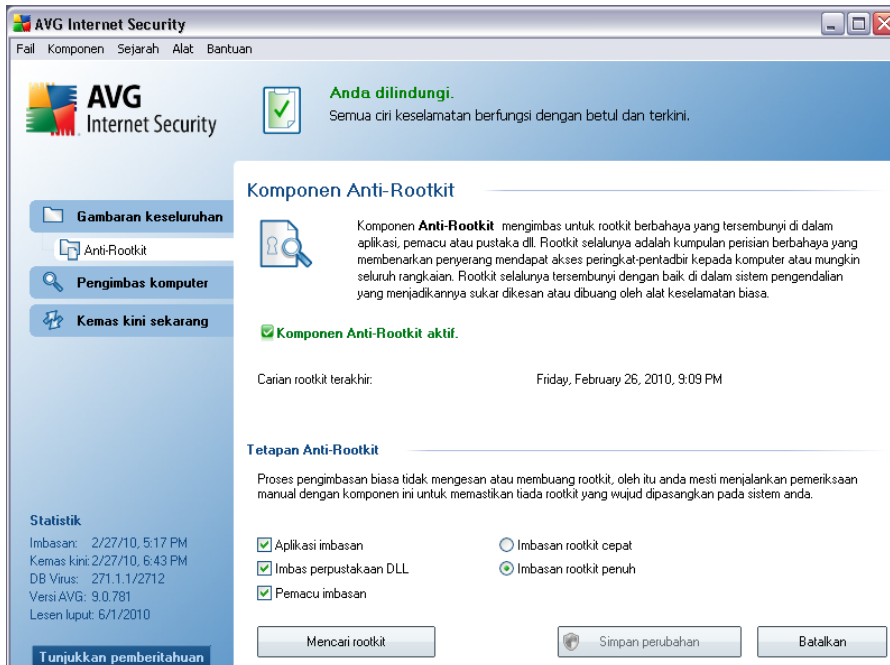
8.4. AntiRootkit

Rootkit adalah atur cara yang direka bentuk untuk melakukan kawalan asas sistem komputer tanpa kebenaran daripada pemilik sistem dan pengurus yang sah. Akses kepada perkakasan jarang diperlukan kerana rootkit bertujuan untuk menyita kawalan sistem pengendalian yang sedang dijalankan pada perkakasan. Biasanya, rootkit bertindak untuk mengaburi kehadirannya pada sistem melalui subversi atau pengelakan daripada mekanisme keselamatan sistem pengendalian. Biasanya, ia juga adalah Trojan, dengan itu, menipu pengguna dengan mempercayai bahawa ia selamat untuk dijalankan pada sistemnya. Teknik yang digunakan untuk melaksanakan ini termasuk menyembunyikan proses yang sedang dijalankan daripada menyelia atur cara atau menyembunyikan fail atau data sistem daripada sistem pengendalian.

8.4.1. Prinsip AntiRootkit

AVG Anti-Rootkit adalah alat khusus untuk mengesan dan membuang rootkit yang berbahaya secara berkesan, cth. atur cara dan teknologi yang boleh menyamar kehadiran perisian berniat jahat pada komputer anda. **AVG Anti-Rootkit** boleh mengesan rootkit berdasarkan pada set peraturan yang dipratakaktif. Sila maklum bahawa semua rootkit dikesan (*bukan hanya* yang dijangkiti). Jika **AVG Anti-Rootkit** menemui rootkit, ia tidak semestinya bermaksud bahawa rootkit dijangkiti. Kadangkala, rootkit digunakan sebagai pemacu atau ia adalah sebahagian daripada aplikasi yang betul.

8.4.2. Antara Muka AntiRootkit



Antara muka **AntiRootkit** memberikan penerangan ringkas mengenai kefungsiian komponen, memberitahu status terkini komponen (*Komponen Anti-Rootkit aktif.*) dan juga memberikan maklumat mengenai kali terakhir ujian **AntiRootkit** dilancarkan.

Pada bahagian bawah dialog, anda boleh dapati bahagian **tetapan AntiRootkit** di mana anda boleh menyediakan beberapa fungsi permulaan bagi pengimbasan kehadiran rootkit. Pertama sekali, tandakan kotak semak masing-masing untuk menentukan objek yang harus diimbas:

- **Aplikasi imbasan**
- **Imbas pustaka DLL**
- **Pemacu imbasan**

Seterusnya, anda boleh memilih mod pengimbasan rootkit:

- **Imbasan rootkit cepat** - mengimbas semua proses berjalan, pemacu yang dimuatkan dan folder sistem (*biasanya, c:\Windows*)
- **Imbasan rootkit penuh** - mengimbas semua proses berjalan, pemacu yang



dimuatkan, folder sistem (*biasanya, c:\Windows*), campur semua cakera tempatan (*termasuk cakera denyar tetapi tidak termasuk cakera liut/pemacu CD*)

Butang kawalan tersedia:

- **Cari rootkit** - memandangkan imbasan rootkit bukan bahagian tersirat bagi [Imbasan seluruh komputer](#), anda boleh menjalankan imbasan rootkit secara terus dari antara muka **AntiRootkit** menggunakan butang ini
- **Simpan perubahan** - tekan butang ini untuk menyimpan semua perubahan yang dibuat dalam antara muka ini dan untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen)
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen) tanpa menyimpan sebarang perubahan yang anda telah lakukan

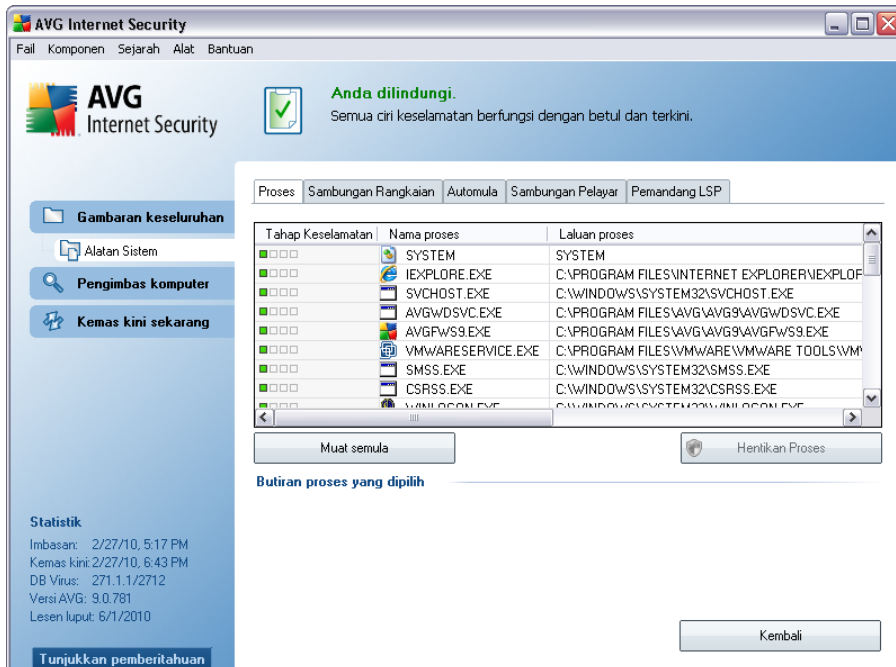
8.5. Alatan Sistem

Alat Sistem merujuk kepada alat yang menawarkan ringkasan terperinci bagi persekitaran dan sistem pengendalian **AVG 9 Internet Security**. Komponen memaparkan gambaran keseluruhan bagi:

- [Proses](#) - senarai proses (cth. pelaksanaan aplikasi) yang sedang aktif pada komputer anda
- [Sambungan rangkaian](#) - senarai sambungan yang sedang aktif
- [Automula](#) - senarai semua aplikasi yang dilakukan sewaktu permulaan sistem Windows
- [Sambungan Pelayar](#) - senarai plug-in (cth. aplikasi) yang dipasang di dalam pelayar Internet
- [Pemerhati LSP](#) - senarai Pembekal Khidmat Berlapis (LSP)

Gambaran keseluruhan khusus boleh diedit tetapi ini hanya disyorkan untuk pengguna yang sangat berpengalaman!

8.5.1. Proses



Dialog **Proses** mengandungi senarai proses (*cth. aplikasi yang dijalankan*) yang sedang aktif pada komputer anda. Senarai tersebut dibahagikan kepada beberapa kolom:

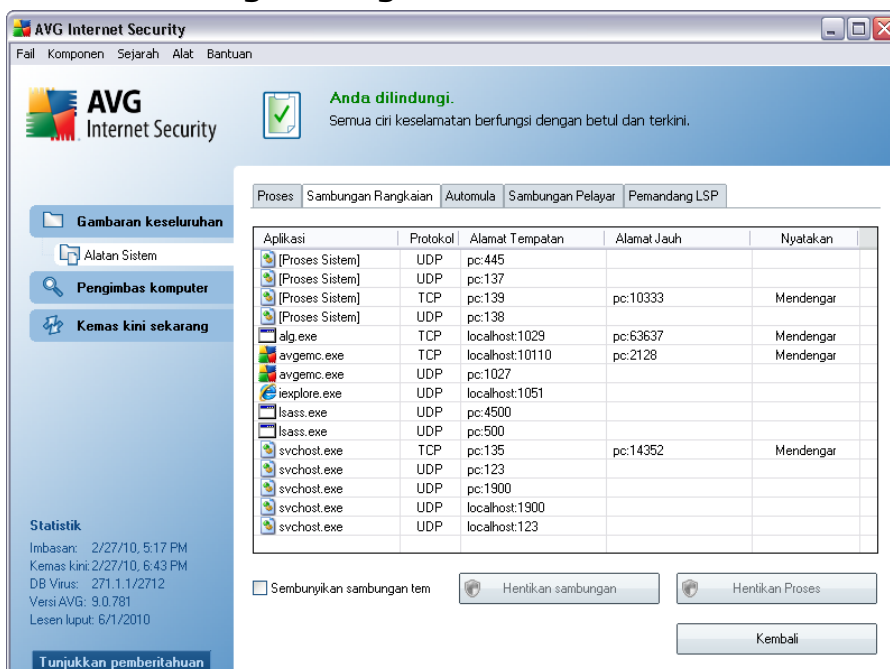
- **Tahap Keseriusan** - pengesanan grafik bagi keseriusan proses tersebut pada skala empat tahap daripada (■□□□) yang kurang penting sehingga (■■■■ yang kritikal)
- **Nama proses** - nama proses yang dijalankan
- **Laluan** - laluan fizikal ke proses yang dijalankan
- **Window** - jika boleh, menunjukkan nama aplikasi Window
- **Internet** - menunjukkan jika proses yang dijalankan juga menyambung ke Internet (*Ya/Tidak*)
- **Perkhidmatan** - menunjukkan jika proses yang dijalankan adalah perkhidmatan (*Ya/Tidak*)
- **PID** - nombor pengenalanpastian proses adalah pengenalan pasti dalaman Window unik

Butang kawalan

Butang kawalan tersedia dalam antara muka **Alat Sistem** adalah seperti berikut:

- **Muat Semula** - mengemas kini senarai proses mengikut status terkini
- **Tamatkan Proses** - anda boleh memilih satu atau lebih aplikasi dan kemudian, menamatkannya dengan menekan butang ini. **Kami amat menyarankan untuk tidak menamatkan sebarang sambungan, melainkan anda betul-betul pasti bahawa ia mewakili ancaman sebenar!**
- **Kembali** - mengalihkan anda semula ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen).

8.5.2. Sambungan Rangkaian



Dialog **Sambungan Rangkaian** mengandungi senarai sambungan yang sedang aktif. Senarai tersebut dibahagikan kepada kolom berikut:

- **Aplikasi** - nama aplikasi berkaitan dengan sambungan (*dengan pengecualian bagi Windows 2000 di mana maklumat os tidak tersedia*)

- **Protokol** - jenis protokol penghantaran digunakan untuk sambungan:
 - o TCP - protokol yang digunakan berkaitan dengan Protokol Internet (IP) untuk menghantar maklumat pada Internet
 - o UDP - sebagai ganti kepada protokol TCP
- **Alamat tempatan** - alamat IP bagi komputer tempatan dan nombor port yang digunakan
- **Alamat jauh** - alamat IP bagi komputer jauh dan nombor port yang disambungkan. Jika boleh, ia juga akan mencari nama hos bagi komputer jauh.
- **Keadaan** - menunjukkan keadaan semasa yang paling mungkin (*Disambungkan, Pelayan harus tutup, Dengar, Tutup aktif selesai, Tutup pasif, Tutup aktif*)

Untuk menyenaraikan hanya sambungan luaran, tandakan rait kotak semakan **Sembunyikan sambungan tempatan** dalam bahagian bawah dialog di bawah senarai.

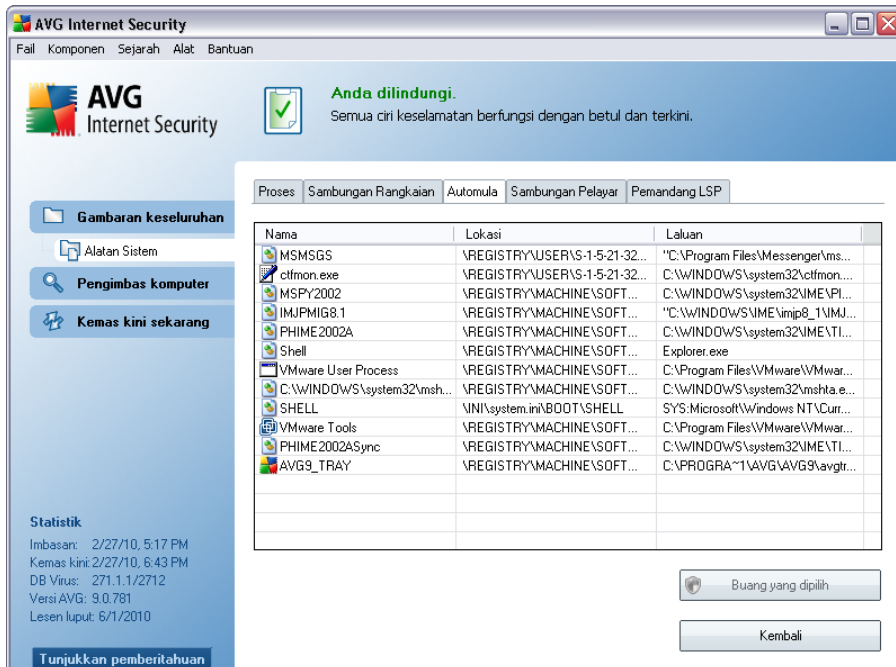
Butang kawalan

Butang kawalan yang tersedia adalah:

- **Tamatkan Sambungan** - menutup satu atau lebih sambungan yang dipilih dalam senarai
- **Tamatkan Proses** - menutup satu atau lebih aplikasi berkaitan dengan sambungan yang dipilih dalam senarai
- **Kembali** - kembali semula ke [antara muka AVG](#) lalai (gambaran keseluruhan komponen).

Kadangkala, anda boleh menamatkan hanya aplikasi yang sedang dalam keadaan bersambung. Kami amat menyarankan untuk tidak menamatkan sebarang sambungan, melainkan anda betul-betul pasti bahawa ia mewakili ancaman sebenar!

8.5.3. Automula

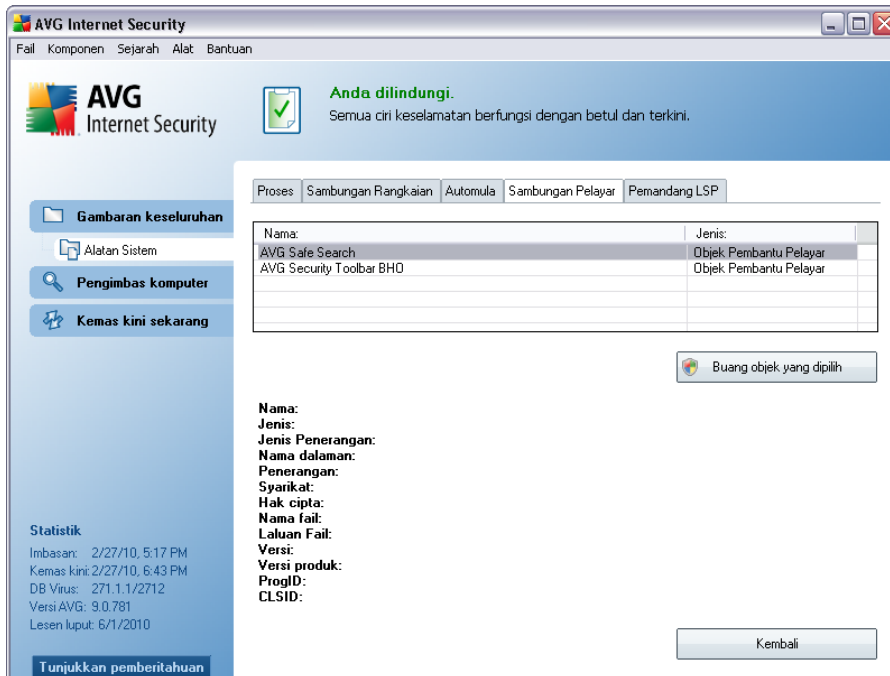


Dialog **Automula** dialog menunjukkan senarai semua aplikasi yang dilakukan sewaktu permulaan sistem Windows. Selalunya, beberapa aplikasi malware menambah diri mereka sendiri secara automatik kepada laluan masuk pendaftaran permulaan.

Anda boleh memadam satu atau lebih entri dengan memilihnya dan menekan butang **Buang yang terpilih**. Butang **Kembali** mengalihkan anda semula ke [antara muka pengguna AVG](#) (gambaran keseluruhan komponen).

Kami benar-benar mencadangkan tidak memadamkan mana-mana aplikasi dari senarai, kecuali anda benar-benar yakin ia mewakili ancaman sebenar!

8.5.4. Sambungan Pelayar



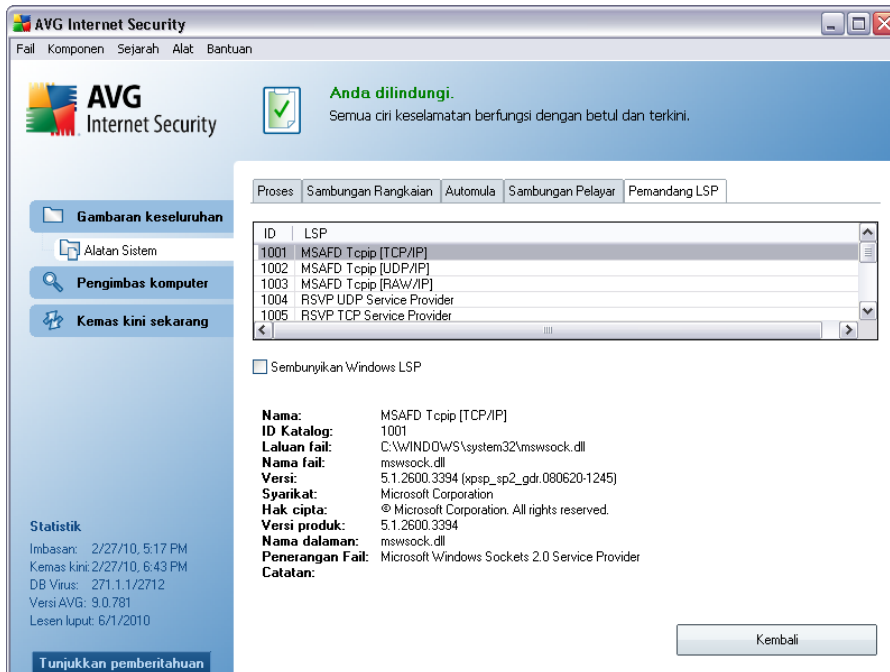
Dialog **Sambungan Pelayar** mengandungi senarai plug-in (*cth. aplikasi*) yang dipasang di dalam pelayar Internet. Senarai ini mungkin mengandungi plug-in aplikasi tetap serta potensi atur cara malware. Klik pada objek dalam senarai untuk mendapatkan maklumat terperinci pada plug-in yang dipilih yang akan dipaparkan dalam bahagian bawah dialog.

Butang kawalan

Butang kawalan tersedia pada tab **Sambungan Pelayar** adalah:

- **Buang objek yang dipilih** - buang plug-in yang sedang diserlahkan dalam senarai. **Kami amat menyarankan untuk tidak memadam sebarang plug-in daripada senarai, melainkan anda benar-benar pasti bahawa ia memberikan ancaman sebenar!**
- **Kembali** - mengalihkan anda kembali ke [antara muka pengguna AVG](#) (gambaran keseluruhan komponen)

8.5.5. Pemandang LSP



Dialog **Pemandang LSP** menunjukkan senarai Pembekal Perkhidmatan Berlapis (LSP).

Pembekal Perkhidmatan Berlapis (LSP) adalah pemacu sistem yang dipautkan ke dalam perkhidmatan rangkaian bagi sistem pengendalian Windows. Ia mempunyai akses kepada semua data yang masuk dan meninggalkan komputer, termasuk kebolehan untuk mengubah suai data ini. Beberapa LSP diperlukan untuk membenarkan Windows menyambungkan anda kepada komputer lain, termasuk Internet. Walau bagaimanapun, beberapa aplikasi malware tertentu juga mungkin memasang dengan sendiri seperti LSP, kemudian, mempunyai akses kepada semua data yang dipindahkan oleh komputer anda. Oleh itu, semakin semula ini mungkin membantu anda memeriksa semua kemungkinan ancaman LSP.

Dalam keadaan tertentu, ia juga berkemungkinan memperbaiki LSP yang telah rosak (*contohnya, apabila fail telah dialihkan tetapi entri pendaftaran kekal tidak disentuh*). Butang baru untuk memperbaiki isu itu dipaparkan sebaik saja LSP yang boleh dibaiki ditemui.

Untuk memasukkan Windows LSP dalam senarai, nyah tandakan kotak semak **Sembunyikan Windows LSP**. Butang **Undur** mengalihkan anda semula ke [antara muka pengguna AVG](#) (gambaran keseluruhan komponen).

8.6. Firewall

Firewall adalah sistem yang menguat kuasa dasar kawalan akses di antara dua atau lebih rangkaian dengan menyekat/membenarkan lalu lintas. Firewall mengandungi set peraturan yang melindungi rangkaian dalaman daripada serangan yang berasal dari luar (biasanya dari Internet) dan mengawal semua komunikasi pada setiap port rangkaian tunggal. Komunikasi dinilai menurut peraturan yang ditakrifkan dan kemudian, sama ada dibenarkan atau dilarang. Jika Firewall mengenal pasti sebarang cubaan gangguan, ia "menyekat" cubaan dan tidak membenarkan penceroboh mengakses komputer.

Firewall dikonfigurasi untuk membenarkan atau menolak komunikasi dalaman/luaran (kedua-dua cara, dalam atau luar) melalui port yang ditakrifkan dan untuk aplikasi perisian yang ditakrifkan. Contohnya, firewall boleh dikonfigurasi untuk hanya membenarkan data web mengalir masuk dan keluar menggunakan Microsoft Explorer. Sebarang cubaan untuk menghantar data web oleh sebarang penyemak imbas lain akan disekat.

Firewall melindungi maklumat yang dikenal pasti peribadi daripada dihantar dari komputer anda tanpa kebenaran anda. Ia mengawal cara komputer anda bertukar data dengan komputer lain pada Internet atau rangkaian setempat. Dalam organisasi, firewall juga melindungi komputer tunggal daripada serangan yang dimulakan oleh pengguna dalaman pada komputer lain dalam rangkaian.

Pengesyoran: Secara umum, ia tidak disyorkan untuk menggunakan lebih daripada satu firewall pada komputer individu. Keselamatan komputer tidak dipertingkatkan jika anda memasang lebih banyak firewall. Adalah lebih berkemungkinan bahawa beberapa konflik di antara dua aplikasi ini akan berlaku. Oleh sebab itu, kami mengesyorkan anda menggunakan hanya satu firewall pada komputer anda dan menyahaktifkan semua yang lain, seterusnya, menyingkirkan risiko kemungkinan konflik dan sebarang masalah yang berkaitan dengannya.

8.6.1. Prinsip Firewall

Dalam AVG, komponen **Firewall** mengawal semua lalu lintas pada setiap port rangkaian komputer anda. Berdasarkan pada peraturan yang ditakrifkan, **Firewall** menilai aplikasi yang sama ada dijalankan pada komputer anda (dan ingin menyambungkan ke rangkaian Internet/setempat) atau aplikasi yang mendekati komputer anda dari luar yang cuba menyambung ke PC anda. Untuk setiap aplikasi ini, kemudian **Firewall** membenarkan atau melarang komunikasi pada port rangkaian. Secara lalai, jika aplikasi diketahui (cth. tidak mempunyai peraturan **Firewall** yang ditakrifkan), **Firewall** akan menanyakan anda sama ada untuk membenarkan atau menyekat cubaan komunikasi.

Nota: AVG Firewall bukan bertujuan untuk platform pelayan!

Apa yang AVG Firewall boleh lakukan:

- membenarkan atau menghalang percubaan komunikasi oleh aplikasi [dikenali](#) secara automatik, atau meminta pengesahan anda
- Gunakan [profil](#) lengkap dengan peraturan pratkrif, mengikut keperluan anda
- [Tukar profil](#) secara automatik apabila menyambung kepada pelbagai rangkaian, atau menggunakan pelbagai penyesuai rangkaian

8.6.2. Profil Firewall

Firewall membenarkan anda mentakrifkan peraturan keselamatan tertentu berdasarkan pada sama ada komputer anda terletak pada domain, atau ia komputer berdiri sendiri, atau mungkin komputer bimbit. ******* Setiap opsyen ini memerlukan perlindungan yang berbeza tahap, dan setiap tahap dilindungi oleh profil masing-masing. Secara ringkas, profil [Firewall](#) adalah konfigurasi khusus komponen [Firewall](#) dan anda boleh menggunakan sebilangan konfigurasi yang dipratkrif seperti itu.

Profil yang ada

- **Benarkan semua** - profil sistem [Firewall](#) yang telah dipratetapkan oleh pengilang dan sentiasa wujud. Apabila profil ini diaktifkan, semua komunikasi rangkaian dibenarkan dan tiada peraturan dasar keselamatan yang dikenakan, seperti perlindungan [Firewall](#) dimatikan (*cth. semua aplikasi dibenarkan tetapi paket masih diperiksa - untuk menyahdayakan sepenuhnya sebarang penapisan yang anda perlukan untuk menyahdayakan Firewall*). Profil sistem tidak boleh disalin, dipadamkan, dan tetapannya tidak boleh diubah.
- **Sekat semua** - profil sistem [Firewall](#) yang telah dipratetap oleh pengilang dan sentiasa wujud. Apabila profil ini diaktifkan, semua komunikasi rangkaian disekat, dan komputer tidak boleh diakses dari luar, atau berkomunikasi di luar. Profil sistem tidak boleh disalin, dipadamkan, dan tetapannya tidak boleh diubah.
- **Profil tersuai:**
 - o **Sambungkan secara terus ke Internet** – sesuai untuk komputer rumah desktop biasa disambungkan secara terus ke Internet atau notebook yang menyambung ke Internet di luar rangkaian syarikat selamat. Pilih opsyen ini jika anda bersambung dari rumah atau anda dalam rangkaian syarikat kecil dengan tiada kawalan pusat. Serta, pilih opsyen ini semasa

mengembara dan menyambung dengan komputer bimbit anda dari pelbagai tempat yang tidak diketahui dan berkemungkinan berbahaya (*kafe internet, bilik hotel, dll.*). Lebih banyak peraturan had yang akan dibuat kerana ia dianggap bahawa komputer ini tidak mempunyai perlindungan tambahan dan oleh itu, memerlukan perlindungan maksimum.

- o **Komputer dalam domain** – sesuai untuk komputer dalam rangkaian setempat, cthnya. sekolah atau rangkaian korporat. Adalah dianggap bahawa rangkaian dilindungi oleh beberapa langkah tambahan agar tahap keselamatan boleh jadi lebih rendah daripada komputer berdiri sendiri sahaja.
- o **Rangkaian kecil rumah atau pejabat** – sesuai hanya untuk komputer dalam rangkaian kecil, cth. di rumah atau dalam perniagaan kecil, biasanya hanya beberapa komputer yang disambungkan bersama, tanpa pentadbir "pusat".

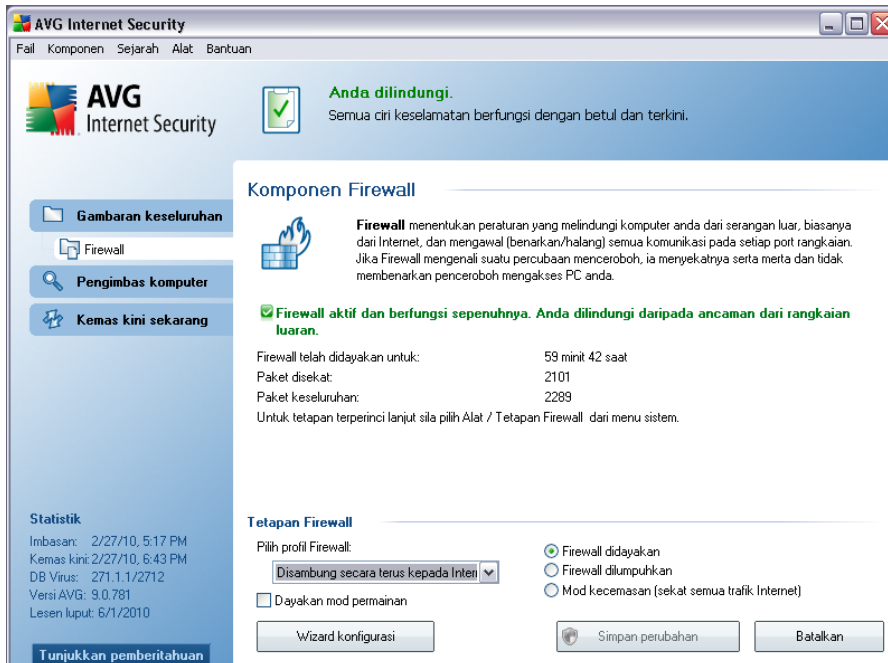
Pertukaran profil

Ciri pertukaran profil membenarkan [**Firewall**](#) untuk beralih secara automatik ke profil yang ditakrifkan semasa menggunakan penyesuaian rangkaian tertentu atau semasa disambungkan ke jenis rangkaian tertentu. Jika belum ada profil yang telah diperuntukkan ke kawasan rangkaian, maka, pada sambungan berikutnya ke kawasan tersebut [**Firewall**](#) akan memaparkan dialog yang meminta anda menguntukkan profil.

Anda boleh menguntukkan profil ke semua antara muka atau kawasan rangkaian dan menentukan tetapan selanjutnya dalam dialog [**Profil Kawasan dan Penyesuaian**](#), di mana anda juga boleh menyahdayakan ciri tersebut jika anda tidak mahu menggunakannya (*kemudian, untuk sebarang jenis sambungan, profil lalai akan digunakan*).

Biasanya, pengguna yang mempunyai komputer bimbit dan menggunakan pelbagai jenis sambungan akan mendapati ciri ini berguna. Jika anda mempunyai komputer desktop, dan hanya menggunakan satu jenis sambungan (*cth. sambungan kabel kepada Internet*), anda tidak perlu terganggu dengan pertukaran profil kerana kemungkinan besar anda tidak akan menggunakannya.

8.6.3. Antara Muka Firewall



Antara muka **Firewall** memberikan beberapa maklumat asas mengenai kefungsiian komponen dan gambaran keseluruhan ringkas bagi statistik **Firewall** :

- **Firewall telah didayakan untuk** - masa berlalu sejak Firewall kali terakhir dilancarkan
- **Paket yang disekat** - bilangan paket yang disekat daripada keseluruhan jumlah paket yang diperiksa
- **Paket keseluruhan** - bilangan semua paket yang diperiksa sewaktu Firewall dijalankan

Konfigurasi komponen asas

- **Pilih profil Firewall** - dari menu gulung ke bawah, pilih salah satu profil yang ditakrifkan - dua profil tersedia pada setiap masa (profil lalai yang dinamakan **Benarkan semua** dan **Sekat semua**), profil lain ditambah secara manual melalui pengeditan profil dalam dialog **Profil** dalam **Tetapan Firewall**.
- **Dayakan mod permainan** - Tandakan pilihan ini untuk memastikan bahawa

semasa menjalankan aplikasi skrin penuh (permainan, persembahan PowerPoint dll.), **Firewall** tidak akan memaparkan dialog menanyakan anda sama ada hendak membenarkan atau menghalang komunikasi untuk aplikasi tidak diketahui. Jika aplikasi tidak diketahui cuba berkomunikasi pada rangkaian dalam masa tersebut, **Firewall** akan membenarkan atau menyekat cubaan secara automatik menurut tetapan dalam profil semasa.

- **Status Firewall:**

- o **Firewall didayakan** - pilih pilihan ini untuk membenarkan komunikasi kepada aplikasi tersebut yang diperuntukkan sebagai 'dibenarkan' dalam set peraturan yang ditakrifkan dalam profil **Firewall** yang dipilih
- o **Firewall dinyahdayakan** - pilihan ini mematikan **Firewall** sepenuhnya, semua lalu lintas rangkaian dibenarkan tetapi tidak ditanda!
- o **Mod kecemasan (sekat semua lalu lintas internet)** - pilih opsi ini untuk menyekat semua lalu lintas pada setiap port rangkaian tunggal; **Firewall** masih dijalankan tetapi semua lalu lintas rangkaian dihentikan

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang perubahan kepada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja. Jika anda perlu mengubah konfigurasi Firewall, pilih item menu sistem **tetapan Alat/Firewall** dan edit konfigurasi Firewall dalam dialog **Tetapan Firewall** yang baru dibuka.

Butang kawalan

- **Wizard konfigurasi** - tekan butang untuk beralih ke dialog masing-masing (yang digunakan dalam proses pemasangan) dipanggil **Bahagian Penggunaan Komputer** di mana, anda boleh mentakrifkan konfigurasi komponen **Firewall**
- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batalan** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lahai (gambaran keseluruhan komponen)

8.7. Pengimbas E-mel

Salah satu sumber virus dan trojan yang paling biasa adalah melalui e-mel. Pemalsuan dan spam membuatkan e-mel menjadi sumber risiko yang lebih hebat. Akaun e-mel percuma adalah lebih berkemungkinan menerima e-mel berniat jahat seperti itu (*kerana ia jarang menggunakan teknologi antispam*), dan pengguna rumah bergantung agak kuar pada e-mel seperti itu. Serta pengguna rumah yang melayari tapak yang tidak diketahui dan mengisi borang dalam talian dengan data peribadi (*seperti alamat e-mel mereka*) meningkatkan pendedahan kepada serangan melalui e-mel. Syarikat biasanya menggunakan akaun e-mel korporat dan menggunakan penapis antispam dan lain-lain untuk mengurangkan risiko.

8.7.1. Prinsip Pengimbas E-mel

Komponen **Pengimbas E-mel** mengimbas e-mel masuk/keluar secara automatik. Anda boleh menggunakannya dengan klien e-mel yang tidak mempunyai plug-in sendiri dalam AVG (*cth. Outlook Express, Mozilla, Incredimail, dll.*).

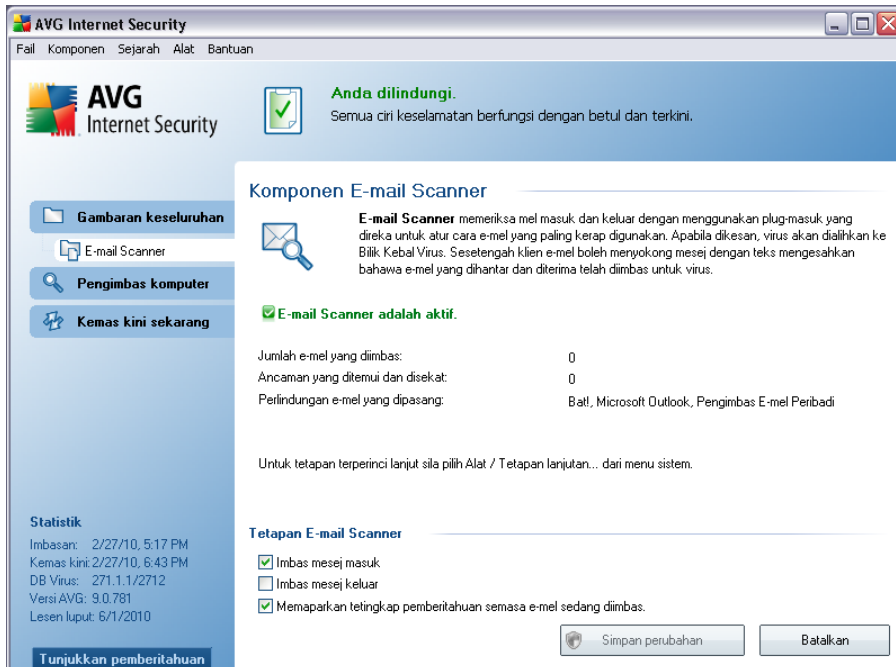
Sewaktu pemasangan [AVG](#) AVG terdapat pelayan automatik dibuat untuk kawalan e-mel: satu untuk memeriksa e-mel masuk dan yang kedua untuk memeriksa e-mel keluar. Menggunakan dua pelayan ini, e-mel diperiksa secara automatik pada port 110 dan 25 (*port standard untuk menghantar/menerima e-mel*).

Pengimbas E-mel berfungsi sebagai antara muka di antara klien e-mel dan pelayan e-mel pada Internet.

- **Mel masuk:** Apabila menerima mesej daripada pelayan, komponen **Pengimbas E-mel** mengujinya untuk virus, membuang lampiran yang dijangkiti dan menambah perakuan. Semasa dikesan, virus dikuarantin dalam [Bilik Kebal Virus](#) dengan serta-merta. Kemudian mesej itu diberikan kepada klien e-mel.
- **Mel Keluar:** Mesej dihantar dari klien e-mel ke Pengimbas E-mel; ia menguji mesej dan lampirannya untuk virus dan kemudian, menghantar mesej ke pelayan SMTP (*mengimbas e-mel keluar dinyahdayakan secara lalai dan boleh disediakan secara manual*).

Nota: Pengimbas E-mel AVG bukan bertujuan untuk platform pelayan!

8.7.2. Antara Muka Pengimbas E-mel



Dalam dialog komponen **Pengimbas E-mel** anda boleh menemui teks ringkas yang menerangkan kefungsiian komponen, maklumat pada status semasanya (*Pengimbas E-mel masih aktif.*), dan statistik berikut:

- **Jumlah e-mel yang diimbas** - berapa banyak mesej e-mel yang diimbas sejak **Pengimbas E-mel** dilancarkan kali terakhir (*jika perlu, nilai ini boleh ditetapkan semula; cth. untuk tujuan statistik - Tetapkan semula nilai*)
- **Ancaman ditemui dan disekat** - memberikan bilangan jangkitan yang dikesan dalam setiap mesej e-mel sejak kali terakhir **Pengimbas E-mel** dilancarkan
- **Perlindungan e-mel yang dipasang** - maklumat mengenai plug-in perlindungan e-mel khusus merujuk kepada klien e-mel lalai anda yang dipasang

Konfigurasi komponen asas

Di bahagian bawah dialog, anda boleh menemui bahagian yang dinamakan **tetapan Pengimbas E-mel** di mana anda boleh mengedit beberapa ciri permulaan bagi kefungsiian komponen:

- **Imbas mesej masuk** - memeriksa item untuk menentukan bahawa semua e-mel yang dihantar ke akaun anda harus diimbis untuk virus. Secara lalai, item ini dihidupkan dan adalah disyorkan untuk tidak menukar tetapan ini!
- **Imbas mesej keluar** - memeriksa item untuk mengesahkan bahawa semua e-mel yang dihantar dari akaun anda harus diimbis untuk virus. Secara lalai, item ini dimatikan.
- **Paparkan ikon pemberitahuan semasa E-mel diimbis** - periksa item untuk mengesahkan anda hendak diberitahu melalui dialog pemberitahuan yang dipaparkan pada ikon AVG pada dulang sistem sewaktu pengimbasan mel anda melalui komponen [Pengimbas E-mel](#). Secara lalai, item ini dihidupkan dan adalah disyorkan untuk tidak menukar tetapan ini!

Konfigurasi lanjutan bagi komponen **Pengimbas E-mel** boleh diakses melalui item **tetapan Alat/Lanjutan** bagi menu sistem; walau bagaimanapun, konfigurasi lanjutan disarankan untuk pengguna berpengalaman sahaja!

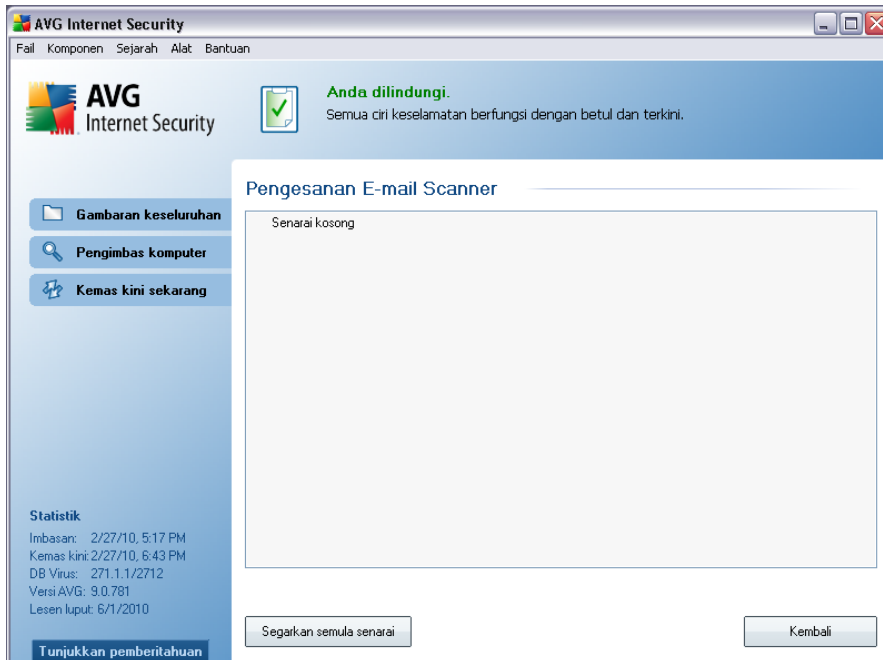
Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

Butang kawalan

Butang kawalan dalam antara muka **Pengimbas E-mel** adalah seperti berikut:

- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen)

8.7.3. Pengesanan Pengimbas E-mel



Dalam dialog **Pengesanan Pengimbas E-mel** (boleh diakses melalui pengesanan pilihan menu sistem *Sejarah / Pengimbas E-mel*) anda boleh melihat senarai semua penemuan yang dikesan oleh komponen **Pengimbas E-mel**. Untuk setiap objek yang dikesan, maklumat berikut disediakan:

- **Jangkitan**- penerangan (malahan juga nama) bagi objek yang dikesan
- **Objek** - lokasi objek
- **Keputusan** - tindakan dilakukan dengan objek yang dikesan
- **Masa pengesanan** - tarikh dan masa objek mencurigakan dikesan
- **Jenis Objek** - jenis objek yang dikesan

Di bahagian bawah dialog, di bawah senarai, anda akan menemui maklumat mengenai jumlah bilangan objek dikesan yang disenaraikan di atas. Seterusnya, anda boleh mengeksport keseluruhan senarai objek yang dikesan dalam fail (**Eksport senarai ke fail**) dan padam semua entri pada objek dikesan (**Kosongkan senarai**).

Butang kawalan

Butang kawalan tersedia dalam antara muka **pengesanan Pengimbas E-mel** adalah seperti berikut:

- **Muat semula senarai** - mengemas kini senarai ancaman yang dikesan
- **Kembali** - mengalihkan anda semula ke [antara muka pengguna AVG](#) lahai (gambaran keseluruhan komponen)

8.8. Perlindungan ID

AVG Identity Protection adalah produk antimalware yang memberi tumpuan kepada mengelakkan pencuri identiti daripada mencuri kata laluan anda, butiran akaun bank, nombor kad kredit dan barangan digital peribadi yang lain yang bernilai daripada semua jenis perisian berniat jahat (*malware*) yang mensasarkan PC anda. Ia memastikan semua atur cara yang dijalankan pada PC anda beroperasi dengan betul. **AVG Identity Protection** mengesan dan menyekat kelakuan yang mencurigakan pada asas berterusan dan melindungi komputer anda daripada semua malware baru.

8.8.1. Prinsip Perlindungan ID

AVG Identity Protection adalah komponen antimalware yang melindungi anda daripada semua jenis malware (*perisian pengintip, bot, pencuri identiti, ...*) menggunakan teknologi kelakuan dan memberikan perlindungan hari sifar untuk virus baru. Apabila malware menjadi sofistikated dan datang dalam bentuk atur cara normal yang boleh mendedahkan PC anda kepada penyerang jauh bagi pencuri identiti, **AVG Identity Protection** melindungi anda daripada pelaksanaan baru ini yang berasaskan malware. Ia adalah perlindungan percuma kepada [AVG Anti-Virus](#) yang melindungi anda daripada fai berasaskan dan diketahui virus menggunakan mekanisme tandatangan dan pengimbasan.

Kami amat mengesyorkan anda mempunyai kedua-dua komponen [AVG Anti-Virus](#) dan **AVG Identity Protection dipasang, untuk mempunyai perlindungan lengkap untuk PC anda.**

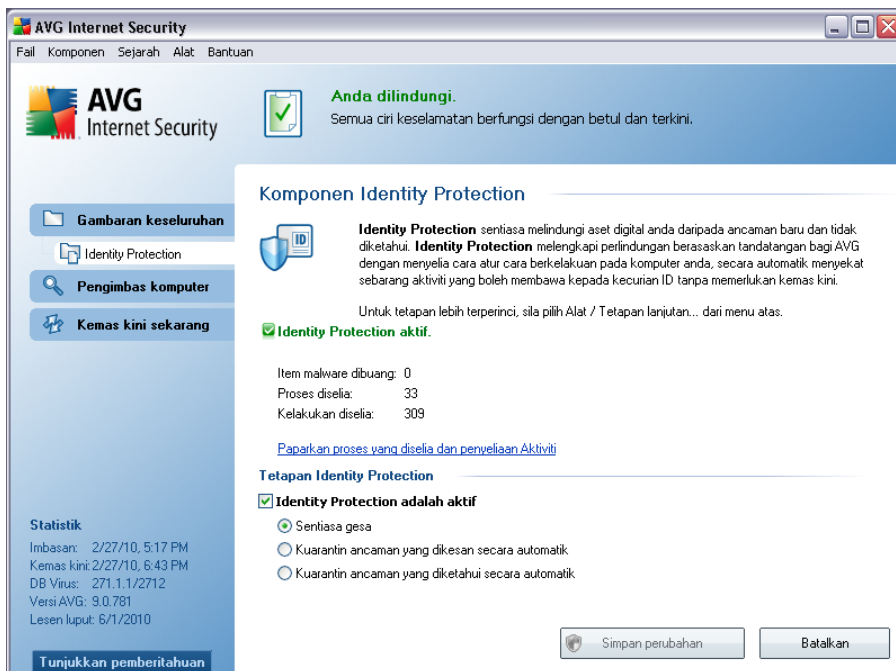
8.8.2. Antara Muka Perlindungan ID

Antara muka komponen **Perlindungan Identiti** memberikan penerangan ringkas bagi kefungsiian asas komponen, statusnya (*AVG Perlindungan Identiti adalah aktif dan berfungsi sepenuhnya.*) dan beberapa data statistik:

- **Item malware dibuang** - memberikan bilangan aplikasi yang dikesan sebagai

malware dan dibuang

- **Proses diselia** - bilangan aplikasi yang sedang dijalankan yang diselia oleh IDP
- **Kelakuan diselia** - bilangan tindakan khusus yang sedang dijalankan dalam aplikasi yang diselia



Konfigurasi komponen asas

Di bahagian bawah dialog, anda akan menemui bahagian **tetapan Perlindungan Identiti** di mana anda boleh mengedit beberapa ciri permulaan bagi kefungsiian komponen:

- **Perlindungan Identiti adalah aktif** - (*dihidupkan secara lalai*): tanda untuk mengaktifkan komponen IDP dan untuk membuka opsyen pengeditan selanjutnya.

Dalam sesetengah kes, **Perlindungan Identiti** mungkin melaporkan bahawa beberapa fail yang sah adalah mencurigakan atau berbahaya. Memandangkan **Perlindungan Identiti** mengesan ancaman berdasarkan pada kelakuan mereka, ini biasanya berlaku apabila beberapa atur cara cuba menyelia penekanan kekunci, memasang atur cara lain atau pemacu baru yang dipasang pada komputer.

Oleh itu, sila pilih salah satu opsi berikut yang menentukan kelakuan komponen **Perlindungan Identiti** sekiranya mengesan aktiviti mencurigakan:

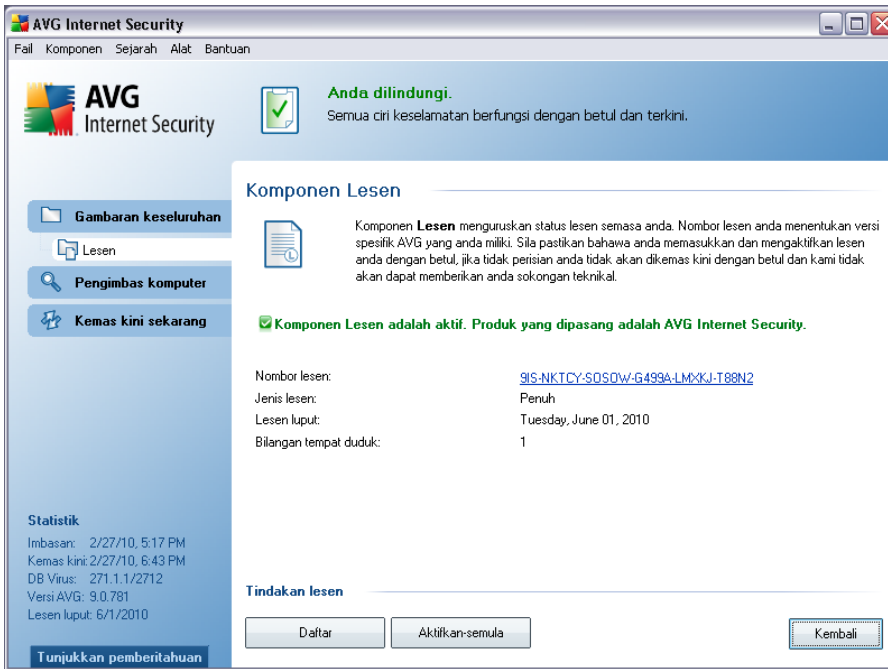
- o **Sentiasa gesa** - jika aplikasi dikesan sebagai malware, anda akan ditanya sama ada ia harus disekat (*pilihan ini dihidupkan secara lalai dan disyorkan untuk tidak mengubahnya melainkan anda mempunyai sebab sebenar untuk melakukannya*)
- o **Kuarantin ancaman yang dikesan secara automatik** - semua aplikasi dikesan sebagai malware akan disekat secara automatik
- o **Kuarantin ancaman yang diketahui secara automatik** - hanya aplikasi dengan kepastian mutlak dikesan sebagai malware akan disekat

Butang kawalan

Butang kawalan yang tersedia dalam antara muka **Perlindungan Identiti** adalah seperti berikut:

- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen)

8.9. Lesen



Dalam antara muka komponen **Lesen** anda akan menemui teks ringkas menerangkan kefungsiian komponen, maklumat pada status terkini (*Komponen lesen adalah aktif*), dan maklumat berikut:

- **Nombor lesen** - memberikan bentuk sebenar nombor lesen anda. Semasa memasukkan nombor lesen anda, anda perlu betul-betul tepat dan menaipnya betul-betul seperti yang ditunjukkan. Oleh itu, kami amat mengesyorkan untuk sentiasa menggunakan kaedah "salin & tampal" untuk sebarang manipulasi dengan nombor lesen.
- **Jenis lesen** - menentukan jenis produk yang dipasang.
- **Lesen tamat tempoh** - tarikh ini menentukan tempoh kesahan lesen anda. Jika anda hendak terus menggunakan **AVG 9 Internet Security** selepas tarikh ini, anda perlu memperbaharui lesen anda. [Pembaharuan lesen boleh dilakukan dalam talian](http://www.avg.com/) pada tapak web AVG (<http://www.avg.com/>).
- **Bilangan tempat duduk** - berapa banyak stesen kerja pada mana anda tertakluk untuk memasang **AVG 9 Internet Security** anda.

Butang kawalan

- **Daftar** - menyambungkan ke halaman pendaftaran bagi tapak web AVG (<http://www.avg.com/>). Sila isikan data pendaftaran anda; hanya pelanggan yang mendaftarkan produk AVG mereka boleh menerima sokongan teknikal percuma.
- **Aktifkan semula** - membuka dialog **Aktifkan AVG** dengan data yang anda telah masukkan dalam dialog **Peribadikan AVG** bagi [proses pemasangan](#). Dalam dialog ini, anda boleh memasukkan nombor lesen anda dengan sama ada menggantikan nombor jualan (*nombor yang anda telah pasangkan AVG*), atau untuk menggantikan nombor lesen lama (*cth. semasa menaik taraf ke produk AVG baru*).

Perhatian: Jika menggunakan versi percubaan bagi **AVG 9 Internet Security**, butang muncul sebagai **Beli sekarang** dan **Aktifkan**, membenarkan anda membeli versi penuh bagi atur cara dengan serta-merta. Untuk **AVG 9 Internet Security** yang dipasang dengan nombor jualan, butang dipaparkan sebagai **Daftar** dan **Aktifkan**.

- **Kembali** - tekan butang ini untuk kembali ke [antara muka AVG](#) lalai (gambaran keseluruhan komponen).

8.10. Pengimbas Pautan

8.10.1. Prinsip Pengimbas Pautan

Komponen **LinkScanner** memberikan perlindungan daripada tapak web yang direka bentuk untuk memasang malware ke dalam komputer anda melalui pelayar web atau plugin. Teknologi **LinkScanner** terdiri daripada dua ciri, [AVG Search-Shield](#) dan [AVG Active Surf-Shield](#):

- [AVG Search Shield](#) mengandungi senarai tapak web (*alamat URL*) yang diketahui berbahaya. Apabila mencari Google, Yahoo!, Bing, Baidu, Altavista atau Yandex, semua keputusan carian diperiksa mengikut senarai ini dan ikon keputusan ditunjukkan (*untuk Yahoo! hasil carian hanya ikon keputusan "tapak web yang dieksploitasi" ditunjukkan*). Serta, jika anda menaip beberapa alamat secara terus ke dalam pelayar anda, klik pautan pada sebarang tapak web atau cth. dalam e-mel anda, ia disemak secara automatik dan disekat jika perlu.
- [AVG Active Surf-Shield](#) mengimbas kandungan tapak web yang anda lawati,

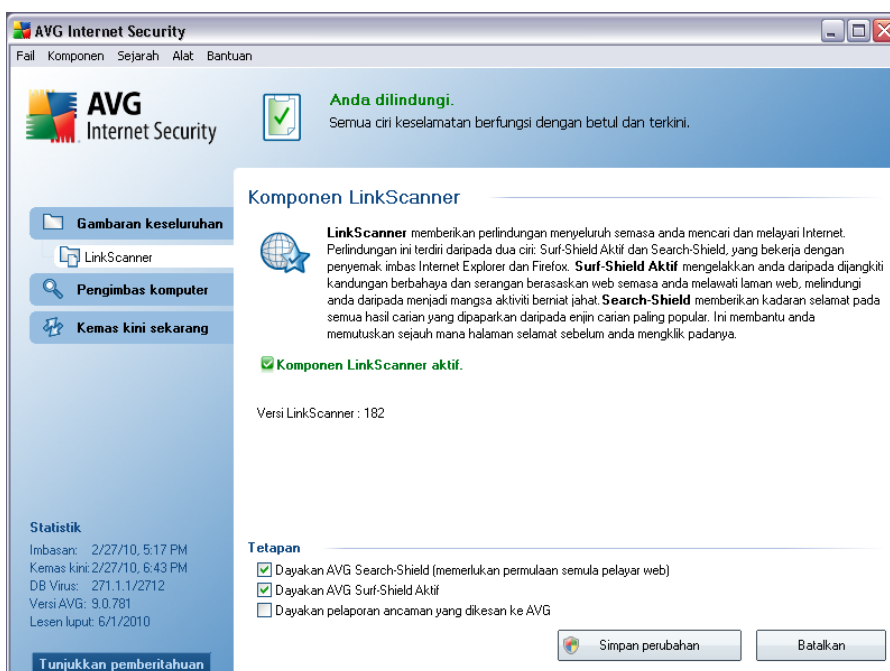
tidak kira alamat tapak web. Walaupun, sesetengah tapak web tidak dikesan oleh **AVG Search Shield** (cth. apabila tapak web berniat jahat dibuat atau apabila tapak web bersih sebelumnya mengandungi beberapa malware), ia akan dikesan dan disekat oleh **AVG Active Surf-Shield** apabila anda cuba melawatinya.

Nota: AVG Link Scanner bukan bertujuan untuk platform pelayan!

8.10.2. Antara Muka Pengimbas Pautan

Komponen **LinkScanner** terdiri daripada dua bahagian yang anda boleh hidupkan/matikan dalam antara muka **komponen LinkScanner**:

Antara muka komponen **LinkScanner** memberikan penerangan ringkas kefungsi dan maklumat komponen pada status semasanya (*komponen LinkScanner adalah aktif.*). Seterusnya, anda boleh mencari maklumat mengenai nombor versi pangkalan data **LinkScanner** terkini (*LinkScanner Version*).



Di bahagian bawah dialog anda boleh mengedit beberapa opsiyen:

- **Dayakan **AVG Search-Shield**** - (*dihidupkan secara lalai*): ikon pemberitahuan maklumat pada carian dilakukan dalam Google, Yahoo!, Bing, Baidu, Yandex atau Altavista: kandungan tapak diperiksa dahulu yang dikembalikan oleh enjin

carian.

- **Dayakan AVG Active Surf-Shield** - (*hidupkan secara lalai*): perlindungan (*masa nyata*) aktif daripada tapak yang boleh mengeksploitasi apabila ia diakses. Sambungan tapak yang diketahui berniat jahat dan kandungannya yang boleh mengeksploitasi apabila ia diakses oleh pengguna melalui penyemak imbas web (*atau sebarang aplikasi lain yang menggunakan HTTP*).
- **Dayakan pelaporan ancaman yang dikesan kepada AVG** - tandakan item ini untuk membenarkan pelaporan semula eksploitasi dan tapak jahat yang ditemui oleh pengguna sama ada melalui **Pelayaran Selamat** atau **Carian Selamat** untuk menyuap maklumat pengumpulan pangkalan data mengenai aktiviti berniat jahat pada web.

8.10.3. AVG Search-Shield

Semasa mencari Internet dengan **AVG Search-Shield** dihidupkan, semua keputusan carian dikembalikan daripada enjin carian paling popular seperti Yahoo!, Google, Bing, Altavista, Yandex, dll. dinilai bagi pautan yang berbahaya atau mencurigakan. Dengan menanda pautan ini dan menandakan pautan jahat, **AVG Link Scanner** memberi amaran kepada anda sebelum anda mengklik pada pautan berbahaya atau mencurigakan, supaya anda boleh memastikan anda hanya pergi ke laman web selamat.

Semasa pautan dinilai pada halaman keputusan carian, anda akan melihat tanda grafik di sebelah pautan yang memberitahu bahawa pengesahan pautan sedang dijalankan. Apabila penilaian selesai, ikon maklumat masing-masing akan dipaparkan.

 Halaman berpaut adalah selamat (*dengan enjin pencarian Yahoo! dalam [AVG Security Toolbar](#) ikon ini tidak akan dipaparkan!*).

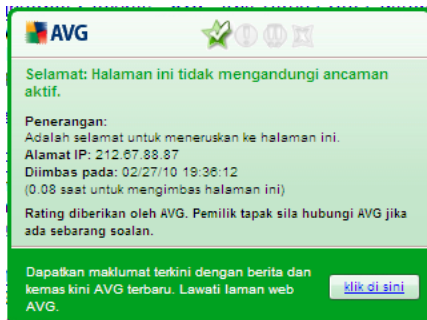
 Halaman yang dipautkan tidak mengandungi ancaman tetapi agak mencurigakan (*dipersoalkan bagi asal atau motif, oleh itu, ia tidak disarankan untuk e-shopping dll.*).

 Halaman yang boleh dipautkan boleh menjadi sama ada selamat sendiri tetapi mengandungi pautan selanjutnya ke halaman berbahaya secara positif; atau kod yang mencurigakan, walaupun, tidak mempunyai sebarang ancaman secara terus buat masa ini.

 Halaman berpaut mengandungi ancaman aktif! Untuk keselamatan anda sendiri, anda tidak akan dibenarkan untuk melawati halaman ini.

 Halaman yang dipautkan tidak boleh diakses dan oleh itu, tidak boleh diimbas.

Menghalakan pada setiap ikon rating akan memaparkan butiran mengenai pautan khusus yang dipersoalkan. Maklumat termasuk butiran tambahan mengenai ancaman (jika ada), alamat IP pautan dan bila halaman diimbis oleh AVG.



8.10.4. AVG Active Surf-Shield

Perlindungan yang berkuasa ini menyekat kandungan sebarang laman web yang anda cuba untuk buka dan mengelaknya daripada dimuat turun ke komputer anda. Dengan ciri ini didayakan, mengklik pautan atau menaip dalam URL ke tapak berbahaya akan menghalang anda daripada membuka laman web secara automatik, dengan itu, melindungi anda daripada dijangkiti secara lalai. Adalah penting untuk mengingati bahawa halaman web dieksploitasi boleh menjangkiti komputer anda hanya dengan melawati tapak yang terlibat, untuk tujuan ini apabila anda meminta halaman web berbahaya mengandungi eksploitasi atau ancaman serius lain, [AVG Link Scanner](#) tidak akan membenarkan penyemak imbas anda memaparkannya.

Jika anda berhadapan dengan tapak web berniat jahat dalam pelayar web anda [AVG Link Scanner](#) akan memberi amaran kepada anda dengan skrin yang sama dengan:



Memasuki tapak web sangat berisiko dan ia tidak disyorkan!

8.11. Perisai Dalam Talian

8.11.1. Prinsip Perisai Dalam Talian

Perisai Dalam Talian adalah sejenis perlindungan residen masa nyata; ia mengimbas kandungan halaman web yang dilawati (dan kemungkinan fail yang dimasukkan dalamnya) walaupun sebelum ini dipaparkan dalam pelayar web anda atau dimuat turun ke komputer anda.

Perisai Dalam Talian mengesan bahawa halaman yang anda akan lawati memasukkan beberapa javascript berbahaya dan mengelakkan halaman daripada dipaparkan. Serta, ia mengenal pasti malware yang terkandung dalam halaman dan menghentikan muat turunnya dengan serta-merta supaya ia tidak pergi ke komputer anda.

Perhatian: AVG Perisai Dalam Talian bukan bertujuan untuk platform pelayan!

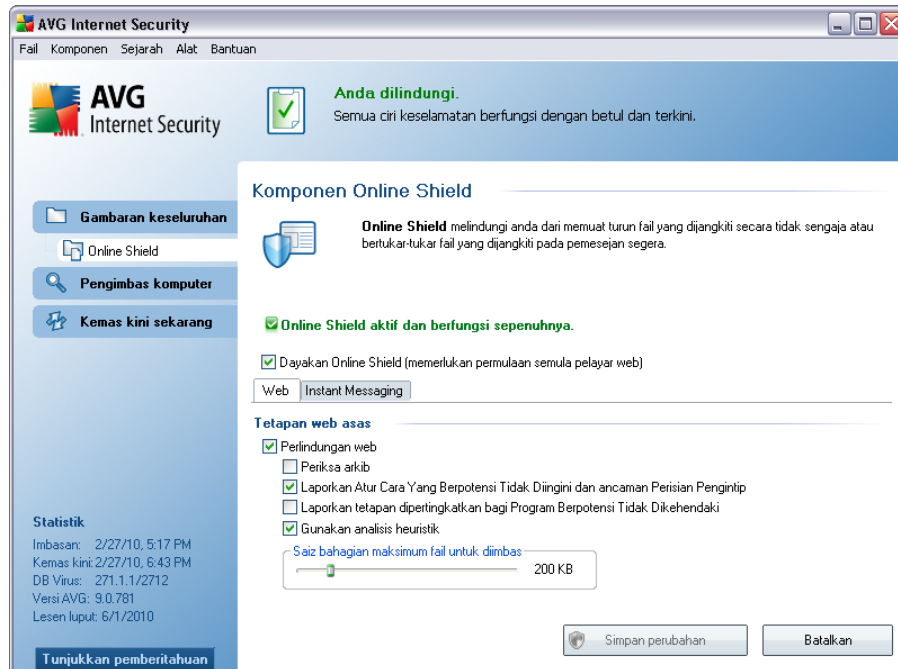
8.11.2. Antara Muka Perisai Dalam Talian

Antara muka komponen **Perisai Dalam Talian** menerangkan kelakuan jenis perlindungan ini. Seterusnya, anda boleh mendapatkan maklumat mengenai status terkini komponen (*Perisai Dalam Talian adalah aktif dan berfungsi sepenuhnya.*). Di bahagian bawah dialog, kemudian, anda akan menemui opsyen pengeditan bagi kefungsiian komponen ini.

Konfigurasi komponen asas

Pertama sekali, anda mempunyai pilihan untuk menghidupkan/mematikan **Perisai Dalam Talian** dengan segera dengan menandakan item **Dayakan Perisai Dalam Talian**. Pilihan ini didayakan secara lalai dan komponen **Perisai Dalam Talian** adalah aktif. Walau bagaimanapun, jika anda tidak mempunyai alasan yang baik untuk mengubah tetapan ini, kami mengesyorkan untuk memastikan komponen aktif. Jika item ditanda dan **Perisai Dalam Talian** dijalankan, lebih banyak pilihan konfigurasi tersedia dan boleh diedit pada dua tab:

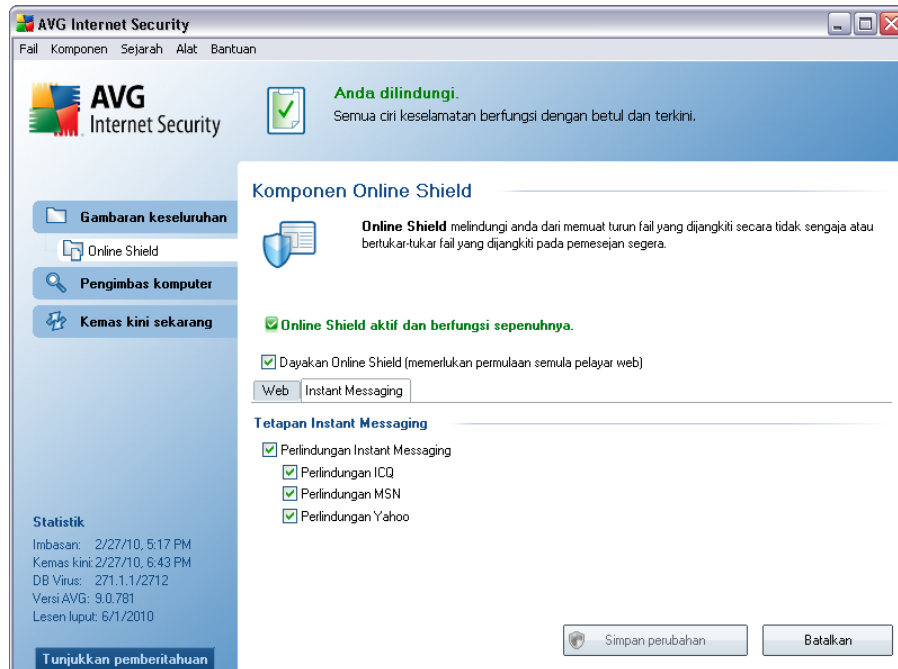
- **Web** - anda boleh mengedit konfigurasi komponen berkenaan imbasan kandungan tapak web. Antara muka penyuntingan ini membenarkan anda untuk mengkonfigurasi opsyen permulaan berikut:



- o **Perindungan web** - pilihan ini mengesahkan bahawa **Perisai Dalam Talian** harus menjalankan pengimbasan bagi kandungan halaman www. Jika opsyen ini dihidupkan (*secara lalai*), seterusnya, anda boleh menghidupkan/mematikan item ini:
 - **Periksa arkib** - imbas kandungan arkib yang berkemungkinan dimasukkan dalam halaman www untuk dipaparkan
 - **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin **AntiPerisian Pengintip**, dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda
 - **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini** - jika pilihan sebelumnya diaktifkan, anda juga boleh menanda kotak ini untuk mengesan pakej diluaskan bagi [perisian pengintip](#): atur cara adalah sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat kemudiannya. Ini adalah ukuran tambahan

yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.

- **Gunakan analisis heuristik** - imbas kandungan bagi halaman untuk dipaparkan menggunakan kaedah analisis heuristik, iaitu persaingan dan penilaian bagi arahan objek diimbis dalam persekitaran komputer maya. Oleh itu, malahan, ia boleh mengesan kod berniat jahat yang belum diterangkan dalam pangkalan data virus (*lihat [Prinsip AntiVirus](#)*).
- **Saiz fail maksimum untuk diimbis** - jika fail yang dimasukkan terdapat dalam halaman yang dipaparkan, anda juga boleh mengimbis kandungannya sebelum ia dimuat turun ke komputer anda. Walau bagaimanapun, pengimbasan fail besar mengambil sedikit masa dan muat turun laman web mungkin menjadi perlahan. Anda boleh menggunakan bar gelangsar untuk menentukan saiz maksimum bagi fail yang masih diimbis dengan **Perisai Dalam Talian**. Walaupun jika fail yang dimuat turun adalah lebih besar daripada yang ditentukan, dan oleh itu, tidak akan diimbis dengan **Perisai Dalam Talian**, anda masih dilindungi: jika fail dijangkiti, [Resident Shield](#) akan mengesannya dengan segera.
- **Pemesejan Segera** - membenarkan anda mengedit tetapan komponen merujuk kepada pengimbasan pemesejan segera (*cth. ICQ, MSN Messenger, Yahoo ...*).



- o Perindungan Pemesejan Segera - tandakan item ini jika anda mahukan Perisai Dalam Talian mengesahkan bahawa komunikasi dalam talian adalah bebas virus. Jika opsyen ini dihidupkan, seterusnya, anda boleh menentukan aplikasi pemesejan segera mana yang anda hendak kawal - buat masa ini **AVG 9 Internet Security** menyokong aplikasi ICQ, MSN dan Yahoo.

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

Butang kawalan

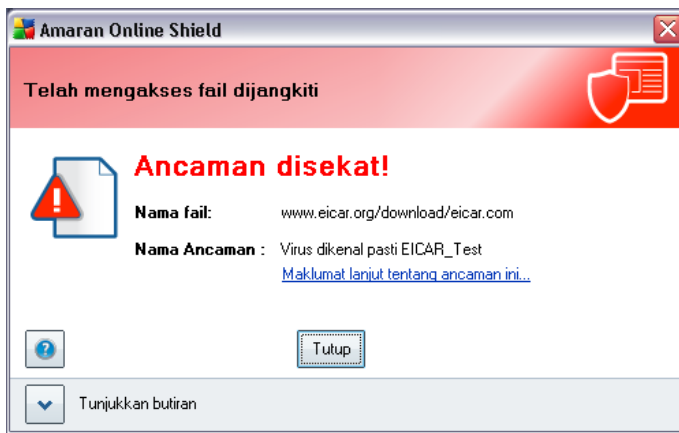
Butang kawalan tersedia dalam antara muka **Perisai Dalam Talian** adalah seperti berikut:

- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini

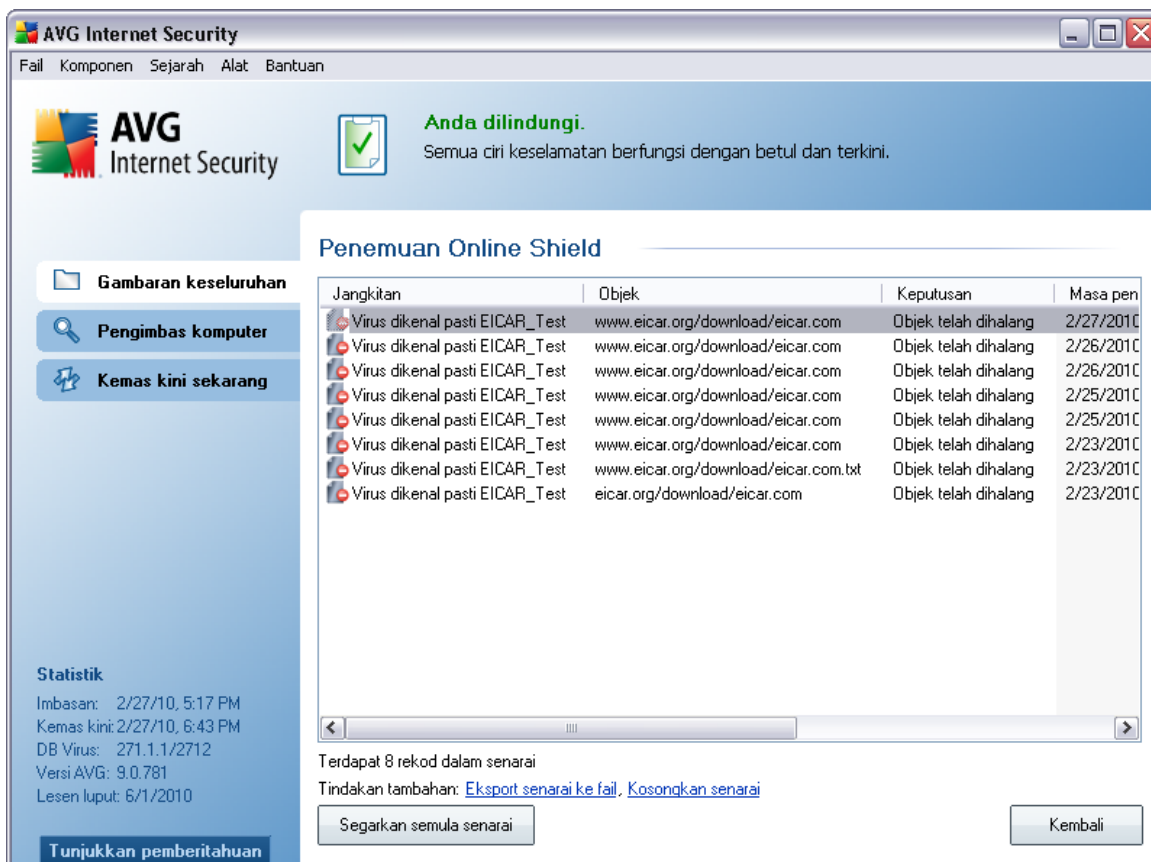
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG laai](#) (gambaran keseluruhan komponen)

8.11.3. Pengesanan Perisai Dalam Talian

Perisai Dalam Talian mengimbas kandungan halaman web yang dilawati dan kemungkinan fail termasuk dalamnya walaupun sebelum ia dipaparkan dalam penyemak imbas web atau dimuat turun ke komputer anda. Jika ancaman dikesan, anda akan diberi amaran dengan serta-merta dengan dialog berikut:



Halaman web yang disyaki tidak akan dibuka dan pengesanan ancaman akan dilog dalam senarai **penemuan Perisai Dalam Talian** - gambaran keseluruhan ini bagi ancaman dikesan boleh diakses melalui menu sistem [penemuan Sejarah / Perisai Dalam Talian](#).



Untuk setiap objek yang dikesan, maklumat berikut disediakan:

- **Jangkitan** - penerangan (*malahan juga nama*) bagi objek yang dikesan
- **Objek** - sumber objek (*halaman web*)
- **Keputusan** - tindakan dilakukan dengan objek yang dikesan
- **Pengesanan masa** - tarikh dan masa ancaman dikesan dan disekat
- **Jenis Objek** - jenis objek yang dikesan
- **Proses** - tindakan apa yang dilakukan untuk memanggil objek berpotensi berbahaya supaya ia boleh dikesan

Di bahagian bawah dialog, di bawah senarai, anda akan menemui maklumat mengenai jumlah bilangan objek dikesan yang disenaraikan di atas. Seterusnya, anda boleh

mengeksport keseluruhan senarai objek yang dikesan dalam fail (***Eksport senarai ke fail***) dan padam semua entri pada objek dikesan (***Kosongkan senarai***). Butang ***Muat semula senarai*** akan mengemas kini senarai penemuan yang dikesan oleh ***Perisai Dalam Talian***. Butang ***Kembali*** mengalihkan anda semula ke [antara muka pengguna AVG](#) (gambaran keseluruhan komponen).

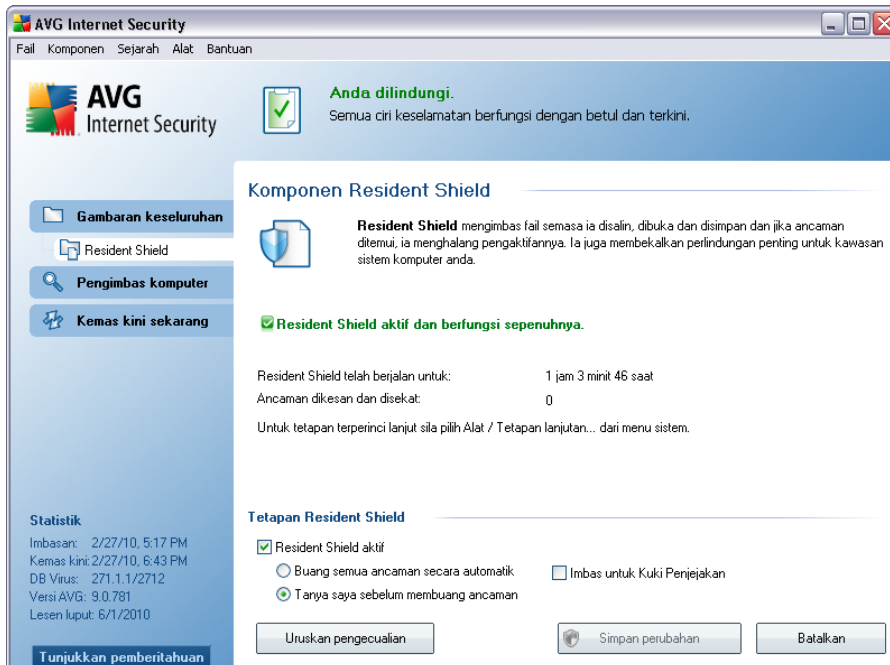
8.12. Resident Shield

8.12.1. Resident Shield Prinsip

Komponen ***Perisai Residen*** memberikan komputer anda perlindungan berterusan. Ia mengimbas setiap fail yang dibuka, disimpan, atau disalin, dan mengawal kawasan sistem komputer. Apabila ***Perisai Residen*** menemui virus dalam fail yang diakses, ia menghentikan operasi yang sedang dijalankan dan tidak membenarkan virus untuk diaktifkan dengan sendiri. Biasanya, anda langsung tidak perasan proses itu, memandangkan ia berjalan "di belakang", dan anda hanya akan diberitahu apabila ancaman ditemui; dalam masa yang sama, ***Perisai Residen*** menyekat pengaktifan ancaman dan membuangnya. ***Perisai Residen*** sedang dimuatkan dalam memori komputer anda sewaktu permulaan sistem.

Amaran: Perisai Residen dimuatkan dalam memori komputer anda semasa permulaan, dan adalah penting anda memastikannya hidup sepanjang masa!

8.12.2. Antara Muka Perisai Residen



Selain gambaran keseluruhan data statistik yang paling penting pada status semasa komponen (*Perisai Residen adalah aktif dan berfungsi sepenuhnya*), antara muka **Perisai Residen** juga menawarkan beberapa opsyen tetapan komponen permulaan. Statistik adalah seperti berikut:

- **Perisai Residen telah menjadi aktif selama** - memberikan masa sejak komponen terkini dilancarkan
- **Ancaman dikesan dan disekat** - bilangan jangkitan yang dikesan yang dielakkan daripada dijalankan/dibuka (*jika perlu, nilai ini boleh ditetapkan semula; cth. untuk tujuan statistik - Tetapkan semula nilai*)

Konfigurasi komponen asas

Dalam bahagian bawah tettingkap dialog, anda akan menemui bahagian yang dipanggil **tetapan Perisai Residen** di mana anda boleh mengedit beberapa tetapan asas bagi kefungsiannya (*konfigurasi terperinci dengan semua komponen lain tersedia melalui item tetapan Alat/Lanjutan bagi menu sistem*).

Opsyen **Perisai Residen adalah aktif** membenarkan anda menghidupkan/mematikan

perlindungan residen dengan mudah. Secara lalai, fungsi dihidupkan. Dengan perlindungan residen dihidupkan, anda seterusnya boleh menentukan cara kemungkinan jangkitan yang dikesan harus dirawat (dibuang).

- o sama ada secara automatik (***Buang semua ancaman secara automatik***)
- o atau hanya selepas kelulusan pengguna (***Tanya saya sebelum membuang ancaman***)

Pilihan ini tidak memberi kesan kepada tahap keselamatan dan ia hanya menjejaskan keutamaan anda.

Dalam kedua-dua kes, anda masih boleh memilih sama ada anda hendak **Mengimbas untuk kuki penjejakan**. Dalam kes tertentu, anda boleh mengalihkan opsyen ini kepada mendapatkan tahap keselamatan maksimum, walau bagaimanapun, ia dimatikan secara lalai. (*kuki = bungkusan teks dihantar oleh pelayan ke pelayar web dan kemudian, dihantar semula tanpa diubah oleh pelayar setiap kali ia mengakses pelayan tersebut. Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat khusus mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*).

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

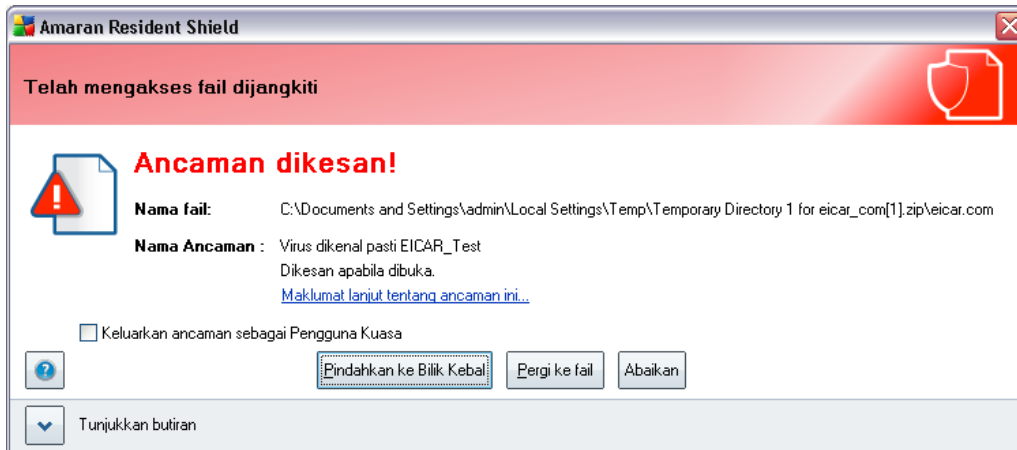
Butang kawalan

Butang kawalan tersedia dalam antara muka **Perisai Residen** seperti berikut:

- **Uruskan pengecualian** - membuka dialog [Perisai Residen - Pengecualian Direktori](#) di mana anda boleh menentukan folder yang harus ditinggalkan daripada pengimbasan [Perisai Residen](#)
- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batalan** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen)

8.12.3. Pengesanan Perisai Residen

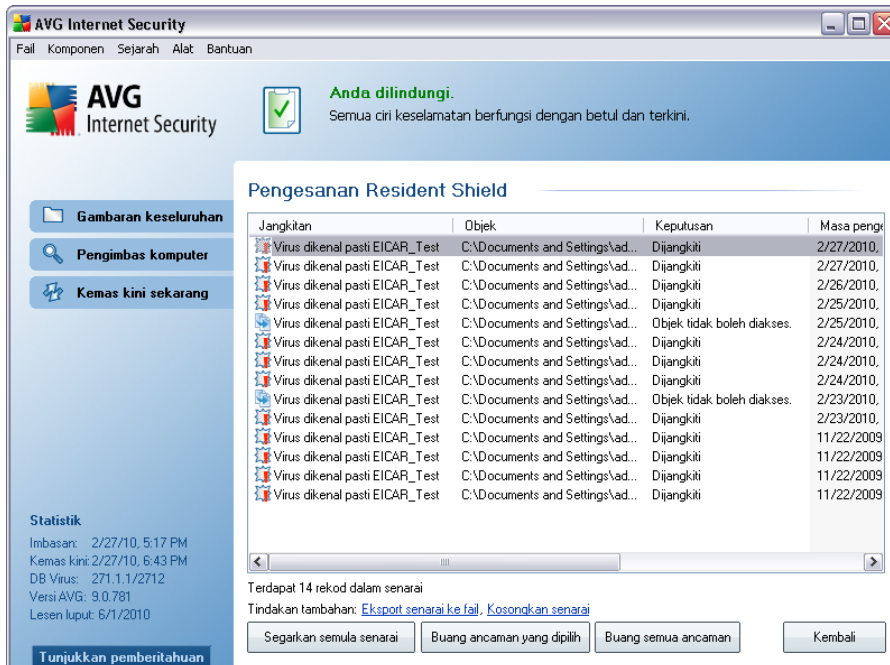
Perisai Residen mengimbas fail semasa ia disalin, dibuka atau disimpan. Apabila virus atau sebarang jenis ancaman dikesan, anda akan diberi amaran serta-merta melalui dialog berikut:



Dialog memberikan maklumat mengenai ancaman yang dikesan dan ia menjemput anda untuk menentukan tindakan apa yang harus diambil sekarang:

- **Pulih** - jika rawatan tersedia, AVG akan memulihkan fail yang dijangkiti secara automatik; opsyen ini adalah tindakan yang disarankan untuk diambil
- **Alih ke Bilik Kebal** - virus tersebut akan dialihkan ke Bilik Kebal [AVG](#)
- **Pergi ke fail** - opsyen ini mengarahkan anda semula ke lokasi sebenar bagi objek yang mencurigakan (*membuka tetingkap Windows Explorer baru*)
- **Abaikan** - kami amat menyarankan UNTUK TIDAK menggunakan opsyen ini melainkan anda mempunyai alasan yang sangat kukuh untuk melakukannya!

Gambaran keseluruhan bagi semua ancaman yang dikesan oleh **Perisai Residen** boleh ditemui dalam **pengesanan Perisai Residen** yang boleh diakses dari opsyen menu sistem [penemuan Perisai Sejarah / Residen](#):



Pengesanan Perisai Residen menawarkan gambaran keseluruhan objek yang dikesan oleh **Perisai Residen**, dinilai sebagai berbahaya dan sama ada dipulihkan atau dialihkan ke **Bilik Kebal Virus**. Untuk setiap objek yang dikesan, maklumat berikut disediakan:

- **Jangkitan** - penerangan (malahan juga nama) bagi objek yang dikesan
- **Objek** - lokasi objek
- **Keputusan** - tindakan dilakukan dengan objek yang dikesan
- **Masa pengesanan** - tarikh dan masa objek dikesan
- **Jenis Objek** - jenis objek yang dikesan
- **Proses** - tindakan apa yang dilakukan untuk memanggil objek berpotensi berbahaya supaya ia boleh dikesan

Di bahagian bawah dialog, di bawah senarai, anda akan menemui maklumat mengenai jumlah bilangan objek dikesan yang disenaraikan di atas. Seterusnya, anda boleh mengeksport keseluruhan senarai objek yang dikesan dalam fail (**Eksport senarai ke fail**) dan padam semua entri pada objek dikesan (**Kosongkan senarai**). Butang **Muat semula senarai** akan mengemas kini senarai penemuan yang dikesan oleh **Perisai Residen**. Butang **Kembali** mengalihkan anda semula ke **antara muka pengguna AVG**.



(gambaran keseluruhan komponen).

8.13. Pengurus Kemas Kini

8.13.1. Kemas Kini Prinsip Pengurus

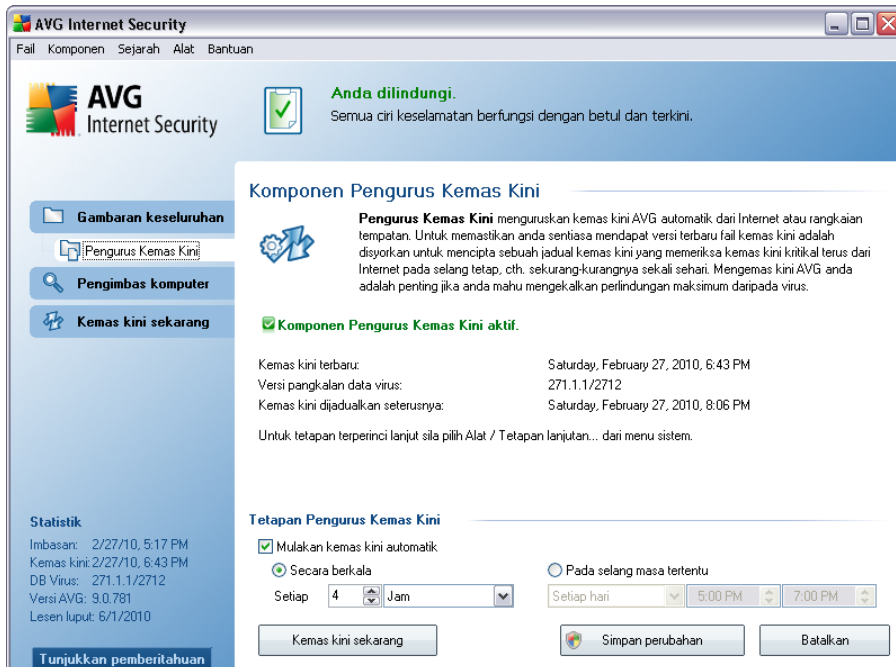
Tiada perisian keselamatan yang boleh menjamin perlindungan sebenar dari pelbagai jenis ancaman melainkan ia dikemas kini secara tetap! Penulis virus sentiasa mencari kecelehan baru yang mereka boleh mengeksploitasi dalam perisian dan juga sistem pengendalian. Virus baru, malware baru, serangan penggadam baru muncul setiap hari. Oleh itu, vendor perisian berterusan mengeluarkan kemas kini dan tampalan keselamatan untuk membaiki sebarang lubang keselamatan yang didapati.

Adalah penting untuk mengemas kini AVG anda secara tetap!

Pengurus Kemas Kini membantu anda mengawal kemas kini tetap. Dalam komponen ini, anda boleh menjadualkan muat turun automatik bagi fail kemas kini sama ada dari Internet atau rangkaian tempatan. Kemas kini definisi virus penting patut dilakukan setiap hari, jika boleh. Kemas kini atur cara yang kurang penting boleh dilakukan setiap minggu.

Nota: Sila berikan perhatian kepada bab [Kemas Kini AVG](#) untuk maklumat lanjut mengenai jenis dan tahap kemas kini!

8.13.2. Kemas Kini Antara Muka Pengurus



Antara muka **Pengurus Kemas Kini** memaparkan maklumat mengenai kefungsiannya, komponen dan status semasanya (*Pengurus kemas kini adalah aktif.*), dan memberikan data statistik yang relevan:

- **Kemas kini terkini** - menentukan bila dan dalam masa bila pangkalan data dikemas kini
- **Versi pangkalan data virus** - menentukan bilangan versi pangkalan data virus terkini; dan nombor ini meningkat dengan setiap kemas kini pangkalan data virus
- **Kemas kini yang dijadualkan seterusnya** - menentukan bila dan masa pangkalan data dijadualkan untuk dikemas kini semula

Konfigurasi komponen asas

Di bahagian bawah dialog, anda boleh menemui bahagian **tetapan Pengurus Kemas Kini** di mana anda boleh melakukan beberapa perubahan kepada peraturan pelancaran proses kemas kini. Anda boleh mentakrifkan sama ada anda mahukan fail kemas kini dimuat turun secara automatik (**Mulakan kemas kini automatik**) atau hanya dalam permintaan. Secara lalai, opsiyen **Mulakan kemas kini automatik** dihidupkan dan kami

mengesyorkan untuk mengekalkannya! Muat turun tetap bagi fail kemas kini terkini adalah penting untuk kefungsiian yang betul bagi sebarang perisian keselamatan!

Seterusnya, anda boleh menentukan bila kemas kini patut dilancarkan:

- o **Secara berkala** - tentukan selang masa
- o **Dalam masa khusus** - tentukan hari dan masa sebenar

Secara lalai, kemas kini ditetapkan pada setiap 4 jam. Ia amat disyorkan untuk mengekalkan tetapan ini melainkan anda mempunyai alasan yang betul untuk mengubahnya!

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

Butang kawalan

Butang kawalan yang tersedia dalam antara muka **Pengurus Kemas Kini** adalah seperti berikut:

- **Kemas kini sekarang** - melancarkan [kemas kini segera](#) dalam permintaan
- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen)



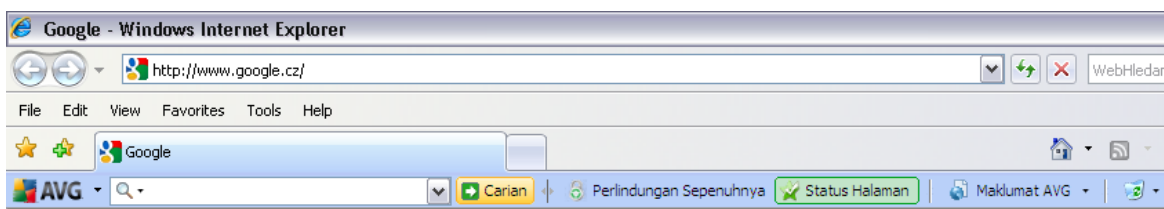
9. AVG Security Toolbar

AVG Security Toolbar adalah alat baru yang berfungsi bersama dengan komponen **AVG Link Scanner** dan memeriksa keputusan carian bagi enjin carian Internet yang disokong (*Yahoo!, Google, Bing, Altavista, Baidu*). **AVG Security Toolbar** boleh digunakan untuk mengawal fungsi **AVG Link Scanner** dan untuk mengubah suai kelakuannya.

Jika anda memilih untuk memasang bar alat sewaktu pemasangan **AVG 9 Internet Security**, ia akan ditambah ke dalam penyemak imbas web anda secara automatik. Jika anda menggunakan beberapa penyemak imbas Internet alternatif (*cth. Avant Browser*) anda boleh menemui kelakuan yang tidak dijangka.

9.1. AVG Security Toolbar Antara muka

AVG Security Toolbar direka bentuk untuk bekerja dengan **MS Internet Explorer** (versi 6.0 atau lebih terkini) dan **Mozilla Firefox** (versi 2.0 atau lebih terkini). Sebaik sahaja anda telah memutuskan anda hendak memasang **AVG Security Toolbar** (sewaktu [proses pemasangan AVG](#) anda diminta untuk memutuskan sama ada anda hendak memasang komponen atau tidak), komponen akan terletak dalam penyemak imbas web anda betul-betul di bawah bar alat:



Nota: *AVG Security Toolbar bukan disasarkan untuk platform pelayan!*

AVG Security Toolbar terdiri daripada yang berikut:

- **logo AVG** - memberikan akses kepada item bar alat umum. Klik butang logo untuk diarahkan semula ke tapak web (<http://www.avg.com/>). Dengan mengklik penuding di sebelah ikon AVG akan membuka yang berikut:
 - o **Maklumat Bar Alat** - pautan kepada halaman utama **AVG Security Toolbar dengan maklumat terperinci mengenai perlindungan bar alat**
 - o **Lancarkan AVG 9 Internet Security** - membuka antara muka pengguna **AVG 9 Internet Security**

- o **Opsyen** - membuka dialog konfigurasi di mana anda boleh mengubah suai tetapan **AVG Security Toolbar** untuk disesuaikan dengan keperluan anda
- lihat bab berikut [Opsyen AVG Security Toolbar](#)
- o **Padam Sejarah** - membenarkan anda *Memadam sejarah yang lengkap* bagi AVG Security Toolbar, atau untuk *Memadam sejarah carian*, *Memadam sejarah pelayar* dan *Padam kuki*.
- o **Kemas kini** - memeriksa untuk kemas kini baru untuk **AVG Security Toolbar anda**
- o **Bantuan** - memberikan pilihan untuk membuka fail bantuan, menyerahkan maklum balas produk, atau melihat butiran versi terkini bagi bar alat
- **Kotak carian** - Masukkan perkataan atau ungkapan ke dalam kotak carian. Tekan **Cari** untuk mula mencari menggunakan enjin carian yang ditentukan (anda boleh menentukan enjin carian yang dikehendaki untuk digunakan dalam [Pilihan Lanjutan AVG Security Toolbar](#), dan anda boleh memilih sama ada Yahoo!, Wikipedia, Baidu, WebHledani atau Yandex), tidak kira halaman apa yang sedang dipaparkan. Kotak carian juga menyenaraikan sejarah carian anda. Carian dilakukan melalui kotak carian dianalisis menggunakan perlindungan [AVG Search-Shield](#).
- **Perlindungan Menyeluruh** - butang ini muncul secara pilihan sebagai sama ada **Perlindungan Menyeluruh / Perlindungan Terhadap / Tiada Perlindungan** bergantung pada **AVG 9 Internet Security** konfigurasi
- **Status Halaman** - secara terus dalam bar alat, butang ini memaparkan penilaian bagi halaman web yang sedang dimuat naik berasaskan kriteria bagi komponen [AVG Search-Shield](#) (halaman adalah selamat / mencurigakan / berbahaya secara positif / mengandungi ancaman / tidak boleh diimbis). Klik butang untuk membuka panel maklumat dengan data terperinci pada halaman web khusus.
- **Maklumat AVG** - memberikan pautan kepada maklumat keselamatan penting yang terletak pada tapak web AVG (<http://www.avg.com/>).
 - o **Maklumat Bar Alat** - pautan kepada halaman utama **AVG Security Toolbar dengan maklumat terperinci mengenai perlindungan bar alat**
 - o **Mengenai ancaman** - membuka halaman web AVG memberikan maklumat mengenai virus dan ancaman terkini pada Internet

- o **AVG News** - membuka halaman web memberikan keluaran berita berkaitan AVg yang terkini
- o **Tahap Ancaman Semasa** - membuka halaman web lab virus dengan paparan grafik bagi tahap ancaman semasa pada web
- o **Ensiklopedia Virus** - membuka halaman Ensiklopedia Virus di mana anda boleh mencari virus khusus melalui nama dan mendapatkan maklumat terperinci bagi setiap satu

9.2. Opsyen AVG Security Toolbar

Semua konfigurasi parameter **AVG Security Toolbar** boleh diakses secara terus dalam panel **AVG Security Toolbar**. Antara muka pengeditan terbuka melalui item menu bar alat **AVG / Pilihan** dalam dialog baru yang dipanggil **Pilihan Bar Alat** yang dibahagikan ke dalam empat bahagian:

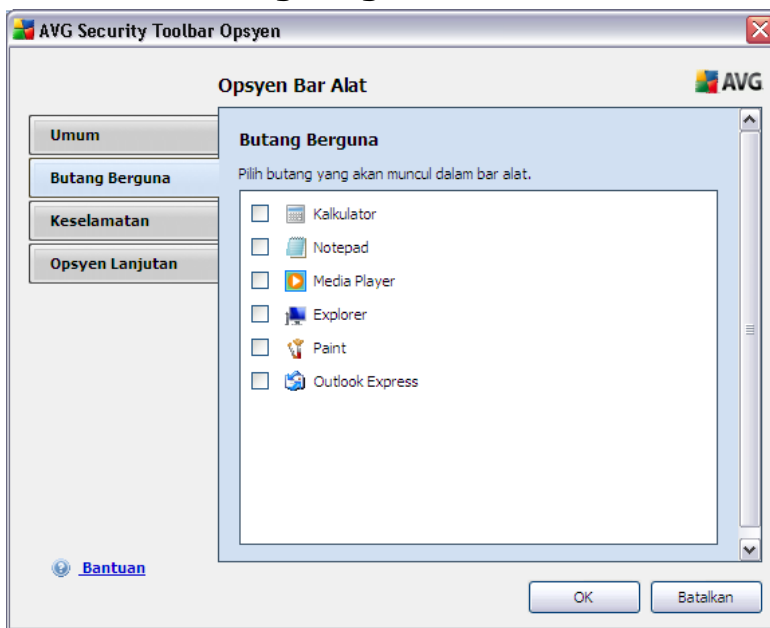
9.2.1. Tab Umum



Pada tab ini anda boleh menentukan butang yang harus dipaparkan / tersembunyi dalam panel **AVG Security Toolbar**. Tandakan sebarang pilihan jika anda mahukan butang masing-masing dipaparkan. Seterusnya, terangkan kegunaan setiap butang bar alat:

- **AVG News Button** - butang membuka halaman web memberikan keluaran berita berkaitan AVG yang terkini
- **News Button** - butang memberikan gambaran keseluruhan berita terkini daripada berita harian
- **AVG Info Button** - butang menawarkan maklumat mengenai bar alat AVG, mengenai ancaman terkini dan tahap ancaman internet, membuka ensiklopedia virus dan memberikan lebih banyak produk AVG berkaitan berita
- **Padam Butang Sejarah** - butang ini membolehkan anda Memadam sejarah lengkap, atau Memadam sejarah carian, Memadam sejarah pelayar, Memadam sejarah muat turun, atau Padam kuki secara terus dari panel AVG Security Toolbar.

9.2.2. Tab Butang Berguna



Tab **Butang Berguna** membenarkan anda memilih aplikasi daripada senarai dan memaparkan ikonnya dalam antara muka bar alat. Ikon tersebut kemudiannya bertindak sebagai pautan pantas membolehkan untuk melancarkan aplikasi masing-masing dengan segera.

9.2.3. Tab Keselamatan



Tab **Keselamatan** dibahagikan ke dalam dua bahagian, **AVG Browser Security** dan **Pengadaran**, di mana anda boleh menanda kotak semakan tertentu untuk menguntukkan kefungsiian **AVG Security Toolbar** yang anda hendak gunakan:

- **AVG Browser Security** - tandakan item ini untuk mengaktifkan atau mematikan perkhidmatan **AVG Search-Shield** dan/atau **AVG Active Surf-Shield**
- **Rating** - pilih simbol grafik yang digunakan untuk rating hasil carian melalui komponen **AVG Search-Shield** yang anda hendak gunakan:

- o  halaman adalah selamat
- o  halaman agak mencurigakan
- o  halaman mengandungi pautan kepada halaman berbahaya secara positif
- o  halaman mengandungi ancaman aktif
- o  halaman tidak boleh diakses, maka, tidak boleh diimbis

Tandakan opsyen masing-masing untuk mengesahkan anda mahu diberitahu mengenai tahap ancaman tertentu ini. Walau bagaimanapun, paparan tanda merah yang diperuntukkan kepada halaman yang mengandungi ancaman aktif dan berbahaya tidak boleh dimatikan. ***Sekali lagi, ia disyorkan untuk mengekalkan konfigurasi lalai yang ditetapkan oleh vendor atur cara melainkan anda mempunyai sebab sebenar untuk mengubahnya.***

9.2.4. Tab Pilihan Lanjutan



Pada tab **Pilihan Lanjutan** pertama sekali, pilih enjin carian yang anda hendak gunakan sebagai lalai. Anda mempunyai pilihan *Yahoo!*, *Baidu*, *WebHledani* dan *Yandex*. Setelah menukar enjin carian lalai, sila mulakan semula penyemak imbas internet anda untuk perubahan berkesan.

Seterusnya, anda boleh mengaktifkan atau mematikan tetapan khusus **AVG Security Toolbar** selanjutnya:

- ***Tetapkan dan kekalkan Yahoo! sebagai pembekal carian untuk bar Alamat*** - (*dihidupkan secara lalai*) - jika ditandakan, opsyen ini membenarkan anda menaip kata kunci carian secara terus ke dalam bar alamat ke dalam pelayar Internet anda dan Yahoo! akan digunakan secara automatik untuk mencari tapak web yang relevan.
- ***Benarkan AVG membuat cadangan mengenai ralat navigasi penyemak***

imbis (404/DNS) - (*dihidupkan secara lalai*) - jika semasa mencari web, anda menemui halaman tidak wujud atau halaman tidak boleh dipaparkan (ralat 404), anda akan diarahkan semula secara automatik ke halaman web yang membenarkan anda memilih daripada gambaran keseluruhan halaman alternatif berkaitan topik.

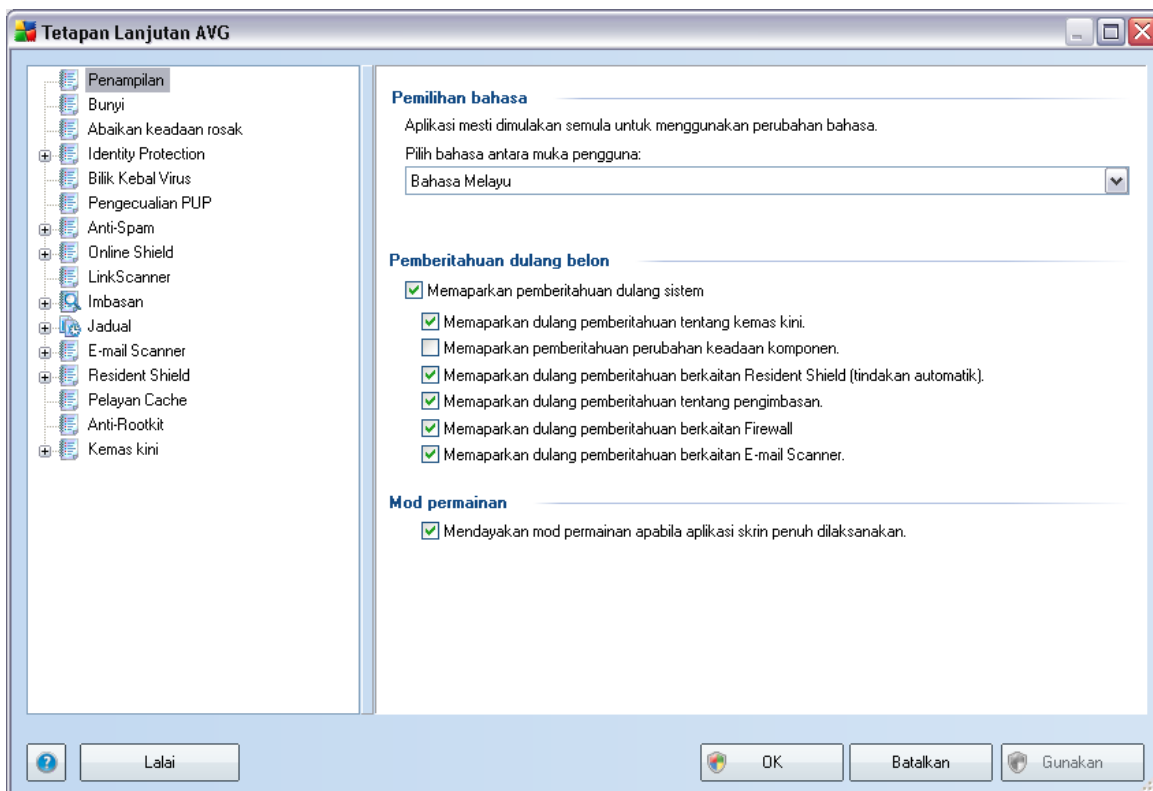
- **Tetapkan dan kekalkan Yahoo! sebagai pembekal carian untuk pelayar anda** - (*dimatikan secara lalai*) - Yahoo! adalah enjin carian lalai untuk carian web dalam AVG Security Toolbar, mengaktifkan opsyen ini, ia juga boleh menjadi enjin carian lalai pelayar web.
- **Paparkan semula AVG Security Toolbar apabila tersembunyi (mingguan)** - (*dihidupkan secara lalai*) - opsyen ini adalah aktif secara lalai dan apabila **AVG Security Toolbar** anda tersembunyi secara tidak sengaja, ia akan memaparkannya semula dalam tempoh masa satu minggu.

10. Tetapan Lanjutan AVG

Dialog konfigurasi lanjutan **AVG 9 Internet Security** terbuka dalam tetingkap baru yang dinamakan **Tetapan AVG Lanjutan**. Tetingkap dibahagikan kepada dua bahagian: bahagian kiri menawarkan navigasi pepohon yang diatur ke opsyen konfigurasi atur cara. Pilih komponen yang anda hendak ubah konfigurasi bagi (*atau bahagian tertentu*) untuk membuka dialog pengeditan dalam bahagian kanan tetingkap.

10.1. Penampilan

Item pertama bagi pepohon navigasi, **Penampilan**, merujuk kepada tetapan umum bagi [antara muka pengguna AVG](#) dan beberapa pilihan permulaan bagi kelakuan aplikasi:

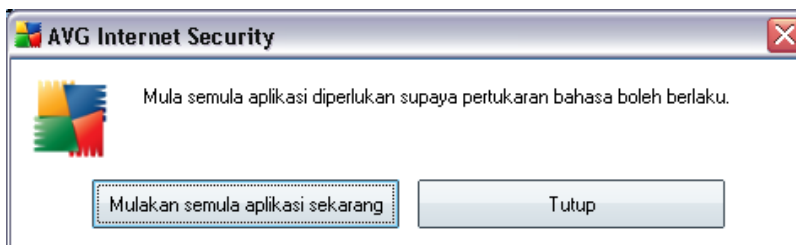


Pemilihan bahasa

Dalam bahagian **Pemilihan bahasa** anda boleh memilih bahasa yang anda kehendaki dari menu jatuh ke bawah; kemudian, bahasa tersebut akan digunakan untuk

keseluruhan [antara muka pengguna AVG](#). Menu jantai turun hanya menawarkan bahasa yang anda telah pilih sebelum ini untuk dipasang sewaktu [proses pemasangan](#) (lihat bab [Pemasangan Tersuai - Pemilihan Komponen](#)). Walau bagaimanapun, untuk selesai menukar aplikasi ke bahasa lain, anda perlu memulakan semula antara muka pengguna; ikuti langkah ini:

- Pilih bahasa aplikasi yang dikehendaki dan sahkan pemilihan anda dengan menekan butang **Guna** (penjuru bawah kanan)
- Tekan butang **OK** untuk mengesahkan
- Pop timbul tettingkap dialog baru memberitahu anda perubahan bahasa antara muka pengguna AVG memerlukan mula semula aplikasi:



Pemberitahuan dulang belon

Dalam bahagian ini, anda boleh menghimpit paparan pemberitahuan belon dulang sistem pada status aplikasi. Secara lalai, pemberitahuan belon boleh dipaparkan dan ia disarankan untuk mengekalkan konfigurasi ini! Pemberitahuan belon biasanya memberitahu mengenai beberapa perubahan status komponen AVG dan anda harus memberikan perhatian kepadanya!

Walaupun bagaimanapun, jika beberapa alasan yang anda tentukan untuk tidak dipaparkan pemberituannya atau anda hendak hanya pemberitahuan tertentu (berkaitan dengan komponen AVG khusus) dipaparkan, anda boleh mentakrifkan dan menentukan keutamaan anda dengan menanda/tidak menanda opsyen berikut:

- **Paparkan pemberitahuan dulang sistem** - secara lalai, item ini ditandakan (*dihidupkan*), dan pemberitahuan dipaparkan. Nyahtanda item ini untuk mematikan sepenuhnya semua paparan pemberitahuan belon. Semasa dihidupkan, anda seterusnya boleh memilih pemberitahuan khusus mana yang harus dipaparkan:
 - **Paparkan pemberitahuan dulang mengenai [kemas kini](#)** - tentukan sama ada maklumat berkenaan pelancaran proses, perkembangan dan

penyelesaian kemas kini AVG harus dipaparkan;

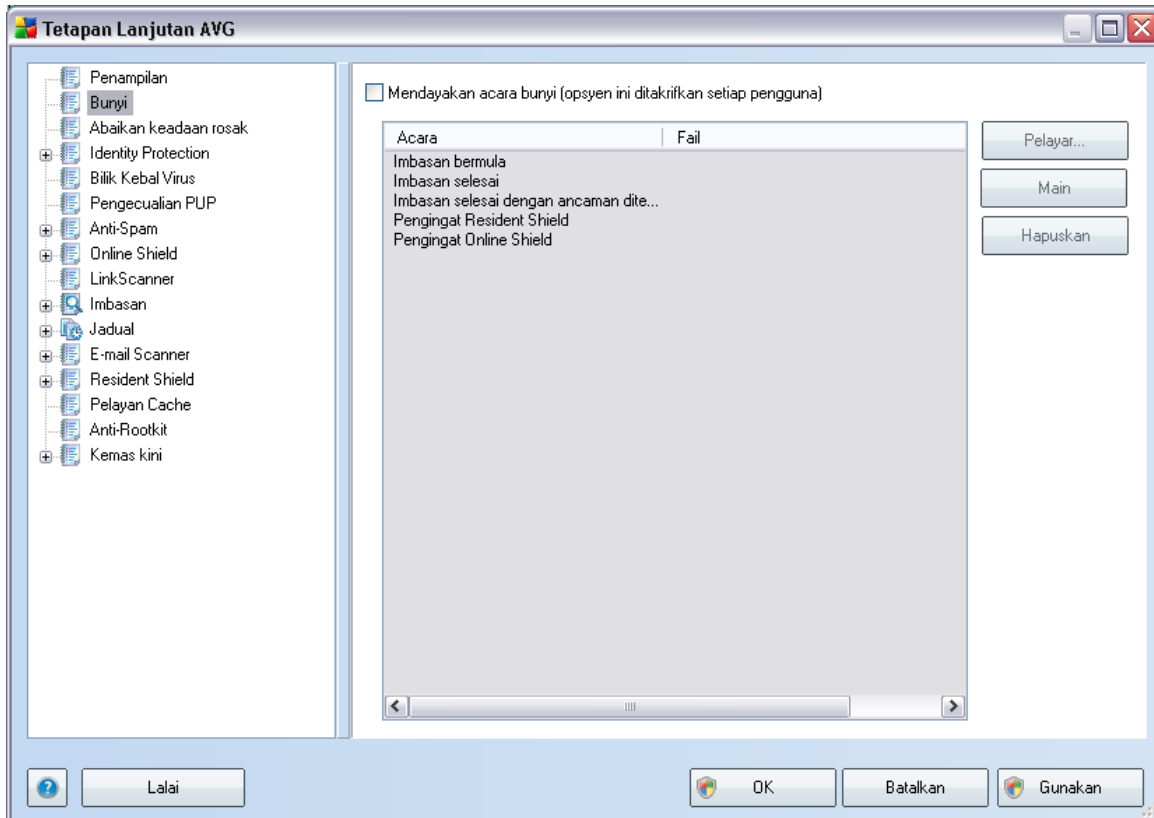
- o **Paparkan pemberitahuan perubahan keadaan komponen** - tentukan sama ada maklumat berkenaan keaktifan/ketidakaktifan komponen atau kemungkinan masalahnya harus dipaparkan. Semasa melaporkan status kerosakan komponen, opsyen ini sama dengan fungsi berguna bagi [ikon dulang sistem](#) (perubahan warna) melaporkan sebarang masalah dalam sebarang komponen AVG;
- o **Paparkan pemberitahuan dulang berkaitan [Perisai Residen](#)** - memutuskan sama ada maklumat berkenaan proses penyimpanan, penyalinan dan pembukaan fail harus dipaparkan atau disekat (*konfigurasi ini hanya menunjukkan jika pilihan [Autopulih](#) Perisai Residen dihidupkan*);
- o **Paparkan pemberitahuan dulang mengenai [pengimbasan](#)** - tentukan sama ada maklumat pada pelancaran automatik bagi imbasan yang dijadualkan, perkembangan dan keputusannya harus dipaparkan;
- o **Paparkan [Firewall](#) berkaitan pemberitahuan dulang** - tentukan sama ada maklumat berkenaan status dan proses Firewall, cth. amaran pengaktifan/penyahaktifan komponen, kemungkinan sekatan lalu lintas dll. harus dipaparkan;
- o **Paparkan [Pengimbas E-mel](#) pemberitahuan dulang berkaitan** - tentukan sama ada maklumat mengenai pengimbasan semua mesej e-mel masuk dan keluar harus dipaparkan.

Mod permainan

Fungsi AVG ini direka bentuk untuk aplikasi skrin penuh di mana kemungkinan belon maklumat AVG (*dipaparkan cth. apabila imbasan yang dijadualkan dimulakan*) akan mengganggu (*ia boleh meminimumkan aplikasi atau merosakkan grafiknya*). Untuk mengelakkan situasi ini, pastikan kotak semakan untuk pilihan **Dayakan mod permainan semasa aplikasi skrin penuh dijalankan** ditandakan (*tetapan lalai*).

10.2. Bunyi

Dalam dialog **Bunyi** anda boleh menentukan sama ada anda hendak memberitahu mengenai tindakan AVG tertentu melalui pemberitahuan bunyi. Jika yang demikian, tandakan opsyen **Dayakan peristiwa bunyi** (*dimatikan secara lalai*) untuk mengaktifkan senarai tindakan AVG:

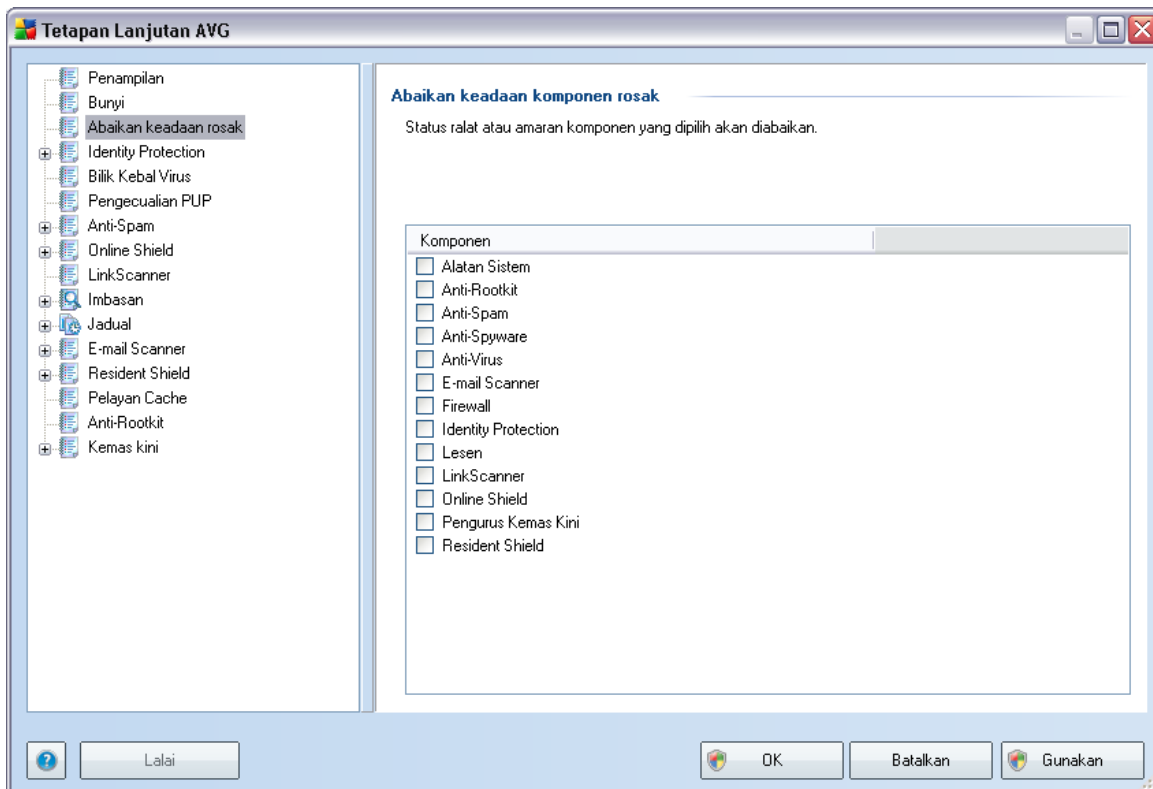


Kemudian, pilih peristiwa tersebut daripada senarai dan semak imbas (**Semak imbas**) cakra anda untuk bunyi yang sesuai yang anda hendak peruntukkan kepada peristiwa ini. Untuk mendengar bunyi yang dipilih, serlahkan peristiwa dalam senarai dan tekan butang **Main**. Gunakan butang **Padam** untuk membuang bunyi yang diperuntukkan kepada peristiwa tertentu.

Nota: Hanya bunyi *.wav yang disokong!

10.3. Abaikan Keadaan Rosak

Dalam dialog **Abaikan keadaan komponen rosak** anda boleh menanda rait komponen yang anda tidak mahu diberitahu:



Secara lalai, tiada komponen yang dipilih dalam senarai ini. Ia bermaksud bahawa jika sebarang komponen mendapat status ralat, anda akan diberitahu mengenainya dengan serta-merta melalui:

- **ikon dulang sistem** - semasa semua bahagian AVG bekerja dengan betul, ikon dipaparkan dalam empat warna; walau bagaimanapun, jika ralat berlaku, ikon muncul dengan tanda seruan berwarna kuning,
- penerangan teks bagi masalah sedia ada dalam bahagian **Maklumat Status Keselamatan** bagi tettingkap utama AVG

Mungkin terdapat situasi bagi sesetengah sebab anda perlu mematikan komponen secara sementara (*ini tidak disarankan, anda harus cuba memastikan semua komponen kekal dihidupkan dan dalam konfigurasi lalai, tetapi ia boleh berlaku*). Dalam

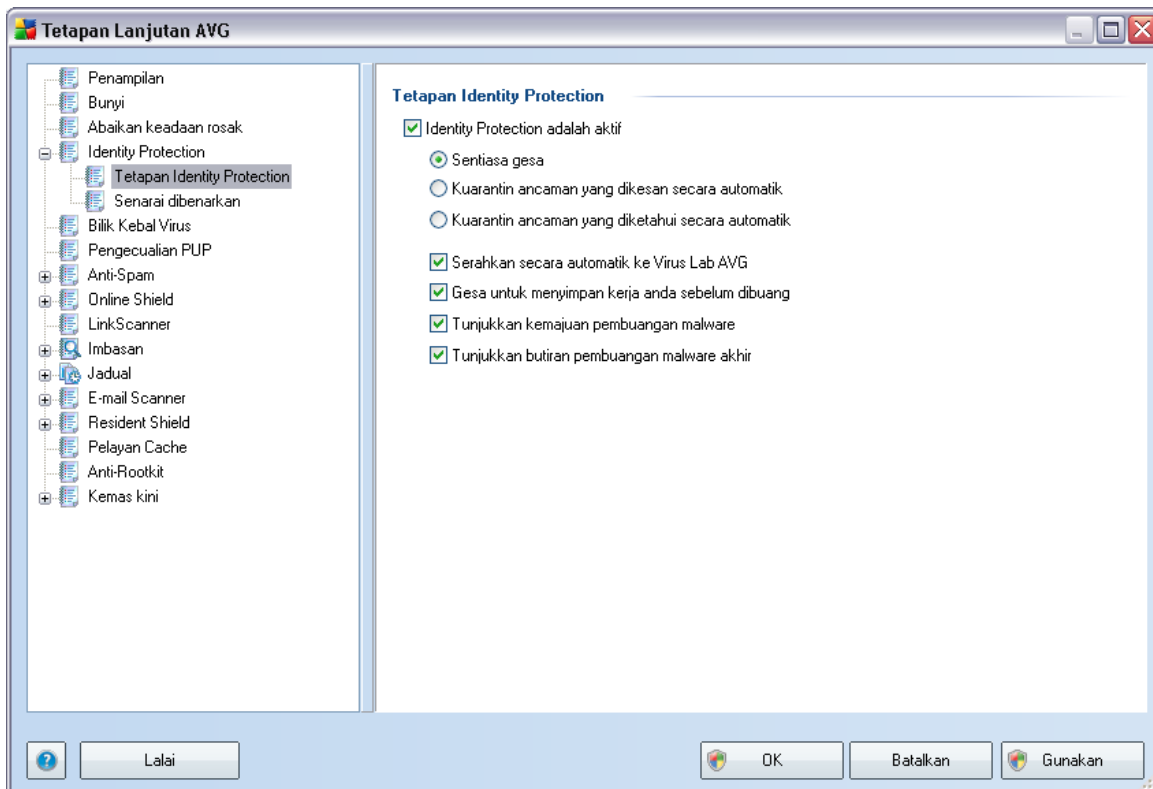
kes itu, ikon dulang sistem secara automatik melaporkan status ralat komponen. Walau bagaimanapun, dalam kes ini, kita tidak dapat bercakap mengenai ralat sebenar memandangkan anda telah mencetuskannya dengan sengaja dan anda mengetahui kemungkinan risiko. Pada masa yang sama, apabila dipaparkan dalam warna kelabu, ikon sebenarnya tidak boleh melaporkan sebarang kemungkinan ralat selanjutnya yang mungkin berlaku.

Untuk situasi ini, dalam dialog di atas, anda boleh memilih komponen yang mungkin berada dalam keadaan ralat (*atau dimatikan*) dan anda tidak mahu diberitahu mengenainya. Opsyen yang sama bagi **Mengabaikan keadaan komponen** juga tersedia untuk komponen tertentu secara terus dari gambaran keseluruhan [komponen dalam tetingkap utama AVG](#).

10.4. Perlindungan Identiti

10.4.1. Tetapan Perlindungan Identiti

Dialog **tetapan Perlindungan Identiti** membenarkan anda menghidupkan/mematikan ciri permulaan bagi komponen **Perlindungan Identiti**:



Perlindungan Identiti adalah aktif (dihidupkan secara lalai) – jangan tandakan untuk mematikan komponen ***Perlindungan Identiti***.

Kami amat mengesyorkan jangan melakukan ini kecuali anda terpaksa!

Apabila ***Perlindungan Identiti*** diaktifkan, anda boleh menentukan apa yang perlu dilakukan apabila ancaman dikesan:

- ***Sentiasa gesa (dihidupkan secara lalai)*** - apabila ancaman dikesan, anda akan ditanya sama ada ia harus dialihkan ke kuarantin untuk memastikan tiada aplikasi yang anda hendak jalankan dibuang.
- ***Kuarantin ancaman dikesan secara automatik*** - tandakan kotak semakan ini untuk mentakrifkan anda hendak semua kemungkinan ancaman dikesan

dibuang ke tempat yang selamat bagi [**Bilik Kebal Virus AVG**](#) dengan segera. Mengekalkan tetapan lalai apabila ancaman dikesan, anda akan ditanya sama ada ia harus dialihkan ke kuarantin untuk memastikan tiada aplikasi yang anda hendak jalankan dibuang.

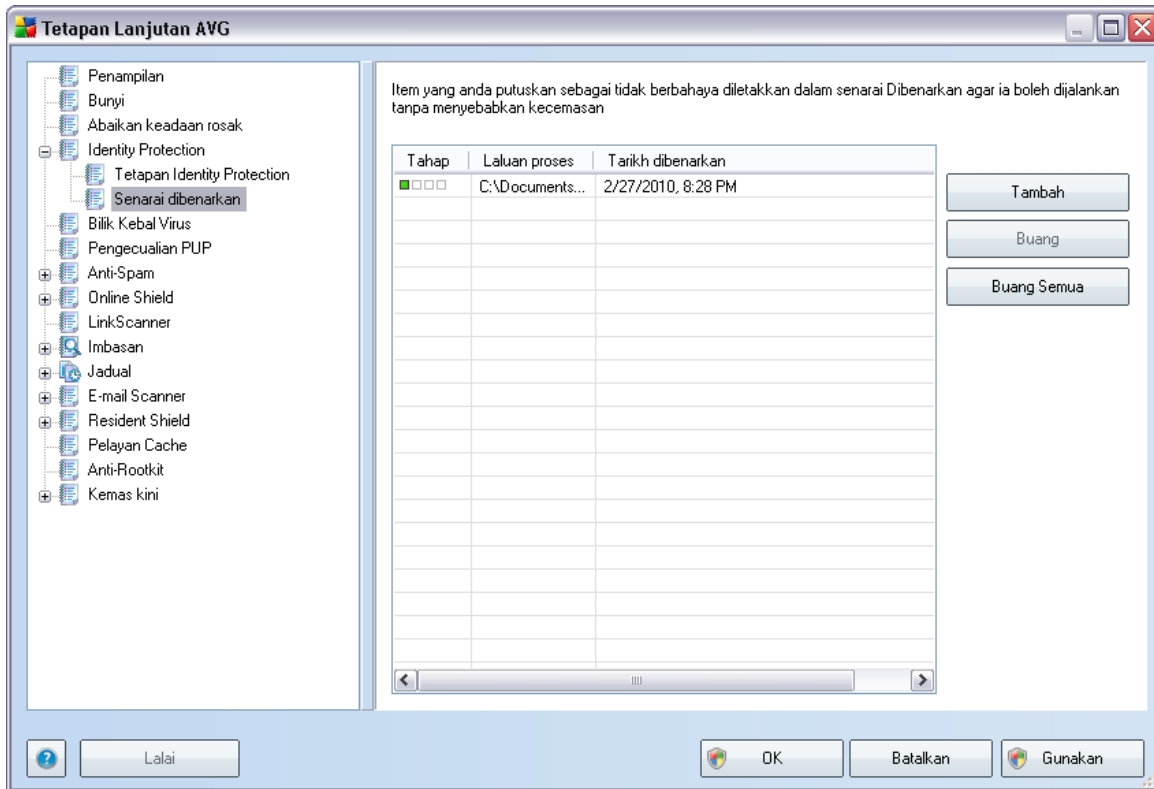
- **Kuarantin ancaman diketahui secara automatik** - biarkan item ini ditanda jika anda hendak semua aplikasi dikesan sebagai kemungkinan malware untuk dialihkan secara automatik dan dengan serta merta ke [**Bilik Kebal Virus AVG**](#).

Seterusnya, anda boleh menguntukkan item tertentu untuk secara pilihan, mengaktifkan lebih kefungsiian **Perlindungan Identiti** :

- **Serahkan kepada AVG Virus Lab secara automatik** - (dihidupkan secara lalai): Sila biarkan kotak semakan ini ditandakan untuk menyuap maklumat pengumpulan pangkalan data mengenai aktiviti berniat jahat pada web dan untuk membantu kami mengenal pasti ancaman baru.
- **Gesa untuk menyimpan kerja anda sebelum pengeluaran** - (dihidupkan secara lalai) - pastikan item ini ditanda jika anda hendak diberi amaran sebelum aplikasi dikesan sebaik sahaja malware dikeluarkan ke kuarantin. Jika anda hanya bekerja dengan aplikasi tersebut, projek anda mungkin hilang dan anda perlu menyimpannya dahulu. sangat mengesyorkan
- **Tunjukkan perkembangan pembuangan malware** - (dihidupkan secara lalai) - dengan item ini dihidupkan, sebaik sahaja kemungkinan malware dikesan, dialog baru terbuka untuk memaparkan perkembangan malware dibuang ke kuarantin.
- **Tunjukkan perkembangan pembuangan malware** - (dihidupkan secara lalai) - dengan item ini dihidupkan, **Perlindungan Identiti** memaparkan maklumat terperinci mengenai setiap objek yang digerakkan ke kuarantin (*tahap keterukan, lokasi ,dll.*).

10.4.2. Senarai dibenarkan

Jika dalam dialog **tetapan Perlindungan Identiti** anda memutuskan untuk mengekalkan item **Kuarantin ancaman yang dikesan secara automatik** tidak ditandakan, setiap kali kemungkinan malware yang berbahaya dikesan, anda akan ditanya sama ada ia harus dibuang. Jika kemudian, anda menguntukkan bahawa aplikasi mencurigakan (*dikesan berasaskan pada kelakuannya*) sebagai selamat dan anda mengesahkannya patut disimpan pada komputer anda, aplikasi akan ditambah pada yang dipanggil **Senarai dibenarkan**, dan ia tidak akan dilaporkan sebagai berpotensi berbahaya lagi:



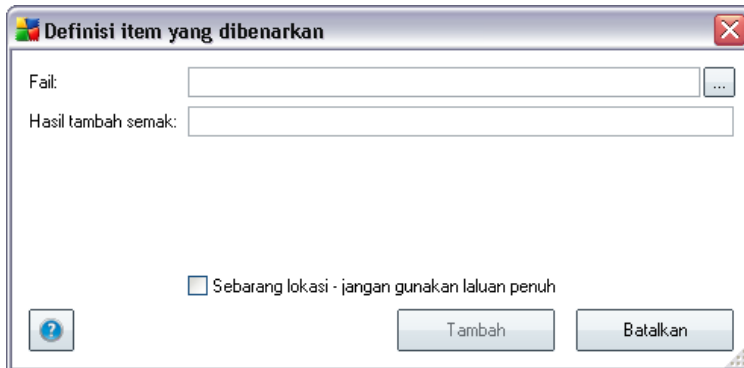
Senarai dibenarkan memberikan maklumat berikut pada setiap aplikasi:

- **Tahap** - pengenalpastian grafik bagi keseriusan proses masing-masing pada skala empat tahap daripada (■□□□) yang kurang kritikal kepada (■■■■ yang kritikal)
- **Laluan proses** - laluan kepada lokasi fail boleh laku (*proses*) aplikasi
- **Tarikh yang dibenarkan** - tarikh apabila anda menguntukkan aplikasi sebagai selamat secara manual

Butang kawalan

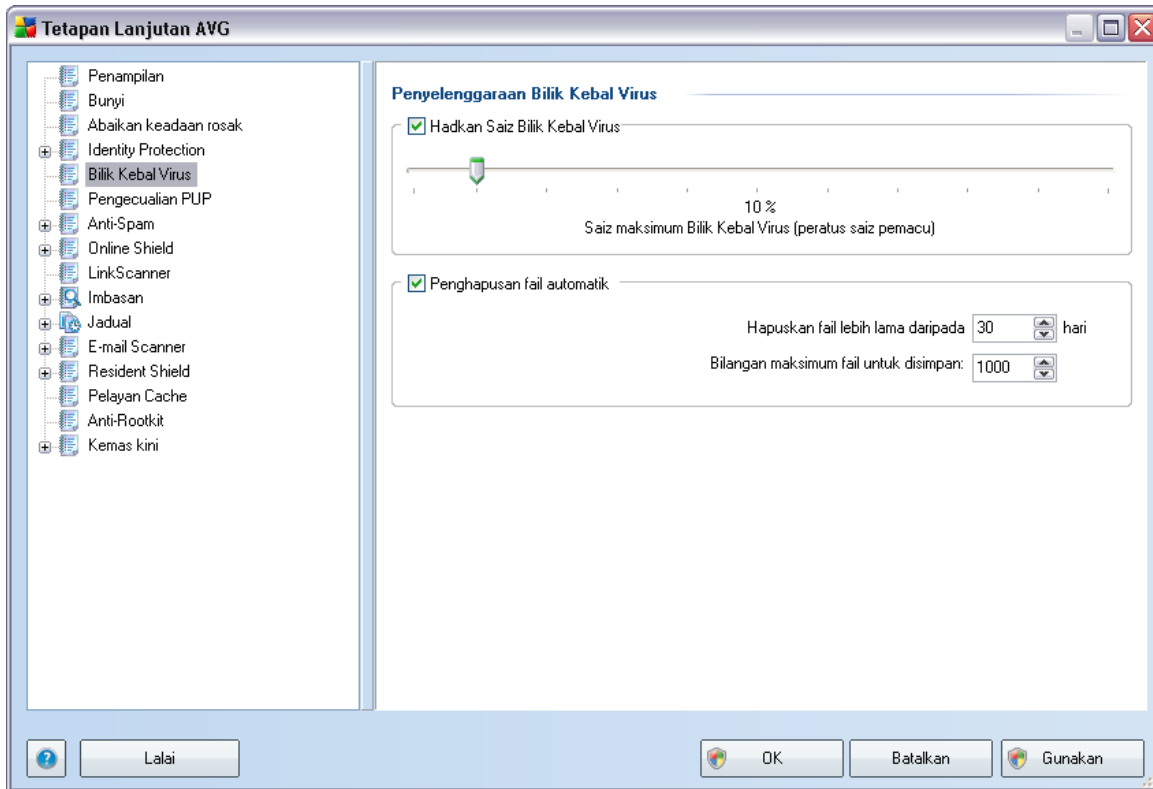
Butang kawalan yang tersedia dalam dialog **Senarai yang dibenarkan** adalah seperti berikut:

- **Tambah** - tekan butang ini untuk menambah aplikasi baru ke senarai yang dibenarkan. Pop timbul dialog yang berikutnya:



- o **Fail** - taipkan laluan penuh ke fail (*aplikasi*) yang anda hendak tandakan sebagai pengecualian
- o **Hasil tambah semak** - memaparkan 'tandatangan' unik bagi fail yang dipilih. Hasil tambah semak ini adalah rentetan aksara yang dijana secara automatik yang membenarkan AVG untuk membezakan fail yang dipilih daripada fail lain dengan jelas. Hasil tambah semak dijana dan dipaparkan selepas penambahan fail berjaya.
- o **Sebarang lokasi** - jangan gunakan laluan penuh - jika anda hendak menentukan fail ini sebagai pengecualian hanya untuk lokasi tertentu, maka, tinggalkan kotak semakan ini tidak bertanda
- **Buang** - tekan untuk membuang aplikasi yang dipilih daripada senarai
- **Buang semua** - tekan untuk membuang semua aplikasi yang disenaraikan

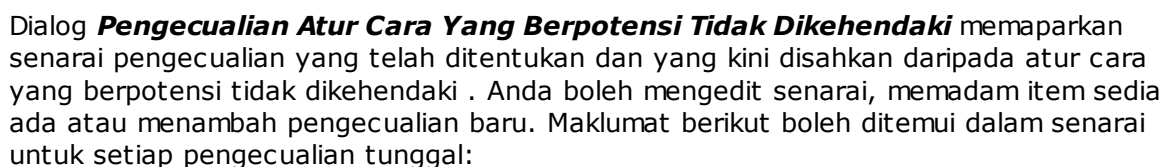
10.5. Bilik Kebal Virus



Dialog **penyelenggaraan Bilik Kebal Virus** membenarkan anda menentukan beberapa parameter berkenaan pentadbiran objek yang disimpan dalam **Bilik Kebal Virus**:

- **Hadkan saiz Bilik Kebal Virus** - gunakan gelangsar untuk menyediakan saiz maksimum bagi **Bilik Kebal Virus**. Saiz tersebut ditentukan mengikut perkadaran dibandingkan dengan saiz cakera setempat anda.
- **Pemadaman fail automatik** - dalam bahagian ini menentukan tempoh masa maksimum bagi objek yang patut disimpan dalam **Bilik Kebal Virus** (**Padam fail yang lebih lama daripada ... hari**), dan bilangan fail maksimum untuk disimpan dalam **Bilik Kebal Virus** (**Bilangan fail maksimum untuk disimpan**)

AVG 9 Internet Security boleh menganalisis dan mengesan aplikasi boleh laku atau pustaka DLL yang berkemungkinan berpotensi tidak diingini dalam sistem. Dalam sesetengah kes, pengguna mungkin mahu mengekalkan atur cara yang tidak dikehendaki tertentu pada atur cara (*komputer yang dipasang dengan sengaja*). Sesetengah atur cara, terutama sekali yang percuma, termasuk adware. Adware seperti itu mungkin dikesan dan dilaporkan oleh AVG sebagai **atur cara yang berpotensi tidak diingini**. Jika anda mahu mengekalkan atur cara seperti itu pada komputer anda, anda boleh mentakrifkannya sebagai pengecualian atur cara berpotensi tidak diingini:

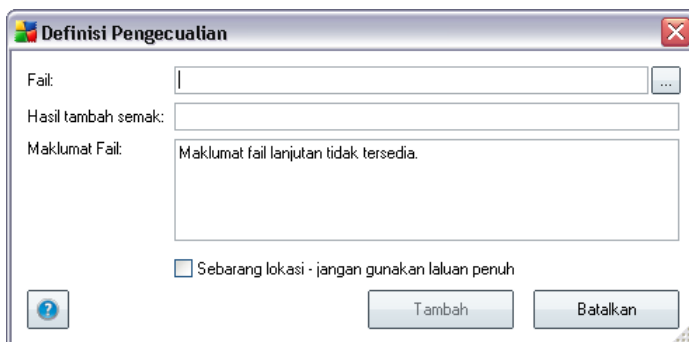


- **Fail** - memberikan nama aplikasi tersebut

- **Laluan Fail** - menunjukkan laluan kepada lokasi aplikasi
- **Hasil tambah semak** - memaparkan 'tandatangan' unik bagi fail yang dipilih. Hasil tambah semak ini adalah rentetan aksara yang dijana secara automatik yang membenarkan AVG untuk membezakan fail yang dipilih daripada fail lain dengan jelas. Hasil tambah semak dijana dan dipaparkan selepas penambahan fail berjaya.

Butang kawalan

- **Edit** - membuka dialog pengeditan (*serupa dengan dialog untuk definisi pengecualian baru, lihat di bawah*) bagi pengecualian yang sudah ditakrifkan di mana anda boleh mengubah parameter pengecualian
- **Buang** - memadam item yang dipilih dari senarai pengecualian
- **Tambah pengecualian** - membuka dialog pengeditan di mana anda boleh mentakrifkan parameter bagi pengecualian baru untuk dicipta:

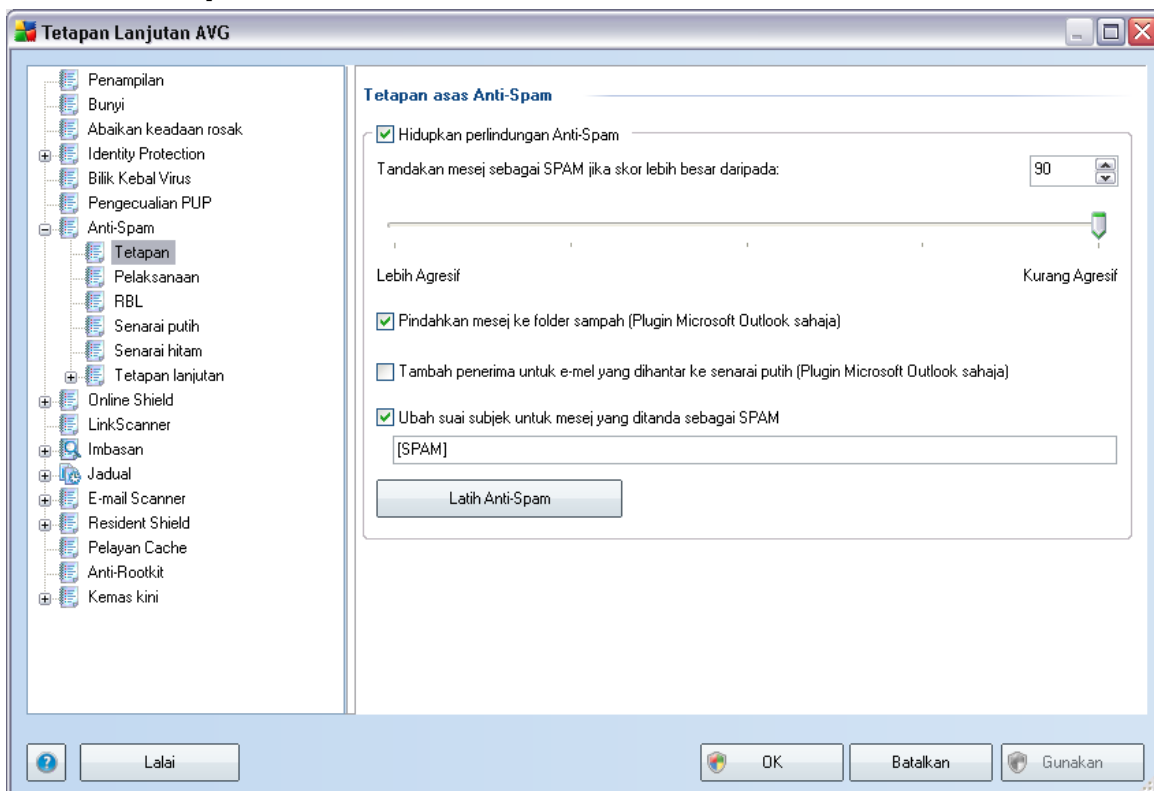


- o **Fail** - taipkan laluan penuh ke fail yang anda ingin tandakan sebagai pengecualian
- o **Hasil tambah semak** - memaparkan 'tandatangan' unik bagi fail yang dipilih. Hasil tambah semak ini adalah rentetan aksara yang dijana secara automatik yang membenarkan AVG untuk membezakan fail yang dipilih daripada fail lain dengan jelas. Hasil tambah semak dijana dan dipaparkan selepas penambahan fail berjaya.
- o **Maklumat Fail** - memaparkan sebarang maklumat tambahan yang tersedia mengenai fail (*maklumat lesen/versi dll.*)
- o **Sebarang lokasi - jangan gunakan laluan penuh** - jika anda mahu

menentukan fail ini sebagai pengecualian hanya untuk lokasi tertentu, maka, biarkan kotak semak ini tidak bertanda

10.7. AntiSpam

10.7.1. Tetapan



Dalam dialog **tetapan asas AntiSpam** anda boleh menanda/tidak menanda kotak semakan **Hidupkan perlindungan AntiSpam** untuk membenarkan/melarang pengimbasan antispam bagi komunikasi e-mel. Opsyen ini dihidupkan secara lalai dan sentiasa disyorkan untuk mengekalkan konfigurasi ini melainkan anda mempunyai sebab sebenar untuk mengubahnya.

Seterusnya, anda juga boleh memilih langkah pemarkahan yang lebih atau kurang agresif. Penapis **AntiSpam** menguntukkan setiap mesej dengan markah (*cth. sejauh mana kandungan mesej sama dengan SPAM*) berdasarkan pada beberapa teknik pengimbasan dinamik. Anda boleh mengubah suai **Tanda mesej sebagai spam jika**

markah lebih daripada menetapkan sama ada dengan menaip nilai (0 hingga 100) atau dengan menggerakkan gelongsor ke kiri atau kanan (*menggunakan gelongsor, julat nilai adalah terhad kepada 50-90*).

Secara umum, kami menyarankan untuk menetapkan ambang di antara 50-90 atau jika anda benar-benar tidak pasti kepada 90. Ini adalah semakan semula umum bagi ambang pemarkahan:

- **Nilai 90-99** - Kebanyakan mesej e-mel masuk akan dihantar secara normal (tanpa ditandakan sebagai [spam](#)). [Spam](#) Yang paling mudah dikenal pasti akan ditapis keluar tetapi jumlah ketara bagi [spam](#) masih lagi dibenarkan.
- **Nilai 80-89** - Mesej e-mel berkemungkinan menjadi [spam](#) akan ditapis keluar. Sesetengah mesej bukan spam mungkin juga ditapis dengan tidak betul.
- **Nilai 60-79** - Dikira sebagai konfigurasi yang agak agresif. Mesej e-mel yang berkemungkinan [spam](#) akan ditapis keluar. Mesej bukan spam juga berkemungkinan ditangkap.
- **Nilai 1-59** - Konfigurasi yang sangat agresif. Mesej e-mel bukan spam berkemungkinan ditangkap sebagai mesej [spam](#) sebenar. Julat ambang ini tidak disarakan untuk penggunaan biasa.
- **Nilai 0** - Dalam mod ini, anda hanya akan menerima mesej e-mel daripada penghantar dalam [Senarai Putih](#) anda. Sebarang mesej e-mel lain akan dikira sebagai [spam](#). **Julat ambang ini tidak disarakan untuk penggunaan biasa.**

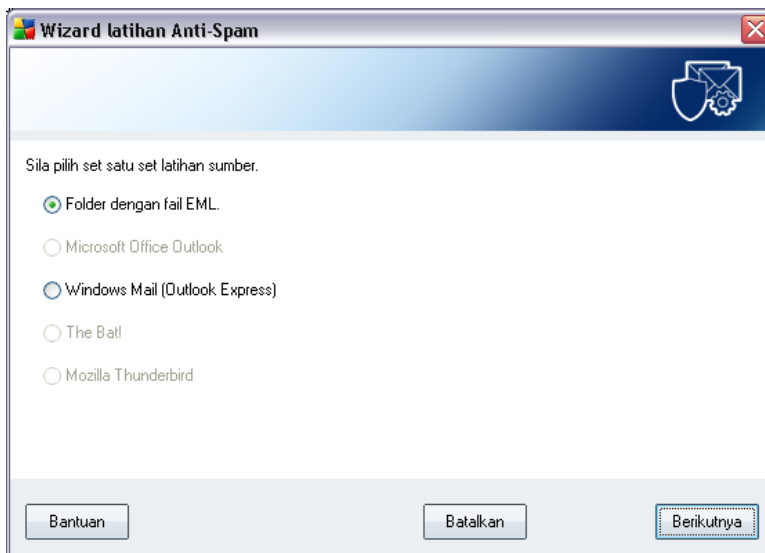
Dalam dialog **tetapan asas AntiSpam** anda boleh seterusnya mentakrifkan cara mesej e-mel [spam](#) yang dikesan diperlakukan:

- **Alihkan mesej ke folder sarap** - tandakan kotak semakan ini untuk mentakrifkan bahawa setiap mesej spam yang dikesan harus dialihkan secara automatik ke folder sarap khusus dalam klien e-mel anda;
- **Tambah penerima bagi e-mel yang dihantar ke [senarai putih](#)** - tandakan rait kotak semakan untuk memastikan semua penerima bagi e-mel yang dihantar boleh dipercayai dan semua mesej e-mel datang dari akaun e-mel mereka boleh dihantar;
- **Ubah suai subjek mesej yang ditandakan sebagai SPAM** - tandakan rait kotak semakan ini jika anda mahu semua mesej dikesan sebagai [spam](#) ditandakan dengan perkataan atau aksara tertentu dalam medan subjek e-mel; teks yang dikehendaki boleh ditaip dalam medan teks yang diaktifkan.

Butang kawalan

Butang Latih AntiSpam membuka wizard latihan **AntiSpam** yang diterangkan secara terperinci dalam [bab berikutnya](#).

Dialog pertama bagi **Anti-Spam Training Wizard** meminta anda memilih sumber mesej e-mel yang anda hendak gunakan untuk latihan. Biasanya, anda akan menggunakan sama ada e-mel yang telah ditandakan dengan SPAM secara tidak betul atau mesej spam yang telah dikenal pasti.



Terdapat opsyen berikut untuk dipilih:

- **Klien e-mel khusus** - jika anda menggunakan salah satu klien e-mel yang disenaraikan (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), hanya pilih pilihan masing-masing
- **Folder dengan fail EML** - jika anda menggunakan sebarang atur cara e-mel, pertama sekali, anda harus menyimpan mesej ke folder khusus (dalam format *.eml*), atau pastikan anda mengetahui lokasi folder mesej klien e-mel anda. Kemudian, pilih **Folder dengan fail EML**, yang akan membolehkan anda mengesan folder yang diinginkan dalam langkah berikutnya

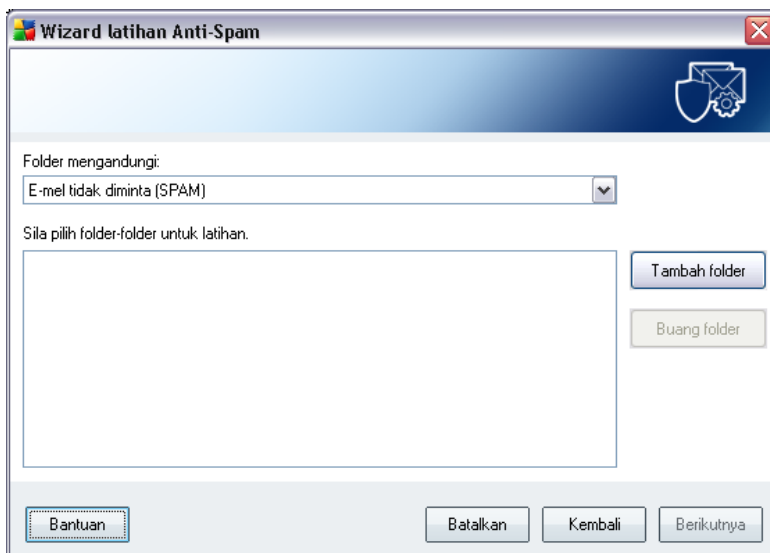
Untuk proses latihan yang lebih cepat dan murah, ia merupakan idea yang baik untuk menyusun e-mel dalam folder terlebih dahulu, agar folder yang anda akan gunakan

untuk latihan mengandungi hanya mesej latihan (sama ada diingini, atau tidak diingini). Bagaimanapun, itu adalah tidak perlu, memandangkan anda akan boleh menapis e-mel kemudian nanti.

Pilih opsyen yang sesuai dan klik **Seterusnya** untuk meneruskan wizard.

Dialog yang dipaparkan dalam langkah ini bergantung kepada pemilihan anda sebelum ini.

Folder dengan fail EML.



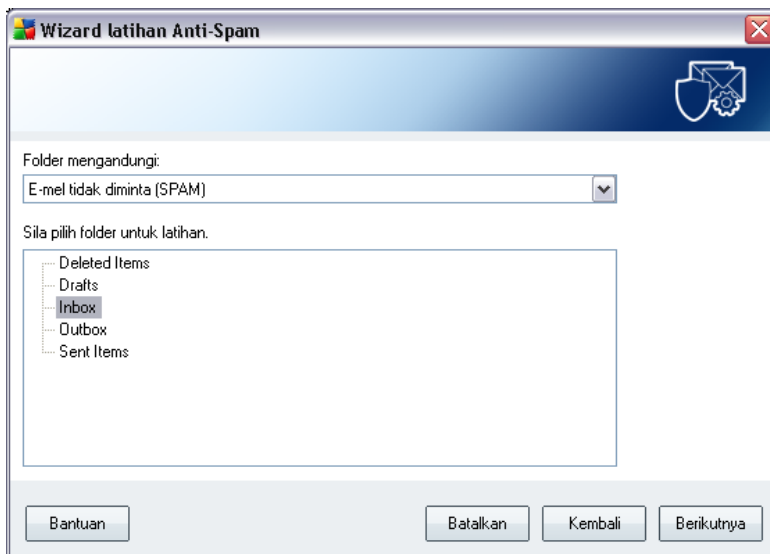
Dalam dialog ini, sila pilih folder dengan mesej yang anda hendak gunakan untuk latihan. Tekan butang **Tambah folder** untuk mencari folder dengan fail .eml (*mesej e-mel yang disimpan*). Folder terpilih akan kemudiannya dipaparkan dalam dialog.

Dalam Folder **mengandungi** menu jatuh bawah, tetapkan salah satu opsyen - sama ada folder yang dipilih mengandungi mesej yang dikehendaki (*HAM*), atau tanpa diminta (*SPAM*). Harap maklum bahawa anda boleh menapis mesej dalam langkah seterusnya supaya folder tidak mengandungi hanya e-mel latihan. Anda juga boleh membuang folder terpilih yang dikehendaki dari senarai dengan mengklik butang **Buang folder**.

Apabila selesai, klik **Berikutnya** dan teruskan kepada [Opsyen penapisan mesej](#).

Klien e-mel khusus

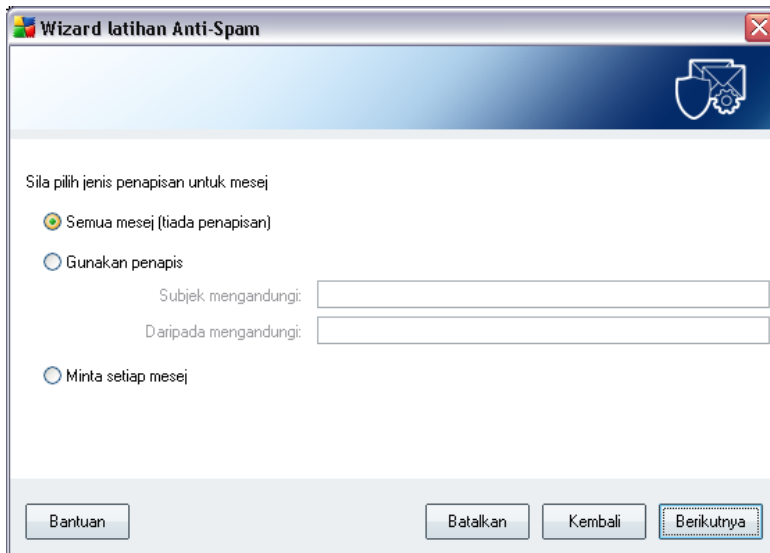
Sebaik sahaja anda mengesahkan salah satu opsyen tersebut, dialog baru akan muncul.



Nota: Dalam kes Microsoft Office Outlook, anda akan digesa untuk memilih profil MS Office Outlook dahulu.

Dalam Folder **mengandungi** menu jatuh bawah, tetapkan salah satu opsyen - sama ada folder yang dipilih mengandungi mesej yang dikehendaki (*HAM*), atau tanpa diminta (*SPAM*). Harap maklum bahawa anda boleh menapis mesej dalam langkah seterusnya supaya folder tidak mengandungi hanya e-mel latihan. Pohon navigasi klien e-mel yang terpilih telah sedia dipaparkan dalam bahagian utama dialog. Sila kesan folder yang diingini dalam pohon dan serlahkannya dengan tetikus anda.

Apabila selesai, klik **Berikutnya** dan teruskan kepada [Opsyen penapisan mesej](#).



Dalam dialog ini, anda boleh menetapkan penapisan mesej e-mel.

Jika anda pasti folder terpilih mengandungi cuma mesej yang anda ingin gunakan untuk latihan, pilih opsiyen ***Semua mesej (tiada penapisan)***.

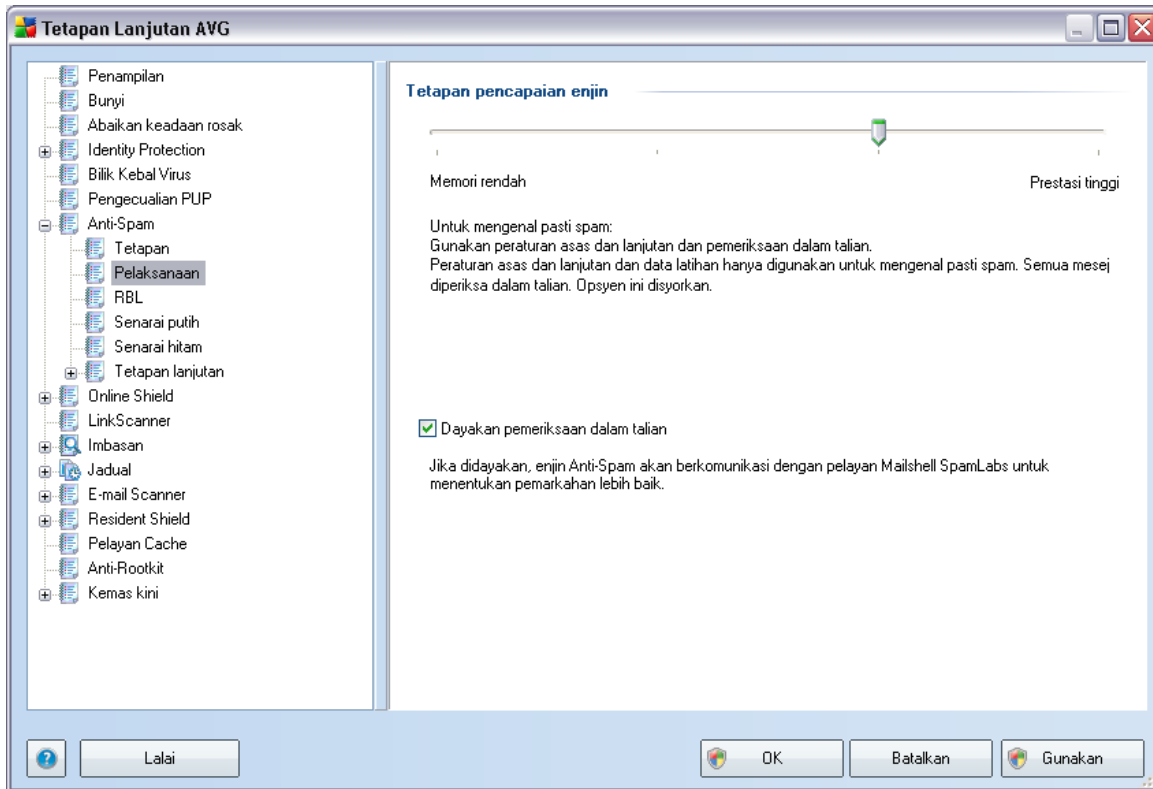
Jika anda tidak pasti mengenai mesej yang terkandung dalam folder dan anda ingin wizard bertanya kepada anda mengenai setiap mesej (supaya anda boleh menentukan sama ada untuk menggunakannya untuk latihan atau tidak) pilih opsiyen ***Tanya bagi setiap mesej***.

Untuk penapisan lebih lanjut, pilih opsiyen ***Gunakan penapis***. Anda boleh mengisikan perkataan (*nama*), sebahagian perkataan atau perenggan untuk dicari dalam subjek e-mel dan/atau medan penghantar. Semua mesej yang sepadan dengan kriteria yang dimasukkan akan digunakan untuk latihan, tanpa penggesaan lanjut.

Perhatian! : Apabila anda mengisi kedua-dua medan teks, alamat yang sepadan dengan cuma satu dari dua keadaan itu akan digunakan, juga!

Apabila opsiyen sesuai telah dipilih, klik ***Berikutnya***. Dialog berikut hanya berguna untuk memberitahu anda bahawa wizard sedia untuk memproses mesej. Untuk memulakan latihan, klik butang ***Berikutnya*** sekali lagi. Kemudian, latihan akan bermula mengikut syarat yang dipilih sebelum ini.

10.7.2. Pencapaian



Dialog **Tetapan prestasi enjin** (dipautkan melalui item **Prestasi** bagi navigasi kiri) menawarkan tetapan prestasi komponen **AntiSpam**. Gerakkan gelangsar ke kiri atau kanan untuk menukar julat tahap prestasi pengimbasan di antara mod prestasi **memori Rendah / Tinggi**.

- **Memori rendah** - sewaktu proses pengimbasan untuk mengenal pasti [spam](#), tiada peraturan yang akan digunakan. Hanya data latihan akan digunakan untuk pengenalanpastian. Mod ini tidak disyorkan untuk penggunaan biasa, melainkan perkakas komputer adalah sangat lemah.
- **Prestasi tinggi** - mod ini akan menggunakan jumlah besar memori. Sewaktu proses pengimbasan untuk mengenal pasti [spam](#), ciri berikut akan digunakan: peraturan dan cache pangkalan data [spam](#), peraturan asas dan lanjutan, alamat IP spam dan pangkalan data spam.

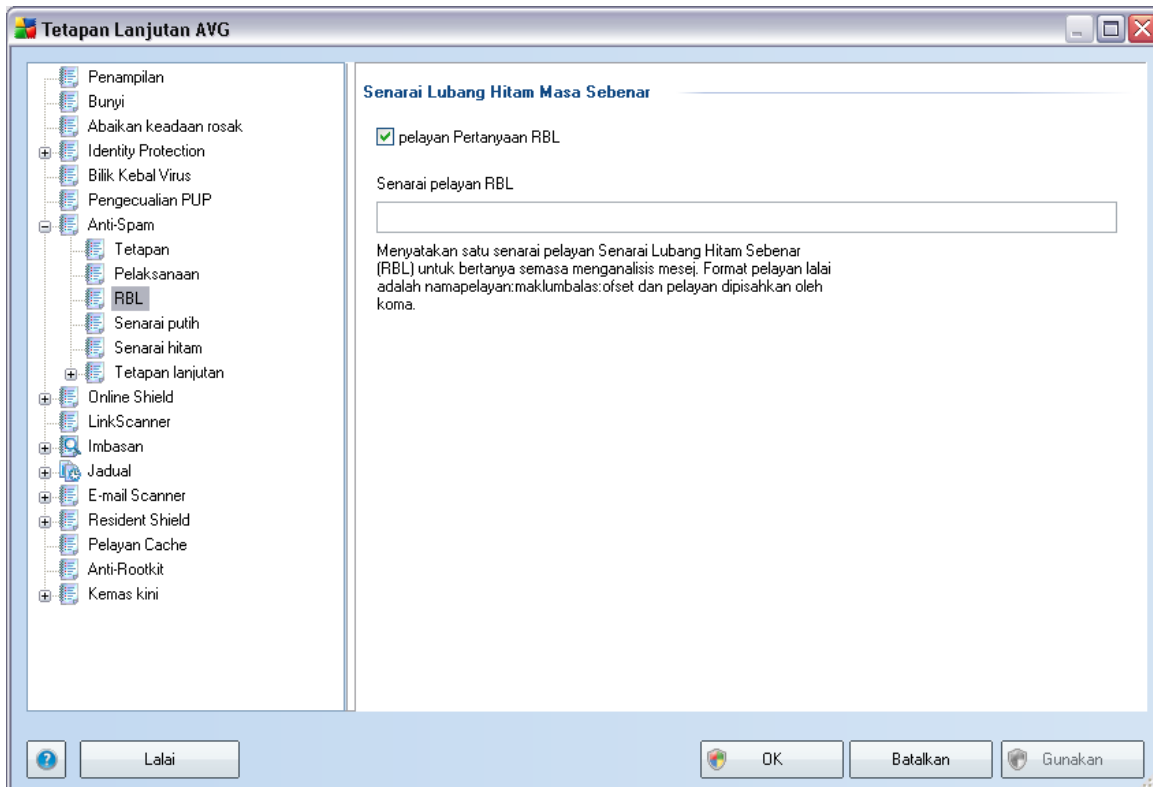
Item **Dayakan semakan dalam talian** dihidupkan secara lalai. Ia memberikan keputusan pengesanan [spam](#) yang lebih tepat melalui komunikasi dengan pelayan

[Mailshell](#) ,cth. data yang diimbas akan dibandingkan dengan pangkalan data dalam talian [Mailshell](#).

Secara umum, ia disyorkan untuk mengekalkan tetapan lalai dan hanya menukarnya jika anda mempunyai sebab yang kukuh untuk melakukannya. Sebarang perubahan kepada konfigurasi ini harus dilakukan oleh pengguna yang pakar sahaja!

10.7.3. RBL

Item **RBL** membuka dialog pengeditan yang dipanggil **Senarai Lubang Hitam Masa Sebenar**:



Dalam dialog ini, anda boleh menghidupkan/mematikan fungsi **pelayan Pertanyaan RBL**.

Pelayan RBL (*Senarai Lubang Hitam Masa Sebenar*) pelayan adalah pelayan DNS dengan pangkalan data meluas bagi penghantar spam yang diketahui. Apabila ciri ini dihidupkan, semua mesej e-mel akan disahkan dengan pangkalan data pelayan RBL dan

ditanda sebagai [spam](#) jika sama dengan sebarang entri pangkalan data. Pangkalan data pelayan RBL mengandungi cap jari spam yang terkini untuk memberikan pengesanan [spam](#) yang terbaik dan paling tepat. Ciri ini berguna terutama sekali untuk pengguna yang menerima sejumlah besar spam yang tidak dikesan secara normal oleh enjin [AntiSpam](#).

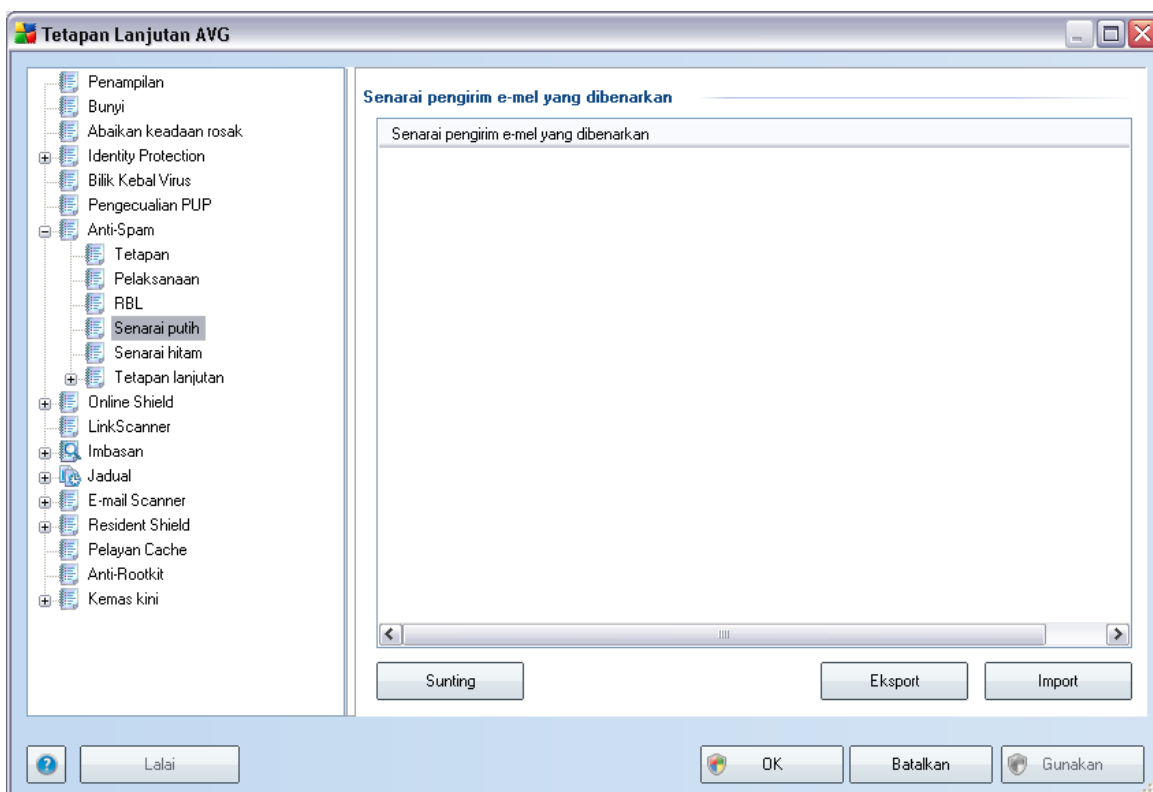
Senarai pelayan RBL membenarkan anda menentukan lokasi pelayan RBL.

Nota: Mendayakan ciri ini mungkin, pada sesetengah sistem dan konfigurasi, melambatkan proses penerimaan e-mel kerana setiap mesej mesti disahkan dengan pangkalan data pelayan RBL.

Tiada data peribadi yang dihantar ke pelayan!

10.7.4. Senarai putih

Item **Senarai putih** membuka dialog yang dinamakan **Senarai penghantar e-mel yang diluluskan** dengan senarai global alamat e-mel penghantar yang diluluskan dan nama domain bagi mesej yang tidak akan ditandakan sebagai [spam](#).



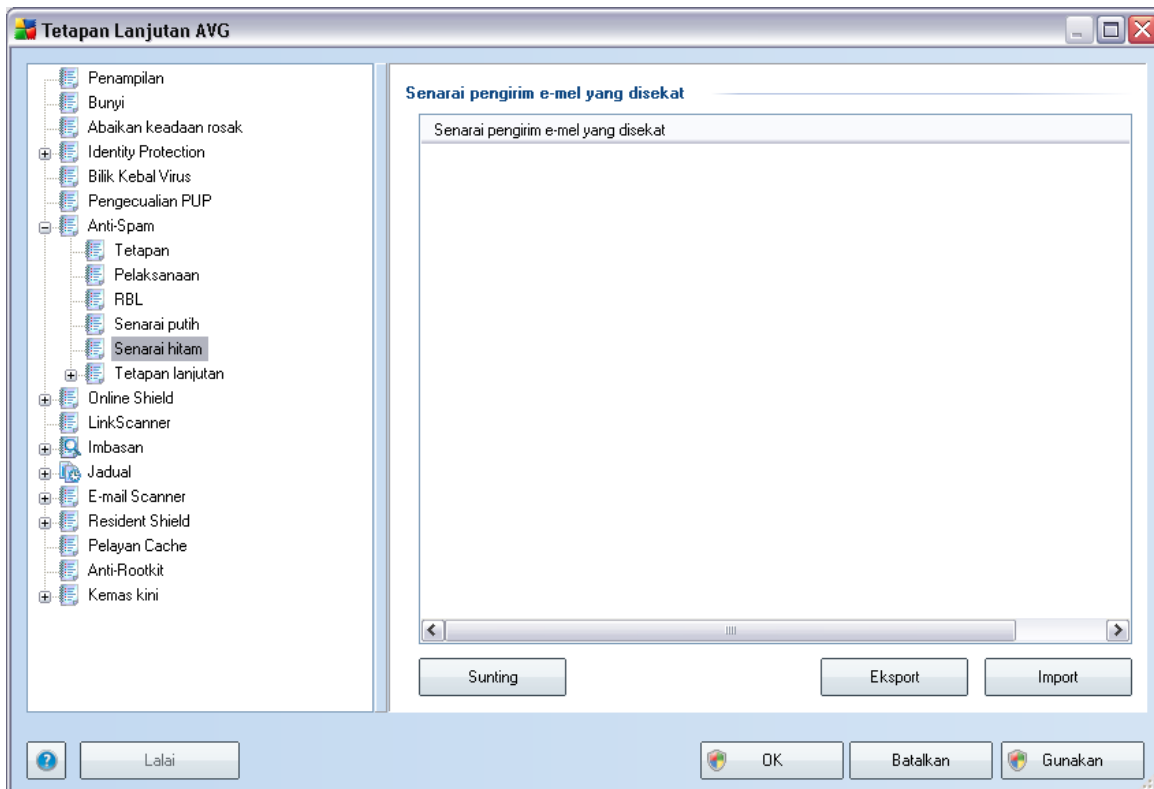
Dalam antara muka pengeditan, anda boleh mengumpulkan senarai penghantar yang anda pasti tidak akan menghantarkan anda mesej yang tidak diingini ([spam](#)). Anda juga boleh mengumpulkan senarai nama domain penuh (*cth. avg.com*), yang anda ketahui tidak menjana mesej spam.

Sebaik sahaja anda mempunyai senarai penghantar seperti itu dan/atau nama domain disediakan, anda boleh memasukkannya melalui salah satu kaedah berikut: melalui entri terus setiap alamat e-mel atau dengan mengimport keseluruhan senarai alamat sekali. Butang kawalan berikut tersedia:

- **Edit** - tekan butang ini untuk membuka dialog, di mana anda boleh memasukkan senarai alamat secara manual (*anda juga boleh menggunakan salin dan tampal*). Masukkan satu item (*penghantar, nama domain*) bagi setiap baris.
- **Eksport** - jika anda bercadang untuk mengeksport rekod untuk tujuan tertentu, anda boleh melakukannya dengan menekan butang ini. Semua rekod akan disimpan ke fail teks kosong.
- **Import** - jika anda sudah mempunyai fail teks bagi alamat/nama domain e-mel yang disediakan, anda boleh mengimportnya dengan mudah dengan memilih butang ini. Fail input mesti dalam format teks biasa dan kandungan mesti mengandungi hanya satu item (*alamat, nama domain*) bagi setiap baris.

10.7.5. Senarai hitam

Item **Senarai Hitam** membuka dialog dengan senarai global alamat e-mel penghantar yang disekat dan nama domain yang mesejnya akan sentiasa ditandakan sebagai [spam](#).



Dalam antara muka pengeditan, anda boleh mengumpulkan senarai penghantar yang anda jangkakan untuk menghantar mesej yang tidak diingini kepada anda ([spam](#)). Anda juga boleh mengumpulkan senarai nama domain penuh (*cth. spammingcompany.com*), yang anda jangkakan atau dari mana anda terima mesej. Semua e-mel daripada alamat/domain yang disenaraikan akan dikenal pasti sebagai spam.

Sebaik sahaja anda mempunyai senarai penghantar seperti itu dan/atau nama domain disediakan, anda boleh memasukkannya melalui salah satu kaedah berikut: melalui entri terus setiap alamat e-mel atau dengan mengimport keseluruhan senarai alamat sekali. Butang kawalan berikut tersedia:

- **Edit** - tekan butang ini untuk membuka dialog, di mana anda boleh memasukkan senarai alamat secara manual (*anda juga boleh menggunakan salin dan tampal*). Masukkan satu item (*penghantar, nama domain*) bagi setiap baris.

- **Eksport** - jika anda bercadang untuk mengeksport rekod untuk tujuan tertentu, anda boleh melakukannya dengan menekan butang ini. Semua rekod akan disimpan ke fail teks kosong.
- **Import** - jika anda sudah mempunyai fail teks bagi alamat/nama domain e-mel yang disediakan, anda boleh mengimportnya dengan mudah dengan memilih butang ini. Fail input mesti dalam format teks biasa dan kandungan mesti mengandungi hanya satu item (*alamat, nama domain*) bagi setiap baris.

10.7.6. Tetap Lanjutan

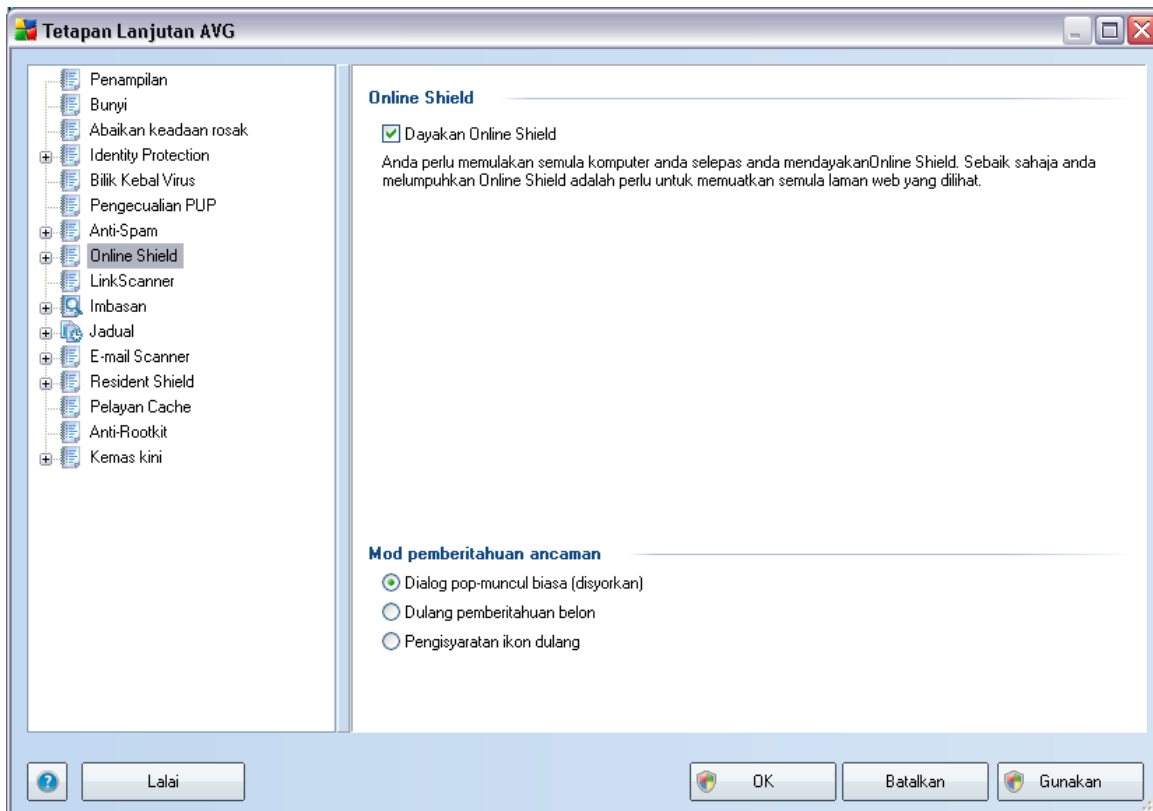
Cabang Tetap Lanjutan mengandungi opsyen tetap meluas untuk komponen AntiSpam . Tetap ini dimaksudkan untuk pengguna berpengalaman, biasanya pentadbir rangkaian yang perlu mengkonfigurasi perlindungan antispam dalam perincian penuh untuk perlindungan terbaik pelayan e-mel. Atas sebab ini, tiada bantuan tambahan tersedia untuk dialog individu; namun, terdapat penerangan ringkas untuk setiap opsyen secara langsung di antara muka pengguna.

Kami amat mengesyorkan untuk tidak mengubah sebarang tetap melainkan anda sangat biasa dengan tetap lanjutan Spamcatcher (MailShell Inc.). Sebarang perubahan yang tidak sesuai mungkin menghasilkan prestasi buruk atau kefungsi komponen secara tidak betul.

Jika anda masih perlu mengubah konfigurasi [AntiSpam](#) pada tahap yang sangat tinggi, sila ikuti arahan yang diberikan secara terus dalam antara muka pengguna. Secara umumnya, dalam setiap dialog anda akan menemui satu ciri khusus tunggal dan anda boleh mengeditnya - penerangannya sentiasa dimasukkan dalam dialog itu sendiri:

- **Cache** - cap jari, reputasi domain, LegitRepute
- **Latihan** - entri perkataan maksimum, ambang latihan auto, berat
- **Penapisan** - senarai bahasa, senarai negara, IP yang diluluskan, IP yang disekat, negara yang disekat, charset yang disekat, penghantar palsu
- **RBL** - Pelayan RBL, hit berbilang, ambang, masa rehat, IP maksimum
- **Sambungan Internet** - tamat masa, pelayan proksi, pengesahan proksi

10.8. Perisai Dalam Talian



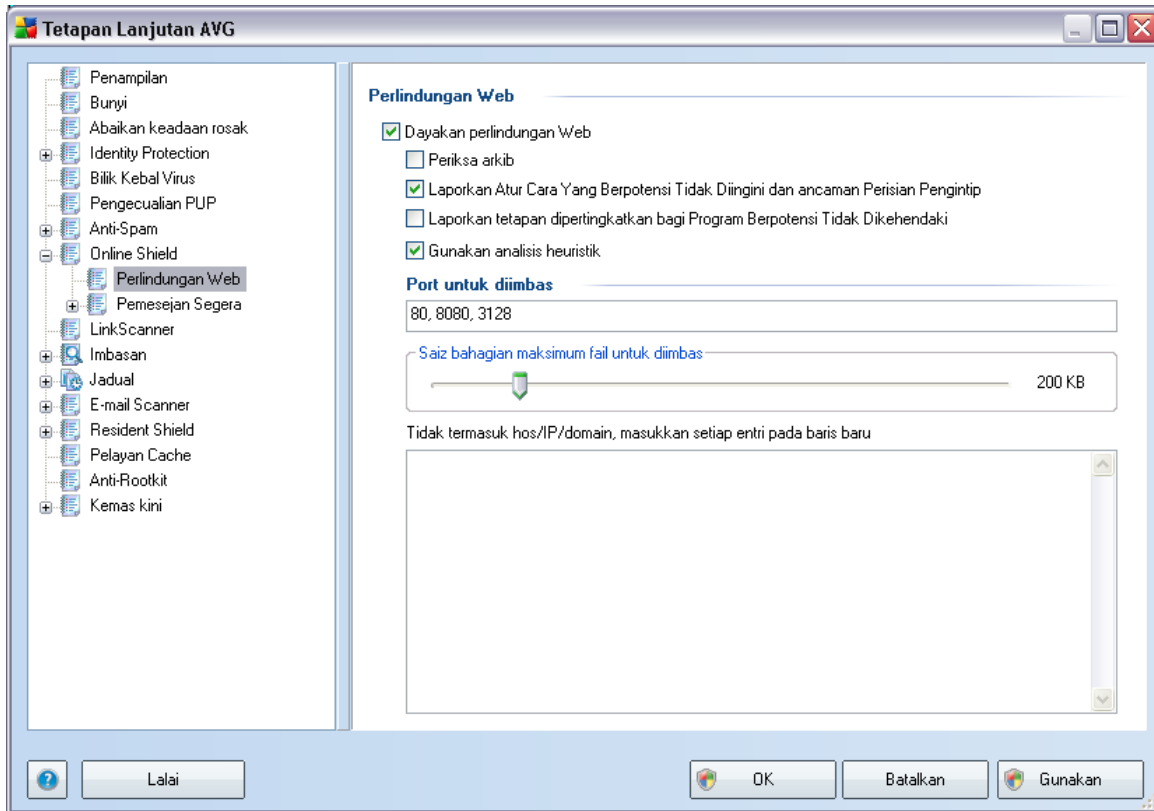
Dialog **Perlindungan Web** membenarkan anda mengaktifkan/menyahaktifkan seluruh komponen **Perisai Web** melalui opsyen **Dayakan Perisai Dalam Talian** (*diaktifkan secara lalai*). Untuk tetapan lanjutan seterusnya bagi komponen ini, sila teruskan ke dialog berikutnya seperti yang disenaraikan dalam navigasi pepohon:

- [**Perlindungan Web**](#)
- [**Pemesejan Segera**](#)

Mod pemberitahuan pepohon

Dalam bahagian bawah dialog, pilih dalam cara mana anda hendak diberitahu mengenai kemungkinan ancaman yang dikesan: melalui dialog pop timbul standard, melalui pemberitahuan belon dulang atau melalui maklumat ikon dulang.

10.8.1. Perlindungan Web



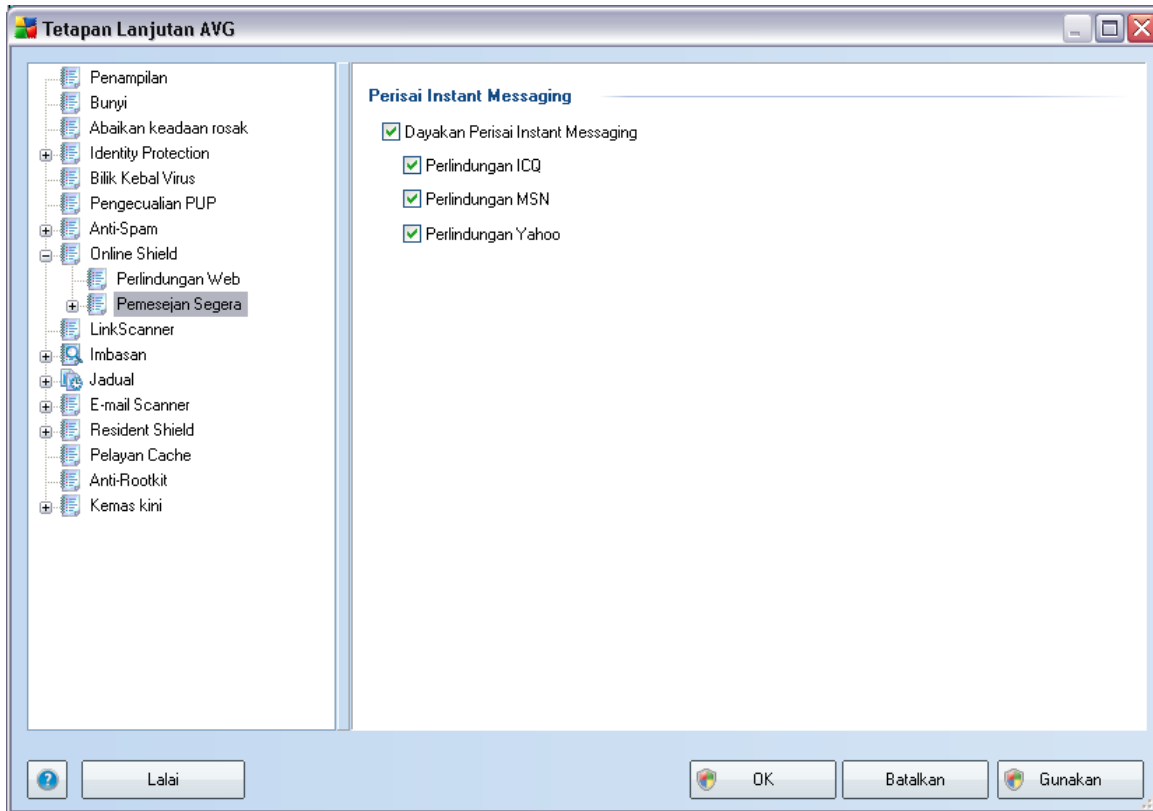
Dalam dialog **Perlindungan Web** anda boleh mengedit konfigurasi komponen berkenaan imbasan kandungan tapak web. Antara muka penyuntingan ini membenarkan anda untuk mengkonfigurasi opsyen permulaan berikut:

- **Dayakan perlindungan Web** - pilihan ini mengesahkan bahawa [Perisai Dalam Talian](#) harus menjalankan pengimbasan kandungan halaman www. Jika opsyen ini dihidupkan (*secara lalai*), seterusnya, anda boleh menghidupkan/mematikan item ini:
 - o **Periksa arkib** - imbas kandungan arkib yang berkemungkinan dimasukkan dalam halaman www untuk dipaparkan.
 - o **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan.](#)

[sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- o **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini** - jika pilihan sebelumnya diaktifkan, anda juga boleh menanda kotak ini untuk mengesan pakej diluaskan bagi [perisian pengintip](#): atur cara adalah sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat kemudiannya. Ini adalah ukuran tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- o **Gunakan analisis heuristik** - imbas kandungan halaman untuk dipaparkan menggunakan kaedah [analisis heuristik](#) (*persaingan dinamik bagi arahan objek yang diimbis dalam persekitaran komputer maya*).
- o **Port untuk diimbis** - medan ini menyenaraikan nombor port komunikasi http standard. Jika konfigurasi komputer anda berbeza, anda boleh mengubah nombor port seperti yang diperlukan.
- o **Bahagian saiz fail maksimum untuk diimbis** - jika fail yang dimasukkan terdapat dalam halaman yang dipaparkan, anda juga boleh mengimbis kandungannya sebelum ia dimuat turun ke komputer anda. Walau bagaimanapun, pengimbasan fail besar mengambil sedikit masa dan muat turun laman web mungkin menjadi perlahan. Anda boleh menggunakan bar gelangsar untuk menentukan saiz maksimum bagi fail yang masih diimbis dengan [Perisai Dalam Talian](#). Walaupun jika fail yang dimuat turun adalah lebih besar daripada yang ditentukan, dan oleh itu, tidak akan diimbis dengan Perisai Dalam Talian, anda masih dilindungi: jika fail dijangkiti, [Resident Shield](#) akan mengesannya dengan serta-merta.
- o **Keluarkan hos/IP/domain** - ke dalam medan teks, anda boleh menaip nama sebenar bagi pelayan (*hos, alamat IP, alamat IP dengan topeng, atau URL*) atau domain yang harus diimbis oleh [Perisai Dalam Talian](#). Oleh itu, hanya kecualikan hos yang anda betul-betul pasti tidak akan memberikan kandungan tapak web berbahaya.

10.8.2. Pemesejan Segera

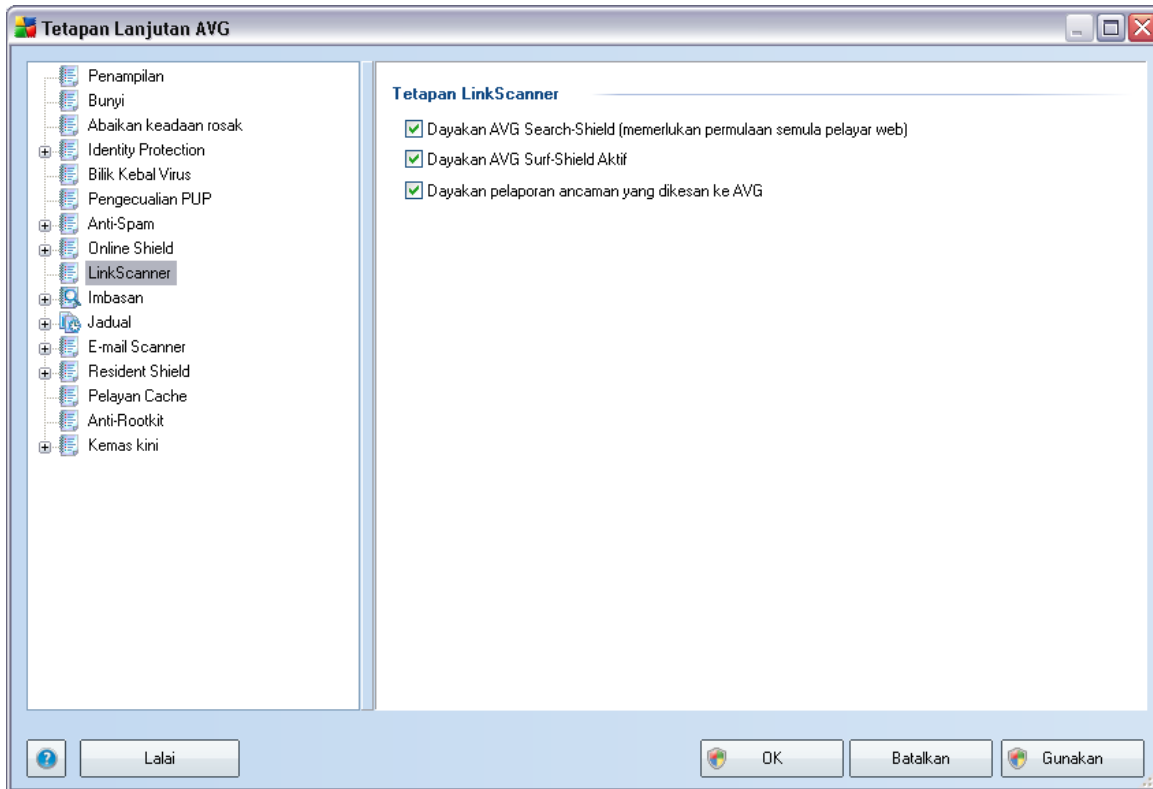


Dalam dialog **Perisai Pemesejan Segera** anda boleh mengedit tetapan komponen **Perisai Dalam Talian** yang merujuk kepada pengimbasan pemesejan segera. Buat masa ini, tiga atur cara pemesejan segera disokong: **ICQ**, **MSN**, dan **Yahoo** - tandakan rait item masing-masing untuk setiap satunya jika anda mahukan **Perisai Dalam Talian** mengesahkan komunikasi dalam talian adalah bebas virus.

Untuk spesifikasi selanjutnya mengenai pengguna dibenarkan/disekat, anda boleh melihat dan mengedit dialog masing-masing (**ICQ Lanjutan**, **MSN Lanjutan**, **Yahoo Lanjutan**) dan tentukan **Senarai Putih** (senarai pengguna yang akan dibenarkan untuk berkomunikasi dengan anda) dan pengguna **Senarai Hitam** (yang harus disekat).

10.9. Pengimbas Pautan

Dialog **tetapan LinkScanner** membenarkan anda menghidupkan/mematikan ciri bagi **LinkScanner**:



- **Dayakan AVG Search-Shield** - (*dihidupkan secara lalai*): ikon pemberitahuan maklumat pada carian yang dilakukan dalam Google, Yahoo, Bing, Yandex, Altavista atau Baidu diperiksa dahulu kandungan tapak oleh enjin carian.
- **Dayakan AVG Active Surf-Shield** - (*hidupkan secara lalai*): perlindungan (*masa nyata*) aktif daripada tapak yang boleh mengeksploitasi apabila ia diakses. Sambungan tapak yang diketahui berniat jahat dan kandungannya yang boleh mengeksploitasi apabila ia diakses oleh pengguna melalui penyemak imbas web (*atau sebarang aplikasi lain yang menggunakan HTTP*).
- **Dayakan pelaporan ancaman yang dikesan kepada AVG** - (*dihidupkan secara lalai*): tandakan item ini untuk membenarkan pelaporan semula eksploitasi dan tapak jahat yang ditemui oleh pengguna sama ada melalui **AVG Active Surf-Shield** atau **AVG Search-Shield** untuk menyuap maklumat

pengumpulan pada aktiviti berniat jahat pada web.

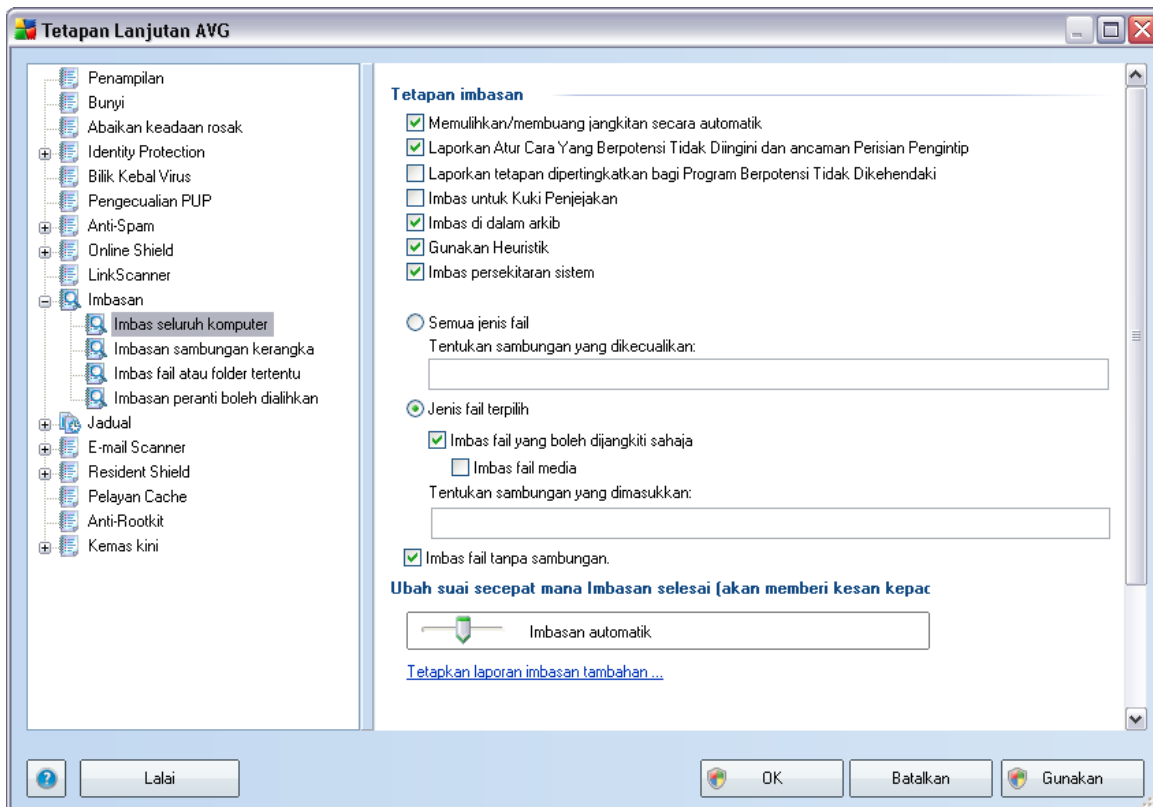
10.10. Imbasan

Tetapan imbasan lanjutan dibahagikan kepada tiga kategori merujuk kepada jenis imbasan khusus seperti yang ditentukan oleh vendor perisian:

- **Imbas Seluruh Komputer** - imbasan dipratakrif standard bagi seluruh komputer
- **Imbasan Sambungan Kerangka** - imbasan khusus bagi objek yang dipilih dari persekitaran Windows Explorer
- **Imbas Fail atau Folder Khusus** - imbasan dipratakrif khusus bagi kawasan yang dipilih pada komputer anda
- **Imbasan Peranti Boleh Dialihkan** - pengimbasan khusus bagi peranti boleh dialihkan yang dilampirkan ke komputer anda

10.10.1. Imbas Seluruh Komputer

Opsyen **Imbas seluruh komputer** membenarkan anda mengedit parameter bagi salah satu imbasan yang dipraktikkan oleh vendor perisian, **Imbas seluruh komputer**:



Tetapan imbasan

Bahagian **Tetapan imbasan** menawarkan senarai parameter imbasan yang boleh dihidupkan/dimatikan secara pilihan:

- **Pulihkan/buang jangkitan secara automatik** - jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika rawatan tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dibuang ke **Bilik Kebal Virus**.
- **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip** - (dihidupkan secara lalai): tandakan untuk mengaktifkan enjin

AntiPerisian Pengintip , dan imbas untuk perisian pengintip serta untuk virus. Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini** - jika pilihan sebelumnya diaktifkan, anda juga boleh menanda kotak ini untuk mengesan pakej diluaskan bagi perisian pengintip: atur cara adalah sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat kemudiannya. Ini adalah ukuran tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas untuk Kuki Penjejakan** - parameter ini bagi komponen AntiPerisian Pengintip menentukan bahawa kuki harus dikesan; (*Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat khusus mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektroniknya*)
- **Imbas dalam arkib** - parameter ini menentukan bahawa imbasan harus memeriksa semua fail malahan yang disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** - analisis heuristik (*persaingan dinamik bagi objek yang dikesan arahan dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan;
- **Imbas persekitaran sistem** - imbasan juga akan memeriksa kawasan sistem komputer anda.

Seterusnya, anda harus menentukan sama ada anda mahu mengimbas

- **Semua jenis fail** dengan kemungkinan pengecualian yang ditakrifkan daripada imbasan dengan memberikan senarai yang pemanjangan fail yang dipisahkan oleh koma (*apabila disimpan, koma bertukar kepada koma bertitik*) yang tidak harus diimbas;
- **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak ini tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan

sambungan fail mana yang sepatutnya sentiasa diimbas.

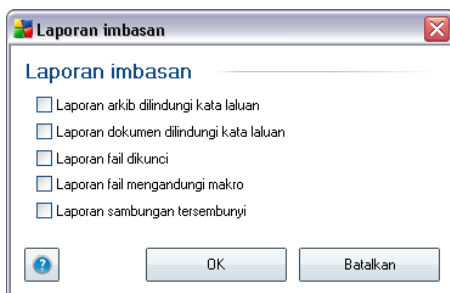
- Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.

Keutamaan proses imbasan

Dalam bahagian **Keutamaan proses imbasan** anda boleh menentukan selanjutnya kelajuan pengimbasan yang dikehendaki bergantung kepada penggunaan sumber sistem. Secara lalai, nilai opsyen ini ditetapkan kepada peringkat sederhana penggunaan sumber automatik. Jika anda hendak imbasan dijalankan dengan pantas, ia akan mengambil masa yang kurang tetapi penggunaan sumber sistem akan meningkat dengan ketara sewaktu imbasan dan akan melambatkan aktiviti anda yang lain pada PC (*opsyen ini boleh digunakan semasa komputer anda dihidupkan tetapi tiada siapa yang menggunakannya*). Sebaliknya, anda boleh mengurangkan penggunaan sumber sistem dengan menambah tempoh pengimbasan.

Tetapkan laporan imbasan tambahan ...

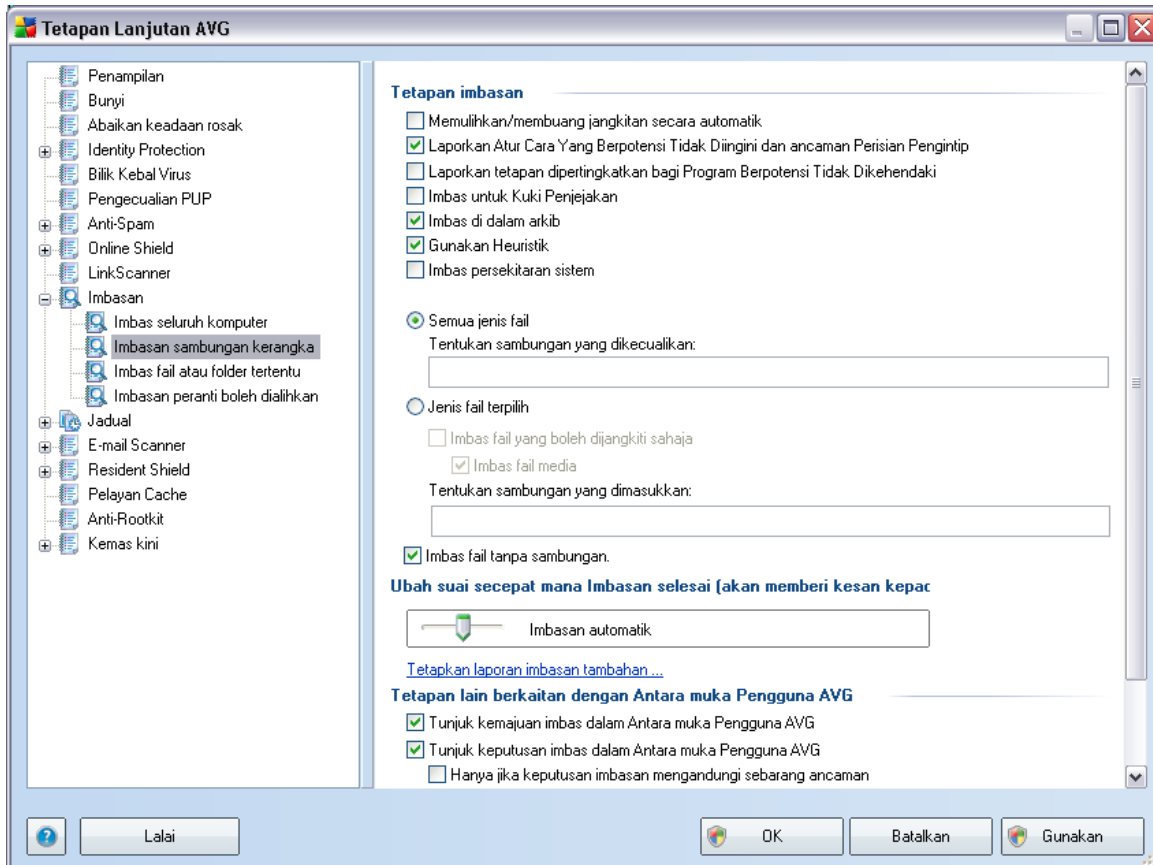
Klik pautan **Tetapkan laporan imbasan tambahan ...** untuk membuka tetingkap dialog tersendiri yang dipanggil **Laporan imbasan** di mana anda boleh menanda rait beberapa item untuk mentakrifkan penemuan imbasan yang harus dilaporkan:



10.10.2. Imbasan Sambungan Kerangka

Sama dengan yang item sebelumnya **Imbas seluruh komputer**, item ini dinamakan **Imbasan sambungan kerangka** juga menawarkan beberapa opsyen untuk pengeditan imbasan yang dipraktakrif oleh vendor perisian. Kali ini, konfigurasi dikaitkan dengan [pengimbasan objek tertentu dilancarkan secara terus dari persekitaran](#)

[Windows Explorer](#) (sambungan kerangka), lihat bab [Mengimbas dalam Windows Explorer](#):



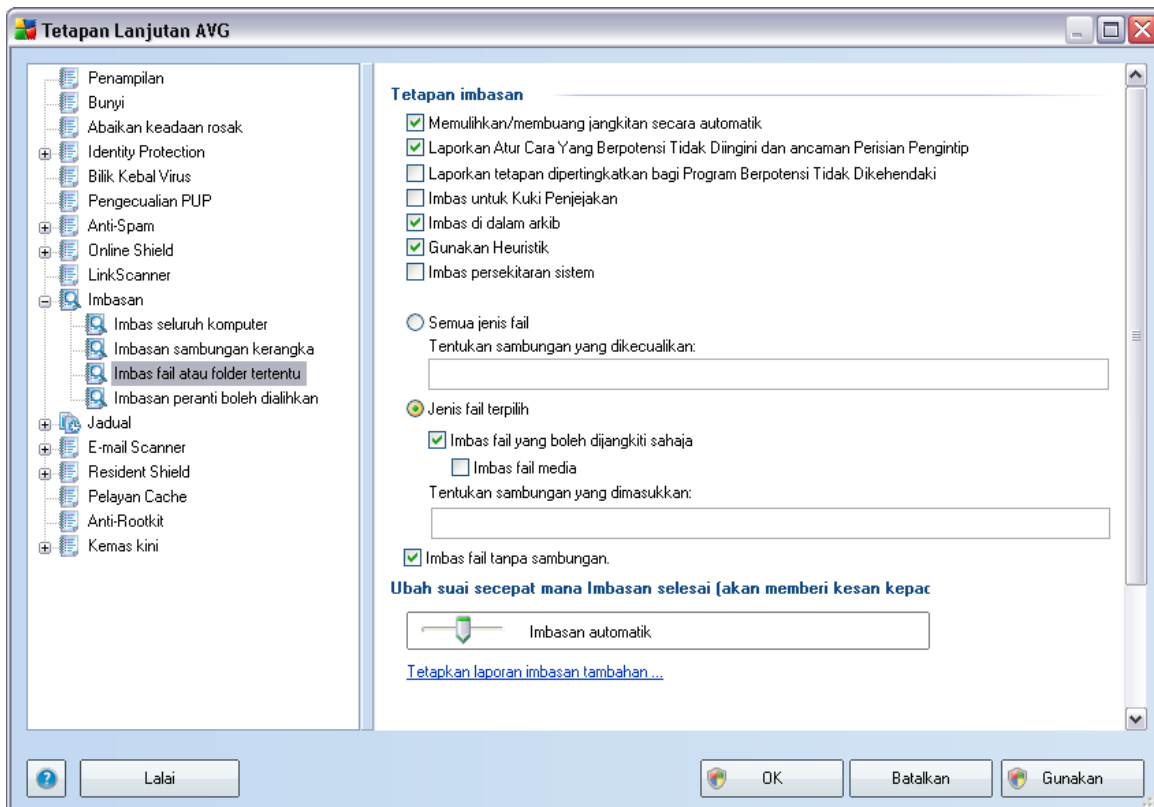
Senarai parameter adalah sama dengan yang tersedia untuk [Imbas seluruh komputer](#). Walau bagaimanapun, tetapan lalai berbeza dengan **Imbas Seluruh Komputer** kebanyakan parameter dipilih sementara untuk **Imbasan sambungan kerangka** ([Pengimbasan dalam Windows Explorer](#)) hanya parameter berkaitan dihidupkan.

Perhatian: Untuk penerangan mengenai parameter tertentu, sila rujuk bab [Tetapan Lanjutan AVG / Imbasan / Imbas Seluruh Komputer](#).

10.10.3. Imbas Fail atau Folder Tertentu

Antara muka pengeditan untuk **Imbas fail atau folder tertentu** adalah sama dengan dialog pengeditan [Imbas Seluruh Komputer](#). Semua opsyen konfigurasi adalah sama; walau bagaimanapun, tetapan lalai adalah lebih tegas untuk [Imbas seluruh komputer](#)

:

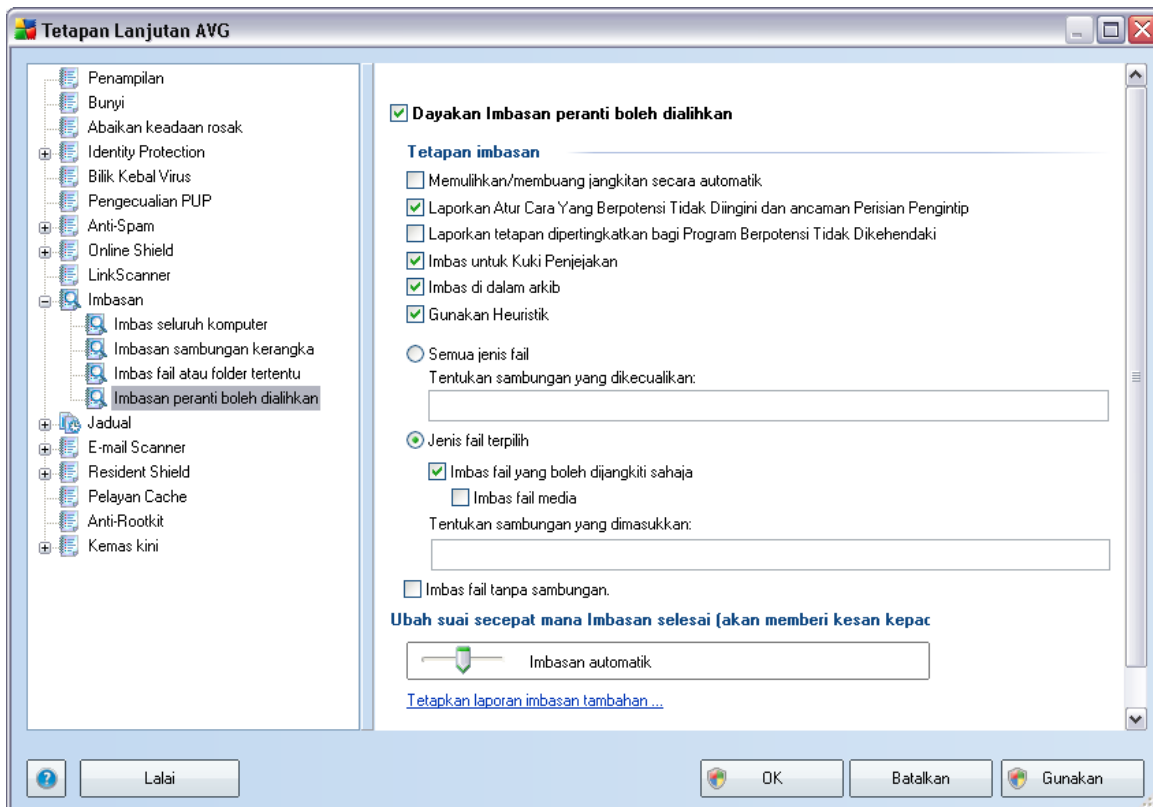


Semua parameter yang disediakan dalam dialog konfigurasi ini hanya digunakan pada kawasan yang dipilih untuk imbasan dengan **Imbas fail atau folder tertentu!**

Nota: Untuk penerangan mengenai parameter tertentu, sila rujuk bab **Tetapan Lanjutan AVG / Imbasan / Imbas Seluruh Komputer**.

10.10.4. Imbasan Peranti Boleh Dialih

Antara muka pengeditan untuk **Imbasan peranti boleh dialihkan** juga sama dengan dialog pengeditan **Imbas Seluruh Komputer**:



Imbasan peranti boleh dialihkan dilancarkan secara automatik apabila anda melampirkan sebarang peranti boleh dialihkan ke komputer anda. Secara lalai, pengimbasan ini dimatikan. Walau bagaimanapun, ia adalah penting untuk mengimbas peranti boleh dialihkan untuk kemungkinan ancaman memandangkan ini adalah sumber jangkitan utama. Untuk membuatkan imbasan ini bersedia dan dilancarkan secara automatik apabila diperlukan, tanda opsyen **Dayakan imbasan peranti boleh dialihkan**.

Nota: Untuk penerangan mengenai parameter tertentu, sila rujuk bab [Tetapan Lanjutan AVG / Imbasan / Imbas Seluruh Komputer](#).

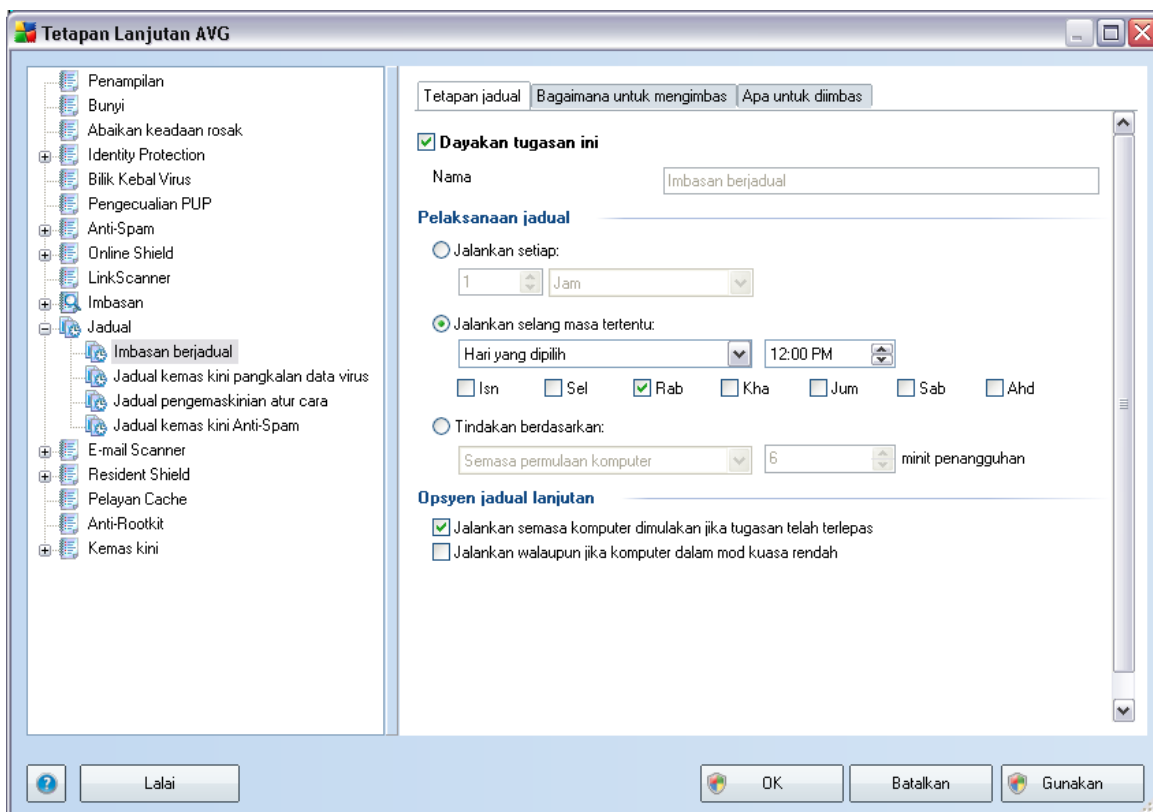
10.11. Jadual

Dalam bahagian **Jadual** anda boleh mengedit tetapan lalai bagi:

- [Jadual imbasan seluruh komputer](#)
- [Jadual kemas kini pangkalan data virus](#)
- [Jadual kemas kini atur cara](#)
- [Jadual kemas kini AntiSpam](#)

10.11.1. Imbasan yang Dijadualkan

Parameter bagi imbasan yang dijadualkan boleh diedit (*atau jadual baru disediakan*) pada tiga tab:



Pada tab **Jadualkan tetapan** anda boleh menanda/menyahtandakan dahulu item **Dayakan tugas ini** untuk menyahaktifkan ujian yang dijadualkan buat sementara dan menghidupkannya semua apabila perlu.

Seterusnya, dalam medan teks dipanggil **Nama** (*dinyahaktifkan untuk semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara. Untuk jadual yang baru ditambah (*anda boleh menambah jadual baru dengan mengklik kanan tetikus item **Imbasan yang dijadualkan** dalam pepohon navigasi kiri*) anda boleh menentukan nama anda sendiri dan jika medan teks akan terbuka untuk pengeditan. Cuba selalu gunakan nama yang ringkas, deskriptif dan sesuai untuk imbasan untuk membuatkan ia mudah untuk kemudian, mengenal pasti imbasan dari yang lain.

Contoh: Ia tidak sesuai untuk memanggil imbasan dengan nama "Imbasan baru" atau "Imbasan saya" memandangkan nama ini tidak merujuk kepada apa yang sebenarnya imbasan periksa. Sebaliknya, contoh nama deskriptif adalah "Imbasan kawasan sistem" dll. Serta, tidak perlu untuk menentukan jika nama imbasan sama ada ia adalah imbasan seluruh komputer atau hanya imbasan fail atau folder yang dipilih - imbasan anda sendiri yang akan sentiasa menjadi versi khusus bagi [imbasan bagi fail atau folder yang dipilih](#).

Di dalam dialog ini anda boleh menentukan lebih lanjut parameter imbasan yang berikut:

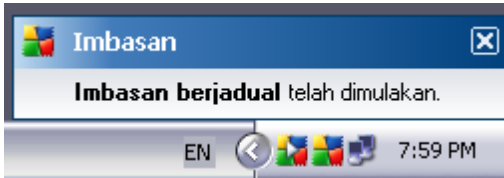
Pelaksanaan jadual

Di sini, anda boleh menentukan jarak waktu untuk pelancaran imbasan baru yang dijadualkan. Pemasaan boleh menjadi sama ada ditakrifkan oleh pelancaran imbasan berulang selepas satu tempoh masa tertentu (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan pada jarak waktu khusus ...**), atau berkemungkinan dengan mentakrifkan peristiwa yang pelancaran imbasan harus dikaitkan dengan (**Tindakan berdasarkan permulaan komputer**).

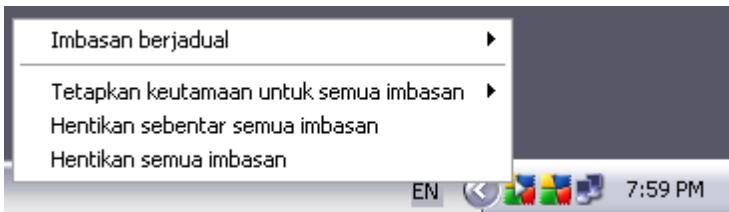
Opsyen jadual lanjutan

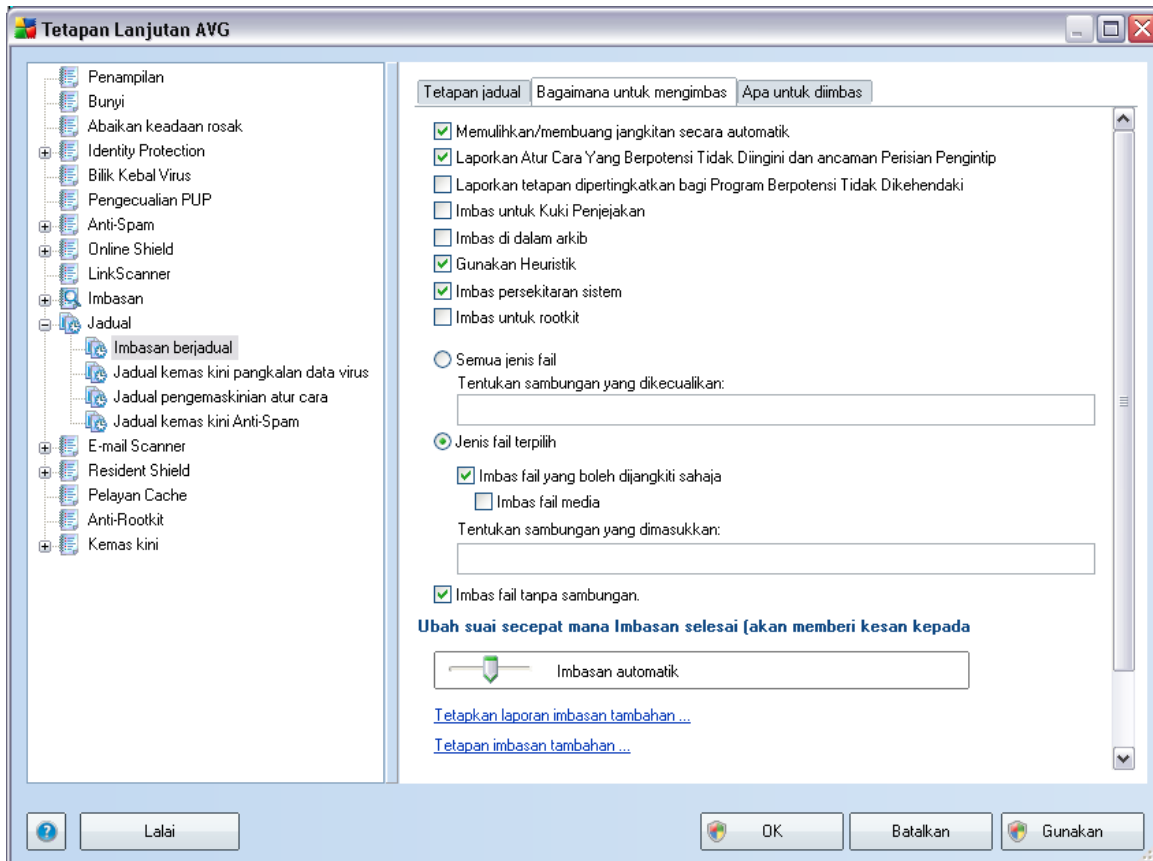
Bahagian ini membenarkan anda untuk mentakrifkan di bawah keadaan mana imbasan patut/tidak patut dilancarkan jika komputer di dalam mod kuasa rendah atau dimatikan sepenuhnya.

Apabila imbasan yang dijadualkan telah dilancarkan dalam masa yang telah ditentukan, anda akan diberitahu mengenai fakta ini melalui tetingkap pop muncul pada [ikon dulang sistem AVG](#):



Kemudian, [Ikon dulang sistem AVG](#) yang baru muncul (*dalam warna penuh dengan anak panah putih - lihat gambar di atas*) memberitahu imbasan yang dijadualkan sedang dijalankan. Klik kanan pada ikon AVG yang sedang dijalankan untuk membuka menu konteks di mana anda boleh menentukan untuk menjedakan atau malahan untuk menghentikan imbasan yang dijalankan:





Pada tab ***Cara untuk mengimbas*** anda akan menemui senarai parameter pengimbasan yang boleh dihidupkan/dimatikan secara pilihan. Secara lalai, kebanyakan parameter dibuka dan kefungsiannya akan dilaksanakan semasa pengimbasan. Melainkan anda mempunyai alasan yang sah untuk mengubah tetapan ini, kami mengesyorkan untuk mengekalkan konfigurasi yang dipratetap ini:

- ***Pulihkan/buang jangkitan secara automatik*** - jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika rawatan tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dibuang ke ***Bilik Kebal Virus***.
- ***Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip*** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin ***AntiPerisian Pengintip***, dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia](#)

[biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini** - jika pilihan sebelumnya diaktifkan, anda juga boleh menanda kotak ini untuk mengesan pakej diluaskan bagi [perisian pengintip](#): atur cara adalah sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat kemudiannya. Ini adalah ukuran tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas untuk Kuki Penjejakan** - (secara lalai, dihidupkan): parameter bagi komponen [AntiPerisian Pengintip](#) ini mentakrifkan bahawa kuki itu mesti dikesan sewaktu pengimbasan (*kuki HTTP digunakan untuk pengesanan, penjejakan dan mengekalkan maklumat khusus mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*)
- **Imbas dalam arkib** - (secara lalai, dihidupkan): parameter ini menetapkan imbasan harus memeriksa semua fail walaupun jika ia disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** - (secara lalai, dihidupkan): analisis heuristik (*persaingan dinamik bagi arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu pengimbasan.
- **Imbas persekitaran sistem** - (secara lalai, dihidupkan): pengimbasan juga akan memeriksa kawasan sistem bagi komputer anda;
- **Imbas untuk rootkit** - tandakan rait item ini jika anda mahu memasukkan pengesanan rootkit ke dalam pengimbasan seluruh komputer. Pengesanan rootkit juga tersedia dengan sendiri dalam komponen [AntiRootkit](#);

Seterusnya, anda harus menentukan sama ada anda mahu mengimbas

- **Semua jenis fail** dengan kemungkinan pengecualian yang ditakrifkan daripada imbasan dengan memberikan senarai yang pemanjangan fail yang dipisahkan oleh koma (*apabila disimpan, koma bertukar kepada koma bertitik*) yang tidak harus diimbas;
- **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau*

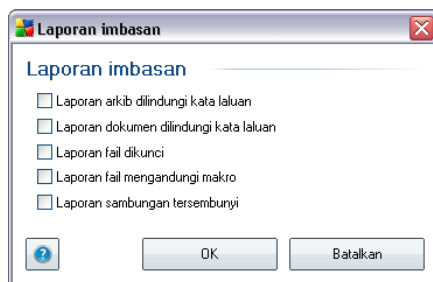
sesetengah fail bukan boleh laku), termasuk fail media (video, fail audio - jika anda membiarkan kotak ini tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.

- Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.

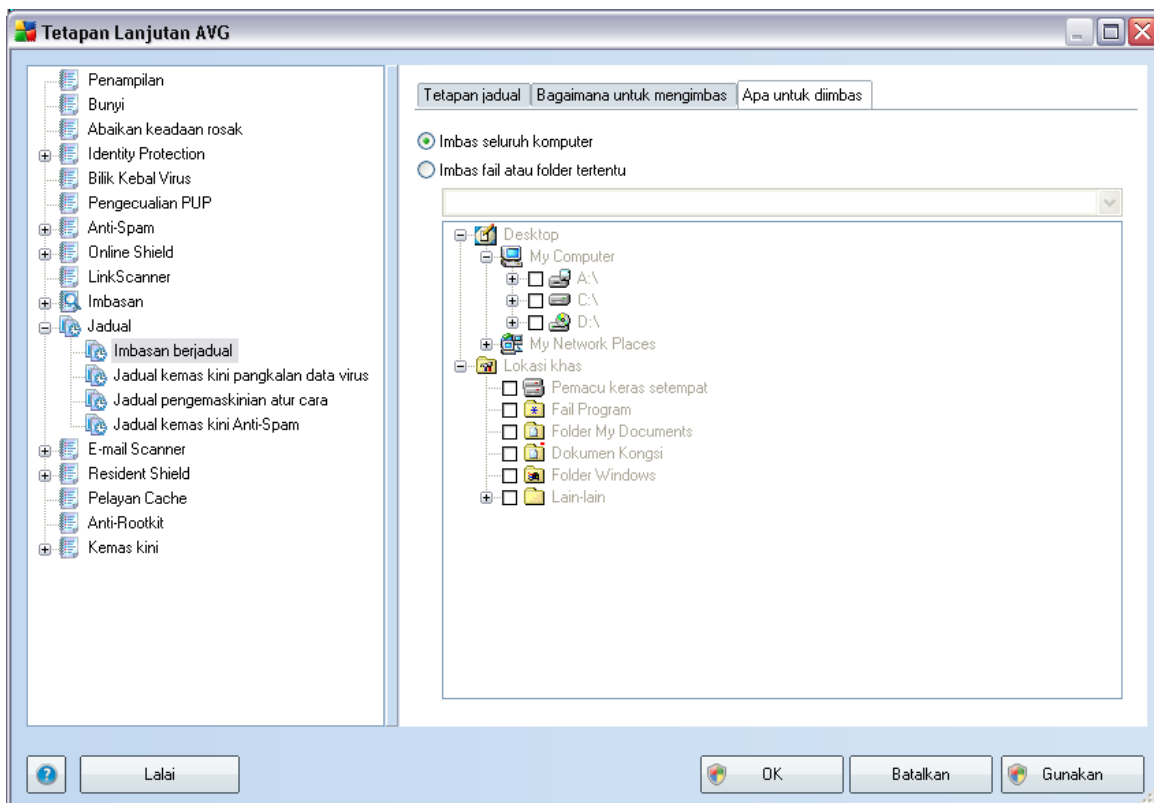
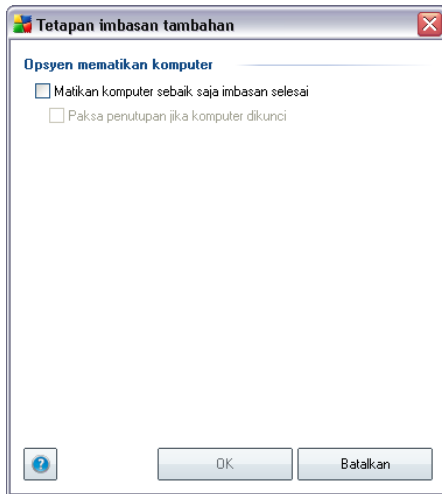
Keutamaan proses imbasan

Dalam bahagian **Keutamaan proses imbasan** anda boleh menentukan selanjutnya kelajuan pengimbasan yang dikehendaki bergantung kepada penggunaan sumber sistem. Secara lalai, opsyen ini ditetapkan kepada tahap sederhana bagi penggunaan sumber automatik. Jika anda mahu pengimbasan dijalankan dengan lebih cepat, ia akan mengambil masa yang kurang tetapi penggunaan sumber sistem akan meningkat secara signifikan sewaktu imbasan dan akan melambatkan aktiviti anda yang lain pada PC (*opsyen ini boleh digunakan semasa komputer anda dihidupkan tetapi tiada siapa yang sedang bekerja dengannya*). Sebaliknya, anda boleh mengurangkan penggunaan sumber sistem dengan menambah tempoh pengimbasan.

Klik pautan **Tetapan laporan imbasan tambahan ...** untuk membuka tettingkap dialog tersendiri yang dipanggil **Laporan imbasan** di mana anda boleh menanda rait beberapa item untuk mentakrifkan penemuan imbasan yang harus dilaporkan:



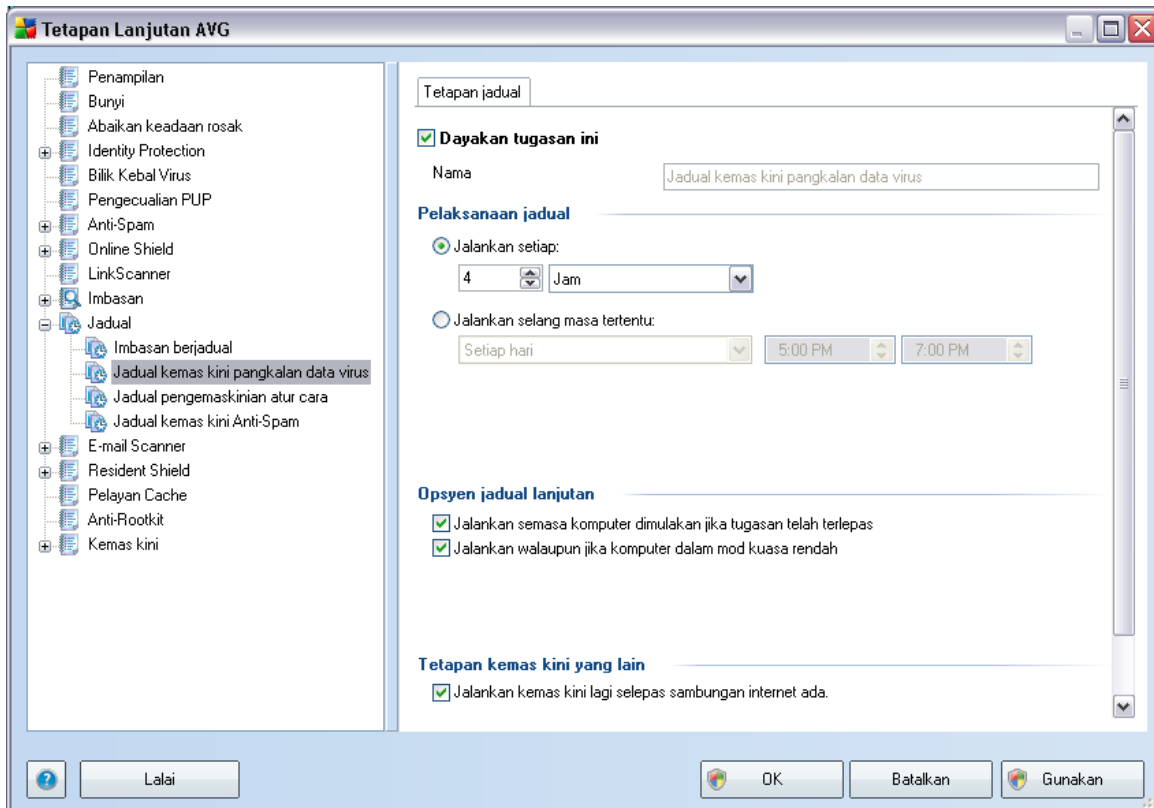
Klik **Tetapan imbasan tambahan ...** untuk membuka dialog **Opsyen mematikan komputer** lain di mana anda boleh menentukan sama ada komputer harus dimatikan secara automatik sebaik sahaja proses pengimbasan yang berjalan tamat. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).



Pada tab ***Apa yang hendak diimbas*** anda boleh menentukan sama ada anda mahu

menjadualkan [pengimbasan seluruh komputer](#) atau [pengimbasan fail atau folder tertentu](#). Jika anda memilih pengimbasan fail atau folder tertentu, dalam bahagian bawah dialog ini, struktur pepohonan yang dipaparkan diaktifkan dan anda boleh menentukan folder untuk diimbas.

10.11.2. Jadual Kemas Kini Pangkalan Data Virus



Pada tab **Jadualkan tetapan** pertama sekali, anda boleh menanda/menyahtanda item **Dayakan tugas ini** untuk menyahaktifkan kemas kini pangkalan data virus yang dijadualkan sementara dan menghidupkannya semula apabila perlu. Penjadualan kemas kini pangkalan data virus asas diliputi dalam komponen [Pengurus Kemas Kini](#). Dalam dialog ini, anda boleh menyediakan beberapa parameter terperinci bagi jadual kemas kini pangkalan data virus. Dalam medan teks yang dipanggil **Nama** (*nyahaktifkan semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.

Pelaksanaan jadual

Dalam bahagian ini, tentukan jarak waktu untuk pelancaran kemas kini pangkalan data virus yang baru dijadualkan. Pemasaan boleh sama ada, ditakrifkan oleh pelancaran kemas kini berulang selepas satu tempoh tertentu bagi masa (***Jalankan setiap ...***) atau dengan menentukan tarikh dan masa sebenar (***Jalankan pada waktu tertentu ...***).

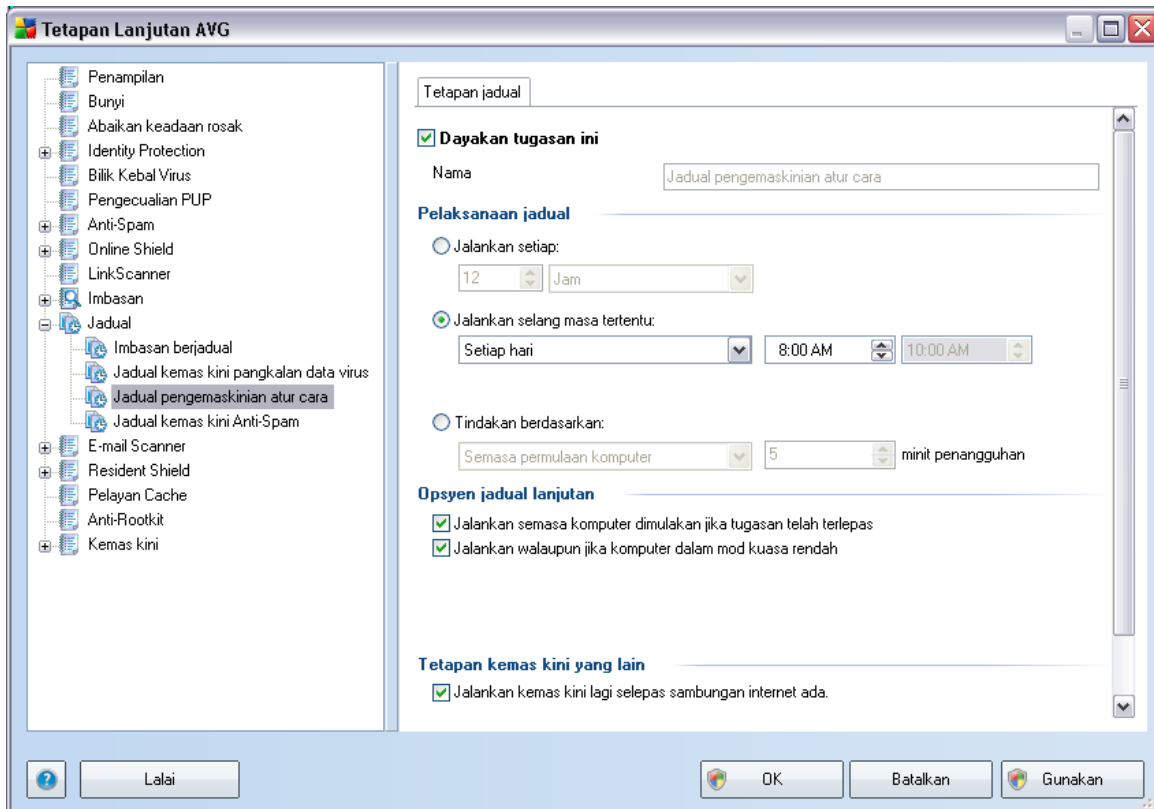
Opsyen jadual lanjutan

Bahagian ini membenarkan anda mentakrifkan di bawah keadaan mana kemas kini pangkalan data virus harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

Tetapan kemas kini yang lain

Akhir sekali, tandakan opsiyen ***Jalankan sebaik sahaja sambungan Internet tersedia*** untuk memastikan jika sambungan internet rosak dan proses kemas kini gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan internet disimpan semula.

Sebaik sahaja kemas kini yang dijadualkan dilancarkan tepat pada masa anda telah tentukan, anda akan diberitahu mengenai fakta ini melalui tettingkap pop timbul yang terbuka pada [ikon dulang sistem AVG](#) (diberikan bahawa anda telah menyimpan konfigurasi lalai bagi dialog [Tetapan/Rupa Lanjutan](#)).



Pada tab **Jadualkan tetapan** anda boleh pertama sekali, menanda atau nyahtanda item **Dayakan tugas ini** untuk menyahaktifkan kemas kini atur cara yang dijadualkan buat sementara dengan mudah dan menghidupkannya semula apabila perlu. Dalam medan teks yang dipanggil **Nama** (*dinyahaktifkan untuk semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.

Pelaksanaan jadual

Di sini, tentukan jarak waktu untuk kemas kini atur cara yang baru dilancarkan. Masa boleh sama ada ditentukan oleh pelancaran kemas kini berulang selepas tempoh masa tertentu (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan dalam masa tertentu ...**), atau kemungkinan dengan menentukan acara yang pelancaran kemas kini harus dikaitkan dengan (**Tindakan berdasarkan pada permulaan komputer**).

Opsyen jadual lanjutan

Bahagian ini membenarkan anda menentukan dalam keadaan apa kemas kini atur cara harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

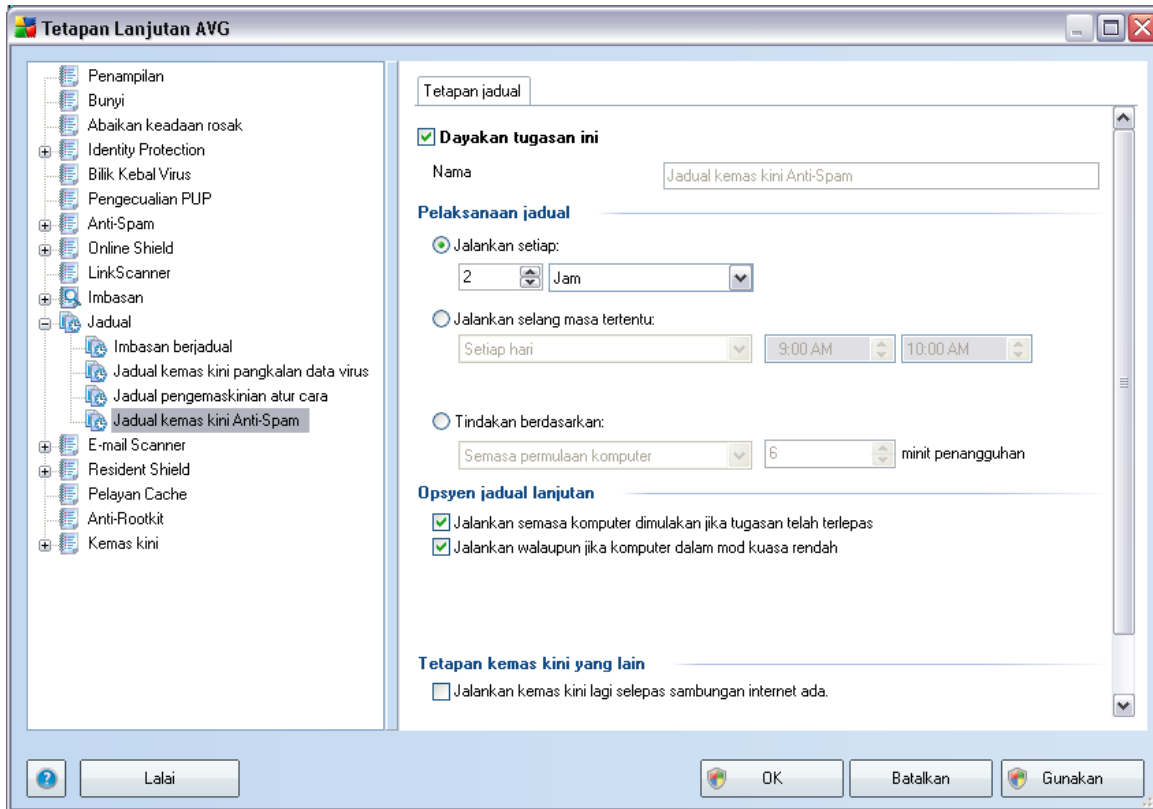
Tetapan kemas kini yang lain

Tandakan opsyen ***Jalankan kemas kini semula sebaik sahaja sambungan Internet tersedia*** untuk memastikan jika sambungan internet rosak dan proses kemas kini gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan internet disimpan semula.

Sebaik sahaja kemas kini yang dijadualkan dilancarkan tepat pada masa anda telah tentukan, anda akan diberitahu mengenai fakta ini melalui tettingkap pop timbul yang terbuka pada [ikon dulang sistem AVG](#) (diberikan bahawa anda telah menyimpan konfigurasi lalai bagi dialog [Tetapan/Rupa Lanjutan](#)).

Perhatian: Jika persamaan masa bagi kemas kini atur cara yang dijadualkan dan imbasan yang dijadualkan berlaku, proses kemas kini adalah lebih utama dan imbasan akan diganggu.

10.11.3. Jadual Kemas Kini AntiSpam



Pada tab **Tetapan jadual** anda boleh menanda/tidak menanda item **Dayakan tugas ini** untuk dengan mudah menyahdayakan kemas kini **AntiSpam** yang dijadualkan buat sementara dan menghidupkannya semula apabila perlu. Penjadualan kemas kini **AntiSpam** asas diliputi dalam komponen **Pengurus Kemas Kini**. Dalam dialog ini, anda boleh menyediakan beberapa parameter terperinci bagi jadual kemas kini. Dalam medan teks yang dipanggil **Nama** (*nyahaktifkan semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.

Pelaksanaan jadual

Di sini, tentukan jarak waktu untuk pelancaran kemas kini **AntiSpam** yang baru dijadualkan. Pengaturan masa boleh sama ada ditentukan oleh pelancaran kemas kini **AntiSpam** selepas tempoh masa tertentu (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan dalam masa tertentu ...**), atau berkemungkinan dengan menentukan acara yang pelancaran kemas kini harus dikaitkan



dengan (***Tindakan berdasarkan permulaan komputer***).

Opsyen jadual lanjutan

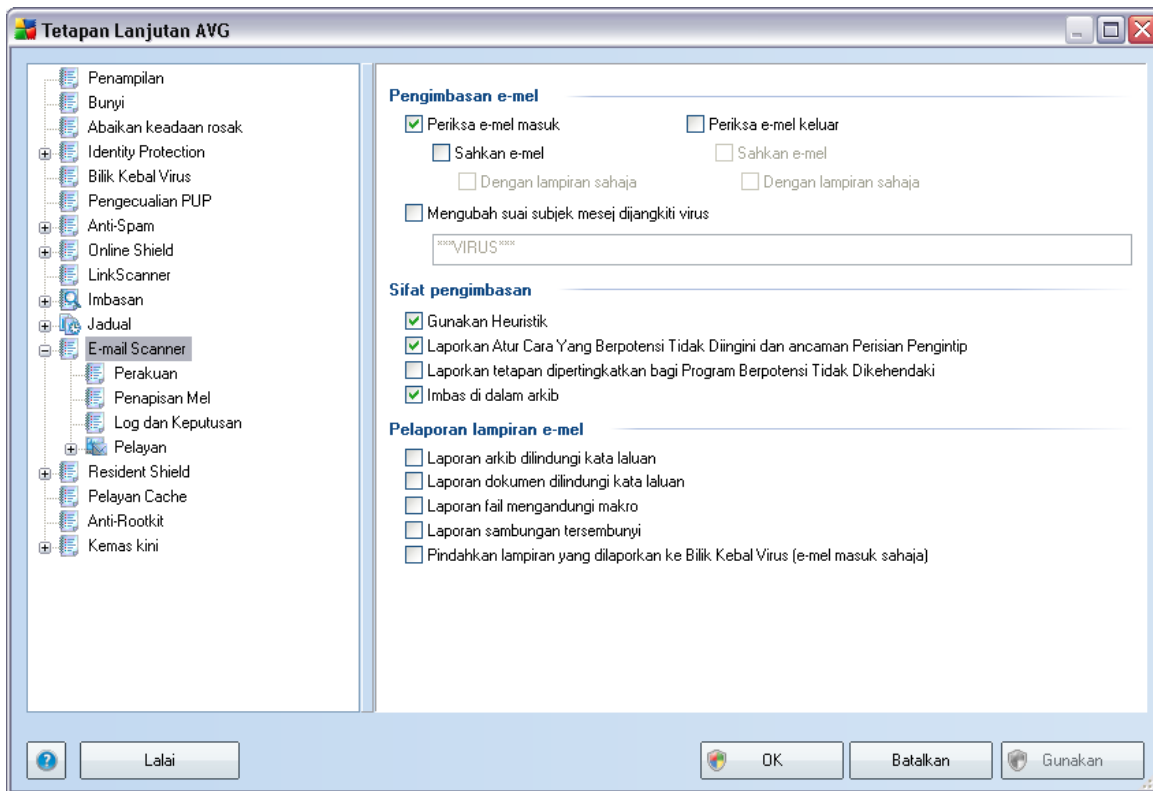
Bahagian ini membolehkan anda menentukan dalam keadaan apa kemas kini [AntiSpam](#) harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

Tetapan kemas kini yang lain

Tanda pilihan ***Jalankan kemas kini semula sebaik sahaja sambungan Internet tersedia*** untuk memastikan jika sambungan internet rosak dan proses kemas kini [Anti-Spam](#) gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan internet disimpan semula.

Sebaik sahaja imbasan yang dijadualkan dilancar tepat masanya yang anda telah tentukan, anda akan diberitahu mengenai fakta ini melalui tettingkap pop timbul yang dibuka pada [ikon dulang sistem AVG](#) (diberikan bahawa anda telah mengekalkan konfigurasi lalai bagi dialog [Tetapan/Rupa Lanjutan](#)).

10.12. Pengimbas E-mel



Dialog **Pengimbas E-mel** dibahagikan ke dalam tiga bahagian:

- **Pengimbasan e-mel** - dalam bahagian ini, anda boleh menetapkan asas ini untuk mesej e-mel masuk dan/atau keluar:
 - o Jika mesej e-mel harus diimbas untuk virus.
 - o Jika teks perakuan harus ditambah kepada hujung setiap mesej untuk menyatakan ia tidak mengandungi virus. Teks boleh diubah suai dalam dialog [Perakuan](#).
 - o Jika teks perakuan harus ditambahkan hanya kepada mesej dengan lampiran.

Untuk **Menggubah subjek mesej dijangkiti virus**, tandakan kotak dan taip nilai yang diinginkan dalam medan teks. Ia kemudiannya akan ditambahkan ke medan subjek setiap mesej e-mel yang dijangkiti untuk pengenalan dan penapisan yang

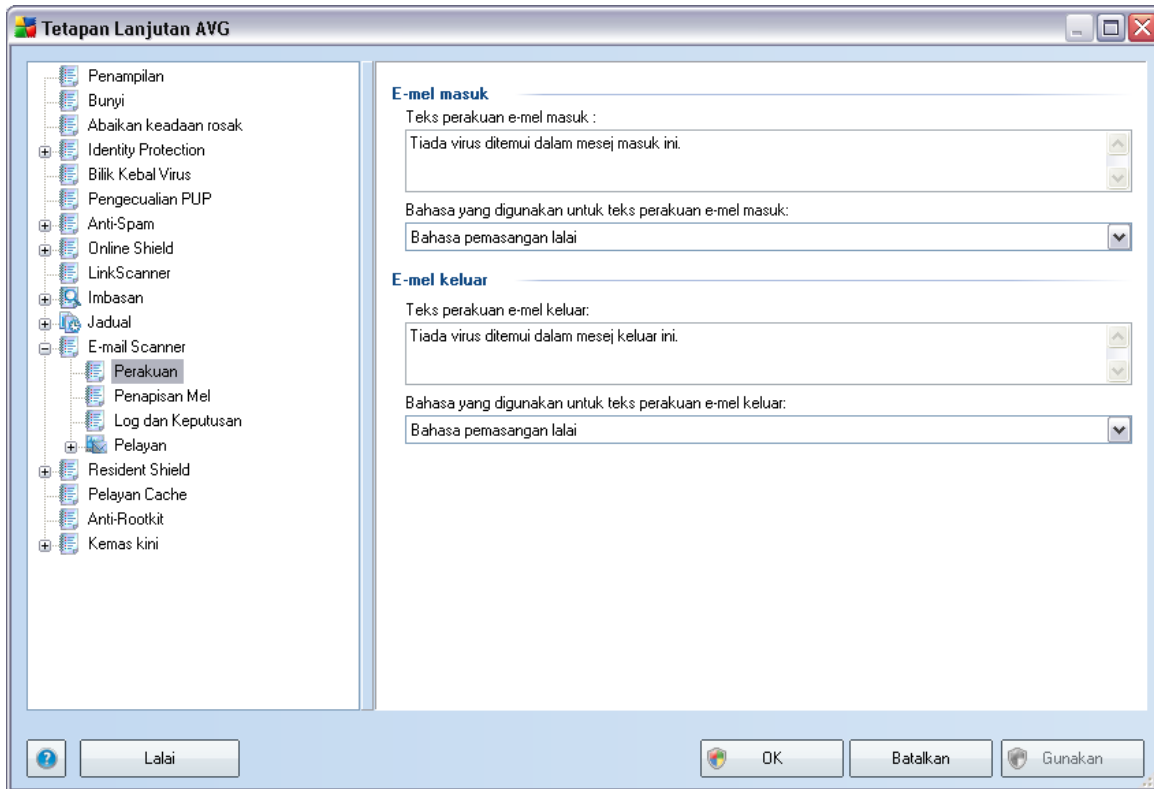
lebih mudah. Nilai lalai ialah ***VIRUS*** yang mana kami syorkan dibiarkan.

- **Sifat pengimbasan** - dalam bahagian ini, anda boleh menentukan cara mesej e-mel akan diimbas:
 - o **Gunakan Heuristik** – tandakan untuk menggunakan [kaedah pengesanan heuristik](#) semasa mengimbas mesej e-mel. Apabila opsyen ini hidup, anda boleh menapis lampiran e-mel bukan sahaja dengan sambungan tetapi juga kandungan sebenar lampiran boleh dipertimbangkan. Penapisan boleh ditetapkan dalam dialog [Penapisan Mel](#).
 - o **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
 - o **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini** - jika pilihan sebelumnya diaktifkan, anda juga boleh menanda kotak ini untuk mengesan pakej diluaskan bagi [perisian pengintip](#): atur cara adalah sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat kemudiannya. Ini adalah ukuran tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
 - o **Imbas dalam arkib** – tandakan untuk mengimbas kandungan arkib yang dilampirkan kepada mesej e-mel.
- **Pelaporan lampiran e-mel** - dalam bahagian ini, anda boleh menetapkan laporan tambahan mengenai fail yang berpotensi berbahaya atau mencurigakan. Sila maklum bahawa tiada dialog amaran yang akan dipaparkan, hanya teks perakuan akan ditambah ke penghujung mesej e-mel, dan semua laporan akan disenaraikan dalam dialog [pengesanan Pengimbas E-mel](#):
 - o **Laporkan arkib yang dilindungi kata laluan** - arkib (ZIP, RAR dll.) yang dilindungi oleh kata laluan adalah tidak mungkin diimbas untuk virus; tandakan kotak untuk melaporkan ini sebagai berpotensi berbahaya.
 - o **Laporkan dokumen yang dilindungi kata laluan** – dokumen dilindungi kata laluan tidak mungkin diimbas untuk virus; tandakan kotak untuk

melaporkannya sebagai berpotensi berbahaya.

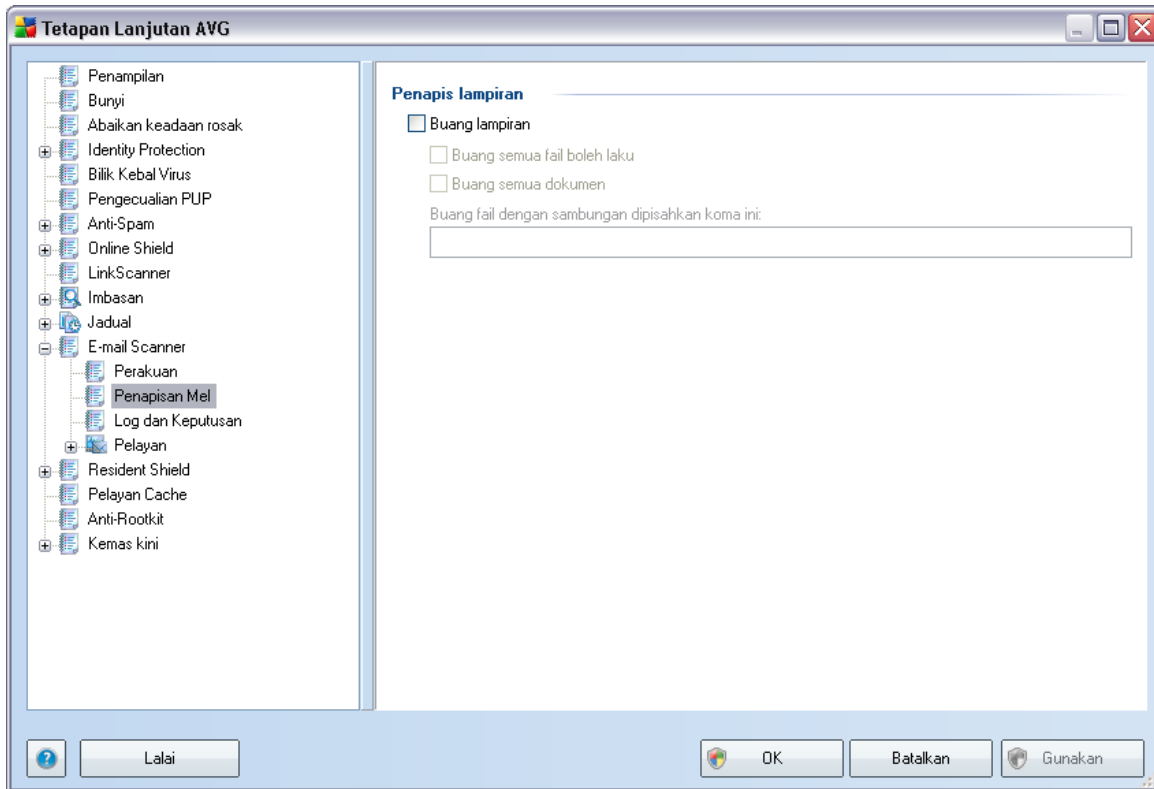
- o **Laporkan fail mengandungi makro** – makro adalah urutan langkah yang dipratakrifkan untuk menjadikan tugas tertentu lebih mudah untuk pengguna (makro MS Word dikenali ramai). Dengan itu, makro boleh mengandungi arahan berpotensi berbahaya, dan anda mungkin ingin menandakan kotak untuk memastikan fail dengan makro akan dilaporkan sebagai mencurigakan.
- o **Laporkan sambungan tersembunyi** - sambungan tersembunyi boleh menjadikan cthnya. fail boleh laku mencurigakan "sesuatu.txt.exe" kelihatan seperti fail teks biasa yang tidak berbahaya "sesuatu.txt"; tandakan kotak untuk melaporkan ini sebagai berpotensi berbahaya.
- o **Alihkan lampiran yang dilaporkan ke Bilik Kebal Virus** - tentukan sama ada anda hendak diberitahu melalui e-mel mengenai arkib yang dilindungi kata laluan, dokumen yang dilindungi kata laluan, makro mengandungi fail dan/atau fail dengan sambungan tersembunyi dikesan sebagai lampiran bagi mesej e-mel yang diimbis. Jika mesej seperti itu dikenal pasti sewaktu pengimbasan, tentukan sama ada objek berjangkit yang dikesan harus dialih ke [Bilik Kebal Virus](#).

10.12.1. Perakuan



Dalam dialog **Sijil** anda boleh menentukan teks apa sebenarnya yang harus terkandung dalam nota sijil dan dalam bahasa apa. Ini harus ditentukan secara berasingan untuk **Mel masuk** dan **Mel keluar**.

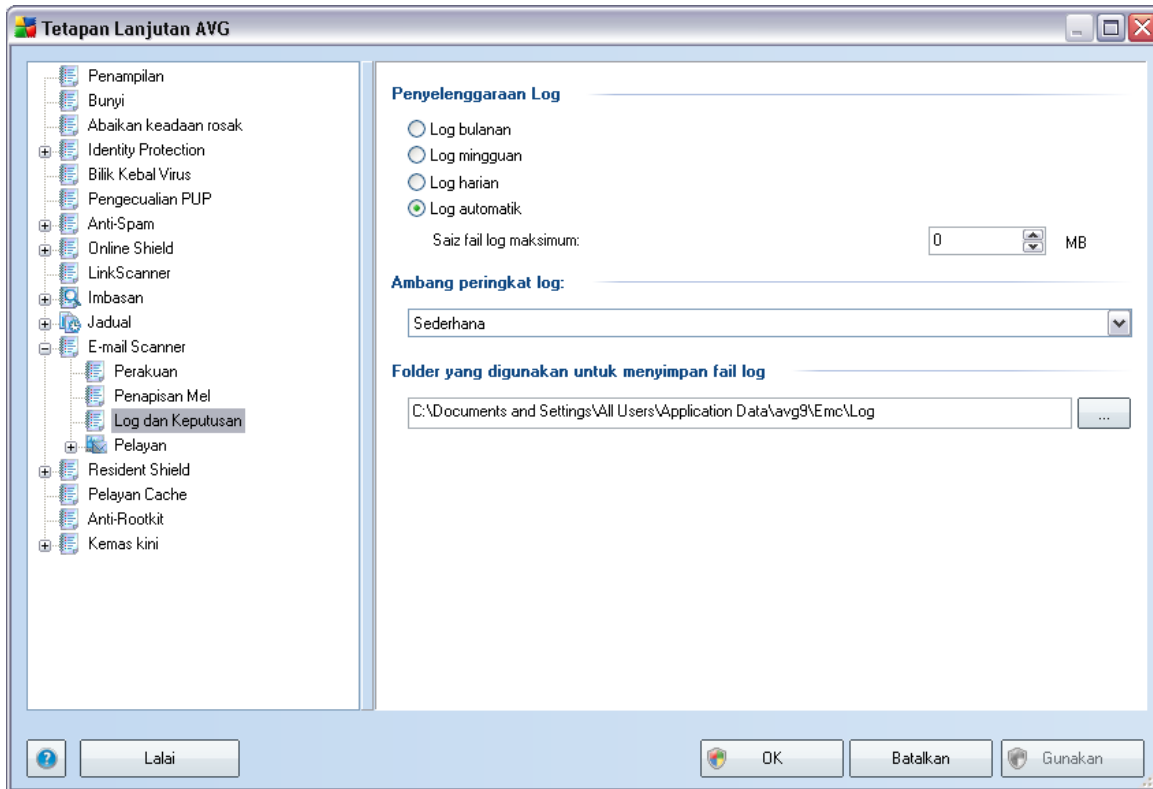
10.12.2. Penapisan Mel



Dialog **Penapis lampiran** membenarkan anda menyediakan parameter untuk pengimbasan lampiran mesej e-mel. Secara lalai, opsiyen **Buang lampiran** dimatikan. Jika anda memutuskan untuk mengaktifkannya, semua lampiran mesej e-mel yang dikesan sebagai berjangkit atau berpotensi berbahaya akan dibuang secara automatik. Jika anda mahu menentukan jenis lampiran khusus yang harus dibuang, pilih opsiyen berikut:

- **Buang semua fail boleh laku** - semua fail *.exe akan dipadamkan
- **Buang semua dokumen** - semua fail *.doc, *.docx, *.xls, *.xlsx akan dipadam
- **Buang fail dengan sambungan yang dipisahkan oleh koma** - akan membuang semua fail dengan sambungan yang ditentukan

10.12.3. Log dan Keputusan

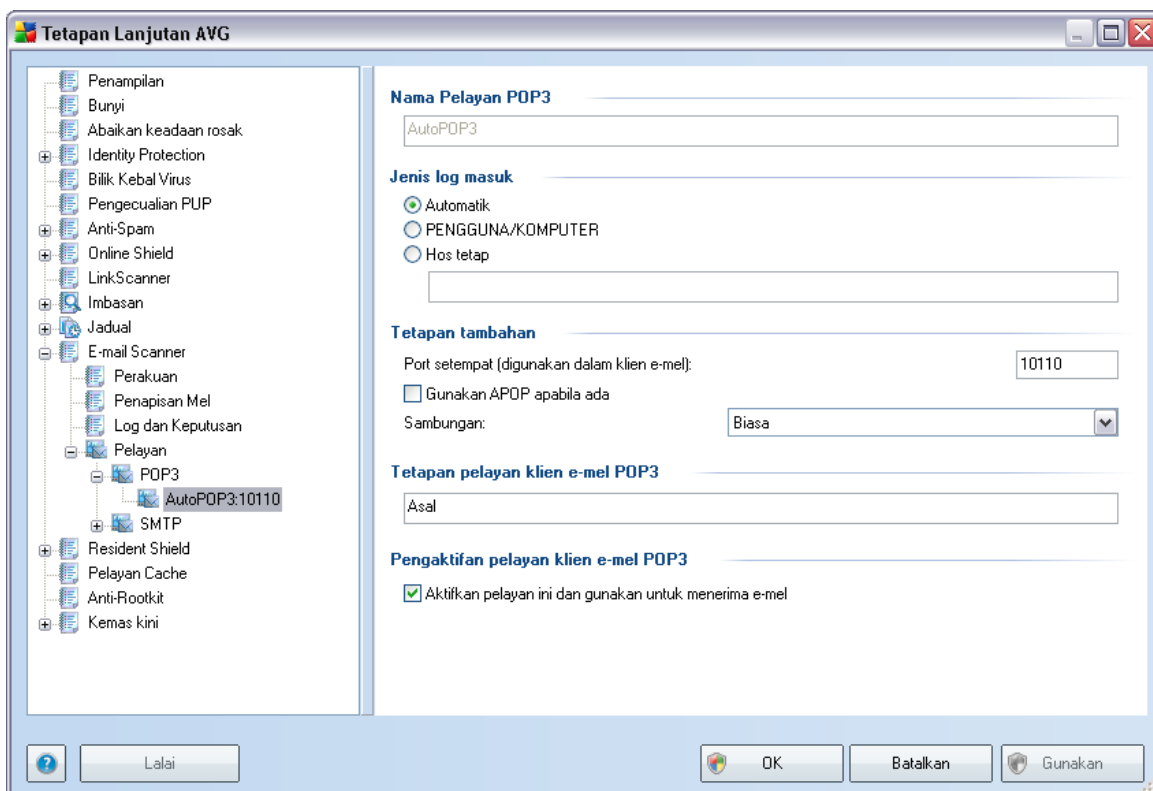


Dialog dibuka melalui item navigasi **Log dan Keputusan** membenarkan anda menentukan parameter untuk penyelenggaraan keputusan pengimbasan e-mel. Dialog dibahagikan kepada beberapa bahagian:

- **Penyelenggaraan Log** - menentukan sama ada anda mahu melog maklumat pengimbasan e-mel mengikut harian, mingguan, bulanan, ... ; serta menentukan saiz maksimum bagi fail log (*dalam MB*)
- **Ambang tahap log** - tahap sederhana disediakan secara lalai - anda boleh memilih tahap lebih rendah (*maklumat sambungan permulaan log*) atau tahap lebih tinggi (*log semua lalu lintas*)
- **Folder yang digunakan untuk menyimpan fail log** - tentukan di mana fail log harus diletakkan

10.12.4. Pelayan

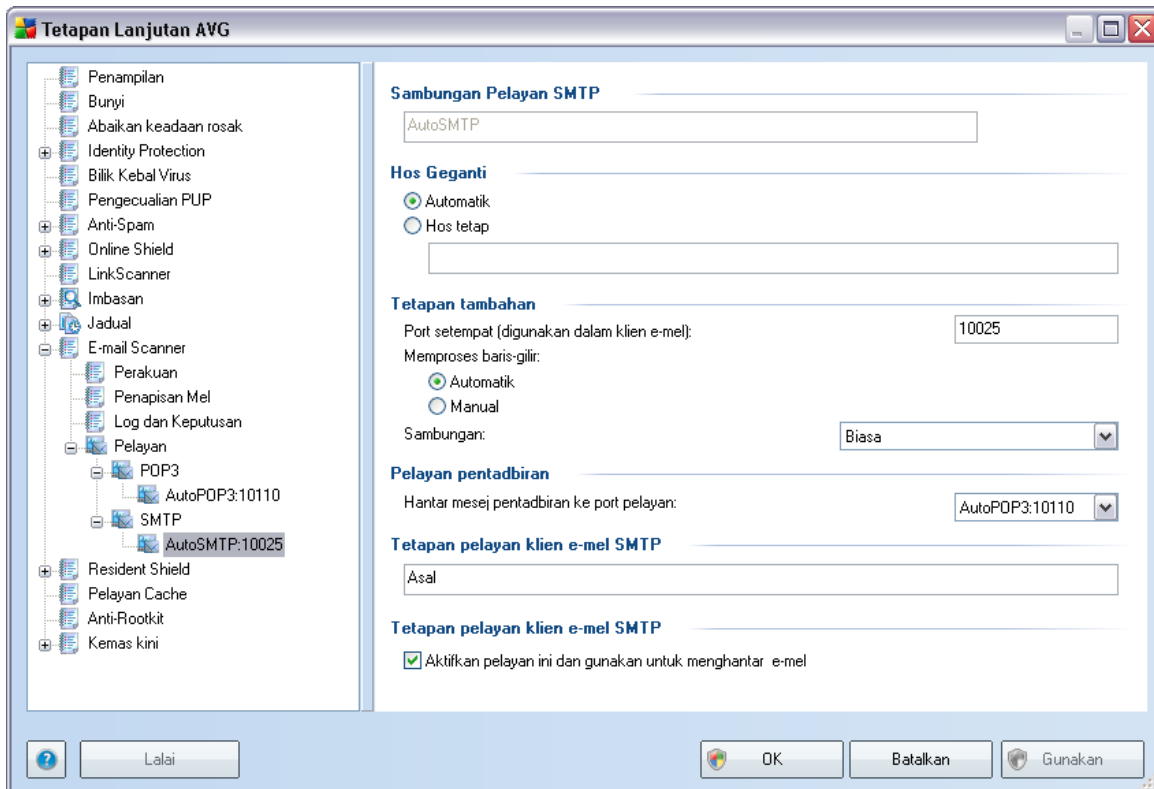
Dalam bahagian **Pelayan** anda boleh mengedit parameter bagi pelayan komponen **Pengimbas E-mel**, atau menyediakan pelayan baru menggunakan butang **Tambah pelayan baru**.



Dalam dialog ini (dibuka melalui **Pelayan / POP3**) anda boleh menyediakan pelayan **Pengimbas E-mel** menggunakan protokol POP3 untuk mel masuk:

- **Nama Pelayan POP3** - taipkan nama pelayan atau kekalkan nama lalai AutoPOP3
- **Jenis log masuk** - menentukan kaedah untuk menentukan pelayan mel yang digunakan untuk mel masuk:
 - o **Automatik** – Log masuk akan dijalankan secara automatik, mengikut tetapan klien e-mel anda.

- o **PENGGUNA/KOMPUTER** – kaedah paling mudah dan paling kerap digunakan untuk menentukan pelayan mel destinasi ialah kaedah proksi. Untuk menggunakan kaedah ini, tentukan nama atau alamat (atau serta port) sebagai sebahagian daripada nama pengguna log masuk untuk pelayan mel yang diberikan, memisahkannya dengan aksara /. Contohnya, untuk akaun user1 pada pelayan pop.acme.com dan port 8200, anda akan menggunakan user1/pop.acme.com:8200 untuk nama log masuk.
- o **Hos tetap** – Dalam kes ini, atur cara akan sentiasa menggunakan pelayan yang dinyatakan di sini. Sila nyatakan alamat atau nama pelayan mel anda. Nama log masuk kekal tidak berubah. Untuk nama, anda boleh menggunakan nama domain (contohnya, pop.acme.com) dan juga alamat IP (contohnya, 123.45.67.89) Jika pelayan mel menggunakan port bukan standard, anda boleh menentukan port ini selepas nama pelayan menggunakan tanda titik bertindih sebagai penentu had (contohnya, pop.acme.com:8200). Port standard untuk komunikasi POP3 ialah 110.
- **Tetapan tambahan** - menentukan parameter yang lebih terperinci:
 - o **Port tempatan** - menentukan port di mana komunikasi dari aplikasi mel anda harus dijangka. Anda kemudiannya mesti menentukan dalam aplikasi mel anda port ini sebagai port untuk komunikasi POP3.
 - o **Gunakan APOP apabila tersedia** - opsyen ini memberikan log masuk pelayan mel yang lebih selamat. Ini memastikan **Pengimbas E-mel** menggunakan kaedah alternatif bagi mengemukakan kata laluan akaun pengguna untuk log masuk, menghantar kata laluan kepada pelayan tidak dalam format terbuka tetapi dalam format disulitkan menggunakan rangkaian pemboleh ubah yang diterima dari pelayan. Biasanya, ciri ini tersedia hanya apabila pelayan mel destinasi menyokongnya.
 - o **Sambungan** - dalam menu jatuh bawah, anda boleh menentukan jenis sambungan apa untuk digunakan (biasa/SSL/SSL lalai). Jika anda memilih sambungan SSL, data yang dihantar disulitkan tanpa risiko dijejaki atau diselia oleh pihak ketiga. Ciri ini juga tersedia hanya apabila pelayan mel destinasi menyokongnya.
- **Tetapan pelayan POP3 klien** - memberikan maklumat ringkas mengenai tetapan konfigurasi yang diperlukan untuk membetulkan konfigurasi klien e-mel anda (supaya **Pengimbas E-mel** akan memeriksa semua mel masuk). Ini adalah ringkasan berdasarkan kepada parameter berhubung kait yang ditentukan dalam dialog ini dan dialog berkaitan lain.
- **Pengaktifan pelayan POP3 klien e-mel** - tanda/tidak menanda item ini untuk mengaktifkan atau menyahaktifkan pelayan POP3 yang ditentukan



Dalam dialog ini (dibuka melalui **Pelayan / SMTP**) anda boleh menyediakan pelayan **Pengimbas E-mel** menggunakan protokol SMTP untuk mel keluar:

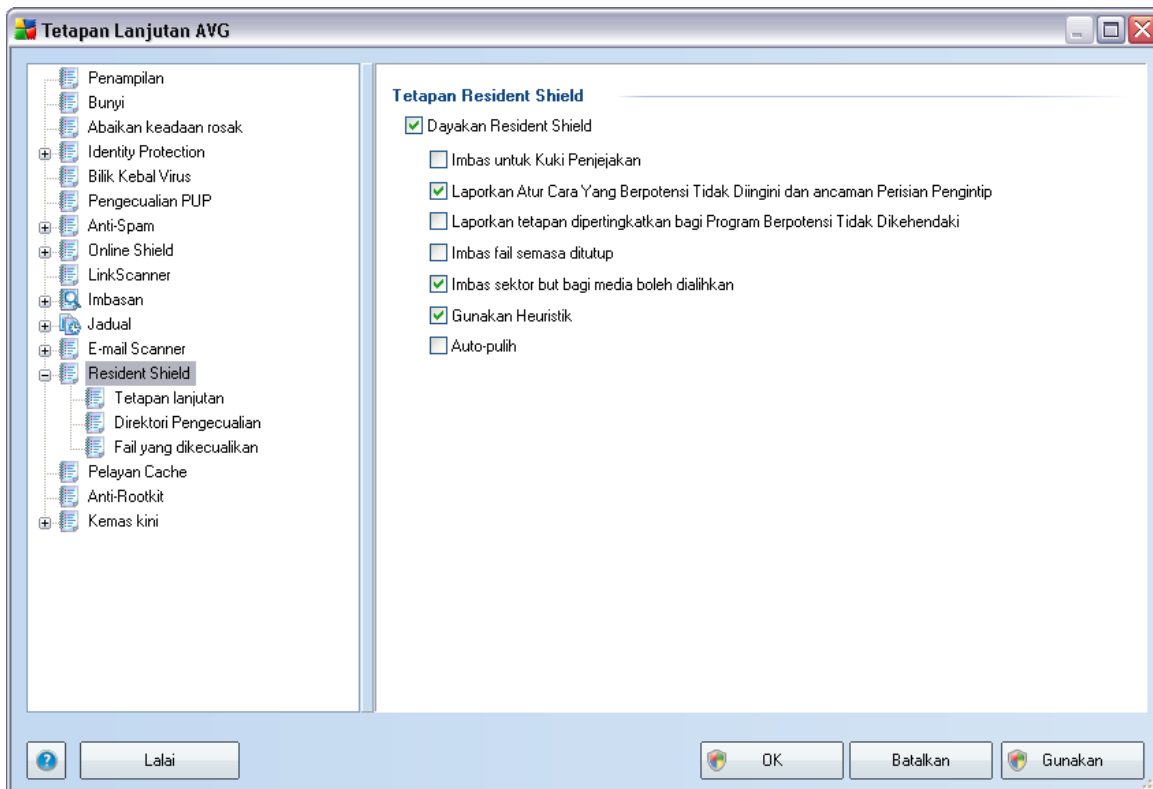
- **Nama Pelayan SMTP** - taipkan nama pelayan atau kekalkan nama lalai Auto SMTP
- **Hos Ganti** - mentakrifkan kaedah untuk menentukan pelayan mel yang digunakan untuk mel keluar:
 - o **Automatik** - log masuk akan dijalankan secara automatik mengikut tetapan klien e-mel anda
 - o **Hos tetap** - dalam kes ini, atur cara akan sentiasa menggunakan pelayar yang ditentukan di sini. Sila nyatakan alamat atau nama pelayan mel anda. Anda boleh menggunakan nama domain (sebagai contoh, smtp.acme.com) dan juga alamat IP (sebagai contoh, 123.45.67.89) sebagai nama. Jika pelayan mel menggunakan port tidak standard, anda boleh menaip port ini di belakang nama pelayan menggunakan noktah bertindih

sebagai penentu hadnya (sebagai contoh, smtp.acme.com:8200). Port standard untuk komunikasi SMTP ialah 25.

- **Tetapan tambahan** - menentukan parameter yang lebih terperinci:
 - o **Port tempatan** - menentukan port di mana komunikasi dari aplikasi mel anda harus dijangka. Kemudian, anda mesti menentukan port ini sebagai port untuk komunikasi SMTP dalam aplikasi mel anda.
 - o **Pemprosesan barisan** - menentukan kelakuan [Pengimbas E-mel](#) semasa memproses keperluan untuk menghantar mesej mel:
 - Automatik - mel keluar dihantar dengan serta-merta kepada pelayan mel sasaran
 - Manual - mesej dimasukkan ke dalam barisan mesej keluar dan dihantar kemudian
 - o **Sambungan** - dalam menu jatuh bawah ini, anda boleh menentukan jenis sambungan mana untuk digunakan (biasa/SSL/SSL laai). Jika anda memilih sambungan SSL, data yang dihantar disulitkan tanpa risiko dijejaki atau diselia oleh pihak ketiga. Ciri ini tersedia hanya apabila pelayan mel destinasi menyokongnya.
- **Pelayan pentadbiran** - menunjukkan bilangan port pelayan yang akan digunakan untuk penghantaran berbalik bagi laporan pentadbiran. Mesej-mesej ini dijana, sebagai contoh, apabila pelayan mel sasaran menolak mesej keluar atau apabila pelayan mel ini tidak tersedia.
- **Tetapan pelayan SMTP klien e-mel** - memberikan maklumat mengenai cara untuk mengkonfigurasi aplikasi mel klien supaya mesej mel keluar diperiksa menggunakan pelayan yang sedang diubah suai untuk memeriksa mel keluar. Ini adalah ringkasan berdasarkan kepada parameter berhubung kait yang ditentukan dalam dialog ini dan dialog berkaitan lain.
- **Pengaktifan pelayan SMTP klien e-mel** - tandakan/jangan tandakan kotak ini untuk mengaktifkan/menyahaktifkan pelayan SMTP yang ditentukan di atas

10.13. Perisai Residen

Komponen **Perisai Residen** memberikan perlindungan langsung bagi fail dan folder daripada virus, perisian pengintip dan malware lain.



Dalam dialog **Tetapan Perisai Residen** anda boleh mengaktifkan atau menyahaktifkan perlindungan **Perisai Residen** sepenuhnya dengan menanda/menyahtanda item **Dayakan Perisai Residen** (*opsyen ini dihidupkan secara lalai*). Selain daripada itu, anda boleh memilih ciri **Perisai Residen** harus diaktifkan:

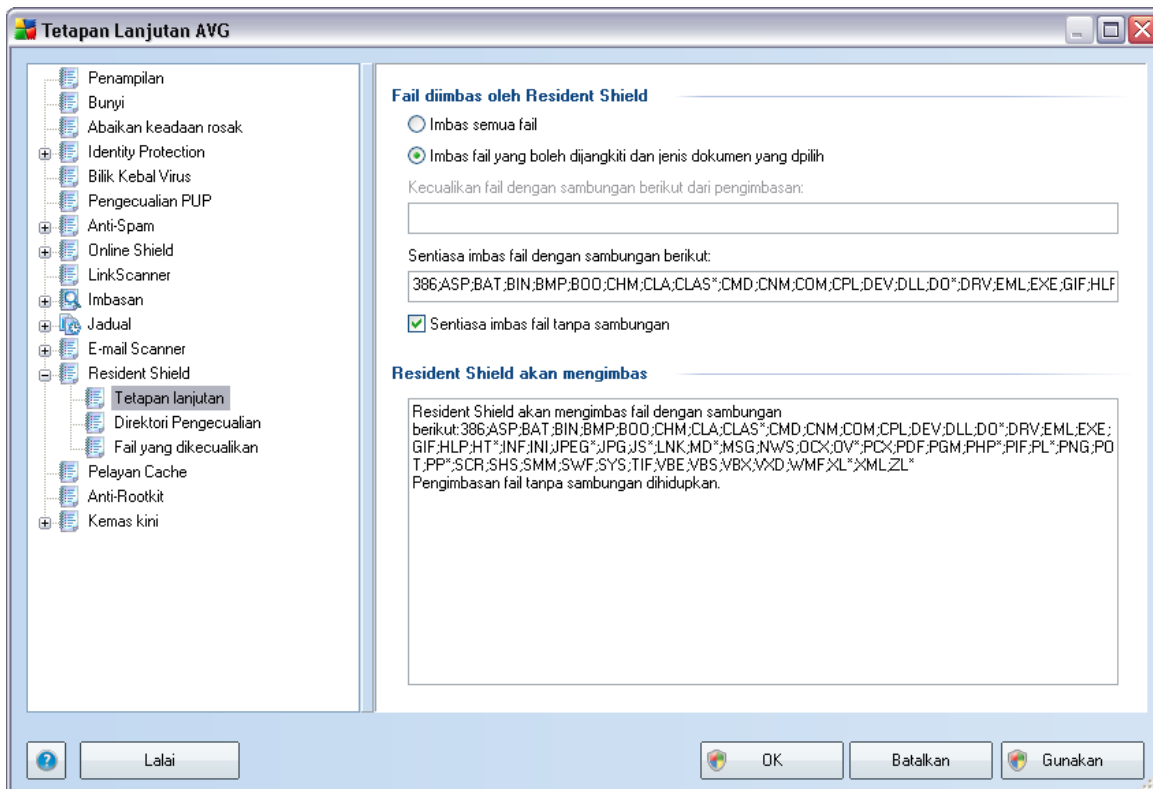
- **Imbas untuk Kuki Penjejakan** - parameter ini menentukan bahawa kuki harus dikesan sewaktu pengimbasan. (*Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik*)
- **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin **AntiPerisian Pengintip**, dan imbas untuk perisian pengintip serta untuk virus. Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia

[biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini** - jika pilihan sebelumnya diaktifkan, anda juga boleh menanda kotak ini untuk mengesan pakej diluaskan bagi [perisian pengintip](#): atur cara adalah sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat kemudiannya. Ini adalah ukuran tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas fail semasa tutup**- pengimbasan semasa tutup memastikan AVG mengimbas objek aktif (cth. aplikasi, dokumen ...) semasa ia dibuka dan juga semasa ia ditutup; ciri ini membantu anda melindungi komputer anda daripada beberapa jenis virus sofistikated
- **Imbas sektor but bagi media boleh dialihkan** - (dihidupkan secara lalai)
- **Gunakan Heuristik** - (dihidupkan secara lalai) [analisis heuristik](#) akan digunakan untuk pengesanan (*persaingan dinamik bagi objek yang diimbis arahan dalam persekitaran komputer maya*)
- **Autopulih** - sebarang jangkitan yang dikesan akan dipulihkan secara automatik jika terdapat rawatan yang tersedia

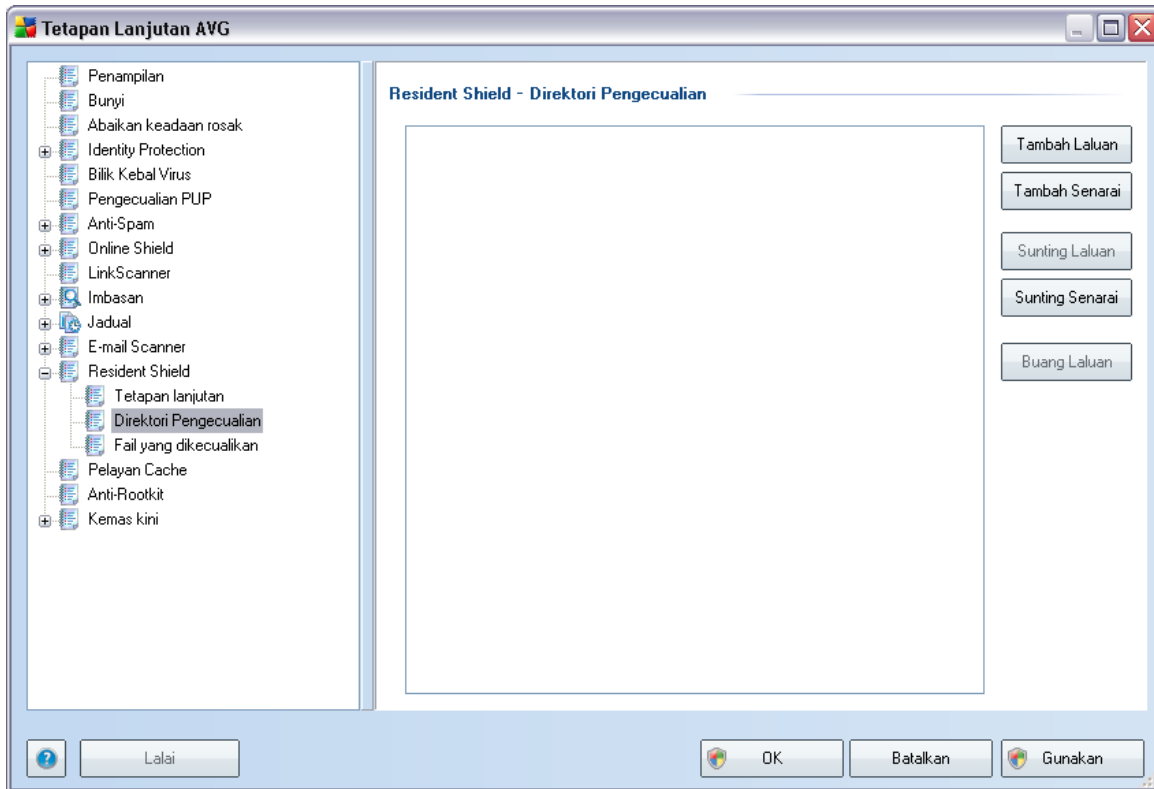
10.13.1. Tetapan Lanjutan

Dalam dialog **Fail yang diimbas oleh Perisai Residen** dialog anda boleh mengkonfigurasi fail mana yang akan diimbas (*oleh sambungan tertentu*):



Tentukan sama ada anda mahu semua fail diimbas atau hanya fail yang boleh dijangkiti - jika sedemikian, anda boleh seterusnya menentukan senarai sambungan yang mentakrifkan fail yang harus dikecualikan daripada pengimbasan dan juga senarai sambungan fail yang menentukan fail yang mesti diimbas dalam apa jua keadaan.

10.13.2. Direktori Tidak Termasuk



Dialog **Perisai Residen - Tidak Termasuk Direktori** menawarkan kemungkinan folder yang ditentukan harus dikeluarkan dari imbasan **Perisai Residen**.

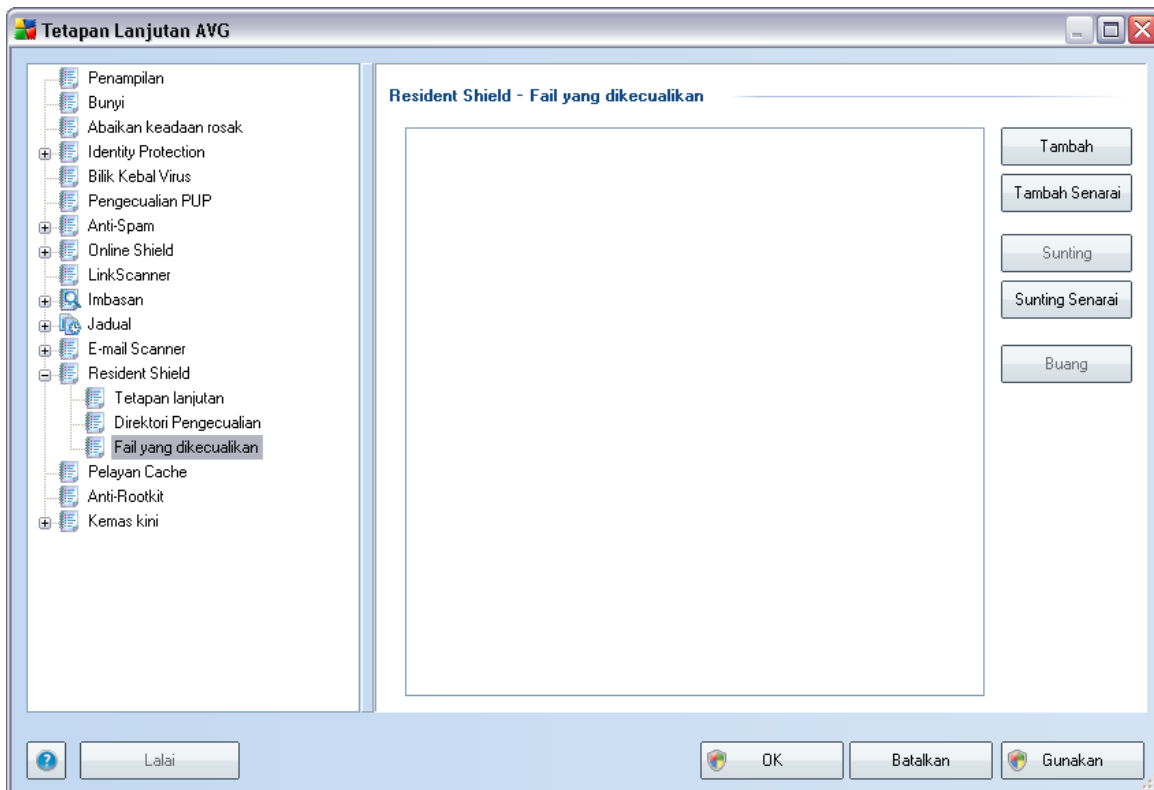
Jika ini tidak penting, kami amat mengesyorkan untuk tidak memasukkan sebarang direktori!

Dialog menyediakan butang kawalan berikut:

- **Tambah laluan**– tentukan direktori untuk mengecualikan daripada imbasan dengan memilihnya satu persatu dari pepohon navigasi cakera setempat
- **Tambah senarai**– membenarkan anda memasukkan keseluruhan senarai direktori untuk mengecualikan daripada imbasan **Perisai Residen**
- **Edit laluan**– membenarkan anda mengedit laluan tertentu ke folder yang dipilih
- **Edit senarai**– membenarkan anda mengedit senarai folder

- **Buang laluan**– membenarkan anda memadam laluan ke folder yang dipilih dari senarai

10.13.3. Fail yang Dikeluarkan



Dialog **Perisai Residen - Tidak termasuk fail** berkelakuan sama seperti yang diterangkan sebelum ini **Perisai Residen - Tidak Termasuk fail** tetapi, sebaliknya folder yang anda boleh mentakrifkan fail khusus sekarang yang harus dikecualikan dari pengimbasan **Perisai Residen**.

Jika ini tidak penting, kami amat mengesyorkan untuk tidak memasukkan sebarang fail!

Dialog menyediakan butang kawalan berikut:

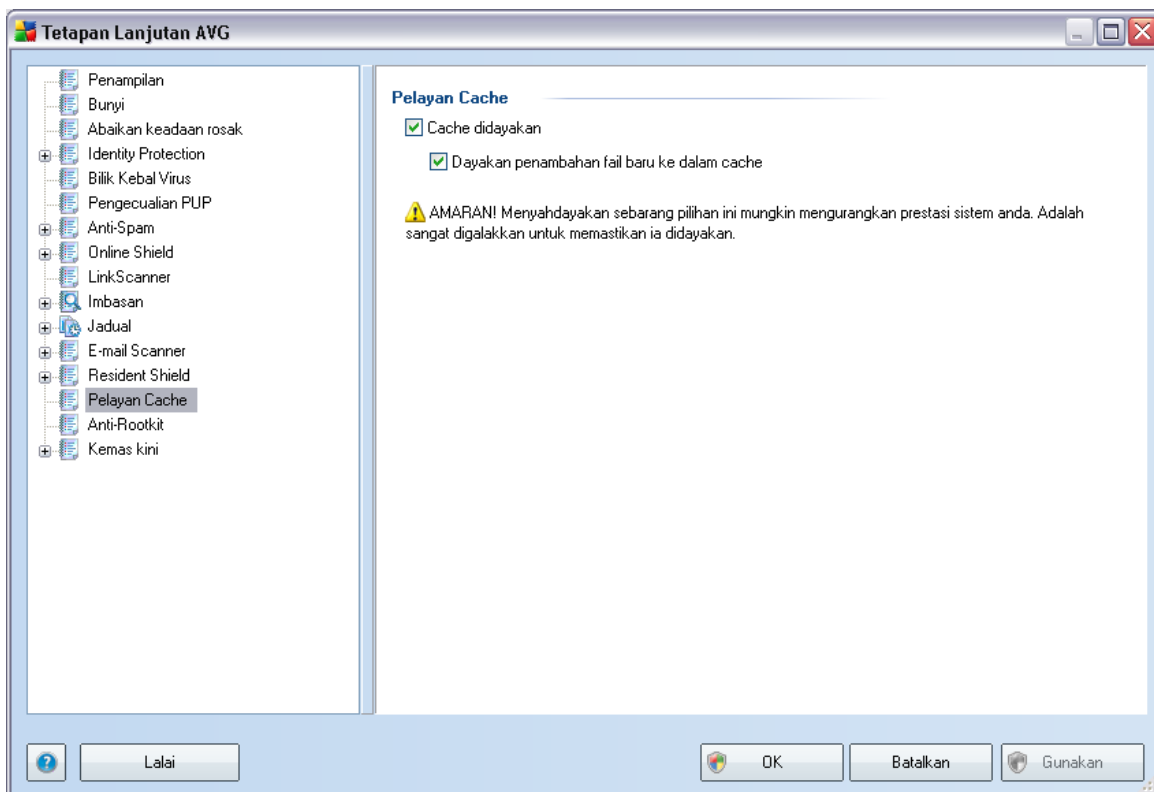
- **Tambah** – tentukan fail untuk dikecualikan daripada pengimbasan dengan memilihnya satu persatu daripada pepohon navigasi cakera tempatan
- **Tambah senarai** – membenarkan anda untuk memasukkan seluruh senarai fail

untuk dikecualikan daripada pengimbasan [Perisai Residen](#)

- **Edit** – membenarkan anda mengedit laluan tertentu ke fail yang dipilih
- **Edit senarai** – membenarkan anda mengedit senarai fail
- **Buang** – membenarkan anda memadam laluan ke fail yang dipilih daripada senarai

10.14. Pelayan Cache

Pelayan Cache adalah proses untuk mempercepatkan sebarang imbasan (*imbasan dengan permintaan, seluruh imbasan komputer yang dijadualkan, imbasan [Perisai Residen](#)*). Ia mengumpul dan memastikan maklumat bagi fail yang boleh dipercayai (*fail sistem dengan tandatangan digital dll.*): Fail-fail ini kemudian, dikira selamat dan ia dilangkau sewaktu imbasan.

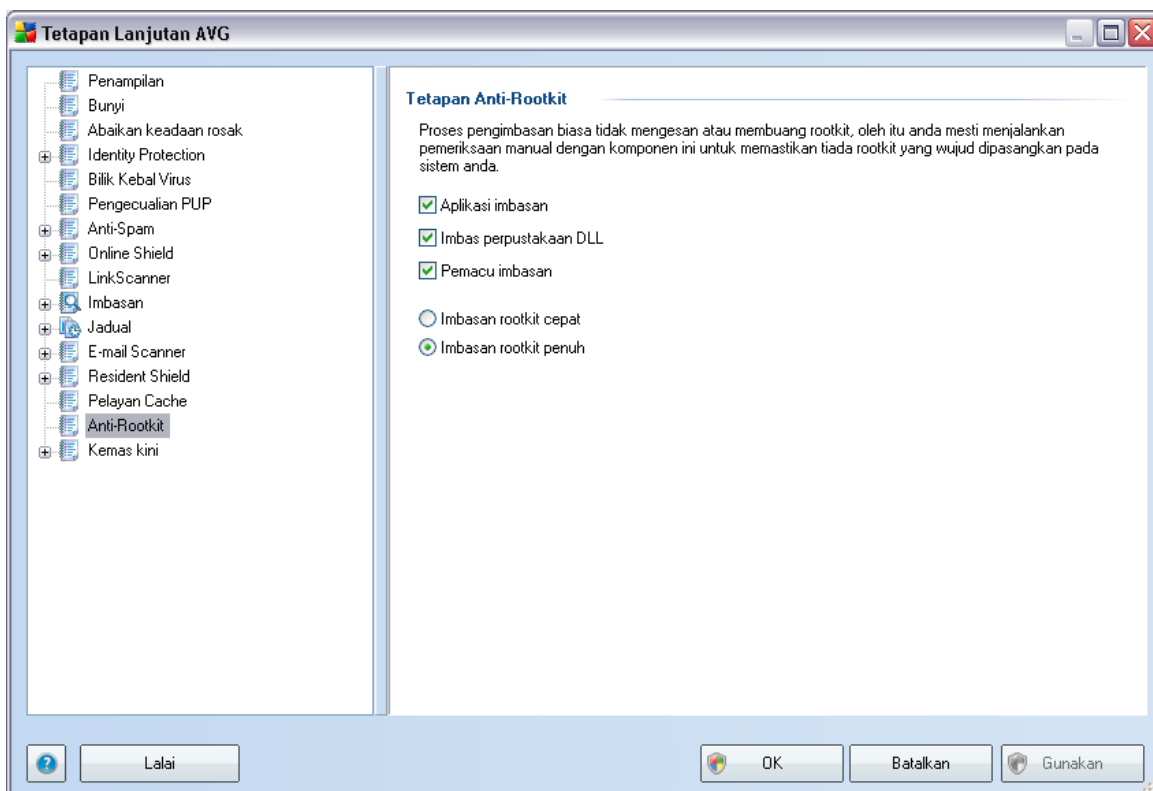


Dialog tetapan menawarkan dua pilihan:

- **Cache didayakan** (*dihidupkan secara lalai*) - jangan tanda kotak untuk mematikan **Pelayan Cache**, dan mengosongkan memori cache. Sila maklum bahawa pengimbasan mungkin memperlahankan, dan seluruh prestasi komputer anda berkurangan kerana setiap fail tunggal yang digunakan akan diimbis untuk virus dan perisian pengintip dahulu.
- **Dayakan penambahan fail baru ke dalam cache** (*dihidupkan secara lalai*) - jangan tanda kotak untuk berhenti menambah lebih banyak fail ke dalam memori cache. Sebarang fail yang telah dibuat cache akan disimpan dan digunakan sehingga cache dimatikan sepenuhnya atau sehingga kemas kini seterusnya bagi pangkalan data virus.

10.15. AntiRootkit

Dalam dialog ini, anda boleh mengedit konfigurasi komponen [AntiRootkit](#):



Mengedit semua fungsi komponen [AntiRootkit](#) seperti yang diberikan dalam dialog ini juga boleh diakses secara terus daripada [antara muka komponen AntiRootkit](#).

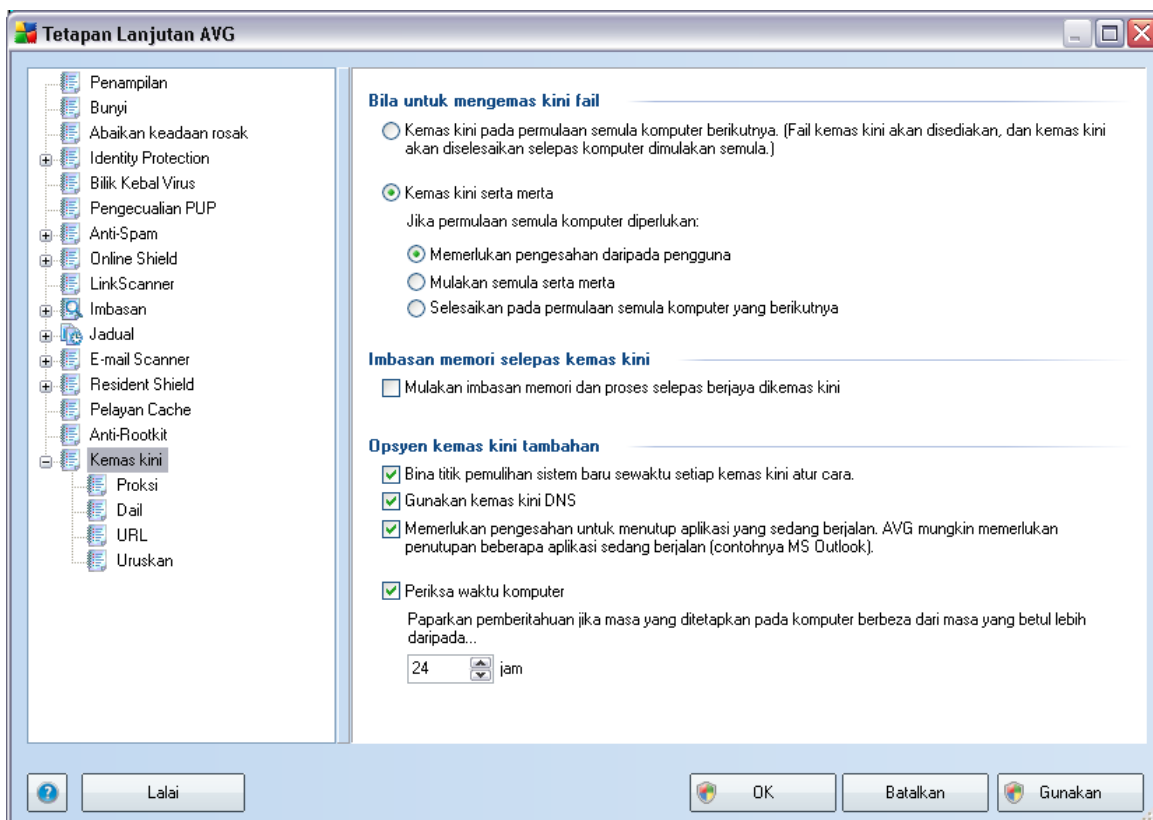
Tandakan kotak semakan masing-masing untuk menentukan objek khusus yang harus diimbas:

- **Aplikasi imbasan**
- **Imbas pustaka DLL**
- **Pemacu imbasan**

Seterusnya, anda boleh memilih mod pengimbasan rootkit:

- **Imbasan rootkit cepat** - mengimbas semua proses berjalan, pemacu yang dimuatkan dan folder sistem (*biasanya, c:\Windows*)
- **Imbasan rootkit penuh** - mengimbas semua proses berjalan, pemacu yang dimuatkan, folder sistem (*biasanya, c:\Windows*), campur semua cakera tempatan (termasuk cakera denyar tetapi tidak termasuk cakera liut/pemacu CD)

10.16. Kemas kini



Item navigasi **Kemas Kini** membuka dialog baru di mana anda boleh menentukan parameter umum berkenaan [kemas kini AVG](#):

Bila untuk mengemas kini fail

Dalam bahagian ini, anda boleh memilih antara dua opsyen alternatif: [kemas kini](#) boleh dijadualkan untuk memulakan semula PC berikutnya atau anda boleh melancarkan [kemas kini](#) dengan serta-merta. Secara lalai, opsyen kemas kini serta-merta dipilih memandangkan ini adalah cara AVG boleh melindungi tahap keselamatan maksimum. Menjadualkan kemas kini untuk permulaan PC berikutnya boleh disyorkan jika anda pasti komputer dimulakan semula secara tetap, sekurang-kurangnya setiap hari.

Jika anda memutuskan untuk mengekalkan konfigurasi lalai dan melancarkan proses kemas kini dengan serta-merta, anda boleh menentukan keadaan di bawah kemungkinan permulaan semula yang diperlukan yang harus dilakukan:

- **Memerlukan pengesahan dari pengguna** - anda akan diminta untuk meluluskan permulaan semula PC yang diperlukan untuk menyelesaikan [proses kemas kini](#)
- **Mula semula serta-merta** - komputer akan dimulakan semula secara automatik selepas [proses kemas kini](#) telah selesai dan kelulusan anda tidak diperlukan
- **Selesai pada mula semula komputer berikutnya** - penyelesaian [proses kemas kini](#) akan ditunda sehingga mula semula komputer berikutnya - sekali lagi, sila ingat bahawa opsyen ini hanya disyorkan jika anda boleh memastikan komputer dimulakan semula secara tetap sekurang-kurangnya setiap hari

Imbasan memori selepas kemas kini

Tandakan kotak semakan ini untuk mentakrifkan bahawa anda hendak melancarkan imbasan memori baru selepas setiap kemas kini yang berjaya dilengkapi Kemas kini yang terkini dimuat turun mungkin telah mengandungi definisi virus baru dan ini boleh digunakan dalam pengimbasan dengan serta-merta.

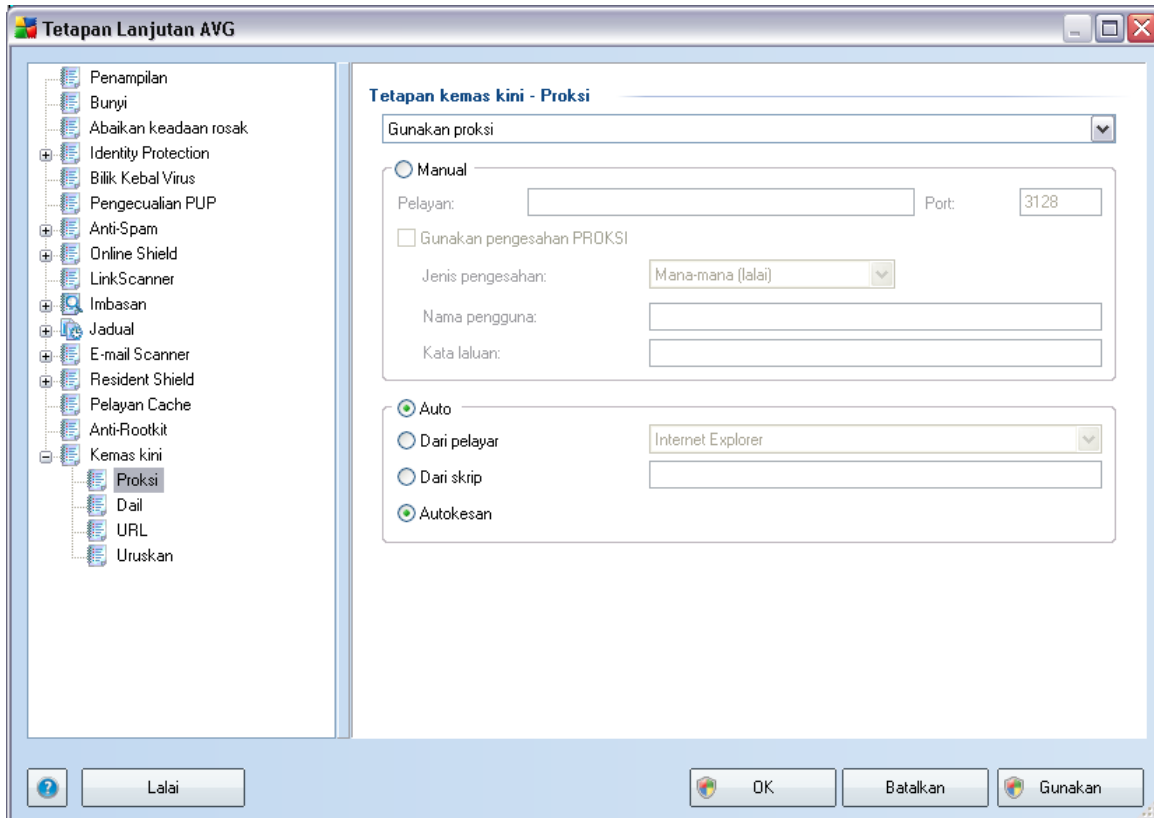
Opsyen kemas kini tambahan

- **Bina titik pemulihan sistem selepas setiap kemas kini atur cara** - sebelum setiap pelancaran kemas kini atur cara AVG, titik pemulihan sistem dibuat. Jika proses kemas kini gagal dan sistem pengendalian anda hancur, anda sentiasa

boleh memulihkan OS anda dalam konfigurasi asal dari titik ini. Opsyen ini boleh diakses melalui Start / All Programs / Accessories / System tools / System Restore, tetapi sebarang perubahan hanya boleh disarankan kepada pengguna berpengalaman sahaja! Pastikan kotak semakan ini ditandakan jika anda hendak menggunakan kefungsiian ini.

- **Gunakan kemas kini DNS** - tandakan kotak semakan ini untuk mengesahkan bahawa anda menggunakan kaedah pengesanan fail kemas kini yang menyingkirkan jumlah data yang dipindahkan di antara pelayan kemas kini dan klien AVG;
- **Memerlukan pengesanan untuk menutup aplikasi yang sedang dijalankan** (*dihidupkan secara lalai*) akan membantu anda memastikan tiada aplikasi yang sedang dijalankan yang akan ditutup tanpa kebenaran anda - jika diperlukan untuk proses kemas kini diselesaikan;
- **Periksa masa komputer** - tandakan opsiyen ini untuk mengesahkan bahawa anda mahu pemberitahuan ini dipaparkan jika masa komputer berbeza dari masa yang betul lebih daripada bilangan jam yang ditetapkan.

10.16.1. Proksi



Pelayan proksi adalah pelayan atau perkhidmatan tersendiri yang dijalankan pada PC yang memberi jaminan sambungan lebih selamat kepada Internet. Menurut peraturan rangkaian yang ditentukan, kemudian, anda boleh mengakses Internet sama ada secara terus atau melalui pelayan proksi; kedua-dua kemungkinan juga boleh dibenarkan dalam masa yang sama. Kemudian, dalam item pertama bagi dialog **Tetapan kemas kini - Proksi** anda perlu memilih dari menu kotak kombo sama ada anda mahu:

- **Gunakan proksi**
- **Jangan gunakan pelayan proksi** - tetapan lalai
- **Cuba penyambungan menggunakan proksi dan jika ia gagal, sambungkan secara langsung**

Jika anda memilih sebarang opsyen menggunakan pelayan proksi, anda perlu menentukan beberapa data selanjutnya. Tetapan pelayan boleh dikonfigurasi sama ada

secara manual atau secara automatik.

Konfigurasi manual

Jika anda memilih konfigurasi manual (semak *opsyen **Manual** untuk mengaktifkan bahagian dialog masing-masing*) anda perlu menentukan item berikut:

- **Pelayan**– menentukan alamat IP pelayan atau nama pelayan
- **Port**– menentukan bilangan port yang mendayakan akses Internet (*secara lalai, nombor ini ditetapkan kepada 3128 tetapi boleh ditetapkan secara berbeza – jika anda tidak pasti, hubungi pentadbir rangkaian anda*)

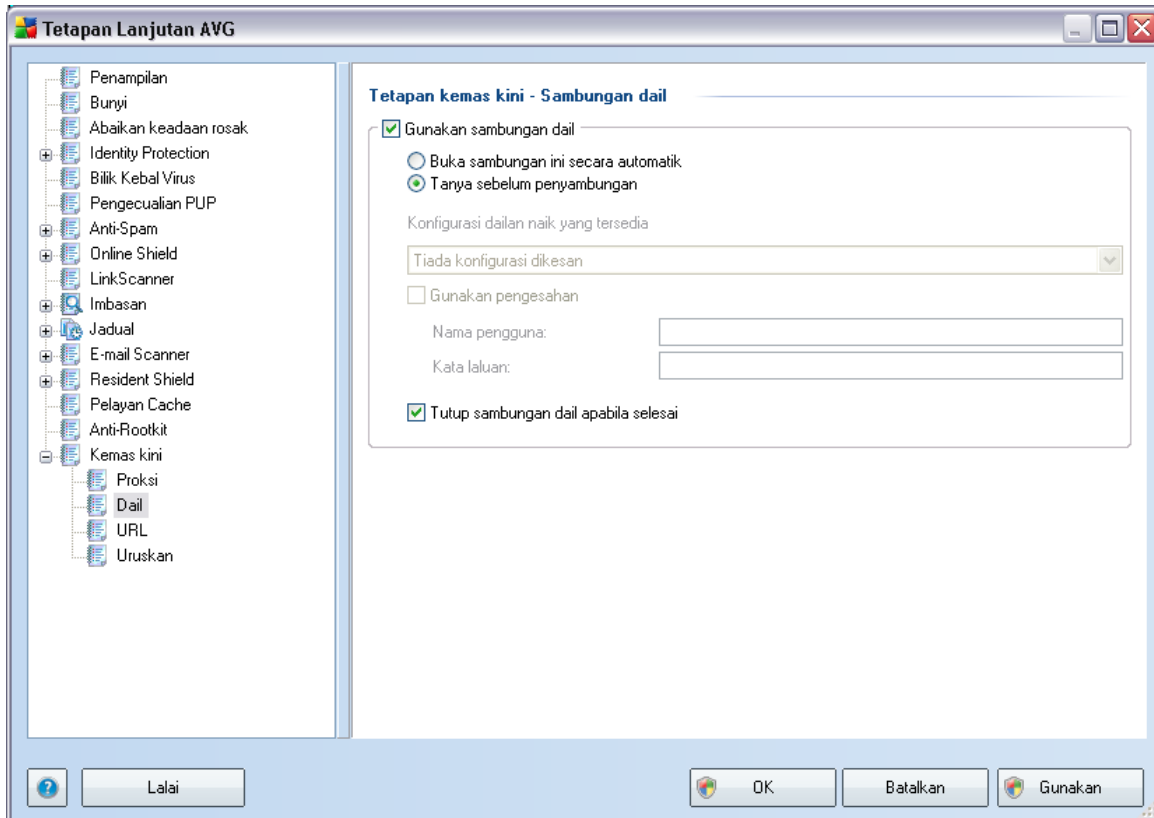
Pelayan proksi juga boleh mengkonfigurasi peraturan tertentu untuk setiap pengguna. Jika pelayan proksi anda disediakan dengan cara ini, tandakan opsyen **Guna pengesahan PROKSI** untuk mengesahkan bahawa nama pengguna dan kata laluan anda sah untuk menyambung kepada Internet melalui pelayan proksi.

Konfigurasi automatik

Jika anda memilih konfigurasi automatik (*tandakan pilihan **Auto** untuk mengaktifkan bahagian dialog masing-masing*) kemudian, sila pilih dari mana konfigurasi proksi akan dilakukan:

- **Dari pelayar** - konfigurasi akan dibaca dari pelayar internet lalai anda
- **Dari skrip** - konfigurasi akan dibaca dari skrip yang dimuat turun dengan fungsi yang mengembalikan alamat proksi
- **Autokesan** - konfigurasi akan dikesan secara automatik secara terus dari pelayan proksi

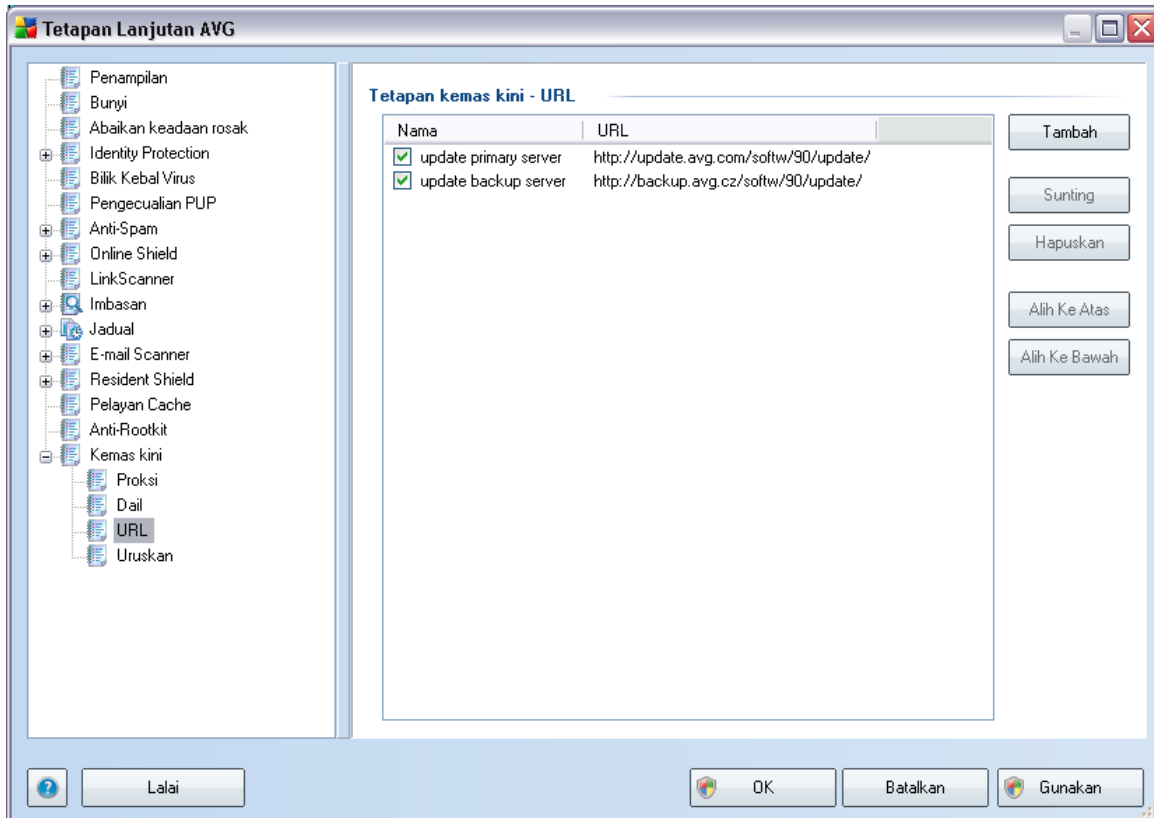
10.16.2. Dailan



Semua parameter yang ditakrifkan secara pilihan dalam dialog **Kemas kini tetapan - sambungan Dailan** merujuk kepada sambungan dailan kepada Internet. Medan dialog adalah tidak aktif sehingga anda menandakan opsiyen **Gunakan sambungan dailan** yang mengaktifkan medan.

Tentukan sama ada anda hendak bersambung kepada Internet secara automatik (**Buka sambungan ini secara automatik**) atau anda mahu mengesahkan sambungan secara manual setiap kali (**Tanya sebelum sambungan**). Untuk sambungan automatik, anda harus seterusnya memilih sama ada sambungan harus ditutup selepas kemas kini selesai (**Tutup sambungan dailan apabila selesai**).

10.16.3. URL

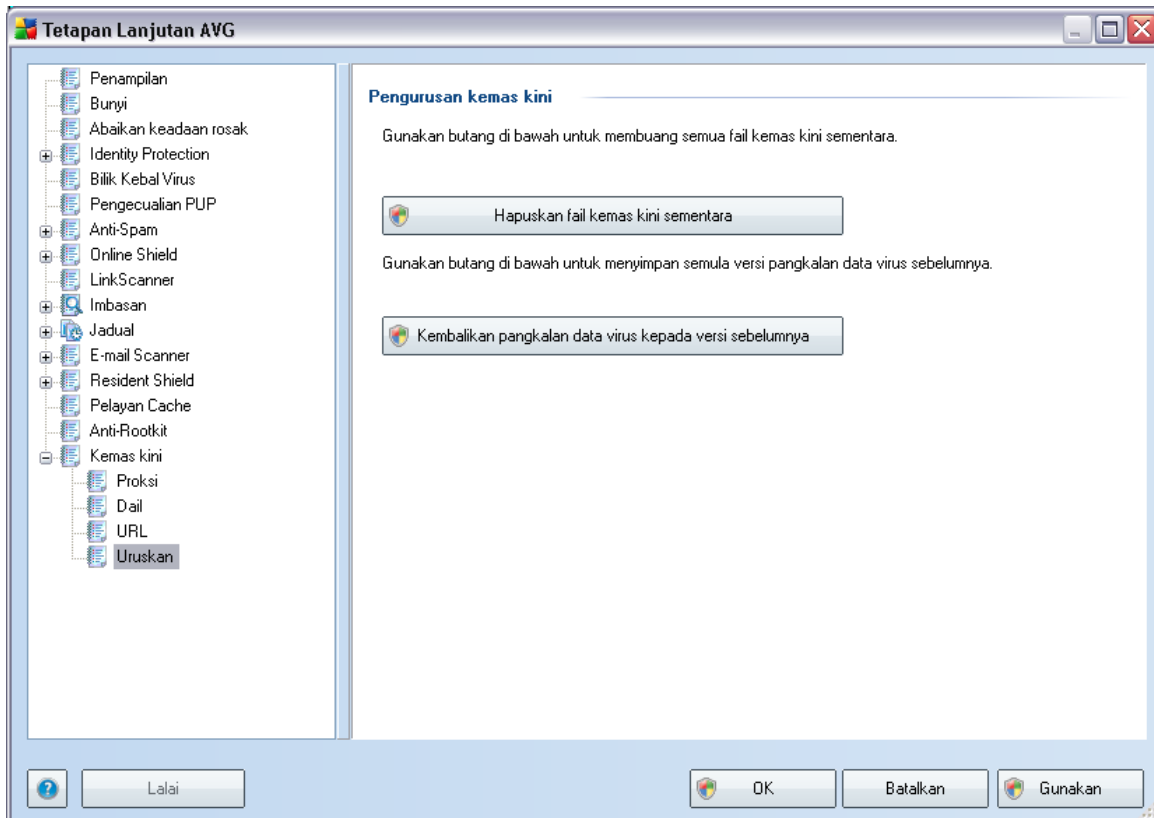


Dialog **URL** menawarkan senarai alamat Internet dari mana fail kemas kini dimuat turun. Senarai dan itemnya boleh diubah suai menggunakan butang kawalan berikut:

- **Tambah**– membuka dialog di mana anda boleh menentukan URL baru untuk ditambah ke senarai
- **Edit** - membuka dialog di mana anda boleh mengedit parameter URL yang dipilih
- **Padam**– memadam URL yang dipilih dari senarai
- **Alih ke Atas**– mengalihkan URL yang dipilih ke satu kedudukan atas dalam senarai
- **Alih ke Bawah** – mengalihkan URL yang dipilih ke satu kedudukan ke bawah dalam senarai

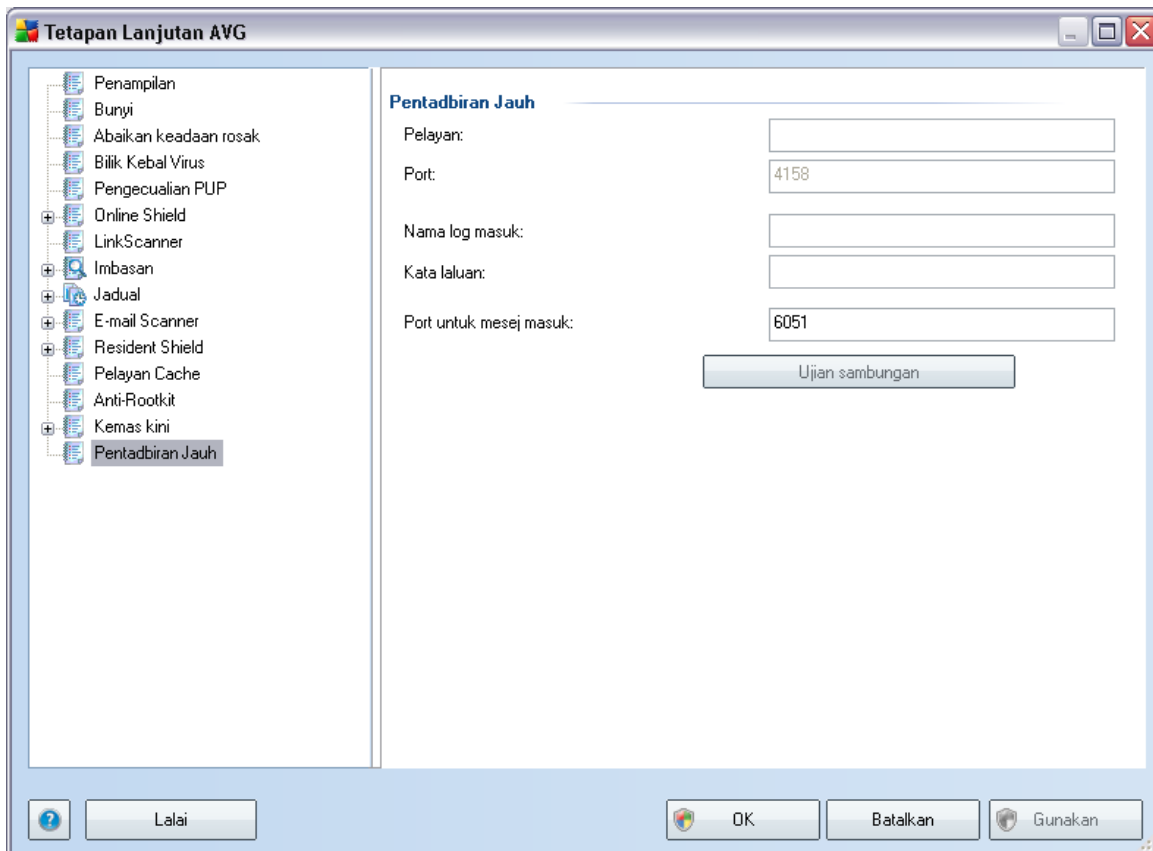
10.16.4. Uruskan

Dialog **Uruskan** menawarkan dua opsi yang boleh diakses melalui dua butang:



- **Padam fail kemas kini sementara** - tekan butang ini untuk memadam semua fail kemas kini berlebihan dari cakera keras anda (*secara lalai, fail ini disimpan selama 30 hari*)
- **Kembalikan semula pangkalan data virus ke versi sebelumnya** - tekan butang ini untuk memadam versi pangkalan virus terkini daripada cakera keras anda, dan untuk kembali ke versi yang disimpan sebelum ini (*versi pangkalan virus baru akan menjadi sebahagian daripada kemas kini berikut*)

10.17. Pentadbiran Jauh



Tetapan **Pentadbiran Jauh** merujuk kepada menyambung stesen klien AVG ke sistem pentadbiran jauh. Jika anda merancang untuk menyambung stesen tersebut ke pentadbiran jauh, sila tentukan parameter berikut:

- **Pelayan** - nama pelayan (atau alamat IP) di mana Pelayan Pentadbir AVG dipasang
- **Port** - memberikan bilangan port di mana klien AVG berkomunikasi dengan Pelayan Pentadbir AVG (*nombor port 4158 dikira sebagai lalai - jika anda menggunakan nombor port ini, anda tidak perlu menentukannya dengan jelas*)
- **Log masuk** - jika komunikasi di antara klien AVG dan AVG Pelayan Pentadbiran AVG ditakrifkan sebagai selamat, berikan nama pengguna anda ...
- **Kata laluan** - ... dan kata laluan anda



- **Port untuk mesej masuk** - bilangan port di mana klien AVG menerima mesej masuk dari Pelayan Pentadbiran AVG

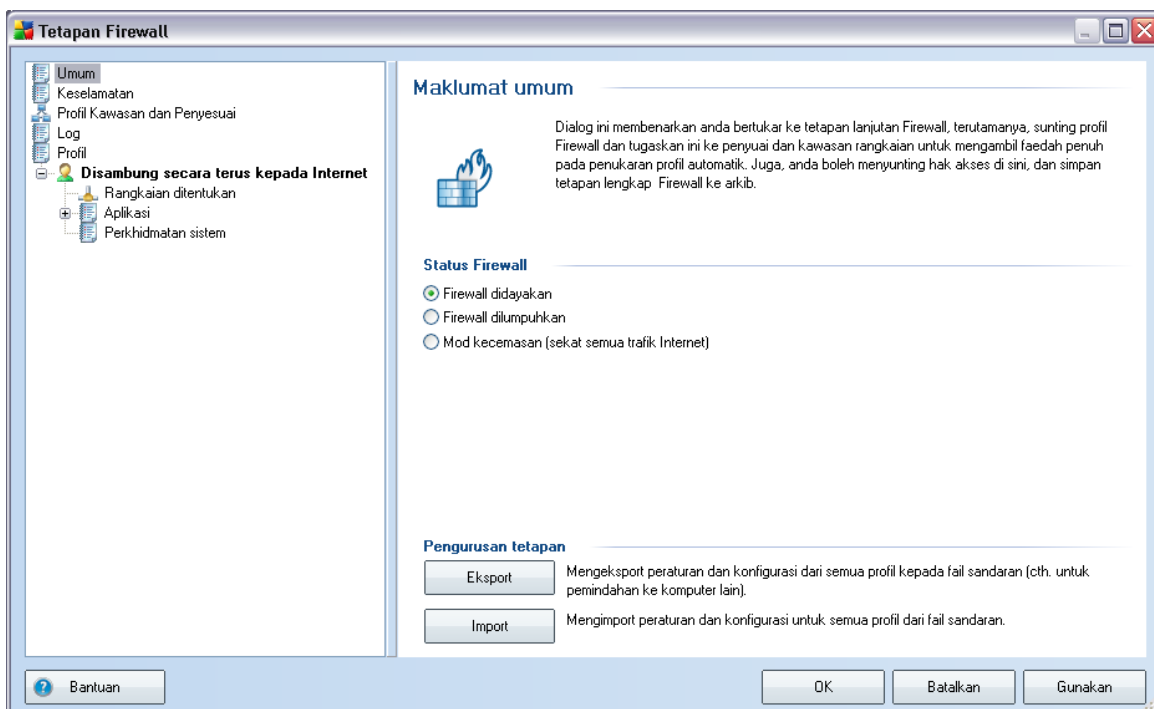
Butang **Uji sambungan** membantu anda mengesahkan bahawa semua data adalah sah dan boleh digunakan untuk berjaya menyambungkan ke DataCenter.

Nota: Untuk penerangan terperinci mengenai pentadbiran jauh, sila rujuk dokumentasi Edisi Rangkaian AVG.

11. Tetapan Firewall

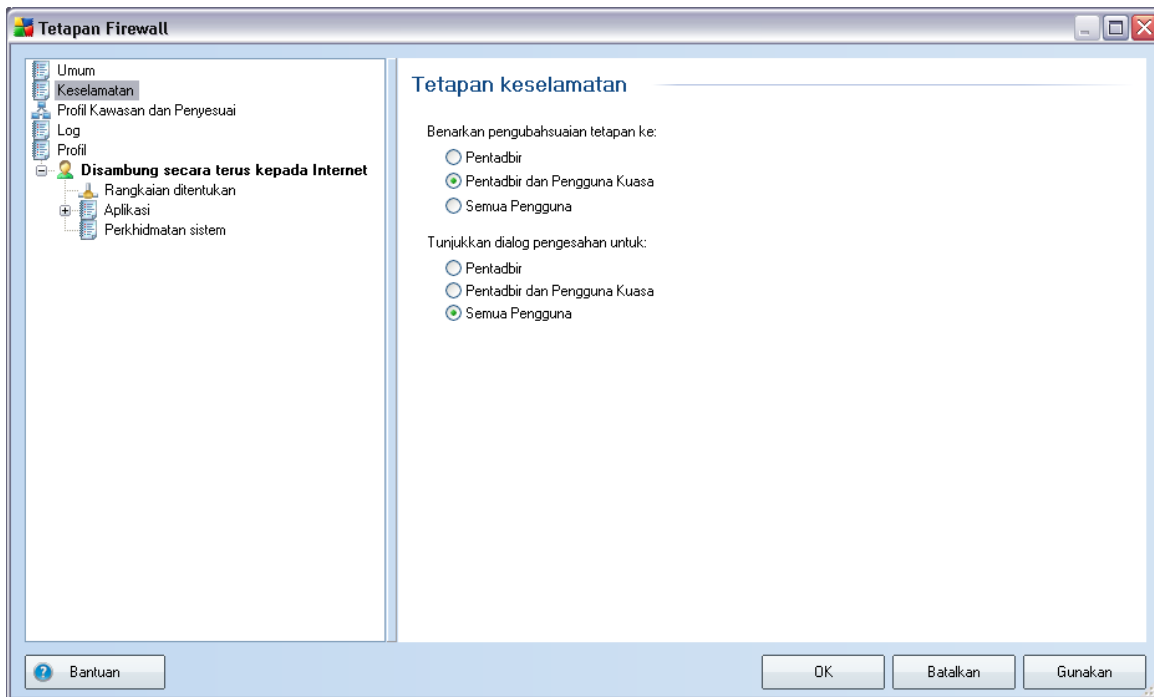
Konfigurasi **Firewall** membuka tetingkap baru di mana beberapa dialog boleh menyediakan parameter yang sangat canggih bagi komponen. ***Walau bagaimanapun, pengeditan konfigurasi lanjutan hanya bertujuan untuk pengguna pakar dan berpengalaman.***

11.1. Umum



Dalam **Maklumat am** anda boleh **Eksport / Import konfigurasi Firewall**; iaitu mengeksport peraturan dan tetapan **Firewall** yang ditakrifkan kepada fail sandaran atau sebaliknya, untuk mengimport seluruh fail sandaran.

11.2. Keselamatan



Dalam dialog **Tetapan keselamatan** anda boleh menentukan peraturan am bagi kemudian **Firewall** tidak kira profil yang dipilih:

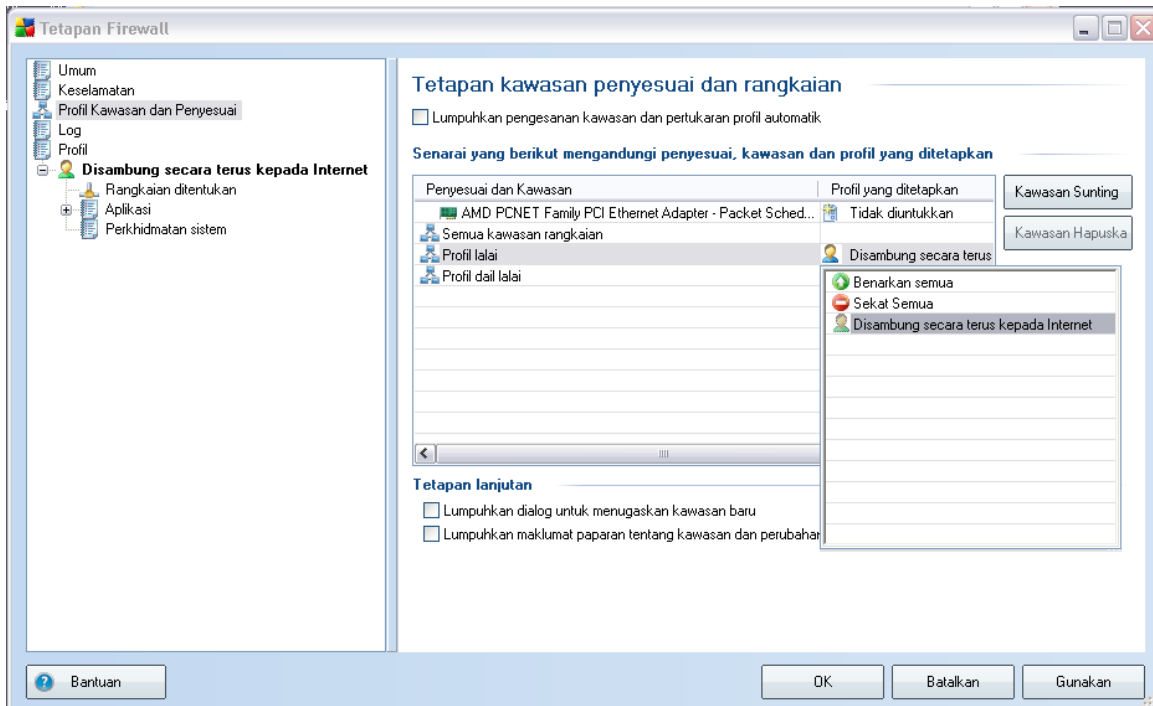
- **Benarkan pengubahsuaian kepada** - tentukan siapa dibenarkan untuk mengubah konfigurasi **Firewall**
- **Tunjukkan dialog pengesahan untuk** - tentukan kepada siapa dialog pengesahan (*dialog yang meminta keputusan dalam situasi yang tidak diliputi oleh peraturan **Firewall***) harus dipaparkan

Dalam kedua-dua kes, anda boleh menguntukkan hak tertentu kepada salah satu daripada kumpulan pengguna berikut:

- o **Pentadbir** – mengawal PC sepenuhnya dan mempunyai hak menguntukkan setiap pengguna ke dalam kumpulan dengan secara khusus menentukan kuat kuasa
- o **Pentadbir dan Pengguna Berkuasa** – pentadbir boleh menguntukkan mana-mana pengguna ke dalam kumpulan tertentu (*Pengguna Berkuasa*) dan menentukan kuat kuasa bagi ahli kumpulan

- o **Semua Pengguna** – pengguna lain tidak diperuntukkan ke dalam sebarang kumpulan tertentu

11.3. Profil Kawasan dan Penyesuai



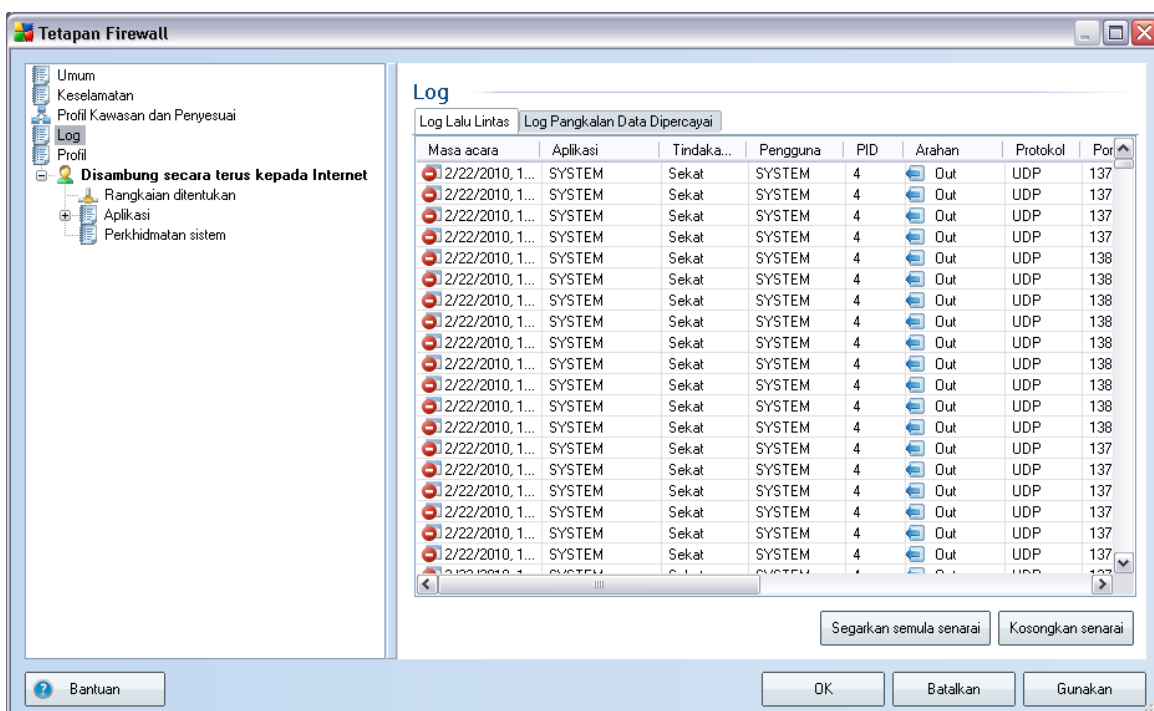
Dalam dialog **Penyesuai dan tetapan kawasan rangkaian** anda boleh mengedit tetapan berkaitan dengan menguntukkan profil yang ditakrifkan kepada penyesuai khusus dan merujuk kepada rangkaian masing-masing:

- **Nyahdaya pengesanan kawasan dan pertukaran profil automatik** - salah satu profil yang ditakrifkan boleh diperuntukkan kepada setiap jenis antara muka rangkaian kepada setiap kawasan masing-masing. Jika anda tidak mahu menentukan profil tertentu, satu profil biasa ditentukan berdasarkan pada pemilihan [penggunaan komputer](#) dan [reka bentuk rangkaian komputer](#) anda sewaktu [Proses Pemasangan](#) akan digunakan. Walau bagaimanapun, jika anda memutuskan untuk membezakan profil dan menguntukkannya ke penyesuai dan kawasan khusus dan kemudian, atas sebab tertentu - anda mahu menukar aturan ini buat sementara, tandakan rait pada opsyen **Nyahdaya pengesanan kawasan dan pertukaran profil automatik**.
- **Senarai penyesuai, kawasan dan profil yang diperuntukkan** - dalam

senarai ini, anda boleh menemui gambaran keseluruhan penyesuai dan kawasan yang dikesan. Untuk setiap satu, anda boleh menguntukkan profil tertentu dari menu profil yang ditentukan. Untuk membuka menu ini, klik item masing-masing dalam senarai penyesuai dan pilih profil.

- **Tetapan lanjutan** - tandakan rait pilihan masing-masing akan menyahaktifkan ciri memaparkan mesej maklumat.

11.4. Log



Dialog **Log** membenarkan anda untuk mengkaji semula senarai semua tindakan **Firewall** yang dilog dan peristiwa dengan penerangan terperinci bagi parameter berkaitan (*waktu peristiwa, nama aplikasi, tindakan log masing-masing, nama pengguna, PID, arah lalu lintas, jenis protokol, bilangan port jauh dan tempatan, dll.*) pada dua tab:

- **Log Lalu Lintas** - menawarkan maklumat mengenai aktiviti bagi semua aplikasi yang telah cuba menyambung ke rangkaian.
- **Log Pangkalan Data yang Dipercayai** - Pangkalan data yang dipercayai adalah maklumat pengumpulan pangkalan data dalaman AVG mengenai aplikasi

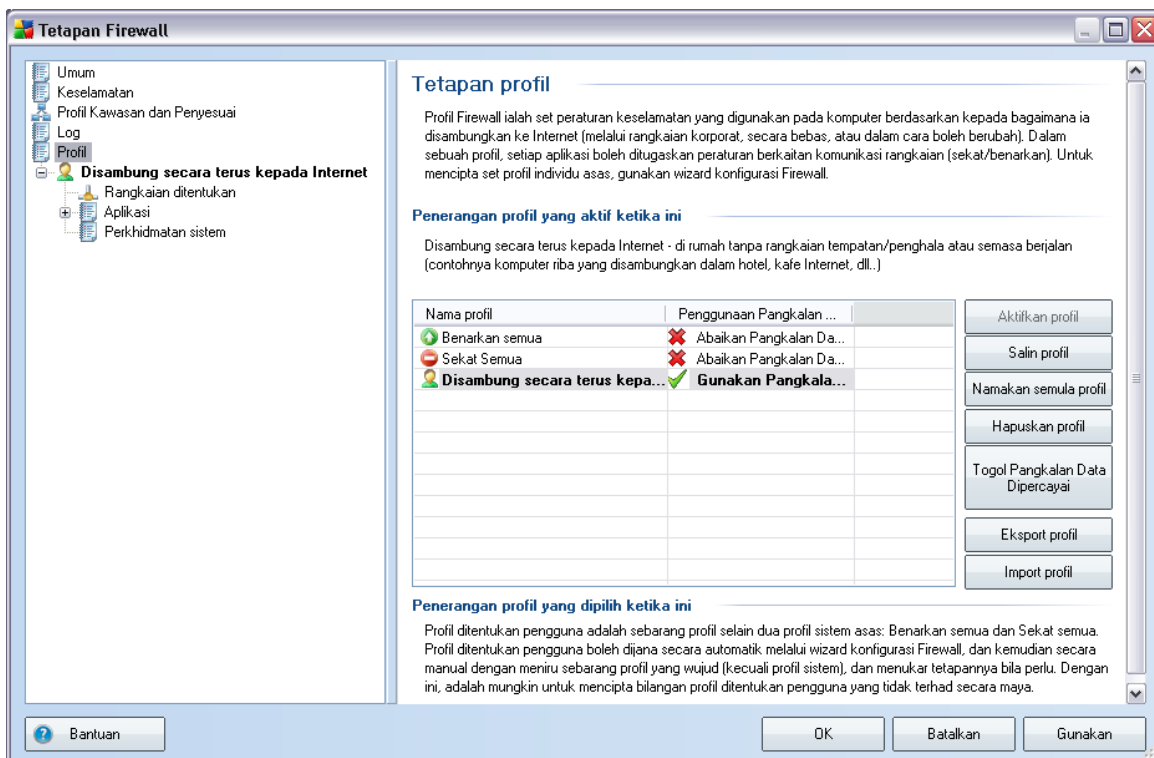
yang diperakui dan dipercayai yang sentiasa boleh dibenarkan untuk berkomunikasi dalam talian. Pertama kali aplikasi baru cuba menyambung ke rangkaian (*cth. apabila tiada lagi peraturan firewall yang ditentukan untuk aplikasi ini*), adalah perlu untuk mengetahui sama ada komunikasi rangkaian harus dibenarkan untuk aplikasi tersebut. Pertama sekali, AVG mencari *Pangkalan data yang dipercayai* dan jika aplikasi disenaraikan, ia akan diberikan akses kepada rangkaian secara automatik. Hanya selepas itu, terdapat maklumat pada aplikasi yang tersedia dalam pangkalan, anda akan ditanya dalam dialog tersendiri sama ada anda hendak membenarkan aplikasi mengakses rangkaian.

Butang kawalan

- **Bantuan** - membuka dialog berkaitan dengan fail bantuan.
- **Muat semula senarai** - semua parameter yang diiloh boleh diatur mengikut atribut yang dipilih: mengikut kronologi (*tarikh*) atau mengikut abjad (*kolum lain*) - cuma klik pengepala kolum masing-masing. Guna butang **Muat semula senarai** untuk mengemas kini maklumat yang baru dipaparkan.
- **Kosongkan senarai** - padam semua entri dalam carta.

11.5. Profil

Dalam dialog **Tetapan profil** anda boleh menemui senarai semua profil yang tersedia.



Semua sistem lain [profil](#) kemudian, boleh diedit betul-betul dalam dialog ini menggunakan butang kawalan berikut:

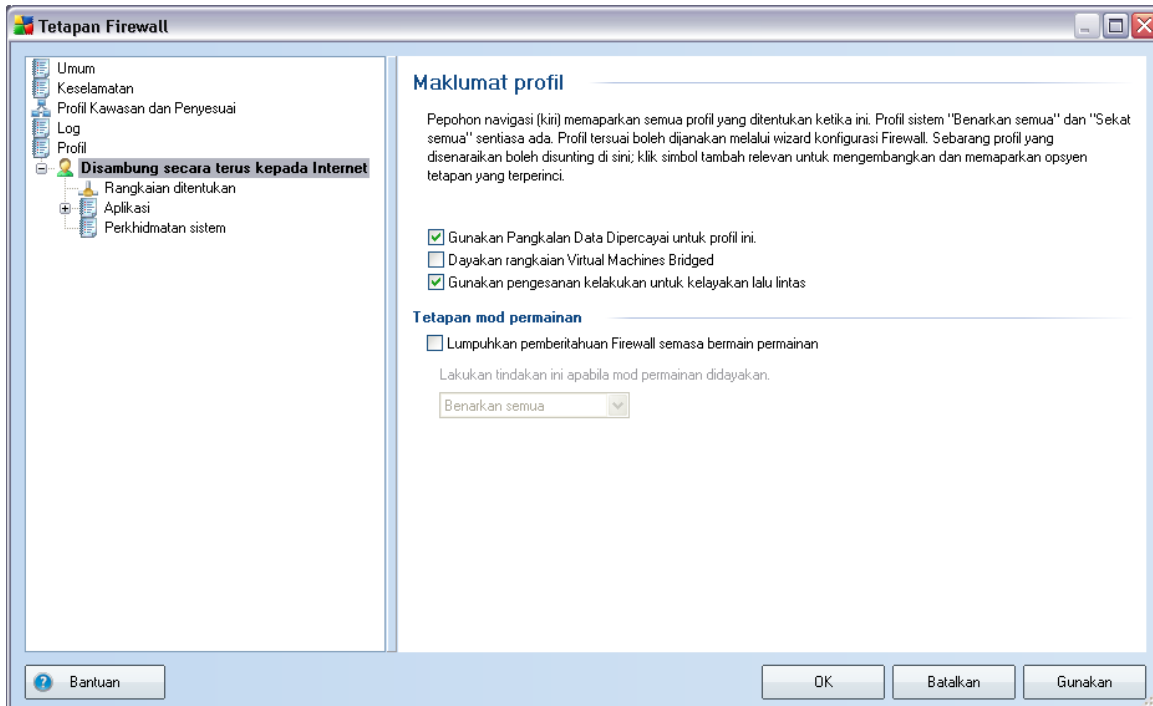
- **Aktifkan profil** - butang ini menetapkan profil yang dipilih sebagai aktif, yang bermaksud konfigurasi profil yang dipilih akan digunakan oleh **Firewall** untuk mengawal lalu lintas rangkaian
- **Buat pendua profil** - membuat salinan yang sama bagi profil yang dipilih, kemudian, anda boleh mengedit dan menamakan semula salinan untuk membuat profil baru berdasarkan pada salinan pendua asal
- **Namakan semula profil** - membenarkan anda menentukan yang baru untuk profil yang dipilih
- **Padam profil** - memadam profil yang dipilih dari senarai

- **Togol Pangkalan Data yang Dipercayai** - untuk profil yang dipilih, anda boleh menentukan untuk menggunakan maklumat *Pangkalan Data yang Dipercayai* (*Pangkalan Data yang Dipercayai adalah data pengumpulan pangkalan data dalaman AVG pada aplikasi yang dipercayai dan diperakui yang sentiasa boleh dibenarkan untuk berkomunikasi dalam talian.*)
- **Eksport profil** - merekodkan konfigurasi profil yang dipilih ke dalam fail yang akan disimpan untuk kemungkinan penggunaan seterusnya
- **Import profil** - mengkonfigurasi tetapan profil yang dipilih berdasarkan pada data yang dieksport dari fail konfigurasi sandaran
- **Bantuan** - membuka fail bantuan berkaitan dialog

Dalam bahagian bawah dialog, sila dapatkan penerangan profil yang baru dipilih dalam senarai di atas.

Berdasarkan kepada nombor profil yang ditentukan yang dinyatakan dalam senarai dalam dialog **Profil**, struktur menu navigasi kiri akan berubah dengan sewajarnya. Setiap profil yang ditentukan membuat cabang khusus di bawah item **Profil**. Kemudian, profil tertentu boleh diedit dalam dialog berikut (*yang sama untuk semua profil*):

11.5.1. Maklumat Profil



Dialog **Maklumat profil** adalah dialog pertama bagi bahagian di mana anda boleh mengedit konfigurasi setiap profil dalam dialog berasingan untuk parameter tertentu bagi profil.

- **Gunakan Pangkalan Data Dipercayai untuk profil ini** - (dihidupkan secara lalai) tandakan pilihan untuk mengaktifkan Pangkalan Data Dipercayai (iaitu, pangkalan data dalaman AVG yang mengumpul maklumat pada aplikasi dipercayai dan diiktiraf berkomunikasi dalam talian. Jika tiada peraturan yang ditentukan untuk aplikasi tersebut lagi, adalah perlu untuk mengetahui sama ada aplikasi boleh diberikan akses kepada rangkaian. AVG mencari Pangkalan Data yang Dipercayai dan jika aplikasi disenaraikan, ia dikira selamat dan akan dibenarkan untuk berkomunikasi pada rangkaian. Jika tidak, anda akan dijemput untuk menentukan sama ada aplikasi harus dibenarkan untuk berkomunikasi pada rangkaian) untuk profil tersebut
- **Dayakan rangkaian Jejambat Mesin Maya** - (dimatikan secara lalai) tandakan rait item ini untuk membenarkan mesin maya dalam VMware menyambung secara terus ke rangkaian
- **Gunakan pengesanan kelakuan untuk kelayakan lalu lintas** - (dihidupkan

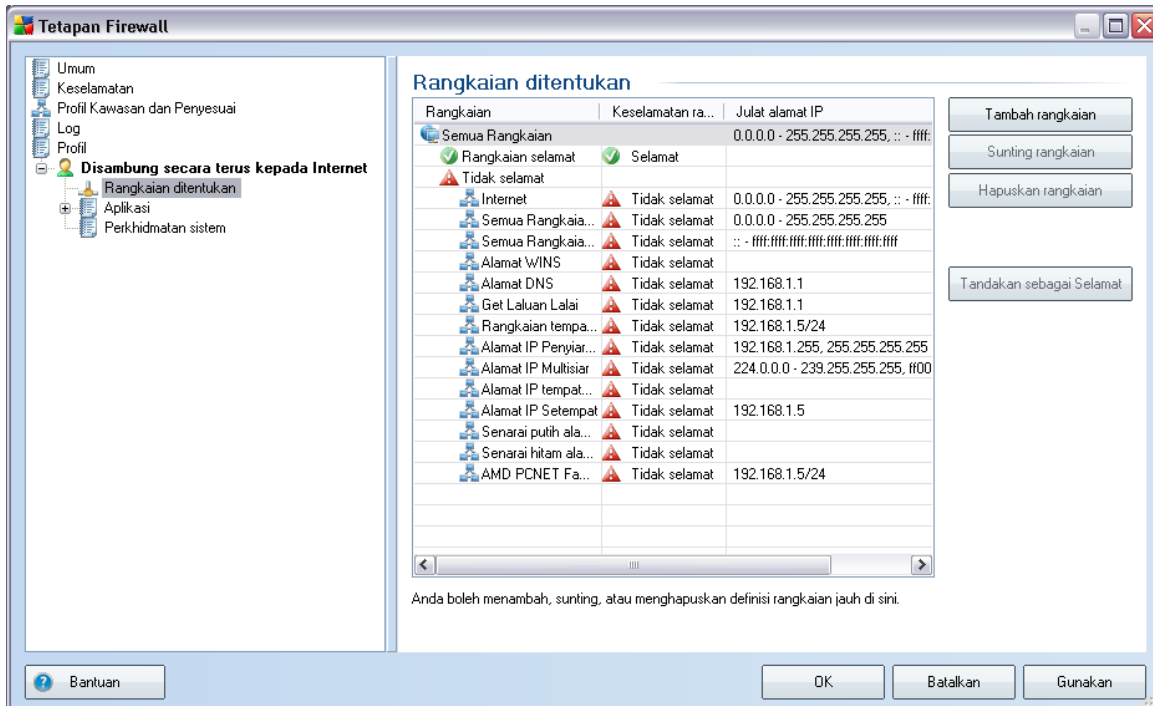
secara lalai) tandakan pilihan ini untuk membenarkan **Firewall** menggunakan kefungsian **Perlindungan Identiti** semasa menilai aplikasi - **Perlindungan Identiti** boleh memberitahu sama ada aplikasi menunjukkan sebarang kelakuan mencurigakan atau ia boleh dipercayai dan dibenarkan untuk berkomunikasi dalam talian.

Tetapan mod permainan

Dalam bahagian **Tetapan mod permainan** anda boleh menentukan dan mengesahkan dengan menanda rait item tersebut sama ada anda hendak mesej maklumat **Firewall** dipaparkan walaupun semasa aplikasi skrin penuh dijalankan pada komputer anda (*biasanya, ini adalah permainan tetapi digunakan kepada sebarang aplikasi skrin penuh, cth. persembahan PPT*). Memandangkan mesej maklumat boleh menjadi agak rosak.

Jika anda menanda rait item **Nyahdayakan pemberitahuan Firewall semasa bermain permainan**, dalam menu gulung bawah, kemudian, pilih tindakan yang harus diambil jika aplikasi baru tanpa peraturan ditentukan tetapi cuba berkomunikasi pada rangkaian (*aplikasi yang biasanya menghasilkan dialog pertanyaan*) semua aplikasi ini boleh sama ada dibenarkan atau disekat.

11.5.2. Rangkaian yang Ditentukan

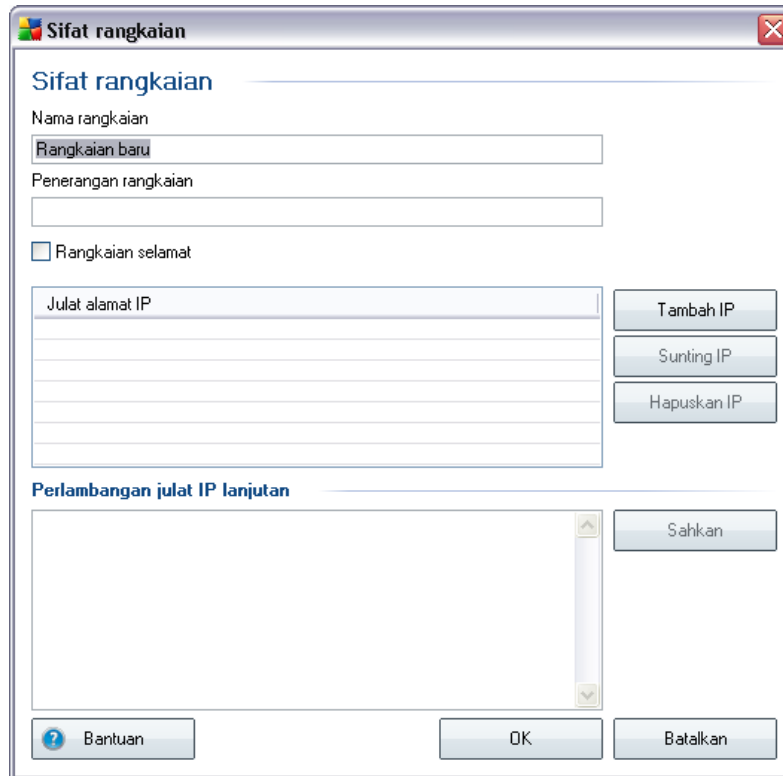


Dialog **Rangkaian yang ditakrifkan** menawarkan senarai semua rangkaian yang komputer anda disambungkan. Maklumat berikut diberikan pada setiap rangkaian yang dikesan:

- **Rangkaian** - senarai nama semua rangkaian yang komputer disambungkan kepadanya.
- **Keselamatan rangkaian** - secara lalai, semua rangkaian dikira tidak selamat dan hanya jika anda pasti rangkaian masing-masing adalah selamat, anda boleh menguntukkannya sedemikian (*klik senarai item merujuk kepada rangkaian masing-masing dan pilih Selamat daripada menu konteks*) - kemudian, semua rangkaian selamat akan dimasukkan ke dalam kumpulan tersebut yang aplikasi boleh berkomunikasi pada set peraturan aplikasi untuk Benarkan untuk selamat
- **Julat alamat IP** - setiap rangkaian akan dikesan secara automatik dan ditentukan dalam bentuk julat alamat IP

Butang kawalan

- **Tambah rangkaian** - membuka tettingkap dialog **Sifat rangkaian** di mana anda boleh mengedit parameter bagi rangkaian yang baru ditakrifkan:



Dalam dialog ini, anda boleh menentukan **Nama rangkaian**, berikan **Penerangan rangkaian** dan berkemungkinan peruntukkan rangkaian sebagai selamat. Rangkaian baru boleh menjadi sama ada ditakrifkan secara manual dalam dialog persendirian yang dibuka melalui butang **Tambah IP** (secara alternatif **Edit IP / Padam IP**), dalam dialog ini anda boleh menentukan rangkaian dengan memberikan julat atau topeng IP.

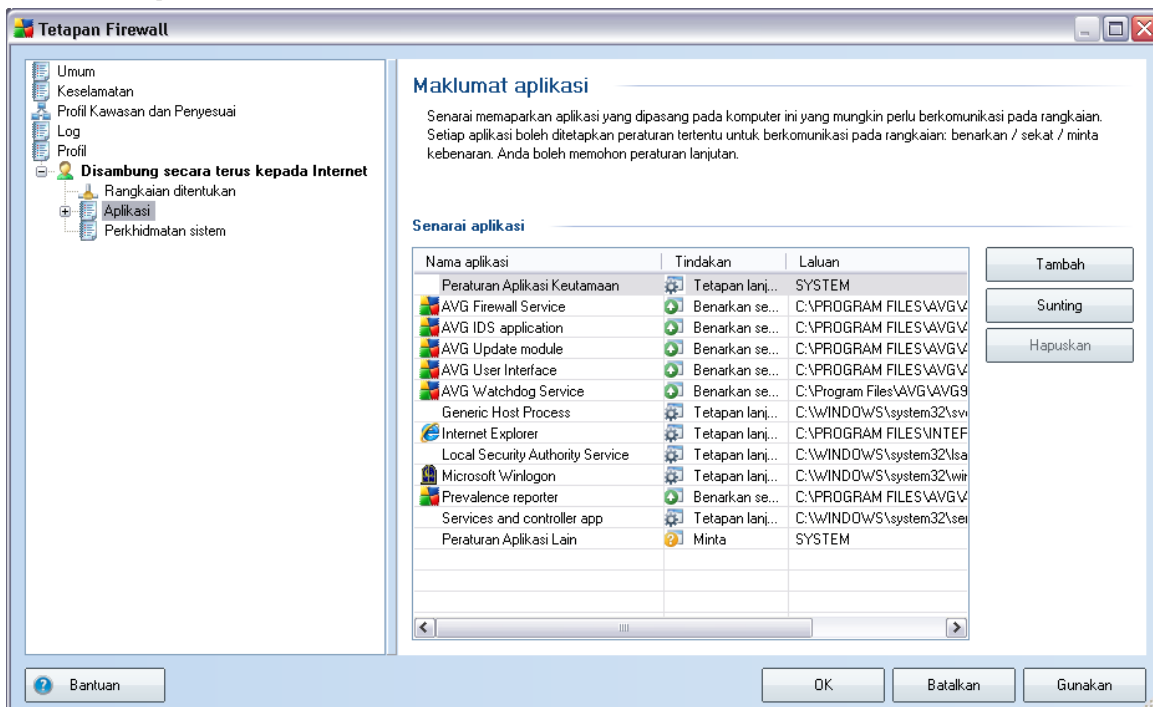
Untuk sebilangan besar rangkaian yang harus ditakrifkan sebagai sebahagian daripada rangkaian yang baru dibuat, anda boleh menggunakan opsyen **Perwakilan julat IP lanjutan**: masukkan senarai semua rangkaian pada medan teks masing-masing (*sebarang format standard disokong*) dan tekan butang **Sahkan** untuk memastikan format boleh dikenal pasti. Kemudian, tekan **OK** untuk mengesahkan dan menyimpan data.

- **Edit rangkaian** - membuka tettingkap dialog **Sifat rangkaian** (*lihat di atas*) di mana anda boleh mengedit parameter bagi rangkaian yang telah ditakrifkan (*dialog adalah sama dengan dialog untuk menambah rangkaian baru, lihat*

penerangan dalam perenggan sebelumnya)

- **Padam rangkaian** - membuang nota rangkaian yang dipilih daripada senarai rangkaian
- **Tandakan sebagai selamat** - secara lalai, semua rangkaian dikira tidak selamat, dan hanya jika anda pasti rangkaian masing-masing adalah selamat, anda boleh menggunakan butang ini untuk menguntukkannya (*dan sebaliknya, sebaik sahaja rangkaian diperuntukkan sebagai selamat, teks butang bertukar kepada "Tandakan sebagai tidak selamat"*).
- **Bantuan** - membuka fail bantuan berkaitan dialog

11.5.3. Aplikasi



Dialog **Maklumat aplikasi** menyenaraikan semua aplikasi yang dipasang yang mungkin perlu berkomunikasi pada rangkaian dan ikon untuk tindakan yang diperuntukkan:

-  Benarkan komunikasi untuk semua rangkaian
-  Benarkan komunikasi untuk rangkaian yang ditentukan sebagai Selamat

sahaja

-  Sekat komunikasi
-  Paparkan dialog tanya (pengguna boleh memutuskan buat masa itu sama ada mereka hendak membenarkan atau menyekat komunikasi)
-  Tetapan lanjutan ditentukan

Aplikasi dalam senarai dikesan pada komputer anda (dan diperuntukkan tindakan masing-masing) sama ada sewaktu carian [Wizard Konfigurasi Firewall](#) atau jika aplikasi yang tidak diketahui atau baru dipasang pada selepas ini.

Perhatian: Sila maklum bahawa hanya aplikasi yang telah dipasang boleh dikesan, jadi jika anda memasang aplikasi baru kemudian, anda akan perlu menentukan peraturan Firewall untuknya. Secara lalai, apabila aplikasi baru cuba menyambung pada rangkaian untuk pertama kali, Firewall akan sama ada membuat peraturan untuknya secara automatik mengikut Pangkalan Data Dipercayai atau bertanyakan kepada anda sama ada untuk membenarkan atau menyekat komunikasi. Dalam kes berikutnya, anda boleh menyimpan jawapan sebagai peraturan kekal (yang kemudian, akan disenaraikan dalam dialog ini).

Sudah tentu, anda juga boleh mentakrifkan peraturan untuk aplikasi baru ini serta-merta - dalam dialog ini, tekan **Tambah** dan isikan butiran aplikasi.

Selain dari aplikasi, senarai juga mengandungi dua item khas:

- **Keutamaan Peraturan Aplikasi** (di bahagian atas senarai) adalah keutamaan dan sentiasa digunakan sebelum peraturan bagi sebarang aplikasi individu.
- **Peraturan Aplikasi Lain** (di bahagian bawah senarai) digunakan sebagai "contoh terakhir", apabila tiada peraturan aplikasi khusus yang digunakan, cth. untuk aplikasi yang tidak diketahui dan tidak ditakrifkan.

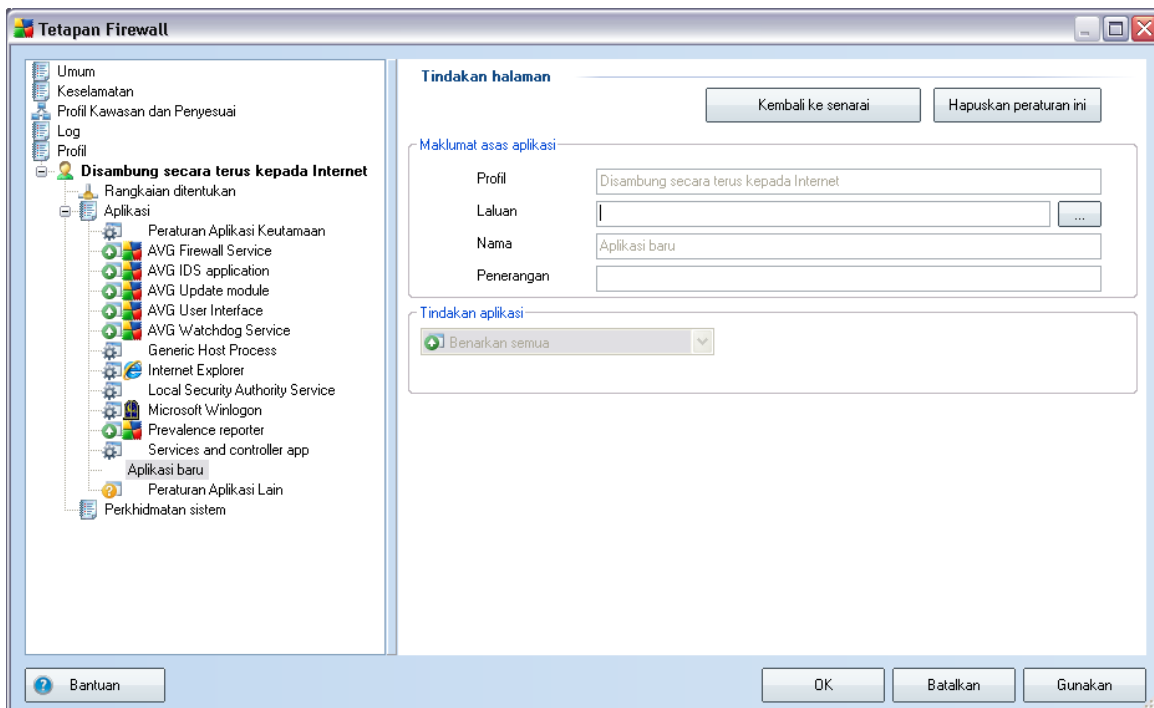
Item ini mempunyai beberapa opsyen tetapan berbeza dari aplikasi biasa, dan hanya ditujukan untuk pengguna berpengalaman. sangat mengesyorkan

Butang kawalan

Senarai boleh diedit dengan menggunakan butang kawalan berikut:

- **Tambah** - membuka dialog [Tindakan Halaman](#) untuk menentukan peraturan aplikasi baru

- **Edit** - membuka dialog **Tindakan halaman** yang sama dengan data yang diberikan untuk pengeditan bagi set peraturan aplikasi sedia ada
- **Padam** - membuang aplikasi yang dipilih daripada senarai
- **Bantuan** - membuka fail bantuan berkaitan dialog



Dalam dialog ini, anda boleh mentakrifkan tetapan untuk aplikasi tertentu secara terperinci.

Tindakan halaman

- Butang **Kembali ke senarai** akan memaparkan gambaran keseluruhan semua peraturan aplikasi yang ditakrifkan.
- Butang **Padam peraturan ini** akan memadam peraturan aplikasi yang sedang dipaparkan. Sila maklum bahawa tindakan ini tidak boleh diundur!

Maklumat asas aplikasi

Dalam bahagian ini, isikan **Nama** aplikasi, dan secara pilihan **Penerangan** (*komen ringkas untuk maklumat anda*). Dalam medan **Laluan**, masukkan laluan penuh ke aplikasi (*fail boleh laku*) pada cakera; secara alternatif, anda boleh mencari aplikasi dalam struktur pepohon dengan mudah selepas menekan butang "...".

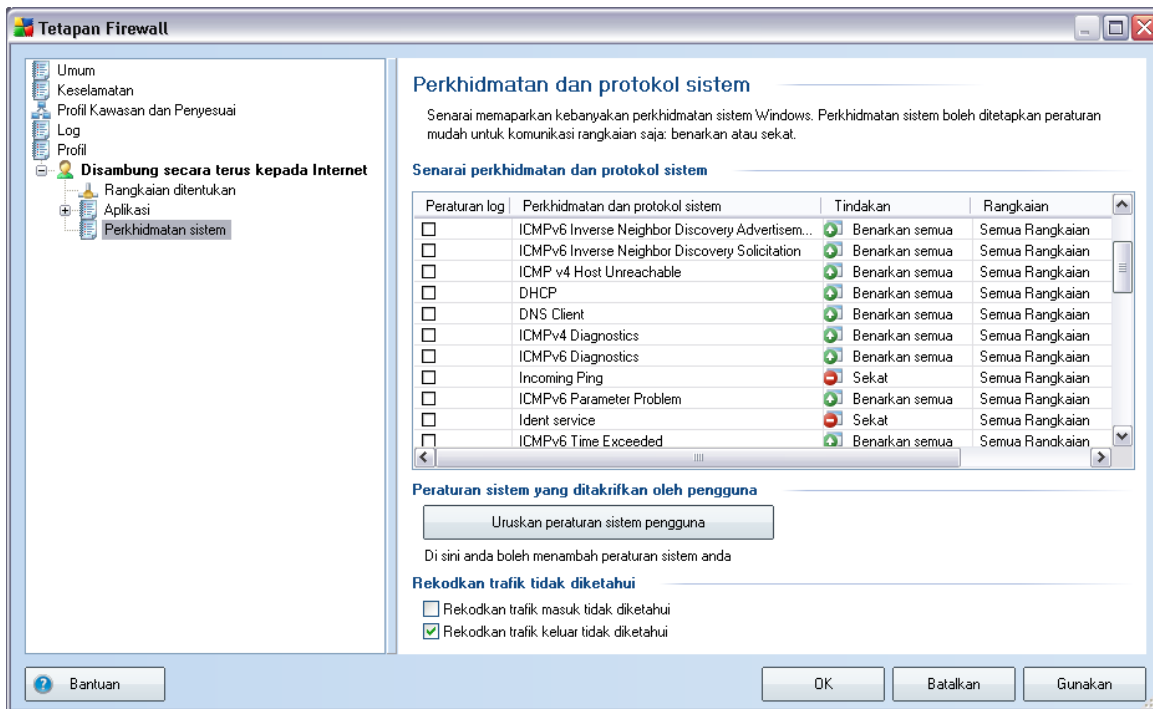
Tindakan aplikasi

Dalam menu jatuh bawah, anda boleh memilih peraturan Firewall untuk aplikasi, cth. apa Firewall patut lakukan apabila aplikasi cuba berkomunikasi pada rangkaian:

-  **Benarkan untuk semua** akan membenarkan aplikasi untuk berkomunikasi di atas semua rangkaian yang ditentukan dan penyesuai tanpa batasan.
-  **Benarkan untuk selamat** akan hanya membenarkan aplikasi untuk berkomunikasi melalui rangkaian yang ditentukan sebagai Selamat (boleh dipercayai).
-  **Sekat** akan menghalang komunikasi secara automatik; aplikasi tidak akan dibenarkan berhubung ke mana-mana rangkaian.
-  **Tanya** akan memaparkan dialog yang membolehkan anda memutuskan sama ada anda mahu membenarkan atau menghalang percubaan komunikasi pada waktu itu.
-  **Tetapan lanjutan** memaparkan pilihan tetapan yang diluaskan dan terperinci di bahagian bawah dialog bahagian **Peraturan butiran aplikasi**. Butiran akan digunakan mengikut susunan senarai, maka anda boleh **Alih ke atas** atau **Alih ke bawah** peraturan dalam senarai seperti yang diperlukan untuk menetapkan keutamaannya. Selepas mengklik peraturan khusus dalam senarai, gambaran keseluruhan bagi butiran peraturan akan dipaparkan di bahagian bawah dialog. Sebarang nilai biru yang digaris bawah boleh ditukar dengan mengklik dalam dialog tetapan masing-masing. Untuk memadam peraturan yang diserlahkan, hanya tekan **Buang**. Untuk menentukan peraturan baru, gunakan butang **Tambah** untuk membuka dialog **Ubah butiran peraturan** yang membenarkan anda menentukan semua butiran yang diperlukan.

11.5.4. Perkhidmatan Sistem

Sebarang pengeditan dalam Dialog perkhidmatan dan protokol sistem yang bertujuan untuk pengguna yang berpengalaman SAHAJA!



Dialog **Perkhidmatan dan protokol sistem** menyenaraikan perkhidmatan dan protokol piawai Windows yang mungkin diperlukan untuk berkomunikasi pada rangkaian. Carta terdiri daripada lajur berikut:

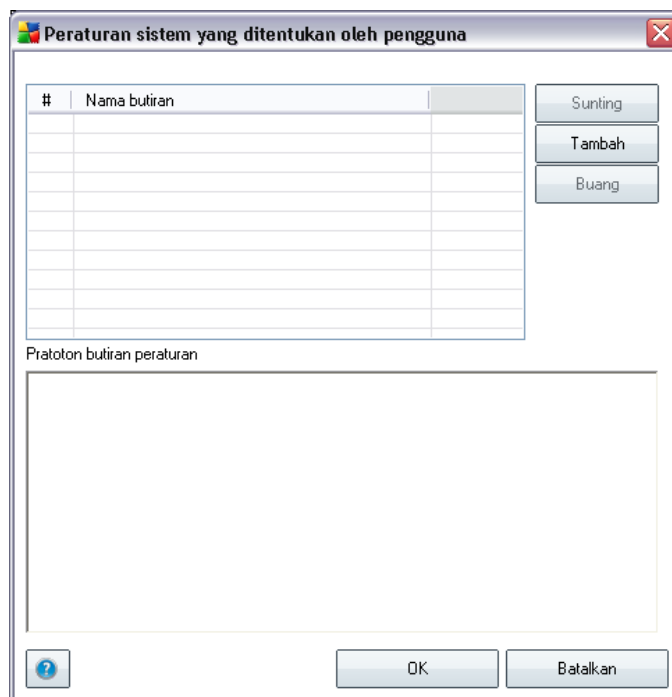
- **Tindakan peraturan log** - kotak ini membolehkan anda menghidupkan rakaman setiap aplikasi peraturan dalam Log.
- **Perkhidmatan dan protokol sistem** - lajur ini menunjukkan nama perkhidmatan sistem masing-masing.
- **Tindakan** - lajur ini memaparkan ikon untuk tindakan yang diperuntukkan:
 - o  Benarkan komunikasi untuk semua rangkaian
 - o  Benarkan komunikasi untuk rangkaian yang ditentukan sebagai Selamat sahaja

o  Sekat komunikasi

- **Rangkaian** - lajur ini menyatakan pada rangkaian tertentu mana peraturan sistem digunakan

Senarai (*termasuk tindakan diperuntukkan*) boleh diedit menggunakan butang berikut:

- Untuk mengedit tetapan bagi sebarang item dalam senarai (*termasuk tindakan diperuntukkan*), klik kanan item dan pilih **Edit**.
- Untuk membuka dialog baru untuk menentukan peraturan perkhidmatan sistem anda sendiri (*lihat gambar di bawah*), tekan butang **Uruskan peraturan sistem pengguna**. Bahagian atas bagi dialog **Peraturan sistem yang ditakrif pengguna** memaparkan gambaran keseluruhan bagi semua butiran bagi peraturan sistem yang diedit, bahagian bawah kemudiannya, memaparkan butiran yang dipilih. Butiran peraturan yang ditentukan pengguna boleh diedit, ditambah, atau dipadam dengan butang masing-masing; butiran ditentukan pengilang hanya boleh diedit:



Amaran: Sila maklum bahawa tetapan peraturan butiran adalah lanjutan,

terutamanya bertujuan untuk pentadbir rangkaian yang memerlukan kawalan penuh pada konfigurasi Firewall. Jika anda tidak biasa dengan jenis protokol komunikasi, nombor port rangkaian, definisi alamat IP dll., harap jangan ubah suai tetapan ini! Jika anda benar-benar perlu mengubah konfigurasi, sila rujuk fail bantuan dialog masing-masing untuk butiran khusus .

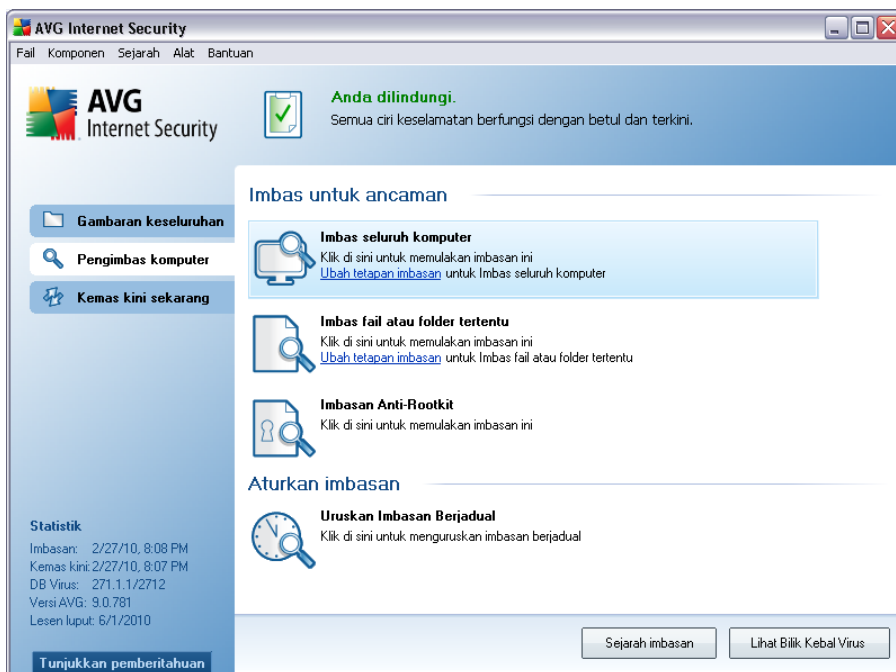
Rekodkan trafik tidak diketahui

- **Log trafik masuk tidak diketahui** – tandakan kotak untuk merekodkan dalam Log setiap percubaan tidak diketahui untuk menyambung ke komputer anda dari luar.
- **Log trafik masuk tidak diketahui** – tandakan kotak untuk merekodkan dalam Log setiap percubaan tidak diketahui dari komputer anda untuk menyambung ke lokasi luar.

12. Pengimbasan AVG

Pengimbasan adalah bahagian penting bagi kefungsiian **AVG 9 Internet Security**. Anda boleh menjalankan ujian yang dalam permintaan atau [menjaduakannya untuk dijalankan secara berkala](#) pada masa yang sesuai.

12.1. Antara Muka Pengimbasan



Antara muka pengimbasan AVG boleh diakses melalui ***pautan pantas*** [Pengimbas Komputer](#). Klik pautan ini untuk beralih ke dialog ***Imbas untuk ancaman***. Dalam dialog ini, anda akan menemui yang berikut:

- gambaran keseluruhan bagi [imbasan yang dipratifikasi](#) - tiga jenis pengimbasan yang ditentukan oleh vendor perisian sedia untuk digunakan dengan serta-merta mengikut permintaan atau jadual:
 - o [Imbas seluruh komputer](#)
 - o [Imbas fail atau folder tertentu](#)
 - o [Imbasan AntiRootkit](#)

- [imbas bahagian](#) yang dijadualkan - di mana anda boleh mentakrifkan ujian baru dan membuat jadual baru seperti yang diperlukan.

Butang kawalan

Butang kawalan tersedia dalam antara muka pengujian adalah yang berikut:

- **Sejarah imbasan** - memaparkan dialog [Gambaran keseluruhan keputusan imbasan](#) dengan sejarah keseluruhan imbasan
- **Lihat Bilik Kebal Virus** - membuka tettingkap baru dengan [Bilik Kebal Virus](#) - ruang di mana jangkitan yang dikesan dikuarantinkan

12.2. Imbasan Pratakrif

Salah satu ciri utama bagi **AVG 9 Internet Security** adalah pengimbasan dalam permintaan. Ujian dalam permintaan direka bentuk untuk mengimbas pelbagai bahagian komputer anda apabila kecurigaan bagi kemungkinan jangkitan virus berlaku. Walau bagaimanapun, ia amat disarankan untuk menjalankan ujian seperti itu secara tetap walaupun jika anda merasakan tiada virus yang boleh ditemui pada komputer anda.

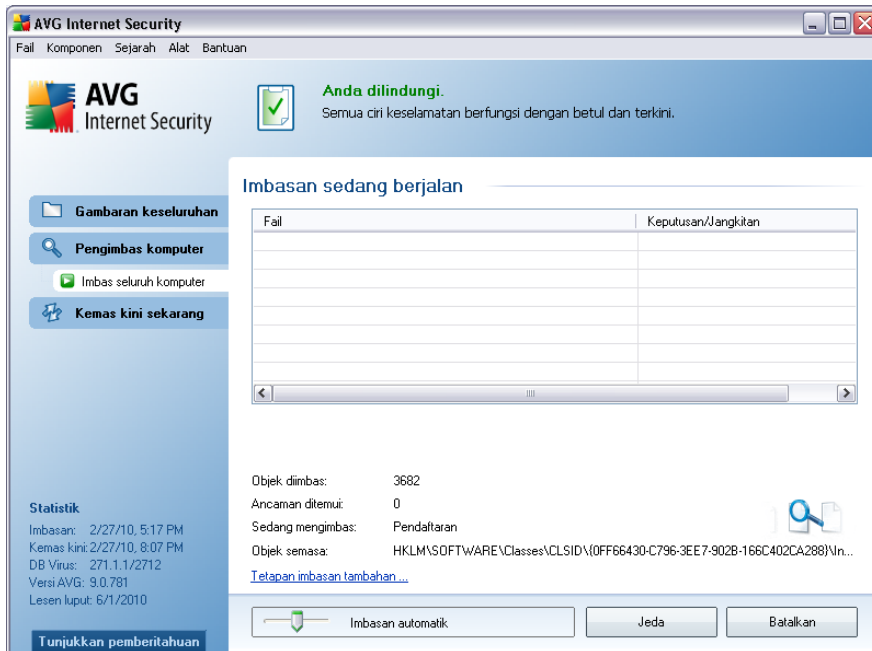
Dalam **AVG 9 Internet Security** anda akan menemui dua jenis pengimbasan yang dipratetapkan oleh vendor perisian:

12.2.1. Imbas Seluruh Komputer

Imbas seluruh komputer - mengimbas seluruh komputer anda untuk kemungkinan jangkitan dan/atau atur cara yang tidak diingini. Ujian ini akan mengimbas semua pemacu keras komputer anda, akan mengesan dan memulihkan sebarang virus yang ditemui atau membuang jangkitan yang dikesan ke [Bilik Kebal Virus](#). Mengimbas seluruh komputer anda perlu dijadualkan pada stesen kerja sekurang-kurangnya sekali seminggu.

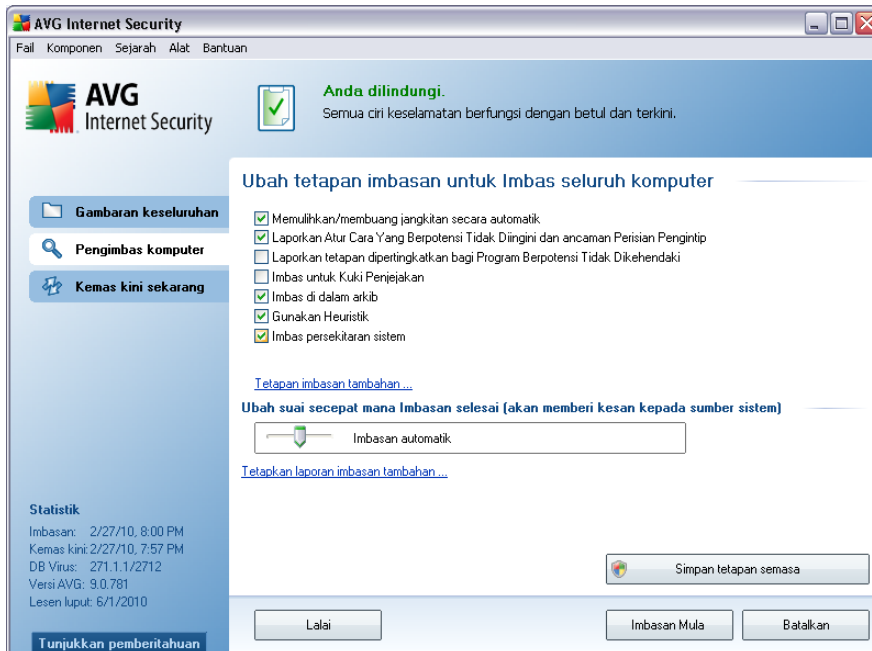
Lancarkan imbasan

Imbas seluruh komputer boleh dilancarkan dari [antara muka imbasan](#) dengan mengklik pada ikon imbasan. Tiada tetapan khusus selanjutnya perlu dikonfigurasi untuk jenis imbasan ini, pengimbasan akan bermula dengan serta-merta dalam dialog **Imbasan sedang dijalankan** (*lihat gambar skrin*). Imbasan boleh diganggu sementara waktu (**Jeda**) atau dibatalkan (**Berhenti**) jika perlu.

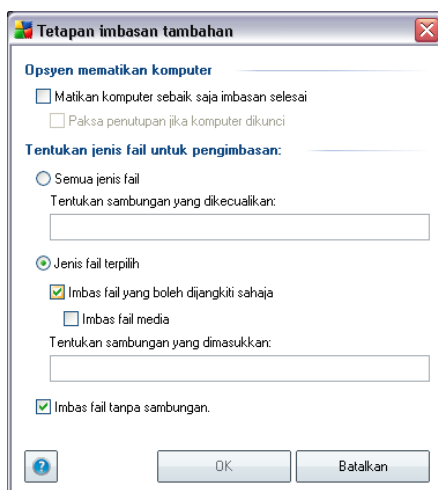


Pengeditan konfigurasi imbasan

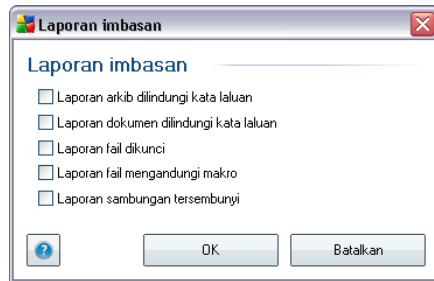
Anda mempunyai opsi pengeditan bagi tetapan lalai yang dipratetapkan bagi **Imbas seluruh komputer**. Tekan pautan **Ubah tetapan imbasan** untuk pergi ke dialog **Ubah tetapan imbasan untuk Mengimbas seluruh komputer**. Adalah digalakkan untuk menyimpan tetapan lalai melainkan anda mempunyai alasan kukuh untuk menukarnya!



- **Parameter imbasan** - dalam senarai parameter imbasan, anda boleh menghidupkan/mematikan parameter tertentu seperti yang diperlukan. Secara lalai, kebanyakan parameter dihidupkan dan ini akan digunakan secara automatik sewaktu imbasan.
- **Tetapan imbasan tambahan** - pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



- o **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).
- o **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbis:
 - **Semua jenis fail** dengan kemungkinan bagi menentukan pengecualian daripada pengimbasan dengan memberikan senarai pemanjangan fail yang dipisahkan oleh koma yang tidak seharusnya diimbis;
 - **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbis, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbis.
 - Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbis setiap masa.
- **Imbas keutamaan proses** - anda boleh menggunakan gelongsor untuk mengubah keutamaan proses imbasan. Secara lalai, keutamaan ditetapkan kepada tahap sederhana (*Imbasan automatik*) yang mengoptimumkan kelajuan proses pengimbasan dan penggunaan sumber sistem. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud muat sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama imbasan berlaku*), atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).
- **Tetapkan laporan imbasan tambahan** - pautan membuka dialog **Imbas laporan** di mana anda boleh memilih jenis kemungkinan penemuan yang harus dilaporkan:



Amaran: Tetapan imbasan ini adalah sama dengan parameter bagi imbasan yang baru ditakrifkan - seperti yang diterangkan dalam bab [Pengimbasan AVG / Penjadualan imbasan / Cara untuk Mengimbas](#). Adakah anda akan memutuskan untuk mengubah konfigurasi lalai bagi **Imbas seluruh komputer** kemudian, anda boleh menyimpan tetapan baru anda sebagai konfigurasi lalai untuk digunakan untuk semua imbasan selanjutnya bagi seluruh komputer.

12.2.2. Imbas Fail atau Folder Tertentu

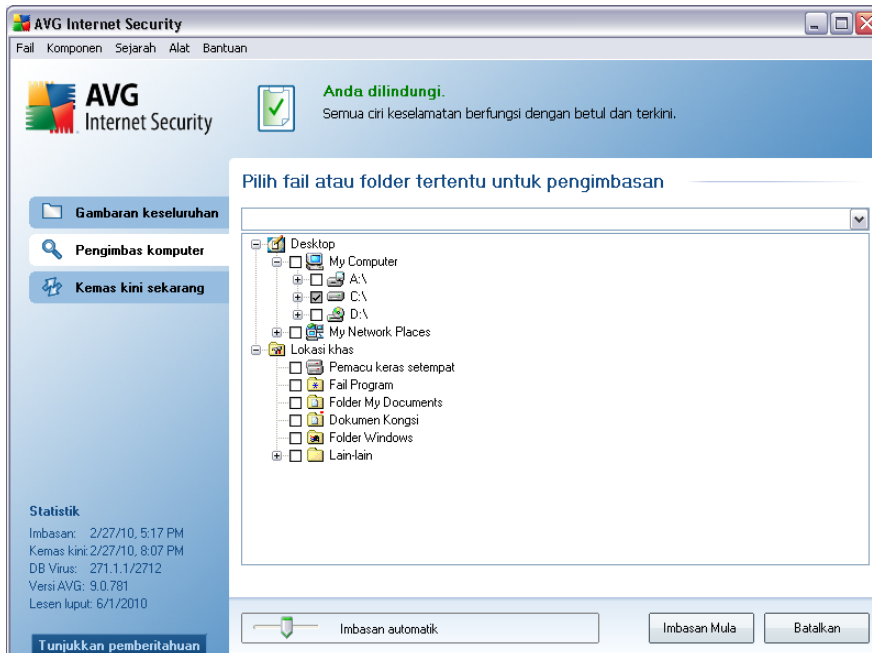
Imbas fail atau folder tertentu - mengimbas hanya kawasan komputer anda yang anda telah pilih untuk diimbas (*folder yang diimbas, cakera keras, cakera liut, CD, dll.*). Perkembangan imbasan jika pengesanan virus dan rawatannya adalah sama dengan imbas seluruh komputer: sebarang virus yang ditemui dipulihkan atau dibuang ke [Bilik Kebal Virus](#). Pengimbasan fail atau folder tertentu boleh digunakan untuk menyediakan ujian anda sendiri dan penjadualannya berdasarkan pada keperluan anda.

Lancarkan imbasan

Imbas fail atau folder tertentu boleh dilancarkan dari [pengimbasan antara muka](#) dengan mengklik pada ikon imbasan. Dialog baru yang dipanggil **Pilih fail atau folder untuk pengimbasan** terbuka. Dalam struktur pepohon komputer anda, pilih folder yang anda hendak imbas. Laluan kepada setiap folder yang dipilih akan dijana secara automatik dan muncul dalam kotak semakan di bahagian atas dialog ini.

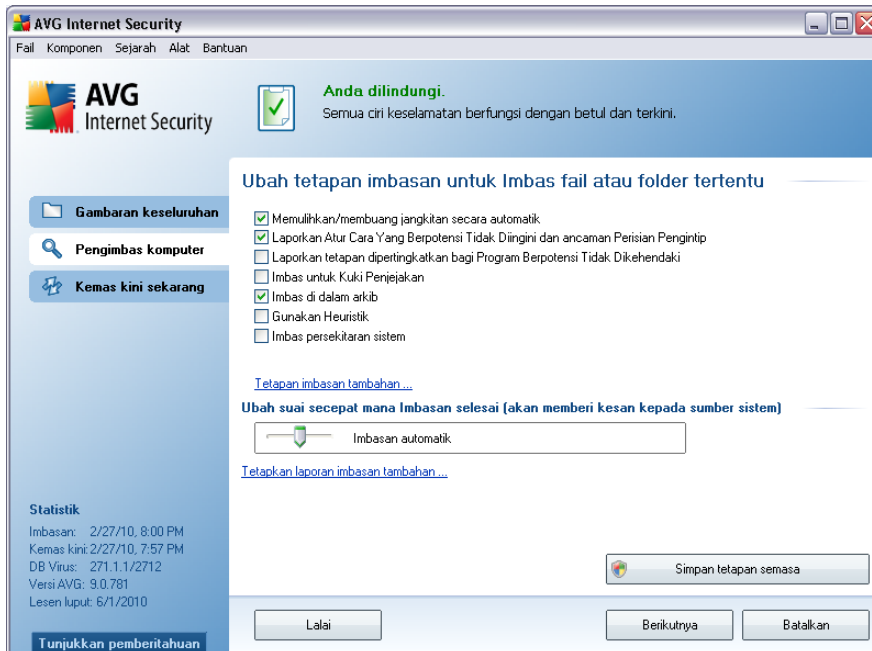
Terdapat juga kemungkinan mempunyai folder tertentu yang diimbas semasa semua subfoldernya tidak dimasukkan dalam imbasan ini, untuk melakukannya, tuliskan tanda tambah "+" di hadapan laluan yang dijana secara automatik (*lihat gambar skrin*). Untuk tidak memasukkan keseluruhan folder dari penggunaan imbasan, gunakan parameter "!".

Akhir sekali, untuk melancarkan imbasan, tekan butang **Mulakan imbasan** ; proses pengimbasan itu sendiri adalah secara dasarnya sama dengan [imbas seluruh komputer](#).

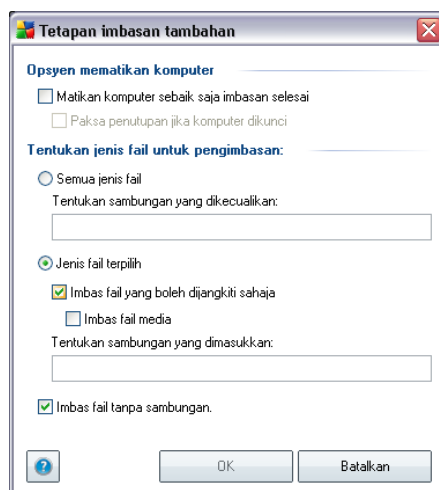


Pengeditan konfigurasi imbasan

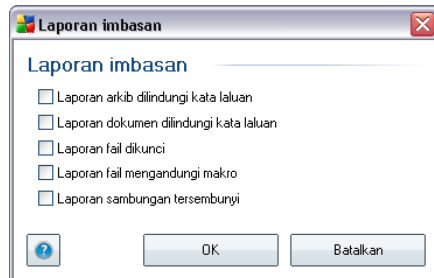
Anda mempunyai opsi pengeditan bagi tetapan lalai yang dipratetapkan bagi **Imbasan fail atau folder tertentu**. Tekan pautan **Ubah tetapan imbasan** untuk pergi ke dialog **Ubah tetapan imbasan untuk Mengimbas fail atau folder tertentu**. **Adalah digalakkan untuk menyimpan tetapan lalai melainkan anda mempunyai alasan kukuh untuk menukarnya!**



- **Parameter pengimbasan** - dalam senarai parameter pengimbasan, anda boleh menghidupkan/mematikan parameter tertentu seperti yang diperlukan (*untuk penerangan terperinci bagi tetapan ini, sila rujuk bab [Tetapan Lanjutan AVG / Pengimbasan / Imbas Fail atau Folder Tertentu](#)*).
- **Tetapan imbasan tambahan** - pautan membuka dialog Tetapan imbasan tambahan di mana anda boleh menentukan parameter berikut:



- o **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).
- o **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbas:
 - **Semua jenis fail** dengan kemungkinan bagi pengecualian yang ditakrifkan daripada pengimbasan dengan memberikan senarai pemanjangan fail yang dipisahkan oleh koma yang tidak harus diimbas;
 - **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
 - Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.
- **Imbas keutamaan proses** - anda boleh menggunakan gelongsor untuk mengubah keutamaan proses imbasan. Secara lalai, keutamaan ditetapkan kepada tahap sederhana (*Imbasan automatik*) yang mengoptimumkan kelajuan proses pengimbasan dan penggunaan sumber sistem. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud muat sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama imbasan berlaku*), atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).
- **Tetapkan laporan imbasan tambahan** - pautan membuka dialog **Imbas Laporan** di mana anda boleh memilih apakah jenis kemungkinan penemuan yang harus dilaporkan:



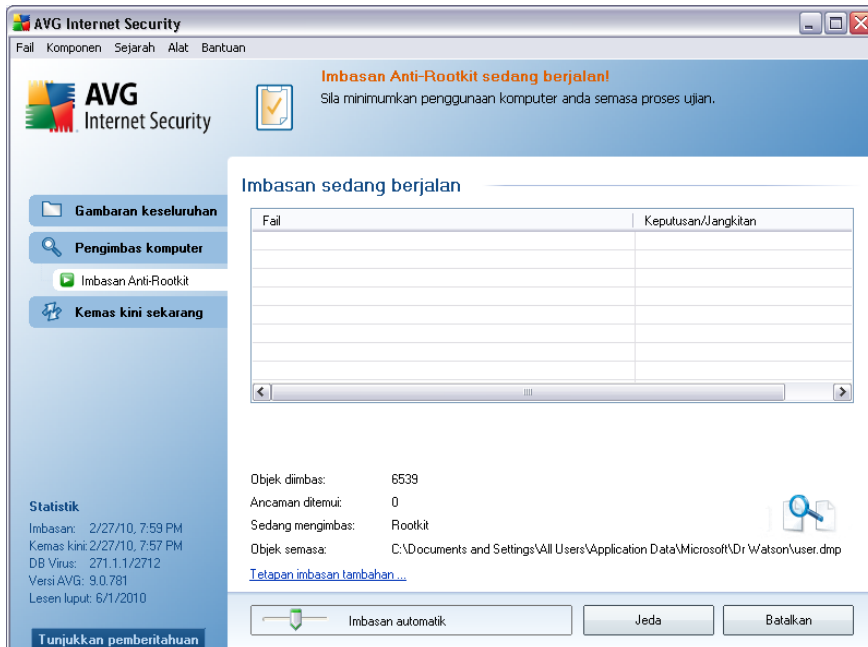
Amaran: Tetapan imbasan ini adalah sama dengan parameter bagi imbasan yang baru ditakrifkan - seperti yang diterangkan dalam bab [Pengimbasan AVG / Penjadualan imbasan / Cara untuk Mengimbas](#). Sekiranya anda hendak memutuskan untuk mengubah konfigurasi lalai bagi **Imbas fail atau folder tertentu** kemudian, anda boleh menyimpan tetapan baru anda sebagai konfigurasi lalai untuk digunakan untuk semua imbasan selanjutnya bagi fail atau folder tertentu. Serta, konfigurasi ini akan digunakan sebagai templat untuk semua imbasan yang baru dijadualkan ([semua imbasan yang dijadualkan adalah berdasarkan pada konfigurasi semasa Imbasan fail atau folder yang dipilih](#)).

12.2.3. Imbasan AntiRootkit

Imbasan AntiRootkit mencari komputer anda untuk kemungkinan rootkit (*atur cara dan teknologi yang boleh menutupi aktiviti malware dalam komputer anda*). Jika rootkit dikesan, ini tidak semestinya bermaksud komputer anda dijangkiti. Dalam sesetengah kes, pemacu atau bahagian tertentu aplikasi biasa mungkin telah mengesan rootkit dengan salah.

Lancarkan imbasan

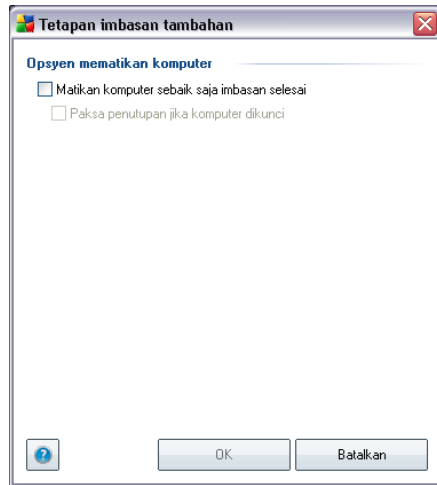
Imbasan AntiRootkit boleh dilancarkan secara terus dari [antara muka imbasan](#) dengan mengklik pada ikon imbasan. Tiada tetapan khusus selanjutnya telah dikonfigurasi untuk jenis imbasan ini, imbasan akan bermula dengan serta-merta dalam dialog **Imbasan sedang dijalankan** (*lihat gambar skrin*). Imbasan boleh diganggu sementara waktu (**Jeda**) atau dibatalkan (**Berhenti**) jika perlu.



Pengeditan konfigurasi imbasan

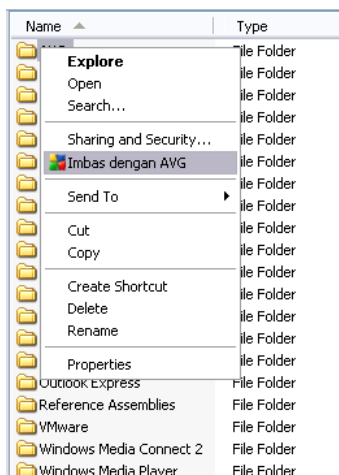
Imbasan AntiRootkit sentiasa dilancarkan dalam tetapan lalai dan pengeditan bagi parameter imbasan hanya boleh diakses dalam dialog [Tetapan Lanjutan AVG / AntiRootkit](#). Dalam [antara muka imbasan](#), hanya konfigurasi berikut yang tersedia:

- **Imbasan automatik** - anda boleh menggunakan gelangsar untuk mengubah keutamaan proses imbasan. Secara lalai, keutamaan ditetapkan kepada tahap sederhana (*Imbasan automatik*) yang mengoptimumkan kelajuan proses pengimbasan dan penggunaan sumber sistem. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud muat sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama imbasan berlaku*), atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).
- **Tetapan imbasan tambahan** - pautan ini membuka dialog **Tetapan imbasan tambahan** baru di mana anda boleh menentukan kemungkinan keadaan matikan komputer berkaitan dengan **Imbasan AntiRootkit** (**Matikan komputer apabila imbasan selesai**, berkemungkinan **Paksa matikan jika komputer dikunci**):



12.3. Pengimbasan dalam Windows Explorer

Selain daripada imbasan dipratakrif yang dilancarkan untuk seluruh komputer atau kawasannya yang dipilih, **AVG 9 Internet Security** juga menawarkan pilihan bagi pengimbasan pantas bagi objek khusus secara terus dalam persekitaran Windows Explorer. Jika anda ingin membuka fail yang tidak diketahui dan anda tidak pasti mengenai kandungannya, anda mungkin mahu memeriksa dengan permintaan. Ikuti langkah-langkah ini:



- Dalam Windows Explorer, serlahkan fail (atau folder) yang anda hendak periksa
- Klik kanan tetikus anda pada objek untuk membuka menu konteks



- Pilih opsyen **Imbas dengan AVG** supaya fail diimbis dengan AVG

12.4. Pengimbasan Garis Perintah

Dalam **AVG 9 Internet Security** terdapat pilihan bagi menjalankan imbasan daripada baris arahan. Anda boleh menggunakan opsyen ini contohnya pada pelayan atau semasa membuat skrip kelompok untuk dilancarkan secara automatik selepas but komputer. Daripada baris arahan, anda boleh melancarkan pengimbasan dengan paling banyak parameter yang ditawarkan dalam antara muka pengguna grafik AVG.

Untuk melancarkan imbasan AVG daripada baris arahan, jalankan arahan berikut dalam folder di mana AVG dipasang.

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

Sintaks arahan

Sintaks arahan berikut:

- **avgscanx /parameter** ... cth. **avgscanx /comp** untuk pengimbasan seluruh komputer
- **avgscanx /parameter /parameter** .. dengan parameter berbilang, ini harus digariskan dalam barisan dan dipisahkan dengan ruang dan aksara garis condong
- jika parameter memerlukan nilai khusus untuk diberikan (cth. **/parameter** imbasan yang memerlukan maklumat mengenai apa kawasan apa yang dipilih pada komputer anda yang akan diimbis dan anda perlu memberikan laluan sebenar kepada bahagian yang dipilih), nilai dibahagikan melalui koma bertitik, contohnya: **avgscanx /scan=C:\;D:**

Parameter imbasan

Untuk memaparkan gambaran keseluruhan parameter sedia ada, taipkan arahan masing-masing bersama-sama parameter **/?** atau **/HELP** (cth. **avgscanx /?**). Satu-satunya parameter wajib adalah **/SCAN** untuk menentukan bahagian komputer yang harus diimbis. Untuk penerangan terperinci tentang opsyen, lihat [gambaran keseluruhan parameter garis arahan](#).

Untuk menjalankan imbasan, tekan **Enter**. Semasa pengimbasan anda boleh menghentikan proses dengan **Ctrl+C** atau **Ctrl+Pause**.

Pengimbasan CMD dilancarkan dari antara muka grafik

Semasa anda menjalankan komputer anda dalam Windows Safe Mode, terdapat juga kemungkinan untuk melancarkan imbasan baris arahan daripada antara muka pengguna grafik. Imbasan itu sendiri akan dilancarkan daripada baris arahan, dialog **Pengarang Baris Perintah** hanya membenarkan anda menentukan parameter pengimbasan paling banyak dalam antara muka grafik yang selesai.

Memandangkan dialog ini hanya boleh diakses dalam Windows Safe Mode, untuk penerangan terperinci bagi dialog ini, sila rujuk fail bantuan terbuka secara terus dari dialog.

12.4.1. Parameter Imbasan CMD

Sila cari senarai semua parameter yang tersedia berikut untuk pengimbasan baris arahan:

- **/SCAN** [Imbas fail atau folder tertentu](#) /SCAN=path;path (e.g. /SCAN=C:\;D:\)
- **/COMP** [Imbas seluruh komputer](#)
- **/HEUR** Guna [analisis heuristik](#)
- **/EXCLUDE** Tidak termasuk laluan atau fail daripada imbasan
- **/@** Fail perintah /nama fail/
- **/EXT** Imbas sambungan ini/contohnya EXT=EXE,DLL/
- **/NOEXT** Jangan imbas sambungan ini /contohnya NOEXT=JPG/
- **/ARC** Imbas arkib
- **/CLEAN** Cuci secara automatik
- **/TRASH** Alihkan fail yang dijangkiti ke [Bilik Kebal Virus](#)
- **/QT** Ujian pantas
- **/MACROW** Laporkan makro

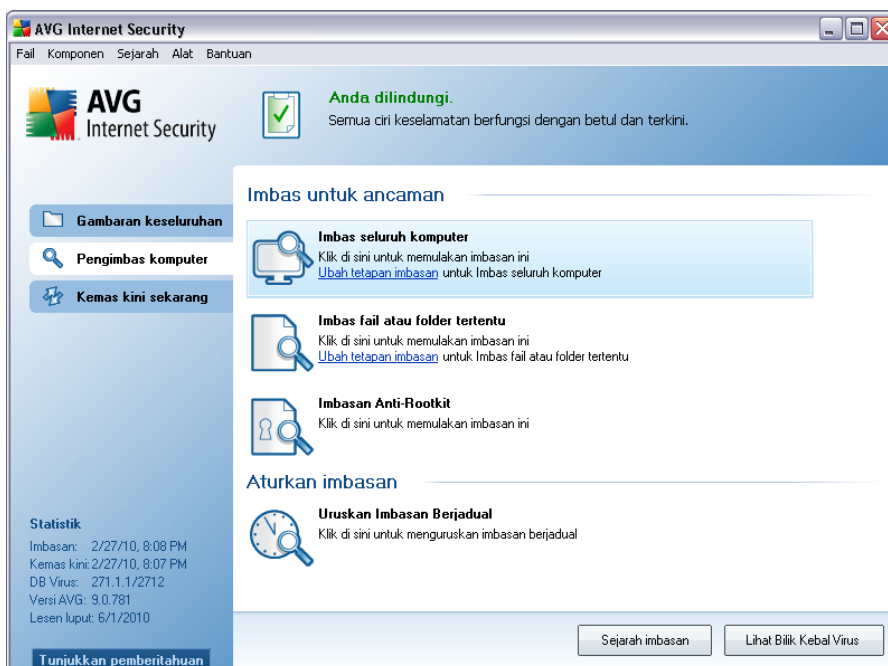
- **/PWDW** Laporkan fail yang dilindungi oleh kata laluan
- **/IGNLOCKED** Abaikan fail yang dikunci
- **/REPORT** Laporkan kepada fail /nama fail
- **/REPAPPEND** Lampirkan kepada fail laporan
- **/REPOK** Laporkan fail yang tidak dijangkiti sebagai OK
- **/NOBREAK** Jangan benarkan CTRL-BREAK dihenti paksa
- **/BOOT** Dayakan semakan MBR/BOOT
- **/PROC** Imbas proses aktif
- **/PUP** Laporkan "[Atur cara yang berkemungkinan tidak dikehendaki](#)"
- **/REG** Imbas pendaftaran
- **/COO** Imbas kuki
- **/?** Memaparkan bantuan pada topik ini
- **/HELP** Paparkan bantuan pada topik ini
- **/PRIORITY** Tetapkan keutamaan imbasan /Rendah, Auto, Tinggi/
(lihat [Tetapan / Imbasan lanjutan](#))
- **/SHUTDOWN** Mematikan komputer apabila imbasan selesai
- **/FORCESHUTDOWN** Paksa komputer dimatikan apabila imbasan selesai
- **/ADS** Imbas Aliran Data Berganti-ganti (NTFS sahaja)

12.5. Penjadualan Imbasan

Dengan **AVG 9 Internet Security** anda boleh menjalankan imbasan dengan permintaan (contohnya, apabila anda mengesyaki jangkitan telah dibawa ke komputer anda) atau berasaskan perancangan yang dijadualkan. Ia amat disyorkan untuk menjalankan imbasan berdasarkan jadual: dengan cara ini, anda boleh memastikan komputer anda dilindungi dari sebarang kemungkinan daripada dijangkiti dan anda tidak perlu risau jika dan di mana untuk dilancarkan

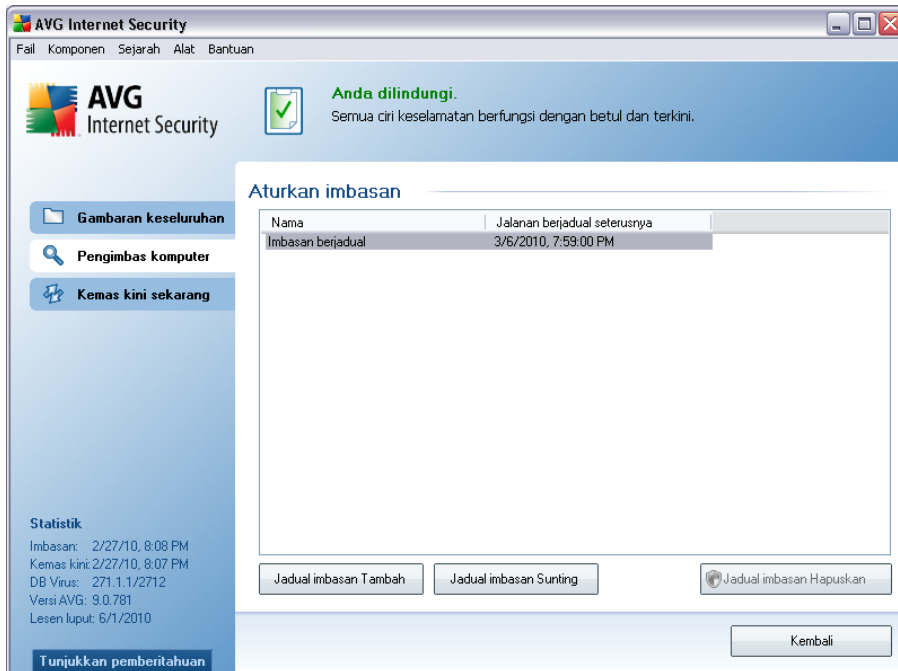
Anda harus melancarkan **Imbas seluruh komputer** secara tetap, sekurang-kurangnya sekali seminggu. Walau bagaimanapun, jika boleh, lancarkan imbas seluruh komputer setiap hari - seperti yang disediakan dalam konfigurasi lalai jadual imbasan. Jika komputer "sentiasa dihidupkan", kemudian, anda boleh menjadualkan imbasan di luar waktu bekerja. Jika komputer kadangkala dimatikan, kemudian, imbasan yang dijadualkan untuk berlaku **pada permulaan komputer semasa tugas telah terlepas**.

Untuk membuat jadual imbasan baru, lihat **antara muka imbasan AVG** dan cari bahagian bawah yang dipanggil **Jadualkan imbasan**:



Aturkan imbasan

Klik ikon grafik dalam bahagian **Jadualkan imbasan** untuk membuka dialog **Jadualkan imbasan** di mana anda menemui senarai semua imbasan yang sedang dijadualkan:

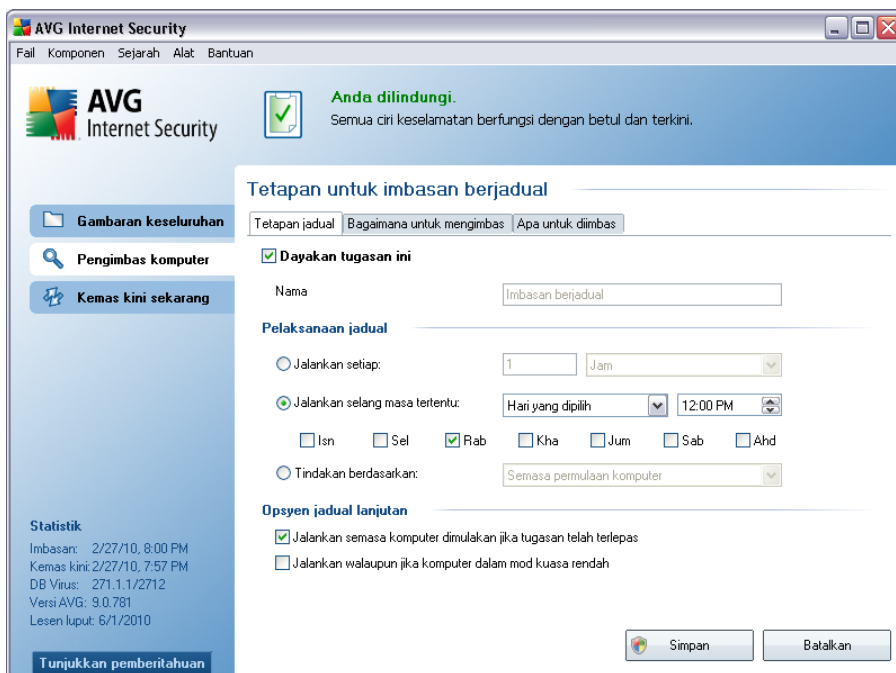


Anda boleh mengedit / menambah imbasan menggunakan butang kawalan berikut:

- **Tambah jadual imbasan** - butang tersebut membuka dialog **Tetapan untuk imbasan yang dijadualkan**, tab [Jadualkan tetapan](#). Dalam dialog ini, anda boleh menentukan parameter bagi ujian yang baru ditakrifkan.
- **Edit jadual imbasan** - butang ini hanya boleh digunakan jika sebelum ini, anda telah memilih ujian sedia ada dari senarai ujian yang dijadualkan. Dalam keadaan tersebut, butang menjadi aktif dan anda boleh mengkliknya untuk beralih ke dialog **Tetapan untuk imbasan yang dijadualkan**, tab [Tetapan jadual](#). Parameter bagi ujian yang dipilih telah ditentukan di sini dan boleh diedit.
- **Padam jadual imbasan** - butang ini juga aktif jika sebelum ini, anda telah memilih ujian sedia ada dari senarai ujian yang dijadualkan. Kemudian, ujian ini boleh dipadamkan dari senarai dengan menekan butang kawalan. Walau bagaimanapun, anda boleh membuang ujian anda sendiri; **Jadual imbasan seluruh komputer** yang dipraktakrifkan dalam tetapan lalai tidak boleh dipadam.
- **Kembali** - kembali ke [antara muka pengimbasan AVG](#)

12.5.1. Tetapan Jadual

Jika anda mahu menjadualkan ujian baru dan pelancaran tetapnya, masukkan dialog **Tetapan untuk ujian yang dijadualkan** (klik butang **Tambah jadual imbasan** dalam dialog **Jadualkan imbasan**). Dialog ini dibahagikan ke dalam tiga tab: **Tetapan jadual** - lihat gambar di bawah (tab lalai yang anda akan diarahkan semula secara automatik ke), **Bagaimana untuk mengimbas** dan **Apa yang hendak diimbas**.



Pada tab **Jadualkan tetapan** anda boleh menanda/menyahtandakan dahulu item **Dayakan tugas ini** untuk menyahaktifkan ujian yang dijadualkan buat sementara dan menghidupkannya semua apabila perlu.

Seterusnya, berikan nama kepada imbasan yang anda akan buat dan jadualkan. Taipkan nama dalam medan teks dengan item **Nama**. Cuba gunakan nama yang ringkas, deskriptif dan sesuai untuk imbasan untuk membuatkan ia mudah untuk mengenal pasti imbasan dari yang lain.

Contoh: Ia tidak sesuai untuk memanggil imbasan dengan nama "Imbasan baru" atau "Imbasan saya" memandangkan nama ini tidak merujuk kepada apa yang sebenarnya imbasan periksa. Sebaliknya, contoh nama deskriptif adalah "Imbasan kawasan sistem" dll. Serta, tidak perlu untuk menentukan jika nama imbasan sama ada ia adalah imbasan seluruh komputer atau hanya imbasan fail atau folder yang dipilih - imbasan anda sendiri yang akan sentiasa menjadi versi khusus bagi [imbasan bagi fail](#)

[atau folder yang dipilih.](#)

Di dalam dialog ini anda boleh menentukan lebih lanjut parameter imbasan yang berikut:

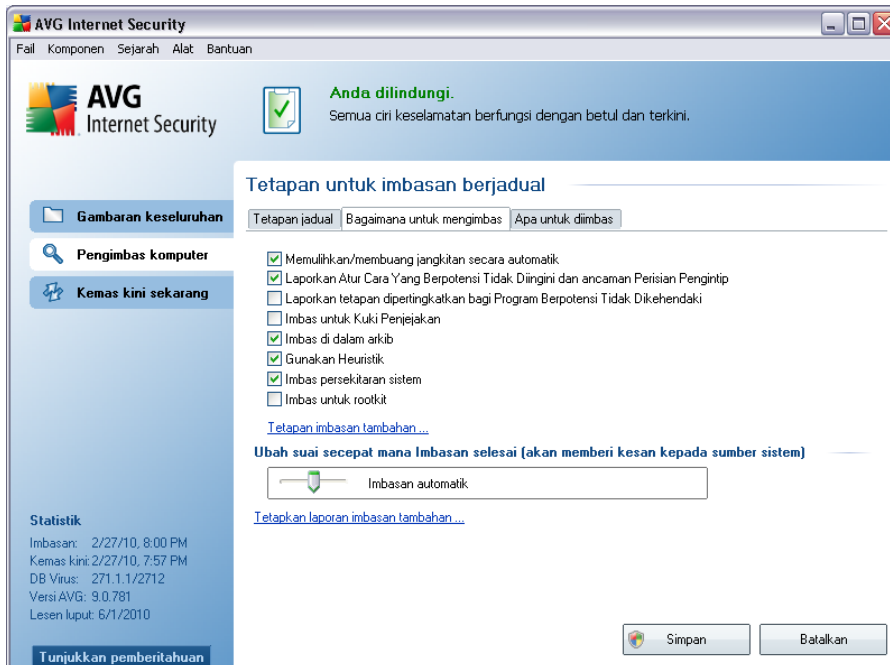
- **Jadualkan untuk dijalankan** - tentukan selang masa untuk pelancaran imbasan yang baru dijadualkan. Pemasaan boleh menjadi sama ada ditentukan oleh pelancaran imbasan berulang selepas satu tempoh masa tertentu (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan dalam masa tertentu ...**), atau berkemungkinan dengan menentukan peristiwa yang pelancaran imbasan harus dikaitkan (**Tindakan berdasarkan pada permulaan komputer**).
- **Opsyen jadual lanjutan** - bahagian ini membenarkan anda menentukan di bawah syarat mana imbasan harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

Butang kawalan Tetapan untuk dialog imbasan berjadual

Terdapat dua butang kawalan yang tersedia pada semua ketiga-tiga tab dialog **Tetapan untuk imbasan yang dijadualkan** (**Jadualkan tetapan**, [Cara untuk mengimbas](#) dan [Apa yang hendak diimbas](#)) dan ini mempunyai kefungsiian yang sama tidak kira pada tab mana yang anda sedang berada:

- **Simpan** - menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#). Oleh itu jika anda ingin mengkonfigurasi parameter ujian pada semua tab, tekan butang untuk menyimpan ia hanya selepas anda telah menyatakan semua keperluan anda.
- **Batal** - membatalkan sebarang perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#).

12.5.2. Bagaimana untuk Mengimbas



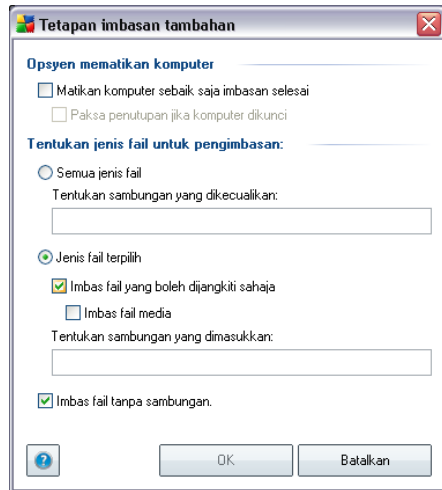
Pada tab ***Cara untuk mengimbas*** anda akan menemui senarai parameter pengimbasan yang boleh dihidupkan/dimatikan secara pilihan. Secara lalai, kebanyakan parameter dibuka dan kefungsiannya akan dilaksanakan semasa pengimbasan. Melainkan anda mempunyai alasan yang sah untuk mengubah tetapan ini, kami menyarankan untuk mengekalkan konfigurasi dipraktakrif:

- ***Pulihkan/buang jangkitan secara automatik*** - (*secara lalai, dihidupkan*): jika virus dikenal pasti sewaktu pengimbasan, ia boleh dipulihkan secara automatik jika rawatan tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik atau jika anda memutuskan untuk mematikan pilihan ini, anda akan diberitahu mengenai pengesanan virus dan perlu memutuskan apa yang perlu dilakukan dengan jangkitan yang dikesan. Tindakan yang disarankan adalah untuk membuang fail yang dijangkiti ke [Bilik Kebal Virus](#).
- ***Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip*** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda

- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini** - jika pilihan sebelumnya diaktifkan, anda juga boleh menanda kotak ini untuk mengesan pakej diluaskan bagi [perisian pengintip](#): atur cara adalah sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat kemudiannya. Ini adalah ukuran tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas untuk Kuki Penjejakan** - (*secara lalai, dihidupkan*): parameter bagi komponen [AntiPerisian Pengintip](#) ini mentakrifkan bahawa kuki itu mesti dikesan sewaktu pengimbasan (*kuki HTTP digunakan untuk pengesanan, penjejakan dan mengekalkan maklumat khusus mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*);
- **Imbas dalam arkib** - (*secara lalai, dihidupkan*): parameter ini mentakrifkan bahawa pengimbasan sepatutnya memeriksa semua fail walaupun jika ia dibungkus dalam sejenis arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** - (*secara lalai, dihidupkan*): analisis heuristik (*persaingan dinamik bagi arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu pengimbasan.
- **Imbas persekitaran sistem** - (*secara lalai, dihidupkan*): pengimbasan juga akan memeriksa kawasan sistem bagi komputer anda;
- **Imbas untuk rootkit** - tandakan rait item ini jika anda mahu memasukkan pengesanan rootkit ke dalam pengimbasan seluruh komputer. Pengesanan rootkit juga tersedia dengan sendiri dalam komponen [AntiRootkit](#);

Kemudian, anda boleh mengubah konfigurasi imbasan seperti berikut:

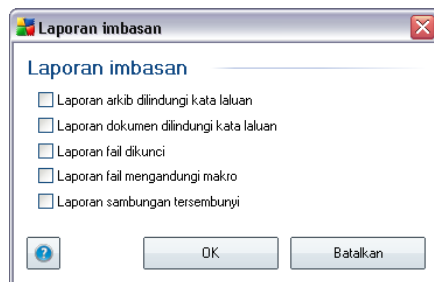
- **Tetapan imbasan tambahan** - pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



- o **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).
- o **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbas:
 - **Semua jenis fail** dengan kemungkinan bagi menentukan pengecualian daripada pengimbasan dengan memberikan senarai pemanjangan fail yang dipisahkan oleh koma yang tidak seharusnya diimbas;
 - **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
 - Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah

lebih mencurigakan dan sepatutnya diimbis setiap masa.

- **Imbas keutamaan proses** - anda boleh menggunakan gelongsor untuk mengubah keutamaan proses imbasan. Secara lalai, keutamaan ditetapkan kepada tahap sederhana (*Imbasan automatik*) yang mengoptimumkan kelajuan proses pengimbasan dan penggunaan sumber sistem. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud muat sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama imbasan berlaku*), atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).
- **Tetapkan laporan imbasan tambahan** - pautan membuka dialog **Imbas laporan** di mana anda boleh memilih jenis kemungkinan penemuan yang harus dilaporkan:



Nota: Secara lalai, konfigurasi pengimbasan disediakan untuk prestasi optimum. Melainkan, anda mempunyai alasan yang sah untuk mengubah tetapan pengimbasan, ia sangat disyorkan untuk kekal dengan konfigurasi yang dipraktik. Sebarang perubahan konfigurasi sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Untuk opsyen pengimbasan selanjutnya, lihat dialog [tetapan Lanjutan](#) yang boleh diakses melalui item menu sistem **tetapan Fail / Lanjutan**.

Butang kawalan

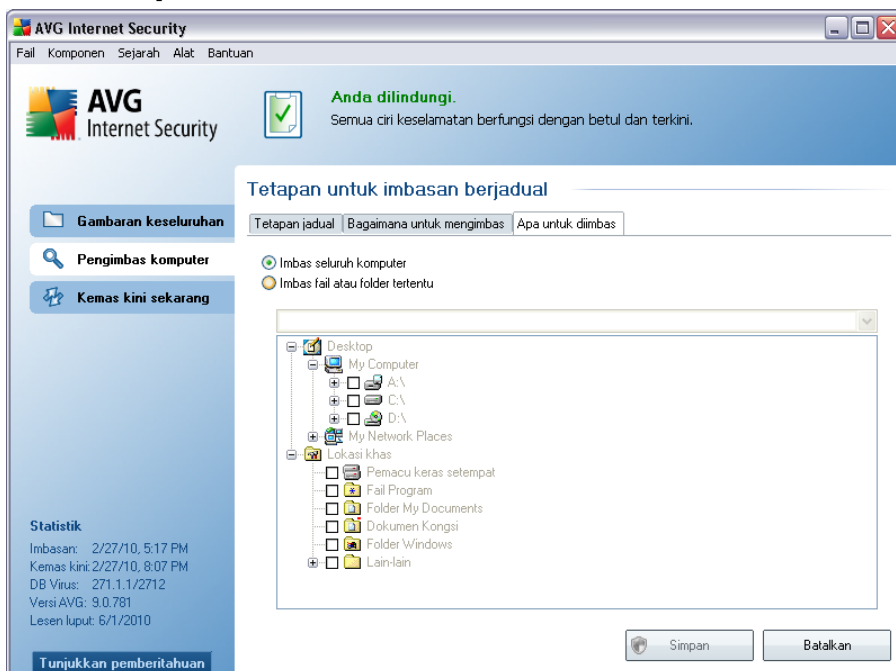
Ini adalah dua butang kawalan yang tersedia pada semua ketiga-tiga tab bagi dialog **Tetapan untuk imbasan berjadual** ([Tetapan jadual](#), **Cara untuk mengimbas** dan [Apa yang hendak diimbis](#)) dan ini mempunyai kefungsi yang sama tidak kira tab mana yang anda gunakan:

- **Simpan** - menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#). Oleh itu jika anda ingin mengkonfigurasi parameter ujian pada semua tab, tekan butang untuk menyimpan ia hanya

selepas anda telah menyatakan semua keperluan anda.

- **Batalan** - membatalkan sebarang perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#).

12.5.3. Apa untuk Diimbas



Pada tab ***Apa yang hendak diimbas*** anda boleh menentukan sama ada anda mahu menjadualkan [pengimbasan seluruh komputer](#) atau [pengimbasan fail atau folder tertentu](#).

Jika anda memilih pengimbasan bagi fail atau folder tertentu, di bahagian bawah dialog, struktur pepohon yang dipaparkan mengaktifkan dan anda boleh menentukan folder untuk diimbas (*perluaskan item dengan mengklik nod tambah sehingga anda menemui folder yang anda hendak imbas*). Anda boleh memilih berbilang folder dengan mengklik pada kotak berkaitan. Folder yang dipilih akan muncul dalam medan teks di bahagian atas dialog, dan menu jatuh bawah akan menyimpan sejarah imbasan terpilih anda untuk kegunaan nanti. Secara alternatif, anda boleh memasukkan laluan penuh ke folder yang diinginkan secara manual(*jika anda masukkan berbilang laluan, adalah perlu untuk memisahkannya dengan koma bertindih tanpa ruang tambahan*).

Dalam struktur pepohon, anda juga boleh melihat dahan yang dipanggil ***Lokasi khas***.



Berikut, cari senarai lokasi yang akan diimbas sebaik sahaja kotak semakan masing-masing ditanda:

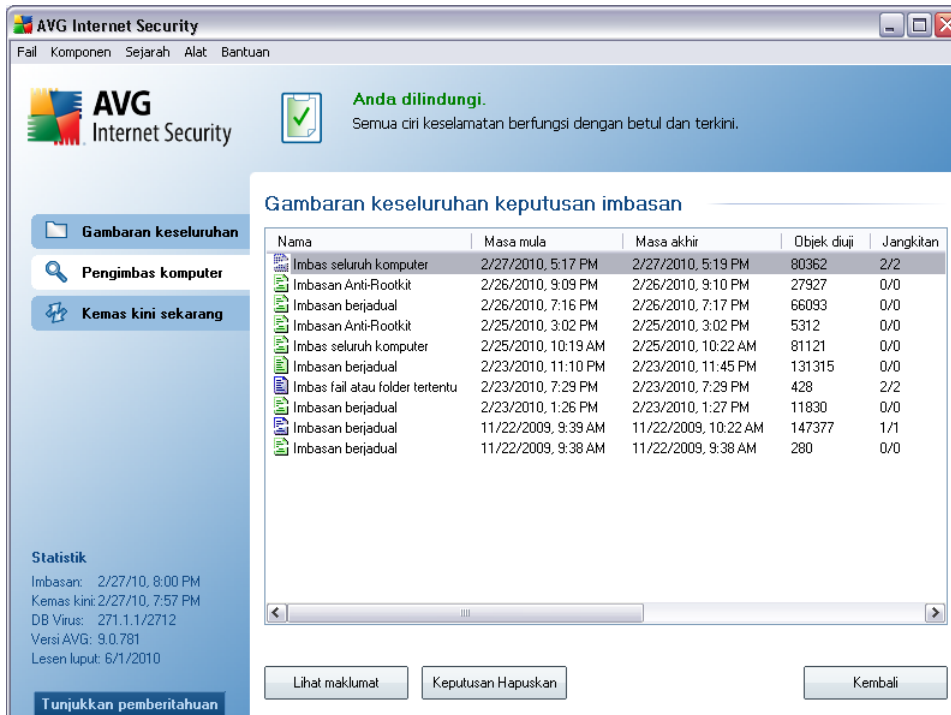
- **Pemacu keras tempatan** - semua pemacu keras bagi komputer anda
- **Fail program** - C:\Program Files\
- **Folder My Documents** - C:\Documents and Settings\User\My Documents\
- **Shared Documents** - C:\Documents and Settings\All Users\Documents\
- **Folder Windows** - C:\Windows\
- **Lain-lain**
 - o *Pemacu sistem* - pemacu keras di mana sistem pengendalian dipasang (biasanya C:)
 - o *Folder sistem* - Windows/System32
 - o *Folder Fail Sementara* - Documents and Settings/User/Local Settings/Temp
 - o *Fail Internet Sementara* - Documents dan Settings/User/Local Settings/Temporary Internet Files

Butang kawalan Tetapan untuk dialog imbasan berjadual

Terdapat dua butang kawalan yang tersedia pada semua ketiga-tiga tab dialog **Tetapan untuk imbasan yang dijadualkan** ([Jadualkan tetapan](#), [Cara untuk mengimbas](#) dan [Apa yang hendak diimbas](#)) dan ini mempunyai kefungsiian yang sama tidak kira pada tab mana yang anda sedang berada:

- **Simpan** - menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#). Oleh itu jika anda ingin mengkonfigurasi parameter ujian pada semua tab, tekan butang untuk menyimpan ia hanya selepas anda telah menyatakan semua keperluan anda.
- **Batal** - membatalkan sebarang perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#).

12.6. Gambaran Keseluruhan Keputusan Imbasan



Dialog **Imbas gambaran keseluruhan keputusan** boleh diakses dari [antara muka pengimbasan AVG](#) melalui butang **Imbas sejarah**. Dialog memberikan senarai semua imbasan yang dilancarkan sebelum ini dan maklumat keputusannya:

- **Nama** - imbas pelantikan; ia boleh jadi sama ada nama salah satu [imbasan yang dipratetap](#) atau nama yang anda telah berikan kepada [imbasan anda yang dijadualkan sendiri](#). Setiap nama termasuk ikon yang menunjukkan keputusan imbasan:

 - ikon hijau memberitahu tiada jangkitan yang dikesan sewaktu imbasan

 - ikon biru mengumumkan terdapat jangkitan dikesan sewaktu imbasan tetapi objek yang dikesan dibuang secara automatik

 - ikon merah memberi amaran terdapat jangkitan dikesan sewaktu imbasan dan ia tidak boleh dibuang!

Setiap ikon boleh menjadi sama ada tegar atau dipotong separuh - ikon

tegar adalah untuk imbasan yang telah selesai dan yang diselesaikan dengan betul; ikon yang dipotong separuh bermaksud imbasan telah dibatalkan atau diganggu.

Nota: Untuk maklumat terperinci mengenai setiap imbasan, sila lihat dialog [Keputusan Imbasan](#) yang boleh diakses melalui butang **Lihat butiran** (di bahagian bawah dialog ini).

- **Masa mula** - tarikh dan masa semasa imbasan dilancarkan
- **Masa tamat** - tarikh dan masa imbasan ditamatkan
- **Objek yang diuji** - bilangan objek yang diperiksa sewaktu imbasan
- **Jangkitan** - bilangan [jangkitan virus](#) yang dikesan / dibuang
- **Perisian pengintip** - bilangan [perisian pengintip](#) yang dikesan / dibuang
- **Amaran** - bilangan [objek mencurigakan](#)
- **Rootkit** - bilangan [rootkit](#)
 - **Imbas maklumat log** - maklumat berkaitan dengan tempoh imbasan dan keputusan (biasanya pada penyelesaian atau gangguan)

Butang kawalan

Butang kawalan untuk dialog **Imbas gambaran keseluruhan hasil** adalah:

- **Lihat butiran** - tekannya untuk beralih ke dialog [Imbas keputusan](#) untuk melihat data terperinci bagi imbasan yang dipilih
- **Padam keputusan** - tekannya untuk membuang item yang dipilih daripada gambaran keseluruhan keputusan imbasan
- **Kembali** - mengalihkan semula ke dialog lalai bagi [antara muka imbasan AVG](#)

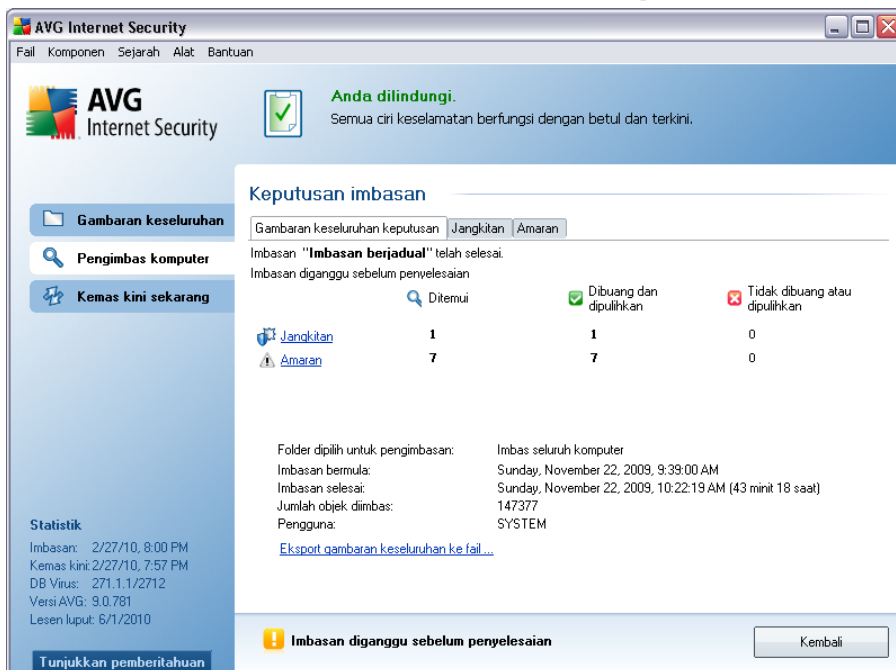
12.7. Keputusan Imbasan Butiran

Jika dalam dialog [Imbas Gambaran Keseluruhan Keputusan](#) imbasan tertentu dipilih, kemudian, anda boleh mengklik butang **Lihat butiran** untuk beralih ke dialog **Imbas Keputusan** yang memberikan data terperinci mengenai tempoh dan keputusan imbasan yang dipilih.

Dialog tersebut seterusnya dibahagikan ke dalam beberapa tab:

- **Gambaran Keseluruhan Keputusan** - tab ini dipaparkan pada setiap masa dan memberikan data statistik yang menerangkan perkembangan imbasan
- **Jangkitan** - tab ini dipaparkan hanya jika jangkitan virus dikesan sewaktu pengimbasan
- **Perisian pengintip** - tab ini dipaparkan hanya jika perisian pengintip dikesan sewaktu pengimbasan
- **Amaran** - tab ini dipaparkan sebagai contoh jika kuki dikesan sewaktu pengimbasan
- **Rootkit** - tab ini dipaparkan hanya jika rootkit dikesan sewaktu pengimbasan
- **Maklumat** - tab ini dipaparkan hanya jika beberapa kemungkinan ancaman dikesan tetapi ini tidak boleh diklasifikasikan sebagai mana-mana kategori di atas; kemudian, tab tersebut memberikan mesej amaran mengenai penemuan. Serta, anda akan menemui di sini maklumat mengenai objek yang tidak boleh diimbas (cth. arkib yang dilindungi kata laluan).

12.7.1. Tab Gambaran Keseluruhan Keputusan



Pada tab **Imbas keputusan** anda boleh mendapatkan statistik terperinci dengan maklumat pada:

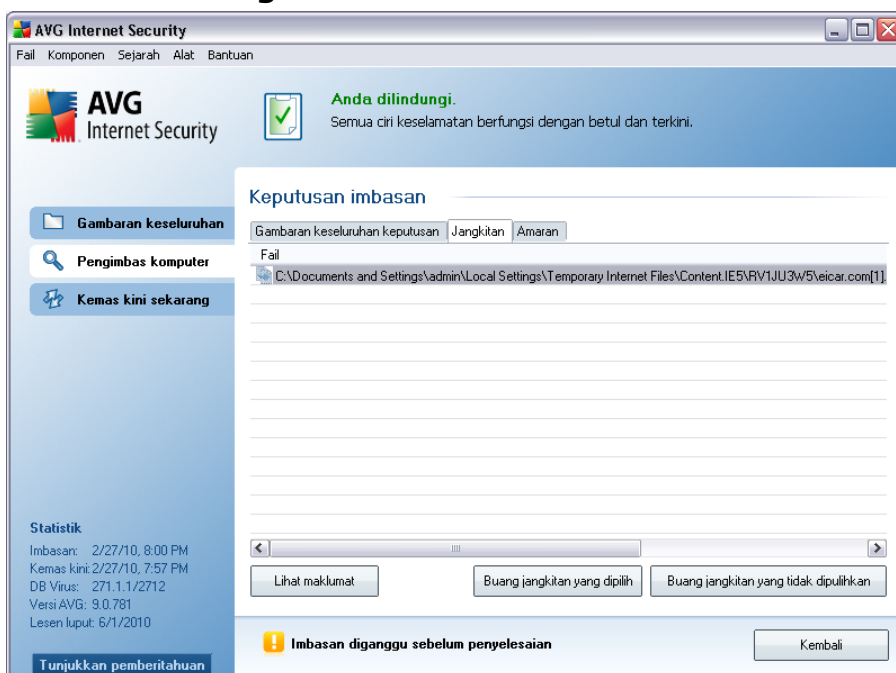
- [jangkitan virus](#) / [perisian pengintip yang dikesan](#)
- [jangkitan virus](#) / [perisian pengintip yang dibuang](#)
- bilangan [jangkitan virus](#) / [perisian pengintip](#) yang tidak boleh dibuang atau dipulihkan

Selain daripada itu, anda akan mendapat maklumat mengenai tarikh dan masa sebenar pelancaran imbasan, dengan jumlah bilangan objek yang diimbas, pada tempoh pengimbasan dan bilangan ralat yang berlaku sewaktu pengimbasan

Butang kawalan

Terdapat hanya satu butang kawalan yang tersedia dalam dialog ini. Butang **Tutup keputusan** kembali ke dialog [Imbas gambaran keseluruhan](#).

12.7.2. Tab Jangkitan



Tab **Jangkitan** hanya dipaparkan dalam dialog **Imbas keputusan** jika [jangkitan virus](#)

dikesan sewaktu pengimbasan. Tab ini dibahagikan kepada tiga bahagian menyediakan maklumat berikut:

- **Fail** - laluan penuh ke lokasi asal bagi objek yang dijangkiti
- **Jangkitan** - nama bagi [virus](#) yang dikesan (*untuk butiran mengenai virus khusus, sila rujuk kepada [Ensiklopedia Virus](#) dalam talian*)
- **Keputusan** - mentakrifkan status terkini bagi objek yang dijangkiti yang dikesan sewaktu imbasan:
 - o yang dijangkiti- objek yang dijangkiti dikesan dan ditinggalkan dalam lokasi asalnya (*contohnya, jika anda telah [mematikan opsyen pemulihan automatik](#) dalam tetapan imbasan khusus*)
 - o yang dipulihkan- objek yang dikesan dipulihkan secara automatik dan ditinggalkan dalam lokasi asalnya
 - o **Dialih ke Bilik Kebal Virus** - objek yang dijangkiti dialihkan ke kuarantin [Bilik Kebal Virus](#)
 - o yang dipadamkan- objek yang dijangkiti dipadamkan
 - o **Ditambah ke pengecualian PUP** - penemuan dinilai sebagai pengecualian dan ditambah kepada senarai pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian PUP](#) bagi tetapan lanjutan*)
 - o **Fail dikunci - tidak diuji** - objek tersebut dikunci dan oleh itu, AVG tidak dapat mengimbasnya
 - o **Berkemungkinan, objek berbahaya** - objek dikesan sebagai berkemungkinan berbahaya tetapi tidak dijangkiti(*sebagai contoh, ia boleh mengandungi*); maklumat harus diambil sebagai amaran sahaja
 - o **But semula diperlukan untuk menyelesaikan tindakan** - objek yang dijangkiti tidak boleh dibuang, untuk membuang sepenuhnya, anda perlu memulakan semula komputer anda

Butang kawalan

Terdapat tiga butang kawalan yang anda dalam dialog ini:

- **Lihat butiran** - butang tersebut membuka tettingkap dialog baru yang

dinamakan **Maklumat keputusan imbasan yang diimbis secara terperinci**:



Dalam dialog ini, anda boleh mendapatkan maklumat pada lokasi objek jangkitan yang dikesan (**Nama sifat**). Menggunakan butang **Sebelumnya / Seterusnya** anda boleh melihat maklumat pada penemuan tertentu. Gunakan butang **Tutup** untuk menutup dialog ini.

- **Buang jangkitan yang dipilih** - gunakan butang untuk mengalih penemuan yang dipilih ke [Bilik Kebal Virus](#)
- **Buang semua jangkitan yang tidak dapat dipulihkan** - butang ini memadam semua penemuan yang tidak dapat dipulihkan atau dialihkan ke [Bilik Kebal Virus](#)
- **Tutup keputusan** - tamatkan gambaran keseluruhan maklumat terperinci dan kembali ke dialog [Imbas gambaran keseluruhan keputusan](#)

12.7.3. Tab Perisian Pengintip

Tab **Perisian Pengintip** hanya dipaparkan dalam dialog **Imbas keputusan** dalam [perisian pengintip jika](#) dikesan sewaktu imbasan. Tab ini dibahagikan kepada tiga bahagian menyediakan maklumat berikut:

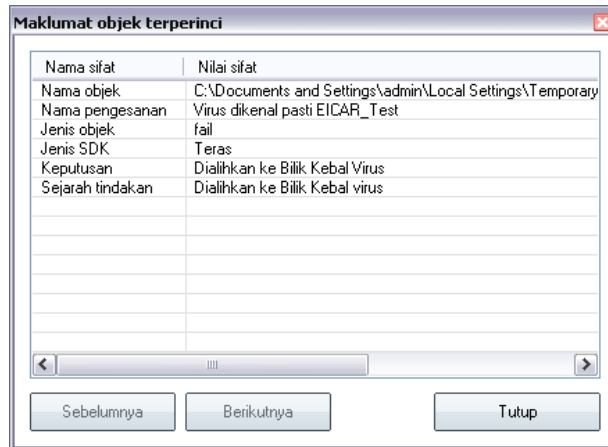
- **Fail** - laluan penuh ke lokasi asal bagi objek yang dijangkiti
- **Jangkitan** - nama yang dikesan [perisian pengintip](#) (untuk butiran mengenai virus tertentu, sila rujuk [Ensiklopedia Virus](#) dalam talian)
- **Keputusan** - mentakrif status objek semasa yang dikesan sewaktu imbasan:

- o dijangkiti - objek yang dijangkiti dikesan dan dibiarkan dalam lokasi asalnya (contohnya, jika anda telah [mematikan opsyen pemulihan automatik](#) dalam tetapan imbasan khusus)
- o yang dipulihkan- objek yang dikesan dipulihkan secara automatik dan ditinggalkan dalam lokasi asalnya
- o ***Dialih ke Bilik Kebal Virus*** - objek yang dijangkiti dialihkan ke kuarantin [Bilik Kebal Virus](#)
- o yang dipadamkan- objek yang dijangkiti dipadamkan
- o ***Ditambah pada pengecualian PUP*** - penemuan dinilai sebagai pengecualian dan ditambah pada senarai pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian PUP](#) bagi tetapan lanjutan*)
- o ***Fail yang dikunci - tidak diuji*** - objek masing-masing dikunci dan oleh sebab itu, AVG tidak dapat mengimbasnya
- o ***Objek berpotensi berbahaya*** - objek dikesan sebagai berpotensi berbahaya tetapi tidak dijangkiti (sebagai contoh, ia boleh mengandungi makro); maklumat adalah hanya amaran
- o ***But semula diperlukan untuk menyelesaikan tindakan*** - objek yang dijangkiti tidak boleh dibuang, untuk membuang sepenuhnya, anda perlu memulakan semula komputer anda

Butang kawalan

Terdapat tiga butang kawalan yang anda dalam dialog ini:

- ***Lihat butiran***- butang tersebut membuka tettingkap dialog baru yang dinamakan ***Maklumat keputusan imbasan yang diimbis secara terperinci***:

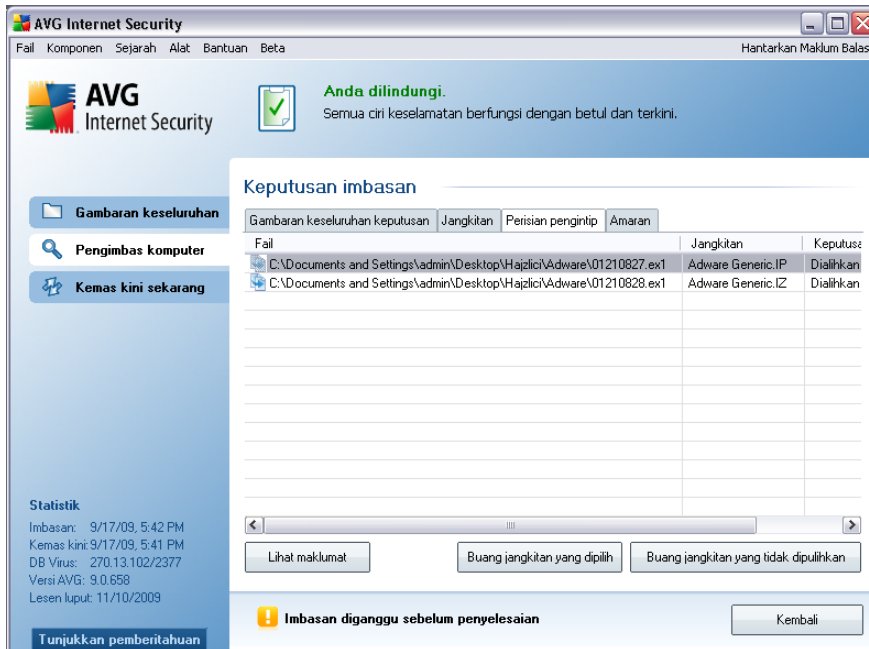


Dalam dialog ini, anda boleh mendapatkan maklumat pada lokasi objek jangkitan yang dikesan (**Nama sifat**). Menggunakan butang **Sebelumnya** / **Seterusnya** anda boleh melihat maklumat pada penemuan tertentu. Gunakan butang **Tutup** untuk meninggalkan dialog ini.

- **Buang jangkitan yang dipilih** - gunakan butang untuk mengalih penemuan yang dipilih ke [Bilik Kebal Virus](#)
- **Buang semua jangkitan yang tidak dapat dipulihkan** - butang ini memadam semua penemuan yang tidak dapat dipulihkan atau dialihkan ke [Bilik Kebal Virus](#)
- **Tutup keputusan** - tamatkan gambaran keseluruhan maklumat terperinci dan kembali ke dialog [Imbas gambaran keseluruhan keputusan](#)

12.7.4. Tab Amaran

Tab **Amaran** memaparkan maklumat pada objek yang "disyaki" (*biasanya fail*) yang dikesan sewaktu pengimbasan. Apabila dikesan oleh [Perisai Residen](#), fail ini disekat daripada diakses. Contoh biasa bagi jenis penemuan ini adalah: fail tersembunyi, kuki, kekunci pendaftaran yang disyaki, dokumen atau arkib yang dilindungi kata laluan, dll. Fail seperti itu tidak membawa sebarang ancaman terus kepada komputer atau keselamatan anda. Maklumat mengenai fail ini biasanya berguna jika terdapat adware atau perisian pengintip yang dikesan pada komputer anda. Jika hanya terdapat Amaran yang dikesan oleh ujian AVG, tiada tindakan yang diperlukan.



Ini adalah penerangan ringkas bagi contoh yang paling biasa bagi objek seperti itu:

- **Fail tersembunyi** - Fail tersembunyi adalah secara lalai tidak boleh dilihat dalam Windows, dan sesetengah virus atau ancaman lain mungkin cuba mengelakkan pengesananannya dengan menyimpan failnya dengan atribut ini. Jika AVG anda melaporkan fail tersembunyi yang anda mengesyaki berniat jahat, anda boleh mengalihkannya ke [Bilik Kebal Virus](#) anda.
- **Kuki** - Kuki adalah fail teks biasa yang digunakan oleh tapak web untuk menyimpan maklumat khusus pengguna yang kemudiannya digunakan untuk memuat reka letak tapak web, prapengisian nama pengguna, dll.
- **Kekunci pendaftaran yang disyaki** - Sesetengah malware menyimpan maklumatnya ke dalam pendaftaran Windows, untuk memastikan ia dimuat pada permulaan atau untuk meluaskan kesannya pada sistem pengendalian.

12.7.5. Tab Rootkit

Tab **Rootkits** memaparkan maklumat mengenai rootkit yang dikesan sewaktu pengimbasan jika anda telah melancarkan [imbasan AntiRootkit](#), atau secara manual, telah menambah pilihan bagi pengimbasan antirootkit ke dalam [Imbas Seluruh Komputer](#) (pilihan ini dimatikan secara lalai).

Rootkit adalah atur cara yang direka bentuk untuk melakukan kawalan asas sistem

komputer tanpa kebenaran daripada pemilik sistem dan pengurus yang sah. Akses kepada perkakasan jarang diperlukan kerana rootkit bertujuan untuk menyita kawalan sistem pengendalian yang sedang dijalankan pada perkakasan. Biasanya, rootkit bertindak untuk mengaburi kehadirannya pada sistem melalui subversi atau pengelakan daripada mekanisme keselamatan sistem pengendalian. Biasanya, ia juga adalah Trojan, dengan itu, menipu pengguna dengan mempercayai bahawa ia selamat untuk dijalankan pada sistemnya. Teknik yang digunakan untuk melaksanakan ini termasuk menyembunyikan proses yang sedang dijalankan daripada menyelia atur cara atau menyembunyikan fail atau data sistem daripada sistem pengendalian.

Secara asasnya, struktur tab ini adalah sama seperti [tab Jangkitan](#) atau [tab Perisian Pengintip](#).

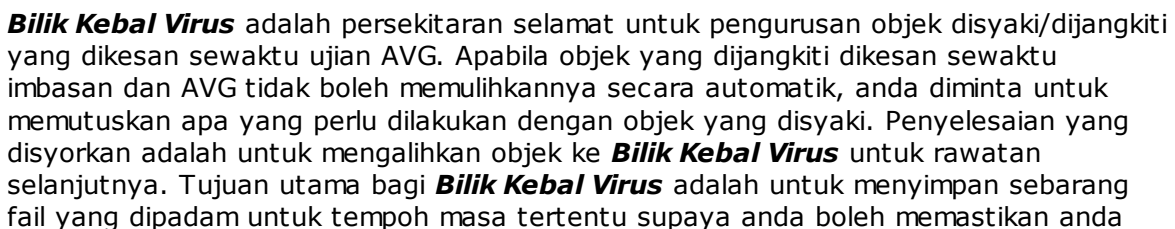
12.7.6. Tab Maklumat

Tab **Maklumat** yang mengandungi data mengenai "penemuan" seperti itu yang tidak boleh dikategorikan sebagai jangkitan, perisian pengintip, dll. Ia boleh sama ada dilabel secara positif sebagai berbahaya tetapi ia masih berbaloi untuk perhatian anda. Imbasan AVG boleh mengesan fail yang mungkin tidak dijangkiti tetapi disyaki. Fail ini dilaporkan sama ada sebagai [Amaran](#) atau sebagai **Maklumat**.

Keseriusan **Maklumat** boleh dilaporkan untuk salah satu sebab berikut:

- **Masa jalan dipek** - Fail dipek dengan salah satu pembungkus masa jalan yang kurang biasa, yang mungkin menunjukkan cubaan untuk mengelakkan pengimbasan fail seperti itu. Walau bagaimanapun, bukan setiap laporan bagi fail seperti itu menunjukkan virus.
- **Rekursif jalan masa yang dipek** - Sama dengan yang di atas, walau bagaimanapun, kurang kerap di kalangan perisian biasa. Fail seperti itu adalah mencurigakan dan pembuangannya atau penghantarannya untuk analisis harus dipertimbangkan.
- **Arkib atau dokumen yang dilindungi kata laluan** - Fail yang dilindungi kata laluan tidak boleh diimbis oleh AVG (*atau biasanya sebarang atur cara antimalware lain*).
- **Dokumen dengan makro** - Dokumen yang dilaporkan mengandungi makro yang mungkin berniat jahat.
- **Sambungan tersembunyi** - Fail dengan sambungan tersembunyi mungkin muncul menjadi cth. gambar, tetapi sebenarnya, ia adalah fail boleh laku (*cth. picture.jpg.exe*). Sambungan kedua tidak boleh dilihat dalam Windows secara lalai dan AVG melaporkan fail seperti itu untuk mengelakkan pembukaannya secara tidak sengaja.

- ## 12.8. Bilik Kebal Virus



tidak memerlukan fail lagi dalam lokasi asalnya. Jika anda mendapati ketiadaan fail menyebabkan masalah, anda boleh menghantarkan fail yang dipersoalkan untuk analisis, atau menyimpannya semula ke lokasi asal.

Antara muka **Bilik kebal virus** terbuka dalam tettingkap berasingan dan menawarkan gambaran keseluruhan maklumat mengenai objek dijangkiti yang dikuarantin:

- **Keterangan** - jika anda memutuskan untuk memasang komponen [Perlindungan Identiti](#) dalam **AVG 9 Internet Security**, pengenalpastian grafik bagi keterangan penemuan masing-masing pada skala empat tahap daripada yang tidak boleh dibantah (■□□□) sehingga kepada sangat berbahaya (■□■□) akan diberikan dalam bahagian ini; dan maklumat mengenai jenis jangkitan (*berdasarkan pada tahap jangkitannya - semua objek yang disenaraikan boleh menjadi secara positif atau berkemungkinan dijangkiti*)
- **Nama Virus** - menentukan nama jangkitan yang dikesan menurut [Ensiklopedia virus](#) (dalam talian)
- **Laluan ke fail** - laluan penuh ke lokasi asal bagi fail yang boleh dijangkiti dikesan
- **Nama objek asal** - semua objek yang dikesan yang disenaraikan dalam carta telah dilabel dengan nama standard yang diberikan oleh AVG sewaktu proses imbasan. Jika objek mempunyai nama asal khusus yang diketahui (*cth. nama lampiran e-mel yang tidak memberi respons kepada kandungan sebenar lampiran*), ia akan diberikan dalam kolum ini.
- **Tarikh simpanan** - tarikh dan masa fail yang dijangkiti dikesan dan dibuang ke **Bilik Kebal Virus**

Butang kawalan

Butang berikut boleh diakses dari antara muka **Bilik Kebal Virus**:

- **Simpan semula** - membuang fail yang dijangkiti kembali ke lokasi asalnya pada cakera anda
- **Simpan Semula Sebagai** - jika anda memutuskan untuk mengalihkan objek boleh dijangkiti yang dikesan dari **Bilik Kebal Virus** ke folder yang dipilih, gunakan butang ini Objek yang disyaki dan dikesan akan disimpan dengan nama asalnya. Jika nama asal tidak diketahui, nama standard akan digunakan.
- **Butiran** - butang ini hanya digunakan pada ancaman yang dikesan oleh

Perlindungan Identiti. Dengan mengklik, ia memaparkan gambaran keseluruhan sinopsis gambaran keseluruhan bagi butiran ancaman (*apakah fail/proses yang telah dijangkiti, ciri-ciri proses dll.*). Sila maklum bahawa untuk semua item lain selain yang dikesan oleh IDP, butang ini berwarna kelabu dan tidak aktif!

- **Padam** - membuang fail yang dijangkiti daripada **Bilik Kebal Virus** sepenuhnya dan tidak boleh diundur
- **Kosongkan Bilik Kebal** - membuang semua **kandungan** Bilik Kebal Virus sepenuhnya. Dengan membuang fail daripada Bilik Kebal Virus, fail-fail ini tidak boleh diundur daripada dibuang daripada cakera (tidak dialihkan ke Tong Kitar Semula).

13. Kemas kini AVG

Memastikan AVG anda terkini adalah penting untuk memastikan semua virus yang baru ditemui akan dikesan secepat mungkin.

Sewaktu [Proses Pemasangan AVG](#) anda dijemput untuk menentukan berapa kerap anda hendak mengemas kini AVG anda. Pilihan yang tersedia adalah **Setiap 4 jam**, atau **Setiap hari** (lihat dialog [Jadualkan imbasan dan kemas kini tetap](#)). Memandangkan kemas kini AVG tidak dikeluarkan mengikut sebarang jadual tetap tetapi sebaliknya dalam reaksi kepada jumlah dan keseriusan ancaman baru, ia disyorkan untuk menyemak kemas kini baru sekurang-kurangnya sekali sehari. Memeriksa setiap 4 jam akan menjamin bahawa **AVG 9 Internet Security** anda juga terkini sewaktu siang.

13.1. Tahap Kemas kini

AVG menawarkan dua tahap kemas kini untuk dipilih dari:

- **Kemas kini definisi** mengandungi perubahan yang diperlukan untuk perlindungan antivirus, Antispam dan antimalware yang boleh dipercayai. Biasanya, ia tidak termasuk sebarang perubahan kepada kod dan mengemas kini hanya pangkalan data definisi. Kemas kini ini harus digunakan sebaik sahaja ia tersedia.
- **Kemas kini atur cara** mengandungi pelbagai perubahan atur cara, pembaikan dan peningkatan.

Apabila [menjadualkan kemas kini](#), anda boleh memilih tahap keutamaan mana yang patut dimuat turun dan digunakan.

Perhatian: Jika persamaan masa bagi kemas kini atur cara yang dijadualkan dan imbasan yang dijadualkan berlaku, proses kemas kini adalah lebih utama dan imbasan akan diganggu.

13.2. Jenis Kemas Kini

Anda boleh membezakan antara dua jenis kemas kini:

- **Kemas kini dalam permintaan** adalah kemas kini AVG segera yang boleh dilakukan pada bila-bila masa jika perlu.
- **Kemas kini yang dijadualkan** - dalam AVG, anda boleh [mempratetapkan rancangan kemas kini](#). Kemudian, kemas kini yang dirancang dilakukan secara berkala mengikut konfigurasi persediaan. Apabila fail kemas kini baru terdapat pada lokasi tertentu, ia dimuat turun sama ada secara terus dari Internet atau dari direktori rangkaian. Apabila tiada kemas kini lebih baru yang tersedia, tiada

apa yang berlaku.

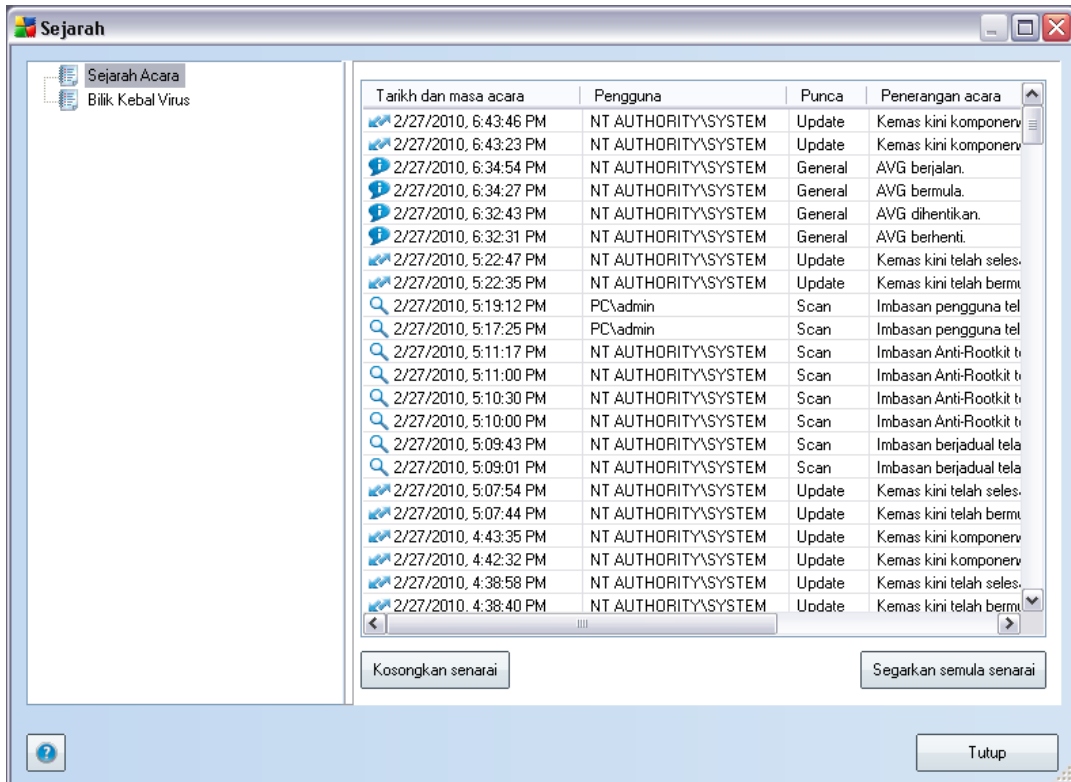
13.3. Kemas Kini Proses

Proses kemas kini boleh dilancarkan dengan serta-merta apabila perlu menggunakan pautan pantas **Kemas kini sekarang*****. Pautan ini tersedia pada setiap masa dari sebarang dialog [antara muka pengguna AVG](#). Walau bagaimanapun, adalah masih amat disyorkan untuk melakukan kemas kini secara tetap seperti yang dinyatakan dalam jadual kemas kini boleh diedit dalam komponen [Pengurus kemas kini](#).

Apabila anda memulakan kemas kini, pertama sekali, AVG akan mengenal pasti sama ada terdapat fail kemas kini baru yang tersedia. Jika ada, AVG memulakan muat turun dan melancarkan proses kemas kini dengan sendiri. Sewaktu proses kemas kini, anda akan diarahkan semula ke antara muka **Kemas kini** di mana anda boleh melihat perkembangan proses dalam persembahan grafiknya serta seperti dalam gambaran keseluruhan parameter statistik yang relevan (*kemas kini saiz fail, data yang diterima, kelajuan muat turun, masa berlalu, ...*).

Nota: Sebelum kemas kini atur cara AVG melancarkan titik pemulihan sistem dibuat. Jika proses kemas kini gagal dan sistem pengendalian anda hancur, anda sentiasa boleh memulihkan OS anda dalam konfigurasi asal dari titik ini. Pilihan boleh diakses melalui Start / All Programs / Accessories / System tools / System Restore. Disyorkan kepada pengguna berpengalaman sahaja!

14. Sejarah Acara



Dialog **Sejarah Acara** boleh diakses dari [menu sistem](#) melalui item **Sejarah/Log Sejarah Acara**. Dalam dialog ini, anda boleh menemui ringkasan peristiwa penting yang berlaku sewaktu operasi **AVG 9 Internet Security**. **Sejarah Acara** merekodkan jenis acara berikut:

- Maklumat mengenai kemas kini aplikasi AVG
- Imbasan, bermula, tamat atau berhenti (termasuk ujian yang dilakukan secara automatik)
- Acara yang bersambung dengan pengesanan virus (oleh [Perisai Residen](#) atau [imbasan](#)) termasuk lokasi ulangan
- Acara penting lain

Butang kawalan



- **Kosongkan senarai** - memadam semua entri dalam senarai acara
- **Muat semula senarai** - memadam semua entri dalam senarai acara



15. Soalan Lazim dan Sokongan Teknikal

Jika anda mempunyai sebarang masalah dengan AVG anda, sama ada perniagaan atau teknikal, sila rujuk kepada bahagian [Soalan Lazim](http://www.avg.com/) bagi tapak web AVG (<http://www.avg.com/>).

Jika anda tidak berjaya dengan mendapatkan bantuan begini, hubungi jabatan sokongan teknikal melalui e-mel. Sila gunakan borang hubungan yang boleh diakses daripada menu sistem melalui **Bantuan / Dapatkan bantuan dalam talian**.