

AVG 9 Anti-Virus plus Firewall

Manual Pengguna

Semakan dokumen 90.6 (14.9.2009)

Hak cipta AVG Technologies CZ, s.r.o. Hak cipta 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	7
2. Keperluan Pemasangan AVG	8
2.1 Sistem Pengendalian yang Disokong	8
2.2 Keperluan Perkakasan Minimum	8
3. Opsyen Pemasangan AVG	9
4. AVG Download Manager	10
4.1 Pemilihan Bahasa	10
4.2 Semakan Kesambungan	11
4.3 Tetapan Proksi	12
4.4 Pilih Jenis Lesen	13
4.5 Muat Turun Fail Untuk Dipasang	14
5. Proses Pemasangan AVG	15
5.1 Lancarkan Pemasangan	15
5.2 Perjanjian Lesen	16
5.3 Memeriksa Status Sistem	16
5.4 Pilih Jenis Pemasangan	17
5.5 Aktifkan Lesen AVG anda	17
5.6 Pemasangan Tersuai - Folder destinasi	19
5.7 Pemasangan Tersuai - Pemilihan Komponen	20
5.8 PusatData AVG	21
5.9 AVG Security Toolbar	22
5.10 Memasang AVG	23
5.11 Jadualkan imbasan dan kemas kini yang tetap	24
5.12 Pemilihan penggunaan komputer	24
5.13 Rekaan rangkaian komputer anda	25
5.14 Konfigurasi perlindungan AVF lengkap	26
6. Selepas Pemasangan	27
6.1 Pendaftaran Produk	27
6.2 Akses ke Antara Muka Pengguna	27
6.3 Mengimbas seluruh komputer	27
6.4 Ujian Eicar	27

6.5 Konfigurasi Lalai AVG	28
7. Antara Muka Pengguna AVG	29
7.1 Menu Sistem	30
7.1.1 Fail	30
7.1.2 Komponen	30
7.1.3 Sejarah	30
7.1.4 Alat	30
7.1.5 Bantuan	30
7.2 Maklumat Status Keselamatan	33
7.3 Pautan Pantas	34
7.4 Gambaran keseluruhan Komponen	35
7.5 Statistik	36
7.6 Ikon Dulang Sistem	36
8. Komponen AVG	38
8.1 AntiVirus	38
8.1.1 Prinsip AntiVirus	38
8.1.2 Antara Muka AntiVirus	38
8.2 AntiPerisian Pengintip	40
8.2.1 Prinsip AntiPerisian Pengintip	40
8.2.2 Antara Muka AntiPerisian Pengintip	40
8.3 Firewall	42
8.3.1 Prinsip Firewall	42
8.3.2 Profil Firewall	42
8.3.3 Antara Muka Firewall	42
8.4 Pengimbas E-mel	47
8.4.1 Prinsip Pengimbas E-mel	47
8.4.2 Antara Muka Pengimbas E-mel	47
8.4.3 Pengesanan Pengimbas E-mel	47
8.5 Lesen	51
8.6 Pengimbas Pautan	52
8.6.1 Prinsip Pengimbas Pautan	52
8.6.2 Antara Muka Pengimbas Pautan	52
8.6.3 AVG Search-Shield	52
8.6.4 AVG Active Surf-Shield	52
8.7 Perisai Web	56
8.7.1 Prinsip Perisai Web	56

8.7.2 Antara Muka Perisai Web	56
8.7.3 Pengesanan Perisai Web	56
8.8 Perisai Residen	61
8.8.1 Perisai Residen Prinsip	61
8.8.2 Antara Muka Perisai Residen	61
8.8.3 Pengesanan Perisai Residen	61
8.9 Pengurus Kemas Kini	66
8.9.1 Kemas Kini Prinsip Pengurus	66
8.9.2 Kemas Kini Antara Muka Pengurus	66
8.10 AVG Security Toolbar	69
8.10.1 AVG Security Toolbar Antara muka	69
8.10.2 Opsyen AVG Security Toolbar	69
9. Tetap Lanjutan AVG	76
9.1 Penampilan	76
9.2 Bunyi	78
9.3 Abaikan Keadaan Rosak	80
9.4 Bilik Kebal Virus	81
9.5 Kekecualian PUP	82
9.6 Perisai Web	85
9.6.1 Perlindungan Web	85
9.6.2 Pemesejan Segera	85
9.7 Pengimbas Pautan	89
9.8 Imbasan	90
9.8.1 Imbas Seluruh Komputer	90
9.8.2 Imbasan Sambungan Kerangka	90
9.8.3 Imbas Fail atau Folder Tertentu	90
9.8.4 Imbasan Peranti Boleh Dialih	90
9.9 Jadual	97
9.9.1 Imbasan yang Dijadualkan	97
9.9.2 Jadual Kemas Kini Pangkalan Data Virus	97
9.9.3 Jadual Kemas Kini Atur Cara	97
9.10 Pengimbas E-mel	108
9.10.1 Perakuan	108
9.10.2 Penapisan Mel	108
9.10.3 Log dan Keputusan	108
9.10.4 Pelayan	108
9.11 Perisai Residen	116

9.11.1	<i>Tetapan Lanjutan</i>	116
9.11.2	<i>Direktori Tidak Termasuk</i>	116
9.11.3	<i>Fail yang Dikecualikan</i>	116
9.12	<i>Kemas kini</i>	122
9.12.1	<i>Proksi</i>	122
9.12.2	<i>Dailan</i>	122
9.12.3	<i>URL</i>	122
9.12.4	<i>Uruskan</i>	122
10.	Tetapan Firewall	129
10.1	<i>Umum</i>	129
10.2	<i>Keselamatan</i>	130
10.3	<i>Profil Kawasan dan Penyesuai</i>	131
10.4	<i>Log</i>	132
10.5	<i>Profil</i>	134
10.5.1	<i>Maklumat Profil</i>	134
10.5.2	<i>Rangkaian yang Ditentukan</i>	134
10.5.3	<i>Aplikasi</i>	134
10.5.4	<i>Perkhidmatan Sistem</i>	134
11.	Pengimbasan AVG	146
11.1	<i>Antara Muka Pengimbasan</i>	146
11.2	<i>Imbasan Pratakrif</i>	147
11.2.1	<i>Imbas Seluruh Komputer</i>	147
11.2.2	<i>Imbas Fail atau Folder Tertentu</i>	147
11.3	<i>Pengimbasan dalam Windows Explorer</i>	155
11.4	<i>Pengimbasan Garis Perintah</i>	156
11.4.1	<i>Parameter Imbasan CMD</i>	156
11.5	<i>Penjadualan Imbasan</i>	159
11.5.1	<i>Tetapan Jadual</i>	159
11.5.2	<i>Bagaimana untuk Mengimbas</i>	159
11.5.3	<i>Apa untuk Diimbas</i>	159
11.6	<i>Gambaran Keseluruhan Keputusan Imbasan</i>	169
11.7	<i>Keputusan Imbasan Butiran</i>	170
11.7.1	<i>Tab Gambaran Keseluruhan Keputusan</i>	170
11.7.2	<i>Tab Jangkitan</i>	170
11.7.3	<i>Tab Perisian Pengintip</i>	170
11.7.4	<i>Tab Amaran</i>	170

11.7.5 Tab Maklumat	170
11.8 Bilik Kebal Virus	179
12. Kemas kini AVG	181
12.1 Tahap Kemas kini	181
12.2 Jenis Kemas Kini	181
12.3 Kemas Kini Proses	181
13. Sejarah Acara	183
14. Soalan Lazim dan Sokongan Teknikal	185

1. Pengenalan

Manual pengguna ini membekalkan dokumentasi menyeluruh untuk **AVG 9 Anti-Virus plus Firewall**.

Tahniah di atas pembelian anda untuk AVG 9 Anti-Virus plus Firewall!

AVG 9 Anti-Virus plus Firewall adalah salah satu rangkaian produk AVG yang memenangi anugerah yang direka bentuk untuk memberikan anda ketenangan minda dan keselamatan menyeluruh untuk PC anda. Seperti semua produk AVG **AVG 9 Anti-Virus plus Firewall** telah direka bentuk semula sepenuhnya dari asas, untuk memberikan perlindungan keselamatan AVG ' yang terkenal dan diperakui dengan cara yang baru, lebih mesra pengguna dan berkesan.

Produk **AVG 9 Anti-Virus plus Firewall** baru anda mempunyai antara muka yang menggaris 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 Anti-Virus plus Firewall 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)

2.2. Keperluan Perkakasan Minimum

Keperluan perkakasan minimum untuk **AVG 9 Anti-Virus plus Firewall** adalah seperti berikut:

- Intel Pentium CPU 1,2 GHz
- 250 MB ruang pacuan keras bebas (untuk tujuan pemasangan)
- 256 MB memori RAM

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 ini anda akan pasti untuk memasang versi AVG 9 Anti-Virus plus Firewall yang tersedia dan terkini.

Kami menyarankan untuk anda mencuba alat [AVG Download Manager](#) kami yang baru untuk membantu anda memilih fail pemasangan yang betul!

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 memilih fail pemasangan yang betul untuk 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 meneruskan dengan memuat turun dan melancarkan [proses pemasangan](#) yang sesuai.

Amaran: Sila maklum bahawa AVG Download Manager tidak sesuai untuk memuat turun rangkaian dan edisi SBS dan hanya sistem pengendalian berikut disokong: Windows 2000 (gulungan SP4 + SRP), Windows XP (SP2 dan lebih tinggi), Windows Vista (semua edisi).

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

4.1. Pemilihan Bahasa

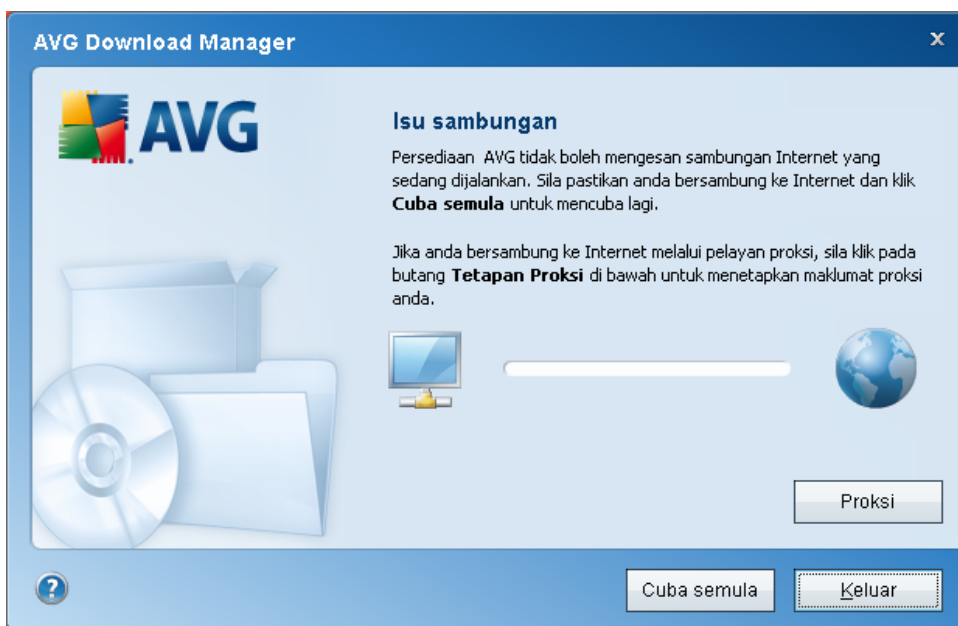


Dalam langkah pertama bagi **AVG Download Manager** pilih bahasa pemasangan dari menu gulung bawah. Harap maklum bahawa pilihan bahasa digunakan untuk proses pemasangan sahaja; selepas pemasangan anda boleh menukar bahasa secara terus dari tetapan atur cara. Kemudian, tekan butang **Berikutnya** untuk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

4.2. Semakan Kesambungan

Dalam langkah seterusnya, **AVG Download Manager** akan cuba menerbitkan sambungan Internet supaya kemas kini tersebut boleh ditempatkan. Anda tidak akan 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 opsyen 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. Pilih Jenis Lesen

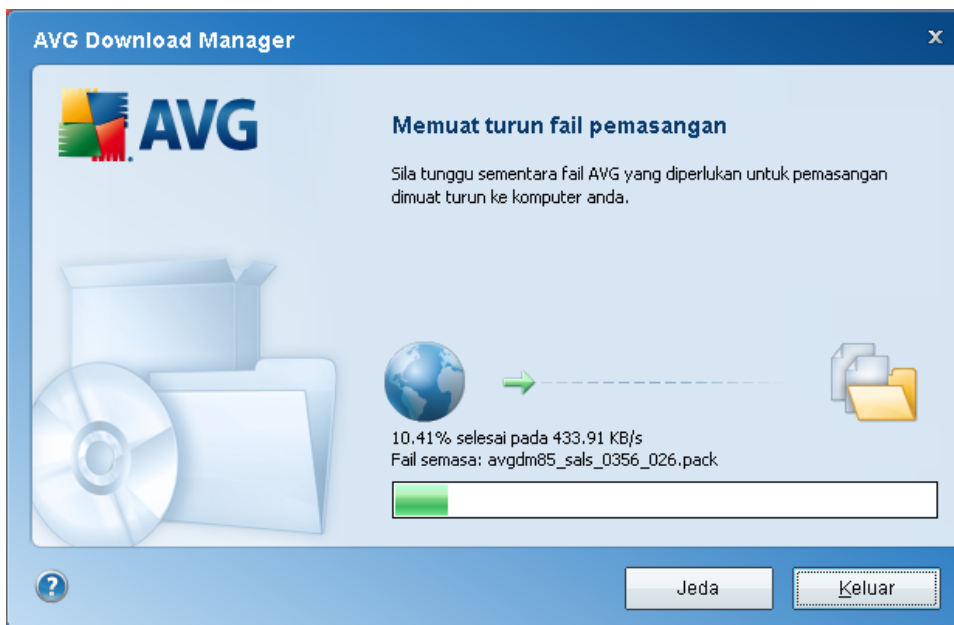


Dalam langkah ini, jika anda digesa untuk memilih jenis lesen produk yang anda

hendak muat turun. Penerangan yang diberikan membenarkan anda memilih yang paling sesuai dengan anda:

- **Versi penuh** - cth. **AVG Anti-Virus, AVG Anti-Virus plus Firewall** atau **AVG Internet Security**
- **Versi percubaan** - memberikan anda peluang untuk menggunakan semua ciri produk penuh AVG untuk tempoh masa terhad selama 30 hari.
- **Versi percuma** - memberikan perlindungan kepada pengguna rumah secara percuma, walau bagaimanapun, fungsi aplikasi adalah terhad! Serta, versi percuma hanya memasukkan beberapa ciri yang tersedia dalam produk berbayar.

4.5. Muat Turun Fail Untuk Dipasang



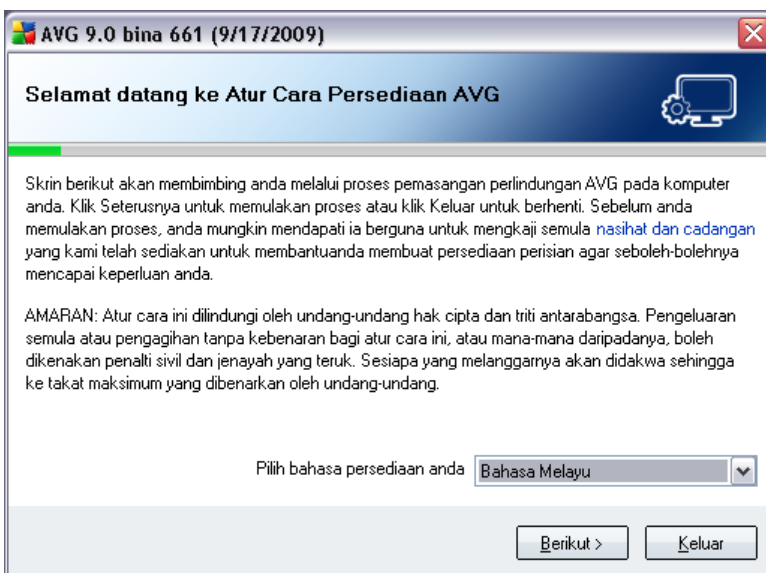
Kini, anda telah diberikan semua maklumat yang diperlukan untuk **AVG Download Manager** untuk memulakan muat turun pakej pemasangan dan lancarkan proses pemasangan. Seterusnya, lanjutkan kepada [Proses Pemasangan AVG](#).

5. Proses Pemasangan AVG

Untuk memasang pada komputer anda, anda perlu mendapatkan fail pemasangan terkini. **AVG 9 Anti-Virus plus Firewall** 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 **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

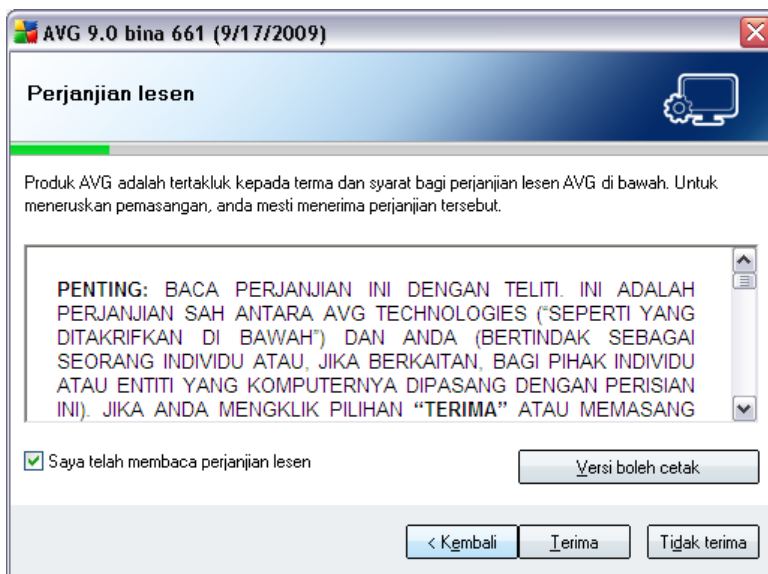


Proses pemasangan bermula dengan tettingkap **Selamat datang ke Atur Cara Persediaan AVG**. Di sini, anda pilih bahasa yang digunakan untuk proses pemasangan. Dalam bahagian bawah tettingkap dialog, cari item **Pilih bahasa persediaan anda**, dan pilih bahasa yang dikehendaki dari menu jatuh bawah. Kemudian,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



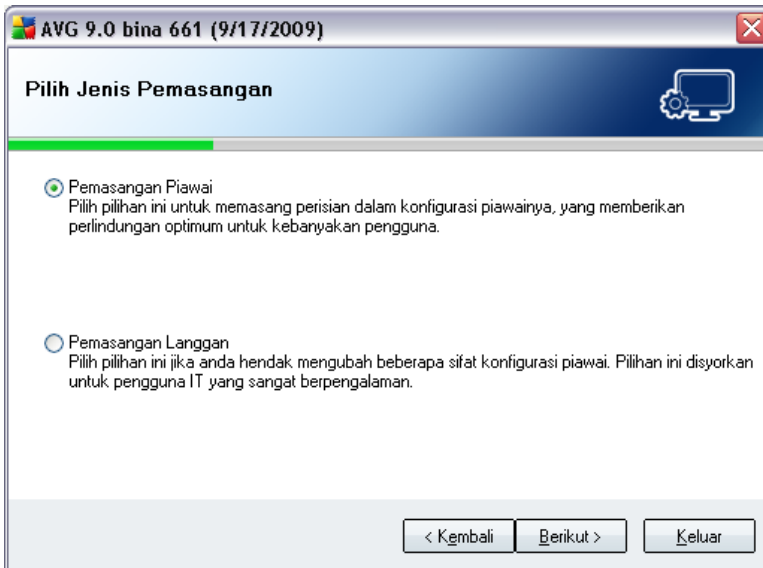
Dialog **Perjanjian Lesen** memberikan kata-kata penuh mengenai perjanjian lesen AVG. Sila bacanya dengan berhati-hati dan sahkan bahawa anda membaca, memahami dan menerima perjanjian dengan menandakan kotak semakan **Saya telah membaca perjanjian lesen** dan menekan butang **Terima**.

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 opsi 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.

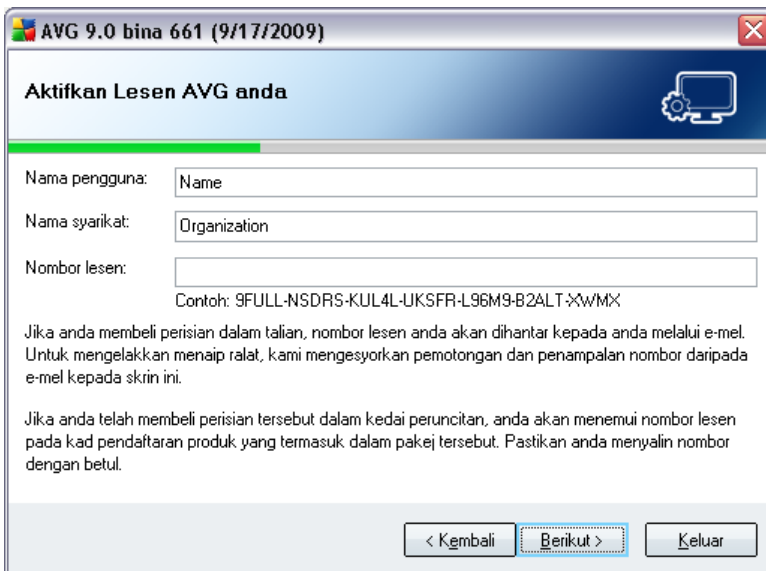
Pemasangan tersuai sepatutnya hanya digunakan oleh pengguna berpengalaman yang mempunyai alasan yang sah untuk memasang AVG dengan tetapan bukan standard. Cth. untuk disesuaikan dengan keperluan sistem khusus.

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 anda ke dalam medan teks **Nombor Lesen**. Nombor jualan boleh ditemui pada pembungkusan CD dalam kotak **AVG 9 Anti-Virus plus Firewall** anda. Nombor lesen akan berada dalam e-mel pengesahan

yang anda terima selepas membeli **AVG 9 Anti-Virus plus Firewall** dalam talian anda. 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 661 (9/17/2009)

Aktifkan Lesen AVG anda

Nama pengguna:

Nama syarikat:

Nombor lesen:

Contoh: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-3wMX

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.

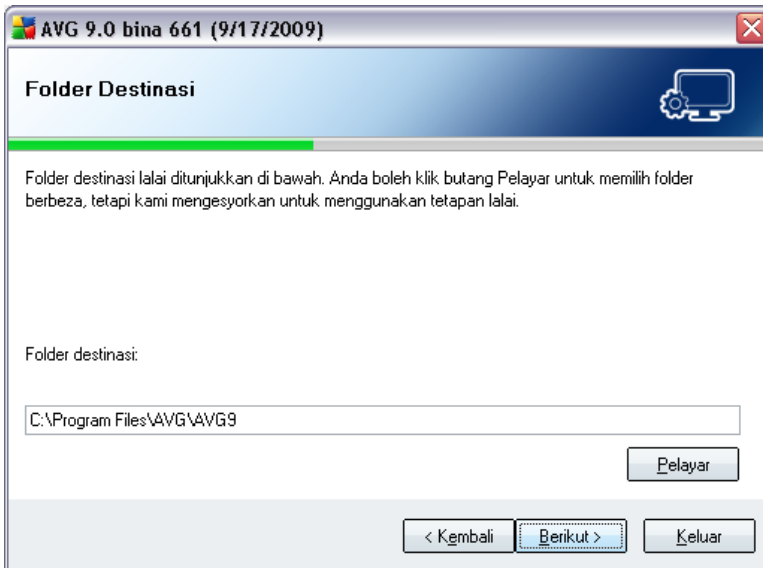
Jika anda telah membeli perisian tersebut dalam kedai peruncitan, anda akan menemui nombor lesen pada kad pendaftaran produk yang termasuk dalam pakej tersebut. Pastikan anda menyalin nombor dengan betul.

< 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

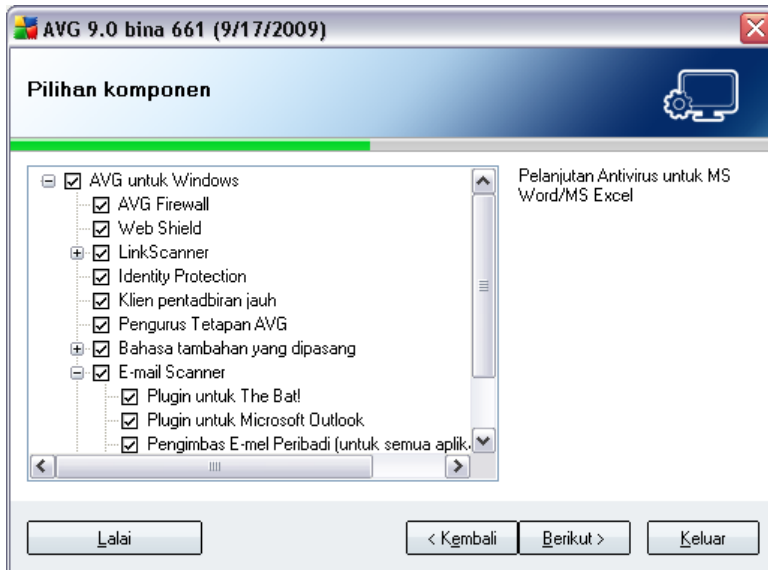


Dialog **Folder Destinasi** membenarkan anda menentukan lokasi di mana harus **AVG 9 Anti-Virus plus Firewall** harus dipasang. Secara lalai, AVG akan dipasang ke folder fail atur cara yang terletak pada pemacu C:. Jika folder tidak wujud lagi, anda akan diminta dalam dialog baru untuk mengesahkan anda 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 **AVG 9 Anti-Virus plus Firewall** komponen 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. Pilihan khusus lain adalah **Plugin for The Bat!** Jika anda menggunakan klien e-mel lain (*MS Exchange, Qualcomm Eudora, ...*), pilih opsiyen **Pengimbas E-mel Peribadi** untuk melindungi komunikasi e-mel anda secara automatik tidak kira atur cara e-mel apa yang anda jalankan.

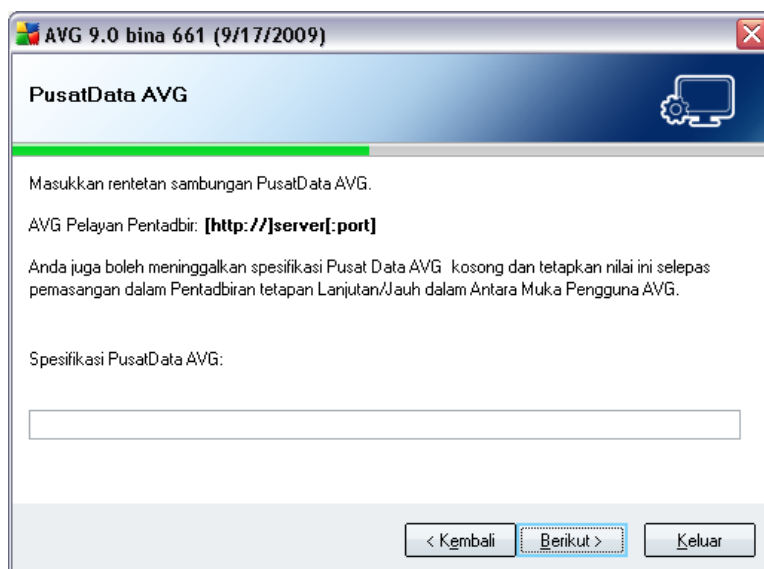
- **Pentadbiran Jauh**

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 dalam dialog **Pemasangan Tersuai - Pemilihan Komponen** sebelumnya anda telah menanda item **Pentadbiran jauh** untuk dipasang, anda perlu 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/>).

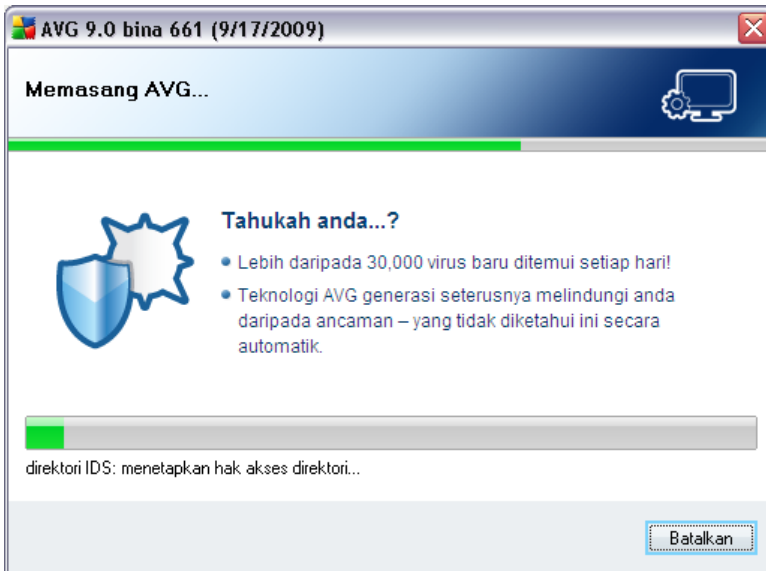
5.9. AVG Security Toolbar



Dalam dialog **AVG Security Toolbar** , tentukan sama ada anda hendak memasang **AVG Security Toolbar** (pengesahan hasil carian bagi enjin carian Internet yang disokong). Jika anda tidak mengubah tetapan lalai, komponen ini akan dipasang secara automatik ke dalam pelayar Internet anda untuk memberikan anda perlindungan dalam talian menyeluruh semasa melayari Internet.

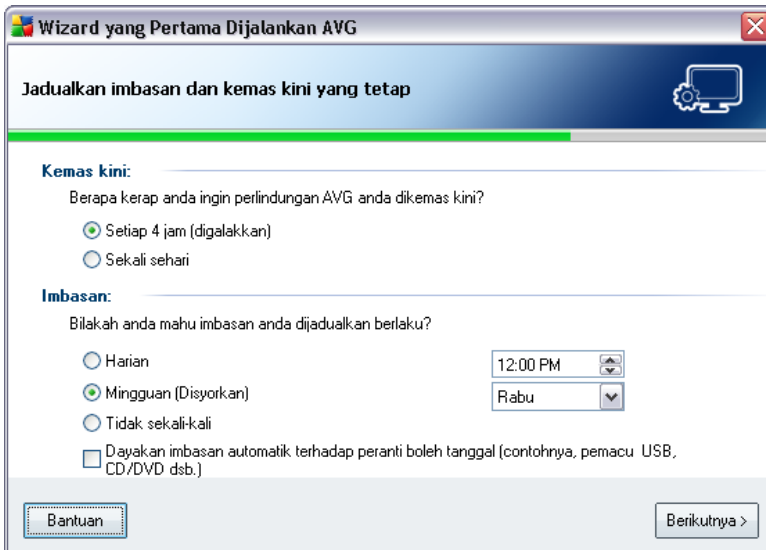
5.10. Memasang AVG

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.

5.11. 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 teruskan.

5.12. Pemilihan penggunaan komputer



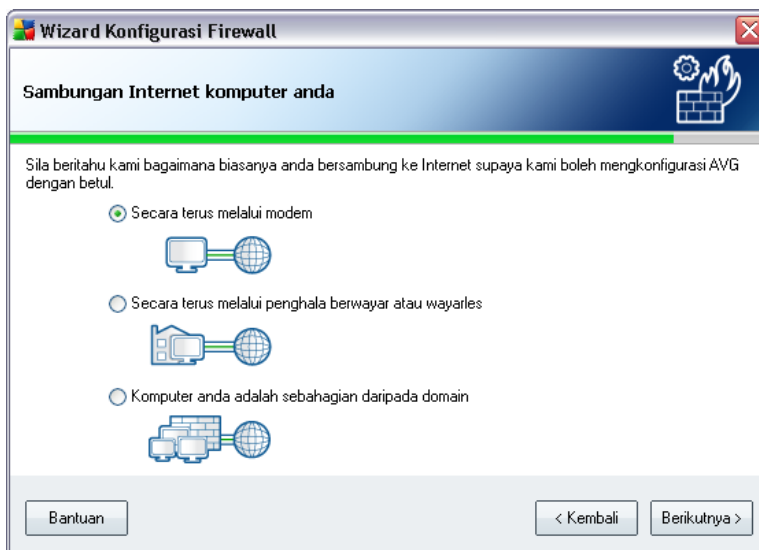
Dalam dialog ini, **Wizard Konfigurasi Firewall** bertanya jenis komputer yang anda gunakan. Contohnya, komputer bimbit anda yang menyambungkan Internet dari banyak lokasi berbeza (*lapangan terbang, bilik hotel, dll.*) memerlukan peraturan keselamatan yang lebih ketat daripada komputer dalam domain (*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.

5.13. Rekaan rangkaian komputer anda



Dalam dialog ini, **Wizard Konfigurasi Firewall** bertanya 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 kepada Internet**

- **Rangkaian rumah kecil**
- **Komputer anda berada dalam domain**

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

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

5.14. Konfigurasi perlindungan AVF lengkap



Kini, **AVG 9 Anti-Virus plus Firewall** anda telah dikonfigurasi.

Dalam dialog ini anda menentukan sama ada anda hendak mengaktifkan opsyen tanpa nama melaporkan eksploitasi dan tapak jahat kepada lab 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. Pendaftaran Produk

Menyelesaikan **AVG 9 Anti-Virus plus Firewall** pemasangan, sila daftarkan produk anda dalam talian pada tapak web AVG (<http://www.avg.com/>), halaman **Pendaftaran** (*ikuti 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.

6.2. 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**

6.3. Mengimbas seluruh komputer

Terdapat kemungkinan risiko bahawa virus komputer telah dihantar ke komputer anda sebelum pemasangan **AVG 9 Anti-Virus plus Firewall**. 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](#).

6.4. Ujian Eicar

Untuk mengesahkan bahawa **AVG 9 Anti-Virus plus Firewall** 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 memuat turun fail ujian, ***Perisai Web*** akan bertindak balas kepadanya dengan amaran. Notis ***Perisai Web*** ini menunjukkan bahawa AVG dipasang dengan betul pada komputer anda.



Jika AVG gagal mengenal pasti fail ujian EICAR sebagai virus, anda harus menyemak konfigurasi atur cara semula!

6.5. Konfigurasi Lalai AVG

Konfigurasi lalai (*cth. cara aplikasi disediakan betul-betul selepas pemasangan*) bagi **AVG 9 Anti-Virus plus Firewall** 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 Anti-Virus plus Firewall buka menggunakan tettingkap utama:



Tettingkap 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 tettingkap*) menawarkan gambaran keseluruhan komponen AVG yang dipasang - [butiran >>](#)
- **Statistik** (*bahagian bawah kiri tettingkap*) memberikan anda semua data statistik berkenaan operasi atur cara - [butiran >>](#)
- **Ikong 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 di bahagian paling atas tettingkap utama **AVG 9 Anti-Virus plus Firewall**. 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 Anti-Virus plus Firewall** . 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](#)
- **Anti-Virus** - membuka halaman lalai bagi komponen [Anti-Virus](#)
- **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***
- ***Pengimbas E-mel*** - membuka halaman lalai bagi komponen ***Pengimbas E-mel***
- ***Lesen*** - membuka halaman lalai bagi komponen ***Lesen***
- ***Perisai Web*** - membuka halaman lalai bagi komponen ***Perisai Web***
- ***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 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 Web*** - membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh ***Perisai Web***
- ***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 Anti-Virus plus Firewall** 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 mentakrifkan dalam struktur pepohon komputer anda bagi fail dan folder mana yang harus diimbas
- **Imbas fail** - membenarkan anda untuk menjalankan ujian dalam permintaan pada fail tunggal yang dipilih dari struktur pepohon cakera anda
- **Kemas kini** - melancarkan proses kemas kini secara automatik **AVG 9 Anti-Virus plus Firewall**
- **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 Anti-Virus plus Firewall** . 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** - membukatapak 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.
- **Mengenai AVG** - membuka dialog **Maklumat** dengan lima tab yang memberikan data mengenai nama atur cara, versi pangkalan data atur cara dan virus, maklumat sistem, perjanjian lesen dan maklumat hubungan mengenai **AVG Technologies CZ**.

7.2. Maklumat Status Keselamatan

Bahagian **Maklumat Status Keselamatan** terletak di bahagian atas tettingkap utama AVG. Dalam bahagian ini, anda sentiasa mendapat maklumat mengenai status semasa bagi **AVG 9 Anti-Virus plus Firewall** 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 banyak komponen dikonfigurasi dengan salah dan anda harus memberikan perhatian kepada sifat/tetapanannya. 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 sebab tertentu anda telah memutuskan untuk [mengabaikan status ralat komponen](#) (opsyen "*Abaikan keadaan komponen*" *tersedia dari menu konteks yang dibuka dengan mengklik kanan pada ikon komponen masing-masing dalam gambaran keseluruhan tettingkap utama AVG*).

Anda mungkin perlu menggunakan opsi ini dalam situasi tertentu tetapi amat disarankan untuk mematikan opsi "**Abaikan keadaan komponen**" secepat mungkin.



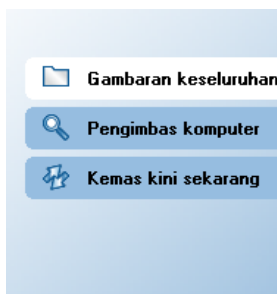
Ikona merah menunjukkan bahawa AVG berada dalam status kritikal ! Satu atau lebih komponen tidak berfungsi dengan betul dan AVG tidak dapat melindungi komputer anda. Sila berikan perhatian serta-merta untuk menyelesaikan masalah yang dilaporkan. Jika anda tidak dapat membetulkan ralat dengan sendiri,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

Adalah amat disarankan 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 (pada bahagian kiri [Antara Muka Pengguna AVG](#)) membenarkan anda mengakses ciri AVG yang paling penting dan paling kerap digunakan dengan serta-merta:



- **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 parameternya - lihat bab [Ujian 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 dijalankan selanjutnya digambarkan secara grafik (*gambar 2*).

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 bahagian **AVG 9 Anti-Virus plus Firewall 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 >>](#)
- **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 >>](#)
- **Pengimbas E-mel** memeriksa semua mel masuk dan keluar bagi virus - [butiran >>](#)
- **Lesen** menyediakan pernyataan penuh mengenai Perjanjian Lesen AVG - [butiran >>](#)
- **Perisai Web** mengimbas semua data yang dimuat turun oleh pelayar 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 kefungsiian 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 opsyen ini untuk menyatakan bahawa anda menyedari [keadaan ralat komponen](#) tetapi untuk sebab tertentu, anda ingin menyimpan AVG anda dan anda tidak mahu diberi amaran daripada warna kelabu bagi [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 8.0.xx, di mana 8.0 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

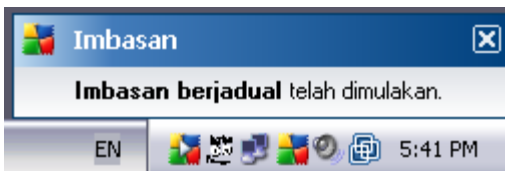
Ikon Dulang Sistem (*pada bar tugas Windows*) menunjukkan status semasa bagi **AVG 9 Anti-Virus plus Firewall** anda. Ia boleh dilihat setiap masa ada dulang sistem anda, tidak kira sama ada tettingkap utama AVG anda dibuka atau ditutup.

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](#)**.

Warna ikon kelabu 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 memberitahu selanjutnya mengenai aktiviti AVG semasa dan kemungkinan perubahan status dalam atur cara (*cth. pelancaran automatik bagi imbasan atau kemas kini yang dijadualkan, pertukaran profil Firewall, perubahan status komponen, kejadian 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 opsyen 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.

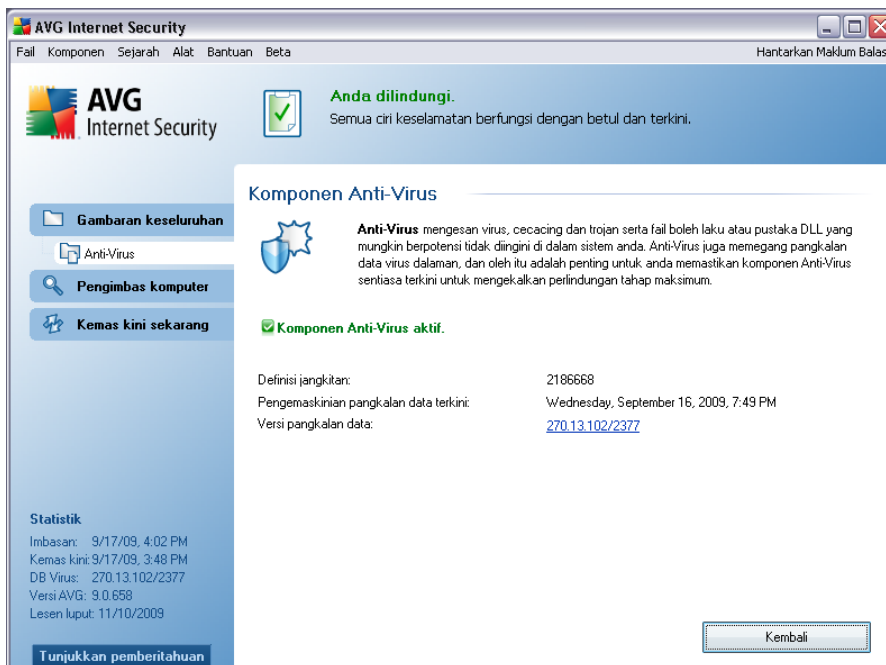
Ciri penting bagi perlindungan antivirus adalah tiada virus yang diketahui boleh dijalankan pada komputer!

Di mana hanya satu teknologi tunggal boleh kekurangan pengesanan atau pengenalanpastian 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 pengendalian yang tersedia dalam antara muka komponen ini (**Kembali**) - tekan butang tersebut 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 harus 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.

8.2. 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 potensi risiko bahawa malware telah dipindahkan ke komputer sebelum pemasangan AVG atau anda telah mengabaikan untuk memastikan **AVG 9 Anti-Virus plus Firewall** adalah terkini dengan pangkalan data terkini dan [kemas kini atur cara](#). 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 kefungsiannya, 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 pengendalian yang tersedia dalam antara muka komponen ini (**Kembali**) - tekan butang tersebut 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 harus 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. 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.

8.3.1. 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 pratakrif, mengikut keperluan anda
- Menyimpan [arkib](#) semua profil dan tetapan yang ditakrifkan
- [Tukar profil](#) secara automatik apabila menyambung kepada pelbagai rangkaian, atau menggunakan pelbagai penyesuai rangkaian

8.3.2. Profil Firewall

Firewall membenarkan anda mentakrifkan peraturan keselamatan khusus berdasarkan kepada sama ada komputer anda terletak dalam domain, atau ia komputer berdiri sendiri, atau 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 dipratakrif seperti itu.

Profil yang ada

- **Benarkan semua** - profil sistem **Firewall** yang telah dipratetap oleh pengeluar dan sentiasa ada. 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 pengeluar

dan sentiasa ada. 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:**

- **Komputer bergerak** – sesuai untuk komputer rumah desktop yang disambungkan secara terus ke Internet atau komputer bimbit menyambung ke Internet di luar rangkaian syarikat selamat. Pilih opsi ini jika anda bersambung dari rumah atau anda dalam rangkaian syarikat kecil dengan tiada kawalan pusat. Serta, pilih opsi 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.
- **Komputer dalam domain** – sesuai untuk komputer dalam rangkaian tempatan, 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.
- **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

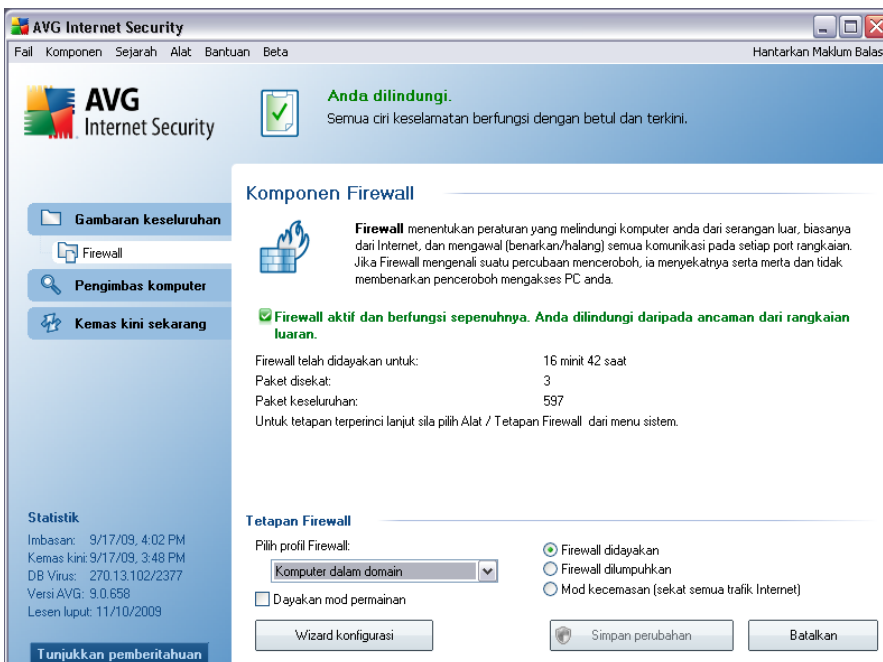
Ciri pertukaran profil membenarkan **Firewall** untuk beralih secara automatik ke profil yang ditakrifkan semasa menggunakan penyesuai rangkaian tertentu atau semasa disambungkan ke jenis rangkaian tertentu. Jika belum ada profil yang telah diperuntukkan ke kawasan rangkaian, maka, pada sambungan berikutnya 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 Penyesuai**, 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.

8.3.3. 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** - Tanda opsyen ini untuk memastikan semasa menjalankan aplikasi skrin penuh (permainan, persembahan PowerPoint dll.), **Firewall** tidak akan memaparkan dialog menanyakan sama ada anda mahu membenarkan atau menyekat komunikasi bagi aplikasi yang 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:**
 - **Firewall didayakan** - pilih opsyen ini untuk membenarkan komunikasi dengan aplikasi tersebut yang diperuntukkan sebagai 'dibenarkan' dalam set peraturan dalam profil **Firewall** yang dipilih
 - **Firewall dinyahdayakan** - opsyen ini mematikan **Firewall** sepenuhnya, semua lalu lintas rangkaian dibenarkan tetapi tidak diperiksa!
 - **Mod kecemasan (sekat semua lalu lintas internet)** - pilih opsyen 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 Fail / 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
- **Batalkan** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen)

8.4. 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 kuat 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.

8.4.1. 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!

8.4.2. 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 diimbas untuk virus. Secara lalai, item ini dihidupkan dan ia disyorkan untuk tidak mengubah tetapan ini!
- **Imbas mesej keluar** - memeriksa item untuk mengesahkan bahawa semua e-mel yang dihantar dari akaun anda harus diimbas untuk virus. Secara lalai, item ini dimatikan.
- **Paparkan ikon pemberitahuan semasa E-mel diimbas** - sewaktu imbasan, komponen **Pengimbas E-mel** memaparkan dialog pemberitahuan yang memberitahu mengenai tugas sebenar yang komponen sedang proses (*menyambung ke pelayan, memuat turun mesej, mengimbas mesej, ...*). Opsyen ini diaktifkan dan tidak boleh diedit.

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

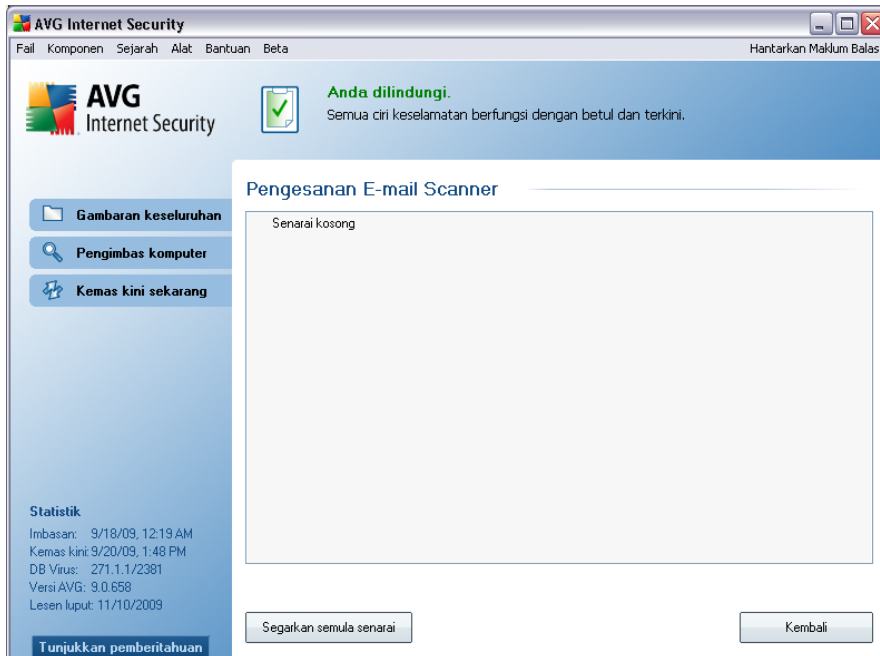
Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan harus dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu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

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)

8.4.3. Pengesanan Pengimbas E-mel



Dalam dialog ***pengesanan Pengimbas E-mel*** (boleh diakses melalui menu sistem opsyen Sejarah / pengesanan 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

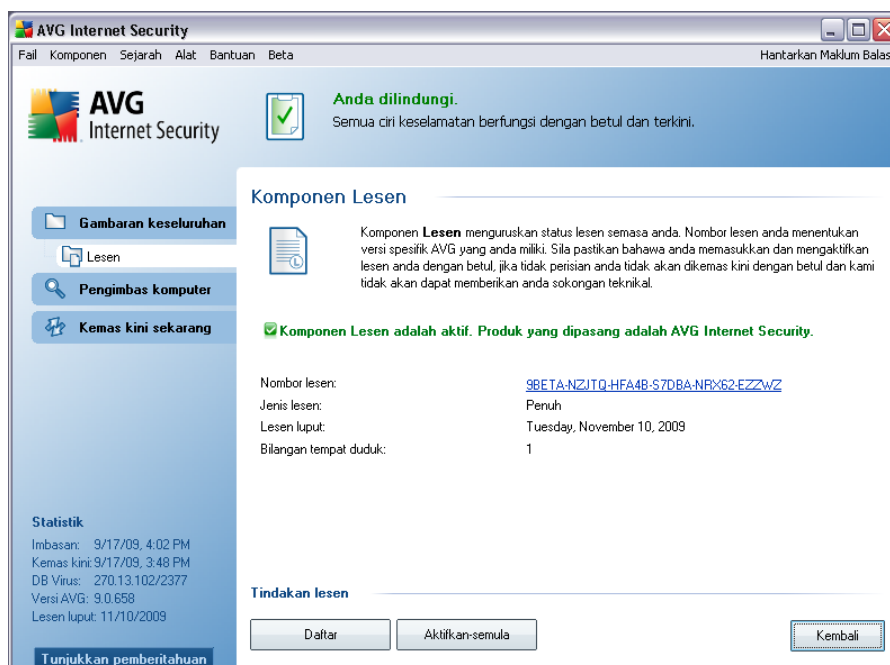
Di bahagian bawah dialog, di bawah senarai, anda akan menemui maklumat mengenai jumlah bilangan objek dikesan yang disenaraikan di atas. Seterusnya, anda boleh mengeksport keseluruhan senarai objek yang dikesan dalam fail (***Eksport senarai ke fail***) dan padam semua entri pada objek dikesan (***Kosongkan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

8.5. 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 Anti-Virus plus Firewall** selepas tarikh ini, anda perlu memperbaharui lesen anda. [Pembaharuan lesen boleh dilakukan dalam talian](#) pada tapak web AVG (<http://www.avg.com/>).
- **Bilangan tempat duduk** - berapa banyak stesen kerja pada mana anda tertakluk untuk memasang **AVG 9 Anti-Virus plus Firewall** 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*).
- **Kembali** - tekan butang ini untuk kembali ke [antara muka AVG](#) lalai (gambaran keseluruhan komponen).

8.6. Pengimbas Pautan

8.6.1. 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!, MSN atau Baidu, semua hasil diperiksa mengikut senarai ini dan ikon keputusan ditunjukkan (*untuk Yahoo! hasil carian hanya ikon keputusan " tapak web yang dieksplotasi" ditunjukkan*). Serta, jika anda menaiki 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.

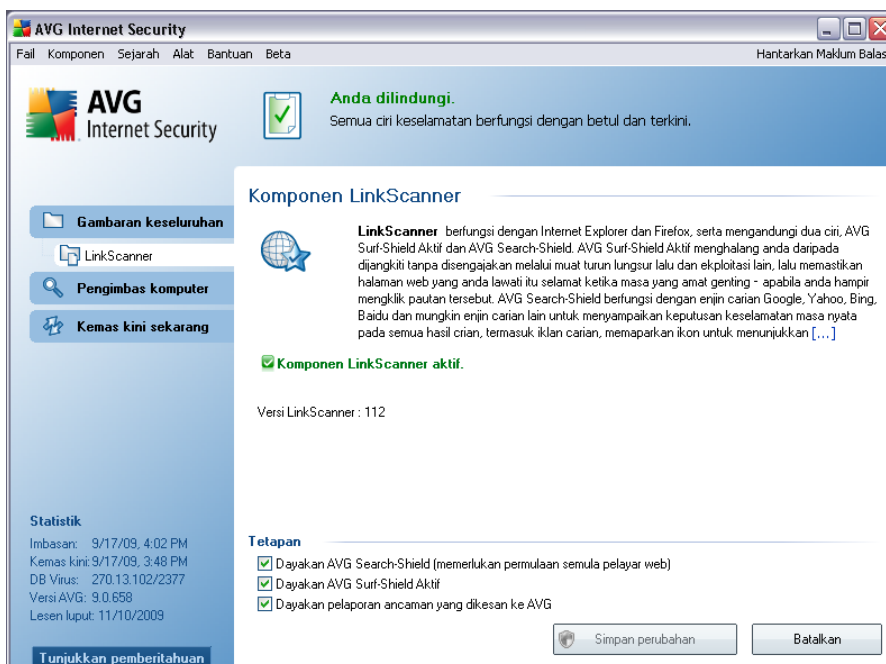
- **AVG Active Surf-Shield** mengimbas kandungan tapak web yang anda lawati, tidak kira alamat tapak web. Walaupun, sesetengah tapak web tidak dikesan oleh **AVG Search Shield** (cth. apabila tapak web berniat jahat dibuat atau apabila tapak web bersih sebelumnya mengandungi beberapa malware), ia akan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

Nota: AVG Link Scanner bukan bertujuan untuk platform pelayan!

8.6.2. 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 kefungsiannya 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](#)** - (*hidupkan secara lalai*): ikon pemberitahuan penasihat pada carian yang dilakukan dalam Google, Yahoo atau MSN yang seterusnya diperiksa kandungan tapak 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.


8.6.3. AVG Search-Shield

Semasa membuat carian di Internet dengan ***AVG Search-Shield*** dihidupkan, semua keputusan carian dikembalikan daripada enjin pencarian paling popular seperti Yahoo!, Google, MSN, dll. dinilai bagi pautan yang berbahaya atau mencurigakan. Dengan memeriksa pautan ini dan menandakan pautan jahat, **[AVG Security Toolbar](#)** memberi amaran kepada anda sebelum anda mengklik pada pautan berbahaya atau mencurigakan supaya anda boleh memastikan anda hanya pergi ke tapak web yang selamat.

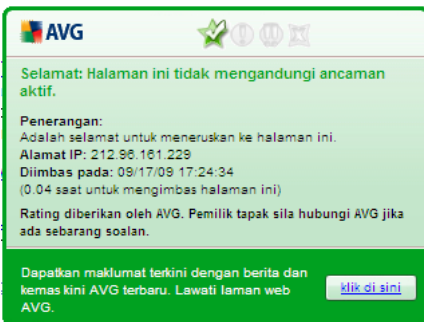
Semasa pautan dinilai pada halaman keputusan carian, anda akan melihat tanda grafik di sebelah pautan yang memberitahu bahawa pengesahan pautan sedang dijalankan. Apabila penilaian selesai, ikon maklumat masing-masing akan dipaparkan.


-  Halaman berpaut adalah selamat (*dengan enjin pencarian enjin pencarian 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 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.

 Laman yang dipautkan 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 diimbis.

Menghalakan pada ikon pengedaran individu 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.



AVG 

Selamat: Halaman ini tidak mengandungi ancaman aktif.

Penerangan:
Adalah selamat untuk meneruskan ke halaman ini.
Alamat IP: 212.98.161.229
Diimbis pada: 09/17/09 17:24:34
(0.04 saat untuk mengimbis halaman ini)

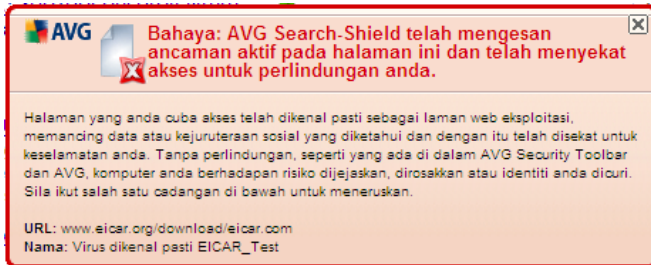
Rating diberikan oleh AVG. Pemilik tapak sila hubungi AVG jika ada sebarang soalan.

Dapatkan maklumat terkini dengan berita dan kemas kini AVG terbaru. Lawati laman web AVG. [klik di sini](#)

8.6.4. 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 laman web yang dieksploitasi boleh menjangkiti komputer anda dengan hanya melawati tapak yang dijangkiti, untuk sebab ini, semasa anda meminta laman web berbahaya yang mengandungi eksploitasi atau ancaman serius lain, [AVG Security Toolbar](#) tidak akan membenarkan pelayar anda memaparkannya.

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



Memasuki tapak web sangat berisiko dan ia tidak disyorkan!

8.7. Perisai Web

8.7.1. Prinsip Perisai Web

Perisai Web 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 Web 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.

Nota: *AVG Web Shield bukan bertujuan untuk platform pelayan!*

8.7.2. Antara Muka Perisai Web

Antara muka komponen **Perisai Web** menerangkan kelakuan perlindungan jenis ini. Seterusnya, anda boleh mendapatkan maklumat mengenai status semasa komponen (*Perisai Web 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 opsyen untuk menghidupkan/mematikan **Perisai Web** dengan serta-merta dengan menanda item **Dayakan Perisai Web**. Opsyen ini didayakan secara lalai dan komponen **Perisai Web** adalah aktif. Walau bagaimanapun, jika anda tidak mempunyai alasan yang baik untuk mengubah tetapan ini, kami mengesyorkan untuk memastikan komponen aktif. Jika item

ditandakan dan **Perisai Web** berjalan, lebih banyak opsyen konfigurasi tersedia dan boleh diedit pada dua tab:

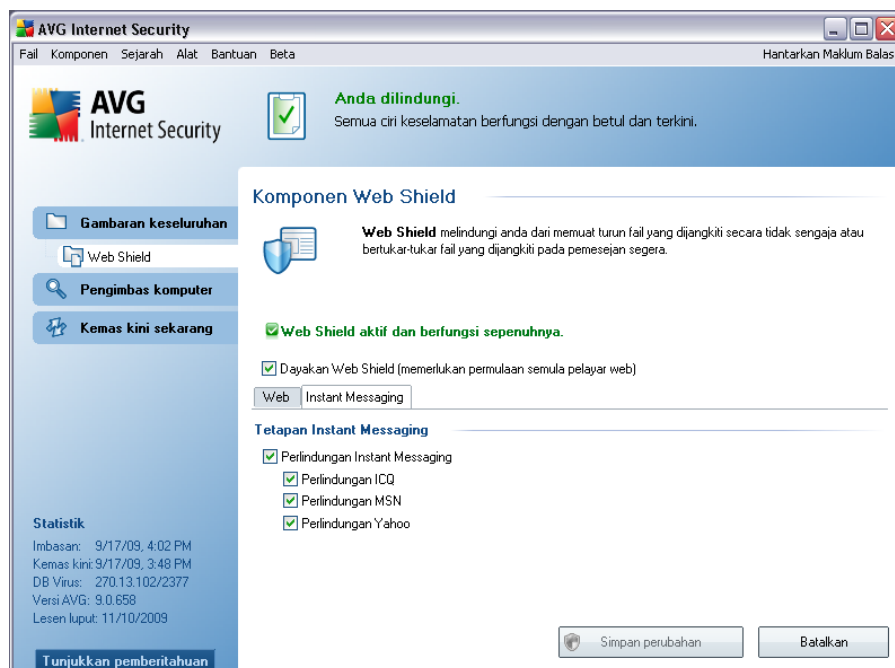
- **Web** - anda boleh mengedit konfigurasi komponen berkenaan imbasan kandungan tapak web. Antara muka penyuntingan ini membenarkan anda untuk mengkonfigurasi opsyen permulaan berikut:



- **Perlindungan web** - opsyen ini mengesahkan bahawa **Perisai Web** patut melakukan imbasan 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
 - **Imbas Atur Cara Yang Berpotensi Tidak Dikehendaki** - imbas atur cara yang berpotensi tidak dikehendaki (*atur cara boleh laku yang boleh beroperasi sebagai perisian pengintip atau adware*) termasuk halaman www untuk dipaparkan
 - **Gunakan analisis heuristik** - imbas kandungan halaman untuk dipaparkan menggunakan kaedah analisis heuristik (*persaingan dinamik bagi arahan objek yang dikesan dalam persekitaran*)

komputer maya - lihat bab [Prinsip AntiVirus](#))

- **Saiz fail maksimum untuk diimbas** - jika fail yang dimasukkan terdapat dalam halaman yang dipaparkan, anda juga boleh mengimbas 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 fail yang masih perlu diimbas dengan **Perisai Web**. Walaupun, jika fail yang dimuat turun adalah lebih besar daripada yang ditentukan, dan oleh itu, tidak akan diimbas dengan **Perisai Web**, anda masih dilindungi: jika fail dijangkiti, **Perisai Residen** akan mengesannya dengan serta-merta.
- **Pemesejan Segera** - membenarkan anda mengedit tetapan komponen merujuk kepada pengimbasan pemesejan segera (*cth. ICQ, MSN Messenger, Yahoo ...*).



- Perlindungan Pemesejan Segera - tandakan item ini jika anda mahu Perisai Web mengenal pasti komunikasi dalam talian adalah bebas daripada virus. Jika opsi ini dihidupkan, seterusnya, anda boleh menentukan aplikasi pemesejan segera mana yang anda hendak kawal - buat masa ini **AVG 9 Anti-Virus plus Firewall** 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 terbuka.

Butang kawalan

Butang kawalan yang tersedia dalam antara muka **Perisai Web** 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)

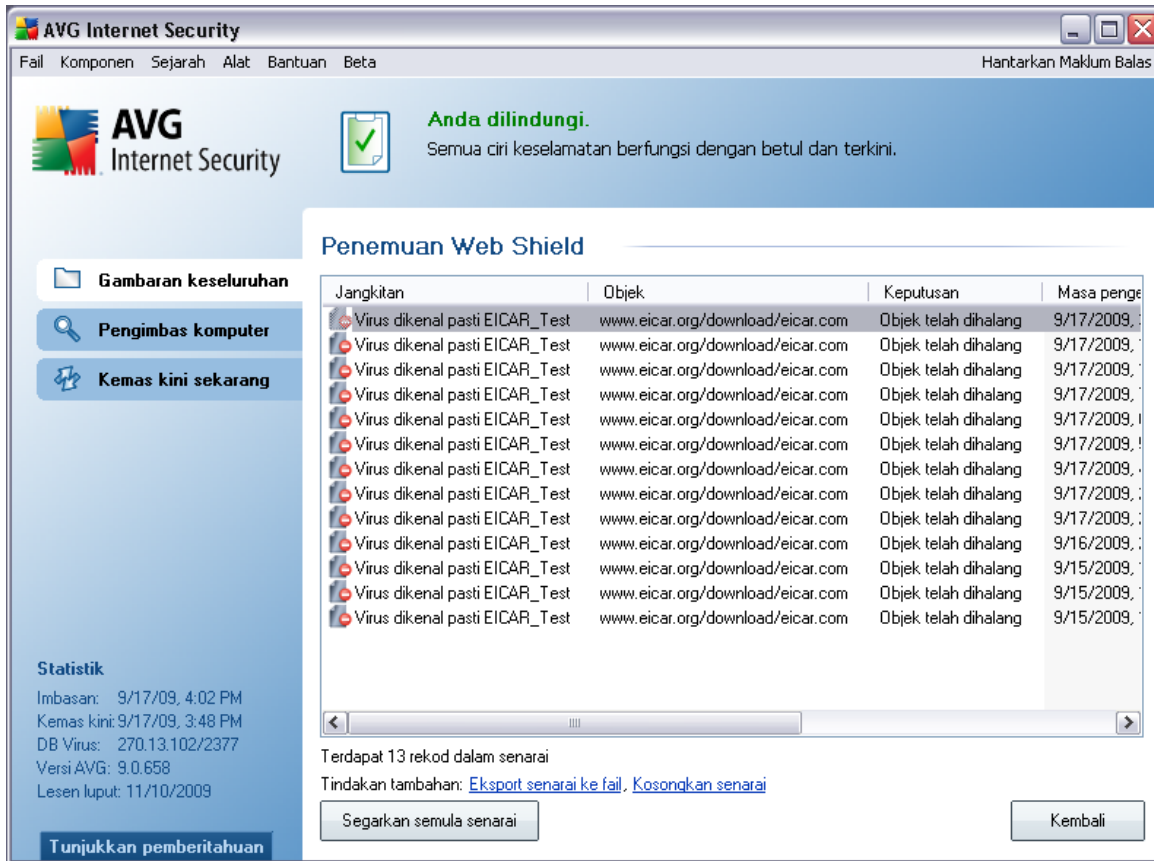
8.7.3. Pengesanan Perisai Web

Perisai Web mengimbas kandungan halaman web yang dilawati dan kemungkinan fail yang dimasukkan di dalamnya, malahan sebelum ini dipaparkan dalam pelayar anda 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 dilogkan dalam senarai **penemuan Perisai Web** - gambaran keseluruhan ini bagi

ancaman yang dikesan boleh diakses melalui menu sistem [penemuan Sejarah / Perisai Web](#).



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 Residen**. Butang **Kembali** mengalihkan anda kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen).

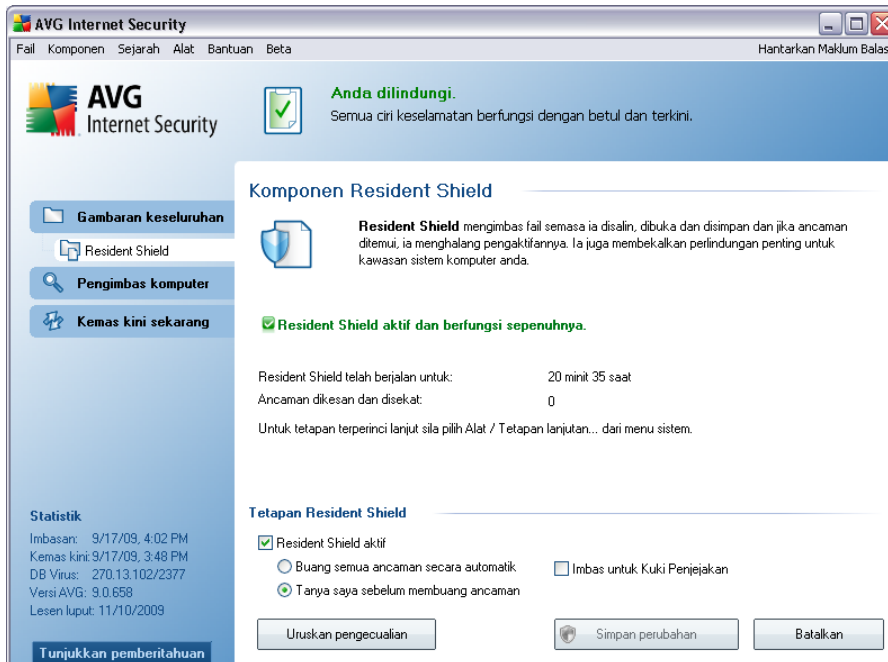
8.8. Perisai Residen

8.8.1. Perisai Residen 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!

8.8.2. 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 opsiyen 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 kefungsiian komponen (*konfigurasi terperinci dengan semua komponen lain tersedia melalui item tetapan Alat/Lanjutan bagi menu sistem*).

Opsiyen **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 ***Buang kuki secara automatik***. Dalam kes tertentu, anda boleh mengalihkan opsi 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 harus 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 terbuka.

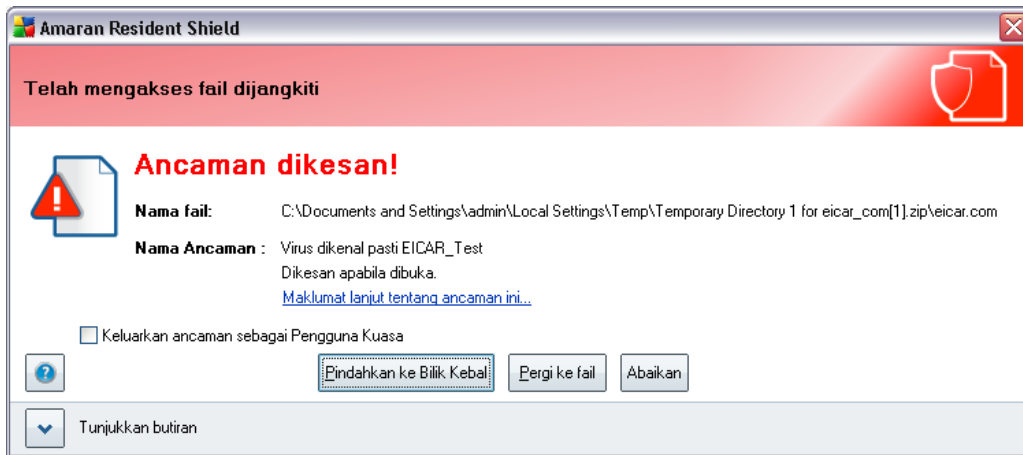
Butang kawalan

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

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

8.8.3. Pengesanan Perisai Residen

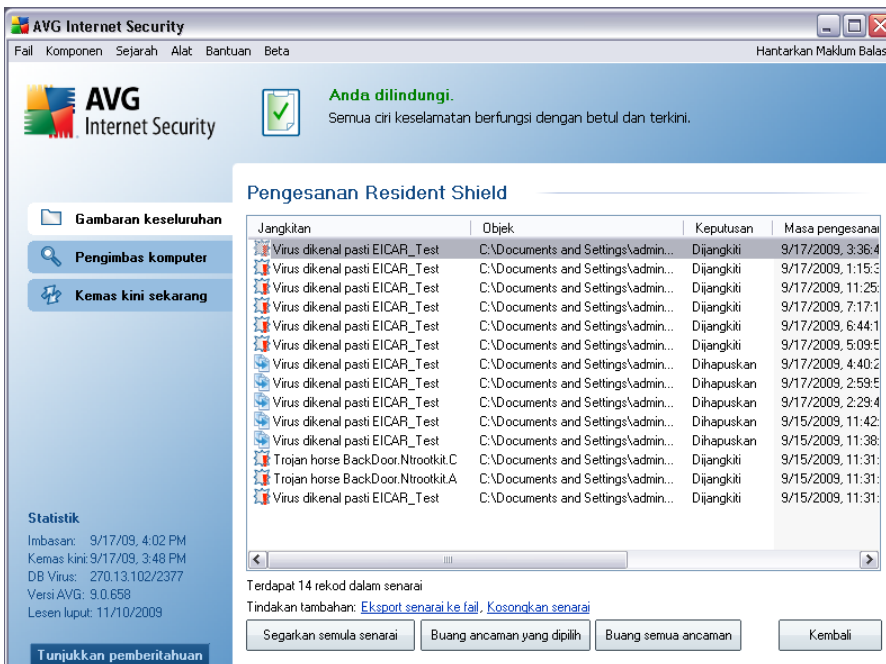
Perisai Residen mengimbas fail semasa ia disalin, dibuka atau disimpan. Apabila virus atau sebarang jenis ancaman dikesan, anda akan diberi amaran serta-merta melalui dialog berikut:



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 tettingkap 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** menukarkan anda kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen).

8.9. Pengurus Kemas Kini

Tiada perisian keselamatan yang boleh menjamin perlindungan sebenar dari pelbagai jenis ancaman melainkan ia dikemas kini secara tetap! Penulis virus sentiasa mencari kecelaan 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!

Pengurus Muat Turun AVG adalah alat ringkas yang memberikan anda cara yang mudah untuk menguruskan muat turun produk utama AVG. Berdasarkan pada pemilihan anda, pengurus muat turun akan mengkonfigurasi produk, jenis lesen dan bahasa tertentu. Kelebihan yang besar bagi utiliti ini adalah untuk membantu anda menguruskan muat turun produk AVG pada terma anda. Tambahan pula, fail pemasangan sentiasa dimuat turun, maka, atur cara AVG dikemas kini sepenuhnya selepas pemasangan.

AVG Download Manager

- Sentiasa memuat turun fail pemasangan terkini;
- Kurangkan saiz fail yang dimuat turun;
- Menyokong sambung semula muat turun jika muat turun gagal atas sebab tertentu;
- Bekerja dengan edisi atur cara AVG yang bertujuan untuk penggunaan rumah

Nota: Sila maklum bahawa AVG Download Manager tidak sesuai untuk memuat turun rangkaian dan edisi SBS dan hanya sistem pengendalian berikut disokong: Windows

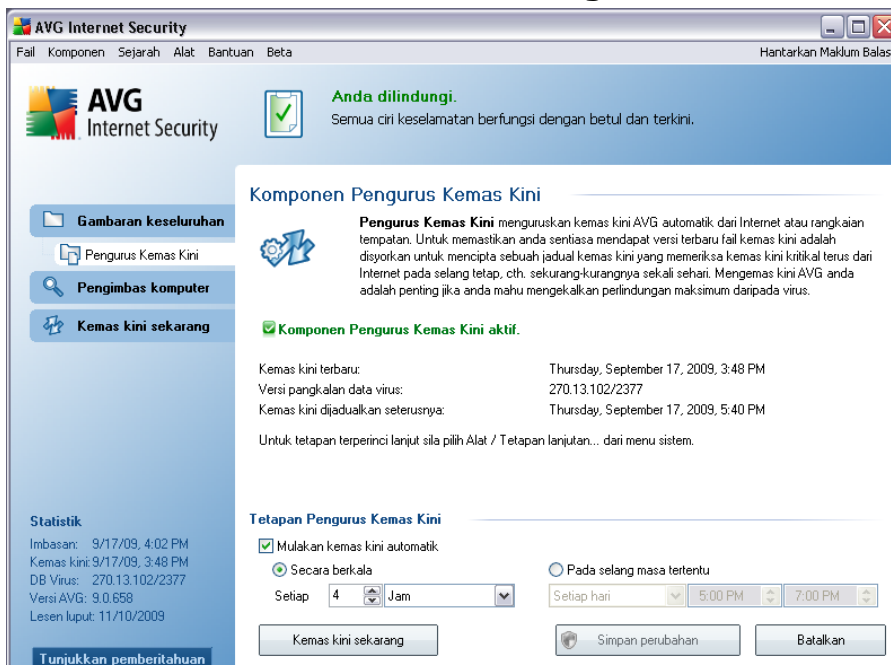
2000 (gulungan SP4 + SRP), Windows XP (SP2 dan lebih tinggi), Windows Vista (semua edisi).

8.9.1. Kemas Kini Prinsip Pengurus

AVG Download Manager beroperasi dalam langkah berikut:

- Pertama, adalah perlu untuk memuat turun aplikasi **Pengurus Muat Turun AVG** dengan sendiri. Apabila dilancarkan, **Pengurus Muat Turun AVG** meminta anda untuk memilih bahasa bagi proses pemasangan.
- Kemudian, **Pengurus Muat Turun AVG** cuba mewujudkan sambungan Internet untuk melakukan ujian kesambungan. Jika ujian kesambungan berjaya, anda boleh memilih versi mana bagi atur cara AVG yang anda hendak pasang (*versi penuh, versi percubaan, edisi percuma*).
- Sebaik sahaja versi atur cara AVG dipilih, anda akan digesa untuk memilih produk yang anda hendak pasang.
- Akhir sekali, semua fail pemasangan yang diperlukan akan dimuat turun. **Pengurus Muat Turun AVG** menutup dan [pemasangan AVG](#) dilancarkan.

8.9.2. Kemas Kini Antara Muka Pengurus



Antara muka **Pengurus Kemas Kini** memaparkan maklumat mengenai kefungsiian 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 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, opsyen **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 kemas kini!

Seterusnya, anda boleh menentukan bila kemas kini patut dilancarkan:

- **Secara berkala** - tentukan selang masa
- **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 terbuka.

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)

8.10. AVG Security Toolbar

AVG Security Toolbar adalah alat yang bekerja bersama dengan komponen [Pengimbas Pautan](#) dan memeriksa hasil carian enjin carian Internet yang disokong (*Yahoo!, Google, MSN, Baidu*).

Jika anda memilih untuk memasang bar alat sewaktu pemasangan **AVG 9 Anti-Virus plus Firewall**, ia akan ditambah ke dalam pelayar web anda secara automatik.

AVG Security Toolbar boleh digunakan untuk mengawal fungsi [Link Scanner](#) dan untuk melaraskan kelakuannya dan untuk mengemas kini **AVG 9 Anti-Virus plus Firewall** anda jika kemas kini baru tersedia.

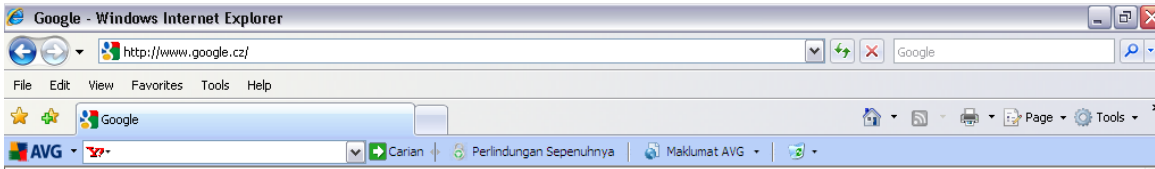
Nota: Jika anda menggunakan beberapa pelayar Internet alternatif (cth. Avant Browser) anda boleh menghadapi kelakuan yang tidak dijangka.

8.10.1. AVG Security Toolbar Antara muka

AVG Security Toolbar direka bentuk untuk berfungsi dengan **MS Internet Explorer** (versi 6.0 atau lebih terkini) dan **Mozilla Firefox** (versi 1.5 atau lebih terkini).

Nota: AVG Security Toolbar bukan disasarkan untuk platform pelayan!

Sebaik sahaja anda telah menentukan bahawa anda hendak memasang **AVG Security Toolbar** (sewaktu [proses pemasangan AVG](#) anda akan ditanya untuk menentukan sama ada anda mahu atau tidak memasang komponen), komponen akan terletak dalam pelayar web anda betul-betul di bawah bar alamat:



AVG Security Toolbar terdiri daripada yang berikut:

- **Butang 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:
 - **Maklumat Bar Alat** - pautan kepada halaman utama **AVG Security Toolbar** dengan maklumat terperinci mengenai perlindungan bar alat
 - **Lancarkan AVG 9.0** - membuka [antara muka pengguna AVG](#)
 - **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](#)
 - **Padam Sejarah** - membenarkan anda *Memadam sejarah yang lengkap* bagi AVG Security Toolbar, atau untuk *Memadam sejarah carian, Memadam sejarah pelayar* dan *Padam kuki*.
 - **Kemas kini** - menyemak untuk kemas kini baru untuk **AVG Security Toolbar anda**
 - **Bantuan** - memberikan opsyen untuk membuka fail bantuan, hubungi [sokongan teknikal AVG](#), atau lihat butiran bagi versi terkini bar alat
- **Kotak carian yang dikuasakan Yahoo!** - cara yang mudah dan selamat untuk mencari pada web menggunakan carian Yahoo!. Masukkan perkataan atau frasa dalam kotak carian, tekan **Cari** untuk memulakan carian pada pelayan Yahoo! secara terus, 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](#).
- **Butang AVG Active Surf-Shield** - butang hidup/mati mengawal status bagi perlindungan [AVG Active Surf-Shield](#)
- **Butang AVG Search-Shield** - butang hidup/mati mengawal status bagi

perlindungan **AVG Active Surf-Shield**

- **Butang Maklumat AVG** - memberikan pautan kepada maklumat keselamatan penting yang terletak pada tapak web AVG (<http://www.avg.com/>).

8.10.2. Opsyen AVG Security Toolbar

Semua konfigurasi parameter **AVG Security Toolbar** boleh diakses secara terus dalam panel **AVG Security Toolbar**. Antar muka pengeditan dibuka melalui item menu bar alat AVG / *Opsyen* dalam dialog yang dipanggil **Opsyen Bar Alat** yang dibahagikan ke dalam tiga bahagian:

- **Umum**



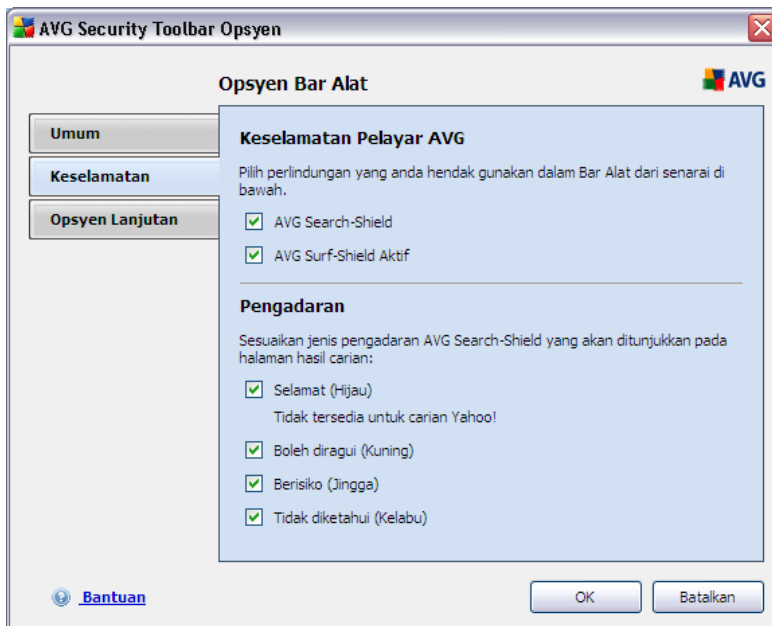
Pada tab, anda boleh menentukan butang yang harus dipaparkan / tersembunyi dalam panel **AVG Security Toolbar**:

- **Butang Berita AVG** - opsyen ini memaparkan butang **Berita AVG**. Menekan butang dalam panel **AVG Security Toolbar** anda boleh membuka menu jatuh ke bawah dengan pautan kepada siaran akhbar berkaitan AVG yang terkini.
- **Butang Maklumat AVG** - butang **Maklumat AVG** membuka menu





dengan opsyen berikut:

- *Maklumat Bar Alat* - membuka halaman produk **AVG Security Toolbar** dengan maklumat terperinci pada komponen
 - *Mengenai Ancaman* - membuka halaman web lab virus AVG dengan maklumat mengenai ancaman semasa, pengesyoran pembuangan virus, senarai Soalan Lazim, dll.
 - *Berita AVG* - membuka halaman web yang memberikan siaran akhbar berkaitan AVG yang terkini
 - *Tahap Ancaman Semasa* - membuka halaman web virus dengan paparan bergraf bagi tahap ancaman semasa pada web
 - *Ensiklopedia Virus* - membuka halaman Ensiklopedia Virus di mana anda boleh mencari virus tertentu melalui nama dan mendapat maklumat terperinci pada setiap satu
- **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**.

- **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** - tanda item ini untuk mengaktifkan atau mematikan perkhidmatan **AVG Search-Shield** dan/atau **AVG Active Surf-Shield**
- **Pengadaran** - pilih simbol grafik yang digunakan untuk pengadaran hasil carian melalui komponen **AVG Search-Shield** yang anda hendak gunakan:
 -  halaman adalah selamat
 -  halaman agak mencurigakan
 -  halaman mengandungi pautan kepada halaman berbahaya secara positif
 -  halaman mengandungi ancaman aktif

-  halaman tidak boleh diakses, maka, tidak boleh diimbas

Tandakan opsiyen 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.***

• Opsyen Lanjutan



Pada tab ***Opsyen Lanjutan*** anda boleh mengaktifkan atau mematikan tetapan ***AVG Security Toolbar*** selanjutnya:

- ***Tetapkan dan kekalkan Yahoo! sebagai pembekal carian untuk bar Alamat*** - (*dihidupkan secara lalai*) - jika ditandakan, opsiyen ini membenarkan anda menaip kata kunci carian secara terus ke dalam bar alamat ke dalam pelayar Internet anda dan perkhidmatan Yahoo! akan digunakan secara automatik untuk mencari tapak web yang relevan.
- ***Tunjukkan Yahoo! kotak carian pada tab baru dalam pelayar*** - (

dihidupkan secara lalai) - jika ditandakan, opsyen ini memaparkan Yahoo! Kotak carian dalam setiap tab pelayar Internet yang dibuka.

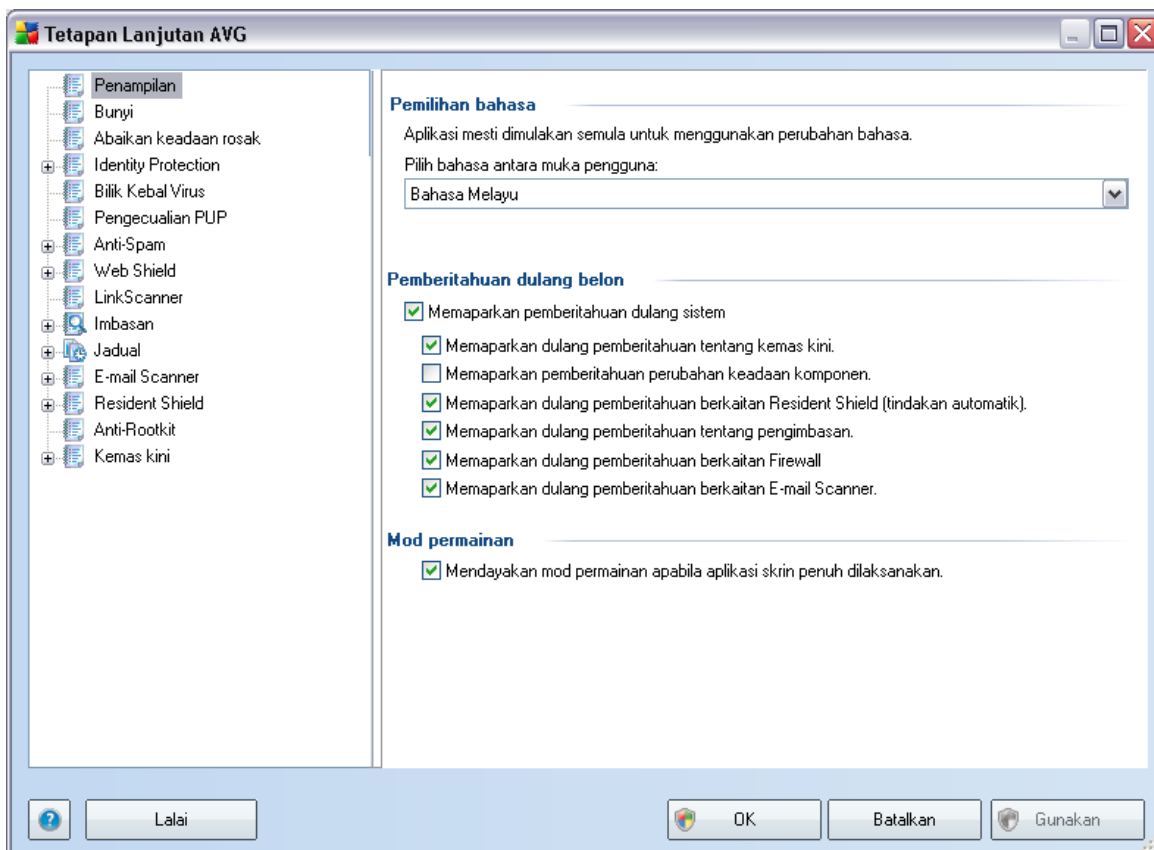
- **Biarkan AVG membuat cadangan pada ralat navigasi pelayar (404/DNS)** - (*dihidupkan secara lalai*) - jika semasa mencari web yang anda jalankan ke dalam halaman tidak wujud atau halaman yang tidak boleh dipaparkan (*ralat 404*), **AVG Security Toolbar** akan menawarkan gambaran keseluruhan halaman berkaitan topik alternatif.
- **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 semua dalam tempoh masa satu minggu.

9. Tetapan Lanjutan AVG

Dialog konfigurasi lanjutan bagi **AVG 9 Anti-Virus plus Firewall** membuka tettingkap 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 tertentunya*) untuk membuka dialog pengeditan dalam bahagian kanan tettingkap.

9.1. Penampilan

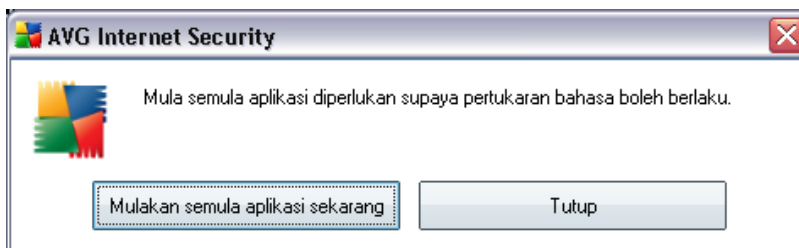
Item pertama bagi pepohon navigasi, **Penampilan**, merujuk kepada tetapan umum bagi [antara muka pengguna AVG](#) dan beberapa pilihan permulaan bagi kelakukan aplikasi:



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 jatuh ke bawah 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 pemberitahuannya atau anda hendak hanya pemberitahuan tertentu (berkaitan dengan komponen AVG khusus) dipaparkan, anda boleh mentakrifkan dan menentukan keutamaan anda dengan menanda/tidak menanda opsi berikut:

- **Paparkan pemberitahuan dulang sistem** - secara lalai, item ini ditanda (*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:

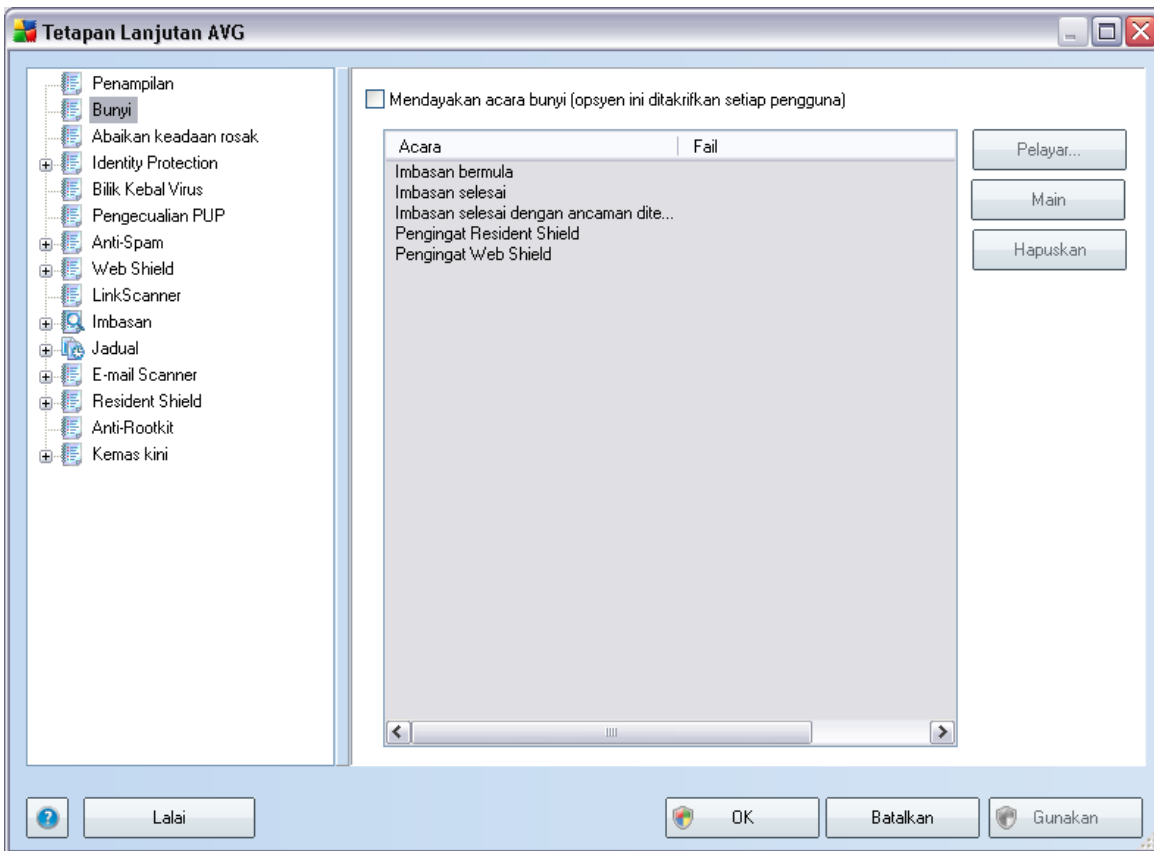
- **Paparkan pemberitahuan dulang mengenai kemas kini** - tentukan sama ada maklumat berkenaan pelancaran proses, perkembangan dan penyelesaian kemas kini AVG harus dipaparkan;
- **Paparkan pemberitahuan perubahan keadaan komponen** - tentukan sama ada maklumat berkenaan keaktifan/ketidaktifan komponen atau kemungkinan masalahnya harus dipaparkan. Semasa melaporkan status kerosakan komponen, opsi ini sama dengan fungsi berguna bagi ikon dulang sistem (perubahan warna) melaporkan sebarang masalah dalam sebarang komponen AVG;
- **Paparkan pemberitahuan dulang berkaitan dengan Perisai Residen** - tentukan sama ada maklumat berkenaan menyimpan, menyalin fail dan membuka proses harus dipaparkan atau dihipit;
- **Paparkan pemberitahuan dulang mengenai pengimbasan** - tentukan sama ada maklumat pada pelancaran automatik bagi imbasan yang dijadualkan, perkembangan dan keputusannya harus dipaparkan;
- **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;
- **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 yang perlu berkomunikasi pada Internet dan kemungkinan dialog pertanyaan AVG akan menjejaskan aplikasi (*kecilkannya atau rosakkan grafiknya*). Untuk mengelakkan situasi ini, pastikan kotak semakan untuk pilihan **Dayakan mod permainan semasa aplikasi skrin penuh dijalankan** ditandakan (*tetapan lalai*).

9.2. Bunyi

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

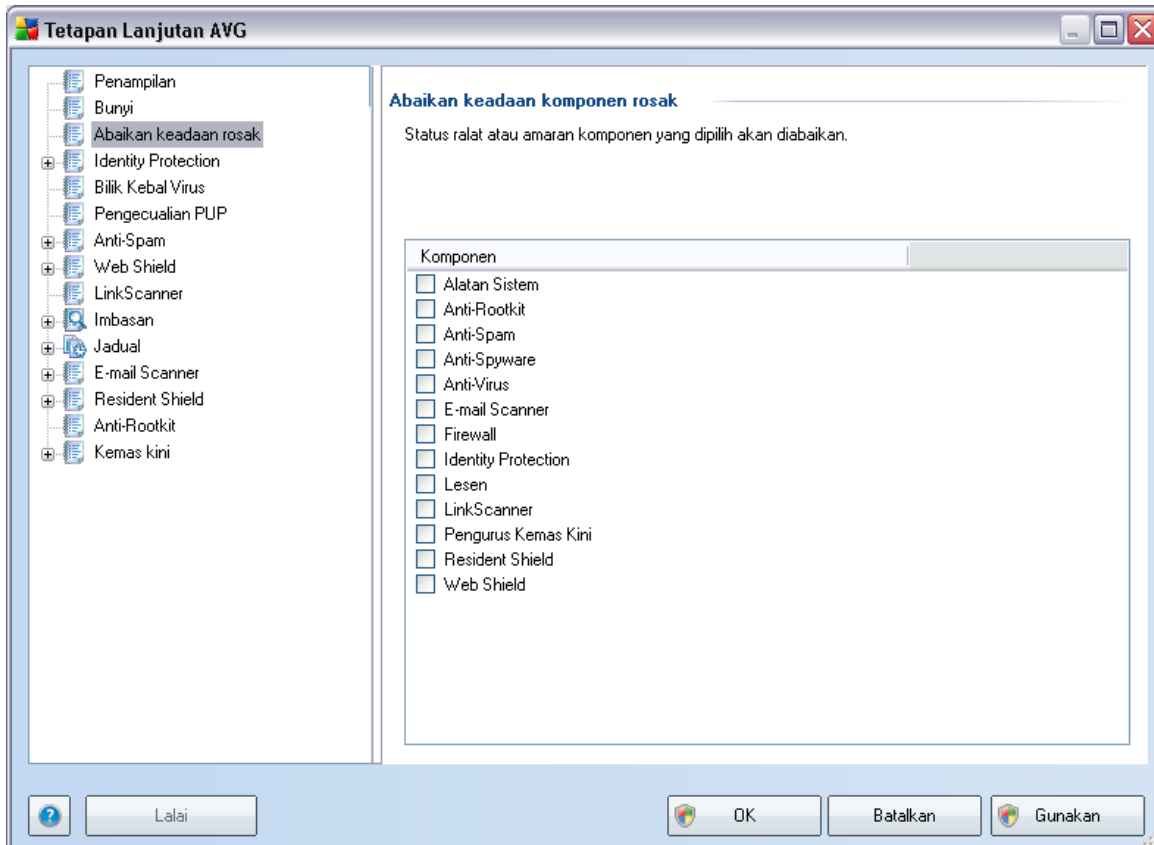


Kemudian, pilih peristiwa tersebut daripada senarai dan semak imbas (**Semak imbas**) cakera anda untuk bunyi yang sesuai yang anda hendak peruntukkan kepada peristiwa ini. Untuk mendengar bunyi yang dipilih, serlahkan peristiwa dalam senarai dan tekan butang **Main**. Gunakan butang **Padam** untuk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

Nota: Hanya bunyi *.wav yang disokong!

9.3. 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:

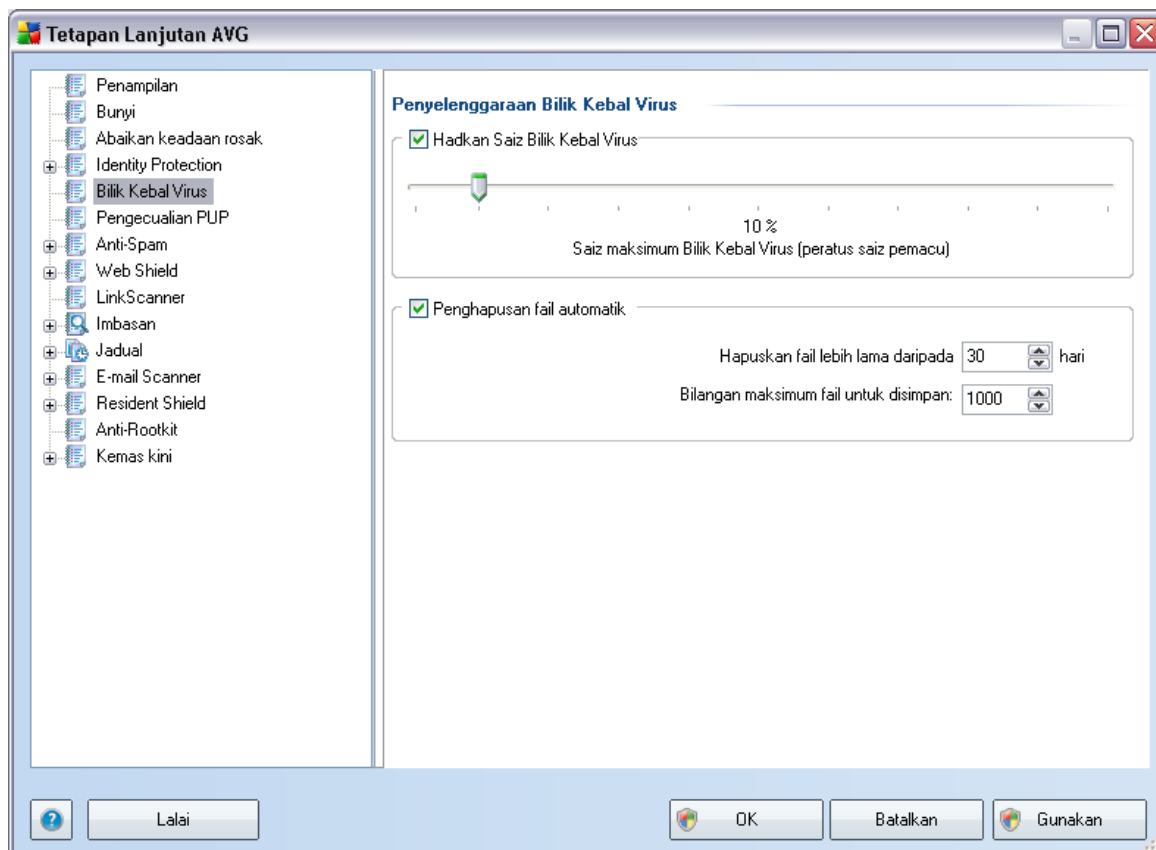
- **ikon dulang sistem** - semasa semua bahagian AVG bekerja dengan betul, ikon dipaparkan dalam empat warna; walau bagaimanapun, jika ralat berlaku, ikon muncul dengan tanda seruan berwarna kuning,
- penerangan teks bagi masalah sedia ada dalam bahagian **Maklumat Status Keselamatan** bagi tettingkap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

9.4. Bilik Kebal Virus



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

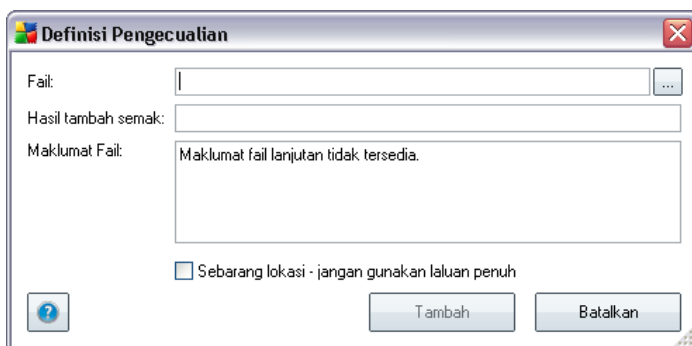
- **Hadkan saiz Bilik Kebal Virus** - gunakan gelangсар untuk menyediakan saiz maksimum bagi **Bilik Kebal Virus**. Saiz tersebut ditentukan mengikut perkadaran dibandingkan dengan saiz cakera setempat anda.
- **Pemadaman fail automatik** - dalam bahagian ini menentukan tempoh masa maksimum bagi objek 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***)

9.5. Kekecualian PUP

AVG 9 Anti-Virus plus Firewall boleh menganalisis dan mengesan aplikasi boleh laku atau perpustakaan DLL yang 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:

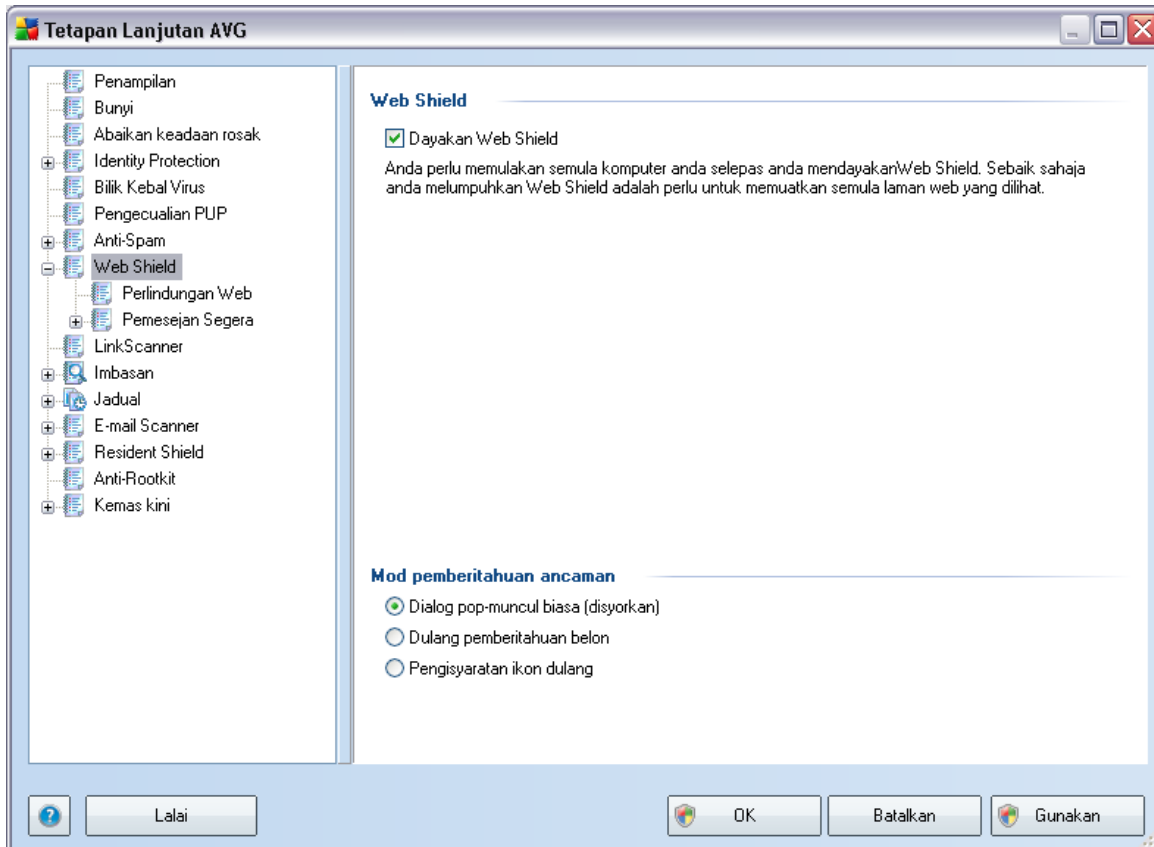
Butang kawalan

- **Edit** - membuka dialog pengeditan (*sama dengan dialog untuk definisi pengecualian baru, lihat di bawah*) bagi pengecualian yang telah ditentukan di mana anda boleh mengubah parameter pengecualian
- **Buang** - memadam item yang dipilih dari senarai pengecualian
- **Tambah pengecualian** - membuka dialog pengeditan di mana anda boleh menentukan parameter bagi pengecualian baru yang akan dibuat:



- **Fail** - taipkan laluan penuh ke fail yang anda ingin tandakan sebagai pengecualian
- **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.
- **Maklumat Fail** - memaparkan sebarang maklumat tambahan yang tersedia mengenai fail (*maklumat lesen/versi dll.*)
- **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

9.6. Perisai Web



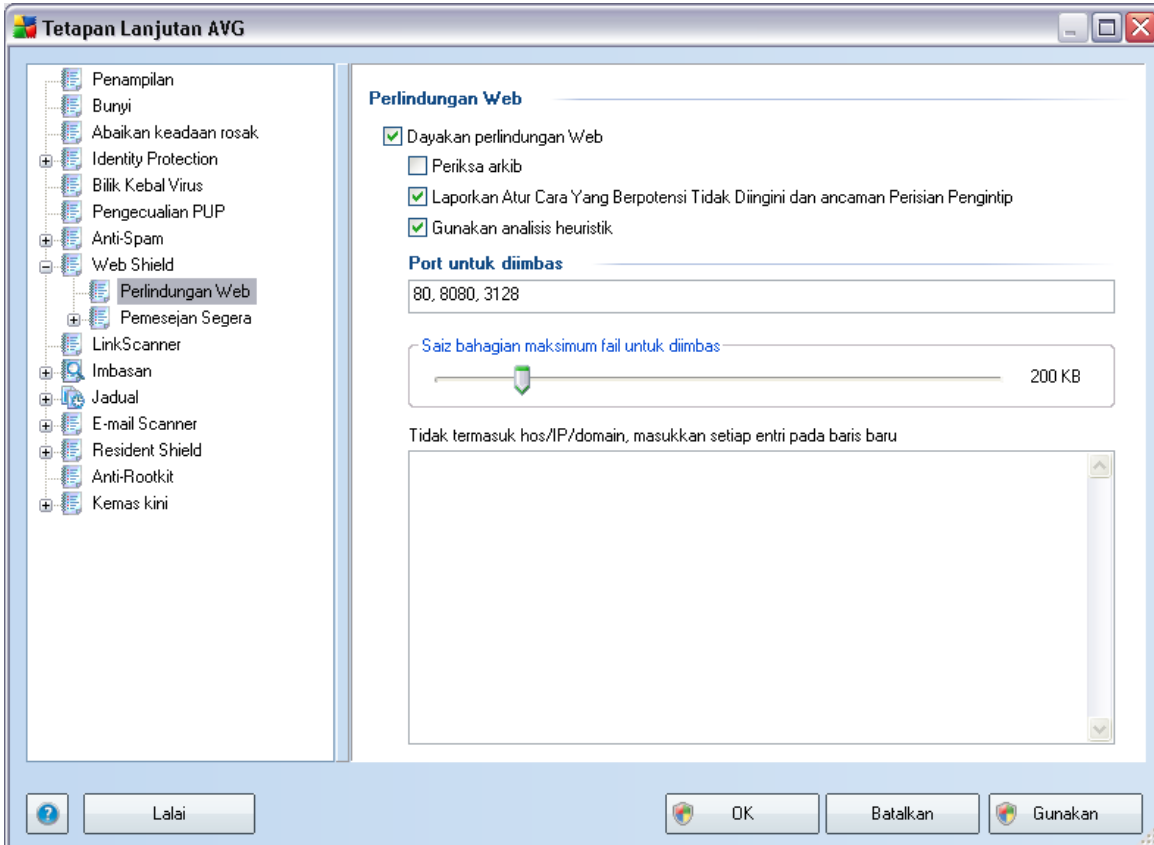
Dialog **Perlindungan Web** membenarkan anda mengaktifkan/menyahaktifkan seluruh komponen **Perisai Web** melalui opsyen **Dayakan Perisai Web** (*diaktifkan secara lalai*). Untuk tetapan lanjutan seterusnya bagi komponen ini, sila teruskan ke dialog berikutnya seperti yang disenaraikan dalam navigasi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

9.6.1. Perlindungan Web



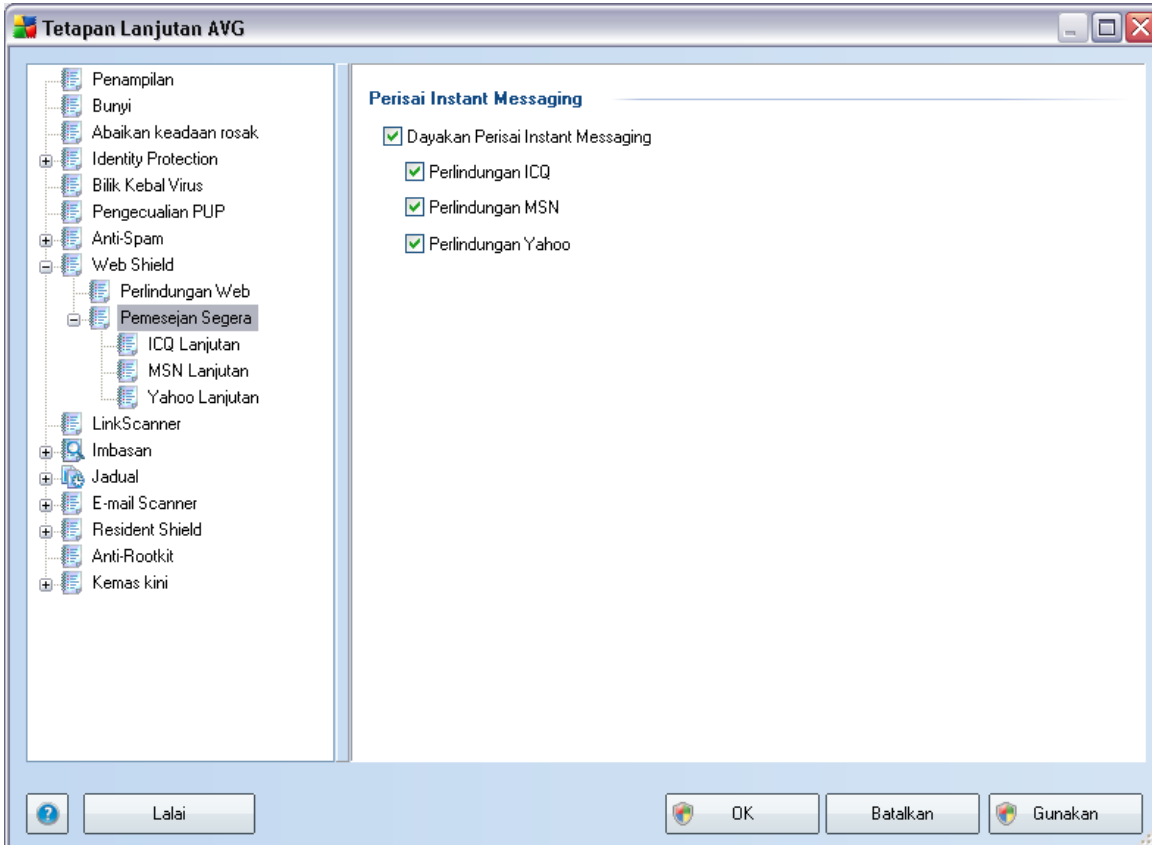
Dalam dialog **Perlindungan Web** anda boleh mengedit konfigurasi komponen berkenaan imbasan kandungan tapak web. Antara muka penyuntingan ini membenarkan anda untuk mengkonfigurasi opsyen permulaan berikut:

- **Dayakan perlindungan Web** - opsyen ini mengesahkan bahawa **Perisai Web** patut melakukan pengimbasan 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.
 - **Imbas Atur Cara Yang Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip** - imbas atur cara yang berpotensi tidak dikehendaki (*atur cara boleh laku yang boleh dijalankan sebagai perisian*

pengintip atau adware) termasuk dalam halaman www untuk dipaparkan, dan jangkitan [perisian pengintip](#).

- **Gunakan analisis heuristik** - imbas kandungan halaman untuk dipaparkan menggunakan kaedah [analisis heuristik](#) (*persaingan dinamik bagi arahan objek yang dikesan dalam persekitaran komputer maya*).
- **Port untuk diimbis** - medan ini menyenaraikan nombor port komunikasi http standard. Jika konfigurasi komputer anda berbeza, anda boleh mengubah nombor port seperti yang diperlukan.
- **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 fail yang masih perlu diimbis dengan [Perisai Web](#). Walaupun, jika fail yang dimuat turun adalah lebih besar daripada yang ditentukan, dan oleh itu, tidak akan diimbis dengan Perisai Web, anda masih dilindungi: jika fail dijangkiti, [Perisai Residen](#) akan mengesannya dengan sertamerta.
- **Tidak memasukkan hos/IP/domain** - dalam medan teks anda boleh menaip nama sebenar pelayan (*hos, alamat IP, alamat IP dengan topeng atau URL*) atau domain yang tidak perlu diimbis oleh [Perisai Web](#). Oleh itu, hanya kecualikan hos yang anda betul-betul pasti tidak akan memberikan kandungan tapak web berbahaya.

9.6.2. Pemesejan Segera

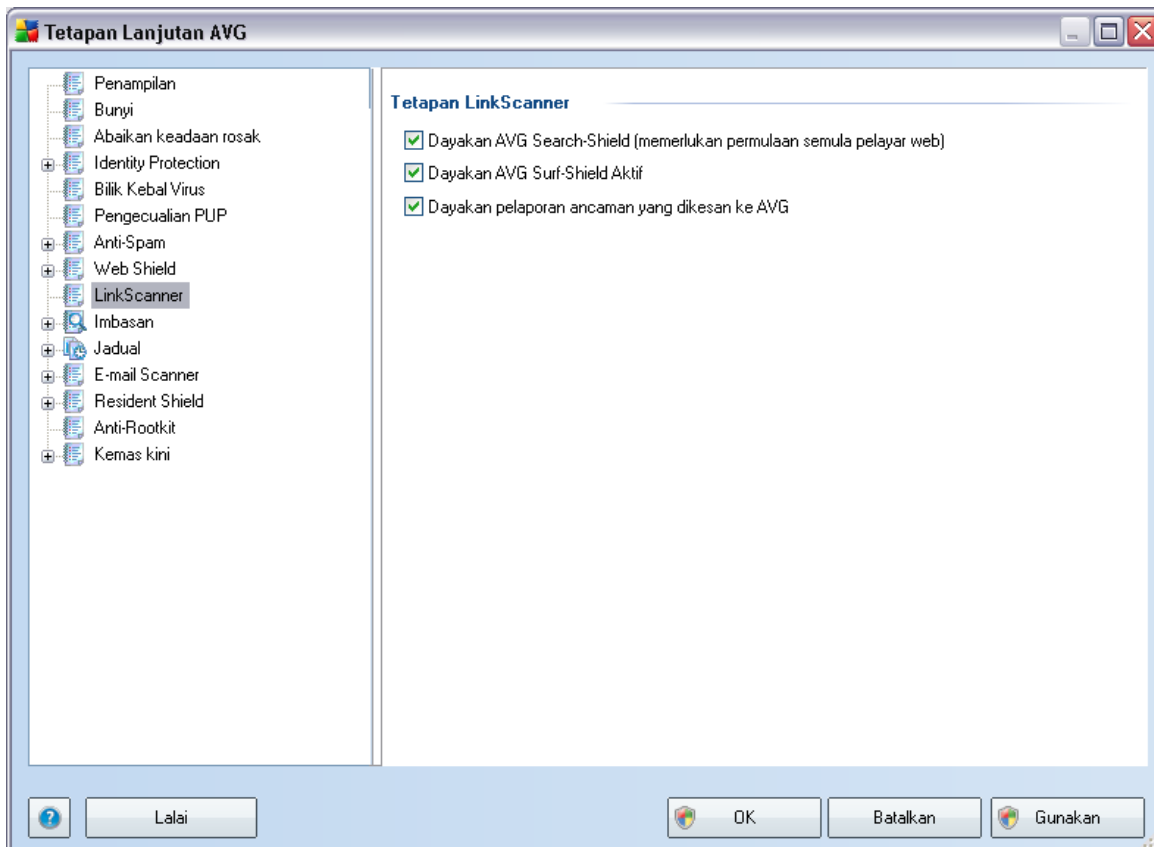


Dalam dialog **Perisai Pemesejan Segera** anda boleh mengedit tetapan komponen **Perisai Web** yang merujuk kepada pengimbasan pemesejan segera. Buat masa ini, tiga atur cara pemesejan segera berikut disokong: **ICQ**, **MSN** dan **Yahoo** - tandakan rait item masing-masing untuk setiap satu daripadanya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

Untuk pengkhususan selanjutnya bagi pengguna yang dibenarkan/disekat, anda boleh melihat dan mengedit dialog tersebut (**ICQ Lanjutan**, **MSN Lanjutan**, **Yahoo Lanjutan**) dan tentukan senarai **Senarai Putih** (pengguna yang akan dibenarkan untuk berkomunikasi dengan anda) dan **Senarai Hitam** (pengguna yang sepatutnya diseekat).

9.7. Pengimbas Pautan

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



- **Dayakan AVG Search-Shield** - (*dihidupkan secara lalai*): ikon pemberitahuan penasihat pada carian yang dilakukan dalam Google, Yahoo, MSN atau Baidu diperiksa dahulu kandungan tapak yang dikembalikan 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.

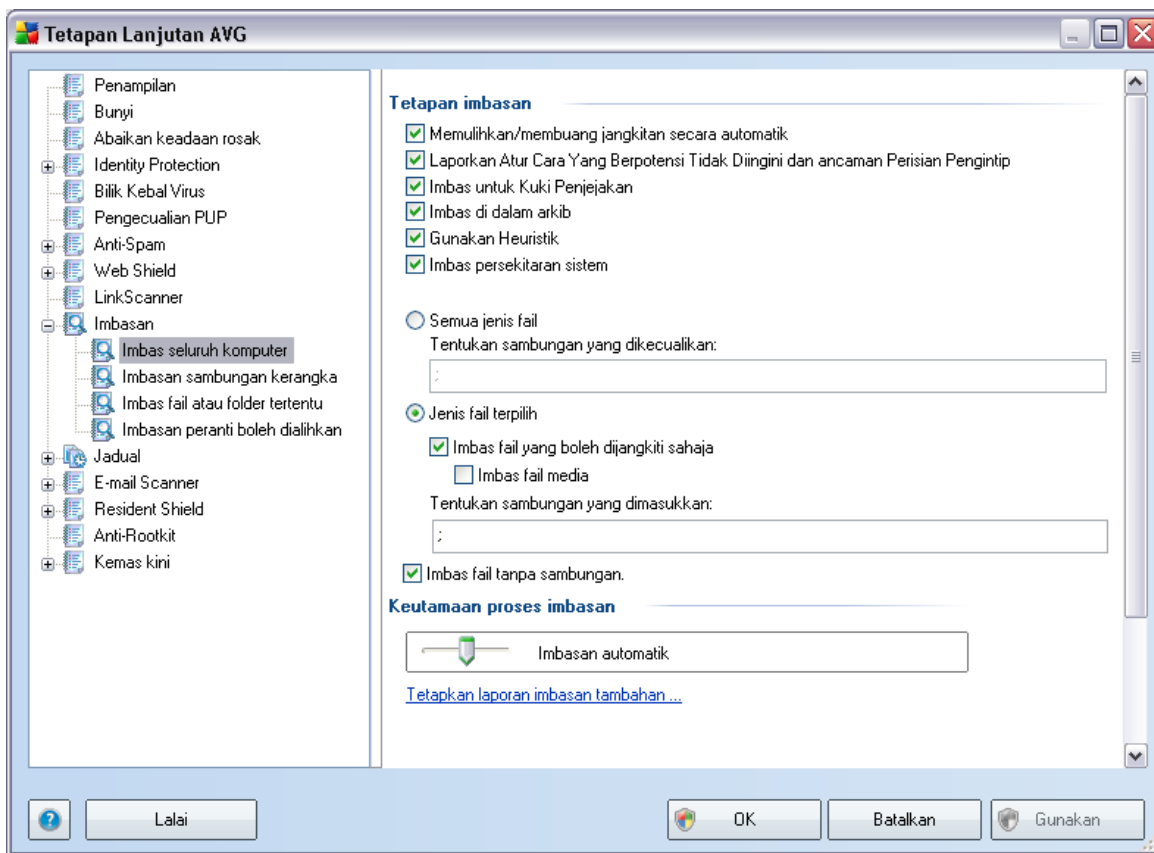
9.8. Imbasan

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

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

9.8.1. Imbas Seluruh Komputer

Opsyen **Imbas seluruh komputer** membenarkan anda mengedit parameter bagi salah satu imbasan yang dipraktifikkan 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, atau jika anda memutuskan untuk mematikan opsyen ini, anda akan diberitahu mengenai pengesanan virus dan perlu memutuskan apa yang perlu dilakukan dengan jangkitan yang dikesan. Kaedah yang disyorkan adalah untuk membuang fail yang dijangkiti ke [Bilik Kebal Virus](#).
- **Laporkan Atur Cara dan Ancaman Perisian Pengintip yang Berpotensi Tidak Dikehendaki** - parameter ini mengawal kefungsi [AntiVirus](#) yang membenarkan [pengesanan atur cara yang berpotensi tidak dikehendaki](#) (*fail*)

boleh laku yang boleh dijalankan sebagai perisian pengintip atau adware) dan ini boleh disekat atau dibuang;

- **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 ditentukan dari pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan oleh koma yang harus diimbas; atau
- **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.

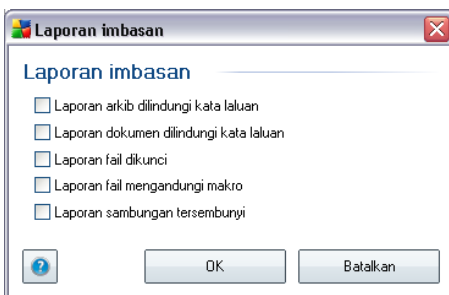
Keutamaan proses imbasan

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.

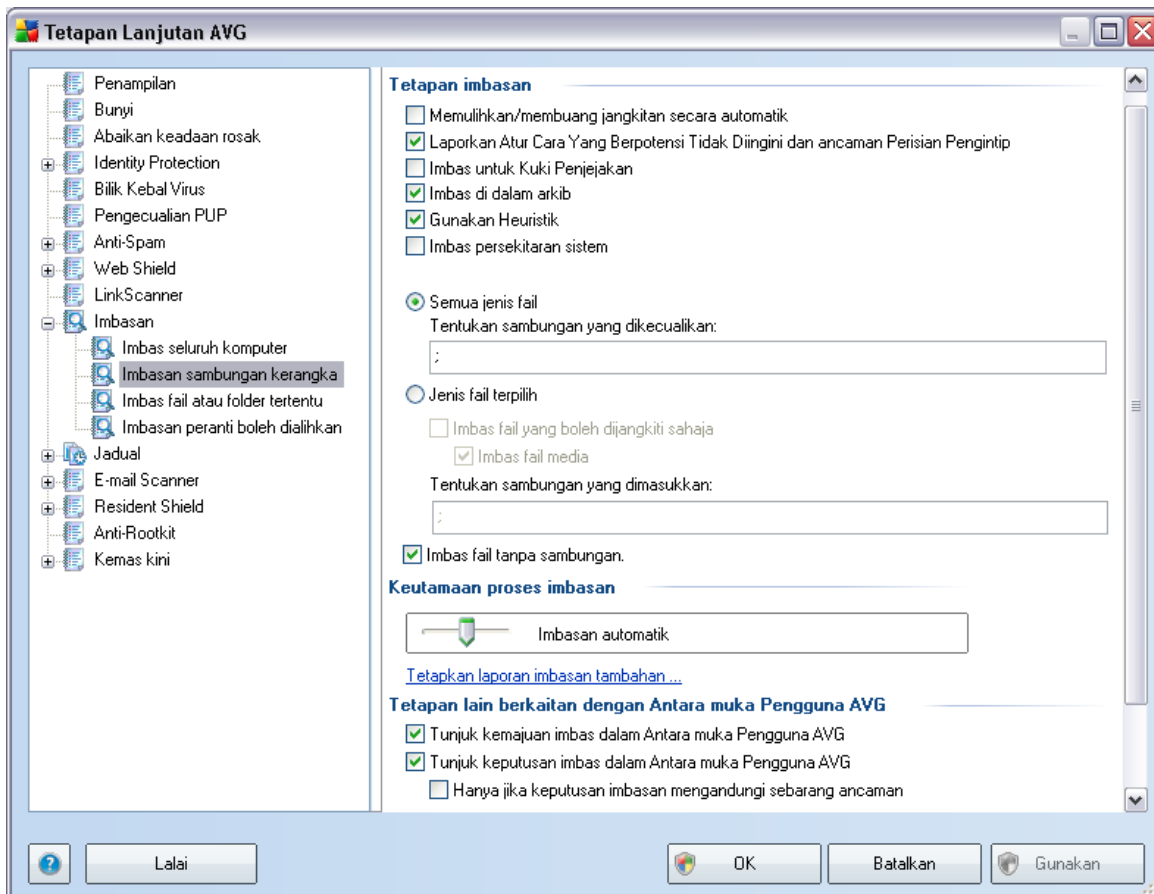
Tetapkan laporan imbasan tambahan ...

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



9.8.2. 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***:

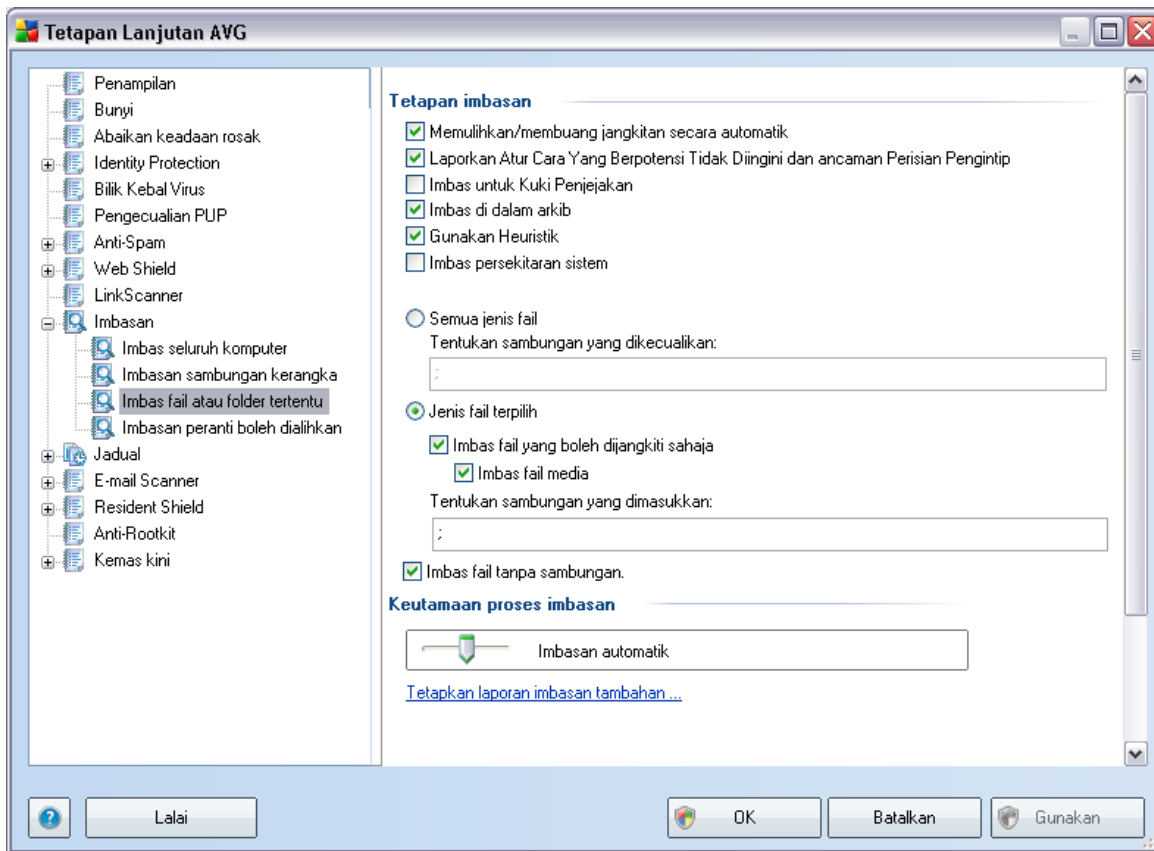


Senarai parameter adalah sama dengan yang tersedia untuk **Imbas seluruh komputer**. Walau bagaimanapun, tetapan lalai berbeza: dengan ***Imbas Seluruh Komputer*** kebanyakan parameter dipilih sementara untuk ***Imbasan sambungan kerangka*** (**Mengimbas dalam Windows Explorer**) hanya parameter yang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

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

9.8.3. Imbas Fail atau Folder Tertentu

Antara muka pengeditan untuk ***Imbas fail atau folder tertentu*** adalah sama dengan dialog pengeditan **Imbas Seluruh Komputer**. Semua opsi konfigurasi adalah sama; walau bagaimanapun, tetapan lalai adalah lebih tegas untuk **Imbas seluruh komputer**:

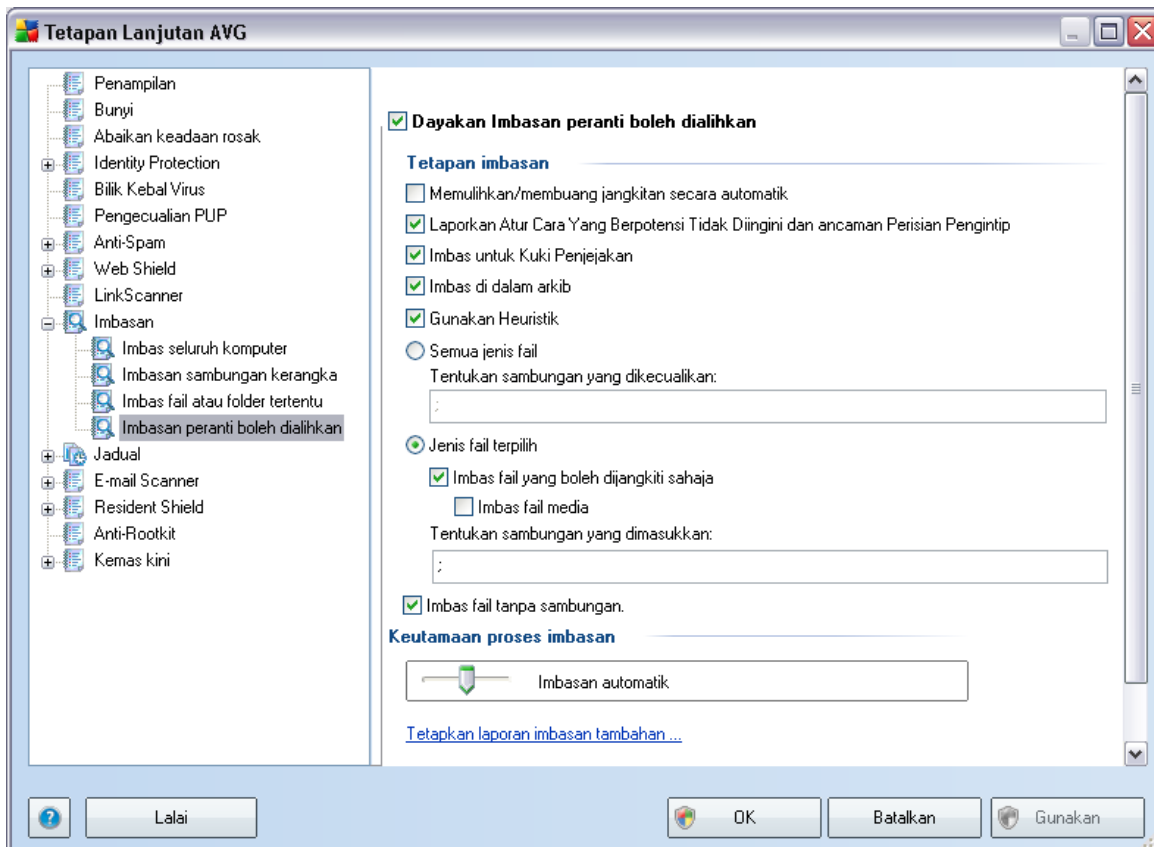


Semua parameter yang disediakan dalam dialog konfigurasi ini hanya digunakan pada kawasan yang dipilih untuk imbasan dengan **Imbas fail atau folder tertentu!** Jika anda menanda rait opsyen **Imbas untuk rootkit** dalam dialog konfigurasi ini, hanya ujian rootkit pantas akan dilakukan, cth. imbasan rootkit bagi kawasan yang dipilih sahaja.

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

9.8.4. 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**.

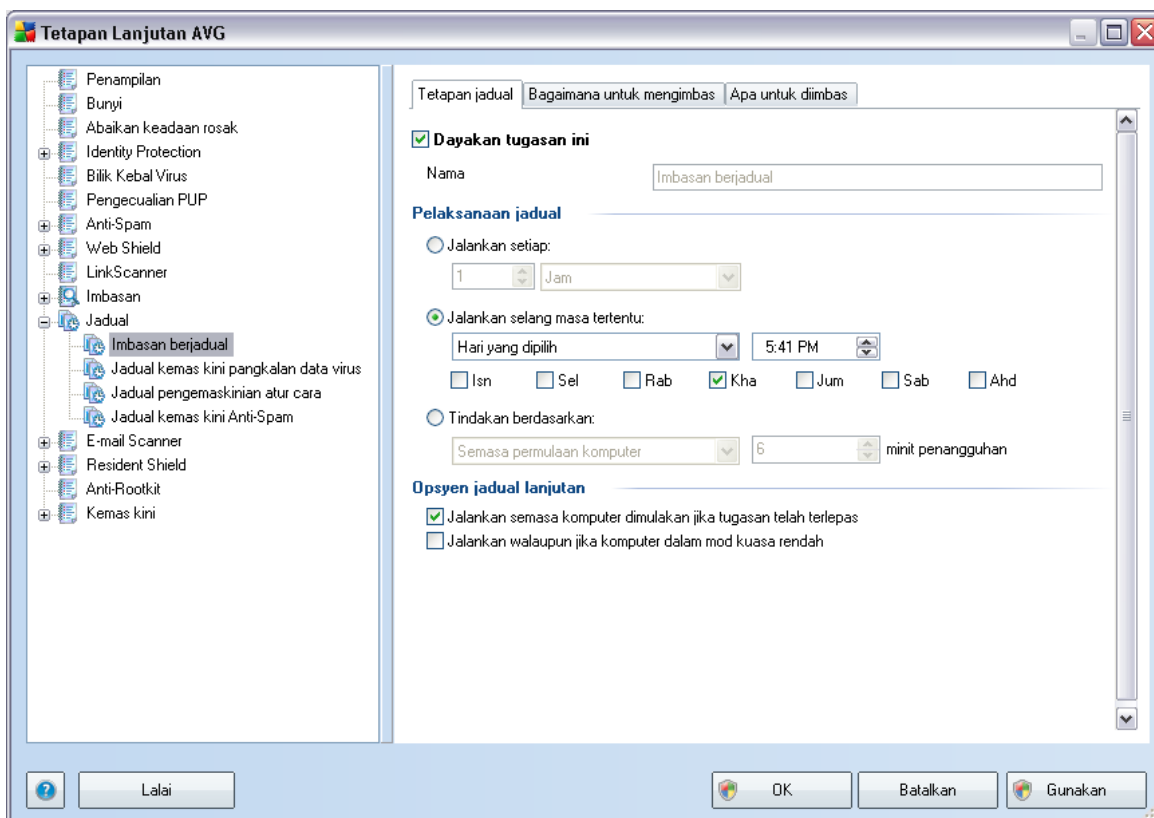
9.9. Jadual

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

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

9.9.1. Imbasan yang Dijadualkan

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



Pada tab **Jadualkan tetapan** anda boleh menanda/menyah Tandakan dahulu item

Dayakan tugas ini untuk menyahaktifkan ujian yang dijadualkan buat sementara dan menghidupkannya semua apabila perlu.

Seterusnya, dalam medan teks yang 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:

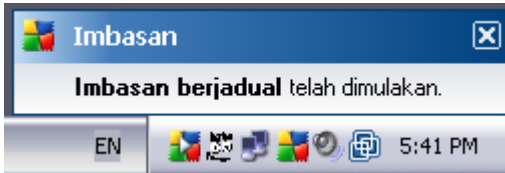
Pelaksanaan jadual

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

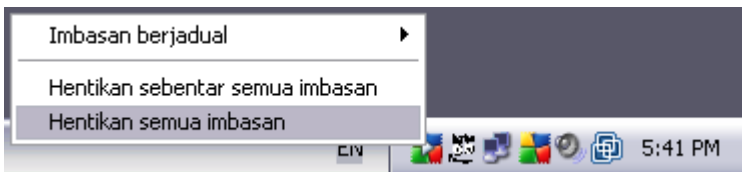
Opsyen jadual lanjutan

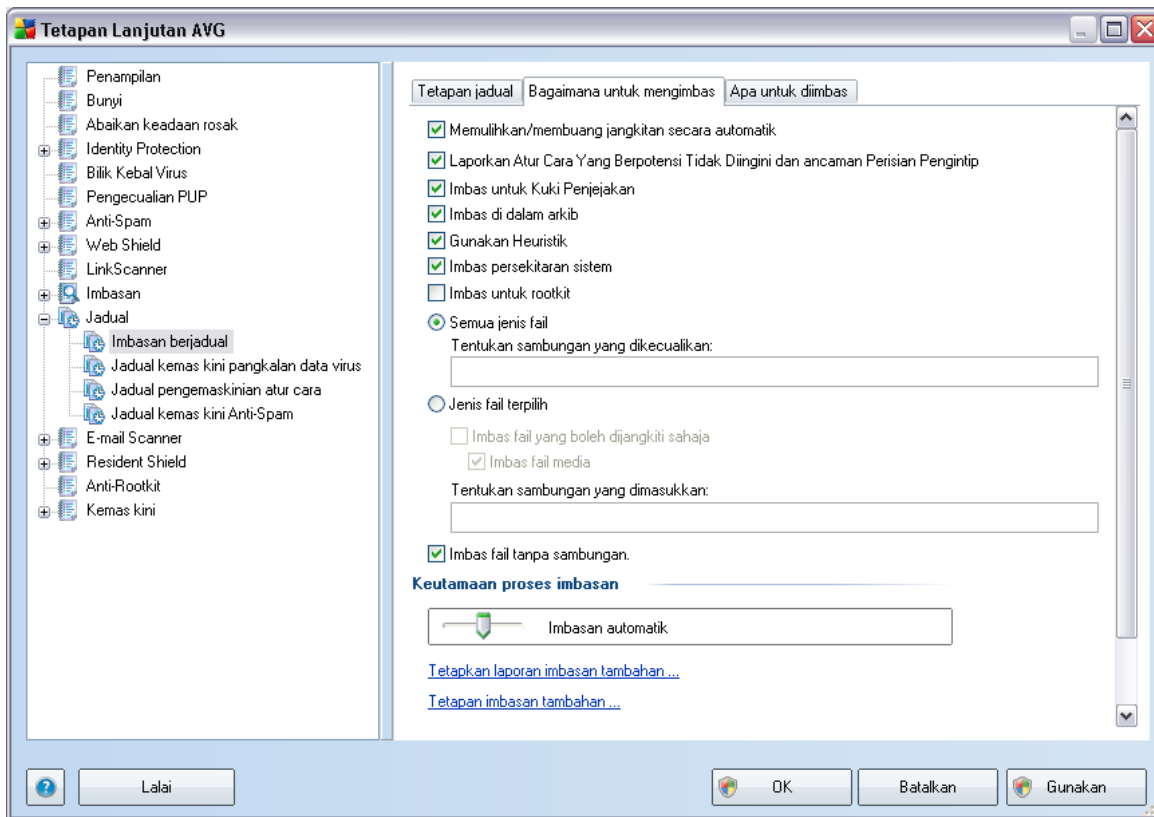
Bahagian ini membenarkan anda untuk mentakrifkan di bawah keadaan mana imbasan patut/tidak patut dilancarkan jika komputer di dalam mod kuasa rendah atau dimatikan sepenuhnya.

Apabila imbasan yang dijadualkan telah dilancarkan dalam masa yang telah ditentukan, anda akan diberitahu mengenai fakta ini melalui tettingkap 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*** - (*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 opsyen 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 Potensi Atur Cara yang Tidak Dikehendaki dan ancaman Perisian Pengintip*** - (*dihidupkan secara lalai*): parameter ini mengawal

kefungsian [AntiVirus](#) yang membenarkan [pengesanan atur cara yang berpotensi tidak dikehendaki](#) (*fail boleh laku yang boleh dijalankan sebagai perisian pengintip atau adware*) dan kemudian, ini boleh disekat atau dibuang;

- **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 diimbis 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

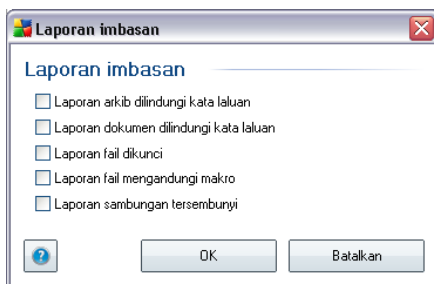
- **Semua jenis fail** dengan kemungkinan pengecualian yang ditentukan dari pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan oleh koma yang harus diimbis; atau
- **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*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.

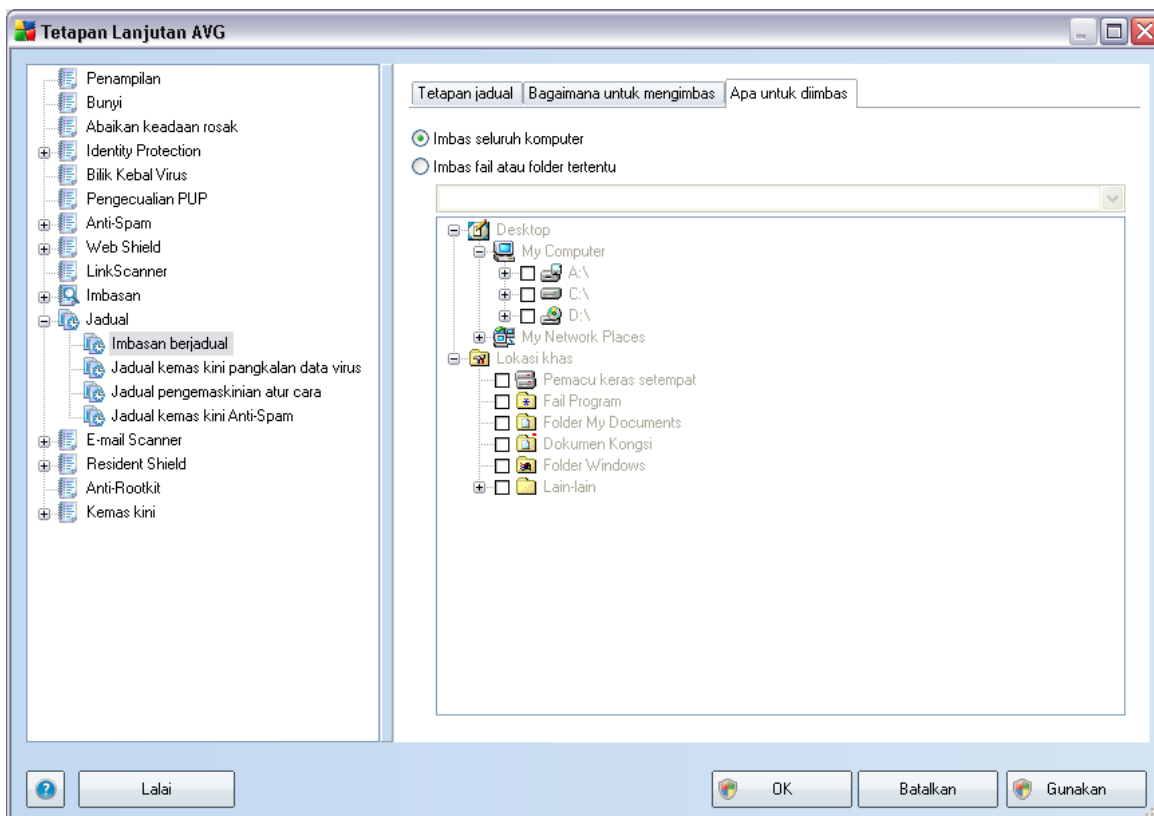
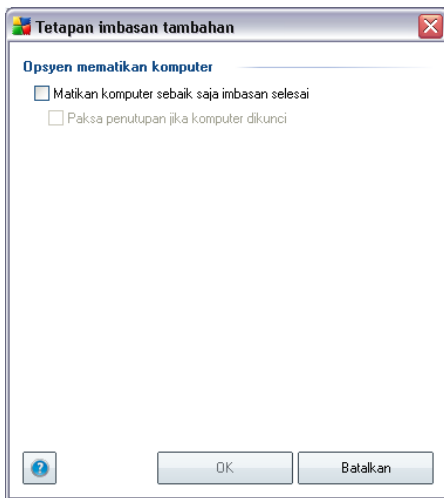
Keutamaan proses imbasan

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

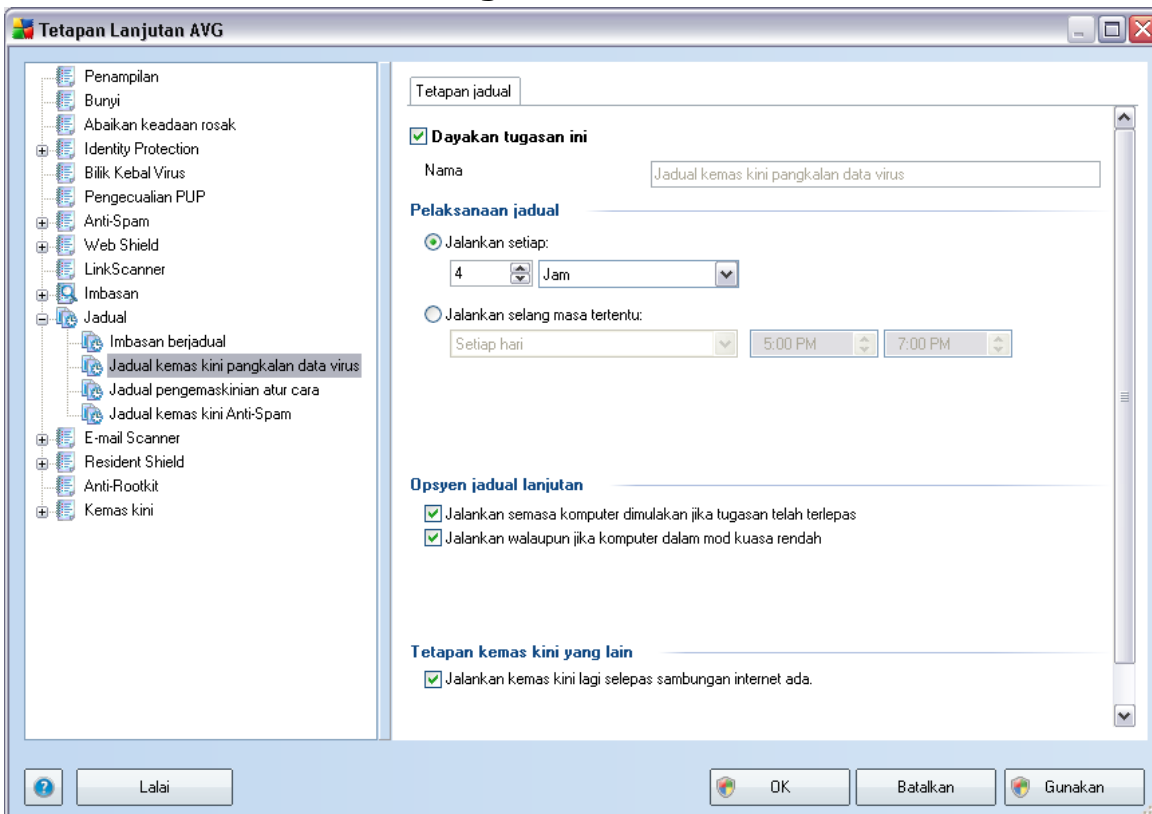


Klik **Tetapan imbasan tambahan ...** untuk membuka dialog **Opsyen mematikan komputer** lain di mana anda boleh menentukan sama ada komputer harus dimatikan secara automatik sebaik sahaja proses pengimbasan yang berjalan tamat. Dengan mengesahkan opsyen ini akan (**Mematikan komputer apabila selesai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



Pada tab ***Apa yang hendak diimbis*** 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 diimbis.

9.9.2. 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*** (*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 pada item **Jadual kemas kini pangkalan data virus** dalam pepohon navigasi kiri*) anda boleh menentukan nama anda sendiri dan jika medan teks akan dibuka untuk pengeditan. Sentiasa cuba gunakan nama yang ringkas, deskriptif dan sesuai untuk jadual anda untuk menjadikannya mudah untuk mengenal pastinya kemudian.

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 tempoh masa tertentu (***Jalankan setiap ...***) atau dengan mentakrifkan tarikh dan masa sebenar (***Jalankan pada masa tertentu ...***), atau kemungkinan dengan mentakrifkan peristiwa pelancaran kemas kini yang patut dikaitkan dengan (***Tindakan berdasarkan pada permulaan komputer***).

Opsyen jadual lanjutan

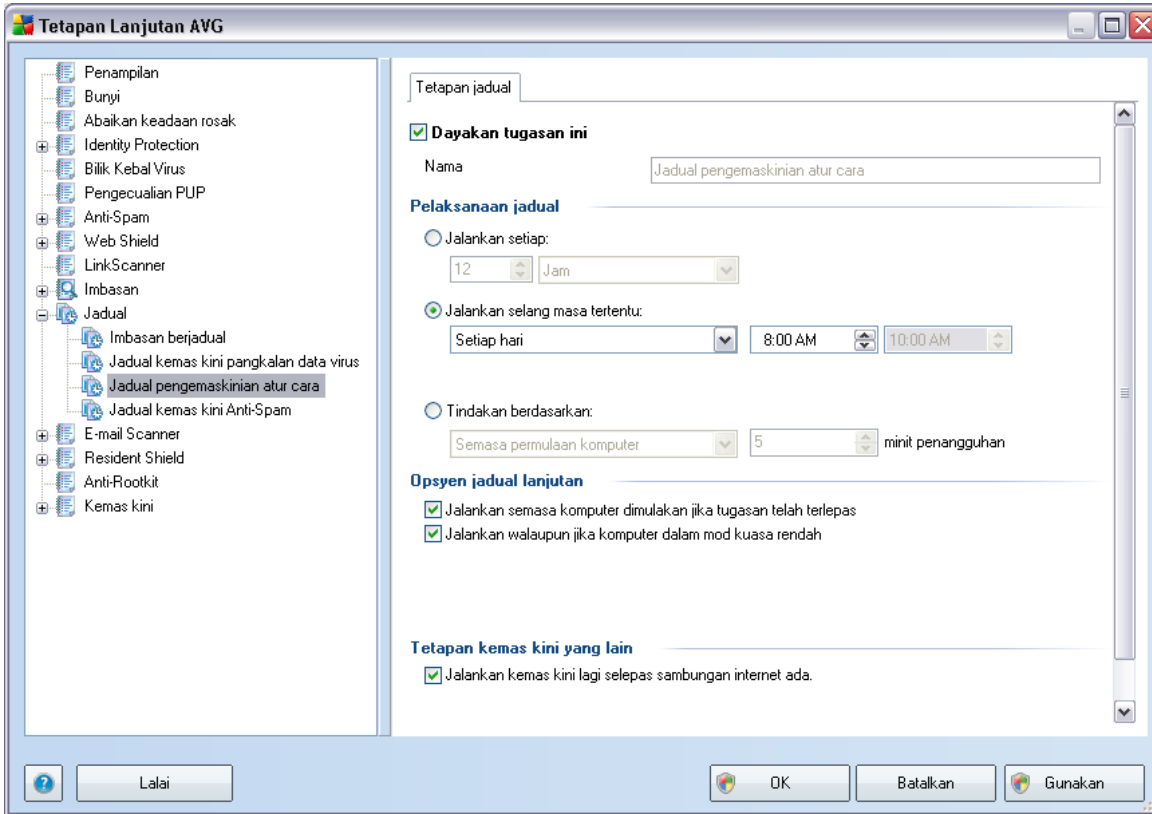
Bahagian ini membenarkan anda mentakrifkan di bawah keadaan mana kemas kini pangkalan data virus harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

Tetapan kemas kini yang lain

Akhir sekali, tandakan opsyen ***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 dalam masa yang anda tentukan, anda akan diberitahu mengenai kenyataan ini melalui tettingkap pop timbul yang dibuka pada [ikon dulang sistem AVG](#) (*yang diberikan yang anda telah kekalkan konfigurasi lalai bagi dialog **Tetapan/Penampilan Lanjutan***).

9.9.3. Jadual Kemas Kini Atur Cara



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. Untuk jadual yang baru ditambah (*anda boleh menambah jadual baru dengan mengklik kanan tetikus pada item **Jadual kemas kini atur cara** dalam pepohon navigasi kiri*) anda boleh menentukan nama anda sendiri dan dalam kes itu, medan teks akan dibuka untuk pengeditan. Sentiasa cuba gunakan nama yang ringkas, deskriptif dan sesuai untuk jadual anda untuk menjadikannya mudah untuk mengenal pastinya kemudian.

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

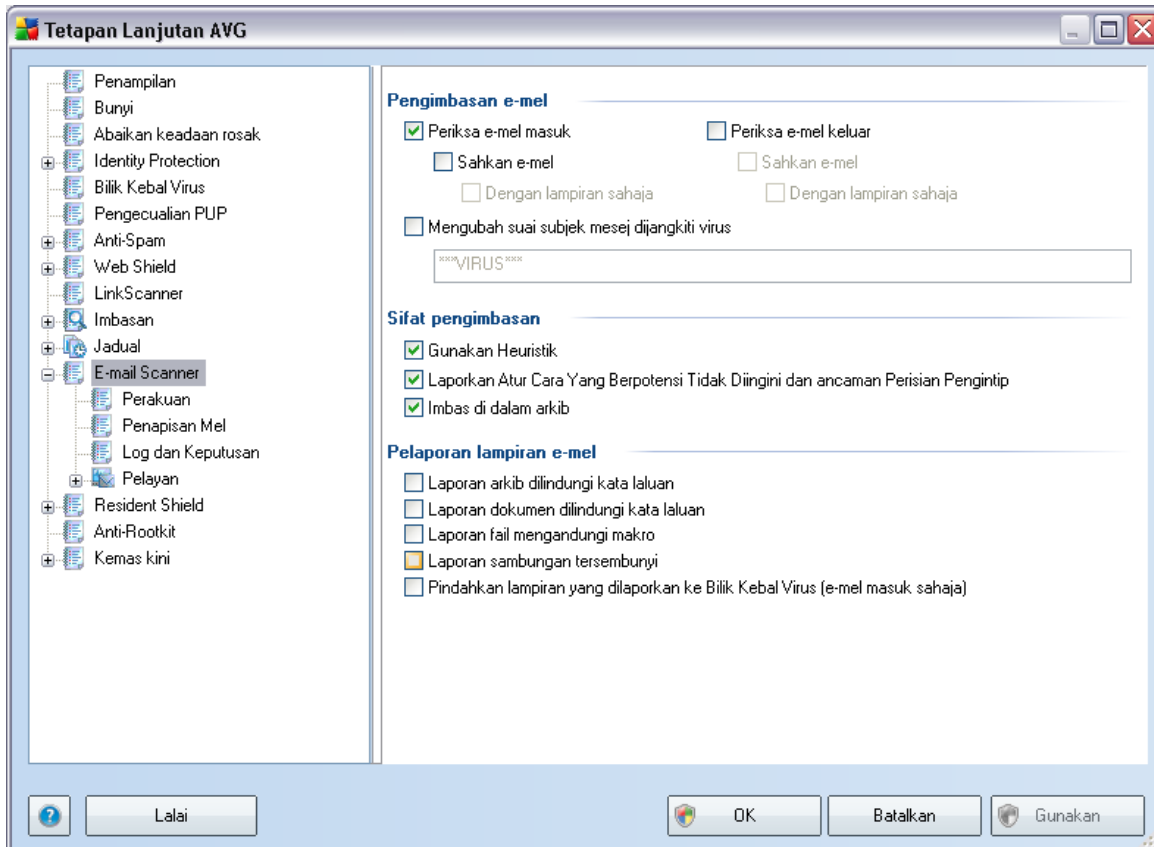
Bahagian ini membenarkan anda menentukan dalam keadaan apa kemas kini atur cara harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

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 dalam masa yang anda tentukan, anda akan diberitahu mengenai kenyataan ini melalui tettingkap pop timbul yang dibuka pada [ikon dulang sistem AVG](#) (yang diberikan yang anda telah kekalkan konfigurasi lalai bagi dialog ***Tetapan/Penampilan Lanjutan***).

9.10. Pengimbas E-mel



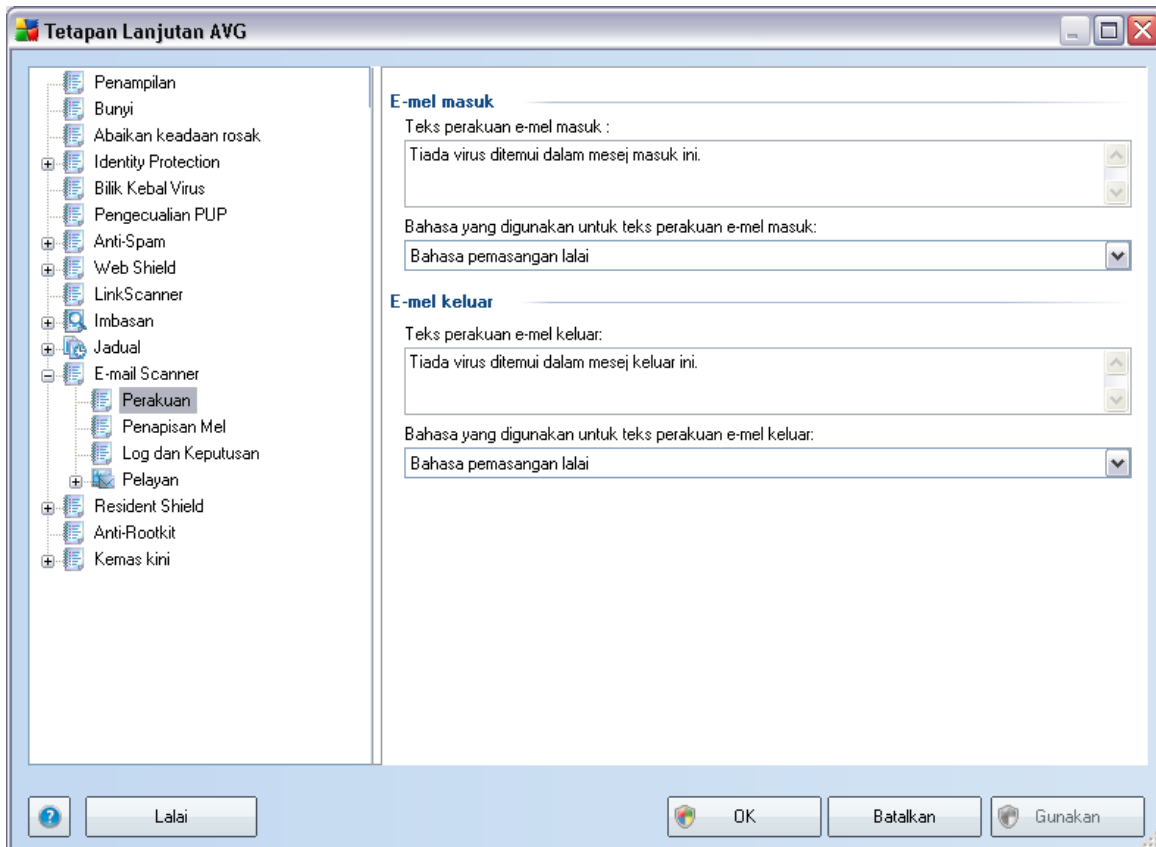
Dialog **Pengimbas E-mel** dibahagikan ke dalam tiga bahagian:

- **Pengimbasan e-mel** - dalam bahagian ini, pilih sama ada anda mahu mengimbas mesej e-mel masuk/keluar dan sama ada semua e-mel harus diperakui atau hanya e-mel dengan lampiran (perakuan *e-mel bebas virus tidak disokong dalam format HTML/RTF*). Secara tambahan, anda boleh memilih jika anda mahu AVG mengubah suai subjek untuk mesej yang mengandungi potensi virus. Tandakan rait kotak semakan **Ubah suai subjek mesej yang dijangkiti virus** dan ubah teks masing-masing (nilai lalai adalah *****VIRUS*****).
- **Mengimbas ciri** - menentukan sama ada kaedah [analisis heuristik](#) harus digunakan sewaktu pengimbasan (**Gunakan heuristik**), sama ada anda hendak menyemak kehadiran [atur cara yang berpotensi tidak dikehendaki](#) (**Laporkan Potensi Atur Cara yang Tidak Dikehendaki dan Ancaman**

Perisian Pengintip), dan sama ada arkib harus diimbis juga (**Imbas dalam arkib**).

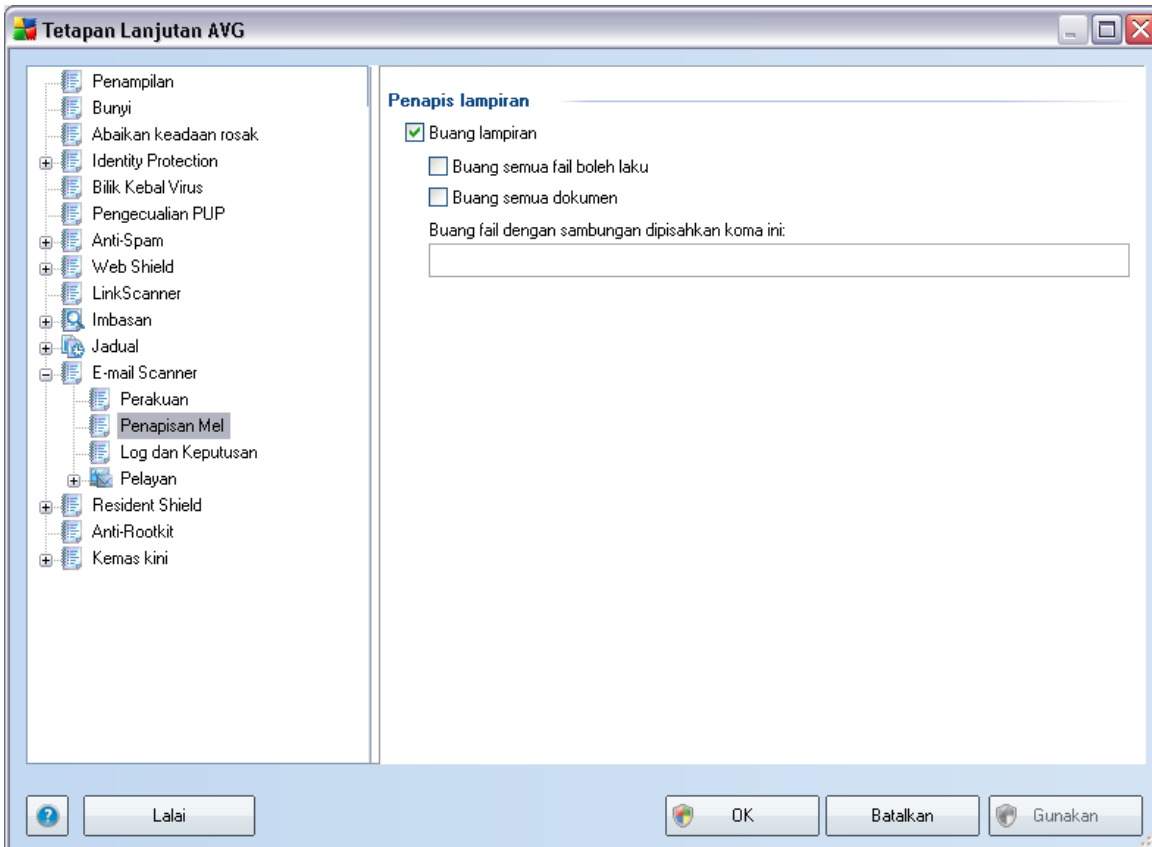
- **Lampiran e-mel melaporkan** - tentukan sama ada anda mahu diberitahu melalui e-mel mengenai arkib yang dilindungi kata laluan, dokumen yang dilindungi kata laluan, makro yang mengandungi fail dan/atau fail dengan sambungan tersembunyi yang dikesan sebagai lampiran bagi mesej e-mel yang diimbis. Jika mesej seperti itu dikenal pasti sewaktu pengimbasan, tentukan sama ada objek berjangkit yang dikesan harus dialih ke **Bilik Kebal Virus**.

9.10.1. 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**.

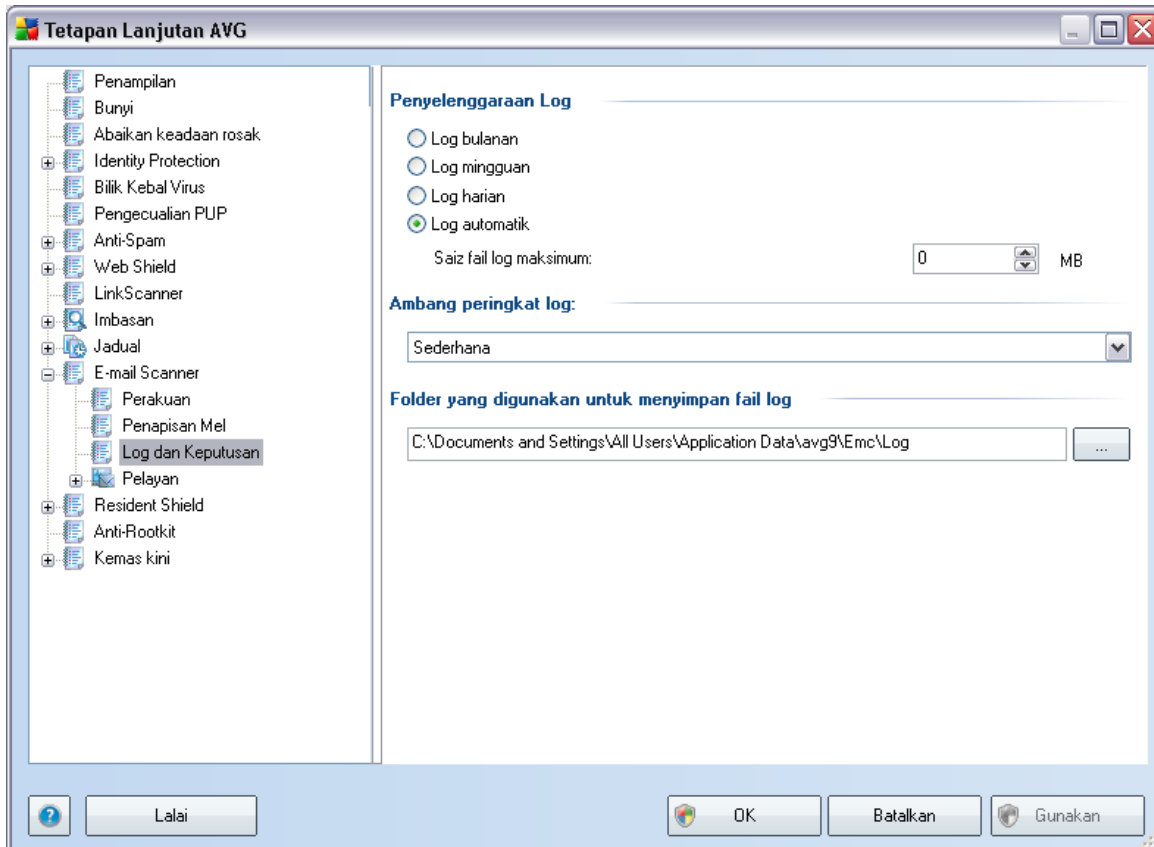
9.10.2. Penapisan Mel



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 akan dipadamkan
- **Buang fail dengan sambungan yang dipisahkan oleh koma** - akan membuang semua fail dengan sambungan yang ditentukan

9.10.3. Log dan Keputusan

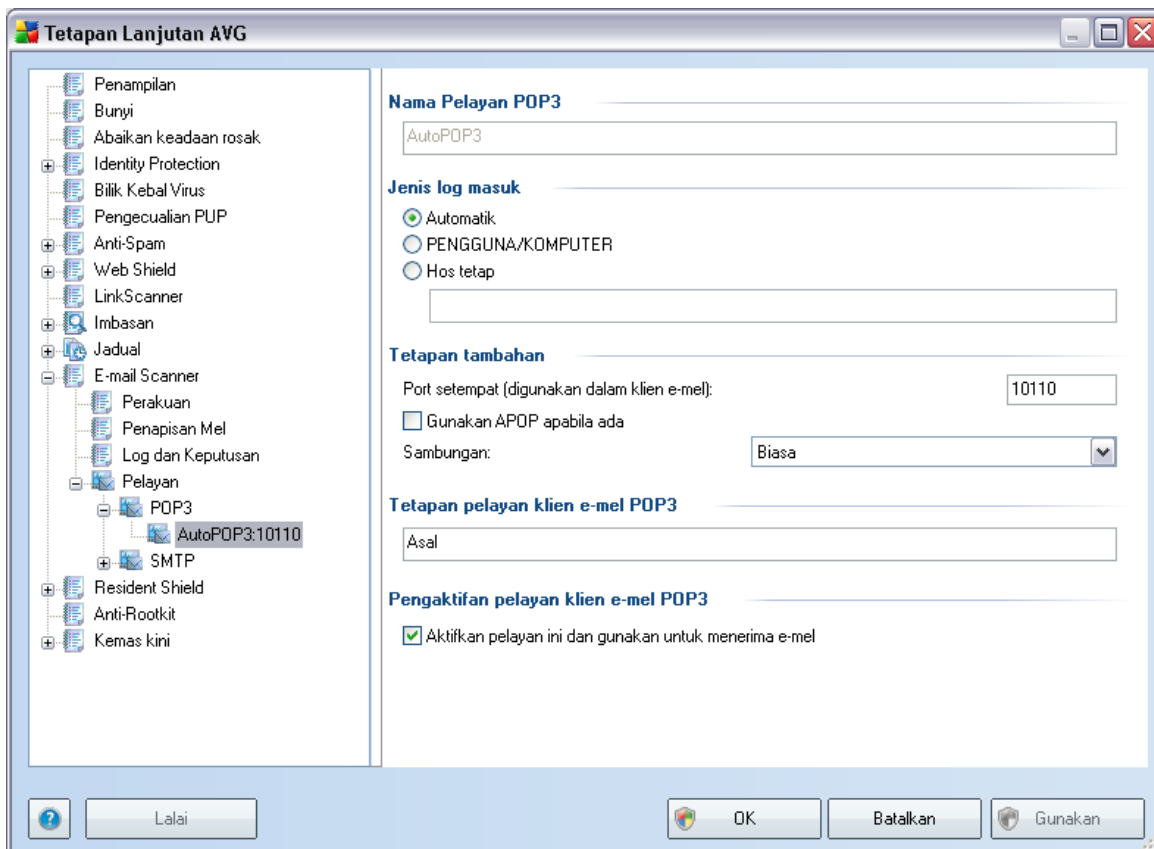


Dialog dibuka melalui item navigasi **Log dan Keputusan** membenarkan anda menentukan parameter untuk penyelenggaraan keputusan pengimbasan e-mel. Dialog dibahagikan kepada beberapa bahagian:

- **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

9.10.4. 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:

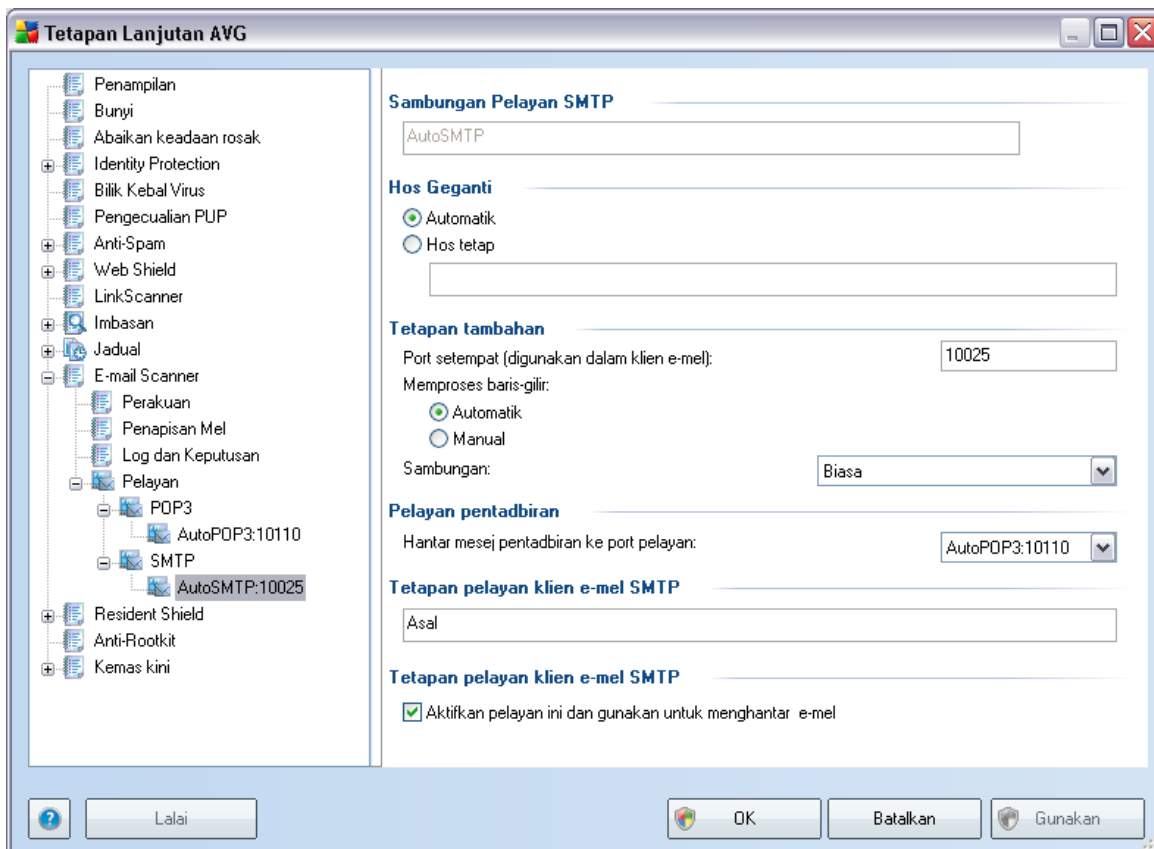
- **Nama Pelayan POP3** - taipkan nama pelayan atau kekalkan nama lalai AutoPOP3
- **Jenis log masuk** - menentukan kaedah untuk menentukan pelayan mel yang digunakan untuk mel masuk:
 - **Automatik** – Log masuk akan dijalankan secara automatik, mengikut

tetapan klien e-mel anda.

- **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.
- **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:
 - **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.
 - **Gunakan APOP apabila tersedia** - opsi 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.
 - **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.
- **Pengaktifan pelayan POP3 klien e-mel** - memberikan maklumat ringkas mengenai tetapan konfigurasi yang diperlukan untuk mengkonfigurasi klien e-

mel anda dengan betul **Pengimbas E-mel** akan menyemak 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



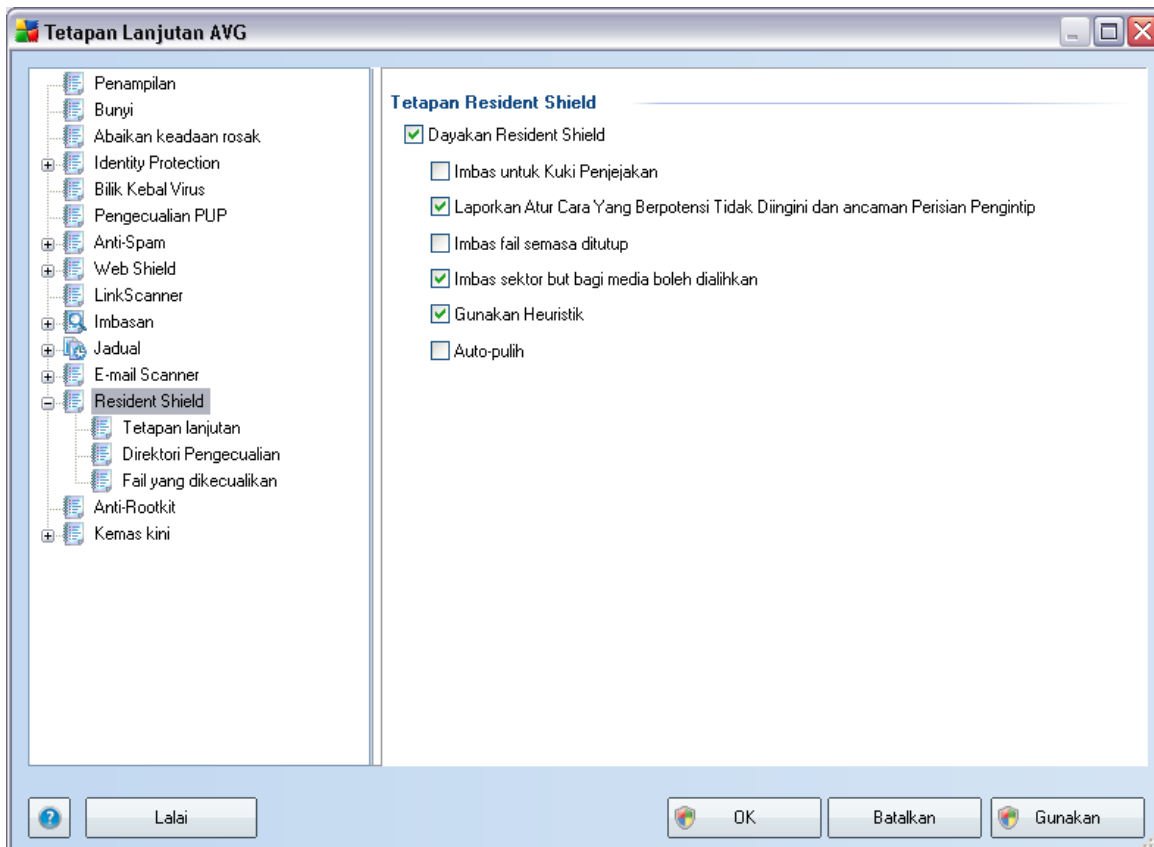
Dalam dialog ini (dibuka melalui ***Pelayan / SMTP***) anda boleh menyediakan pelayan **Pengimbas E-mel** menggunakan protokol SMTP untuk mel keluar:

- ***Nama Pelayan SMTP*** - taipkan nama pelayan atau kekalkan nama lalai Auto SMTP
- ***Hos Gganti*** - mentakrifkan kaedah untuk menentukan pelayan mel yang digunakan untuk mel keluar:

- **Automatik** - log masuk akan dijalankan secara automatik mengikut tetapan klien e-mel anda
- **Hos tetap** - dalam kes ini, atur cara akan sentiasa menggunakan pelayan 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 pengehadnya (sebagai contoh, smtp.acme.com:8200). Port standard untuk komunikasi SMTP ialah 25.
- **Tetapan tambahan** - menentukan parameter yang lebih terperinci:
 - **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.
 - **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
 - **Sambungan** - dalam menu jatuh bawah ini, anda boleh menentukan jenis sambungan mana untuk digunakan (biasa/SSL/SSL lalai). Jika anda memilih sambungan SSL, data yang dihantar disulitkan tanpa risiko dijejaki atau diseliasa 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.

9.11. 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:

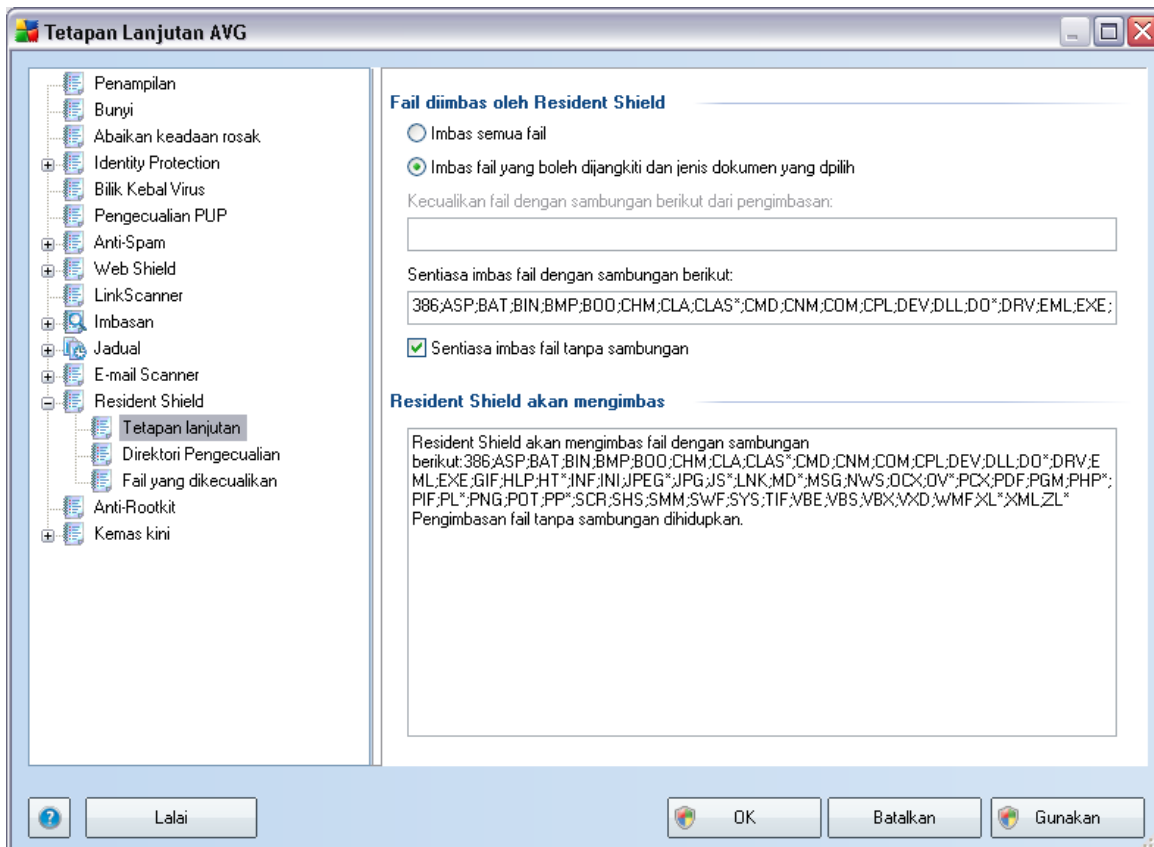
- **Imbas untuk Kuki Penjejakan** - parameter ini menentukan bahawa kuki harus dikesan sewaktu pengimbasan. (Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik)
- **Imbas Atur Cara Yang Berpotensi Tidak Dikehendaki dan Ancaman**

Perisian Pengintip - (dihidupkan secara lalai) mengimbas [atur cara yang berpotensi tidak dikehendaki](#) (aplikasi boleh laku yang boleh berkelakuan seperti pelbagai jenis perisian pengintip atau adware)

- **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 diimbas arahan dalam persekitaran komputer maya*)
- **Autopulih** - sebarang jangkitan yang dikesan akan dipulihkan secara automatik jika terdapat rawatan yang tersedia

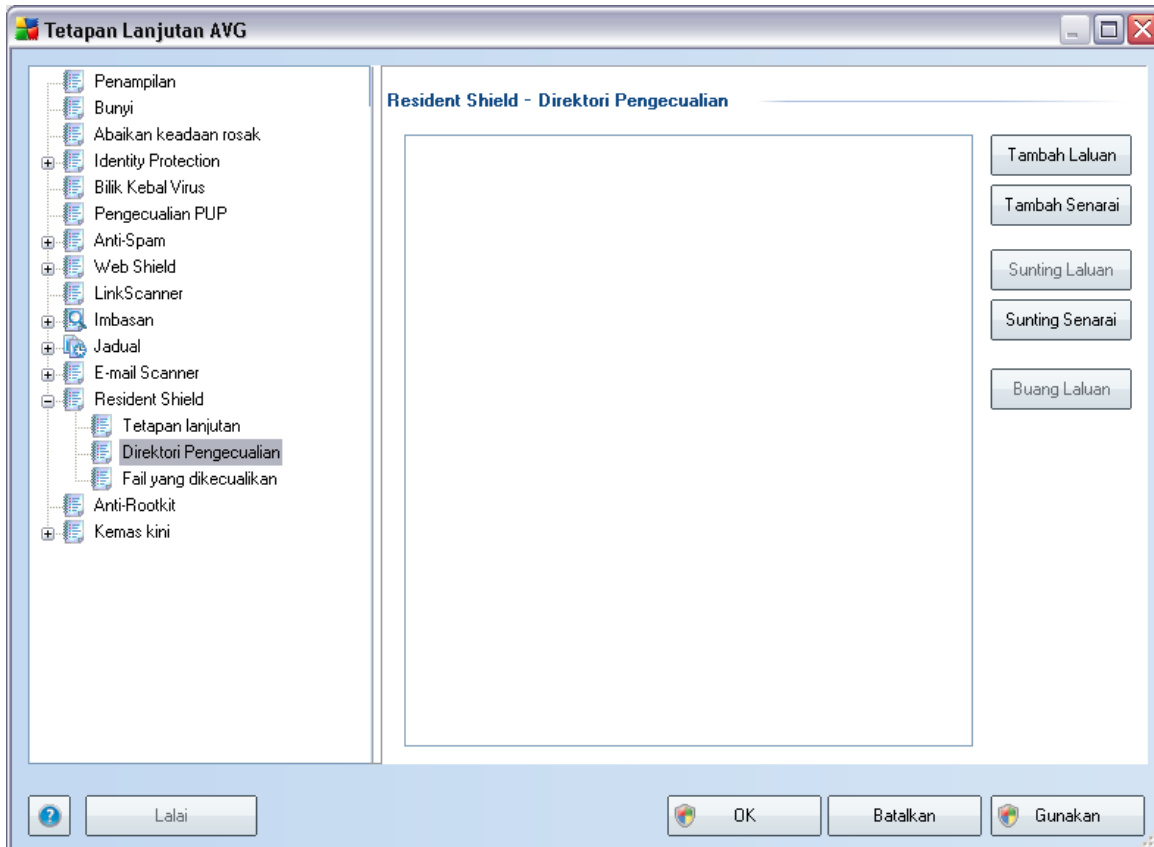
9.11.1. Tetapan Lanjutan

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.

9.11.2. 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!

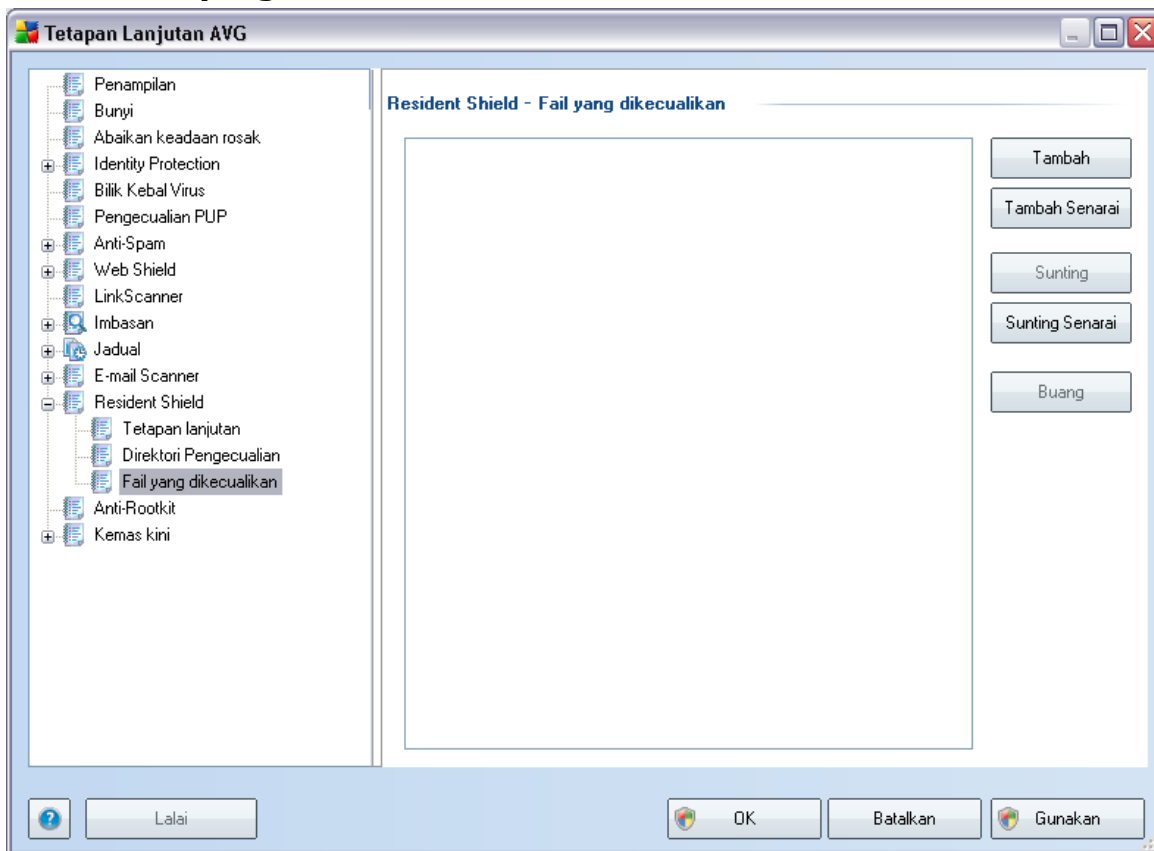
Dialog menyediakan butang kawalan berikut:

- **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

9.11.3. Fail yang Dikecualikan



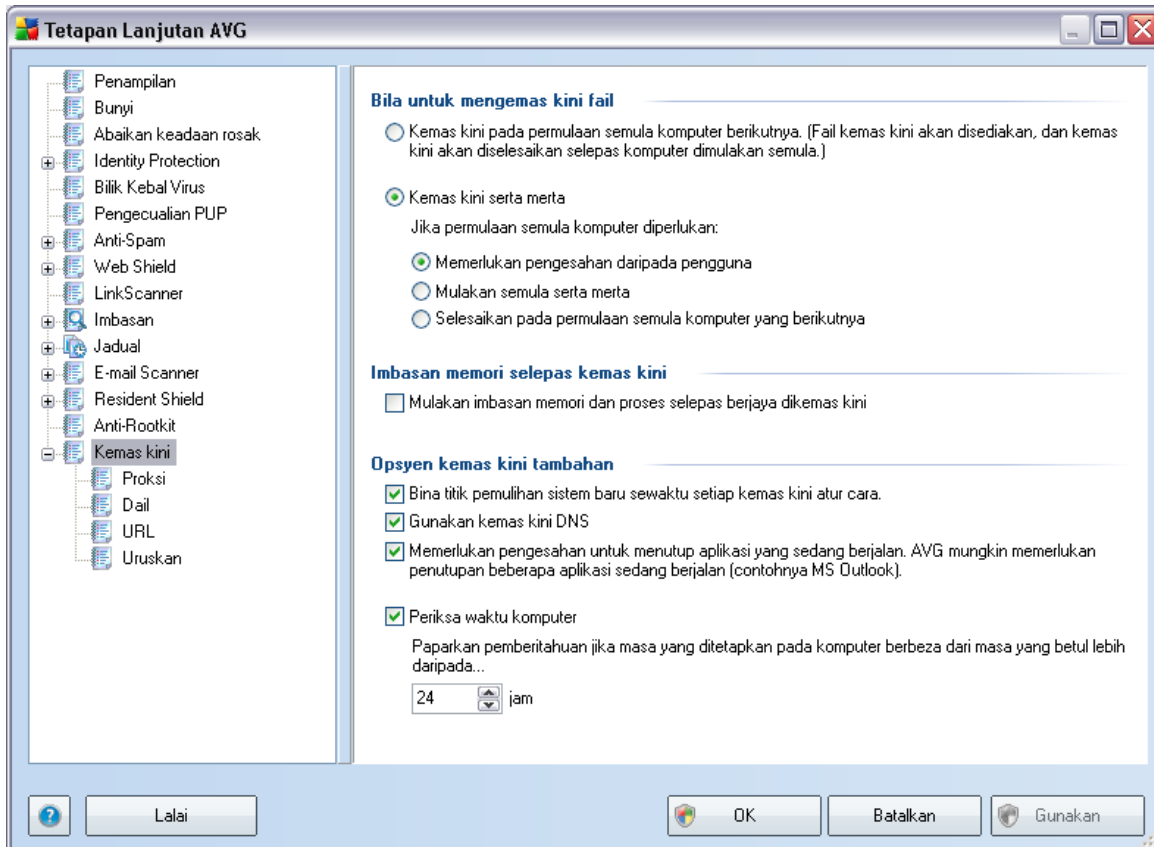
Dialog **Perisai Residen - Tidak termasuk fail** berkelakuan sama seperti yang diterangkan sebelum ini [Perisai Residen - Tidak Termasuk fail](#) tetapi, sebaliknya folder yang anda boleh mentakrifkan fail khusus sekarang yang harus dikeluarkan dari pengimbasan [Perisai Residen](#).

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

Dialog menyediakan butang kawalan berikut:

- **Tambah** – mentakrifkan direktori khusus untuk tidak termasuk daripada pengimbasan dengan memilihnya satu persatu dari pepohon navigasi cakera tempatan
- **Tambah senarai** – membenarkan anda memasukkan keseluruhan senarai direktori untuk mengecualikan daripada imbasan [Perisai Residen](#)
- **Edit** – membenarkan anda mengedit laluan yang ditentukan kepada folder yang dipilih
- **Edit senarai** – membenarkan anda mengedit senarai folder
- **Buang** – membenarkan anda memadam laluan kepada folder yang dipilih daripada senarai

9.12. 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 dilengkapkan Kemas kini yang terkini dimuat turun mungkin telah mengandungi definisi virus baru dan ini boleh digunakan dalam pengimbasan dengan serta-merta.

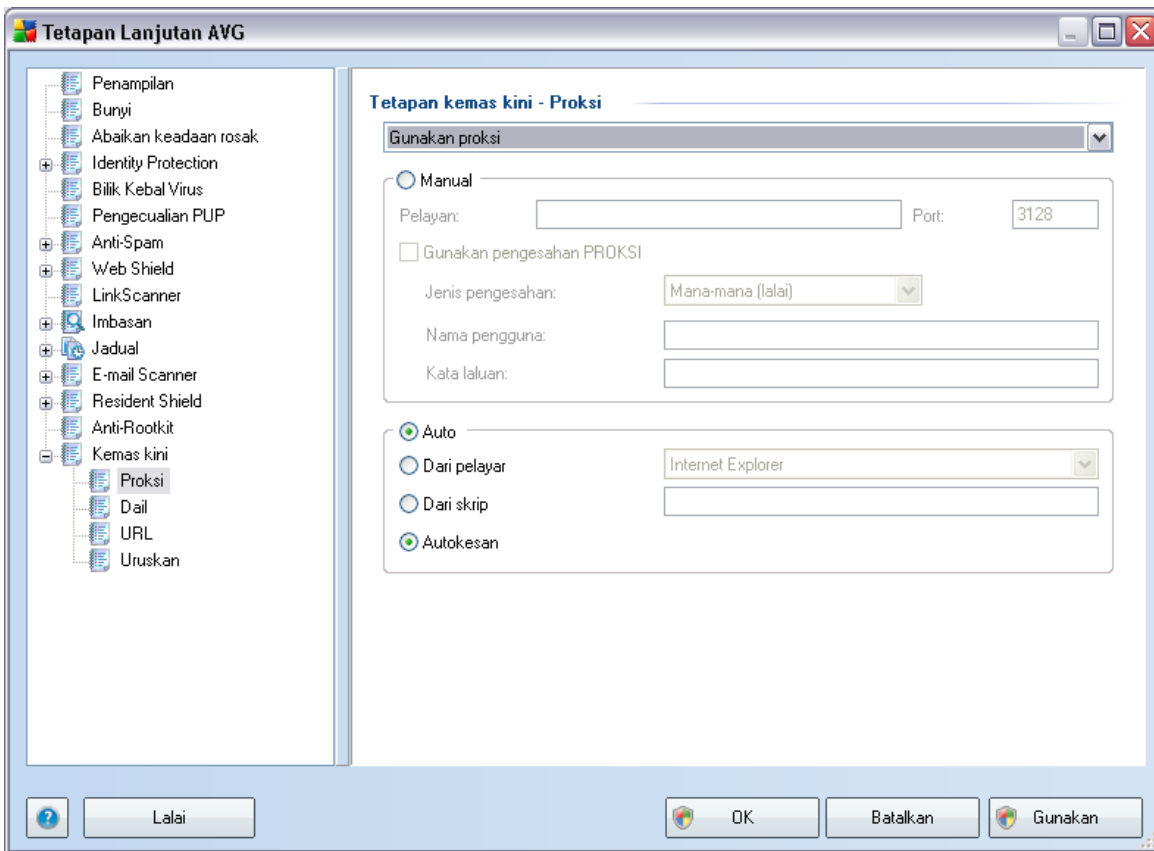
Opsyen kemas kini tambahan

- **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 kefungisian 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 pengesahan 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 opsi ini untuk mengesahkan bahawa anda mahu pemberitahuan ini dipaparkan jika masa komputer berbeza dari masa yang betul lebih daripada bilangan jam yang ditetapkan.

9.12.1. 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**
- **Cuba sambungan menggunakan proksi dan jika ia gagal, sambung secara terus** - tetapan lalai

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*)

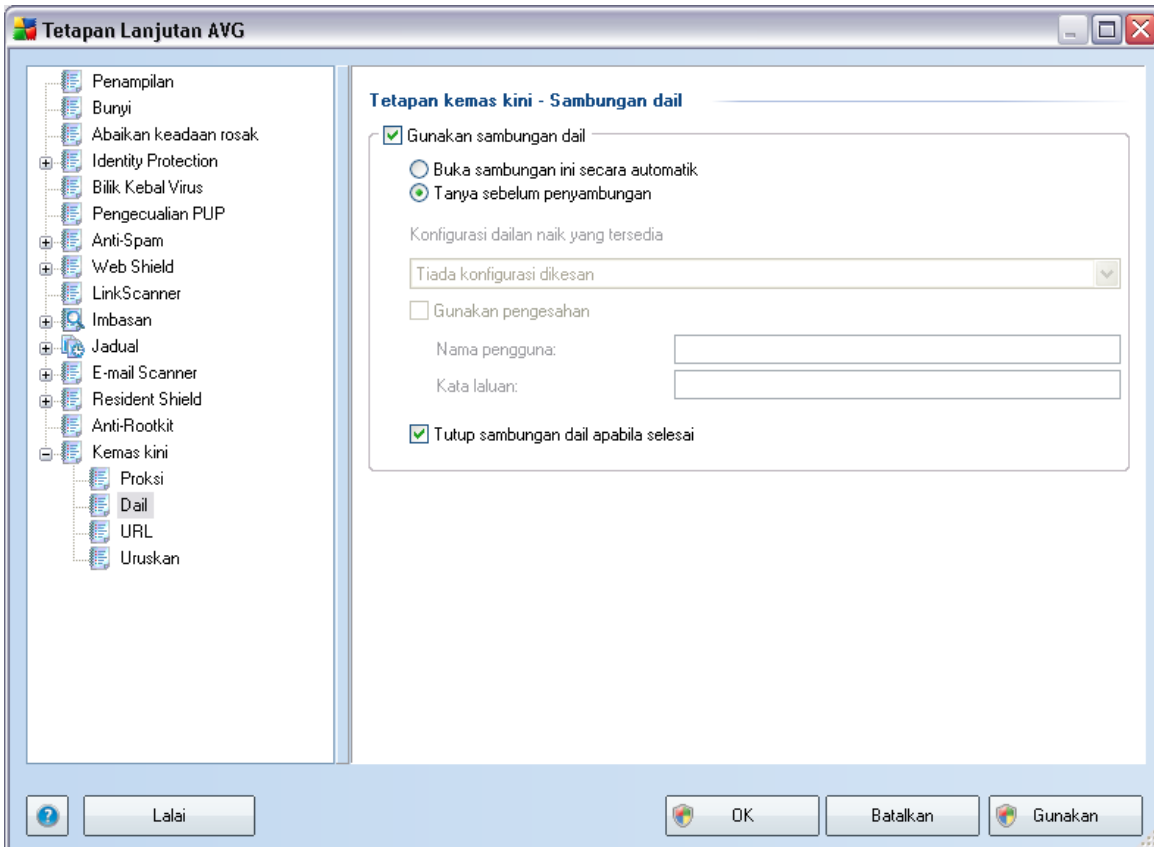
Pelayan proksi juga boleh mengkonfigurasi peraturan tertentu untuk setiap pengguna. Jika pelayan proksi anda disediakan dengan cara ini, tandakan opsyen **Guna pengesahan PROKSI** untuk mengesahkan bahawa nama pengguna dan kata laluan anda sah untuk menyambung kepada Internet melalui pelayan proksi.

Konfigurasi automatik

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

- **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

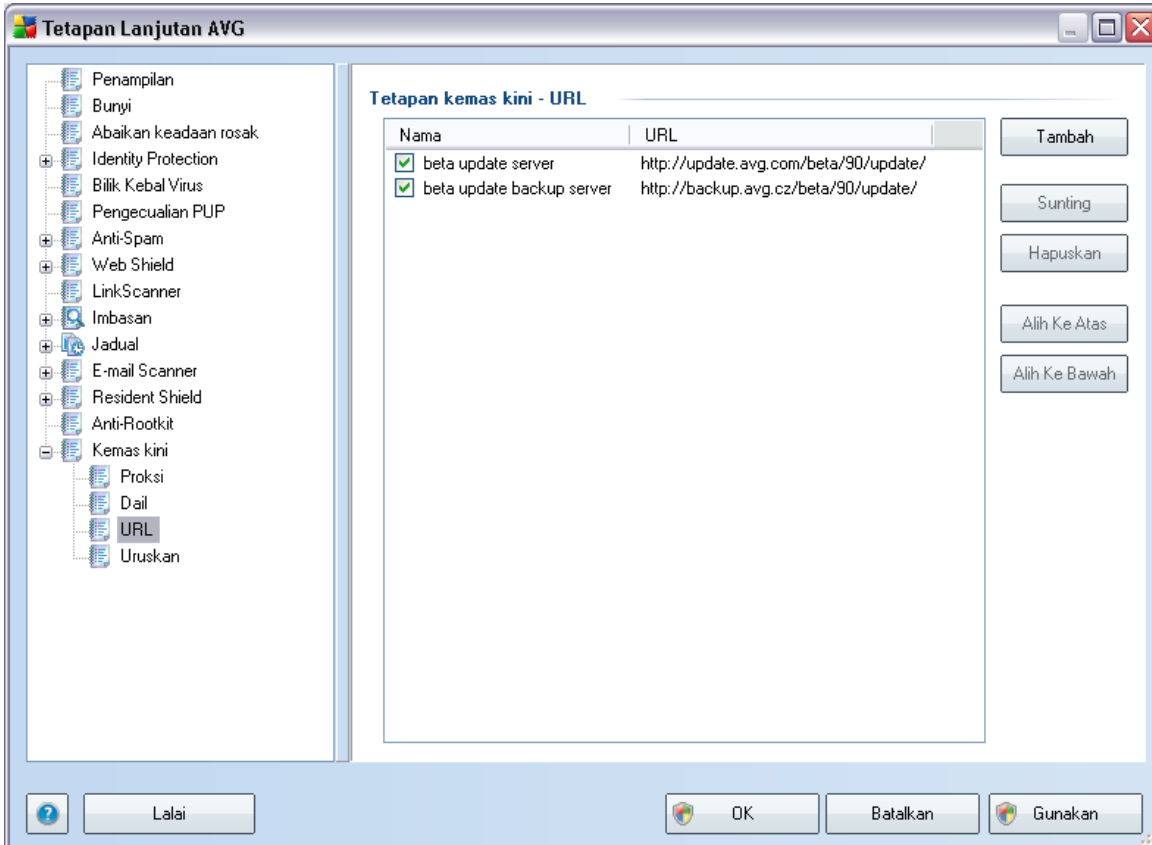
9.12.2. Dailan



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**).

9.12.3. URL



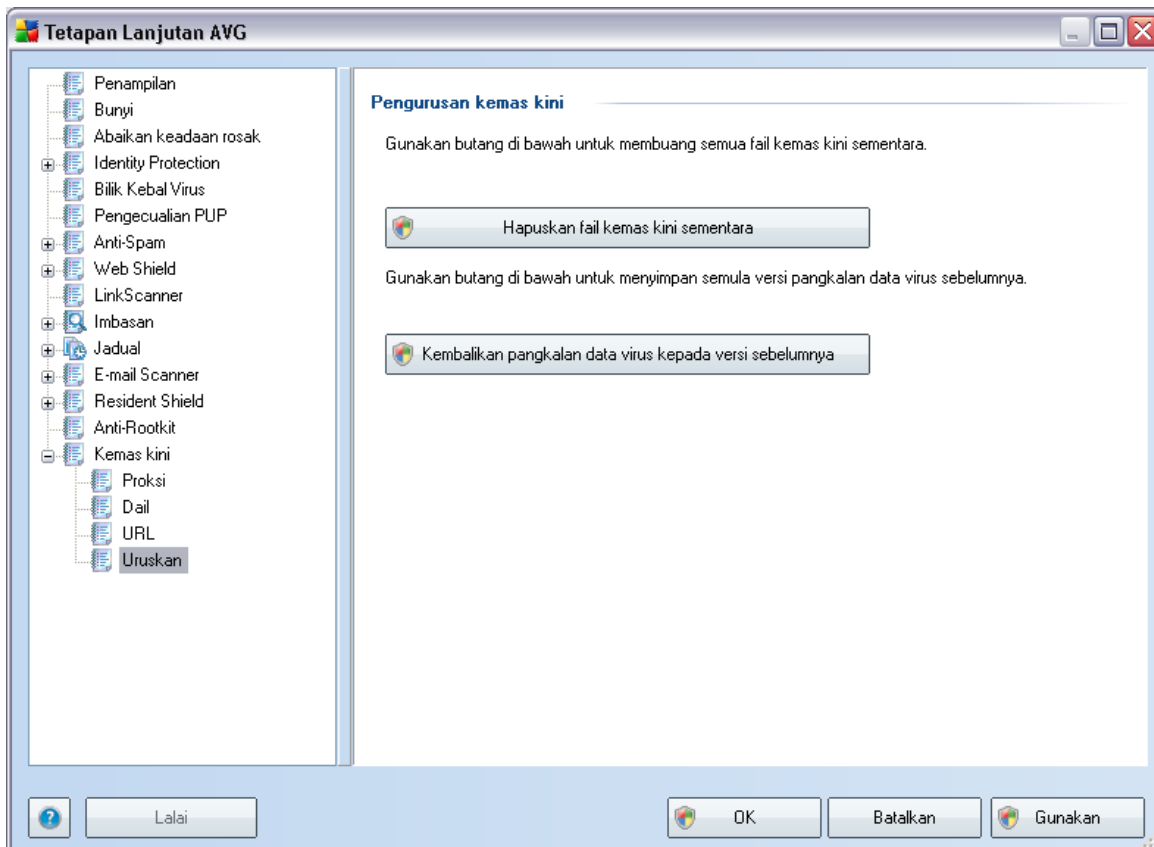
Dialog **URL** menawarkan senarai alamat Internet dari mana fail kemas kini dimuat turun. Senarai dan itemnya boleh diubah suai menggunakan butang kawalan berikut:

- **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

9.12.4. Uruskan

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

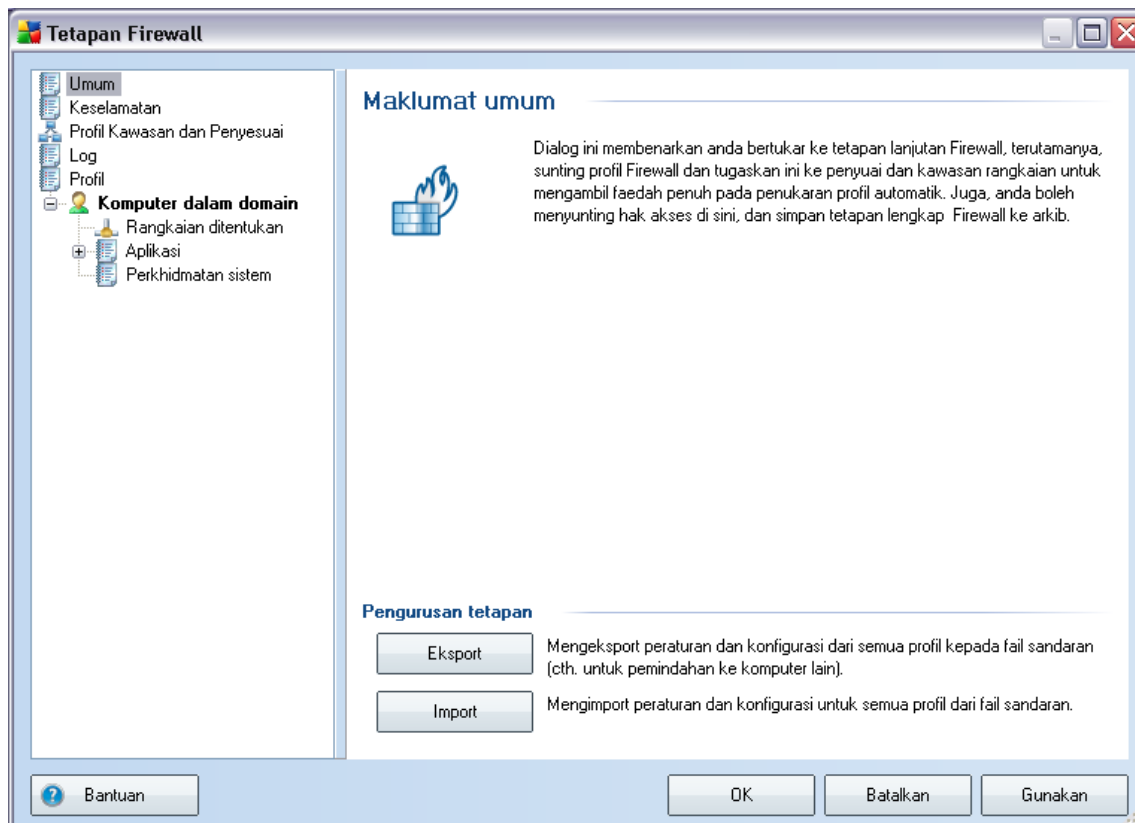


- **Padam fail kemas kini sementara** - tekan butang ini untuk memadam semua fail kemas kini berlebihan dari cakera keras anda (*secara lalai, fail ini disimpan selama 30 hari*)
- **Kembalikan pangkalan data virus ke versi sebelumnya** – tekan butang ini untuk memadam versi pangkalan virus terkini dari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

10. Tetapan Firewall

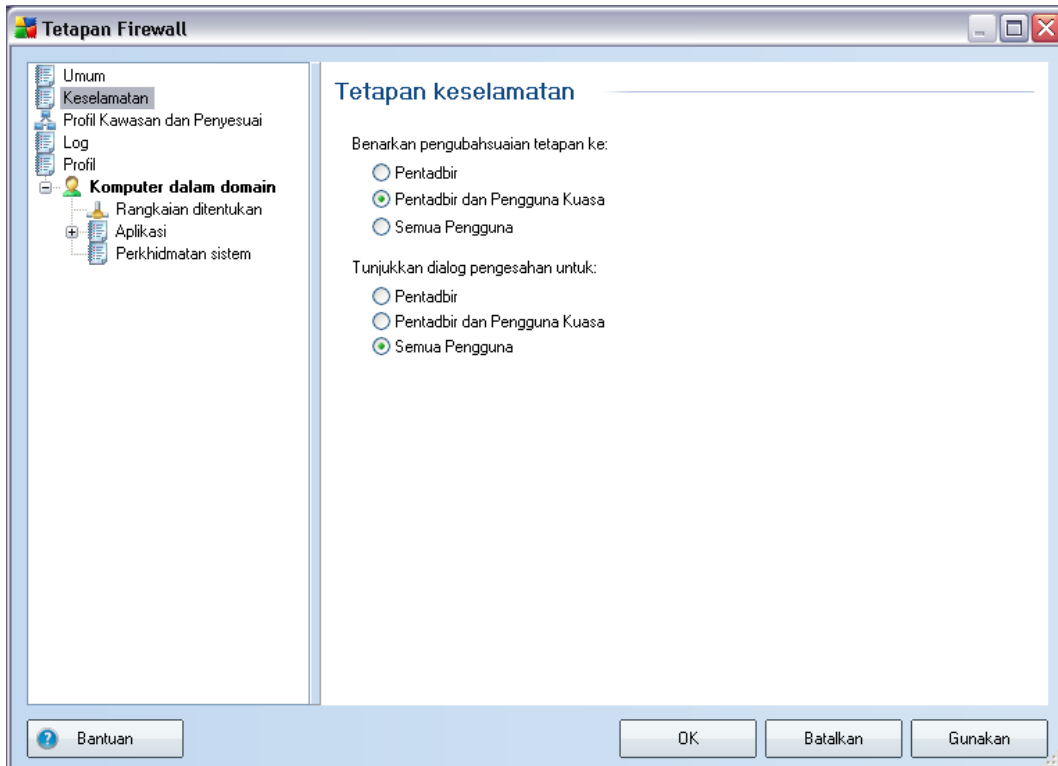
Konfigurasi **Firewall** membuka tettingkap baru di mana beberapa dialog boleh menyediakan parameter yang sangat canggih bagi komponen. **Walau bagaimanapun, pengeditan konfigurasi lanjutan hanya bertujuan untuk pengguna pakar dan berpengalaman.**

10.1. Umum



Dalam **Maklumat umum** anda boleh **Mengeksport / Mengimport konfigurasi Firewall**; cth. mengeksport peraturan dan tetapan **Firewall** kepada fail sandaran atau sebaliknya untuk mengimport keseluruhan fail sandaran.

10.2. Keselamatan



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

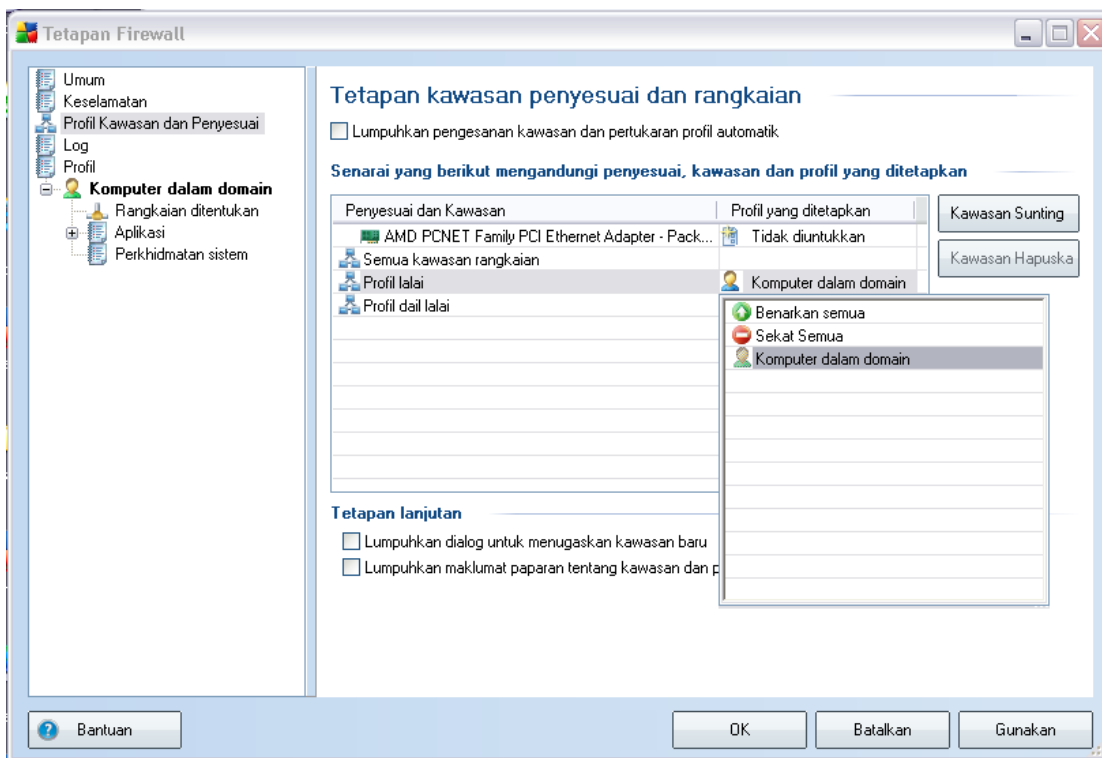
- **Benarkan pengubahsuaian kepada** - tentukan siapa dibenarkan untuk mengubah konfigurasi **Firewall**
- **Tunjukkan dialog pengesahan untuk** - tentukan kepada siapa dialog pengesahan (*dialog yang meminta keputusan dalam situasi yang tidak diliputi oleh peraturan **Firewall***) harus dipaparkan

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

- **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

10.3. Profil Kawasan dan Penyesuai



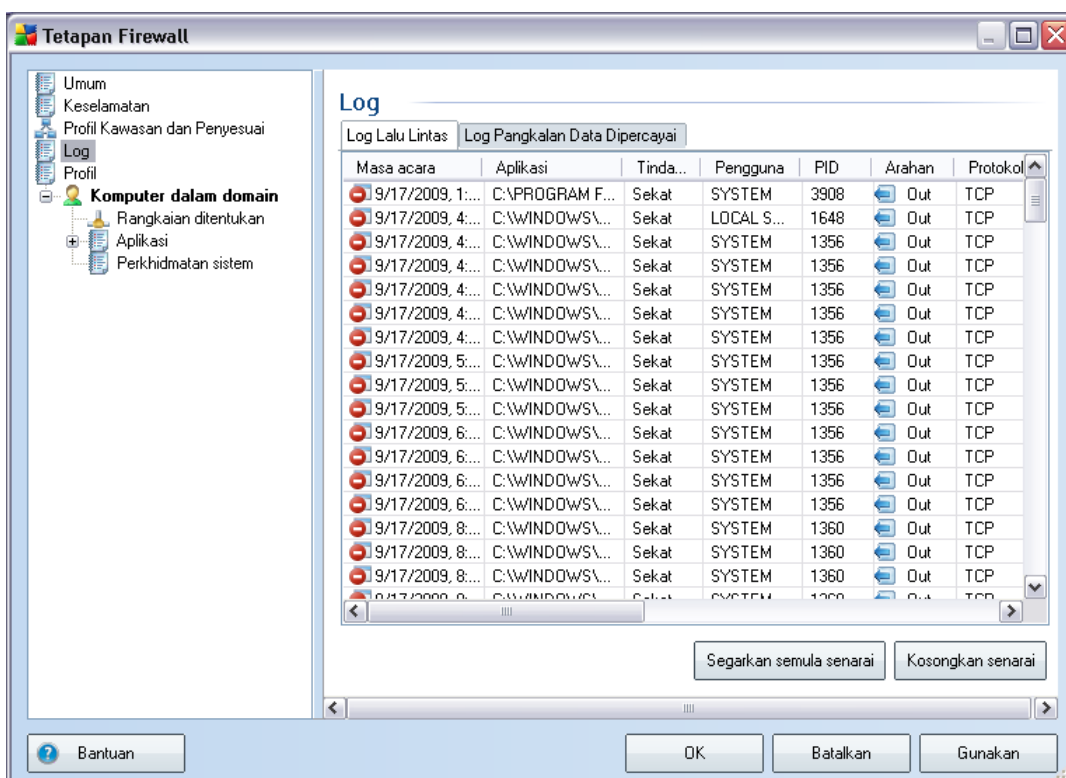
Dalam dialog **Penyesuai dan tetapan kawasan rangkaian** anda boleh mengedit tetapan berkaitan dengan menguntukkan profil yang ditakrifkan kepada penyesuai khusus dan merujuk kepada rangkaian masing-masing:

- **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*** - menandakan rait pada opsyen masing-masing akan menyahaktifkan ciri paparan mesej maklumat..

10.4. Log



Dialog **Log** membenarkan anda menyemak semula senarai semua tindakan dan peristiwa **Firewall** yang dilog dengan penerangan terperinci bagi parameter yang relevan (*masa peristiwa, nama aplikasi, tindakan log tersebut, nama pengguna, PID,*

arah lalu lintas, jenis protokol, bilangan port jauh dan tempatan, dll.) pada dua tab:

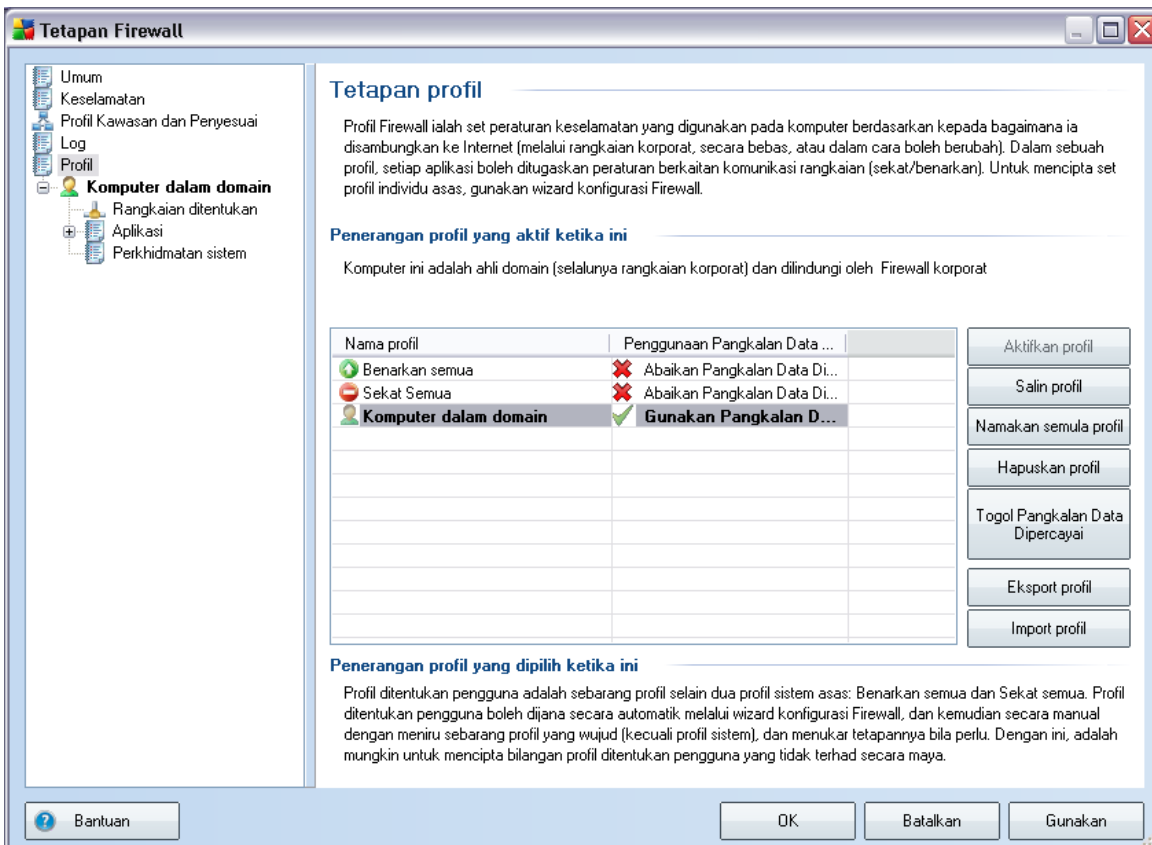
- **Log Lalu Lintas** - menawarkan maklumat mengenai aktiviti bagi semua aplikasi yang telah cuba menyambung ke rangkaian.
- **Log Pangkalan Data yang Dipercayai** - Pangkalan data yang dipercayai adalah maklumat pengumpulan pangkalan data dalaman AVG mengenai aplikasi yang diperakui dan dipercayai yang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

10.5. 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

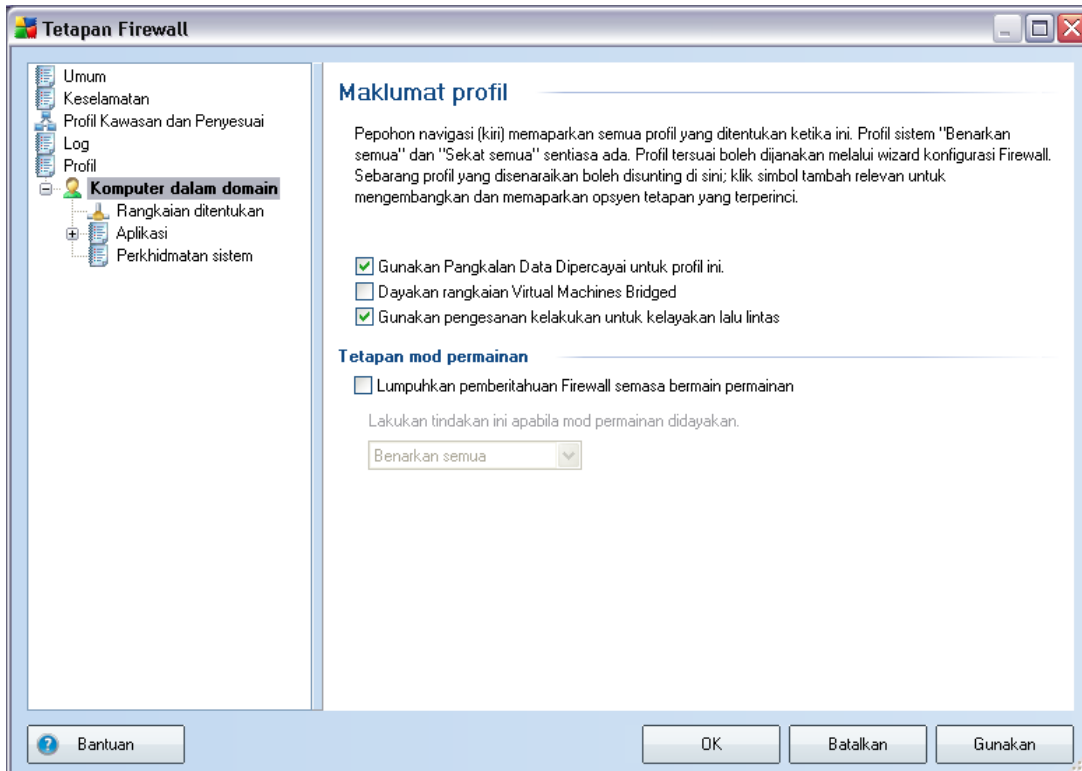
profil yang dipilih

- **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*):

10.5.1. 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.

- **Pro tento profil použit Duveryhodnou databázi** - (dihidupkan secara lalai) tandakan opsyen untuk mengaktifkan *Pangkalan Data yang Dipercayai* (Cth. maklumat pengumpulan pangkalan data dalaman AVG pada aplikasi komunikasi dalam talian yang dipercayai dan diperakui. 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 Virtual Machines Bridget** - (dimatikan secara lalai) tandakan rait item ini untuk membenarkan mesin maya dalam VMware untuk bersambung secara terus ke rangkaian

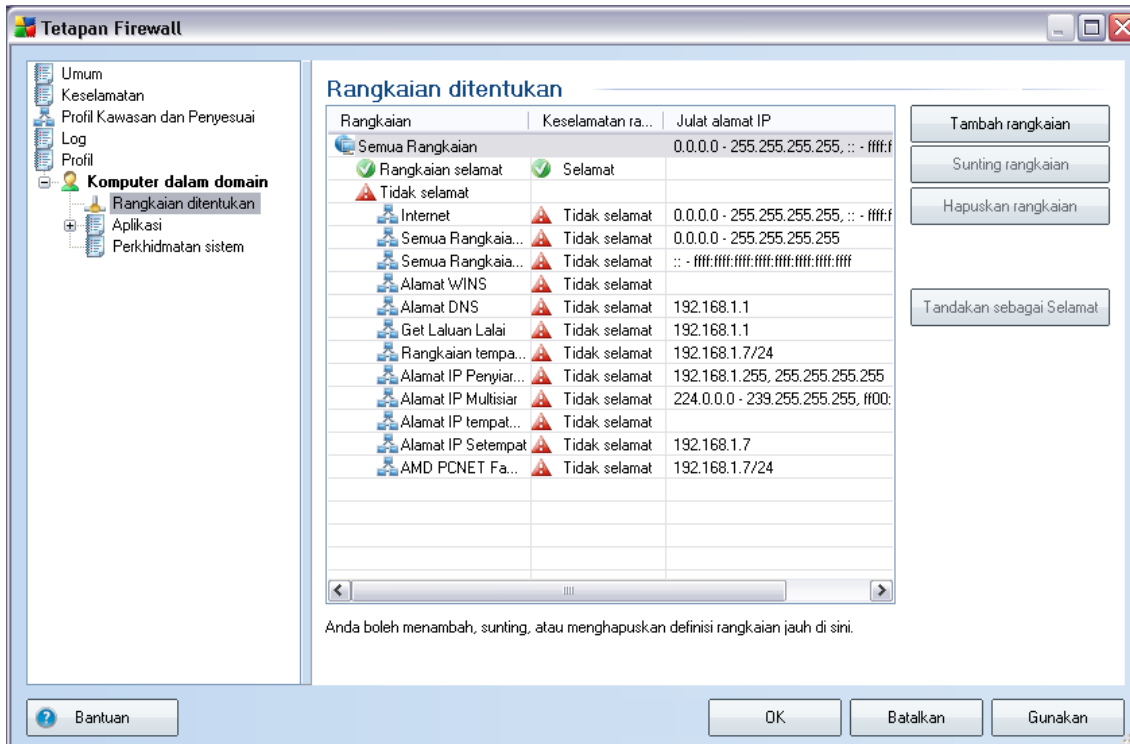
- **Gunakan pengesanan kelakuan untuk kelayakan lalu lintas** - (*dihidupkan secara lalai*) tandakan opsi ini untuk membenarkan **Firewall** menggunakan kefungsi **LinkScanner** semasa menilai aplikasi - **LinkScanner** boleh memberitahu sama ada aplikasi menunjukkan sebarang kelakuan mencurigakan atau 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.

10.5.2. Rangkaian yang Ditetapkan

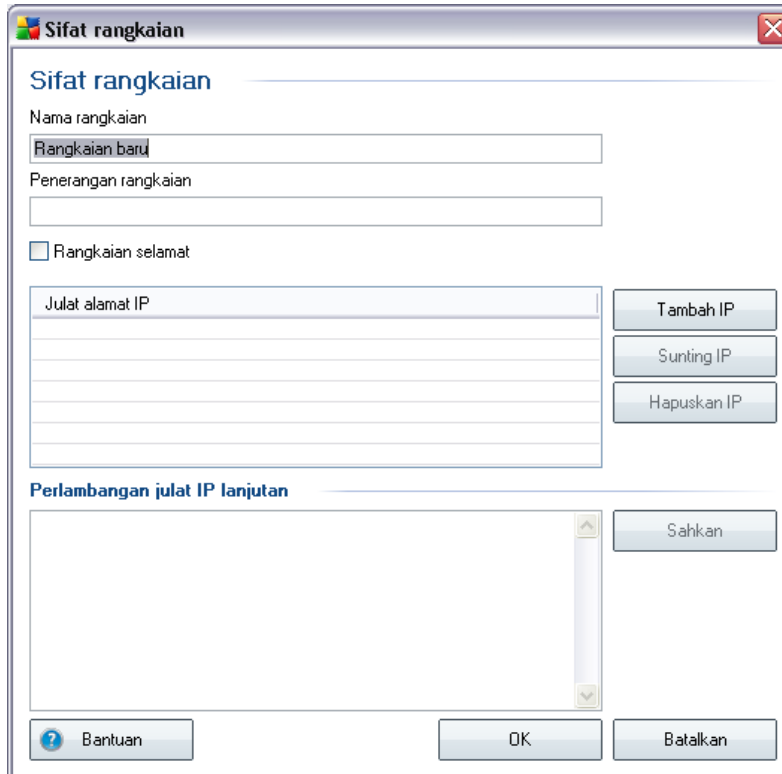


Dialog **Rangkaian yang ditakrifkan** menawarkan senarai semua rangkaian yang komputer anda disambungkan. Maklumat berikut diberikan pada setiap rangkaian yang dikesan:

- **Rangkaian** - senarai nama semua rangkaian yang komputer disambungkan kepadanya.
- **Keselamatan rangkaian** - secara lalai, semua rangkaian dikira tidak selamat dan hanya jika anda pasti bahawa rangkaian masing-masing adalah selamat, anda boleh menguntukkannya supaya (*mengklik item senarai merujuk kepada rangkaian masing-masing dan pilih Selamat daripada menu konteks*) - semua rangkaian selamat kemudian, akan dimasukkan ke dalam kumpulan yang aplikasi boleh berkomunikasi dengan 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:



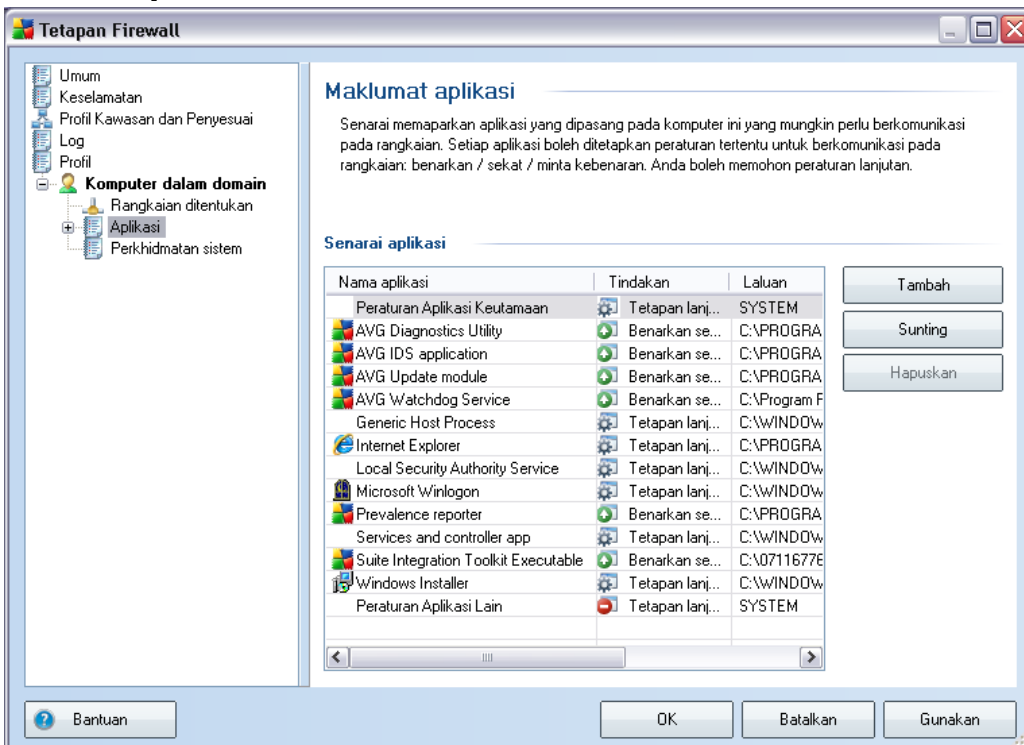
Dalam dialog ini, anda boleh menentukan **Nama rangkaian**, berikan **Penerangan rangkaian** dan berkemungkinan peruntukkan rangkaian sebagai selamat. Rangkaian baru boleh menjadi sama ada ditakrifkan secara manual dalam dialog tersendiri yang dibuka melalui butang **Tambah IP** (secara alternatif, **Edit 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 bahawa rangkaian masing-masing adalah selamat, anda boleh menggunakan butang ini untuk menguntukkannya
- **Bantuan** - membuka fail bantuan berkaitan dialog

10.5.3. Aplikasi

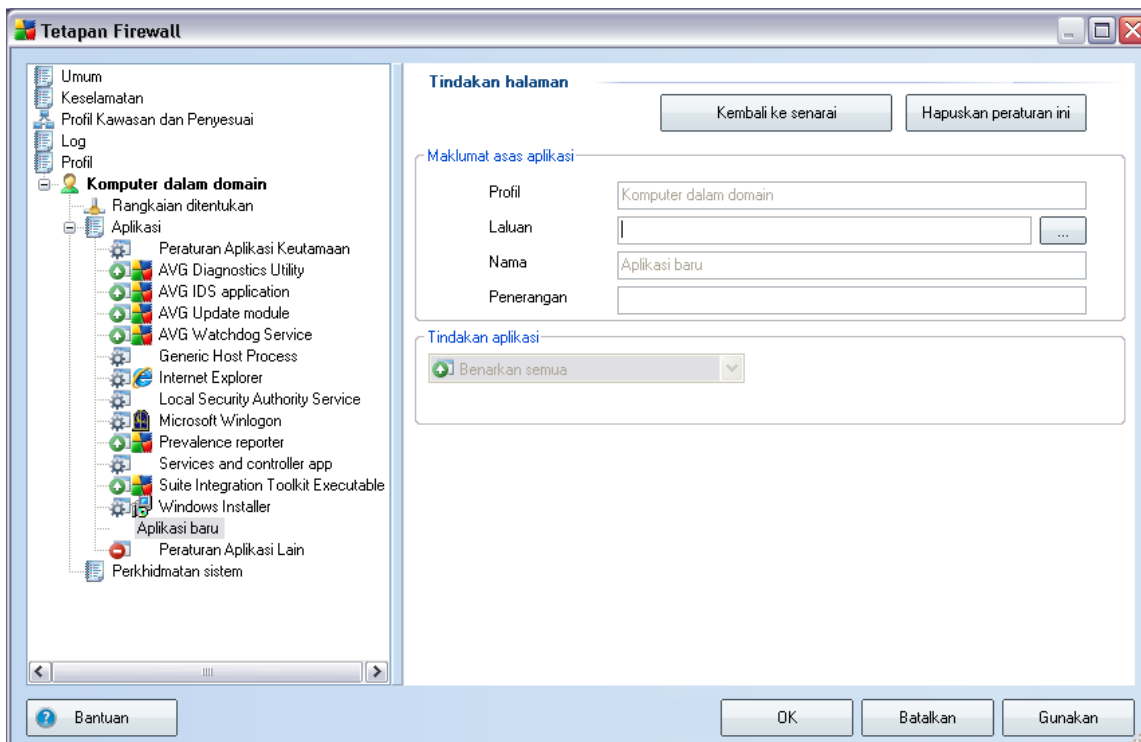


Dalam dialog **Maklumat aplikasi** anda boleh menjumpai gambaran keseluruhan semua aplikasi yang berkomunikasi pada rangkaian. Senarai boleh diedit dengan

menggunakan butang kawalan berikut:

- **Tambah** - membuka dialog untuk [mentakrifkan set peraturan aplikasi](#)
- **Edit** - membuka dialog yang sama untuk [mengedit set peraturan aplikasi sedia ada](#)
- **Padam** - membuang aplikasi yang dipilih daripada senarai
- **Bantuan** - membuka fail bantuan berkaitan dialog

Dialog untuk menentukan set peraturan aplikasi baru dibuka menggunakan butang **Tambah** dari dialog [Aplikasi](#) dalam [Tetapan Firewall](#):

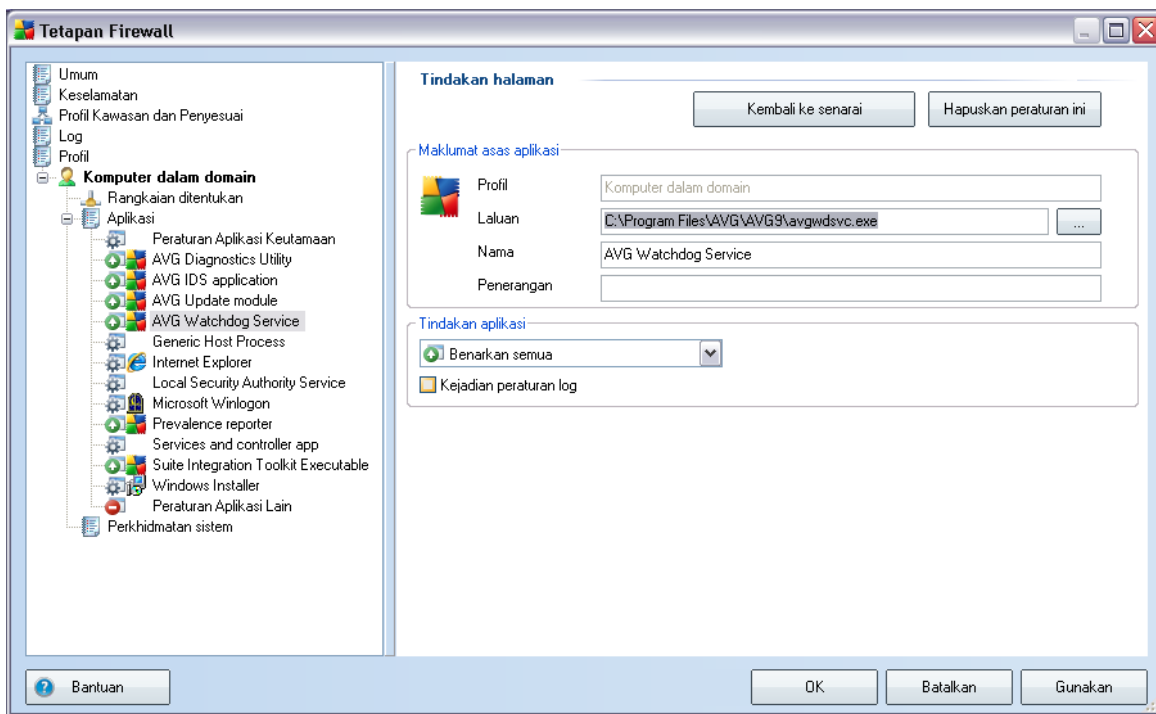


Dalam dialog ini anda boleh menentukan:

- **Maklumat asas aplikasi** - nama aplikasi, penerangan ringkasnya dan laluan ke lokasinya pada cakera

- **Tindakan aplikasi** - dari menu jantai bawah, pilih peraturan yang harus digunakan pada kelakuan aplikasi:
 - **Tetapan lanjutan** - opsyen ini membolehkan anda mengedit set peraturan secara terperinci pada bahagian bawah dialog ini; *untuk penerangan bagi bahagian ini, sila lihat bab [Edit Aplikasi](#)*
 - **Benarkan semua** - sebarang percubaan komunikasi bagi aplikasi akan dibenarkan
 - **Benarkan dengan selamat** - aplikasi hanya akan dibenarkan untuk berkomunikasi pada rangkaian selamat (*contohnya, komunikasi pada rangkaian syarikat yang dilindungi akan dibenarkan sementara komunikasi pada Internet akan dihalang*); untuk gambaran keseluruhan dan penerangan bagi rangkaian selamat, sila lihat dialog [Rangkaian](#)
 - **Minta** - setiap kali aplikasi mencuba untuk berkomunikasi pada rangkaian, anda akan diminta untuk menentukan sama ada komunikasi harus dibenarkan atau dihalang
 - **Halang** - semua percubaan komunikasi bagi aplikasi akan dihalang

Dialog untuk mengedit set peraturan aplikasi sedia ada dibuka menggunakan butang **Edit** daripada dialog **Aplikasi** dalam **Tetapan Firewall**:



Dalam dialog ini, anda boleh mengedit semua parameter aplikasi:

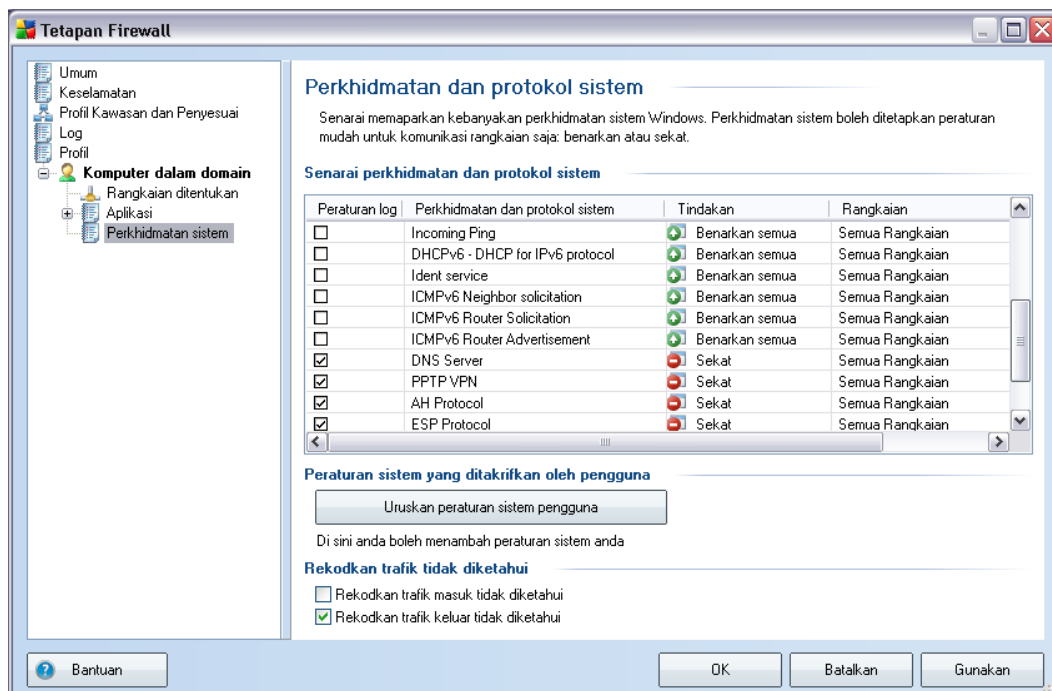
- **Maklumat asas aplikasi** - nama aplikasi, penerangan ringkasnya dan laluan ke lokasinya pada cakera
- **Tindakan aplikasi** - dari menu jantai bawah, pilih peraturan yang harus digunakan pada kelakuan aplikasi:
 - **Tetapan lanjutan** - opsi ini membenarkan anda mengedit set peraturan secara terperinci di bahagian bawah dialog ini
 - **Benarkan kepada semua** - sebarang percubaan komunikasi bagi aplikasi akan dibenarkan
 - **Benarkan dengan selamat** - aplikasi hanya akan dibenarkan untuk berkomunikasi pada rangkaian selamat (*contohnya, komunikasi pada rangkaian syarikat yang dilindungi akan dibenarkan sementara*)

komunikasi pada Internet akan dihalang); untuk gambaran keseluruhan dan penerangan bagi rangkaian selamat, sila lihat dialog **Rangkaian**

- **Minta** - setiap kali aplikasi mencuba untuk berkomunikasi pada rangkaian, anda akan diminta untuk menentukan sama ada komunikasi harus dibenarkan atau dihalang
- **Halang** - semua percubaan komunikasi bagi aplikasi akan dihalang
- **Log ulangan peraturan** - tandakan opsyen ini untuk mengesahkan anda mahu melog semua tindakan **Firewall** berkenaan aplikasi yang anda telah konfigurasi set peraturannya. Kemudian, entri log masing-masing boleh ditemui dalam dialog **Log**.

10.5.4. Perkhidmatan Sistem

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



Dialog

Perkhidmatan dan protokol sistem membuka perkhidmatan dan protokol sistem yang berkomunikasi pada rangkaian. Di bawah senarai, anda boleh menemui dua opsyen: tanda/nyahtandanya untuk mengesahkan anda hendak **dilog** semua lalu lintas yang diketahui dalam kedua-dua arah (*masuk atau keluar*).

Butang kawalan

- **Tambah / Edit** - kedua-dua butang membuka dialog yang sama di mana anda boleh mengedit parameter perkhidmatan sistem . Butang **Tambah** membuka dialog kosong dan dalam mod asas (*tiada bahagian tetapan lanjutan; tetapi bahagian ini boleh dibuka dengan memilih tetapan lanjutan untuk tindakan aplikasi*); butang **Edit** membuka dialog yang sama dengan data yang telah dimasukkan merujuk kepada perkhidmatan sistem yang dipilih.

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

11. Pengimbasan AVG

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

11.1. 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 dipraktikkan](#) - tiga jenis pengimbasan yang ditentukan oleh vendor perisian sedia untuk digunakan dengan serta-merta mengikut permintaan atau jadual:
 - [Imbas seluruh komputer](#)
 - [Imbas fail atau folder tertentu](#)
- [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

11.2. Imbasan Pratakrif

Salah satu ciri utama bagi **AVG 9 Anti-Virus plus Firewall** adalah pengimbasan yang 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.

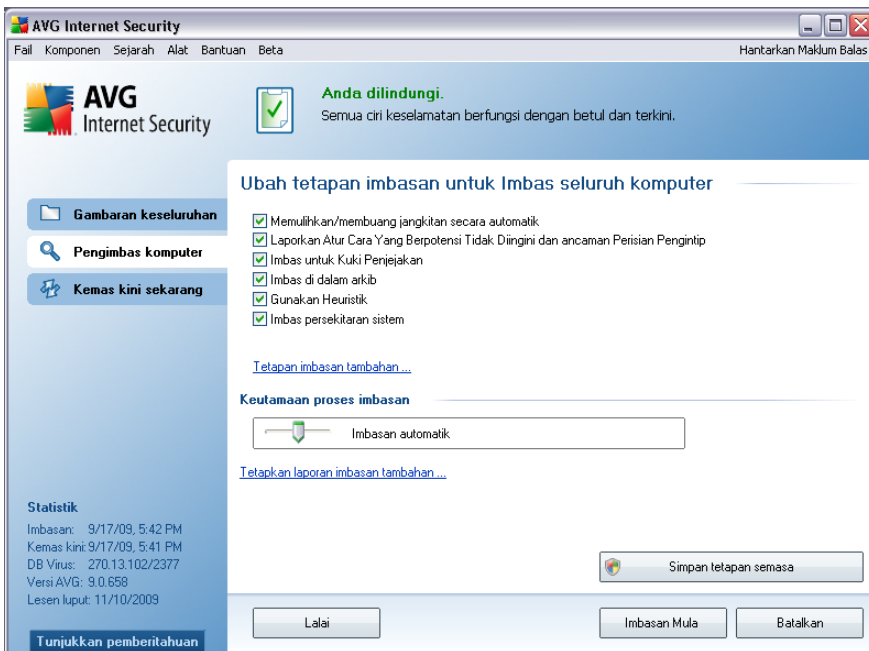
Dalam **AVG 9 Anti-Virus plus Firewall** anda akan menemui dua jenis pengimbasan yang dipratetapkan oleh vendor perisian:

11.2.1. Imbas Seluruh Komputer

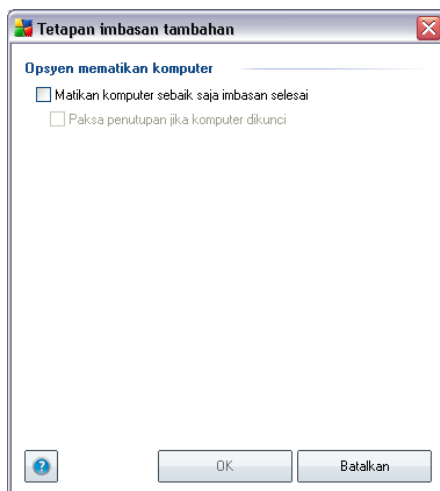
Imbas seluruh komputer - mengimbas seluruh komputer anda untuk kemungkinan jangkitan dan/atau atur cara yang tidak diingini. Ujian ini akan mengimbas semua pemacu keras komputer anda, akan mengesan dan memulihkan sebarang virus yang ditemui atau membuang jangkitan yang dikesan ke [Bilik Kebal Virus](#).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

Lancarkan imbasan

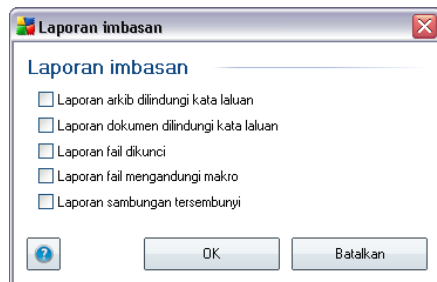
Imbas seluruh komputer boleh dilancarkan dari [antara muka imbasan](#) dengan mengklik pada ikon imbasan. Tiada tetapan khusus selanjutnya yang perlu dikonfigurasi untuk jenis imbasan ini, imbasan akan bermula dengan serta-merta dalam dialog **Imbasan sedang dijalankan** (*lihat gambar skrin*). Imbasan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



- **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:



- **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini akan (**Mematikan komputer apabila selesai imbasan**), opsyen baru diaktifkan yang membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa matikan komputer dikunci**).
- **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbas:
 - **Semua jenis fail** dengan kemungkinan pengecualian yang ditentukan dari pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan oleh koma yang harus diimbas; atau
 - **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 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.

11.2.2. Imbas Fail atau Folder Tertentu

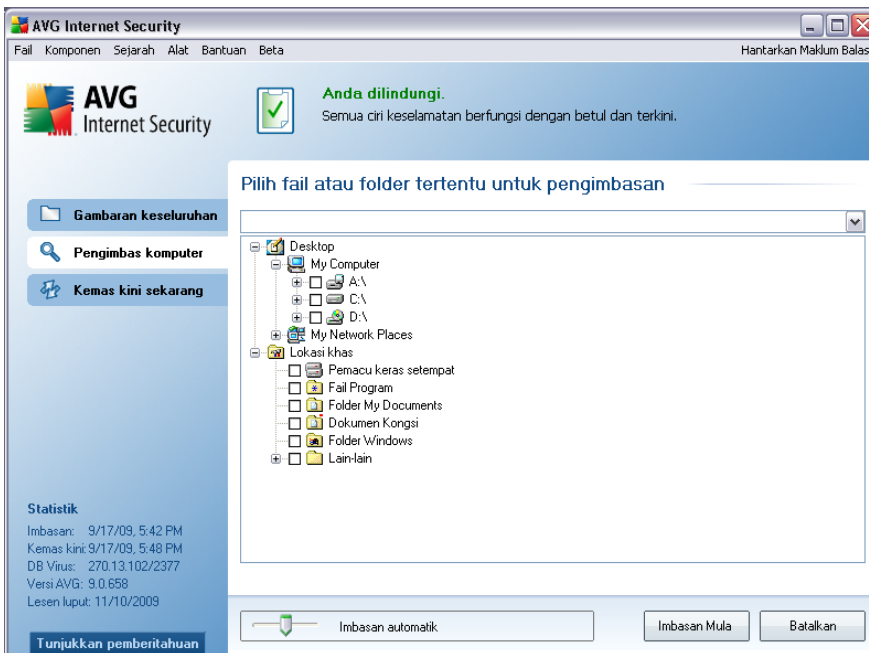
Imbas fail atau folder tertentu - mengimbas hanya kawasan komputer anda yang anda telah pilih untuk diimbas (*folder yang diimbas, cakera keras, cakera liut, CD, dll.*). Perkembangan imbasan jika pengesanan virus dan rawatannya adalah sama dengan imbas seluruh komputer: sebarang virus yang ditemui dipulihkan 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.

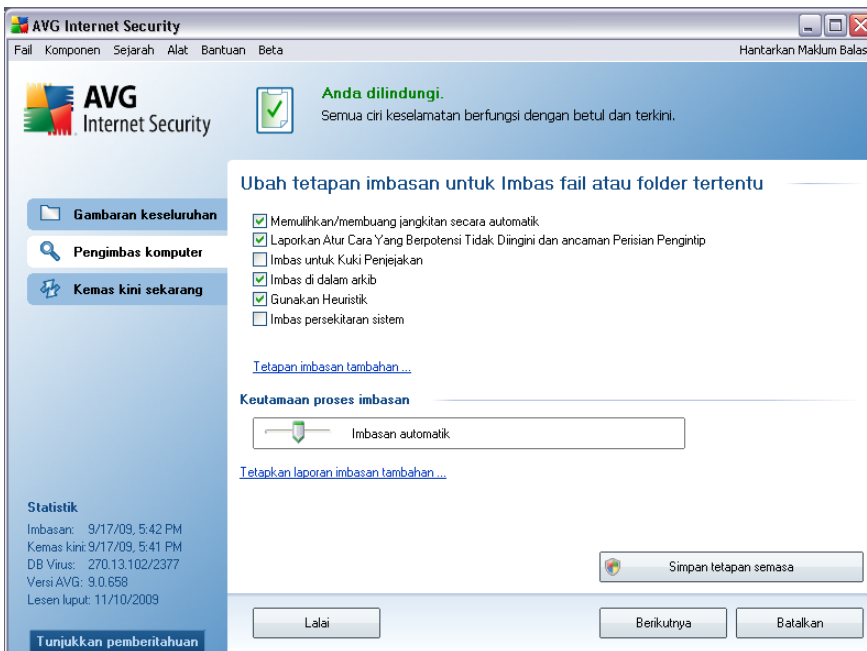
Terdapat juga kemungkinan mempunyai folder tertentu yang diimbas semasa semua subfoldernya tidak dimasukkan dalam imbasan ini, untuk melakukannya, tuliskan tanda tambah "-" di hadapan laluan yang dijana secara automatik (*lihat gambar skrin*). Untuk tidak memasukkan keseluruhan folder dari penggunaan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

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

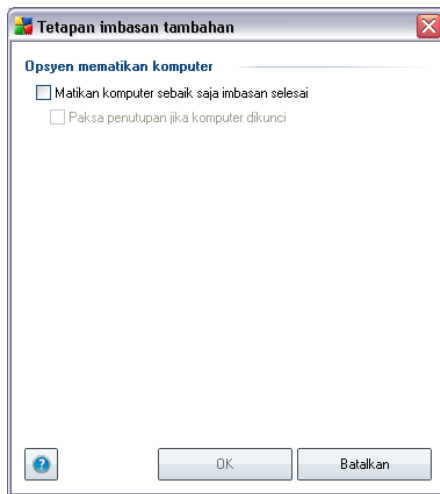


Pengeditan konfigurasi imbasan

Anda mempunyai opsiyen 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!**



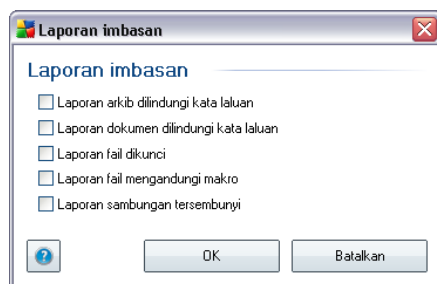
- **Parameter pengimbasan** - dalam senarai parameter pengimbasan, anda boleh menghidupkan/mematikan parameter tertentu seperti yang diperlukan (*untuk penerangan terperinci bagi tetapan ini, sila rujuk bab [Tetapan Lanjutan AVG / Pengimbasan / Imbas Fail atau Folder Tertentu](#)*).
- **Tetapan imbasan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



- **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini akan (**Mematikan komputer apabila selesai imbasan**), opsyen baru diaktifkan yang membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa matikan komputer dikunci**).
- **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbas:
 - **Semua jenis fail** dengan kemungkinan pengecualian yang ditentukan dari pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan oleh koma yang harus diimbas; atau
 - **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 ditanda, 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 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](#). Adakah anda harus 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](#)).

11.3. Pengimbasan dalam Windows Explorer

Selain daripada imbasan dipraktikkan yang dilancarkan untuk seluruh komputer atau kawasan yang dipilih, **AVG 9 Anti-Virus plus Firewall** juga menawarkan opsiyen bagi pengimbasan pantas bagi objek tertentu 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:

- **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 disediakan (cth. parameter **/scan** yang memerlukan maklumat pada bahagian mana pada komputer anda yang dipilih yang perlu diimbas dan anda perlu memberikan laluan sebenar ke bahagian yang dipilih), nilai dibahagiakan dengan koma, 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 diimbas. 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.

11.4.1. 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

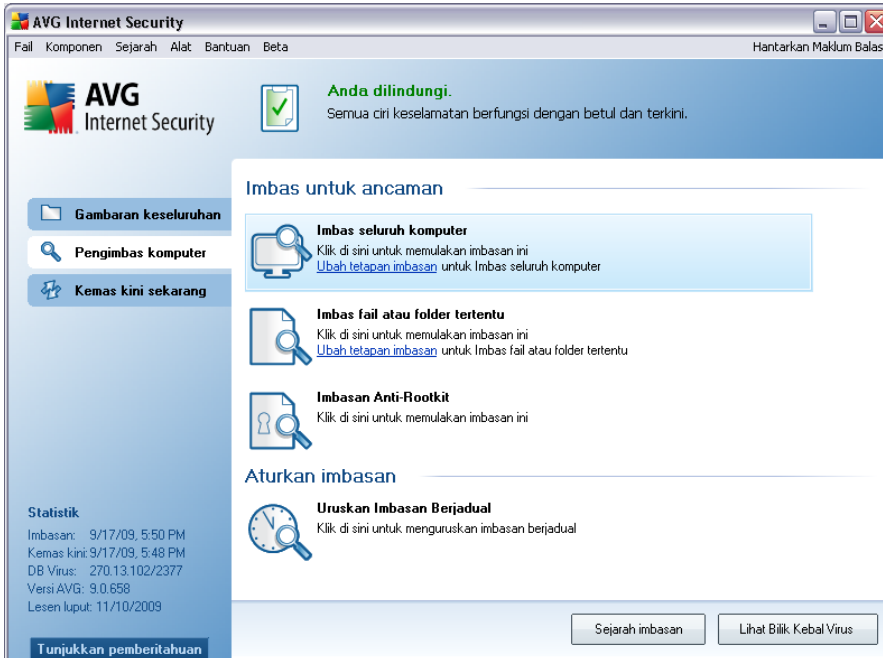
- **/COO** Imbas kuki
- **/?** Memaparkan bantuan pada topik ini
- **/HELP** Paparkan bantuan pada topik ini
- **/PRIORITY** Tetapkan keutamaan imbasan /Rendah, Auto, Tinggi/
(lihat [Tetapan / Imbasan lanjutan](#))
- **/SHUTDOWN** Mematikan komputer apabila imbasan selesai
- **/FORCESHUTDOWN** Paksa komputer dimatikan apabila imbasan selesai
- **/ADS** Imbas Aliran Data Berganti-ganti (NTFS sahaja)

11.5. Penjadualan Imbasan

Dengan **AVG 9 Anti-Virus plus Firewall** anda boleh menjalankan imbasan yang dikehendaki (contohnya semasa anda mengesyaki jangkitan telah diseret ke komputer anda) atau berdasarkan kepada rancangan 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

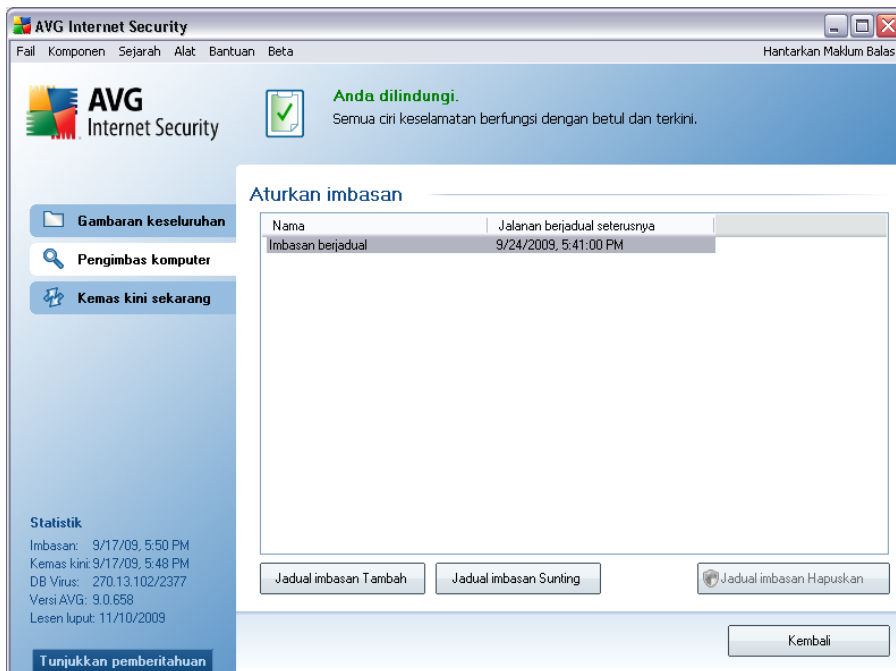
Anda harus melancarkan **Imbas seluruh komputer** secara tetap, sekurang-kurangnya sekali seminggu. Walau bagaimanapun, jika boleh, lancarkan imbas seluruh komputer setiap hari - seperti yang disediakan dalam konfigurasi lalai jadual imbasan. Jika komputer "sentiasa dihidupkan", kemudian, anda boleh 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:

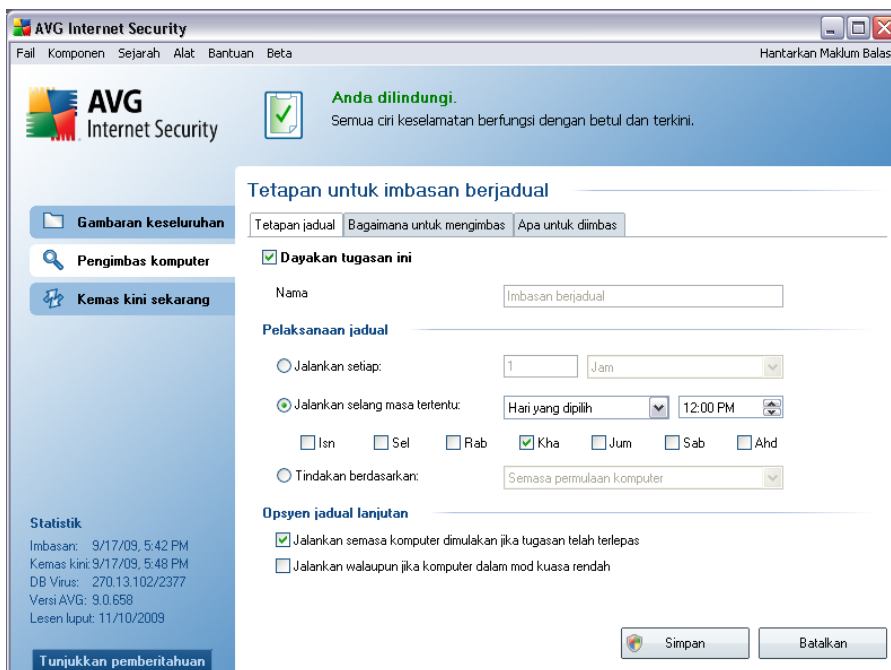


Anda boleh mengedit / menambah imbasan menggunakan butang kawalan berikut:

- **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](#)

11.5.1. Tetapan Jadual

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



Pada tab **Tetapan jadual** pertama sekali, anda boleh menanda/menyahtanda item **Dayakan tugasan ini** untuk menyahaktifkan ujian berjadual buat sementara waktu dengan mudah dan menghidupkannya semula 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:

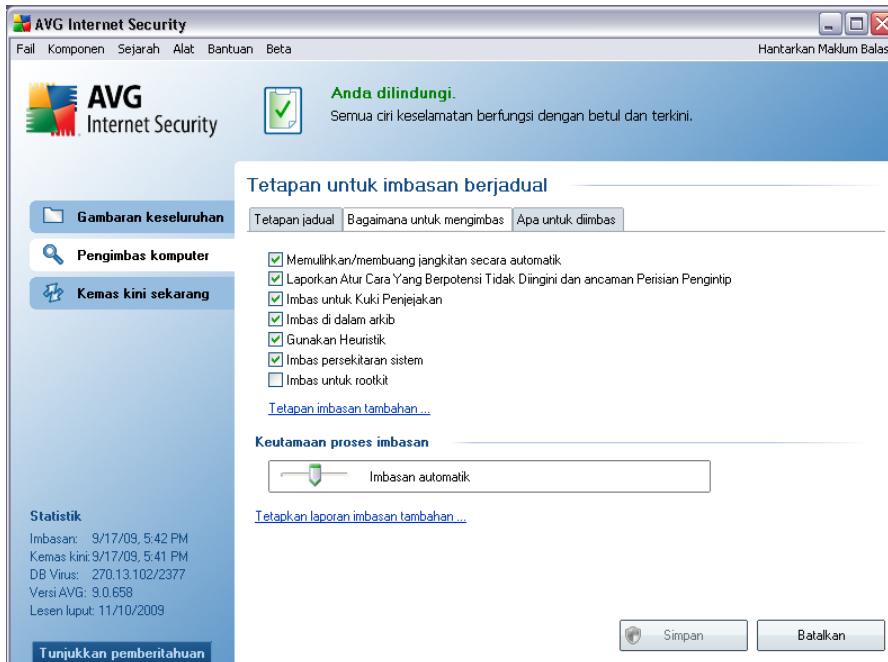
- **Jadualkan untuk dijalankan** - tentukan selang masa untuk pelancaran imbasan yang baru dijadualkan. Pemasaan boleh menjadi sama ada ditentukan oleh pelancaran imbasan berulang selepas satu tempoh masa tertentu (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan dalam 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 Tetap untuk dialog imbasan berjadual

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 diimbas](#)) dan ini mempunyai kefungsiian 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.
- **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](#).

11.5.2. Bagaimana untuk Mengimbas



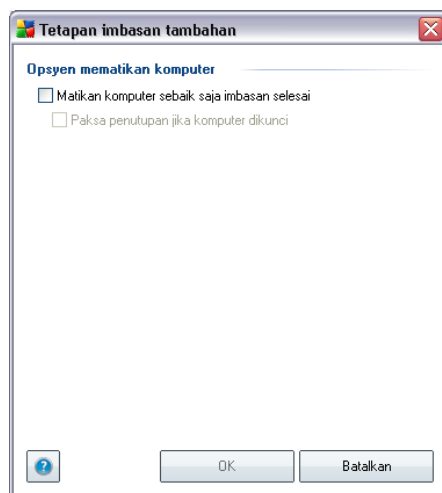
Pada tab ***Cara untuk mengimbas*** anda akan menemui senarai parameter pengimbasan yang boleh dihidupkan/dimatikan secara pilihan. Secara lalai, kebanyakan parameter dibuka dan kefungsiannya akan dilaksanakan semasa pengimbasan. Melainkan anda mempunyai alasan yang sah untuk mengubah tetapan ini, kami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

- ***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 Potensi Atur Cara yang Tidak Dikehendaki dan ancaman Perisian Pengintip*** - (*dihidupkan secara lalai*): parameter ini mengawal kefungsiannya ***AntiVirus*** yang membenarkan ***pengesanan atur cara yang berpotensi tidak dikehendaki*** (*fail boleh laku yang boleh dijalankan sebagai perisian pengintip atau adware*) dan kemudian, ini boleh disekat atau dibuang;

- **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 pengesahan, 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;

Kemudian, anda boleh mengubah konfigurasi imbasan seperti berikut:

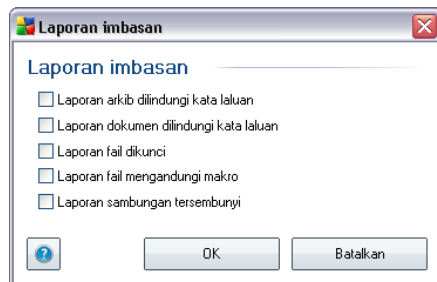
- **Tetapan imbasan tambahan** - pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



- **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini akan (**Mematikan komputer apabila selesai imbasan**), opsyen baru diaktifkan yang membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa matikan**

komputer dikunci).

- **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbas:
 - **Semua jenis fail** dengan kemungkinan pengecualian yang ditentukan dari pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan oleh koma yang harus diimbas; atau
 - **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berpotensi 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** - opsiyen 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 jenis kemungkinan penemuan yang harus dilaporkan:



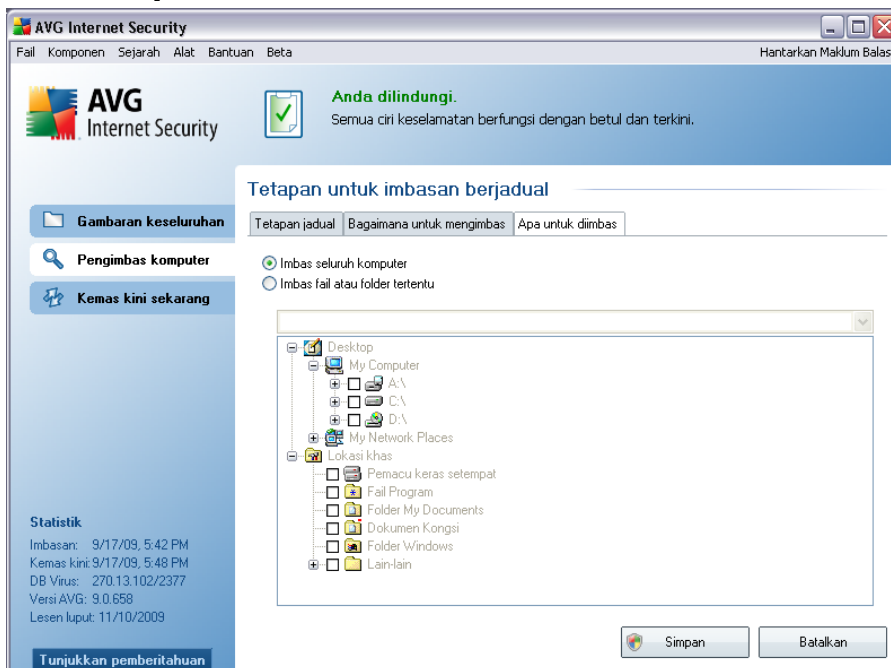
Nota: Secara lalai, konfigurasi pengimbasan disediakan untuk prestasi optimum. Melainkan, anda mempunyai alasan yang sah untuk mengubah tetapan pengimbasan, ia sangat disyorkan untuk kekal dengan konfigurasi yang dipraktakrif. Sebarang perubahan konfigurasi sepatutnya dilakukan oleh pengguna berpengalaman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

Butang kawalan

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.
- **Batalkan** - 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](#).

11.5.3. 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 fail atau folder tertentu, dalam bahagian bawah dialog ini, struktur pepohon yang dipaparkan diaktifkan dan anda boleh menentukan folder untuk diimbas.

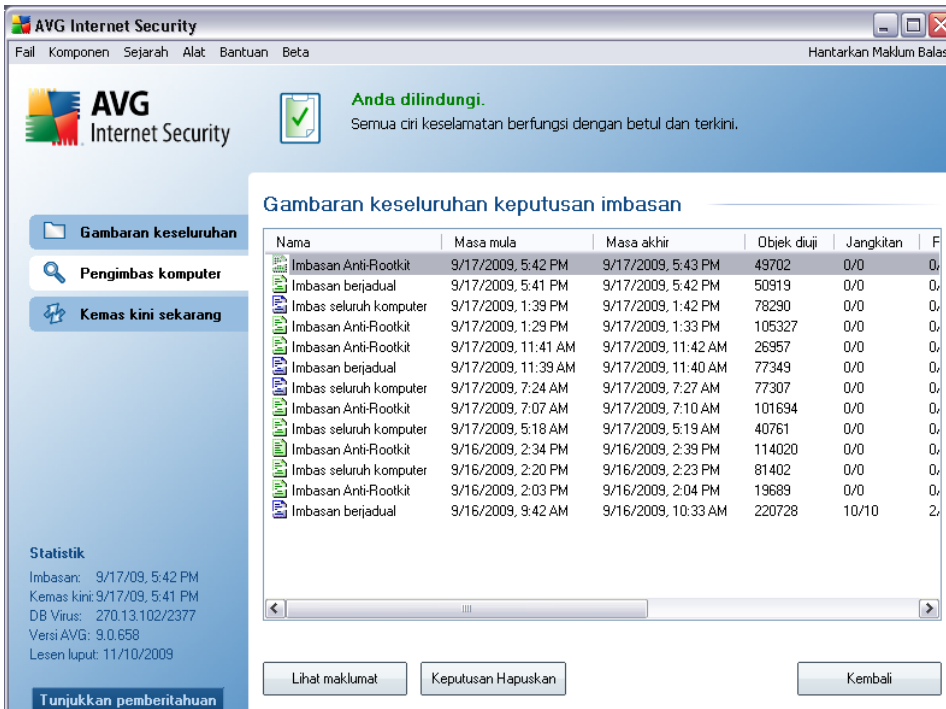
Butang kawalan Tetapan untuk dialog imbasan berjadual

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

11.6. Gambaran Keseluruhan Keputusan Imbasan



Nama	Masa mula	Masa akhir	Objek diuji	Jangkitan	F
Imbasan Anti-Rootkit	9/17/2009, 5:42 PM	9/17/2009, 5:43 PM	49702	0/0	0,
Imbasan berjadual	9/17/2009, 5:41 PM	9/17/2009, 5:42 PM	50919	0/0	0,
Imbas seluruh komputer	9/17/2009, 1:39 PM	9/17/2009, 1:42 PM	78290	0/0	0,
Imbasan Anti-Rootkit	9/17/2009, 1:29 PM	9/17/2009, 1:33 PM	105327	0/0	0,
Imbasan Anti-Rootkit	9/17/2009, 11:41 AM	9/17/2009, 11:42 AM	26957	0/0	0,
Imbasan berjadual	9/17/2009, 11:39 AM	9/17/2009, 11:40 AM	77349	0/0	0,
Imbas seluruh komputer	9/17/2009, 7:24 AM	9/17/2009, 7:27 AM	77307	0/0	0,
Imbasan Anti-Rootkit	9/17/2009, 7:07 AM	9/17/2009, 7:10 AM	101694	0/0	0,
Imbas seluruh komputer	9/17/2009, 5:18 AM	9/17/2009, 5:19 AM	40761	0/0	0,
Imbasan Anti-Rootkit	9/16/2009, 2:34 PM	9/16/2009, 2:39 PM	114020	0/0	0,
Imbas seluruh komputer	9/16/2009, 2:20 PM	9/16/2009, 2:23 PM	81402	0/0	0,
Imbasan Anti-Rootkit	9/16/2009, 2:03 PM	9/16/2009, 2:04 PM	19689	0/0	0,
Imbasan berjadual	9/16/2009, 9:42 AM	9/16/2009, 10:33 AM	220728	10/10	2,

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
- **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** - butang ini hanya aktif jika imbasan tertentu dipilih dalam gambaran keseluruhan di atas; tekannya untuk beralih ke dialog [Imbas hasil](#) untuk melihat data terperinci mengenai imbasan yang dipilih
- **Padam keputusan** - butang ini hanya aktif jika imbasan tertentu dipilih dalam gambaran keseluruhan di atas; tekannya untuk membuang item yang dipilih dari gambaran keseluruhan keputusan imbasan
- **Kembali** - mengalihkan semula ke dialog lalai bagi [antara muka imbasan AVG](#)

11.7. Keputusan Imbasan Butiran

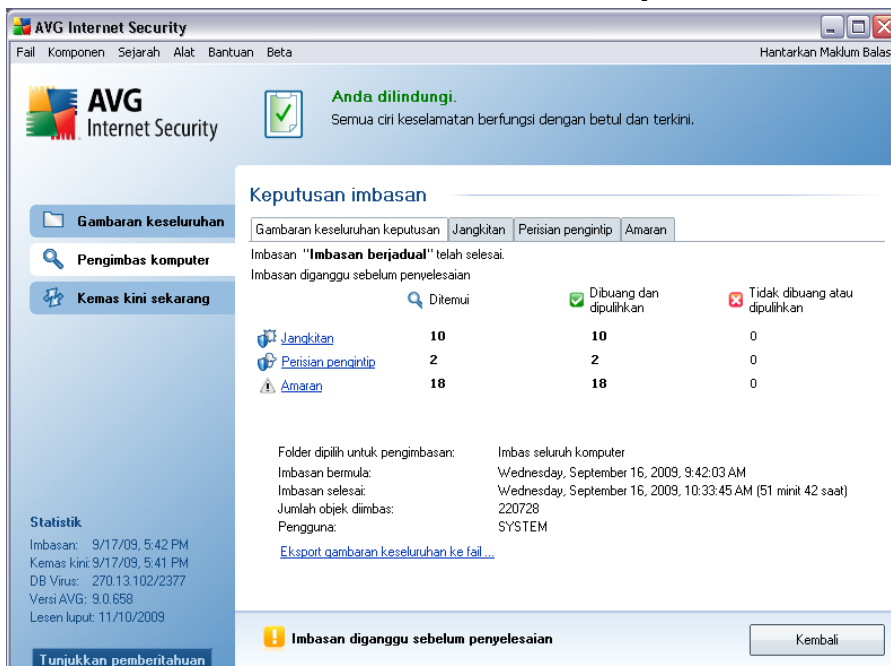
Jika dalam dialog [Imbas Gambaran Keseluruhan Keputusan](#) imbasan tertentu dipilih, kemudian, anda boleh mengklik butang **Lihat butiran** untuk beralih ke dialog **Imbas Keputusan** yang memberikan data terperinci mengenai tempoh dan

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 hanya jika beberapa objek tidak dapat diimbas yang 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

11.7.1. Tab Gambaran Keseluruhan Keputusan



AVG Internet Security

Fail Komponen Sejarah Alat Bantuan Beta Hantarkan Maklum Balas

AVG Internet Security

Anda dilindungi.
Semua ciri keselamatan berfungsi dengan betul dan terkini.

Keputusan imbasan

Gambaran keseluruhan keputusan Jangkitan Perisian pengintip Amaran

Imbasan "Imbasan berjadual" telah selesai.
Imbasan diganggu sebelum penyelesaian

	Ditemui	Dibuang dan dipulihkan	Tidak dibuang atau dipulihkan
Jangkitan	10	10	0
Perisian pengintip	2	2	0
Amaran	18	18	0

Folder dipilih untuk pengimbasan: Imbas seluruh komputer
 Imbasan bermula: Wednesday, September 16, 2009, 9:42:03 AM
 Imbasan selesai: Wednesday, September 16, 2009, 10:33:45 AM (51 minit 42 saat)
 Jumlah objek diimbas: 220728
 Pengguna: SYSTEM

[Eksport gambaran keseluruhan ke fail ...](#)

Imbasan diganggu sebelum penyelesaian

Kembali

Statistik
 Imbasan: 9/17/09, 5:42 PM
 Kemas kini: 9/17/09, 5:41 PM
 DB Virus: 270.13.102/2377
 Versi AVG: 9.0.658
 Lesen luput: 11/10/2009

Tunjukkan pemberitahuan

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

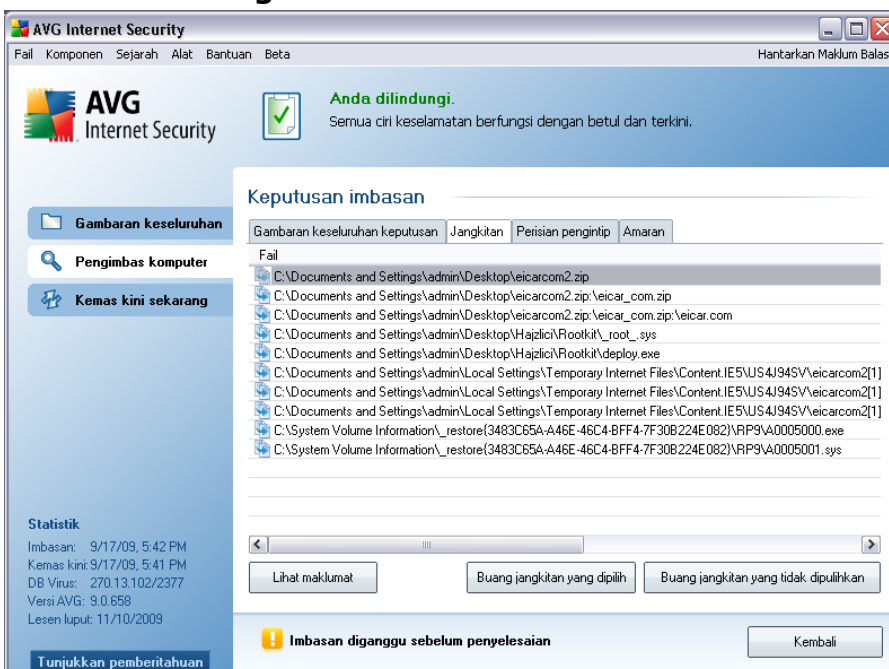
- [jangkitan virus](#) / [perisian pengintip yang dikesan](#)
- [jangkitan virus](#) / [perisian pengintip yang dibuang](#)
- bilangan [jangkitan virus](#) / [perisian pengintip](#) yang tidak boleh dibuang atau dipulihkan

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](#).

11.7.2. 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:
 - yang dijangkiti- objek yang dijangkiti dikesan dan ditinggalkan dalam lokasi asalnya (*contohnya, jika anda telah [mematikan opsyen pemulihan automatik](#) dalam tetapan imbasan khusus*)
 - yang dipulihkan- objek yang dikesan dipulihkan secara automatik dan ditinggalkan dalam lokasi asalnya
 - **Dialih ke Bilik Kebal Virus** - objek yang dijangkiti dialihkan ke kuarantin [Bilik Kebal Virus](#)
 - yang dipadamkan- objek yang dijangkiti dipadamkan
 - **Ditambah ke pengecualian PUP** - penemuan dinilai sebagai pengecualian dan ditambah kepada senarai pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian PUP](#) bagi tetapan lanjutan*)
 - **Fail dikunci - tidak diuji** - objek tersebut dikunci dan oleh itu, AVG tidak dapat mengimbasnya
 - **Berkemungkinan, objek berbahaya** - objek dikesan sebagai berkemungkinan berbahaya tetapi tidak dijangkiti(*sebagai contoh, ia boleh mengandungi*); maklumat harus diambil sebagai amaran sahaja
 - **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:

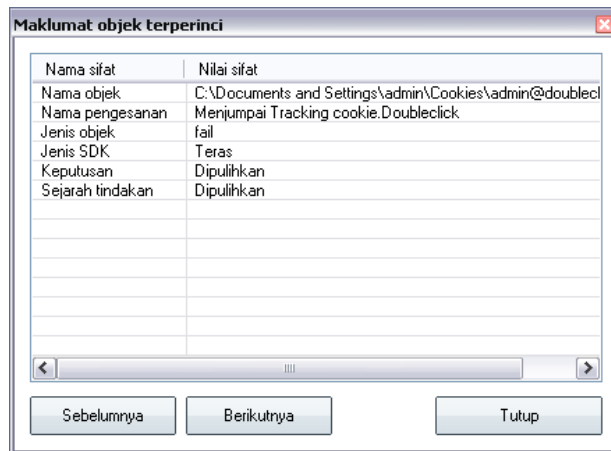
- **Lihat butiran** - butang tersebut membuka tettingkap dialog baru yang

- dijangkiti - objek yang dijangkiti dikesan dan dibiarkan dalam lokasi asalnya (contohnya, jika anda telah [mematikan opsyen pemulihan automatik](#) dalam tetapan imbasan khusus)
- **Dipulihkan** - objek yang dijangkiti dipulihkan secara automatik dan dibiarkan dalam lokasi asalnya
- **Beralih ke Bilik Kebal Virus** - objek yang dijangkiti dialih ke kuarantin [Bilik Kebal Virus](#)
- dipadamkan - objek yang dijangkiti dipadamkan
- **Ditambah pada pengecualian PUP** - penemuan dinilai sebarai pengecualian dan ditambah pada senarai pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian PUP](#) bagi tetapan lanjutan*)
- **Fail yang dikunci - tidak diuji** - objek masing-masing dikunci dan oleh sebab itu, AVG tidak dapat mengimbasnya
- **Objek berpotensi berbahaya** - objek dikesan sebagai berpotensi berbahaya tetapi tidak dijangkiti (sebagai contoh, ia boleh mengandungi makro); maklumat adalah hanya amaran
- **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 ada dalam dialog ini:

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

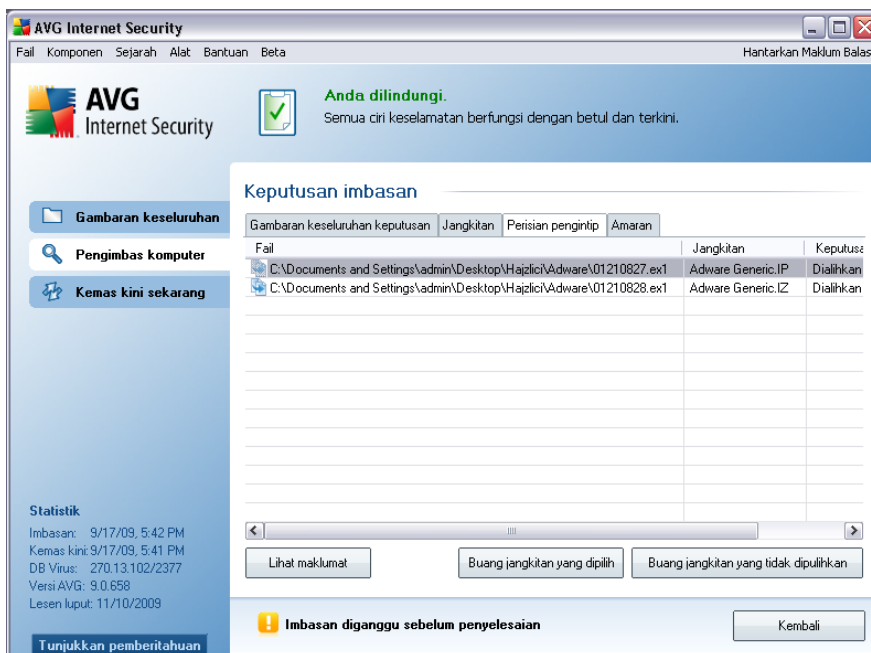


Dalam dialog ini, anda boleh mendapatkan maklumat pada lokasi objek jangkitan yang dikesan (***Nama sifat***). Dengan menggunakan butang ***Berikutnya / Seterusnya*** anda boleh melihat maklumat pada penemuan khusus. Gunakan butang ***Tutup*** untuk meninggalkan dialog ini.

- ***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](#)

11.7.4. 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 pendaftar Windows, untuk memastikan ia dimuat pada permulaan atau untuk meluaskan kesannya pada sistem pengendalian.

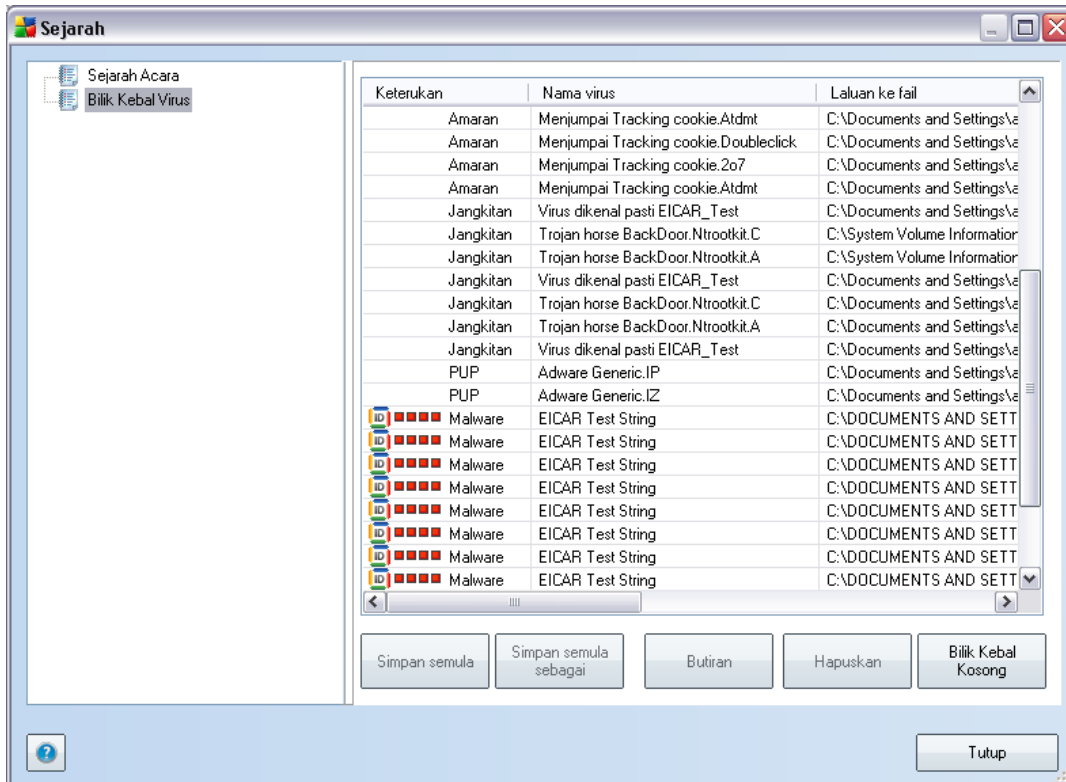
11.7.5. Tab Maklumat

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 diimbas 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.
- **Laluan fail tidak betul** - Jika beberapa fail sistem penting dijalankan daripada selain laluan lalai (*cth. winlogon.exe yang dijalankan dari selain daripada folder Windows*), AVG melaporkan percanggahan ini. Dalam sesetengah kes, virus menggunakan nama bagi proses standard untuk membuatkan kehadirannya kurang ketara dalam sistem.
- **Fail dikunci** - Fail yang dilaporkan dikunci, seterusnya, tidak boleh diimbas oleh AVG. Ini biasanya bermaksud bahawa sesetengah fail digunakan oleh sistem secara berterusan (*cth. fail pertukaran*).

11.8. Bilik Kebal Virus



Bilik Kebal Virus adalah persekitaran selamat untuk pengurusan objek disyaki/dijangkiti yang dikesan sewaktu ujian AVG. Apabila objek yang dijangkiti dikesan sewaktu imbasan dan AVG tidak boleh memulihkannya secara automatik, anda diminta untuk memutuskan apa yang perlu dilakukan dengan objek yang disyaki. Penyelesaian yang disyorkan adalah untuk mengalihkan objek ke **Bilik Kebal Virus** untuk rawatan selanjutnya.

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

- **Keseriusan** - memberikan pengenalpastian grafik bagi keseriusan penemuan tersebut pada skala empat tahap dari (■□□□) yang tidak boleh dipertikai sehingga (■■■■) yang paling berbahaya
- **Jenis jangkitan** - membezakan jenis penemuan berdasarkan pada tahap jangkitannya (*semua objek yang disenaraikan atau berpotensi 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 kolom 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.
- **Padam** - membuang fail yang dijangkiti dari **Bilik Kebal Virus** sepenuhnya
- **Kosongkan Bilik Kebal** - membuang semua **kandungan** Bilik Kebal Virus sepenuhnya

12. Kemas kini AVG

Memastikan AVG anda terkini adalah penting untuk memastikan semua virus yang baru ditemui akan dikesan secepat mungkin. 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 pangkalan AVG Virus anda adalah terkini juga sewaktu siang.

12.1. Tahap Kemas kini

AVG menawarkan dua tahap kemas kini untuk dipilih dari:

- **Kemas kini definisi** mengandungi perubahan yang diperlukan untuk perlindungan antivirus 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.

12.2. 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.

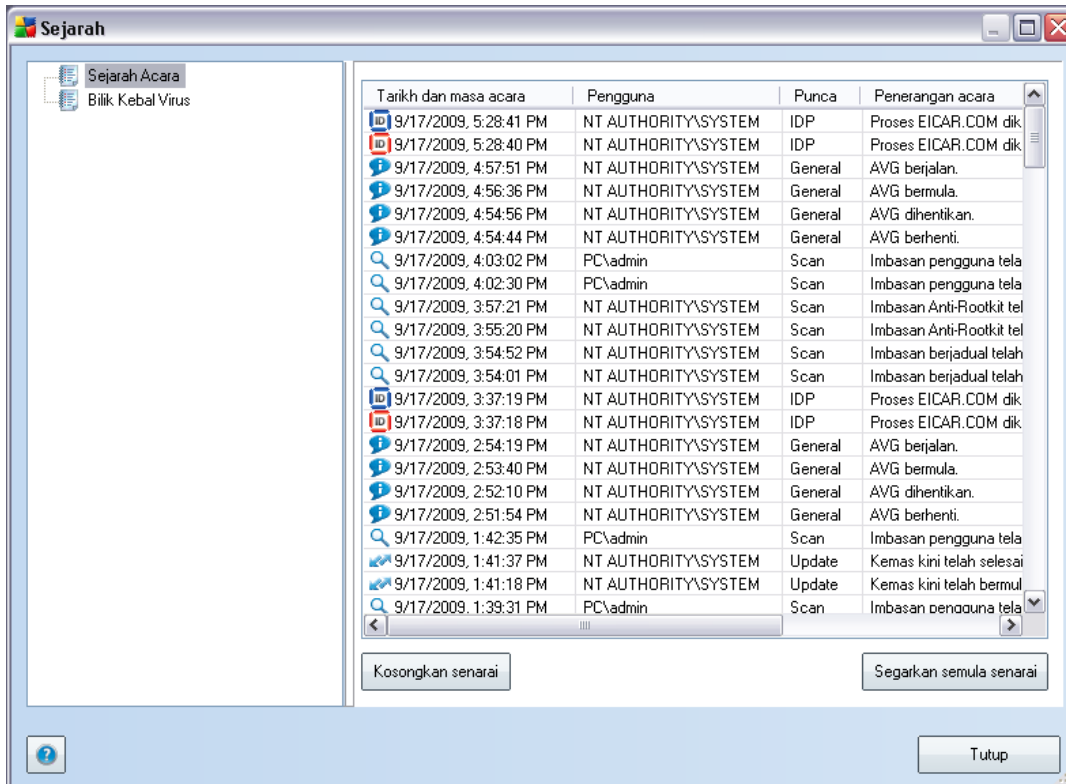
12.3. Kemas Kini Proses

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, ia 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 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. Opsyen ini boleh diakses melalui Start / All Programs / Accessories / System tools / System Restore. Disyorkan untuk pengguna berpengalaman sahaja!*

13. Sejarah Acara



Dialog **Sejarah Acara** boleh diakses dari [menu sistem](#) melalui item **Sejarah/Log Sejarah Acara**. Dalam dialog ini, anda boleh menemui ringkasan acara penting yang berlaku sewaktu operasi **AVG 9 Anti-Virus plus Firewall**. **Sejarah Acara** merekod 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

14. Soalan Lazim dan Sokongan Teknikal

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

Jika anda tidak berjaya menemui 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**.