



# AVG Internet Security 2012

## Manual Pengguna

### **Semakan dokumen 2012.20 (3/29/2012)**

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

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

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

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

Produk ini menggunakan perpustakaan pemampatan libzip2, Hak Cipta (c) 1996-2002 Julian R. Seward.



## Kandungan

<b>1. Pengenalan</b>	<b>7</b>
<b>2. Keperluan Pemasangan AVG</b>	<b>8</b>
2.1 Sistem Pengendalian yang Disokong	8
2.2 Keperluan Minimum & Disyorkan HW	8
<b>3. Proses Pemasangan AVG</b>	<b>9</b>
3.1 Selamat datang: Pemilihan Bahasa	9
3.2 Selamat datang: Perjanjian Lesen	10
3.3 Aktifkan Lesen anda	11
3.4 Pilih jenis pemasangan	12
3.5 Opsyen tersuai	14
3.6 Pasang AVG Security Toolbar	15
3.7 Perkembangan pemasangan	16
3.8 Pemasangan berjaya	17
<b>4. Selepas Pemasangan</b>	<b>18</b>
4.1 Pendaftaran produk	18
4.2 Akses ke antara muka pengguna	18
4.3 Mengimbas seluruh komputer	18
4.4 Ujian Eicar	18
4.5 Konfigurasi lalai AVG	19
<b>5. Antara Muka Pengguna AVG</b>	<b>20</b>
5.1 Menu Sistem	21
5.1.1 Fail	21
5.1.2 Komponen	21
5.1.3 Sejarah	21
5.1.4 Alat	21
5.1.5 Bantuan	21
5.1.6 Sokongan	21
5.2 Maklumat Status Keselamatan	28
5.3 Pautan Pantas	29
5.4 Gambaran keseluruhan Komponen	30
5.5 Ikon Dulang Sistem	32
5.6 Penasihat AVG	34
5.7 Alat AVG	34



<b>6. Komponen AVG</b>	<b>37</b>
6.1 Anti-Virus	37
6.1.1 Enjin Pengimbasan	37
6.1.2 Perlindungan Residen	37
6.1.3 Perlindungan AntiPerisian Pengintip	37
6.1.4 Antara Muka Anti-Virus	37
6.1.5 Pengesanan Resident Shield	37
6.2 LinkScanner	43
6.2.1 Antara Muka LinkScanner	43
6.2.2 Pengesanan Search-Shield	43
6.2.3 Pengesanan Surf-Shield	43
6.2.4 Pengesanan Online Shield	43
6.3 Perlindungan E-mel	49
6.3.1 E-mail Scanner	49
6.3.2 Anti-Spam	49
6.3.3 Antara Muka Perlindungan E-mel	49
6.3.4 Pengesanan Pengimbas E-mel	49
6.4 Firewall	53
6.4.1 Prinsip Firewall	53
6.4.2 Profil Firewall	53
6.4.3 Antara Muka Firewall	53
6.5 AntiRootkit	57
6.5.1 Antara Muka AntiRootkit	57
6.6 Alatan Sistem	59
6.6.1 Proses	59
6.6.2 Sambungan Rangkaian	59
6.6.3 Automula	59
6.6.4 Sambungan Penyemak Imbas	59
6.6.5 Pemandang LSP	59
6.7 Penganalisis PC	65
6.8 Identity Protection	66
6.8.1 Antara Muka Identity Protection	66
6.9 Pentadbiran Jauh	69
<b>7. App saya</b>	<b>70</b>
7.1 AVG Family Safety	70
7.2 AVG LiveKive	71
7.3 AVG Mobilation	71



7.4 AVG PC Tuneup.....	72
<b>8. AVG Security Toolbar.....</b>	<b>74</b>
<b>9. AVG Do Not Track.....</b>	<b>76</b>
9.1 Antara muka AVG Do Not Track.....	77
9.2 Maklumat tentang proses penjejakan.....	78
9.3 Menyekat proses penjejakan.....	79
9.4 Tetapan AVG Do Not Track.....	80
<b>10. Tetapan Lanjutan AVG.....</b>	<b>83</b>
10.1 Penampilan.....	83
10.2 Bunyi.....	86
10.3 Menyahdayakan perlindungan AVG buat sementara waktu.....	87
10.4 AntiVirus.....	89
10.4.1 Resident Shield.....	89
10.4.2 Pelayan Cache.....	89
10.5 Perlindungan e-mel.....	95
10.5.1 Pengimbas E-mel.....	95
10.5.2 AntiSpam.....	95
10.6 LinkScanner.....	113
10.6.1 Tetapan LinkScanner.....	113
10.6.2 Online Shield.....	113
10.7 Imbasan.....	117
10.7.1 Imbasan seluruh komputer.....	117
10.7.2 Imbasan sambungan kerangka.....	117
10.7.3 Imbasan fail atau folder khusus.....	117
10.7.4 Imbasan peranti boleh dialihkan.....	117
10.8 Jadual.....	123
10.8.1 Imbasan yang Dijadualkan.....	123
10.8.2 Jadual Kemas Kini Definisi.....	123
10.8.3 Jadual Kemas Kini Atur Cara.....	123
10.8.4 Jadual Kemas Kini AntiSpam.....	123
10.9 Kemas kini.....	134
10.9.1 Proksi.....	134
10.9.2 Dailan.....	134
10.9.3 URL.....	134
10.9.4 Uruskan.....	134
10.10 AntiRootkit.....	140



10.10.1 Kekecualian .....	140
10.11 Identity Protection .....	142
10.11.1 Tetapan Identity Protection .....	142
10.11.2 Senarai dibenarkan .....	142
10.12 Atur Cara yang Berpotensi Tidak Diingini .....	146
10.13 Bilik Kebal Virus .....	149
10.14 Program Pembaikan Produk .....	149
10.15 Abaikan status ralat .....	152
10.16 Penasihat – Rangkaian Diketahui .....	153
<b>11. Tetapan Firewall .....</b>	<b>154</b>
11.1 Umum .....	154
11.2 Keselamatan .....	155
11.3 Profil Kawasan dan Penyesuai .....	156
11.4 IDS .....	158
11.5 Log .....	160
11.6 Profil .....	161
11.6.1 Maklumat Profil .....	161
11.6.2 Rangkaian yang Ditentukan .....	161
11.6.3 Aplikasi .....	161
11.6.4 Perkhidmatan Sistem .....	161
<b>12. Pengimbasan AVG .....</b>	<b>172</b>
12.1 Antara Muka Pengimbasan .....	172
12.2 Imbasan Pratakrif .....	173
12.2.1 Imbasan Seluruh Komputer .....	173
12.2.2 Imbas Fail atau Folder Tertentu .....	173
12.3 Pengimbasan dalam Windows Explorer .....	182
12.4 Pengimbasan Garis Perintah .....	182
12.4.1 Parameter Imbasan CMD .....	182
12.5 Penjadualan Imbasan .....	185
12.5.1 Tetapan Jadual .....	185
12.5.2 Bagaimana untuk Mengimbas .....	185
12.5.3 Apa untuk Diimbas .....	185
12.6 Gambaran Keseluruhan Keputusan Imbasan .....	195
12.7 Butiran Keputusan Imbasan .....	196
12.7.1 Tab Gambaran Keseluruhan Keputusan .....	196
12.7.2 Tab Jangkitan .....	196
12.7.3 Tab Perisian Pengintip .....	196



12.7.4 Tab Amaran.....	196
12.7.5 Tab Rootkit.....	196
12.7.6 Tab Maklumat .....	196
12.8 Bilik Kebal Virus.....	204
<b>13. Kemas kini AVG.....</b>	<b>206</b>
13.1 Pelancaran kemas kini.....	206
13.2 Perkembangan kemas kini.....	206
13.3 Tahap kemas kini.....	207
<b>14. Sejarah Acara .....</b>	<b>209</b>
<b>15. Soalan Lazim dan Sokongan Teknikal.....</b>	<b>211</b>



## 1. Pengenalan

Manual pengguna ini memberikan dokumentasi menyeluruh untuk **AVG Internet Security 2012**.

**AVG Internet Security 2012** memberikan berbilang lapisan perlindungan untuk segala-gala yang anda lakukan dalam talian, yang bermaksud anda tidak perlu risau mengenai kecurian identiti, virus atau melawati tapak berbahaya. AVG Protective Cloud Technology dan AVG Community Protection Network disertakan, bermaksud kami mengumpul maklumat ancaman terkini dan berkongsinya dengan komuniti kami untuk memastikan anda mendapat perlindungan terbaik:

- Beli-belah dan buat urusan bank dalam talian secara selamat dengan Firewall, AntiSpam & AVG Identity Protection
- Kekal selamat pada rangkaian sosial dengan AVG Social Networking Protection
- Layari dan cari dengan yakin dengan perlindungan masa nyata LinkScanner



## 2. Keperluan Pemasangan AVG

### 2.1. Sistem Pengendalian yang Disokong

**AVG Internet Security 2012** adalah bertujuan untuk melindungi stesen kerja dengan sistem pengendalian berikut:

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

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

**Nota:** Komponen [Perlindungan ID](#) tidak disokong pada Windows XP x64. Pada sistem pengendalian ini, anda boleh memasang AVG Internet Security 2012 tetapi hanya tanpa komponen IDP.

### 2.2. Keperluan Minimum & Disyorkan HW

Keperluan perkakasan minimum untuk **AVG Internet Security 2012**:

- Intel Pentium CPU 1,5 GHz
- 512 MB memori RAM
- 1000 MB bagi ruang kosong pemacu keras (untuk tujuan pemasangan)

Keperluan perkakasan disyorkan untuk **AVG Internet Security 2012**:

- Intel Pentium CPU 1,8 GHz
- 512 MB memori RAM
- 1550 MB bagi ruang kosong pemacu keras (untuk tujuan pemasangan)





### 3. Proses Pemasangan AVG

#### Di mana saya boleh mendapatkan fail pemasangan?

Untuk memasang **AVG Internet Security 2012** pada komputer anda, anda perlu mendapatkan fail pemasangan terkini. Untuk memastikan anda memasang versi terkini bagi **AVG Internet Security 2012**, adalah disyorkan untuk memuat turun fail pemasangan dari laman web AVG (<http://www.avg.com/>). Seksyen **Pusat Sokongan / Muat Turun** memberikan gambaran keseluruhan berstruktur bagi fail pemasangan untuk setiap edisi AVG.

Jika anda tidak pasti fail mana yang anda perlu muat turun dan pasang, anda mungkin ingin menggunakan perkhidmatan **Pilih produk** di bahagian bawah halaman web. Selepas anda menjawab tiga soalan mudah, perkhidmatan ini menentukan fail sebenar yang anda perlukan. Tekan butang **Teruskan** untuk dihalu semula ke senarai lengkap bagi fail muat turun yang disesuaikan untuk keperluan peribadi anda.

#### Bagaimanakan rupa proses pemasangan?

Sebaik sahaja anda telah memuat turun dan menyimpan fail pemasangan pada cakera keras anda, anda boleh melancarkan proses pemasangan. Pemasangan ialah urutan ringkas dan mudah untuk memahami dialog. Setiap dialog menerangkan secara ringkas apa yang perlu dilakukan pada setiap langkah proses pemasangan. Berikut, kami memberikan penerangan terperinci bagi setiap tettingkap dialog:

#### 3.1. Selamat datang: Pemilihan Bahasa

Proses pemasangan bermula dengan dialog **Selamat Datang ke AVG Installer** :



Dalam dialog ini anda boleh memilih bahasa yang digunakan untuk proses pemasangan. Pada penjuru kanan dialog, klik kotak kombo untuk menggulung ke bawah menu bahasa. Pilih bahasa

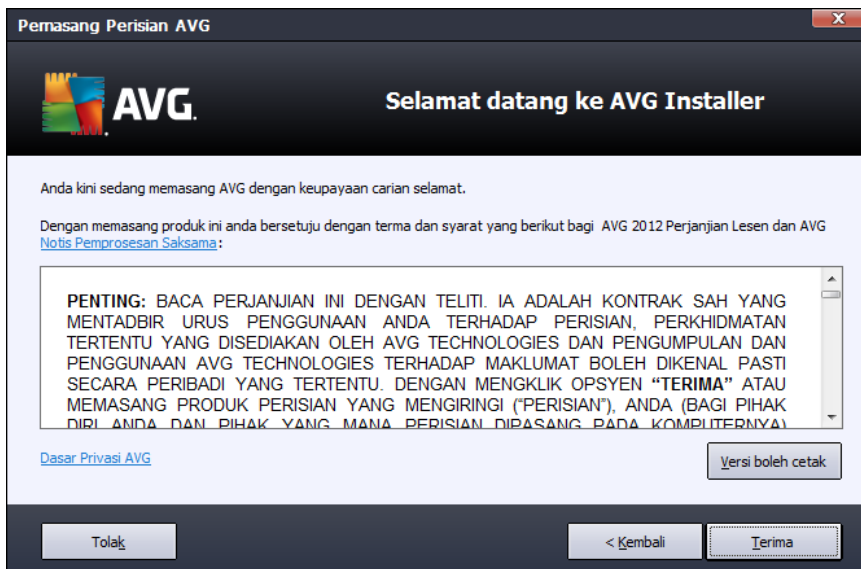


yang dikehendaki, dan proses pemasangan akan meneruskan selanjutnya dalam bahasa pilihan anda.

**Perhatian: Buat masa ini, anda hanya memilih bahasa bagi proses pemasangan. Aplikasi AVG Internet Security 2012 akan dipasang dalam bahasa yang dipilih, dan dalam bahasa Inggeris yang sentiasa dipasang secara automatik. Walau bagaimanapun, anda boleh mempunyai lebih banyak bahasa dan untuk bekerja dengan AVG Internet Security 2012 dalam mana-mana yang ini. Anda akan dijemput untuk mengesahkan pilihan penuh anda bagi bahasa alternatif dalam salah satu dialog persediaan berikut yang dinamakan [Pilihan Tersuai](#).**

### 3.2. Selamat datang: Perjanjian Lesen

Dalam langkah seterusnya, dialog **Selamat Datang ke AVG Installer** memberikan penerangan penuh mengenai perjanjian lesen AVG:



Sila baca keseluruhan teks dengan teliti. Untuk mengesahkan bahawa anda telah membaca, memahami dan menerima perjanjian ini tekan butang **Terima**. Jika anda tidak bersetuju dengan perjanjian lesen ini, tekan butang **Tolak**, dan proses pemasangan akan ditamatkan serta-merta.

#### Dasar Privasi AVG

Selain daripada perjanjian lesen, dialog persediaan ini juga memberikan anda pilihan untuk mengetahui selanjutnya mengenai dasar privasi AVG. Pada penjuru bawah kiri bagi dialog, anda boleh nampak pautan **Dasar Privasi AVG**. Kliknya untuk dihala semula ke laman web AVG (<http://www.avg.com/>) yang anda boleh mendapatkan prinsip dasar privasi AVG Technologies lengkap.

#### Butang kawalan

Dalam dialog persediaan pertama, terdapat hanya dua butang kawalan yang tersedia:



- **Versi boleh cetak** – Klik untuk mencetak penerangan penuh perjanjian lesen AVG.
- **Tolak** – Klik untuk menolak perjanjian lesen. Proses persediaan akan berhenti dengan serta-merta. **AVG Internet Security 2012** tidak akan dipasang!
- **Undur** – Klik untuk kembali satu langkah ke belakang ke dialog persediaan sebelumnya.
- **Terima** - Klik untuk mengesahkan bahawa anda telah membaca, memahami dan menerima perjanjian lesen. Pemasangan akan diteruskan, dan anda akan pergi ke satu langkah seterusnya ke dialog persediaan berikut.

### 3.3. Aktifkan Lesen anda

Dalam dialog **Aktifkan Lesen Anda** anda dijemput untuk mengisi nombor lesen anda ke dalam medan teks yang disediakan:

**Pemasang Perisian AVG**

**AVG** Aktifkan Lesen Anda

Nombor Lesen:

Contoh: IQNP6-9BCA8-PUQU2-A5HCK-GP338L-93OCB

Jika anda membeli perisian AVG 2012 dalam talian anda, nombor lesen anda telah dihantar 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. Sila pastikan anda menyalin nombor dengan betul.

Batalkan < Kembali Berikutnya >

#### Di manakah untuk mencari nombor lesen

Nombor jualan boleh ditemui pada bungkusan CD dalam kotak **AVG Internet Security 2012** anda. Nombor lesen akan berada dalam e-mel pengesahan yang anda terima selepas membeli **AVG Internet Security 2012** anda dalam talian. Anda mesti menaip nombor betul-betul seperti yang ditunjukkan. Jika bentuk digital nombor lesen tersedia (*dalam e-mel*), ia disyorkan untuk menggunakan kaedah salin dan tampal untuk memasukkannya.

#### Bagaimana untuk menggunakan kaedah Salin & Tampal

Menggunakan kaedah **Salin & Tampal** untuk memasukkan nombor lesen **AVG Internet Security 2012** anda ke dalam atur cara memastikan nombor itu dimasukkan dengan betul. Sila ikuti langkah-langkah ini:



- Buka e-mel yang mengandungi nombor lesen anda.
- Klik butang tetikus kiri pada permulaan nombor lesen, tahan dan seret tetikus ke hujung nombor, dan kemudian, lepaskan butang. Sekarang, nombor perlu diserlahkan.
- Tekan dan tahan **Ctrl** dan kemudian, tekan **C**. Ia menyalin nombor.
- Halakan dan klik kedudukan di mana anda hendak menampal nombor yang disalin.
- Tekan dan tahan **Ctrl** dan kemudian, tekan **V**. Ia menampal nombor ke lokasi yang anda pilih.

### Butang kawalan

Sama seperti dalam kebanyakan dialog persediaan, terdapat tiga butang kawalan yang tersedia:

- **Batal** – Klik untuk keluar dari proses persediaan dengan serta-merta; **AVG Internet Security 2012** tidak akan dipasang!
- **Undur** – Klik untuk kembali ke dialog persediaan sebelumnya.
- **Seterusnya** – Klik untuk teruskan pemasangan dan pergi satu langkah seterusnya.

### 3.4. Pilih jenis pemasangan

Dialog **Pilih jenis pemasangan** menawarkan pilihan dua opsyen pemasangan: **Ekspres** dan **Pemasangan Tersuai**:





## Pemasangan ekspres

Untuk kebanyakan pengguna, adalah amat disyorkan supaya menyimpan pemasangan **Ekspres** standard yang memasang **AVG Internet Security 2012** dalam mod automatik penuh dengan tetapan dipratakrifkan oleh vendor atur cara, termasuk [Alat AVG](#). Konfigurasi ini memberikan keselamatan maksimum yang digabungkan dengan penggunaan optimum sumber. Pada masa hadapan, jika keperluan meningkat untuk mengubah konfigurasi, anda akan sentiasa mempunyai kemungkinan untuk melakukannya secara terus dalam aplikasi **AVG Internet Security 2012**.

Dalam opsyen ini anda boleh melihat dua kotak semak yang telah sedia disahkan dan adalah amat disyorkan supaya membiarkan kedua-dua opsyen ditandakan.

- **Saya ingin menetapkan AVG Secure Search sebagai pembekal carian lalai saya** – biar ditandakan untuk mengesahkan bahawa anda mahu menggunakan enjin AVG Secure Search yang bekerjasama dengan komponen [Link Scanner](#) untuk keselamatan maksimum anda di dalam talian.
- **Saya ingin memasang AVG Security Toolbar** – biar ditandakan untuk memasang [AVG Security Toolbar](#) yang melindungi keselamatan maksimum anda semasa menyemak lalu Internet.

Tekan butang **Seterusnya** untuk meneruskan ke dialog [Pasang AVG Security Toolbar](#) berikut.

## Pemasangan tersuai

**Pemasangan Tersuai** sepatutnya hanya digunakan oleh pengguna berpengalaman yang mempunyai alasan yang sah untuk memasang **AVG Internet Security 2012** menggunakan tetapan bukan standard, cth. untuk disesuaikan dengan keperluan sistem khusus.

Jika anda memutuskan untuk memilih opsyen ini, bahagian baharu yang dipanggil **Folder Destinasi** muncul dalam dialog. Di sini, anda seharusnya menentukan lokasi di mana **AVG Internet Security 2012** harus dipasangkan. Secara lalainya, **AVG Internet Security 2012** akan dipasangkan ke folder fail program yang terletak di pemacu C:, seperti yang dinyatakan dalam medan teks dalam dialog. Jika anda hendak mengubah lokasi ini, gunakan butang **Semak Imbas** untuk memaparkan struktur pemacu dan pilih folder berkaitan. Untuk kembali semula ke destinasi lalai yang dipratetap oleh vendor perisian gunakan butang **Lalai**.

Kemudian, tekan butang **Seterusnya** untuk meneruskan ke dialog [Opsyen Tersuai](#).

## Butang kawalan

Sama seperti dalam kebanyakan dialog persediaan, terdapat tiga butang kawalan yang tersedia:

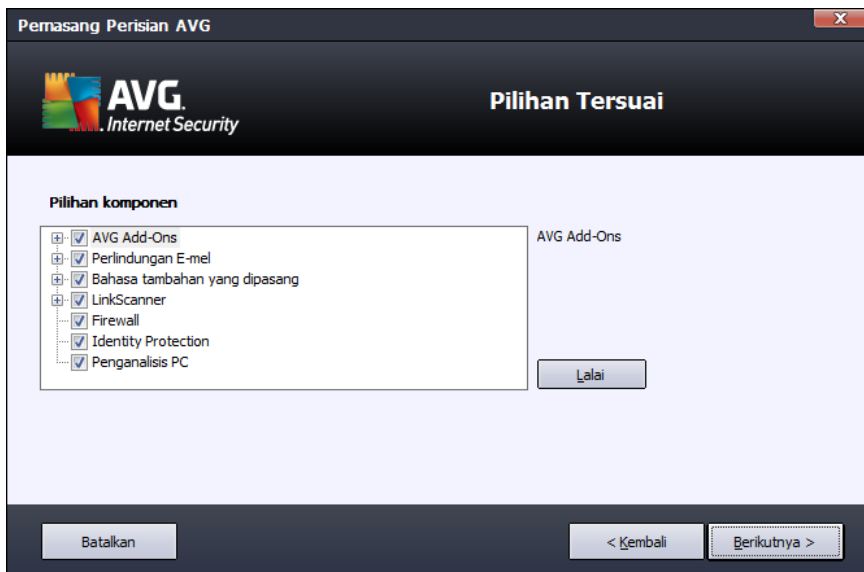
- **Batal** – Klik untuk keluar dari proses persediaan dengan serta-merta; **AVG Internet Security 2012** tidak akan dipasang!
- **Undur** – Klik untuk kembali ke dialog persediaan sebelumnya.



- **Seterusnya** – Klik untuk teruskan pemasangan dan pergi satu langkah seterusnya.

### 3.5. Opsyen tersuai

Dialog **Opsyen Tersuai** membenarkan anda untuk menetapkan parameter terperinci bagi pemasangan:



Seksyen **Pemilihan Komponen** menyediakan gambaran keseluruhan bagi semua komponen **AVG Internet Security 2012** yang boleh dipasang. Jika tetapan lalai tidak sesuai dengan anda, anda boleh membuang/menambah komponen tertentu.

**Walau bagaimanapun, anda hanya boleh memilih dari komponen yang termasuk dalam edisi AVG yang anda beli!**

Serlahkan mana-mana item dalam senarai **Pemilihan Komponen**, dan penerangan ringkas komponen berkaitan akan dipaparkan di sebelah kanan seksyen ini. Untuk maklumat terperinci mengenai kefungsiannya setiap komponen sila rujuk bab [Gambaran Keseluruhan Komponen](#) dokumentasi ini. Untuk kembali semula ke konfigurasi lalai yang dipratetap oleh vendor perisian gunakan butang **Lalai**.

#### Butang kawalan

Sama seperti dalam kebanyakan dialog persediaan, terdapat tiga butang kawalan yang tersedia:

- **Batal** – Klik untuk keluar dari proses persediaan dengan serta-merta; **AVG Internet Security 2012** tidak akan dipasang!
- **Undur** – Klik untuk kembali ke dialog persediaan sebelumnya.
- **Seterusnya** – Klik untuk teruskan pemasangan dan pergi satu langkah seterusnya.



### 3.6. Pasang AVG Security Toolbar



Dalam dialog **Pasang AVG Security Toolbar**, tentukan sama ada anda hendak memasang [AVG Security Toolbar](#). Jika anda tidak mengubah tetapan lalai, komponen ini akan dipasang secara automatik ke dalam penyemak imbas Internet anda (*penyemak imbas yang disokong buat masa ini adalah Microsoft Internet Explorer v. 6.0 atau lebih tinggi, dan Mozilla Firefox v. 3.0 atau lebih tinggi*) dan memberikan anda perlindungan dalam talian menyeluruh semasa melayari Internet.

Serta, anda mempunyai opsiyen untuk menentukan sama ada anda hendak memilih *AVG Secure Search (powered by Google)* sebagai pembekal carian lalai anda. Jika benar, biarkan kotak semak berkaitan bertanda.

#### Butang kawalan

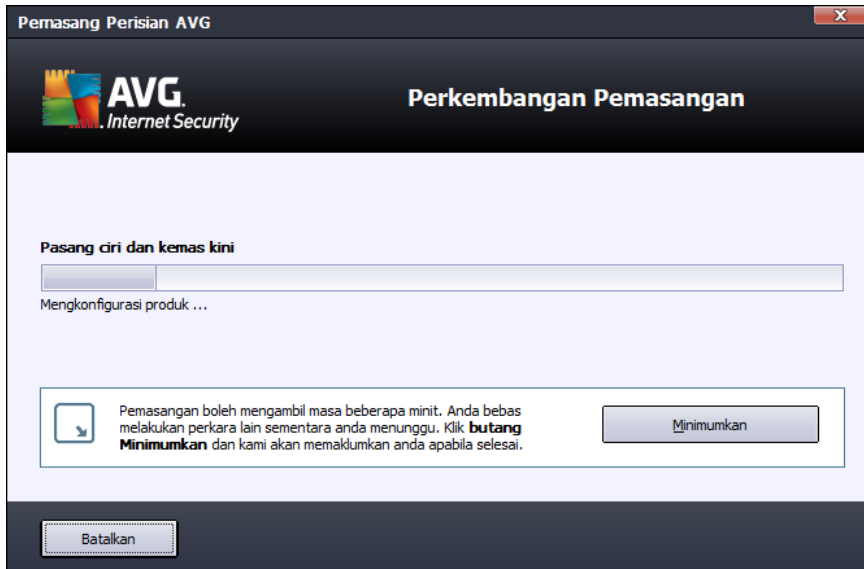
Sama seperti dalam kebanyakan dialog persediaan, terdapat tiga butang kawalan yang tersedia:

- **Batal** – Klik untuk keluar dari proses persediaan dengan serta-merta; **AVG Internet Security 2012** tidak akan dipasang!
- **Undur** – Klik untuk kembali ke dialog persediaan sebelumnya.
- **Seterusnya** – Klik untuk teruskan pemasangan dan pergi satu langkah seterusnya.



### 3.7. Perkembangan pemasangan

Dialog *Perkembangan Pemasangan* menunjukkan perkembangan proses pemasangan dan tidak memerlukan sebarang campur tangan:



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

#### Butang kawalan

Dalam dialog ini, terdapat hanya satu butang kawalan tersedia – **Batal**. Butang ini hanya perlu digunakan jika anda ingin menghentikan proses pemasangan yang dijalankan. Sila ingat bahawa dalam kes seperti itu, **AVG Internet Security 2012** anda tidak akan dipasang!





### 3.8. Pemasangan berjaya

Dialog *Pemasangan berjaya* mengesahkan bahawa **AVG Internet Security 2012** anda telah dipasang dan dikonfigurasi sepenuhnya:



#### Program Pembaikan Produk

Di sini anda boleh memutuskan sama ada anda ingin menyertai Program Pembaikan Produk (*untuk butiran, lihat bab [Tetapan Lanjutan AVG / Program Pembaikan Produk](#)*) yang mengumpul maklumat tanpa nama mengenai ancaman yang dikesan untuk meningkatkan tahap keselamatan Internet keseluruhannya. Jika anda bersetuju dengan kenyataan ini, sila kekalkan pilihan **Saya bersetuju untuk menyertai keselamatan web AVG 2012 dan Program Pembaikan Produk ...** yang ditanda (*pilihan disahkan, secara lalai*).

#### Komputer dihidupkan semula

Untuk memuktamadkan proses pemasangan anda perlu memulakan semula komputer anda: pilih sama ada anda ingin **Mula Semula Sekarang**, atau anda ingin menangguhkan tindakan ini – **Mula Semula Kemudian**.



## 4. Selepas Pemasangan

### 4.1. Pendaftaran produk

Setelah menyelesaikan pemasangan, **AVG Internet Security 2012**, sila daftarkan produk anda dalam talian di laman web (<http://www.avg.com/>). 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.

Cara paling mudah untuk mendaftar secara terus dari antara muka pengguna **AVG Internet Security 2012**. Dalam menu utama, sila pilih item [Bantu/Daftar sekarang](#). Anda akan dihala semula ke halaman **Pendaftaran** di laman web AVG (<http://www.avg.com/>). Sila ikut arahan yang diberikan dalam halaman.

### 4.2. Akses ke antara muka pengguna

[Dialog utama AVG](#) boleh diakses dalam beberapa cara:

- klik dua kali [ikon dulang sistem AVG](#)
- klik dua kali ikon AVG pada desktop
- dari menu **Start / All Programs / AVG 2012**

### 4.3. Mengimbas seluruh komputer

Terdapat kemungkinan risiko bahawa virus komputer telah dihantar ke komputer anda sebelum pemasangan **AVG Internet Security 2012**. Atas sebab itu, anda harus menjalankan [Imbas seluruh komputer](#) untuk memastikan tiada jangkitan pada PC anda. Imbasan pertama mungkin mengambil sedikit masa (*kira-kira satu jam*) tetapi adalah disyorkan untuk melancarkannya bagi memastikan bahawa komputer anda tidak terjejas akibat ancaman. Untuk arahan bagi menjalankan [Imbas seluruh komputer](#) rujuk bab [Pengimbasan AVG](#).

### 4.4. Ujian Eicar

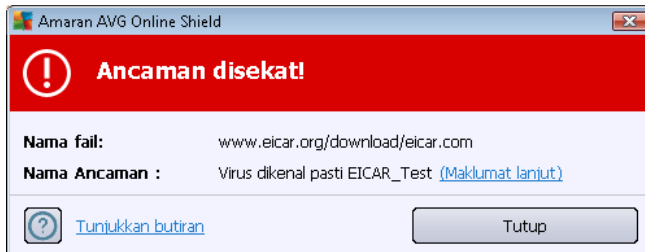
Untuk mengesahkan bahawa **AVG Internet Security 2012** telah dipasang dengan betul, anda boleh melakukan ujian EICAR.

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](http://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 bagi fail ujian, [Online Shield](#) (*sebahagian daripada komponen [Link Scanner](#)*) akan bertindak balas kepadanya dengan amaran. Notis ini menunjukkan bahawa AVG



dipasang dengan betul pada komputer anda.



Dari tapak web <http://www.eicar.com>, anda juga boleh memuat turun versi yang dimampatkan bagi 'virus' EICAR (cth. dalam bentuk *eicar\_com.zip*). [Perisai Dalam Talian](#) membenarkan anda untuk memuat turun fail ini dan menyimpannya pada cakera tempatan anda tetapi, kemudian, [Resident Shield](#) ( dalam komponen [Anti-Virus](#)) mengesan 'virus' apabila anda cuba mengeluarkannya.

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

#### 4.5. Konfigurasi lalai AVG

Konfigurasi lalai (*jaitu bagaimana aplikasi disediakan betul-betul selepas pemasangan*) bagi **AVG Internet Security 2012** disediakan oleh vendor perisian supaya semua komponen dan fungsi ditiun untuk mencapai prestasi optimum.

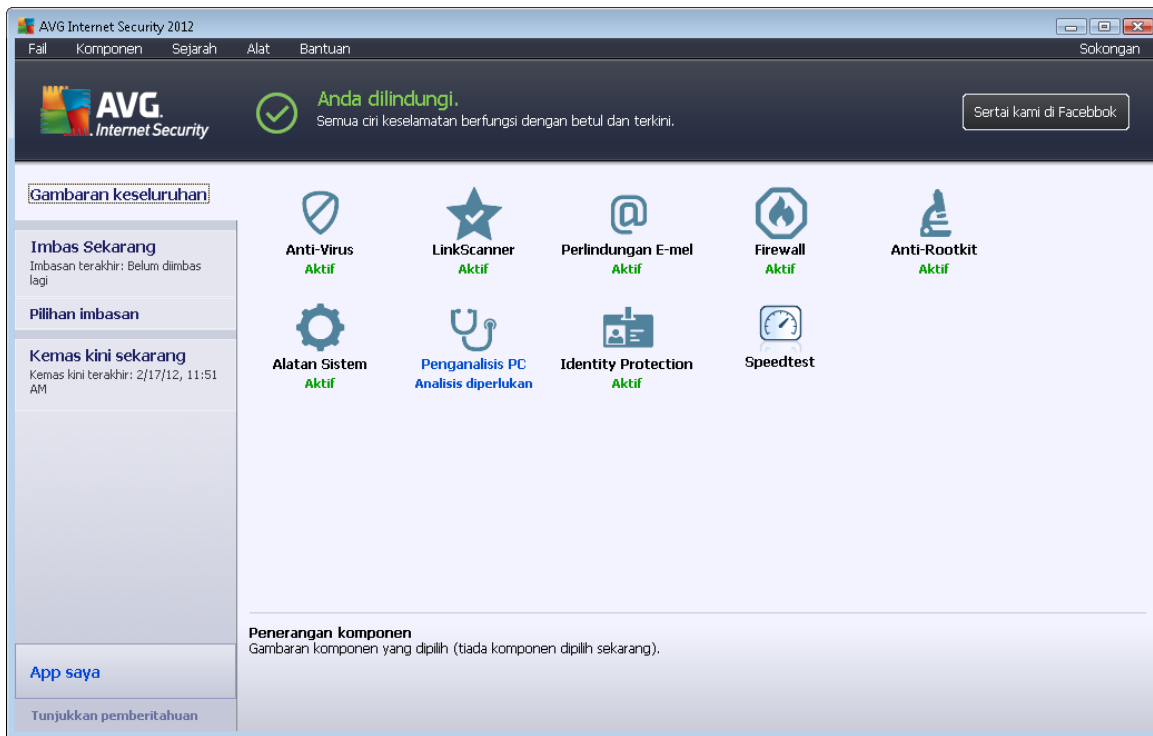
***Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG! Perubahan kepada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja.***

Beberapa pengeditan minor bagi tetapan [komponen AVG](#) boleh diakses secara terus daripada antara muka pengguna komponen khusus. Jika anda rasa 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.



## 5. Antara Muka Pengguna AVG

AVG Internet Security 2012 membuka tettingkap utama:



Tettingkap utama dibahagikan kepada beberapa bahagian:

- **Menu Sistem** (*baris sistem tertinggi dalam tettingkap*) adalah navigasi standard yang membolehkan anda mengakses semua komponen, perkhidmatan dan ciri bagi **AVG Internet Security 2012** – [butiran >>](#)
- **Maklumat Status Keselamatan** (*seksyen atas bagi tettingkap*) memberikan anda maklumat mengenai status terkini bagi **AVG Internet Security 2012** anda – [butiran >>](#)
- **ΒΟΥΤΑΝΥ Sertai kami di Facebook** (*bahagian atas sebelah kanan tettingkap*) membolehkan anda menyertai [Komuniti AVG di Facebook](#). Namun, butang ini hanya kelihatan sekiranya semua komponen berfungsi sepenuhnya dengan betul (*untuk butiran mengenai cara untuk mengenali status komponen AVG lihat bab [Maklumat Status Keselamatan](#)*)
- **Pautan Pantas** (*bahagian kiri tettingkap*) membenarkan anda untuk mengakses dengan cepat tugas paling penting dan paling kerap digunakan bagi **AVG Internet Security 2012** – [butiran >>](#)
- **Aplikasi Saya** (*seksyen bawah kiri bagi tettingkap*) membuka gambaran keseluruhan bagi aplikasi tambahan yang tersedia untuk **AVG Internet Security 2012**: [LiveKive](#), [Family Safety](#) dan [PC Tuneup](#)
- **Gambaran Keseluruhan Komponen** (*seksyen tengah bagi tettingkap*) memberikan gambaran keseluruhan bagi semua komponen yang dipasang dalam **AVG Internet**



Security 2012 - [butiran >>](#)

- **Ikon Dulang Sistem** (penjuru kanan bawah bagi monitor, pada dulang sistem) menunjukkan status terkini bagi **AVG Internet Security 2012** - [butiran >>](#)
- **Alat AVG** (bari sisi Windows, disokong dalam Windows Vista/7) membolehkan akses pantas kepada pengimbasan dan kemas kini dalam **AVG Internet Security 2012** – [butiran >>](#)

## 5.1. Menu Sistem

**Menu sistem** adalah navigasi standard yang digunakan dalam semua aplikasi Windows. Ia terletak secara mendatar pada bahagian paling atas bagi tettingkap utama **AVG Internet Security 2012**. Gunakan menu sistem untuk mengakses komponen, ciri dan perkhidmatan AVG tertentu.

Menu sistem dibahagikan dalam lima bahagian utama:

### 5.1.1. Fail

- **Keluar** – menutup antara muka pengguna **AVG Internet Security 2012**. Walau bagaimanapun, aplikasi AVG akan terus dijalankan di latar belakang dan komputer anda masih akan dilindungi!

### 5.1.2. 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** mengesan virus, perisian pengintip, cecacing, trojan, fail atau pustaka boleh laku yang tidak diingini dalam sistem anda, dan melindungi anda dari adware berniat jahat - [butiran >>](#)
- **LinkScanner** melindungi anda dari serangan berasaskan web semasa anda mencari dan melayari Internet – [butiran >>](#)
- **Perlindungan E-mel** memeriksa mesej e-mel masuk anda untuk SPAM, dan menghalang virus, serangan pemalsuan atau ancaman lain – [butiran >>](#)
- **Firewall** mengawal semua komunikasi pada setiap port rangkaian, melindungi anda dari serangan berniat jahat dan menghalang semua cubaan gangguan - [butiran >>](#)
- **Anti-Rootkit** mengimbas untuk rootkit berbahaya yang tersembunyi dalam aplikasi, pemacu atau pustaka – [butiran >>](#)
- **Alat Sistem** menawarkan ringkasan terperinci bagi persekitaran AVG dan maklumat sistem pengendalian – [butiran >>](#)
- **Penganalisis PC** menyediakan maklumat mengenai status komputer anda – [butiran >>](#)



- **Identity Protection** melindungi aset digital anda secara berterusan daripada ancaman yang baharu dan tidak diketahui – [butiran >>](#)
- **Pentadbiran Jauh** hanya dipaparkan dalam AVG Business Edition jika anda telah menetapkan semasa [proses pemasangan](#) bahawa anda ingin komponen ini dipasang

### 5.1.3. Sejarah

- [Imbas keputusan](#) – beralih ke antara muka pengujian AVG, secara khusus kepada dialog [Gambaran Keseluruhan Keputusan Imbasan](#)
- [Pengesanan Resident Shield](#) – membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh [Resident Shield](#)
- [Pengesanan Pengimbas E-mel](#) – buka dialog dengan gambaran keseluruhan bagi lampiran mesej mel yang dikesan sebagai berbahaya oleh komponen [Perlindungan E-mel](#)
- [Penemuan Perisai Dalam Talian](#) – membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh perkhidmatan [Perisai Dalam Talian](#) dalam komponen [LinkScanner](#)
- [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 semua tindakan **AVG Internet Security 2012** yang dilog
- [Log Firewall](#) – membuka antara muka tetapan Firewall pada tab [Log](#) dengan gambaran keseluruhan semua tindakan Firewall

### 5.1.4. Alat

- [Imbasan komputer](#) – Melancarkan imbasan keseluruhan komputer.
- [Imbas folder dipilih...](#) – Mengalihkan ke [antara muka pengimbasan AVG](#) dan membenarkan anda mentakrif dalam struktur pepohon komputer anda fail dan folder mana yang harus diimbas.
- **Imbas fail...** – Membolehkan anda menjalankan ujian mengikut permintaan ke atas satu fail khusus. Klik opsyen ini untuk membuka tettingkap baharu dengan struktur pepohon cakera anda. Pilih fail yang diingini dan sahkan pelancaran imbasan.
- [Kemas kini](#) – Melancarkan proses kemas kini **AVG Internet Security 2012** secara automatik.
- **Kemas kini dari direktori...** – Menjalankan proses kemas kini dari fail kemas kini yang terletak dalam folder tertentu pada cakera setempat 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 Internet Security 2012. Secara umum, adalah disyorkan untuk mengekalkan tetapan lalai bagi aplikasi seperti yang ditakrifkan oleh vendor perisian.
- [Tetapan firewall...](#) – Membuka dialog sendiri untuk konfigurasi lanjutan bagi komponen [Firewall](#).

### 5.1.5. Bantuan

- **Kandungan** – membuka fail bantuan AVG
- **Dapatkan Sokongan** – membuka laman web AVG (<http://www.avg.com/>) di halaman pusat sokongan pelanggan
- **Web AVG anda** – membuka tapak web AVG (<http://www.avg.com/>)
- **Mengenai Virus dan Ancaman** – membuka [Ensiklopedia Virus](#) dalam talian di mana anda boleh mendapatkan maklumat terperinci mengenai virus yang dikenal pasti
- **Aktifkan semula** – membuka dialog **Aktifkan AVG** dengan data yang anda telah masukkan dalam dialog [Peribadikan AVG](#) bagi [proses pemasangan](#). Dalam dialog ini, anda boleh memasukkan nombor lesen anda dengan sama ada menggantikan nombor jualan ( yang anda telah pasangkan AVG), atau untuk menggantikan nombor lesen lama (*cth. semasa menaik taraf ke produk AVG baharu*).
- **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.

**Nota:** Jika menggunakan versi percubaan bagi **AVG Internet Security 2012**, dua item yang muncul kemudian sebagai **Beli sekarang** dan **Aktifkan**, membolehkan anda membeli versi penuh atur cara dengan serta-merta. Untuk **AVG Internet Security 2012** yang dipasang dengan nombor jualan, item dipaparkan sebagai **Daftar** dan **Aktifkan**.

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

### 5.1.6. Sokongan

Pautan **Sokongan** membuka dialog **Maklumat** dialog baharu dengan semua jenis maklumat yang anda mungkin perlu semasa cuba mendapatkan bantuan. Dialog termasuk data asas mengenai atur cara AVG anda yang dipasang (*versi atur cara / pangkalan data*), butiran lesen, dan senarai pautan sokongan pantas

Dialog **Maklumat** dibahagikan ke dalam enam tab:



Tab **Versi** dibahagikan ke dalam tiga seksyen:

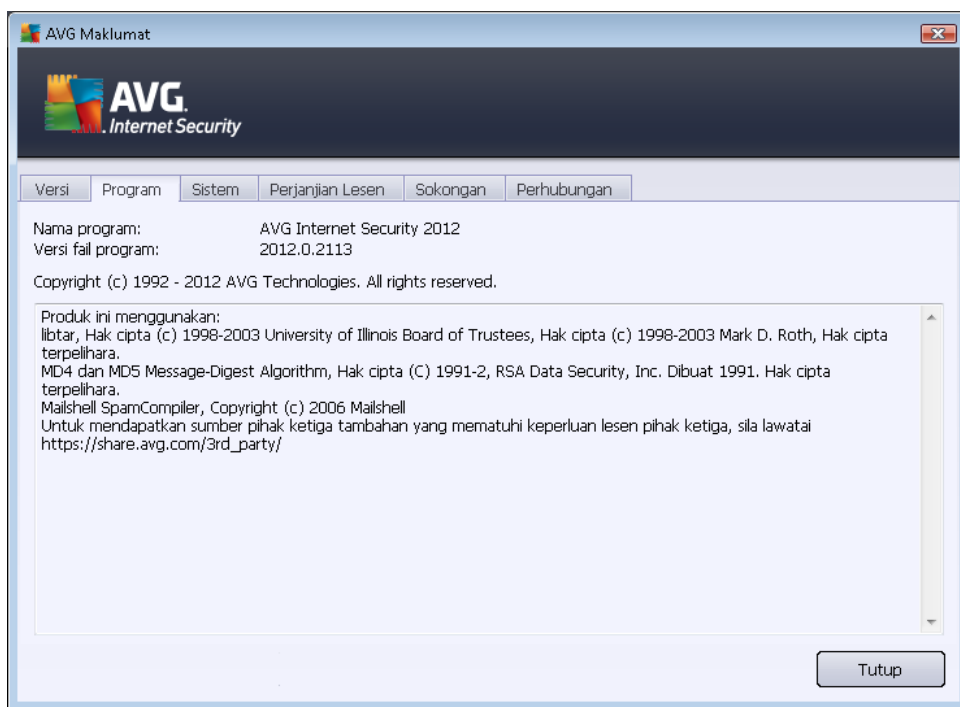


- **Maklumat Sokongan** - Memberikan maklumat mengenai versi **AVG Internet Security 2012**, versi pangkalan data virus, versi pangkalan data [AntiSpam](#) dan versi [LinkScanner](#) .
- **Maklumat Pengguna** - Memberikan maklumat mengenai pengguna dan syarikat berlesen.
- **Butiran Lesen** - Memberikan maklumat mengenai lesen anda (*nama produk, jenis lesen, nombor lesen, tarikh tamat tempoh dan bilangan tempat duduk*). Dalam seksyen ini, anda juga boleh menggunakan pautan **Daftar** untuk mendaftarkan **AVG Internet Security 2012** anda dalam talian; ia membenarkan anda menggunakan [sokongan teknikal AVG](#) sepenuhnya. Serta, gunakan pautan **Aktifkan semula** untuk membuka dialog **Aktifkan AVG**: isikan nombor lesen anda ke dalam medan masing-masing untuk sama ada menggantikan nombor jualan anda (*yang anda gunakan sewaktu pemasangan AVG Internet Security 2012*), atau untuk menukar nombor lesen semasa anda untuk *lain (cth. semasa menaik taraf ke produk AVG lebih tinggi)*.

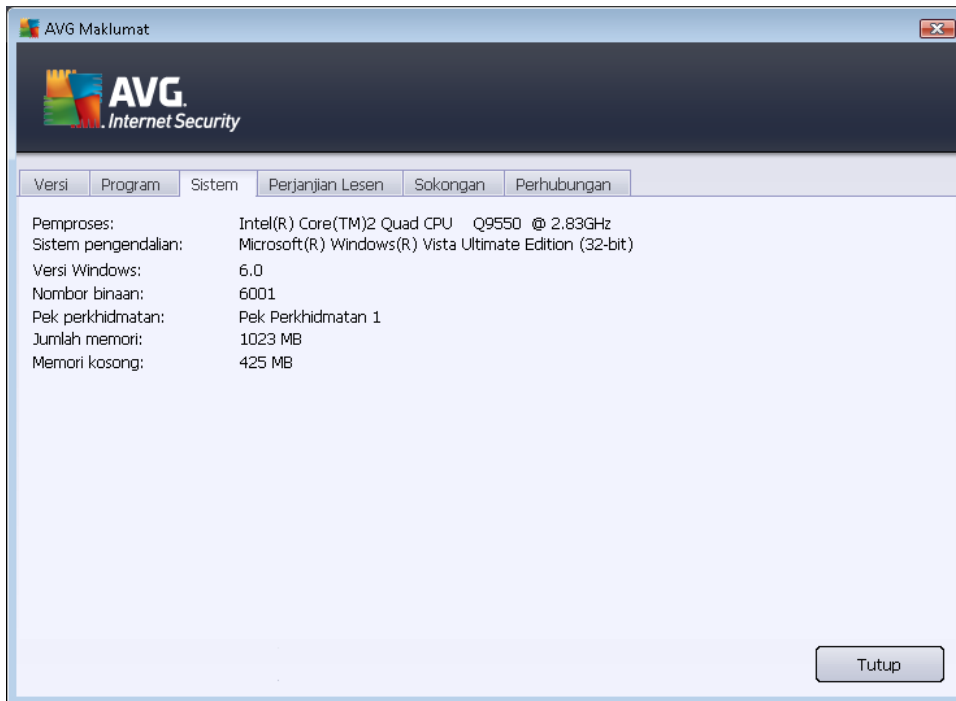




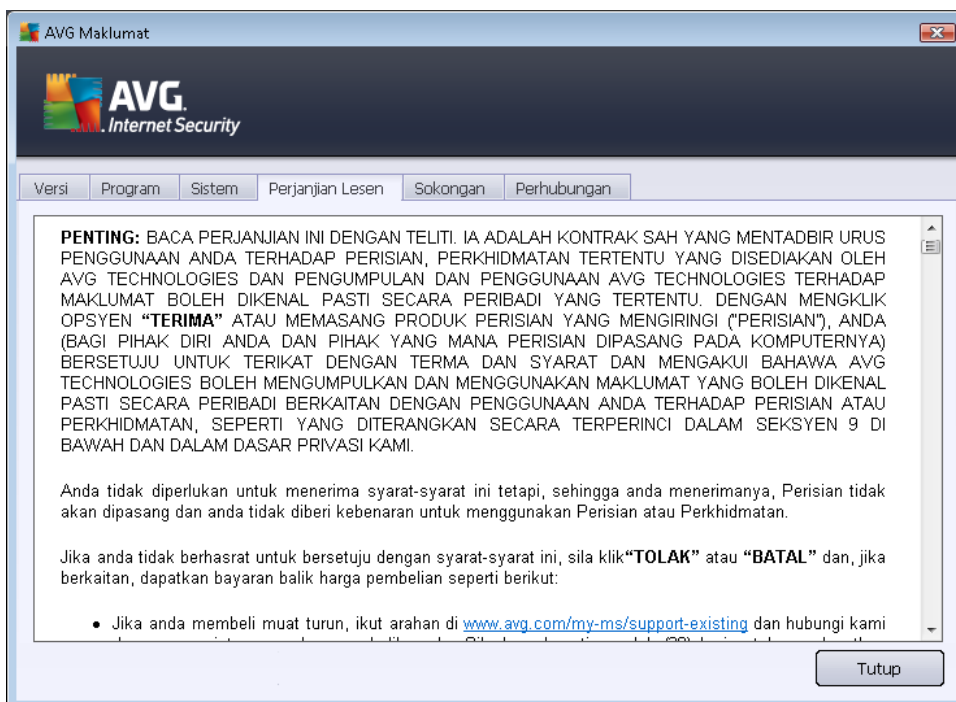
Pada tab **Atur Cara** anda boleh mendapat maklumat mengenai versi fail atur cara **AVG Internet Security 2012**, dan mengenai kod pihak ketiga yang digunakan dalam produk:



Tab **Sistem** memberikan senarai parameter bagi sistem operasi anda (*jenis pemproses, sistem operasi dan versinya, nombor binaan, pek perkhidmatan yang digunakan, jumlah saiz memori dan saiz memori kosong*):



Pada tab **Perjanjian Lesen** anda boleh membaca perjanjian lesen penuh di antara anda dan AVG Technologies:





Tab **Sokongan** memberikan senarai kesemua kemungkinan menghubungi sokongan pelanggan. Serta, ia memberikan pautan ke laman web AVG (<http://www.avg.com/>), forum AVG, Soalan Lazim, ... Seterusnya, anda boleh mendapatkan maklumat yang anda mungkin gunakan semasa menghubungi pasukan sokongan pelanggan:

**AVG Maklumat**

**AVG**  
Internet Security

Versi Program Sistem Perjanjian Lesen **Sokongan** Perhubungan

**Maklumat Sokongan**

Versi AVG : 2012.0.2113  
Versi pangkalan data virus: 2396/4814

**Pautan Sokongan Pantas**

[Soalan Lazim](#)  
[Forum AVG](#)  
[Muat turun](#)  
[Akaun Saya](#)

**Perlindungan e-mel yang dipasang**

Microsoft Outlook, Pengimbas E-mel Peribadi

**Butiran Lesen**

Nama Produk: AVG Internet Security 2012  
Jenis Lesen: Penuh [Daftar](#)  
Nombor Lesen: IMNJI-QH9WL-NEVNU-AUNQF-MJRI7-3 ([salin ke papan klip](#))  
Tarikh Luput Lesen: Wednesday, December 31, 2014  
Bilangan tempat duduk: 1  
[Aktifkan-semula](#)

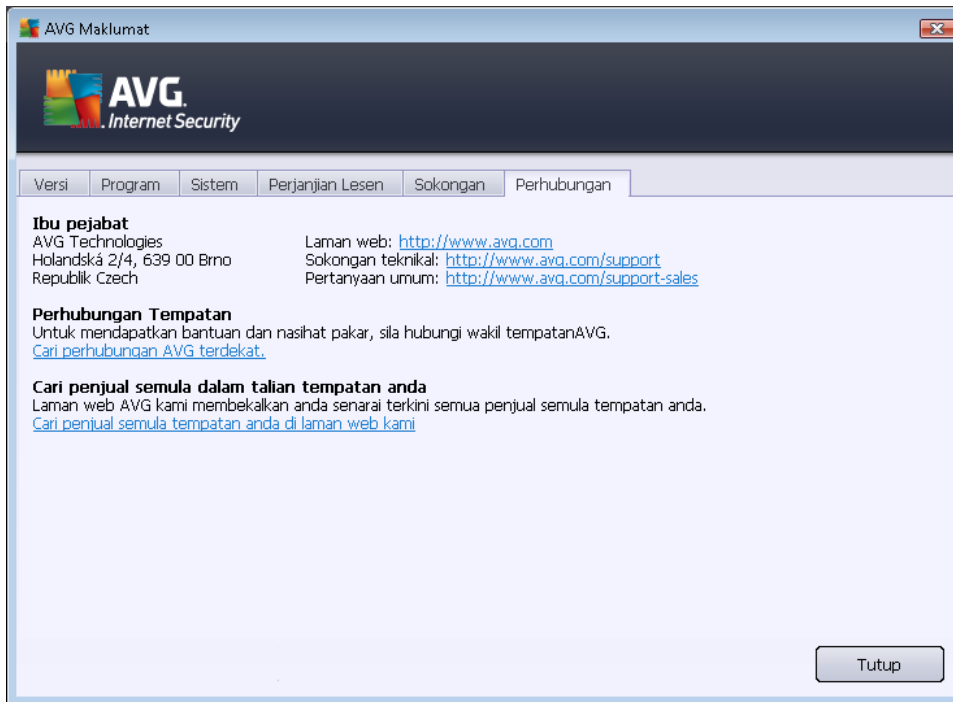
**Pusat Sokongan**

Dapatkan bantuan untuk produk AVG anda dalam talian - dapatkan jawapan kepada soalan anda atau hubungi pakar anda untuk mendapatkan sokongan!

Sokongan Dalam Talian Tutup



Tab **Kenalan** memberikan senarai semua kenalan kepada AVG Technologies, dan juga kenalan kepada wakil tempatan AVG dan penjual semula:



## 5.2. Maklumat Status Keselamatan

Seksyen **Maklumat Status Keselamatan** terletak di bahagian atas tettingkap utama **AVG Internet Security 2012**. Dalam bahagian ini, anda akan sentiasa mendapatkan maklumat mengenai status keselamatan terkini bagi **AVG Internet Security 2012** anda. Sila lihat gambaran keseluruhan ikon yang berkemungkinan bertindih dalam bahagian ini dan maksudnya:



- Ikon hijau menunjukkan bahawa **AVG Internet Security 2012 anda berfungsi sepenuhnya**. Komputer anda dilindungi sepenuhnya, terkini dan semua komponen dipasang berfungsi dengan betul.



– Ikon kuning memberi amaran bahawa **satu atau lebih komponen dikonfigurasi dengan salah** dan anda harus memberikan perhatian kepada sifat/tetapannya. Tiada masalah kritikan dalam **AVG Internet Security 2012** dan anda berkemungkinan telah memutuskan untuk mematikan beberapa komponen atas sebab tertentu. Anda masih dilindungi! Walau bagaimanapun, sila berikan perhatian kepada masalah tetapan komponen! Namanya akan diberikan dalam bahagian **Maklumat Status Keselamatan**.

Ikon kuning juga muncul jika atas sebab tertentu, anda telah memutuskan untuk mengabaikan status ralat komponen. Opsyen **Abaikan keadaan komponen** tersedia dari



menu konteks (*dibuka oleh klik kanan tetikus anda*) pada ikon komponen masing-masing dalam [gambaran keseluruhan komponen](#) bagi tettingkap utama **AVG Internet Security 2012**. Pilih pilihan ini untuk menyatakan anda menyedari tentang keadaan ralat komponen tetapi, atas sebab tertentu, anda hendak menyimpan **AVG Internet Security 2012** dan anda tidak mahu diberi amaran oleh [ikon dulang sistem](#). Anda mungkin perlu menggunakan opsiyen ini dalam situasi tertentu tetapi amat disyorkan untuk mematikan opsiyen **Abaikan keadaan komponen** secepat mungkin.

Selain itu, ikon kuning juga akan dipaparkan jika **AVG Internet Security 2012** anda memerlukan komputer supaya dimulakan semula (**Mula semula diperlukan**). Sila berikan perhatian kepada amaran ini dan mulakan semula PC anda menggunakan butang **Mula semula sekarang**.



– Ikon oren menunjukkan bahawa **AVG Internet Security 2012 berada dalam status kritikal!** Satu atau lebih komponen tidak berfungsi dengan betul dan **AVG Internet Security 2012** 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](#).

**Sekiranya, AVG Internet Security 2012 tidak ditetapkan ke prestasi optimum, butang baharu dinamakan Betulkan (secara alternatif Betulkan semua jika masalah berkenaan melibat lebih daripada satu komponen) muncul di sebelah maklumat status keselamatan. Tekan butang ini untuk melancarkan proses automatik pemeriksaan dan konfigurasi atur cara. Ini adalah cara mudah untuk menetapkan AVG Internet Security 2012 ke prestasi optimum dan mencapai tahap keselamatan maksimum!**

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

**Nota:** maklumat status AVG Internet Security 2012 juga boleh diperoleh pada bila-bila masa dari [ikon dulang sistem](#).

### 5.3. Pautan Pantas

**Pautan pantas** terletak di sebelah kiri [antara muka pengguna AVG Internet Security 2012](#). Pautan ini membenarkan anda untuk mengakses ciri yang paling penting dan paling kerap digunakan bagi aplikasi dengan segera, iaitu pengimbasan dan kemas kini. Pautan pantas boleh diakses dari semua dialog bagi antara muka pengguna:





**Pautan pantas** dibahagikan ke dalam tiga seksyen secara grafik:

- **Imbas sekarang** - Secara lalai, butang memberikan maklumat mengenai imbasan terakhir yang dilancarkan (*iaitu jenis imbasan, dan tarikh pelancaran terakhir*). Klik arahan **Imbas sekarang** untuk melancarkan imbasan yang sama sekali lagi. Jika anda ingin melancarkan imbasan lain, klik pautan **Opsyen imbasan**. Dengan cara ini, anda membuka [antara muka pengimbasan AVG](#) yang anda boleh menjalankan imbasan, menjadualkan imbasan atau mengedit parameternya. (*Untuk butiran, lihat bab [Pengimbasan AVG](#)*)
- **Pilihan imbasan** - Gunakan pautan ini untuk beralih dari sebarang dialog AVG yang sedang terbuka ke tettingkap lalai dengan [gambaran keseluruhan semua komponen yang dipasang](#). (*Untuk butiran, lihat bab [Gambaran Keseluruhan Komponen](#)*)
- **Kemas kini sekarang** – Pautan memberikan tarikh dan masa bagi [kemas kini](#) kali terakhir dilancarkan. Tekan butang untuk menjalankan proses kemas kini dengan serta-merta, dan untuk mengikuti perkembangannya. (*Untuk butiran, lihat bab [Kemas Kini AVG](#)*)

**Pautan pantas** boleh diakses dari [Antara Muka Pengguna AVG](#) pada setiap masa. Apabila anda menggunakan pautan pantas untuk menjalankan proses tertentu, sama ada imbas atau kemas kini, aplikasi akan bertukar ke dialog baharu tetapi pautan pantas masih tersedia. Tambahan pula, proses yang dijalankan seterusnya ditafsirkan secara grafik dalam navigasi, supaya anda mempunyai kawalan penuh semua proses yang dilancarkan yang dijalankan dalam **AVG Internet Security 2012** buat masa itu.

## 5.4. Gambaran keseluruhan Komponen

### Seksyen Gambaran Keseluruhan Komponen

Seksyen **Gambaran Keseluruhan Komponen** terletak di bahagian tengah [antara muka pengguna AVG Internet Security 2012](#) anda. Bahagian tersebut dibahagikan kepada dua bahagian:

- **Gambaran keseluruhan bagi semua komponen yang dipasang** terdiri daripada panel grafik untuk semua komponen yang dipasang. Setiap panel dilabel oleh ikon komponen dan memberikan maklumat mengenai sama ada komponen masing-masing aktif atau tidak aktif buat masa ini.
- **Penerangan komponen** terletak di bahagian bawah dialog ini. Penerangan tersebut secara ringkas menerangkan kefungsi asas komponen. Ia juga memberikan maklumat mengenai status terkini bagi komponen yang dipilih.

### Senarai komponen yang dipasang

Dalam **AVG Internet Security 2012** bahagian **Gambaran Keseluruhan Komponen** mengandungi maklumat mengenai komponen berikut:

- **Anti-Virus** mengesan virus, perisian pengintip, cecacing, trojan, fail atau pustaka boleh laku yang tidak diingini dalam sistem anda, dan melindungi anda dari adware berniat jahat - [butiran >>](#)



- **LinkScanner** melindungi anda dari serangan berasaskan web semasa anda mencari dan melayari Internet – [butiran >>](#)
- **Perlindungan E-mel** memeriksa mesej e-mel masuk anda untuk SPAM, dan menghalang virus, serangan pemalsuan atau ancaman lain – [butiran >>](#)
- **Firewall** mengawal semua komunikasi pada setiap port rangkaian, melindungi anda dari serangan berniat jahat dan menghalang semua cubaan gangguan – [butiran >>](#)
- **Anti-Rootkit** mengimbas untuk rootkit berbahaya yang tersembunyi dalam aplikasi, pemacu atau pustaka – [butiran >>](#)
- **Alatan Sistem** menawarkan ringkasan terperinci bagi persekitaran AVG dan maklumat sistem pengendalian – [butiran >>](#)
- **Penganalisis PC** penganalisis menyediakan maklumat mengenai status komputer anda – [butiran >>](#)
- **Identity Protection** melindungi aset digital anda secara berterusan daripada ancaman yang baharu dan tidak diketahui – [butiran >>](#)
- **Pentadbiran Jauh** hanya dipaparkan dalam AVG Business Edition jika anda telah menetapkan semasa [proses pemasangan](#) anda ingin komponen ini dipasang

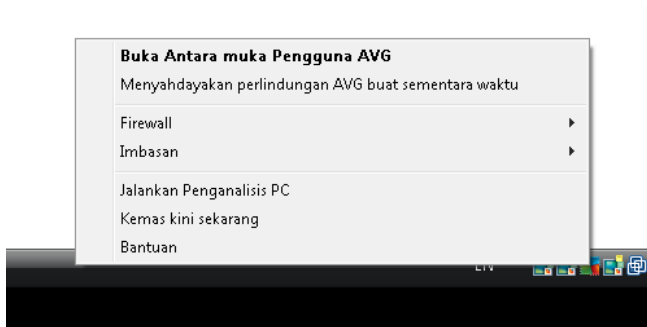
### Tindakan boleh diakses

- **Gerakkan tetikus pada sebarang ikon komponen** untuk menyerlahkannya dalam gambaran keseluruhan komponen. Pada masa yang sama, penerangan kefungsiian asas komponen muncul di bahagian bawah [antara muka pengguna](#).
- **Klik sekali pada sebarang ikon komponen** untuk membuka antara muka komponen itu sendiri dengan senarai data statistik asas.
- **Klik kanan tetikus anda pada ikon komponen** untuk mengembangkan menu konteks dengan beberapa pilihan:
  - **Buka** – Klik pilihan ini untuk membuka dialog komponen itu sendiri (*sama seperti dengan satu klik pada ikon komponen*).
  - **Abaikan keadaan komponen ini** – Pilih pilihan ini untuk menyatakan bahawa anda menyedari tentang [keadaan ralat komponen](#) tetapi, atas sebab tertentu, anda ingin mengekalkan status ini, dan anda tidak mahu diberi amaran oleh [ikon dulang sistem](#).
  - **Buka tetapan Lanjutan ...** - Pilihan ini hanya tersedia untuk beberapa komponen; iaitu yang memberikan kemungkinan bagi [tetapan lanjutan](#).







## 5.5. Ikon Dulang Sistem

**Ikon Dulang Sistem AVG** (pada bar tugas Windows anda, penjuru bawah kanan monitor anda) menunjukkan status semasa bagi **AVG Internet Security 2012** anda. Ia boleh dilihat pada setiap masa pada dulang sistem anda, tidak kira sama ada [antara muka pengguna](#) bagi **AVG Internet Security 2012** anda dibuka atau ditutup:



### Paparan Ikon Dulang Sistem AVG

-  Dalam warna penuh dengan tiada elemen ditambah, ikon menunjukkan bahawa semua komponen **AVG Internet Security 2012** aktif dan berfungsi sepenuhnya. Walau bagaimanapun, ikon juga boleh dipaparkan dengan cara ini dalam situasi apabila salah satu komponen tidak berfungsi sepenuhnya tetapi, pengguna telah memutuskan untuk [mengabaikan keadaan komponen](#). (Telah mengesahkan opsiyen abaikan keadaan komponen yang anda nyatakan anda menyedari tentang [keadaan ralat komponen](#) tetapi, atas sebab tertentu, anda ingin menyimpannya, dan anda tidak mahu diberi amaran mengenai situasi tersebut.)
-  Ikon dengan tanda seru menandakan bahawa komponen (atau malahan, lebih banyak komponen) berada dalam [keadaan ralat](#). Sentiasa beri perhatian kepada amaran seperti itu dan cuba keluarkan isu konfigurasi bagi komponen yang tidak disediakan dengan betul. Untuk boleh melakukan perubahan dalam konfigurasi komponen, klik dua kali ikon dulang sistem untuk membuka [antara muka pengguna aplikasi](#). Untuk maklumat terperinci mengenai komponen mana yang berada dalam [keadaan ralat](#) sila rujuk seksyen [maklumat status keselamatan](#).
-  Ikon dulang sistem boleh seterusnya dipaparkan dalam warna penuh dengan pancaran denyar dan berputar bagi cahaya. Versi grafik ini menandakan proses kemas kini yang sedang dilancarkan.
-  Paparan alternatif bagi ikon warna penuh dengan anak panah bermaksud bahawa pada **AVG Internet Security 2012** imbasan baru dijalankan.

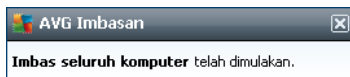
### Maklumat Ikon Dulang Sistem AVG

**Ikon Dulang Sistem AVG** seterusnya, memaklumkan mengenai aktiviti semasa dalam **AVG**





**Internet Security 2012**, anda dan kemungkinan perubahan status dalam atur cara (*cth. pelancaran automatik bagi imbasan atau kemas kini yang dijadualkan, Pertukaran profil Firewall, perubahan status komponen, perulangan status ralat, ...*) melalui tettingkap pop timbul yang dibuka dari ikon dulang sistem:



### Tindakan boleh diakses dari Ikon Dulang Sistem AVG

**Ikon Dulang Sistem AVG** juga boleh digunakan sebagai pautan pantas untuk mengakses [antara muka pengguna](#) bagi **AVG Internet Security 2012**, hanya klik dua kali pada ikon. Dengan mengklik kanan ikon, anda membuka menu konteks ringkas dengan opsyen berikut:

- **Buka Antara Muka Pengguna AVG** – Klik untuk membuka [antara muka pengguna](#) bagi **AVG Internet Security 2012**
- **Nyahdaya perlindungan AVG buat sementara waktu** – Opsyen ini membolehkan anda untuk mematikan keseluruhan perlindungan yang dilindungi oleh **AVG Internet Security 2012** anda dengan sekali gus. Jangan lupa bahawa anda tidak seharusnya menggunakan opsyen ini melainkan ia adalah benar-benar perlu! Dalam kebanyakan kes, adalah tidak perlu menyahdayakan **AVG Internet Security 2012** sebelum memasang perisian atau pemacu baharu, walaupun jika pemasangan atau wizard perisian mencadangkan bahawa atur cara dan aplikasi yang dijalankan harus dimatikan dahulu untuk memastikan tiada gangguan yang tidak dikehendaki sewaktu proses pemasangan. Jika anda perlu menyahdayakan **AVG Internet Security 2012** buat sementara waktu, anda hendaklah mendayakannya semula sebaik sahaja anda selesai. Jika anda bersambung ke Internet atau rangkaian semasa perisian antivirus anda dinyahdayakan, komputer anda terdedah kepada serangan.
- **Firewall** – klik untuk membuka menu konteks bagi opsyen tetapan [Firewall](#) di mana anda boleh mengedit parameter utama: [Status Firewall](#) (*Firewall didayakan/Firewall dinyahdayakan/Mod Kecemasan*), [penukaran mod permainan](#) dan [profil Firewall](#).
- **Imbasan** – Klik untuk membuka menu konteks bagi [imbasan dipraktifik](#) (*imbasan Seluruh Komputer dan Imbas Fail atau Folder Khusus*) dan pilih imbasan yang diperlukan, ia akan dilancarkan serta-merta.
- **Menjalankan imbasan...** - Item ini dipaparkan hanya jika imbasan sedang berjalan pada komputer anda. Untuk imbasan ini anda boleh menetapkan prioritinya, secara alternatif menghentikan atau menjeda imbasan yang sedang berjalan. Selain itu, tindakan berikut boleh diakses: *Tetap prioriti bagi semua imbasan, Jeda semua imbasan atau Hentikan semua imbasan.*
- **Jalankan Penganalisis PC** – Klik untuk melancarkan komponen [Penganalisis PC](#).
- **Kemas kini sekarang** – Melancarkan kemas kini [segera](#).
- **Bantuan** – Membuka fail bantuan pada halaman mula.



## 5.6. Penasihat AVG

**Penasihat AVG** adalah ciri prestasi yang terus mengawasi semua proses yang berjalan dalam PC anda untuk mengesan kemungkinan masalah dan menawarkan petua tentang cara untuk mengelakkan masalah tersebut. **Penasihat AVG** boleh dilihat dalam bentuk pop timbul boleh gelongsor di atas dulang sistem.



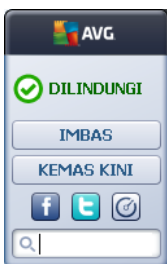
**Penasihat AVG** boleh kelihatan dalam situasi berikut:

- Penyemak imbas internet yang anda sedang gunakan kehabisan memori yang boleh melambatkan kerja anda (*Penasihat AVG hanya menyokong penyemak imbas Internet Explorer, Chrome, Firefox, Opera dan Safari*);
- Proses yang sedang dijalankan dalam komputer anda sedang menggunakan terlalu banyak memori dan melambatkan prestasi PC;
- Komputer anda akan bersambung secara automatik kepada WiFi yang tidak diketahui.

Dalam setiap situasi ini, **Penasihat AVG** memberi amaran kepada anda tentang kemungkinan masalah yang boleh berlaku dan ia memberikan nama dan ikon proses yang sedang bercanggah atau aplikasi. Juga, **Penasihat AVG** mencadangkan langkah apa yang harus diambil untuk mengelakkan kemungkinan masalah tersebut.



## 5.7. Alat AVG

**Alat AVG** dipaparkan pada desktop Windows (*Bar Sisi Windows*). Aplikasi ini hanya disokong dalam sistem pengendalian Windows Vista dan Windows 7. **Alat AVG** menawarkan akses segera kepada kefungsiian **AVG Internet Security 2012** yang paling penting, iaitu [pengimbasan](#) dan [pengemaskinian](#):



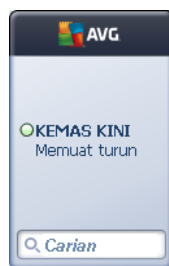
## Akses pantas kepada pengimbasan dan mengemas kini

Jika diperlukan, **alat AVG** membolehkan anda melancarkan imbasan atau kemas kini dengan serta-merta:

- **Imbas sekarang** – Klik pautan **Imbas sekarang** untuk memulakan terus [imbasan seluruh komputer](#). Anda boleh melihat kemajuan proses pengimbasan dalam antara muka pengguna berganti alat ini. Gambaran keseluruhan statistik ringkas menyediakan maklumat mengenai bilangan objek yang diimbas, ancaman yang dikesan, dan ancaman yang dipulihkan. Semasa imbasan anda sentiasa boleh menjeda , atau menghentikan  proses pengimbasan. Untuk data terperinci berkaitan keputusan imbasan, sila rujuk dialog [Gambaran keseluruhan keputusan imbasan](#) yang boleh dibuka secara terus dari alat tersebut melalui pilihan **Tunjukkan butiran** (keputusan imbasan masing-masing akan disenaraikan di bawah Imbasan alat bar sisi).




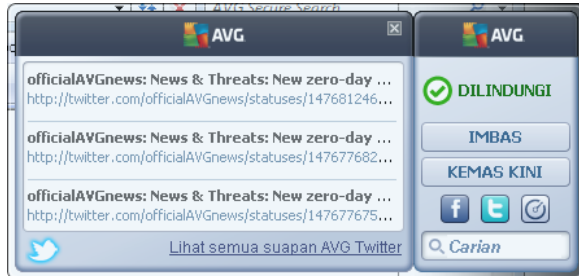
- **Kemas kini sekarang** – Klik pautan **Kemas kini sekarang** untuk melancarkan terus **AVG Internet Security 2012** kemas kini dari dalam alat:





## Akses rangkaian sosial


**Alat AVG** juga memberikan pautan pantas yang menghubungkan anda ke rangkaian sosial utama. Gunakan butang masing-masing untuk dihubungkan ke komuniti AVG dalam Twitter, Facebook atau LinkedIn:

- **Pautan Twitter**  – Membuka antara muka **alat AVG** baharu memberikan gambaran keseluruhan suapan AVG terkini yang dipos di Twitter. Ikuti pautan **Lihat semua suapan AVG Twitter** untuk membuka penyemak imbas Internet anda dalam tettingkap baharu, dan anda akan dihalakan semula terus ke laman web Twitter, khususnya ke halaman yang dikhususkan bagi berita berkaitan AVG:



- **Pautan Facebook**  - Membuka penyemak imbas Internet anda di laman web Facebook, khususnya di halaman **komuniti AVG**.
- **LinkedIn**  - Opsyen ini hanya tersedia dalam pemasangan rangkaian (*jaitu sekiranya anda telah memasang AVG menggunakan salah satu lesen AVG Business Editions*), dan ia membuka penyemak imbas internet anda pada laman web **AVG SMB Community** dalam rangkaian sosial LinkedIn.

#### Ciri lain yang boleh diakses melalui alat

- **Penganalisis PC**  - Membuka antara muka pengguna di dalam komponen [Penganalisis PC](#) dan memulakan terus analisis.
- **Kotak carian** - Taipkan kata kunci dan dapatkan keputusan carian dengan serta-merta dalam tettingkap yang baru dibuka dengan penyemak imbas web lalai anda.



## 6. Komponen AVG

### 6.1. Anti-Virus

Komponen **Anti-Virus** ialah asas bagi **AVG Internet Security 2012** dan ia menggabungkan beberapa ciri asas bagi atur cara keselamatan:

- [Enjin Pengimbasan](#)
- [Perlindungan Residen](#)
- [Perlindungan AntiPerisian Pengintip](#)

#### 6.1.1. Enjin Pengimbasan

Enjin pengimbasan yang merupakan asas komponen **Anti-Virus** 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 dihapuskan atau dikuarantin dalam [Bilik Kebal Virus](#).

**Ciri penting bagi perlindungan AVG Internet Security 2012 adalah tiada virus yang diketahui boleh dijalankan pada komputer!**

#### Cara pengesanan

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. **Anti-Virus** menggunakan kaedah pengesanan berikut:

- 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

Di mana hanya satu teknologi tunggal boleh kekurangan pengesanan atau pengenalpastian virus, **Anti-Virus** menggabungkan beberapa teknologi untuk memastikan komputer anda dilindungi daripada virus. **AVG Internet Security 2012** boleh menganalisis dan mengesan aplikasi boleh laku atau pustaka DLL yang berpotensi tidak diingini dalam sistem. Kami memanggil ancaman seperti itu *Atur Cara Berpotensi Tidak Diingini* (*pelbagai jenis perisian pengintip, adware, dll.*). Tambahan pula, **AVG Internet Security 2012** 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.

**AVG Internet Security 2012 memberikan perlindungan tanpa henti kepada komputer anda!**



### 6.1.2. Perlindungan Residen

AVG Internet Security 2012 memberikan anda perlindungan berterusan dalam bentuk yang dipanggil perlindungan residen. Komponen **Anti-Virus** mengimbas setiap fail tunggal (*dengan sambungan khas atau tanpa sambungan langsung*) yang dibuka, disimpan atau disalin. Ia mengawal kawasan sistem bagi komputer, dan media boleh dialihkan (*cakera denyar dll.*). Apabila virus ditemui dalam fail yang diakses, ia menghentikan operasi yang sedang dijalankan dan tidak membenarkan virus untuk diaktifkan dengan sendiri. Biasanya, anda tidak menyedari proses tersebut, apabila perlindungan residen dijalankan "dalam latar belakang". Anda hanya dimaklumkan apabila ancaman ditemui; pada masa yang sama, **Anti-Virus** menghalang pengaktifan ancaman dan mengeluarkannya.

***Perlindungan residen dimuatkan ke dalam memori komputer anda sewaktu permulaan, dan adalah penting untuk anda memastikan ia dihidupkan pada setiap masa!***

### 6.1.3. Perlindungan AntiPerisian Pengintip

**AntiPerisian Pengintip** terdiri daripada pangkalan data perisian pengintip untuk mengenal pasti jenis definisi perisian pengintip yang diketahui. Pakar perisian pengintip AVG bekerja keras untuk mengenal pasti dan menerangkan corak perisian pengintip terkini sebaik sahaja ia muncul dan kemudian, menambah definisi pada pangkalan data. Melalui proses kemas kini, definisi baru ini dimuat turun ke komputer anda agar anda sentiasa dilindungi daripada jenis perisian pengintip terkini. **AntiPerisian Pengintip** membolehkan anda mengimbas komputer anda sepenuhnya untuk malware/perisian pengintip. Ia juga mengesan malware yang tidur dan tidak aktif, cth. malware yang telah dimuat turun tetapi belum lagi diaktifkan.

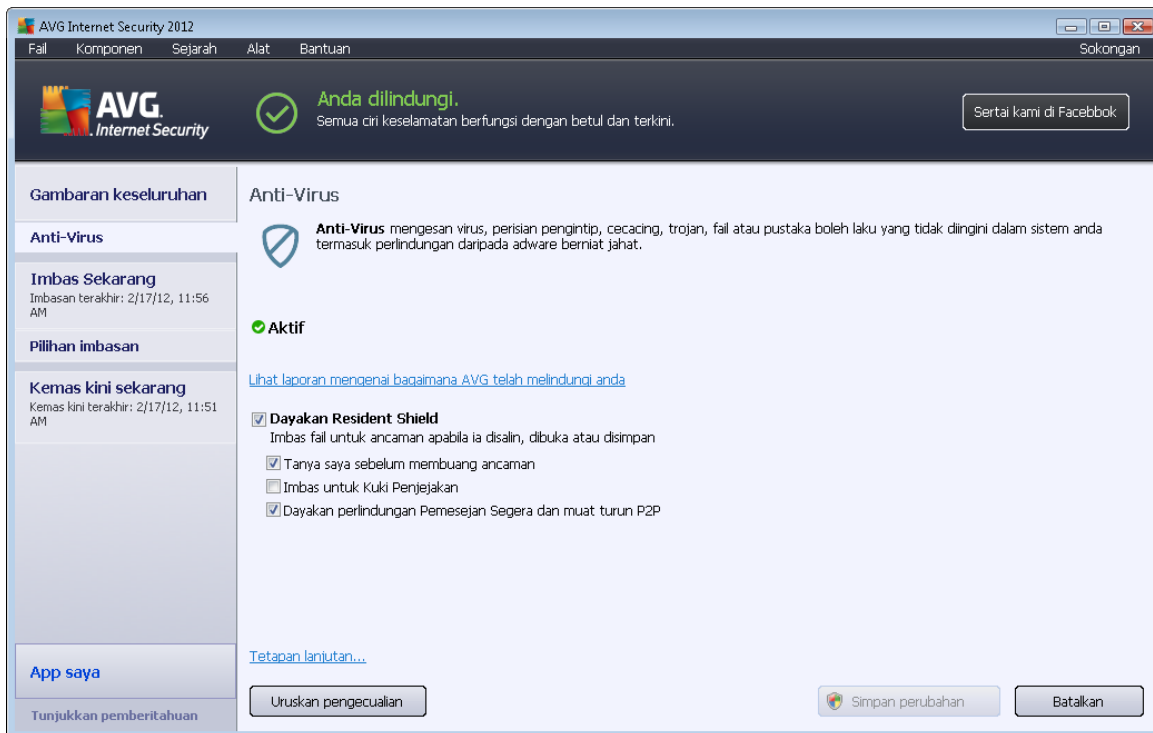
#### **Apa itu perisian pengintip?**

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 Resident Shield dan mengimbas aplikasi anda di latar belakang apabila anda menjalankannya.



#### 6.1.4. Antara Muka Anti-Virus

Antara muka komponen **Anti-Virus** memberikan maklumat ringkas mengenai kefungsiian komponen, maklumat mengenai status terkini komponen (*Aktif*), dan opsyen konfigurasi asas bagi komponen:



#### Opsyen konfigurasi

Dialog menyediakan beberapa opsyen konfigurasi asas bagi ciri yang tersedia dalam komponen **Anti-Virus**. Berikut, anda boleh mendapatkan penerangan ringkas mengenai ini:

- **Lihat laporan dalam talian mengenai bagaimana AVG telah melindungi anda** – Pautan menghalakan anda semula ke halaman khusus pada laman web AVG (<http://www.avg.com/>). Dalam halaman tersebut, anda boleh mendapatkan gambaran keseluruhan statistik terperinci bagi semua **AVG Internet Security 2012** aktiviti yang dilakukan pada komputer anda dalam tempoh masa tertentu, dan secara jumlah.
- **Dayakan Resident Shield** – opsyen ini membenarkan anda menghidupkan/mematikan perlindungan residen dengan mudah. Resident Shield mengimbas fail semasa ia disalin, dibuka atau disimpan. Apabila virus atau sebarang jenis ancaman dikesan, anda akan diberi amaran serta-merta. Secara lalai, fungsi dihidupkan, dan adalah disyorkan untuk terus menghidupkannya! Dengan perlindungan residen dihidupkan, anda seterusnya boleh menentukan cara kemungkinan jangkitan yang dikesan harus dirawat:
  - **Tanya saya sebelum mengalih keluar ancaman** – Biarkan opsyen ini ditandakan bagi mengesahkan anda mahu ditanya pada bila-bila masa ancaman dikesan sebelum ia dialih keluar ke [Bilik Kebal Virus](#). Pilihan ini tidak memberi kesan kepada



tahap keselamatan dan ia hanya menjejaskan keutamaan anda.

- **Imbas untuk Kuki Penjejakan** – Secara bebas pada opsyen sebelum ini, anda boleh memutuskan sama ada anda ingin mengimbas untuk kuki penjejakan. (*Kuki adalah bungkusan teks dihantar oleh pelayan ke penyemak imbas web dan kemudian, dihantar semula tanpa diubah oleh penyemak imbas 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.*) Dalam kes tertentu, anda boleh mengalihkan opsyen ini kepada mendapatkan tahap keselamatan maksimum, walau bagaimanapun, ia dimatikan secara lalai.
- **Dayakan perlindungan Mesej Segera dan muat turun P2P** - Tandakan item ini jika anda mahu mengesahkan bahawa komunikasi mesej segera (*cth. ICQ, MSN Messenger, ...*) adalah bebas virus.
- **Tetapan lanjutan...** – Klik pautan untuk dihalo semula ke dialog masing-masing dalam [Tetapan lanjutan](#) bagi **AVG Internet Security 2012**. Di situ, anda boleh mengedit konfigurasi komponen secara terperinci. Walau bagaimanapun, sila maklum bahawa konfigurasi lalai bagi semua komponen disediakan supaya **AVG Internet Security 2012** memberikan prestasi optimum, dan keselamatan maksimum. Melainkan anda mempunyai sebab sebenar untuk melakukannya, adalah disyorkan untuk mengekalkan konfigurasi lalai!

## Butang kawalan

Dalam dialog, anda boleh menggunakan butang kawalan berikut:

- **Urus pengecualian** – Buka dialog baharu yang dinamakan **Resident Shield – Pengecualian**. Konfigurasi pengecualian daripada imbasan Resident Shield juga boleh diakses dari menu utama, selepas jujukan [Tetapan lanjutan / Anti-Virus / Resident Shield / Pengecualian](#) (*sila lihat bab masing-masing untuk penerangan terperinci*). Dalam dialog tersebut, anda boleh menentukan fail dan folder tertentu yang perlu dikecualikan daripada pengimbasan Resident Shield. Jika ini tidak penting, kami sangat mengesyorkan untuk tidak mengecualikan sebarang item! Dialog menyediakan butang kawalan berikut:
  - **Tambah Laluan** – Tentukan direktori (*atau direktori-direktori*) untuk dikecualikan daripada pengimbasan dengan memilihnya satu persatu dari pepohon navigasi cakera tempatan.
  - **Tambah Fail** – Tentukan fail untuk dikecualikan daripada pengimbasan dengan memilihnya satu persatu dari pohon navigasi cakera tempatan.
  - **Edit Item** – Membenarkan anda mengedit laluan yang ditentukan kepada fail atau folder yang dipilih.
  - **Buang Item** – Membenarkan anda memadam laluan ke item yang dipilih daripada senarai.
  - **Edit Senarai** - Membenarkan anda mengedit seluruh senarai pengecualian yang





ditakrifkan dalam dialog baharu yang berkelakuan seperti editor teks standard.

- **Gunakan** - Simpan semua perubahan kepada tetapan komponen yang dilakukan dalam dialog ini, dan kembali ke [antara muka pengguna](#) utama bagi **AVG Internet Security 2012** (*gambaran keseluruhan komponen*).
- **Batal** – Batalkan semua perubahan kepada tetapan komponen yang dilakukan dalam dialog ini. Tiada perubahan yang akan disimpan. Anda akan kembali ke [antara muka pengguna](#) utama bagi **AVG Internet Security 2012** (*gambaran keseluruhan komponen*).

### 6.1.5. Pengesanan Resident Shield

#### Ancaman dikesan!

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



Dalam dialog amaran ini anda akan menemui data mengenai fail yang dikesan dan ditentukan sebagai dijangkiti (*Nama fail*), nama jangkitan yang dikenal pasti (*Nama ancaman*), dan pautan ke [Ensiklopedia Virus](#) di mana anda boleh menemui maklumat terperinci mengenai jangkitan yang dikesan, jika diketahui (*Maklumat lanjut*).

Seterusnya, anda perlu memutuskan tindakan apa yang perlu dilakukan sekarang. Beberapa opsyen alternatif tersedia. **Sila maklum bahawa, pada keadaan tertentu (apa jenis fail yang dijangkiti, dan di mana ia terletak), tidak semua opsyen sentiasa tersedia!**

- **Rawat** – butang ini hanya muncul jika jangkitan yang dikesan boleh dirawat. Kemudian, ia mengalihnya keluar dari fail, dan memulihkan fail ke keadaan asal. Jika fail itu sendiri merupakan virus, gunakan fungsi ini untuk memadamnya (*iaitu dialih keluar ke [Bilik Kebal Virus](#)*).
- **Alih ke Bilik Kebal (Disyorkan)** – virus tersebut akan dialihkan ke [Bilik Kebal Virus](#)



- **Pergi ke fail** - opsi ini mengalihkan anda semula ke lokasi sebenar objek yang mencurigakan (*membuka tettingkap Windows Explorer baharu*)
- **Abaikan ancaman** – kami amat menyarankan UNTUK TIDAK menggunakan opsi ini melainkan anda mempunyai alasan yang sangat kukuh untuk melakukannya!

**Nota:** Mungkin berlaku saiz objek yang dikesan melebihi had ruang bebas dalam Bilik Kebal Virus. Jika yang demikian, pop timbul mesej amaran memaklumkan anda mengenai isu apabila anda cuba mengalihkan objek yang dijangkiti ke Bilik Kebal Virus. Walau bagaimanapun, saiz Bilik Kebal Virus boleh diedit. Adalah ditentukan sebagai peratus boleh diubah suai bagi saiz sebenar cakera keras anda. Untuk meningkatkan saiz Bilik Kebal Virus anda, pergi ke dialog [Bilik Kebal Virus](#) dalam [Tetapan Lanjutan AVG](#), melalui opsi 'Had saiz Bilik Kebal Virus'.

Di bahagian bawah dialog ini anda boleh menemui pautan **Tunjuk butiran** - klik untuk membuka tettingkap pop timbul dengan maklumat terperinci mengenai proses yang berjalan semasa jangkitan dikesan, dan pengenalan proses berkenaan.

### Gambaran keseluruhan pengesanan Resident Shield

Gambaran keseluruhan bagi semua ancaman yang dikesan oleh [Resident Shield](#) boleh ditemui dalam dialog **pengesanan Resident Shield** yang boleh diakses dari opsi menu sistem [pengesanan Sejarah / Resident Shield](#):

AVG Internet Security 2012

Fail Komponen Sejarah Alat Bantuan Sokongan

**AVG** Internet Security

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

Sertai kami di Facebook

#### Gambaran keseluruhan Pengesanan Resident Shield

Jangkitan	Objek	Keputusan	Masa pengesanan	Jenis Objek	Proses
Virus dikenal pasti EI...	c:\Users\Administrator\...	Dijangkiti	2/17/2012, 11:58:02 AM	fail	C:\Wind

Terdapat 1 rekod dalam senarai  
Tindakan tambahan: [Eksport senarai ke fail](#), [Kosongkan senarai](#)

Segarkan semula senarai Buang yang dipilih Buang semua ancaman Kembali

App saya Tunjukkan pemberitahuan

**Pengesanan Resident Shield** menawarkan gambaran keseluruhan objek yang dikesan oleh [Resident Shield](#), 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 **Resident Shield**. Butang **Undur** mengalihkan anda semula ke [dialog utama AVG](#) lalai (*gambaran keseluruhan komponen*).

## 6.2. LinkScanner

**LinkScanner** melindungi anda daripada bilangan ancaman 'hari ini ada, esok tiada' yang semakin meningkat di web. Ancaman ini boleh disembunyikan pada sebarang jenis laman web, daripada kerajaan kepada jenama yang besar dan terkenal kepada perniagaan kecil, dan ia jarang kekal di tapak berkenaan lebih daripada 24 jam. **LinkScanner** melindungi anda dengan menganalisis halaman web di sebalik semua pautan di mana-mana halaman web yang anda lihat dan memastikan ia selamat pada satu-satunya masa yang paling penting – semasa anda ingin mengklik pautan berkenaan.

### **LinkScanner bukan bertujuan untuk platform pelayan!**

Teknologi **LinkScanner** terdiri daripada ciri utama berikut:

- **Search-Shield** mengandungi senarai laman web (*alamat URL*) yang diketahui berbahaya. Semasa membuat carian di Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask dan Seznam, semua hasil carian disemak mengikut senarai ini dan ikon keputusan ditunjukkan (*untuk Yahoo! hanya ikon keputusan "laman web yang dieksploitasi" ditunjukkan*).
- **Surf-Shield** mengimbas kandungan laman web yang anda lawati, tidak kira alamat laman web berkenaan. Walaupun sesetengah tapak web tidak dikesan oleh **Search-Shield** (*cth. apabila laman web berniat jahat yang baharu dibuat atau apabila laman web yang dahulu bersih kini mengandungi beberapa malware*), ia akan dikesan dan disekat oleh **Surf-Shield** sebaik sahaja anda cuba melawatinya.
- **Online Shield** berfungsi sebagai perlindungan masa nyata semasa melayari Internet. Ia mengimbas kandungan halaman web yang dilawati dan kemungkinan fail yang dimasukkan di dalamnya, malahan sebelum ia dipaparkan dalam penyemak imbas anda atau dimuat turun ke komputer anda. **Online Shield** mengesan virus dan perisian pengintip yang terkandung dalam halaman yang anda akan lawati dan menghentikan muat turun dengan



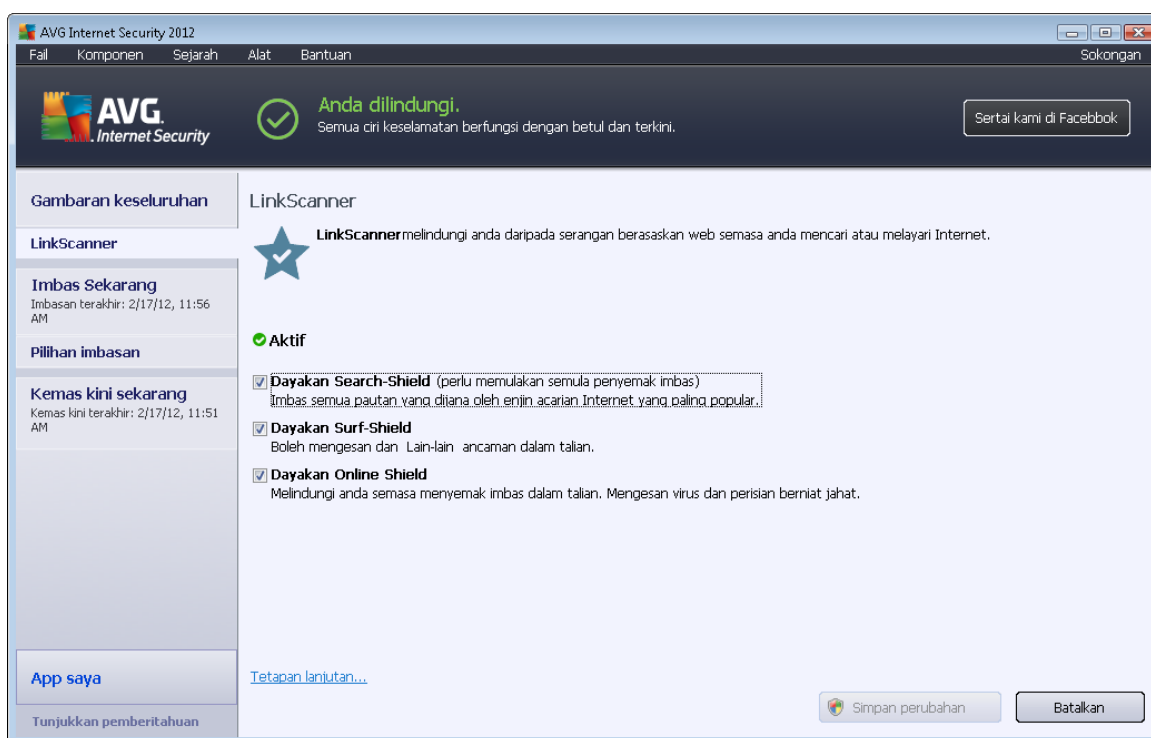
segera supaya tiada ancaman yang akan pergi ke komputer anda.

- **Peningkat AVG** membenarkan main balik video dalam talian yang lebih lancar dan membuatkan muat turun tambahan lebih mudah. Apabila proses peningkatan video sedang dijalankan, anda akan dimaklumkan melalui tettingkap pop timbul dulang sistem.



### 6.2.1. Antara Muka LinkScanner

Dialog utama komponen [LinkScanner](#) memberikan penerangan ringkas bagi kefungsiian dan maklumat komponen mengenai status semasa (*Aktif*):



Dalam bahagian bawah dialog, beberapa konfigurasi asas bagi komponen tersedia:

- **Dayakan [Search-Shield](#)** – (*dihidupkan secara lalai*): Jangan tanda kotak hanya jika anda mempunyai sebab yang munasabah untuk mematikan kefungsiian Search Shield.
- **Dayakan [Surf-Shield](#)** – (*dihidupkan secara lalai*): Perlindungan aktif (*masa nyata*) daripada laman bersifat 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 [Online Shield](#)** – (dihidupkan secara lalai): Pengimbasan masa nyata bagi halaman web yang anda akan lawati untuk kemungkinan virus atau perisian pengintip. Jika ia dikesan, muat turun berhenti dengan serta-merta supaya tiada ancaman dapat pergi ke komputer anda.

### 6.2.2. Pengesanan Search-Shield

Semasa membuat carian di Internet dengan **Search-Shield** dihidupkan, semua keputusan carian dikembalikan daripada enjin pencarian paling popular (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg dan SlashDot*) dinilai untuk pautan berbahaya atau mencurigakan. Dengan menanda pautan ini dan menandakan pautan jahat, [LinkScanner](#) memberi amaran kepada anda sebelum anda mengklik pada pautan berbahaya atau mencurigakan, supaya anda boleh memastikan anda hanya pergi ke laman web selamat.

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



Laman yang dipautkan adalah selamat.



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



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

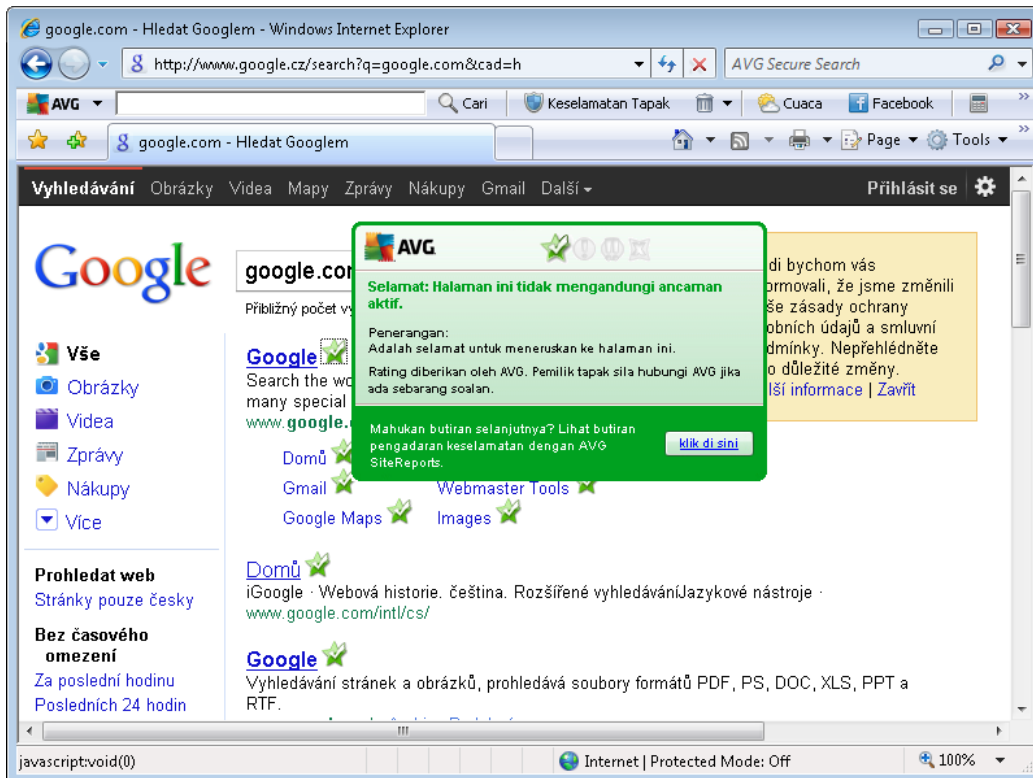


Halaman berpaut mengandungi ancaman aktif! Untuk keselamatan anda sendiri, anda tidak akan dibenarkan untuk melawati halaman ini.



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

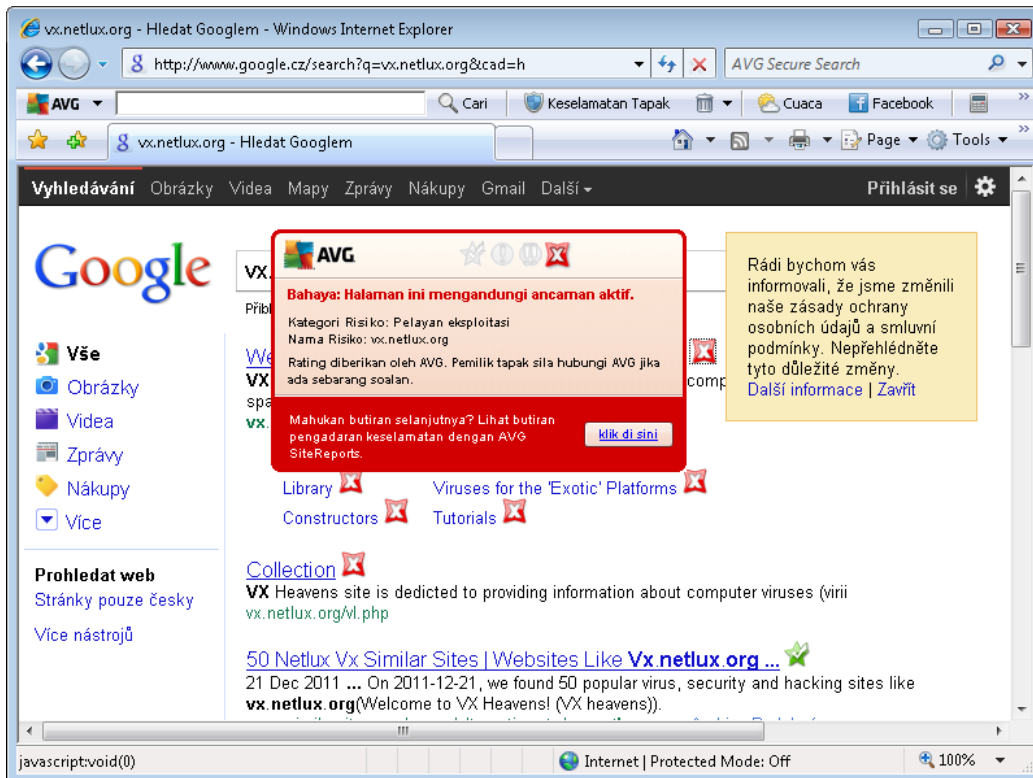
Menghalakan pada setiap ikon pengedaran akan memaparkan butiran mengenai pautan khusus yang dipersoalkan. Maklumat termasuk butiran tambahan mengenai ancaman (*jika ada*):



### 6.2.3. Pengesanan Surf-Shield

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

Jika anda berhadapan dengan tapak web berniat jahat dalam penyemak imbas web anda [LinkScanner](#) akan memberi amaran kepada anda dengan skrin yang sama dengan:



**Memasuki tapak web sangat berisiko dan ia tidak disyorkan!**

#### 6.2.4. Pengesanan Online Shield

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

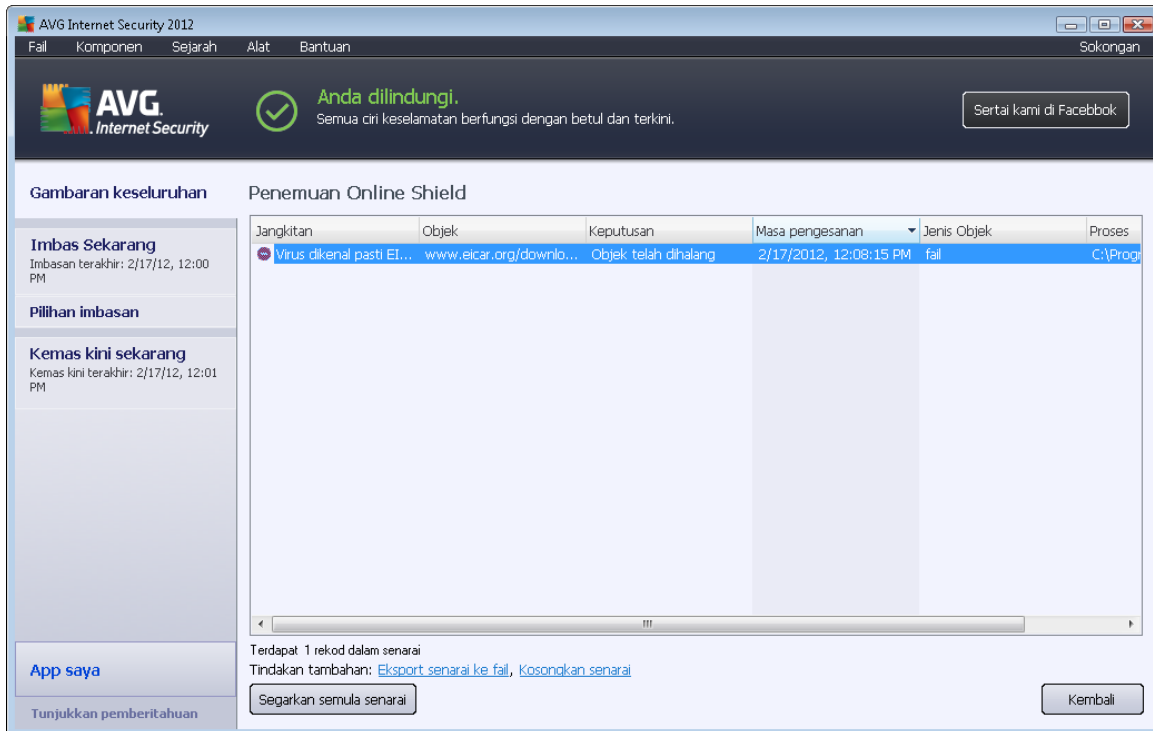


Dalam dialog amaran ini anda akan menemui data mengenai fail yang dikesan dan ditentukan sebagai dijangkiti (*Nama fail*), nama jangkitan yang dikenal pasti (*Nama ancaman*), dan pautan ke [Ensiklopedia Virus](#) di mana anda boleh menemui maklumat terperinci mengenai jangkitan yang dikesan (*jika diketahui*). Dialog ini menyediakan butang berikut:

- **Tunjuk butiran** - klik butang **Tunjuk butiran** untuk membuka tettingkap pop-timbul baru di mana anda boleh menemui maklumat mengenai proses yang berjalan semasa jangkitan dikesan, dan pengenalan proses berkenaan.

- **Tutup** - klik butang ini untuk menutup dialog amaran.

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



Untuk setiap objek yang dikesan, maklumat berikut disediakan:

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

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





## Butang kawalan

- **Muat semula senarai** – kemas kini senarai penemuan yang dikesan oleh **Online Shield**
- **Undur** – kembalike [dialog utama AVG](#) lalai (*gambaran keseluruhan komponen*)

## 6.3. Perlindungan E-mel

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

Komponen **Perlindungan E-mel** bertanggungjawab untuk mengimbas setiap mesej e-mel, yang dihantar atau diterima; apabila virus dikesan di dalam e-mel, ia dibuang ke [Bilik Kebal Virus](#) dengan serta-merta. Komponen juga boleh menapis keluar jenis lampiran e-mel tertentu dan menambah teks pensijilan pada mesej bebas jangkitan. **Perlindungan E-mel** terdiri daripada dua fungsi utama:

- [Pengimbas E-mel](#)
- [AntiSpam](#)

### 6.3.1. E-mail Scanner

**Pengimbas E-mel Peribadi** mengimbas e-mel masuk/keluar secara automatik. Anda boleh menggunakannya bersama klien e-mel yang tidak mempunyai pasang masuknya sendiri di dalam AVG (*tetapi boleh turut digunakan untuk mengimbas mesej e-mel untuk klien e-mel yang disokong AVG menggunakan pasang masuk khusus, iaitu Microsoft Outlook, The Bat dan Mozilla Thunderbird*). Ia perlu digunakan terutamanya bersama aplikasi e-mel seperti Outlook Express, Incredimail, dll.

Sewaktu [pemasangan](#) 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).*

***Pengimbas E-mel bukan bertujuan untuk platform pelayan!***

### **6.3.2. Anti-Spam**

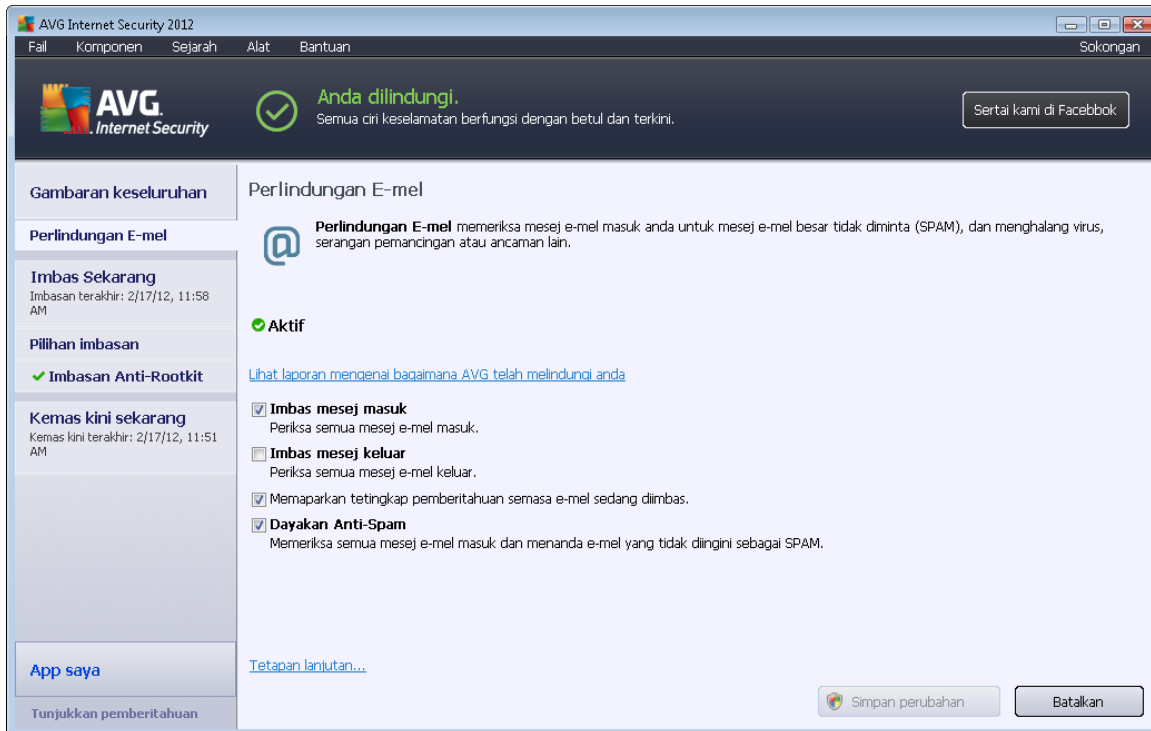
#### **Bagaimana AntiSpam berfungsi?**

**Anti-spam** memeriksa semua mesej e-mel masuk dan menandakan e-mel yang tidak diingini sebagai SPAM. **Anti-Spam** boleh mengubah suai subjek e-mel (*yang telah dikenal pasti sebagai spam*) dengan menambah rentetan teks khas. Anda boleh menapis e-mel anda dalam klien e-mel anda dengan mudah. **Anti-Spam** komponen menggunakan beberapa kaedah analisis untuk memproses setiap mesej e-mel, menawarkan kemungkinan perlindungan maksimum terhadap mesej e-mel. **Anti-Spam** menggunakan pangkalan data yang biasa dikemas kini untuk pengesanan spam. Adalah berkemungkinan untuk menggunakan pangkalan data umum [pelayan RBL](#) (*bagi alamat e-mel "spammer diketahui"*) dan untuk menambah alamat e-mel secara manual ke [Senarai Putih](#) anda (*jangan tandakan sebagai spam*) dan [Senarai Hitam](#) (*sentiasa tandakan sebagai spam*).

#### **Apa itu spam?**

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

### 6.3.3. Antara Muka Perlindungan E-mel



Dalam dialog **Perindungan E-mel** anda boleh menemui teks ringkas yang menerangkan kefungsiian komponen dan maklumat pada status semasanya (*Aktif*). Gunakan **Lihat laporan dalam talian untuk bagaimana AVG telah melindungi anda** pautan untuk menyemak semula statistik terperinci bagi aktiviti dan pengesanan **AVG Internet Security 2012** pada halaman yang dikhaskan bagi laman web AVG (<http://www.avg.com/>).

#### Tetapan Perlindungan E-mel Asas

Dalam dialog **Perindungan E-mel** anda boleh mengedit selanjutnya beberapa ciri asas bagi kefungsiian komponen:

- **Imbas mesej masuk** (*dihidupkan secara lalai*) - Tandakan kotak untuk menentukan bahawa semua e-mel yang dihantarke akaun anda perlu diimbas untuk mengesan virus.
- **Imbas mesej keluar** (*dimatikan secara lalai*) - Tandakan kotak untuk mengesahkan bahawa semua e-mel yang dihantar dari akaun anda perlu diimbas untuk mengesan virus.
- **Paparkan tettingkap pemberitahuan semasa e-mel diimbas** (*dihidupkan secara lalai*) – Tandakan item untuk mengesahkan anda hendak dimaklumkan melalui dialog pemberitahuan yang dipaparkan pada [ikon AVG pada dulang sistem](#) sewaktu pengimbasan e-mel anda.
- **Dayakan AntiSpam** (*dihidupkan secara lalai*) - Tandakan item untuk menentukan sama ada anda inginkan mel masuk anda ditapis untuk e-mel yang tidak diminta.



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

### Butang kawalan

Butang kawalan tersedia dalam dialog *Perlindungan 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 [dialog utama AVG](#) lalai (*gambaran keseluruhan komponen*)

### 6.3.4. Pengesanan Pengimbas E-mel

Jangkitan	Objek	Keputusan	Masa pengesanan	Jenis Objek
✓ Virus dikenali pasti ET...	eicar_com.zip	Dialihkan ke Bilik Kebal ...	2/17/2012, 11:55:41 AM	fail
✓ Virus dikenali pasti ET...	eicar_com.zip	Dialihkan ke Bilik Kebal ...	2/17/2012, 11:55:33 AM	fail

Dalam dialog *Pengesanan Pengimbas E-mel* (boleh diakses melalui opsyen menu sistem *Sejarah / pengesanan Pengimbas E-mel*) anda boleh melihat senarai semua penemuan yang dikesan oleh komponen [Perlindungan 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.
- **Undur** – Membawa anda kembali ke dialog yang dipaparkan sebelum ini.

## 6.4. 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.

**Komputer yang tidak dilindungi oleh Firewall menjadi sasaran mudah untuk penggadam komputer dan kecurian data.**

**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.*

### **6.4.1. Prinsip Firewall**

Dalam **AVG Internet Security 2012**, **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 menyambung ke rangkaian Internet/ setempat*), atau aplikasi yang mendekati komputer anda dari luar cuba menyambung ke PC anda. Untuk setiap aplikasi ini, kemudian **Firewall** membenarkan atau melarang komunikasi pada port rangkaian. Secara lalai, jika aplikasi tidak diketahui (*iaitu tidak mempunyai peraturan Firewall yang ditakrifkan*), **Firewall** akan menanyakan kepada anda sama ada anda hendak membenarkan atau menghalang cubaan komunikasi.

**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 prataktif, mengikut keperluan anda
- [Tukar profil](#) secara automatik apabila menyambung kepada pelbagai rangkaian, atau menggunakan pelbagai penyesuaian rangkaian

### **6.4.2. Profil Firewall**

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

#### **Profil yang ada**

- **Benarkan semua** - profil sistem [Firewall](#) yang telah dipratetapkan oleh pengilang dan sentiasa wujud. Apabila profil ini diaktifkan, semua komunikasi rangkaian dibenarkan dan tiada peraturan dasar keselamatan yang dikenakan, seperti perlindungan [Firewall](#) dimatikan (cth. semua aplikasi dibenarkan tetapi paket masih diperiksa – untuk menyahdayakan sepenuhnya sebarang penapisan yang anda perlukan untuk menyahdayakan Firewall). Profil sistem ini tidak boleh dibuat pendua, dipadam dan tetapannya tidak boleh diubah suai.
- **Sekat semua** – profil sistem [Firewall](#) yang telah dipratetap oleh pengilang dan sentiasa wujud. Apabila profil ini diaktifkan, semua komunikasi rangkaian dihalang, dan komputer tidak boleh diakses dari rangkaian luar dan tidak boleh berkomunikasi di luar. Profil sistem tidak boleh disalin, dipadamkan, dan tetapannya tidak boleh diubah.



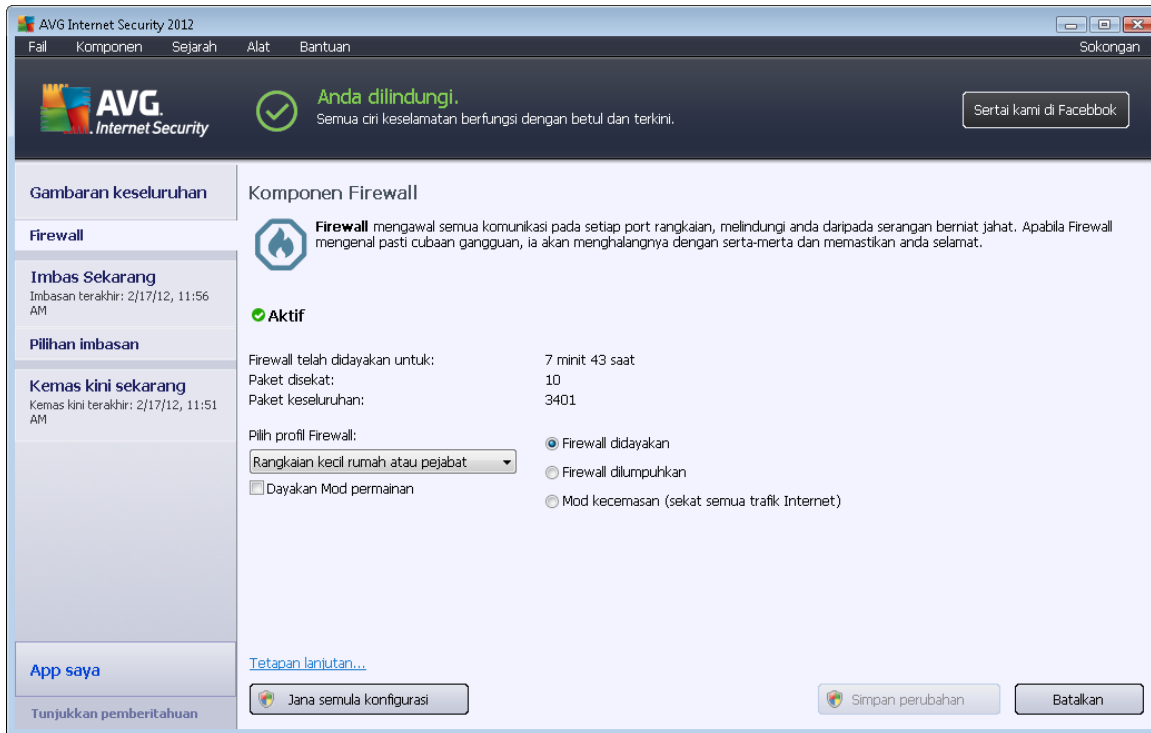
- **Profil tersuai** – profil tersuai membolehkan anda menggunakan kelebihan penukaran profil automatik yang terutama sekali, berguna jika anda menyambung pelbagai rangkaian secara kerap (*cth. dengan notebook*). Profil tersuai dijana secara automatik selepas **AVG Internet Security 2012** pemasangan, dan meliputi sebarang keperluan individu untuk peraturan dasar [Firewall](#). Profil tersuai berikut tersedia:
  - **Disambungkan ke Internet secara terus** – sesuai untuk komputer rumah desktop biasa atau notebook yang disambungkan secara terus ke Internet, tanpa sebarang perlindungan tambahan. Opsyen ini juga disyorkan apabila anda menyambung notebook anda ke pelbagai rangkaian yang tidak diketahui dan berkemungkinan tidak selamat (*cth. dalam kafe Internet, bilik hotel, dll.*). Peraturan [Firewall](#) yang paling tegas bagi profil ini memastikan komputer tersebut dilindungi sepenuhnya.
  - **Komputer dalam domain** – sesuai untuk komputer dalam rangkaian tempatan, biasanya, di sekolah atau di tempat kerja. Ia menganggap bahawa rangkaian ditadbir secara profesional dan dilindungi oleh beberapa langkah tambahan supaya tahap keselamatan boleh menjadi lebih rendah daripada dalam kes yang dinyatakan di atas, membolehkan akses kepada folder dikongsi, unit cakera dll.
  - **Rangkaian rumah atau pejabat kecil** – sesuai untuk komputer dalam rangkaian kecil, biasanya, di rumah atau dalam perniagaan kecil. Biasanya, jenis rangkaian ini tiada pentadbir "pusat", dan hanya terdiri daripada beberapa komputer disambungkan bersama, biasanya berkongsi pencetak, pengimbas atau peranti yang sama, yang mana peraturan [Firewall](#) mesti gambarkan.

### 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.

### 6.4.3. Antara Muka Firewall



Dialog utama yang dinamakan **Komponen Firewall** memberikan sedikit maklumat asas mengenai kefungsiannya, statusnya (*Aktif*), dan gambaran keseluruhan ringkas mengenai statistik komponen:

- **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

#### Tetapan Firewall asas

- **Pilih profil Firewall** – dari menu gulung ke bawah, pilih salah satu profil yang ditakrifkan ( untuk penerangan terperinci bagi setiap profil dan penggunaan yang diyorkannya, sila rujuk bab [Profil Firewall](#))
- **Dayakan mod Permainan** – Tandakan opsi ini untuk memastikan semasa menjalankan aplikasi skrin penuh (*permainan, pembentangan, filem, dll.*), [Firewall](#) tidak akan memaparkan dialog menanyakan kepada anda sama ada hendak membenarkan atau menghalang komunikasi untuk aplikasi tidak diketahui. Jika aplikasi tidak diketahui cuba berkomunikasi pada rangkaian dalam masa tersebut, [Firewall](#) akan membenarkan atau menyekat cubaan secara automatik menurut tetapan dalam profil semasa. **Nota:** Dengan mod permainan dihidupkan, semua tugas yang dijadualkan (imbasan, kemas kini)





ditanggihkan sehingga aplikasi ditutup.

- Seterusnya, dalam seksyen tetapan asas, anda boleh memilih dari tiga opsi alternatif yang mentakrifkan status semasa bagi komponen [Firewall](#):
  - **Firewall didayakan (secara lalai)** - pilih opsi ini untuk membenarkan komunikasi dengan aplikasi yang diperuntukkan sebagai 'dibenarka' dalam set peraturan yang ditakrifkan dalam profil [Firewall](#) yang dipilih.
  - **Firewall dinyahdayakan** – pilihan ini mematikan [Firewall](#) sepenuhnya, semua lalu lintas rangkaian dibenarkan tetapi tidak ditanda!
  - **Mod kecemasan (sekat semua lalu lintas Internet)** – pilih opsi ini untuk menyekat semua lalu lintas pada setiap port rangkaian tunggal; [Firewall](#) masih dijalankan tetapi semua lalu lintas rangkaian dihentikan.

**Sila maklum:** Vendor perisian telah menyediakan semua komponen AVG Internet Security 2012 untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang perubahan kepada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja. Jika anda perlu mengubah konfigurasi Firewall, pilih item menu sistem **tetapan Alat/Firewall** dan edit konfigurasi Firewall dalam dialog [Tetapan Firewall](#) yang baru dibuka.

### Butang kawalan

- **Jana semula konfigurasi** – tekan butang ini untuk menulis ganti konfigurasi [Firewall](#) semasa, dan untuk kembali ke konfigurasi lalai berdasarkan kepada pengesanan automatik.
- **Simpan perubahan** – tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini.
- **Batal** – tekan butang ini untuk kembali ke [dialog utama AVG](#) lalai (*gambaran keseluruhan komponen*).

## 6.5. AntiRootkit

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

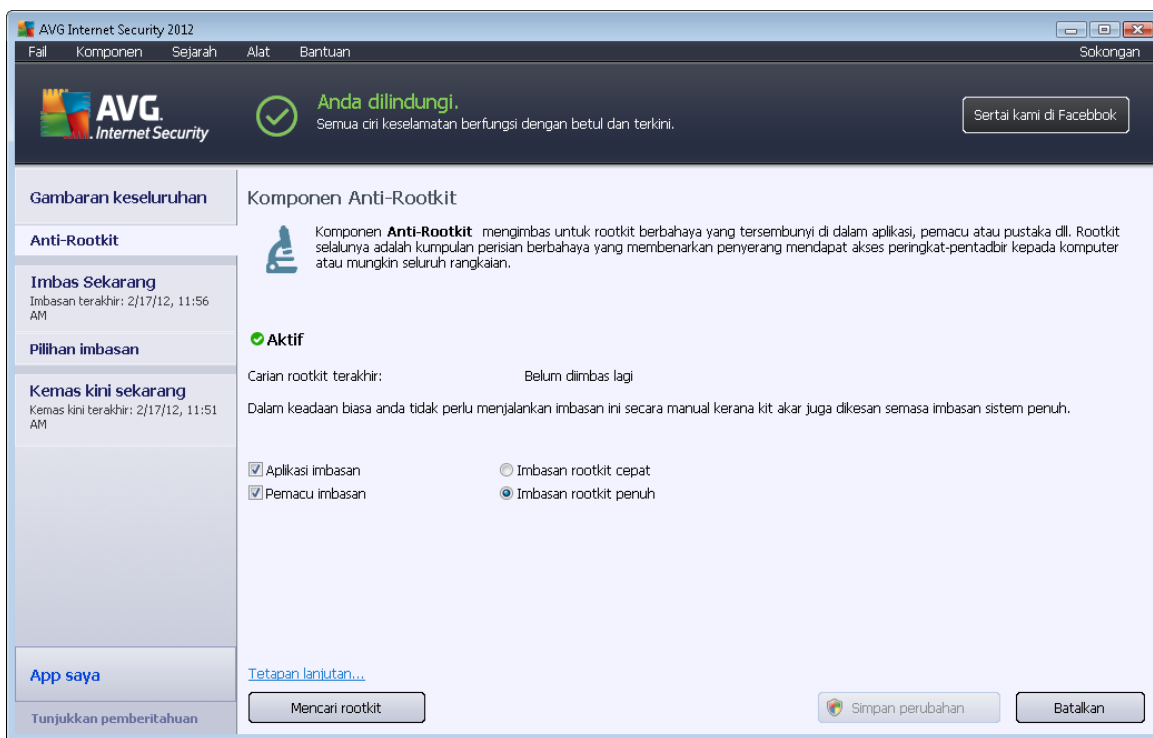
### Apa itu rootkit?

Rootkit adalah atur cara yang direka bentuk untuk melakukan kawalan asas sistem komputer tanpa kebenaran daripada pemilik sistem dan pengurus yang sah. Akses kepada perkakasan jarang



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

### 6.5.1. Antara Muka AntiRootkit



Dialog **AntiRootkit** memberikan huraian ringkas mengenai kefungsian komponen, memberitahu tentang status semasa komponen (*Aktif*), dan juga membawakan maklumat tentang kali terakhir ujian **AntiRootkit** dilancarkan (*Carian rootkit terakhir; ujian rootkit ini adalah proses lalai yang dijalankan dalam [Imbasan Seluruh Komputer](#)*). Dialog **AntiRootkit** seterusnya menyediakan pautan [Tetapan Alat/Lanjutan](#). Gunakan pautan ini untuk diarahkan semula ke persekitaran konfigurasi lanjutan bagi komponen **AntiRootkit**.

**Vendor perisian telah menetapkan semua komponen AVG untuk memberikan persembahan optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja.**

#### Tetapan AntiRootkit asas

Di bahagian bawah dialog, anda boleh menyediakan beberapa fungsi asas bagi pengimbasan kehadiran rootkit. Pertama sekali, tandakan kotak semak masing-masing untuk menentukan objek



yang harus diimbis:

- **Aplikasi imbasan**
- **Pemacu imbasan**

Seterusnya, anda boleh memilih mod pengimbasan rootkit:

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

### Butang kawalan

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

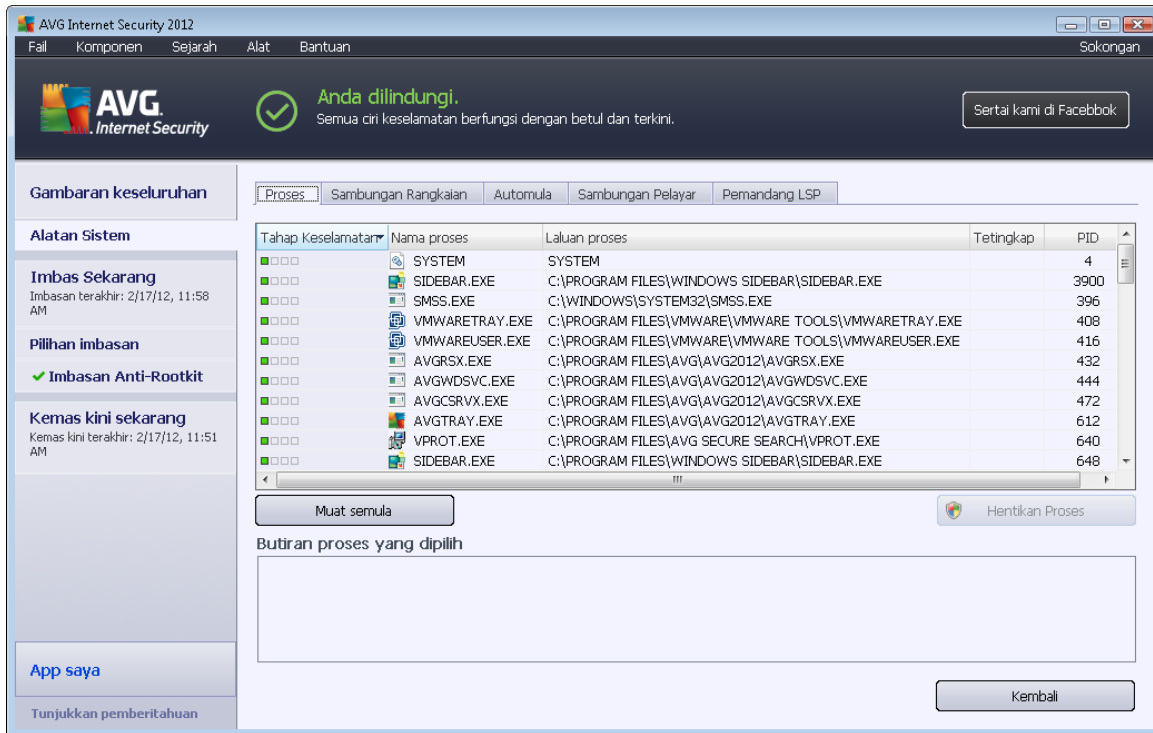
## 6.6. Alatan Sistem

**Alat Sistem** merujuk kepada alat yang menawarkan ringkasan terperinci bagi persekitaran dan sistem pengendalian **AVG Internet Security 2012**. Komponen memaparkan gambaran keseluruhan bagi:

- [Proses](#) – senarai proses (*iaitu aplikasi yang sedang berjalanyang sedang aktif pada komputer anda*)
- [Sambungan rangkaian](#) – senarai sambungan yang sedang aktif
- [Automula](#) – senarai semua aplikasi yang dilakukan sewaktu permulaan sistem Windows
- [Sambungan Penyemak Imbas](#) – senarai pasang masuk (*iaitu aplikasi*) yang dipasang di dalam penyemak imbas Internet anda
- [Pemapar LSP](#) – senarai Pembekal Khidmat Berlapis (*LSP*)

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

### 6.6.1. Proses



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

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

#### Butang kawalan

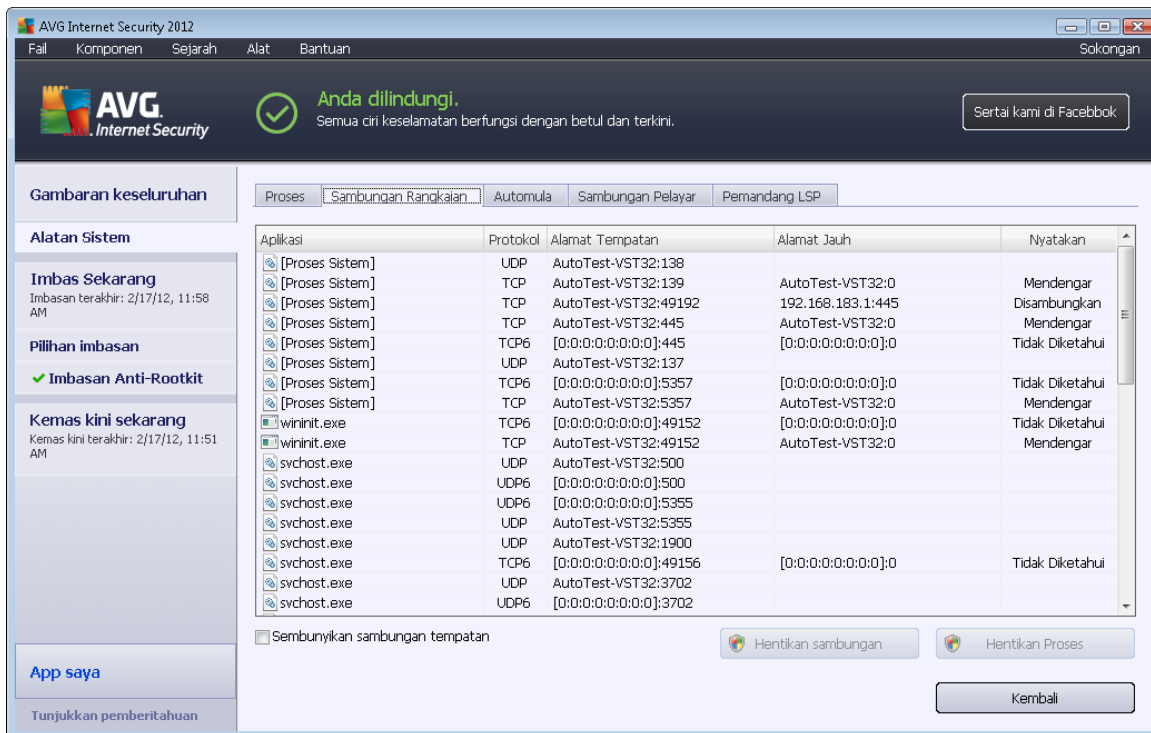
Butang kawalan yang tersedia dalam tab **Proses** adalah seperti berikut:

- **Muat Semula** – mengemas kini senarai proses mengikut status terkini
- **Tamatkan Proses** - anda boleh memilih satu atau lebih aplikasi dan kemudian, menamatkannya dengan menekan butang ini. **Kami amat menyarankan untuk tidak menamatkan sebarang sambungan, melainkan anda betul-betul pasti bahawa ia mewakili ancaman sebenar!**



- **Undur** – mengalihkan anda semula ke [dialog utama AVG](#)lalui (gambaran keseluruhan komponen)

## 6.6.2. Sambungan Rangkaian



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

- **Aplikasi** – nama aplikasi berkaitan dengan sambungan (*dengan pengecualian bagi Windows 2000 di mana maklumat tidak tersedia*)
- **Protokol** – jenis protokol penghantaran digunakan untuk sambungan:
  - TCP – protokol yang digunakan berkaitan dengan Protokol Internet (IP) untuk menghantar maklumat pada Internet
  - UDP – sebagai ganti kepada protokol TCP
- **Alamat tempatan** – alamat IP bagi komputer tempatan dan nombor port yang digunakan
- **Alamat jauh** – alamat IP bagi komputer jauh dan nombor port yang disambungkan. Jika boleh, ia juga akan mencari nama hos bagi komputer jauh.
- **Keadaan** – menunjukkan keadaan semasa yang paling mungkin (*Disambungkan, Pelayan harus tutup, Dengar, Tutup aktif selesai, Tutup pasif, Tutup aktif*)

Untuk menyenaraikan hanya sambungan luaran, tandakan rait kotak semakan **Sembunyikan**



**sambungan tempatan** dalam bahagian bawah dialog di bawah senarai.

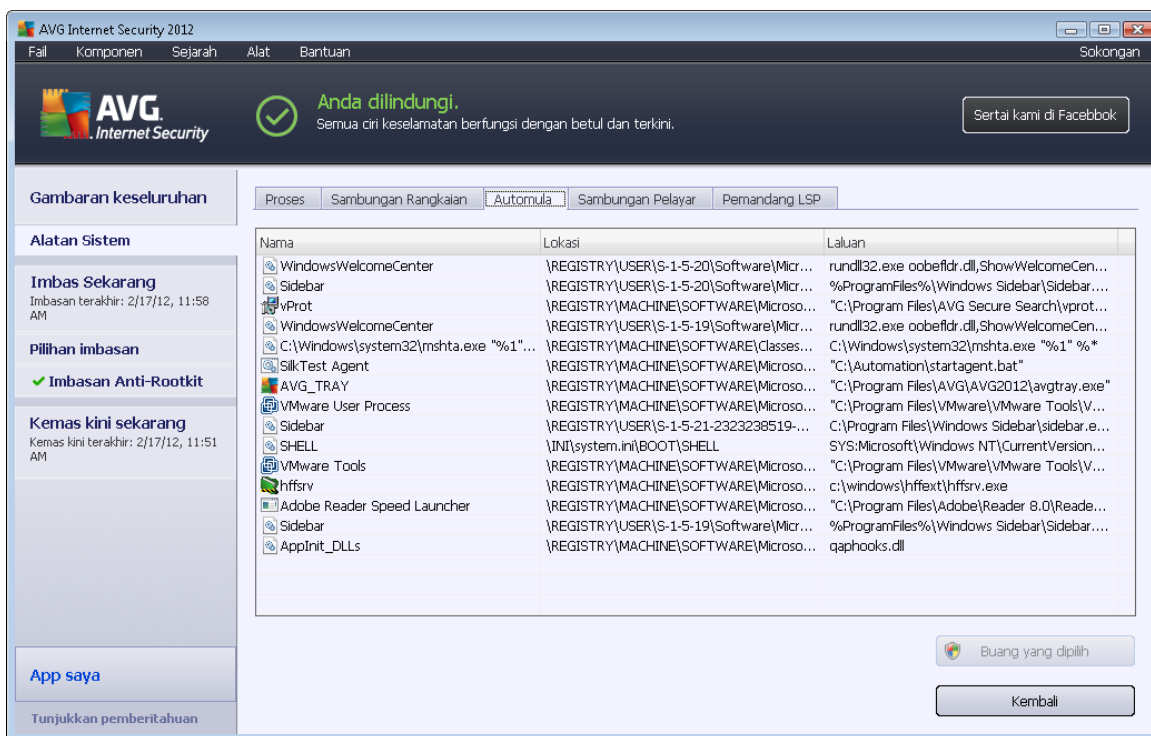
## Butang kawalan

Butang kawalan tersedia dalam tab **Sambungan Rangkaian** adalah seperti berikut:

- **Tamatkan Sambungan** – menutup satu atau lebih sambungan yang dipilih dalam senarai
- **Tamatkan Proses** – menutup satu atau lebih aplikasi berkaitan dengan sambungan yang dipilih dalam senarai
- **Undur** – kembalike [dialog utama AVG](#) lalai (gambaran keseluruhan komponen).

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

### 6.6.3. Automula



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

## Butang kawalan

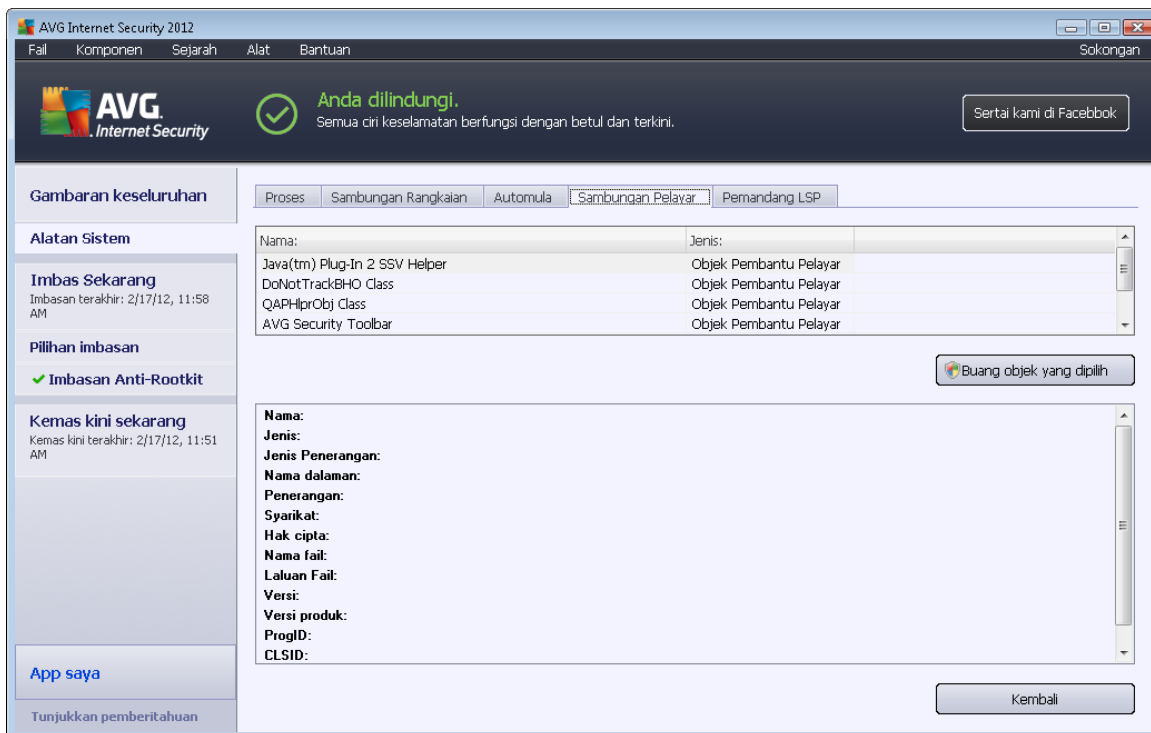


Butang kawalan yang tersedia dalam tab **Auto mula** adalah seperti berikut:

- **Buang yang dipilih** – tekan butang untuk memadam satu atau lebih entri yang dipilih.
- **Undur** - mengalihkan anda kembali ke [dialog utama AVG lalai](#) (gambaran keseluruhan komponen).

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

#### 6.6.4. Sambungan Penyemak Imbas



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

#### Butang kawalan

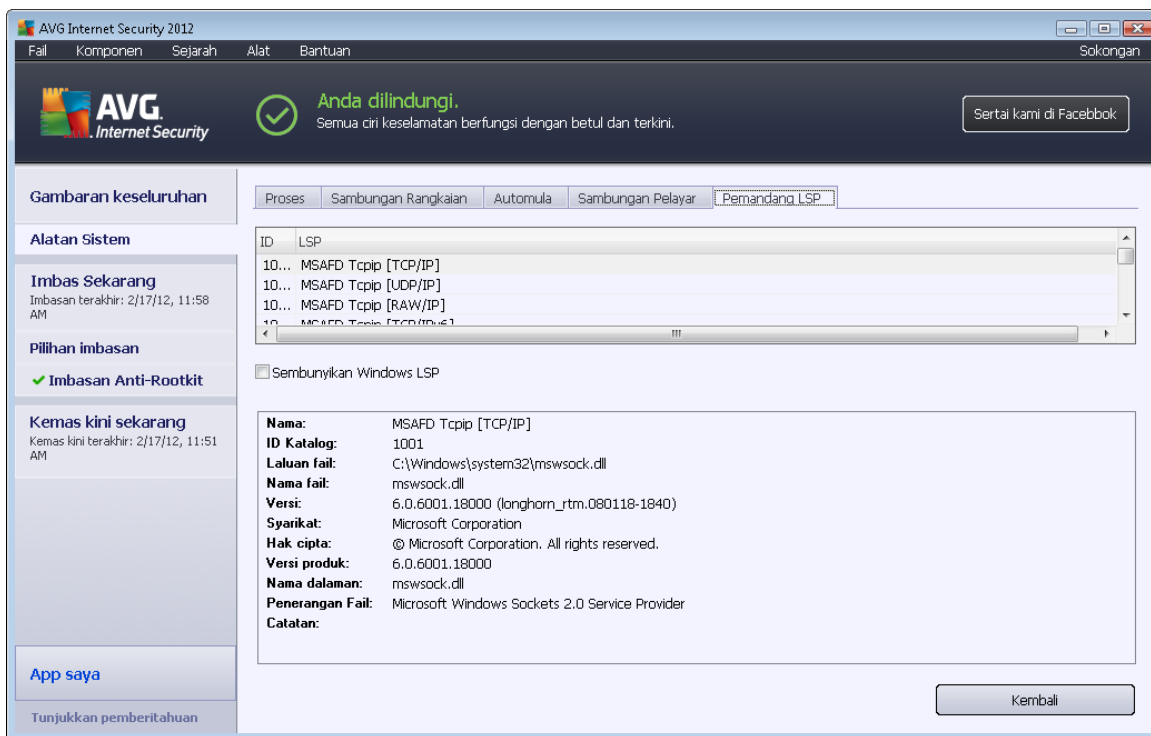
Butang kawalan yang tersedia dalam tab **Sambungan Penyemak Imbas** adalah seperti berikut:

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



komponen).

### 6.6.5. Pemandang LSP



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

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

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

#### Butang kawalan

Butang kawalan yang tersedia dalam tab **LSP Viewer** adalah seperti berikut:

- **Sembunyi Windows LSP** – untuk memasukkan Windows LSP ke dalam senarai, jangan tanda item ini.





- **Undur** – mengalihkan anda kembali ke [dialog utama AVG](#) lalai (*gambaran keseluruhan komponen*).

## 6.7. Penganalisis PC

Komponen **Penganalisis PC** mampu mengimbas komputer anda bagi masalah sistem, dan memberikan anda gambaran keseluruhan telus mengenai apa yang menjejaskan prestasi keseluruhan komputer anda. Dalam antara muka pengguna komponen anda boleh melihat carta yang dibahagikan kepada empat baris yang merujuk kepada kategori tertentu: ralat pendaftar, fail sarap, errors, junk files, pemecahan, dan pintasan rosak:

Kategori	Ralat	Keterangan
<b>Ralat Pendaftar</b>	Ralat menjejaskan kestabilan sistem	
<b>Fail Sarap</b>	Fail ini menggunakan ruang cakera	
<b>Pemecahan</b>	Mengurangkan kelajuan akses cakera	
<b>Pintasan Rosak</b>	Mengurangkan kelajuan semak imbas explorer	

- **Ralat Pendaftar** Akan memberikan anda bilangan ralat dalam Pendaftar Windows . Oleh sebab membaiki Pendaftar memerlukan pengetahuan yang agak tinggi, kami tidak mengesyorkan anda mencuba dan membaikinya sendiri.
- **Fail Sarap** akan memberikan anda bilangan fail yang paling banyak berkemungkinan boleh dilakukan tanpa. Biasanya, ia adalah pelbagai jenis fail sementara, dan fail dalam Tong Kitar Semula.
- **Pemecahan** akan mengira peratusan cakera keras anda yang dipecahkan, iaitu digunakan untuk tempoh yang lama supaya kebanyakan fail, kini, terdapat pada bahagian berbeza bagi cakera fizikal. Anda boleh menggunakan beberapa alat penyahserpihan untuk membetulkan ini.
- **Pintasan Rosak** akan memberitahu anda mengenai pintasan yang tidak lagi berfungsi, membawa kepada lokasi tidak wujud dll.



Untuk memulakan analisis sistem anda, tekan butang **Analisis sekarang**. Anda kemudiannya akan boleh melihat kemajuan analisis dan keputusannya terus di dalam carta:

The screenshot shows the AVG Internet Security 2012 interface. At the top, it says "Anda dilindungi. Semua ciri keselamatan berfungsi dengan betul dan terkini." Below this, there's a section titled "Komponen Penganalisis PC" with a sub-header "Penganalisis PC". A message states: "Penganalisis PC akan mengimbas PC anda dan melaporkan ralat yang menjejaskan prestasinya. Muat turun [AVG PC Tuneup](#) baru untuk membetulkan ralat sekali secara percuma, atau beli untuk tuneup tanpa had selama 12 bulan. [Analisis sekarang](#)".

Below the message, it says "Penganalisis PC telah selesai analisis". There is a table with the following data:

Kategori	Ralat	Keterangan
<b>Ralat Pendaftaran</b> Ralat menjejaskan kestabilan sistem	137 ralat ditemui <a href="#">Butiran...</a>	
<b>Fail Sarap</b> Fail ini menggunakan ruang cakera	293 ralat ditemui <a href="#">Butiran...</a>	
<b>Pemecahan</b> Mengurangkan kelajuan akses cakera	11% dipecahkan <a href="#">Butiran...</a>	
<b>Pintasan Rosak</b> Mengurangkan kelajuan semak imbas explorer	14 ralat ditemui <a href="#">Butiran...</a>	

At the bottom of the interface, there are buttons for "Baki sekarang" and "Batalkan".

Gambaran keseluruhan keputusan menyediakan bilangan masalah sistem yang dikesan (**Ralat**) dibahagikan mengikut kategori tertentu yang diuji. Keputusan analisis juga akan dipaparkan secara grafik pada paksi dalam lajur **Keterangan**.

### Butang kawalan

- **Analisis sekarang** (dipaparkan sebelum analisis bermula) - tekan butang ini untuk melancarkan analisis segera komputer anda
- **Betulkan sekarang** (dipaparkan sebaik sahaja analisis selesai) - tekan butang untuk pergi ke laman web AVG (<http://www.avg.com/>) di halaman yang menyediakan maklumat terperinci dan terkini berkaitan dengan komponen **Penganalisis PC**
- **Batal** – tekan butang ini untuk berhenti menjalankan analisis, atau untuk kembali ke [antara dialog utama AVG](#) lalai (gambaran keseluruhan komponen) sebaik sahaja analisis selesai

## 6.8. Identity Protection

**Identity Protection** adalah komponen antimalware yang melindungi anda daripada semua jenis malware (*perisian pengintip, bot, pencuri identiti, ...*) menggunakan teknologi kelakuan dan memberikan perlindungan hari sifar untuk virus baharu. **Identity Protection** memberi tumpuan kepada mengelakkan pencuri identiti daripada mencuri kata laluan anda, butiran akaun bank, nombor kad kredit dan barangan digital peribadi yang lain yang bernilai daripada semua jenis

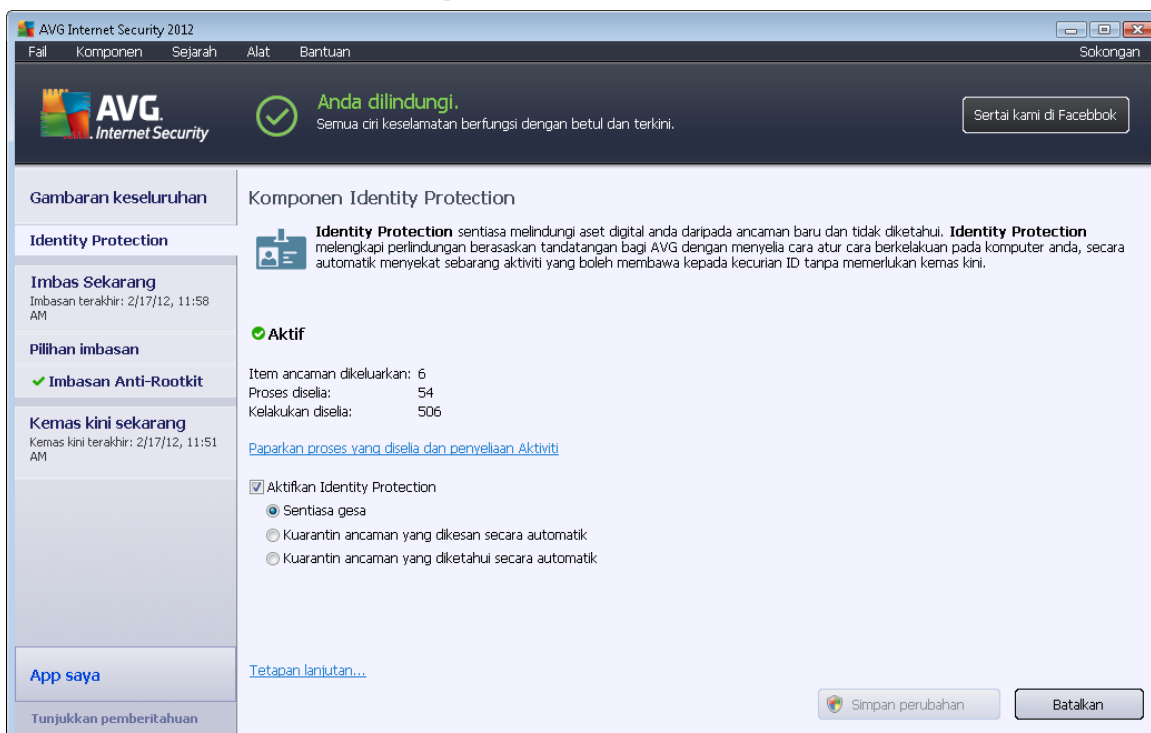


perisian berniat jahat (*malware*) yang menasaskan PC anda. Ia memastikan supaya semua program yang dijalankan pada PC anda atau dalam rangkaian kongsi anda beroperasi dengan betul. **Identity Protection** mengesan dan menyekat kelakuan yang mencurigakan pada asas berterusan dan melindungi komputer anda daripada semua malware baharu.

**Identity Protection** memberikan komputer anda perlindungan masa nyata terhadap ancaman baharu dan malahan, ancaman yang tidak diketahui. Ia mengawasi semua (*termasuk tersembunyi*) proses dan pada lebih 285 corak kelakuan berbeza, dan boleh menentukan sama ada sesuatu berniat jahat berlaku dalam sistem anda. Untuk sebab ini, ia boleh mendedahkan ancaman, malahan, yang belum diterangkan dalam pangkalan data virus. Apabila cebisan kod yang tidak diketahui muncul pada komputer anda, ia diperhatikan dengan serta-merta untuk kelakuan berniat jahat dan dijejaki. Jika fail didapati berniat jahat, **Identity Protection** akan membuang kod ke dalam [Bilik Kebal Virus](#) dan membuat asal sebarang perubahan yang telah dibuat kepada sistem (*suntikan kod, perubahan pendaftar, pembukaan port dll*). Anda tidak perlu memulakan imbasan untuk dilindungi. Teknologi adalah sangat proaktif, jarang sekali, memerlukan kemas kini dan sentiasa dilindungi.

**Identity Protection adalah perlindungan yang perlu kepada Anti-Virus Kami sangat mengesyorkan agar anda mempunyai kedua-dua komponen dipasang, supaya memiliki perlindungan lengkap bagi PC anda!**

### 6.8.1. Antara Muka Identity Protection



Dialog **Identity Protection** memberikan penerangan ringkas mengenai kegunaan asas komponen, statusnya (*Aktif*), dan beberapa data statistik:

- **Item ancaman dibuang** - memberikan bilangan aplikasi yang dikesan sebagai malware, dan dibuang



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

Di bawah anda boleh menemui pautan [Papar proses yang dipantau dan monitor Aktiviti](#) yang akan membawa anda ke antara muka pengguna bagi komponen [Alatan Sistem](#) di mana anda boleh menemui gambaran keseluruhan terperinci bagi semua proses yang dipantau.

### Tetapan Identity Protection Asas

Dalam bahagian bawah dialog, anda boleh mengedit beberapa ciri asas kefungsiian komponen:

- **Aktifkan Identity Protection** - (*dibuka secara lalai*): tanda untuk mengaktifkan komponen IDP dan untuk membuka opsyen pengeditan selanjutnya.

Dalam sesetengah kes, **Identity Protection** mungkin melaporkan bahawa beberapa fail yang sah adalah mencurigakan atau berbahaya. Memandangkan **Identity Protection** mengesan ancaman berdasarkan pada kelakuan mereka, ini biasanya berlaku apabila beberapa atur cara cuba memantau penekanan kekunci, memasang atur cara lain atau pemacu baharu yang dipasang pada komputer. Oleh itu, sila pilih salah satu opsyen berikut yang menentukan kelakuan komponen **Identity Protection** sekiranya mengesan aktiviti mencurigakan:

- **Sentiasa gesa** - jika aplikasi dikesan sebagai malware, anda akan ditanya sama ada ia harus disekat (*pilihan ini dihidupkan secara lalai dan disyorkan untuk tidak mengubahnya melainkan anda mempunyai sebab sebenar untuk melakukannya*)
- **Kuarantin ancaman yang dikesan secara automatik** - semua aplikasi dikesan sebagai malware akan disekat secara automatik
- **Kuarantin ancaman yang diketahui secara automatik** - hanya aplikasi dengan kepastian mutlak dikesan sebagai malware akan disekat
- **Tetapan lanjutan...** – Klik pautan untuk dihalakan semula ke dialog masing-masing dalam [Tetapan lanjutan](#) bagi **AVG Internet Security 2012**. Di situ, anda boleh mengedit konfigurasi komponen secara terperinci. Walau bagaimanapun, sila maklum bahawa konfigurasi lalai bagi semua komponen disediakan supaya **AVG Internet Security 2012** memberikan prestasi optimum, dan keselamatan maksimum. Melainkan anda mempunyai sebab sebenar untuk melakukannya, adalah disyorkan untuk mengekalkan konfigurasi lalai!

### Butang kawalan

Butang kawalan yang tersedia dalam antara muka **Identity Protection** adalah seperti berikut:

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



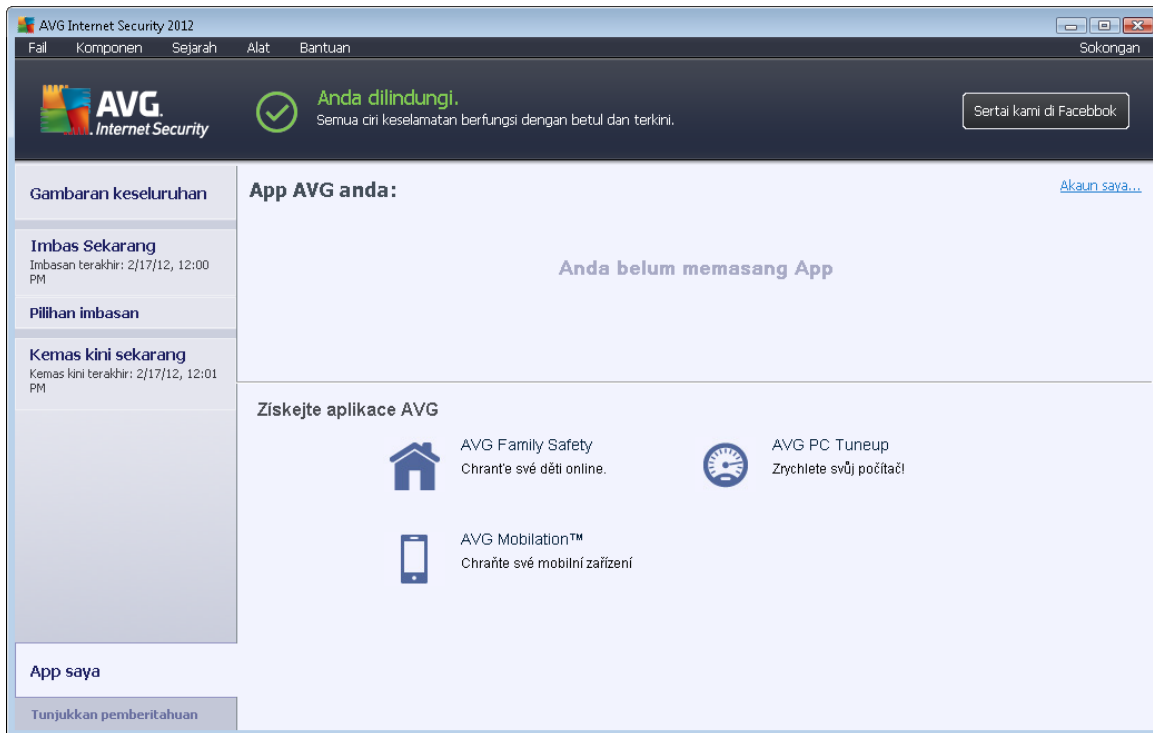
- **Batal** - tekan butang ini untuk kembali ke [dialog utama AVG](#) (gambaran keseluruhan komponen)

## 6.9. Pentadbiran Jauh

Komponen **Pentadbiran Jauh** hanya dipaparkan dalam antara muka pengguna bagi **AVG Internet Security 2012** sekiranya, anda telah memasang Business Edition bagi produk anda (untuk maklumat mengenai lesen yang digunakan untuk pemasangan, sila lihat tab [Versi](#) bagi dialog [Maklumat](#) yang boleh dibuka melalui item menu sistem [Sokongan](#)). Untuk penerangan terperinci mengenai opsyen dan kefungisian komponen dalam sistem Pentadbiran Jauh AVG sila rujuk dokumentasi khusus yang ditetapkan untuk topik ini secara eksklusif. Dokumen ini tersedia untuk muat turun di laman web AVG (<http://www.avg.com/>), dalam seksyen **Pusat sokongan / Muat turun / Dokumentasi**.

## 7. App saya

Dialog **Aplikasi Saya** (boleh diakses terus melalui butang Aplikasi Saya dari dialog utama AVG) memberikan gambaran keseluruhan terhadap aplikasi sendiri AVG, di mana kedua-duanya telah dipasangkan pada komputer anda atau sedia untuk dipasangkan, secara pilihan:



Dialog dibahagikan kepada dua bahagian:

- **Aplikasi AVG Anda** – memberikan gambaran keseluruhan terhadap semua aplikasi sendiri AVG yang telah dipasangkan pada komputer anda;
- **Dapatkan Aplikasi AVG** – menawarkan gambaran keseluruhan aplikasi sendiri AVG yang mungkin anda minati. Aplikasi ini sedia untuk dipasangkan. Tawaran ini berubah secara dinamik berdasarkan pada lesen, lokasi anda serta kriteria lain. Untuk maklumat terperinci tentang aplikasi ini sila rujuk laman web AVG (<http://www.avg.com/>).

Berikut, sila dapatkan gambaran keseluruhan ringkas tentang semua aplikasi tersedia dan penerangan ringkas tentang kefungsiannya:

### 7.1. AVG Family Safety

**AVG Family Safety** membantu anda melindungi anak anda daripada laman web, kandungan media dan carian dalam talian yang tidak sesuai, dan memberikan anda laporan berkenaan aktiviti dalam talian mereka. **AVG Family Safety** menggunakan teknologi ketukan kekunci untuk mengawasi aktiviti anak anda dalam bilik bual dan pada tapak rangkaian sosial. Jika ia menjumpai perkataan, ungkapan atau bahasa yang diketahui digunakan untuk menjadikan kanak-kanak mangsa dalam talian, ia akan memaklumkan kepada anda dengan segera melalui SMS atau e-mel. Aplikasi ini



mbolehkan anda menetapkan tahap perlindungan yang sesuai untuk setiap anak anda dan memantaunya secara berasingan melalui log masuk unik.

**Untuk maklumat terperinci, sila lawati halaman web AVG yang dikhaskan yang anda juga boleh muat turun komponen dengan serta-merta. Untuk melakukannya, anda boleh menggunakan pautan AVG Family Safety dalam dialog [Aplikasi Saya](#).**

## 7.2. AVG LiveKive

**AVG LiveKive** dikhususkan untuk sandaran data dalam talian pada pelayan yang selamat. **AVG LiveKive** secara automatik membuat sandaran semua fail, foto dan muzik anda di satu tempat yang selamat, membolehkan anda berkongsinya dengan keluarga dan rakan serta mengaksesnya dari sebarang peranti didayakan web, termasuk peranti iPhones dan Android. Ciri **AVG LiveKive** termasuk:

- Langkah keselamatan sekiranya komputer anda dan/atau cakera keras rosak
- Akses kepada data anda dari sebarang peranti yang disambungkan ke Internet
- Pengaturan mudah
- Berkongsi dengan sesiapa yang anda benarkan

**Untuk maklumat terperinci, sila lawati halaman web AVG yang dikhaskan yang anda juga boleh muat turun komponen dengan serta-merta. Untuk melakukannya, anda boleh menggunakan pautan AVG LiveKive dalam dialog [Aplikasi Saya](#).**

## 7.3. AVG Mobilation

**AVG Mobilation** melindungi telefon bimbit anda daripada virus dan malware serta memberikan anda keupayaan menjejak telefon pintar anda dari jauh sekiranya anda kehilangannya. Ciri **AVG Mobilation** termasuk:

- *Pengimbas Fail* membolehkan pengimbasan keselamatan fail dalam lokasi storan yang berlainan;
- *Penghenti Tugas* membolehkan anda menghentikan aplikasi sekiranya peranti menjadi perlahan atau terhenti;
- *Pengunci Aplikasi* membolehkan anda mengunci dan melindungi satu atau lebih aplikasi dengan menggunakan kata laluan untuk menghalang penyalahgunaan;
- *Tuneup* mengumpul berbagai parameter sistem (*meter bateri, penggunaan storan, saiz dan lokasi pemasangan aplikasi, dll.*) ke dalam paparan tunggal berpusat untuk membantu anda mengawal prestasi sistem;
- *Sandaran Aplikasi* membolehkan anda membuat sandaran aplikasi pada kad SD dan memulihkannya kemudian;
- *Xipit Spam dan Penipuan* membolehkan anda menandakan mesej SMS sebagai spam dan



melaporkan laman web sebagai penipuan;

- *Padam bersih data peribadi* dari jauh sekiranya telefon anda dicuri;
- *Pelayaran Web Selamat* menawarkan pengawasan masa nyata halaman web yang anda lawati.

**Untuk maklumat terperinci, sila lawati halaman web AVG yang dikhaskan yang anda juga boleh muat turun komponen dengan serta-merta. Untuk melakukannya, anda boleh menggunakan pautan AVG Mobilation dalam dialog [Aplikasi Saya](#).**

#### **7.4. AVG PC Tuneup**

Aplikasi **AVG PC Tuneup** adalah alat lanjutan untuk analisis dan pembetulan sistem terperinci, seperti bagaimana kelajuan dan prestasi keseluruhan komputer anda mungkin diperbaiki. Ciri **AVG PC Tuneup** termasuk:

- *Pencuci Cakera* – Mengeluarkan fail sarap yang melambatkan komputer.
- *Pemecahan Cakera* - Memecahkan pemacu cakera dan mengoptimumkan peletakan fail sistem.
- *Pencuci Pendaftar* – Membaiki ralat pendaftar untuk meningkatkan kestabilan PC.
- *Pemecahan Pendaftar* – Memadatkan jarak yang menggunakan memori penyingkiran.
- *Doktor Cakera* – Mencari sektor rosak, gugusan yang hilang dan ralat direktori serta membaikinya.
- *Pengoptimum Internet* - Mengikuti tetapan satu saiz untuk semua kepada sambungan Internet khas.
- *Pemadam Penjejakan* – Mengeluarkan sejarah komputer dan penggunaan Internet.
- *Pemadam Cakera* – Memadam bersih ruang kosong pada cakera untuk mengelakkan pemulihan data sensitif.
- *Pencarik Fail* – Memadam fail yang dipilih melebihi pemulihan pada cakera atau kayu USB.
- *Pemulihan Fail* – Memulihkan fail yang dipadam dari cakera, kayu USB atau kamera secara tidak sengaja.
- *Pencari Fail Pendua* – Membantu mencari dan mengeluarkan fail pendua yang mengisi ruang cakera.
- *Pengurus Perkhidmatan* – Menyahdaya perkhidmatan yang tidak diperlukan yang melambatkan komputer.
- *Pengurus Permulaan* – membenarkan pengguna mengurus atur cara yang bermula secara





automatik pada but Windows.

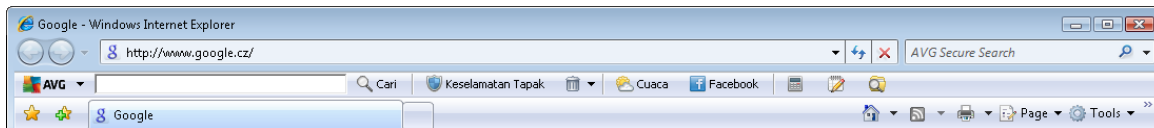
- *Pengurus Nyahpasang* – Menyahpasang sepenuhnya atur cara perisian yang anda tidak perlukan lagi.
- *Pengurus Tweak* - Membenarkan pengguna menala ratusan tetapan Windows yang tersembunyi.
- *Pengurus Tugas* - Menyenaraikan semua proses, perkhidmatan yang dijalankan dan fail yang dikunci.
- *Penjelajah Cakera* - Menunjukkan fail mana yang menggunakan paling banyak ruang pada komputer.
- *Maklumat Sistem* – Memberikan maklumat terperinci mengenai perkakasan dan perisian yang dipasang.

***Untuk maklumat terperinci, sila lawati halaman web AVG yang dikhaskan yang anda juga boleh muat turun komponen dengan serta-merta. Untuk melakukannya, anda boleh menggunakan pautan AVG PC Tuneup dalam dialog [Aplikasi Saya](#).***



## 8. AVG Security Toolbar

**AVG Security Toolbar** ialah alat yang berfungsi bersama dengan komponen [LinkScanner](#), dan mengawal keselamatan maksimum anda semasa menyemak imbas Internet. Dalam **AVG Internet Security 2012**, pemasangan **AVG Security Toolbar** adalah pilihan; sewaktu [proses pemasangan](#) anda dijemput untuk menentukan sama ada komponen perlu dipasang. **AVG Security Toolbar** tersedia secara terus dalam penyemak imbas Internet anda. Buat masa ini, penyemak imbas yang disokong adalah Internet Explorer (*versi 6.0 dan lebih tinggi*), dan/atau Mozilla Firefox (*versi 3.0 dan lebih tinggi*). Tiada penyemak imbas lain yang disokong (*sekiranya, anda menggunakan beberapa penyemak imbas Internet alternatif, cth Avant Browser, anda boleh bertemu kelakuan yang tidak dijangka*).



**AVG Security Toolbar** terdiri daripada yang berikut:

- **Logo AVG** dengan menu jatuh ke bawah:
  - **Gunakan AVG Secure Search** - Membolehkan anda mencari secara terus dari **AVG Security Toolbar** menggunakan enjin **AVG Secure Search**. Semua keputusan carian secara berterusan, diperiksa oleh perkhidmatan [Search-Shield](#), dan anda boleh merasakan pasti selamat dalam talian.
  - **Tahap Ancaman Semasa** - membuka halaman web lab virus dengan paparan grafik bagi tahap ancaman semasa pada web.
  - **Makmal Ancaman AVG** – Membuka laman web **Makmal Ancaman AVG** khusus (di <http://www.avgthreatlabs.com>) di mana anda boleh menemui maklumat tentang berbagai keselamatan laman web dan tahap ancaman semasa dalam talian.
  - **Bantuan Bar Alat** - Membuka bantuan dalam talian yang meliputi semua kefungsiian **AVG Security Toolbar**.
  - **Serahkan maklum balas Produk** - Membuka halaman web dengan borang yang anda boleh isikan dan memberitahu kami mengenai pendapat mengenai **AVG Security Toolbar**.
  - **Mengenai...** - Membuka tettingkap baharu dengan maklumat pada versi **AVG Security Toolbar** yang dipasang buat masa ini.
- **Medan carian** - Cari di Internet menggunakan **AVG Security Toolbar** untuk pasti selamat dan selesai memandangkan semua keputusan carian yang dipaparkan adalah selamat seratus peratus. Isikan kata kunci atau ungkapan ke dalam medan carian, dan tekan butang **Cari** (atau **Enter**). Semua keputusan carian secara berterusan, diperiksa oleh perkhidmatan [Search-Shield](#) (dalam komponen [LinkScanner](#)).
- **Keselamatan Tapak** – Butang ini membuka dialog baru yang membuktikan maklumat mengenai tahap ancaman semasa (*Selamat buat masa ini*) bagi halaman yang baharu sahaja anda lawati. Gambaran keseluruhan ringkas ini boleh dikembangkan dan dipaparkan dengan butiran penuh

semua aktiviti keselamatan yang berkaitan dengan halaman tersebut terus di dalam tettingkap penyemak imbas (*Lihat laporan lengkap*):



- **Padam** – Butang 'tong sampah' memberikan menu gulung bawah di mana anda boleh memilih sama ada anda mahu memadam maklumat mengenai penyemakan imbas, muat turun, borang dalam talian anda atau memadam semua sejarah carian anda sekali gus.
- **Cuaca** – Butang membuka dialog baharu memberikan maklumat mengenai cuaca semasa di lokasi anda, dan ramalan cuaca untuk dua hari akan datang. Maklumat ini sedang dikemas kini secara tetap, setiap 3-6 jam. Dalam dialog, anda boleh menukar lokasi yang dikehendaki secara manual, dan untuk menentukan sama ada anda ingin melihat maklumat suhu dalam Celcius atau Fahrenheit.



- **Facebook** – Butang ini membolehkan anda bersambung ke rangkaian sosial [Facebook](#) secara terus dari dalam **AVG Security Toolbar**.
- Butang pintasan untuk akses pantas kepada aplikasi ini: **Kalkulator**, **Pad Nota**, **Windows Explorer**.



## 9. AVG Do Not Track

**AVG Do Not Track membantu anda mengenal pasti laman web yang mengumpulkan data mengenai aktiviti dalam talian anda.** Ikon dalam penyemak imbas anda menunjukkan tapak web atau pengiklan yang mengumpulkan data mengenai aktiviti anda dan memberikan anda pilihan untuk membenarkan atau tidak membenarkannya.

- **AVG Do Not Track** memberikan anda maklumat tambahan mengenai dasar privasi bagi setiap perkhidmatan berkaitan serta pautan terus untuk Memilih keluar daripada perkhidmatan itu, jika tersedia.
- Selain itu, **AVG Do Not Track** menyokong [protokol W3C DNT](#) untuk memaklumkan tapak secara automatik bahawa anda tidak mahu dijejaki. Pemberitahuan ini didayakan secara lalai tetapi boleh diubah pada bila-bila masa.
- **AVG Do Not Track** disediakan mengikut [terma dan syarat](#) ini.
- **AVG Do Not Track didayakan secara lalai tetapi boleh dinyahdayakan dengan mudah pada bila-bila masa.** Arahan boleh ditemui dalam artikel Soalan Lazim [Menyahdayakan ciri AVG Do Not Track](#).
- Untuk maklumat lanjut mengenai **AVG Do Not Track**, sila lawati [laman web](#) kami.

Buat masa ini, kefungsiian **AVG Do Not Track** disokong dalam penyemak imbas Mozilla Firefox, Chrome dan Internet Explorer. *(Dalam Internet Explorer, ikon AVG Do Not Track terletak di sebelah kanan bar arahan. Jika anda menghadapi masalah untuk melihat ikon AVG Do Not Track dengan tetapan lalai penyemak imbas, sila pastikan anda mengaktifkan bar arahan. Jika anda masih tidak dapat melihat ikon tersebut, sila seret bar arahan ke sebelah kiri untuk mendedahkan semua ikon dan butang yang tersedia dalam bar alat ini.)*

## 9.1. Antara muka AVG Do Not Track

Semasa dalam talian, **AVG Do Not Track** memberi amaran kepada anda sebaik sahaja sebarang jenis aktiviti pengumpulan data dikesan. Anda akan melihat dialog berikut:



Semua perkhidmatan pengumpulan data yang dikesan disenaraikan mengikut nama dalam gambaran keseluruhan **Penjejak di halaman ini**. Terdapat tiga jenis aktiviti pengumpulan data yang dikenali oleh **AVG Do Not Track**:

- **Web Analytics** (*dibenarkan secara lalai*): Perkhidmatan yang digunakan untuk memperbaiki prestasi dan pengalaman laman web berkenaan. Dalam kategori ini anda boleh menemui perkhidmatan seperti Google Analytics, Omniture atau Yahoo Analytics. Kami mengesyorkan supaya tidak menyekat perkhidmatan analisis web kerana laman web mungkin tidak akan berfungsi seperti yang dimaksudkan.
- **Social Buttons** (*dibenarkan secara lalai*): Elemen yang direka bentuk untuk memperbaiki pengalaman perangkaian sosial. Butang sosial disampaikan dari rangkaian sosial ke laman yang sedang anda lawati. Butang tersebut boleh mengumpulkan data mengenai aktiviti dalam talian anda semasa anda dilog masuk. Contoh Butang sosial termasuk: Pemalam Sosial Facebook, Butang Twitter, Google +1.
- **Ad Networks** (*sesetengah disekat secara lalai*): Perkhidmatan yang mengumpulkan atau berkongsi data mengenai aktiviti dalam talian anda pada berbilang laman, sama ada secara langsung atau tidak langsung, untuk menawarkan anda iklan yang diperibadikan tidak seperti iklan berasaskan kandungan. Hal ini ditentukan berdasarkan pada dasar privasi setiap rangkaian iklan seperti yang tersedia pada tapak web perkhidmatan itu. Sesetengah rangkaian iklan disekat secara lalai.



**Nota:** Bergantung kepada perkhidmatan apa yang sedang berjalan dalam latar belakang tapak web, beberapa daripada tiga bahagian yang diterangkan di atas mungkin tidak kelihatan dalam dialog AVG Do Not Track.

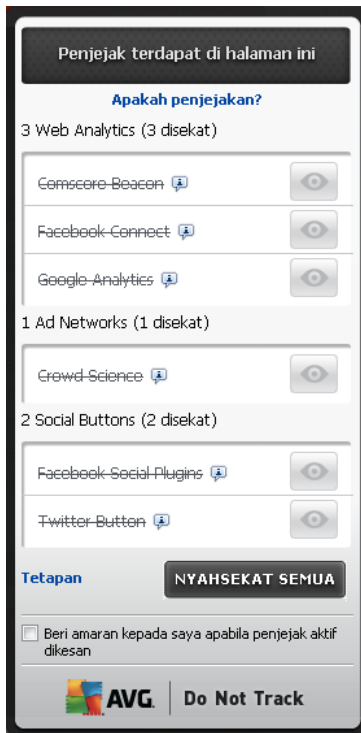
Dialog itu juga mengandungi dua hiperpautan:

- **Apakah penjejakan?** - klik pautan ini di bahagian atas dialog untuk dihalakan semula ke halaman web yang dikhususkan untuk memberi penerangan terperinci terhadap prinsip penjejakan dan huraian jenis penjejakan tertentu.
- **Tetapan** - klik pautan ini di bahagian bawah dialog untuk dihalakan semula ke halaman web yang dikhususkan di mana anda boleh menetapkan konfigurasi tertentu untuk pelbagai parameter **AVG Do Not Track** (lihat bab [tetapan AVG Do Not Track](#) untuk maklumat terperinci)

## 9.2. Maklumat tentang proses penjejakan



Senarai perkhidmatan pengumpulan data yang dikesan hanya menyediakan nama perkhidmatan tertentu sahaja. Untuk membuat keputusan dengan mengetahui sama ada perkhidmatan berkenaan harus disekat atau dibenarkan, anda mungkin perlu mengetahui dengan lebih lanjut. Gerakkan tetikus anda ke atas item senarai berkenaan. Gelembung maklumat akan kelihatan dengan memberikan data terperinci mengenai perkhidmatan tersebut. Anda akan mengetahui sama ada perkhidmatan tersebut mengumpul data peribadi atau data lain yang boleh didapati; sama ada data tersebut dikongsi dengan subjek pihak ketiga yang lain dan sama ada data yang dikumpulkan itu difailkan untuk penggunaan selanjutnya.

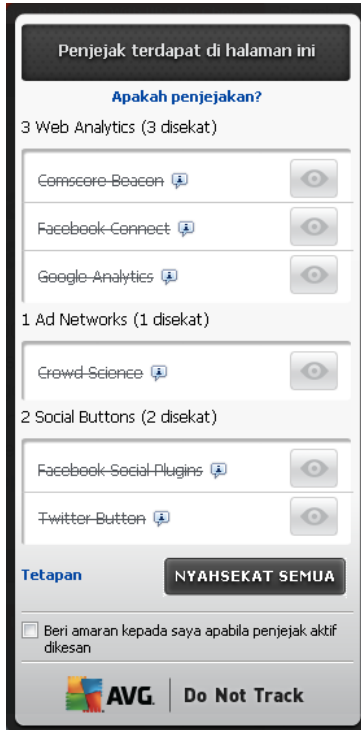
Di bahagian bawah gelembung maklumat anda boleh melihat hiperpautan **Dasar Privasi** yang menghalakan anda semula ke tapak web yang dikhususkan untuk dasar privasi perkhidmatan yang dikesan berkenaan.



### 9.3. Menyekat proses penjejakan

Dengan adanya semua senarai Ad Networks / Social Buttons / Web Analytics, anda kini mempunyai opsyen untuk mengawal perkhidmatan mana yang harus disekat. Anda boleh melakukannya dengan dua cara:

- **Sekat Semua** - Klik butang ini yang terdapat di bahagian bawah dialog bagi menyatakan bahawa anda tidak mahu sebarang aktiviti pengumpulan data sama sekali. *(Namun, sila ingat bahawa tindakan ini mungkin menjejaskan kefungsiian dalam halaman web berkaitan di mana perkhidmatan ini sedang berjalan!)*
-  - Jika anda tidak mahu menyekat semua perkhidmatan yang dikesan sekali gus, anda boleh menentukan secara individu sama ada perkhidmatan tersebut harus dibenarkan atau disekat. Anda boleh membenarkan untuk menjalankan beberapa sistem yang dikesan (*mis. Web Analytics*): sistem ini menggunakan data yang dikumpulkan untuk pengoptimuman laman web mereka sendiri dan dengan cara ini mereka dapat membantu memperbaiki persekitaran Internet umum untuk semua pengguna. Namun, pada masa yang sama anda boleh menyekat aktiviti pengumpulan data bagi semua proses yang dikelaskan sebagai Ad Networks. Cuma klik ikon  bersebelahan perkhidmatan masing-masing untuk menyekat pengumpulan data (*nama proses akan kelihatan sebagai digariskan*) atau untuk membenarkan pengumpulan data sekali lagi.



#### 9.4. Tetapan AVG Do Not Track

Terus dalam dialog **AVG Do Not Track**, terdapat hanya satu opsi konfigurasi: di bahagian bawah anda boleh melihat kotak semak **Beri amaran kepada saya apabila penjejak aktif dikesan**. Secara lalainya, item ini tidak dipilih. Tandakan kotak semak untuk mengesahkan bahawa anda mahu diberitahu setiap kali anda masuk ke halaman web yang mengandungi perkhidmatan pengumpulan data baru yang belum lagi disekat. Apabila ditandakan, jika **AVG Do Not Track** mengesan perkhidmatan pengumpulan data baru dalam halaman yang sedang anda lawati, dialog pemberitahuan muncul di skrin anda. Jika tidak, anda hanya akan perhatikan perkhidmatan yang baru dikesan oleh ikon **AVG Do Not Track** (*terletak dalam bar arahan penyemak imbas anda*) mengubah warnanya daripada hijau kepada kuning.

Walau bagaimanapun, di bahagian bawah dialog **AVG Do Not Track** anda boleh menemui pautan **Tetapan**. Klik pautan tersebut untuk dihalakan semula ke halaman web khusus di mana anda boleh menentukan **Opsi AVG Do Not Track** anda dengan terperinci:





## Opsyen AVG Do Not Track

### Beritahu Saya

Paparkan pemberitahuan untuk  saat

Kedudukan pemberitahuan

- Beri amaran kepada saya apabila penjejak aktif dikesan
- Beritahu tapak web bahawa saya tidak mahu dijejaki (menggunakan [pengepala http](#) Do Not Track)

### Sekat yang berikut

<input checked="" type="checkbox"/>	24/7 Real Media	Ad Networks
<input checked="" type="checkbox"/>	33Across	Ad Networks
<input checked="" type="checkbox"/>	[x+1]	Ad Networks
<input checked="" type="checkbox"/>	Accelerator Media	Ad Networks
<input checked="" type="checkbox"/>	AddtoAny	Ad Networks
<input checked="" type="checkbox"/>	Adition	Ad Networks
<input checked="" type="checkbox"/>	AdReady	Ad Networks
<input checked="" type="checkbox"/>	Aggregate Knowledge	Ad Networks
<input checked="" type="checkbox"/>	Baynote Observer	Ad Networks
<input checked="" type="checkbox"/>	Bizo	Ad Networks

- **Kedudukan pemberitahuan (Atas Sebelah Kanan secara lalainya)** - Buka menu gulung bawah untuk menentukan dalam kedudukan mana anda mahu dialog **AVG Do Not Track** kelihatan pada monitor anda.
- **Papar pemberitahuan selama (10 secara lalainya)** - Dalam medan ini anda harus menentukan berapa lama (*dalam saat*) anda ingin melihat pemberitahuan **AVG Do Not Track** pada skrin anda. Anda boleh menentukan nombor di antara 0 hingga 60 saat (*bagi 0, pemberitahuan tidak akan kelihatan sama sekali pada skrin anda*).
- **Beri amaran kepada saya apabila penjejak aktif dikesan (dimatikan secara lalai)** - Tandakan kotak semak untuk mengesahkan bahawa anda mahu diberitahu setiap kali anda masuk ke halaman web yang mengandungi perkhidmatan pengumpulan data baru yang belum lagi disekat. Apabila ditandakan, jika **AVG Do Not Track** mengesan perkhidmatan pengumpulan data baru dalam halaman yang sedang anda lawati, dialog pemberitahuan muncul di skrin anda. Jika tidak, anda hanya akan perhatikan perkhidmatan yang baru dikesan oleh ikon **AVG Do Not Track** (*terletak dalam bar arahan penyemak imbas anda*) mengubah warnanya daripada hijau kepada kuning.
- **Beritahu laman web bahawa saya tidak mahu dijejaki (dihidupkan secara lalai)** - Biarkan



opsyen ini ditandakan untuk mengesahkan anda mahu **AVG Do Not Track** memberitahu pembekal perkhidmatan perkhidmatan pengumpulan data yang dikesan bahawa anda tidak mahu dijejak.

- **Sekat yang berikut** (*semua perkhidmatan pengumpulan data yang disenaraikan dibenarkan secara lalai*) – Dalam bahagian ini anda boleh melihat kotak yang mengandungi senarai perkhidmatan pengumpulan data yang diketahui yang boleh dikelaskan sebagai Ad Networks. Secara lalainya, **AVG Do Not Track** menyekat beberapa Ad Networks secara automatik dan ia kekal bergantung kepada keputusan anda sama ada selebihnya harus juga disekat atau terus dibenarkan. Untuk melakukannya, hanya klik butang **Sekat Semua** di bawah senarai.

Butang kawalan yang tersedia dalam halaman **Opsyen AVG Do Not Track** adalah seperti berikut:

- **Sekat Semua** – klik untuk menyekat sekali gus semua perkhidmatan yang tersenarai dalam kotak di atas yang dikelaskan sebagai Ad Networks;
- **Benarkan Semua** – klik untuk menyahsekat sekali gus semua perkhidmatan yang disekat sebelum ini yang tersenarai dalam kotak di atas dan dikelaskan sebagai Ad Networks;
- **Lalai** – klik untuk membuang semua tetapan tersuai anda dan untuk kembali ke konfigurasi lalai;
- **Simpan** – klik untuk menggunakan dan menyimpan semua konfigurasi yang anda telah tentukan;
- **Batal** – klik untuk membatalkan semua tetapan yang anda telah tentukan sebelum ini.

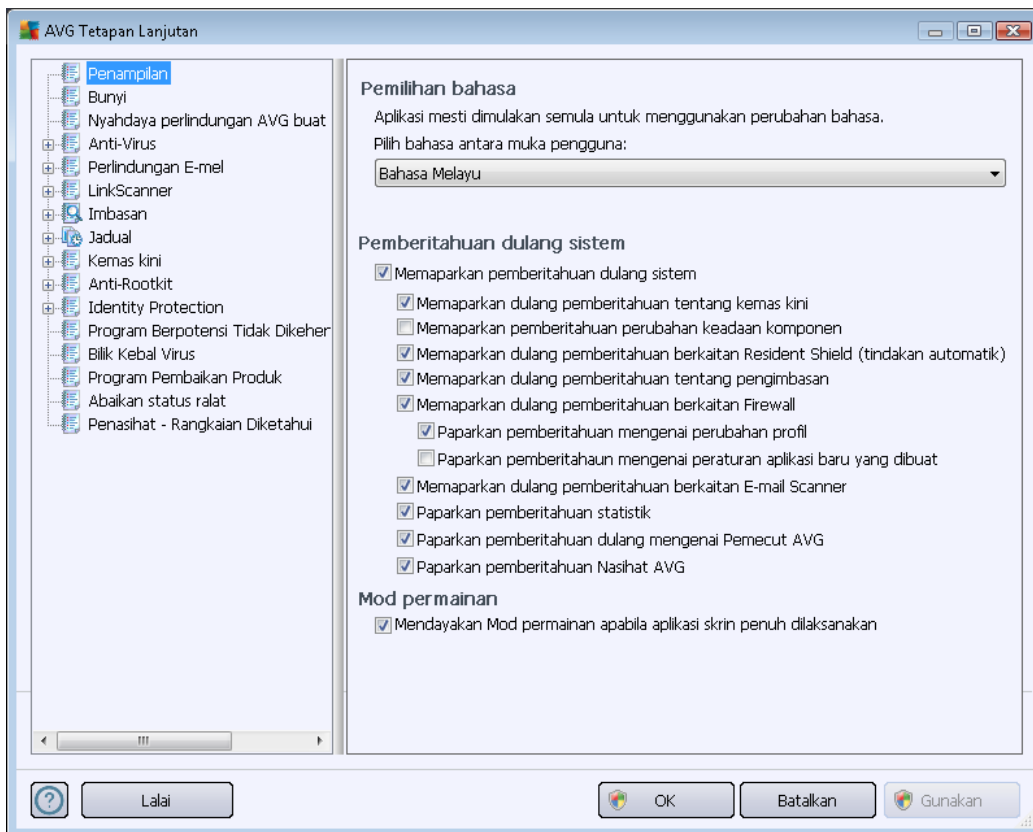


## 10. Tetapan Lanjutan AVG

Dialog konfigurasi lanjutan **AVG Internet Security 2012** terbuka dalam 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 tertentu*) untuk membuka dialog pengeditan dalam bahagian kanan tettingkap.

### 10.1. Penampilan

Item pertama pepohon navigasi, **Penampilan**, merujuk kepada tetapan umum [antara muka pengguna](#) AVG Internet Security 2012 dan memberikan beberapa opsyen asas bagi melakukan aplikasi:

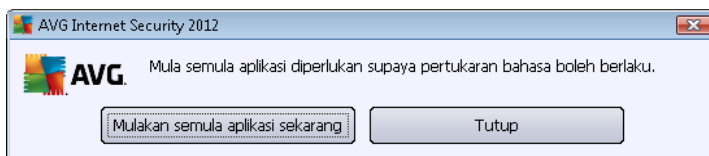


#### Pemilihan bahasa

Dalam seksyen **Pilihan bahasa**, anda boleh memilih bahasa yang anda inginkan dari menu jatuh ke bawah. Bahasa yang dipilih akan kemudiannya digunakan untuk seluruh [antara muka pengguna AVG Internet Security 2012](#). Menu jatuh ke bawah menawarkan bahasa yang anda pilih sebelum ini untuk dipasang semasa [proses pemasangan](#) (*lihat bab [Opsyen tersuai](#)*) dan Bahasa Inggeris (*yang sentiasa dipasang secara automatik, secara lalai*). Untuk selesai menukar **AVG Internet Security 2012** anda ke bahasa lain, anda perlu memulakan semula aplikasi. Sila ikuti langkah-langkah ini:



- Dalam menu jatuh ke bawah, pilih bahasa yang dikehendaki bagi aplikasi
- Sahkan pilihan anda dengan menekan butang **Guna** (*penjuru bawah sebelah kanan bagi dialog*)
- Tekan butang **OK** untuk mengesahkan
- Pop timbul dialog baharu memaklumkan kepada anda bahawa untuk menukar bahasa bagi aplikasi, anda perlu memulakan semula **AVG Internet Security 2012**
- Tekan butang **Mula semula aplikasi sekarang** untuk bersetuju dengan mula semula atur cara, dan tunggu beberapa saat untuk pertukaran bahasa dilakukan:



### Pemberitahuan dulang sistem

Dalam seksyen ini, anda boleh menindas pemberitahuan dulang sistem pada status bagi aplikasi **AVG Internet Security 2012**. Secara lalai, pemberitahuan sistem dibenarkan untuk dipaparkan. Ia amat disyorkan untuk mengekalkan konfigurasi ini! Pemberitahuan sistem memaklumkan, contohnya, bagi pengimbasan atau mengemas kini pelancaran proses, atau pada perubahan status bagi komponen **AVG Internet Security 2012**. Anda sudah tentu perlu beri perhatian kepada pengumuman ini!

Walau bagaimanapun, jika atas beberapa sebab anda memutuskan bahawa anda tidak mahu pemberitahuan ini dipaparkan, atau hanya inginkan pemberitahuan tertentu (*berkaitan dengan komponen AVG Internet Security 2012*) untuk dipaparkan, anda boleh mentakrifkan dan menentukan pilihan anda dengan menanda/tidak menanda pilihan berikut:

- **Paparkan pemberitahuan dulang sistem** (*dihidupkan, secara lalai*) - Secara lalai, semua pemberitahuan dipaparkan. Jangan tanda item ini untuk mematikan sepenuhnya semua paparan sistem. Semasa dihidupkan, anda seterusnya boleh memilih pemberitahuan khusus mana yang harus dipaparkan:
  - **Paparkan pemberitahuan dulang mengenai [kemas kini](#)** (*dihidupkan, secara lalai*) - Tentukan sama ada maklumat berkenaan **AVG Internet Security 2012** pelancaran proses kemas kini, perkembangan, dan pemuktamadan perlu dipaparkan.
  - **Paparkan pemberitahuan perubahan keadaan komponen** (*dimatikan, secara lalai*) – Tentukan sama ada maklumat berkenaan aktiviti/tiada aktiviti komponen, atau berkemungkinan, masalah perlu dipaparkan. Semasa melaporkan status kerosakan komponen, opsyen ini sama dengan fungsi berguna bagi [ikon dulang sistem](#) **AVG Internet Security 2012** melaporkan masalah dalam sebarang komponen .
  - **Paparkan pemberitahuan dulang berkaitan [Resident Shield](#)** (*tindakan automatik*) (*dihidupkan, secara lalai*) – Tentukan sama ada maklumat berkenaan



proses penyimpanan, penyalinan dan membuka fail perlu dipaparkan atau ditindas ( konfigurasi ini hanya ditunjukkan jika opsiyen [Autopulih Resident Shield](#) dihidupkan).

- **Paparkan pemberitahuan dulang mengenai [pengimbasan](#)** (dihidupkan, secara lalai) - Tentukan sama ada maklumat mengenai pelancaran maklumat bagi imbasan yang dijadualkan, perkembangan dan keputusannya perlu dipaparkan.
- **Paparkan pemberitahuan dulang berkaitan [Firewall](#)** (dihidupkan, secara lalai) - Tentukan sama ada maklumat berkenaan status dan proses [Firewall](#), cth. amaran pengaktifan/penyahaktifan komponen, berkemungkinan halangan lalu lintas dll. harus dipaparkan. Item ini memberikan dua lagi opsiyen pilihan khusus (untuk penerangan terperinci bagi setiap satunya, sila rujuk bab [Firewall](#) bagi dokumen ini):
  - **Paparkan pemberitahuan mengenai perubahan profil** (dihidupkan, secara lalai) – Memaklumkan anda mengenai perubahan automatik mengenai profil [Firewall](#).
  - **Paparkan pemberitahuan mengenai peraturan aplikasi baharu yang dibuat** (dimatikan, secara lalai) – Memaklumkan anda mengenai pembuatan automatik bagi peraturan [Firewall](#) untuk aplikasi baru berdasarkan pada senarai selamat.
- **Paparkan pemberitahuan dulang sistem [Pengimbas E-mel](#)** (dihidupkan, secara lalai) – Tentukan sama ada maklumat dengan mengimbas semua mesej e-mel masuk dan keluar perlu dipaparkan.
- **Paparkan pemberitahuan statistik** (dihidupkan, secara lalai) - Memastikan opsiyen ditanda untuk membenarkan pemberitahuan semakan semula statistik untuk dipaparkan dalam dulang sistem.
- **Paparkan pemberitahuan dulang mengenai [Peningkat AVG](#)** (dihidupkan, secara lalai) - Tentukan sama ada maklumat dengan aktiviti [Peningkat AVG](#) perlu dipaparkan. Perkhidmatan [Peningkat AVG](#) yang membenarkan main balik video dalam talian yang lebih lancar dan membuatkan muat turun tambahan lebih mudah.
- **Paparkan pemberitahuan prestasi [Nasihat AVG](#)** (dihidupkan, secara lalai) - [Nasihat AVG](#) memerhatikan penyemak imbas Internet yang disokong prestasi (*Internet Explorer, Chrome, Firefox, Opera dan Safari*) dan akan memaklumkan anda sekiranya, penyemak imbas anda terlebih guna amaun memori yang disyorkan. Dalam situasi seperti itu, prestasi komputer anda mungkin dilambatkan secara signifikan, dan adalah dinasihatkan untuk memulakan semula penyemak imbas Internet anda untuk mempercepatkan proses. Biarkan item **Paparkan pemberitahuan prestasi [Nasihat AVG](#)** dihidupkan untuk dimaklumkan.

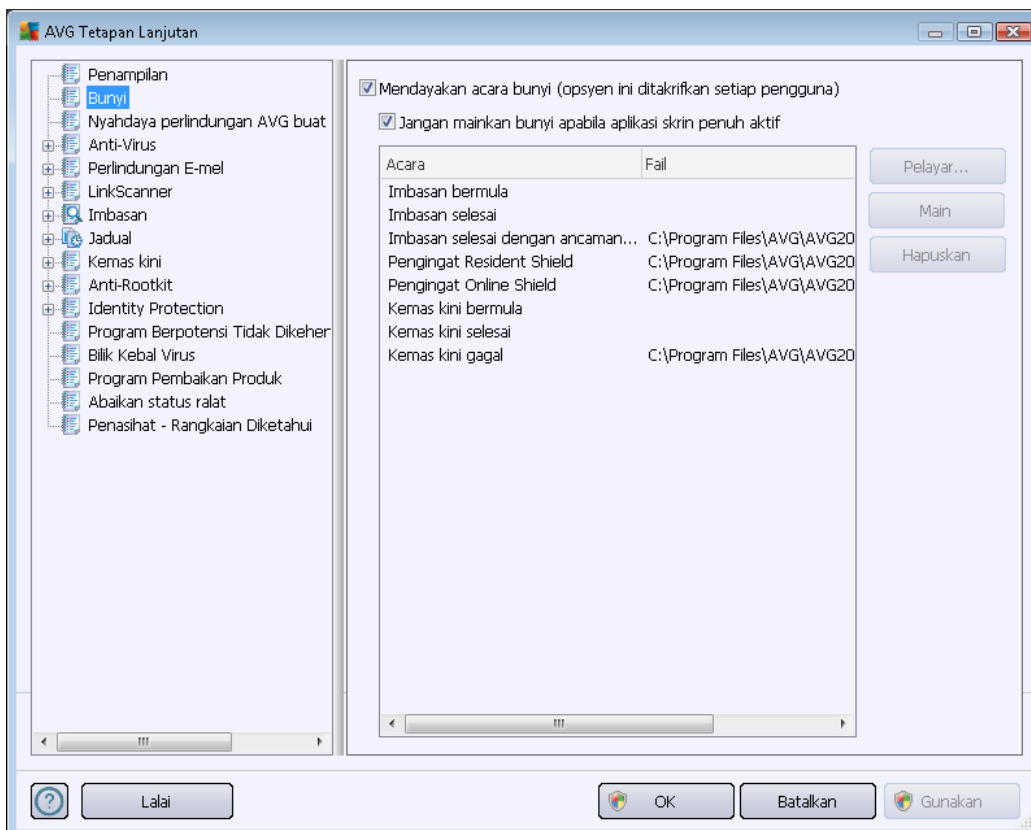


## Mod permainan

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

## 10.2. Bunyi

Dalam dialog **Bunyi** anda boleh menentukan sama ada anda ingin dimaklumkan mengenai tindakan **AVG Internet Security 2012** khusus melalui pemberitahuan bunyi:





Tetapan hanya sah bagi akaun pengguna semasa. Ia bermaksud, setiap pengguna pada komputer boleh mempunyai tetapan bunyi mereka sendiri. Jika anda ingin membenarkan pemberitahuan bunyi, pastikan opsiyen **Dayakan peristiwa bunyi** ditanda (*opsyen dihidupkan, secara lalai*) untuk mengaktifkan senarai bagi semua tindakan yang berkaitan. Seterusnya, anda mungkin ingin menanda opsiyen **Jangan mainkan bunyi apabila aplikasi skrin penuh aktif** untuk menindas pemberitahuan bunyi dalam situasi apabila ia mungkin mengganggu (*lihat juga seksyen mod Permainan bagi bab [Tetapan Lanjutan/Rupa](#) dalam dokumen ini*).

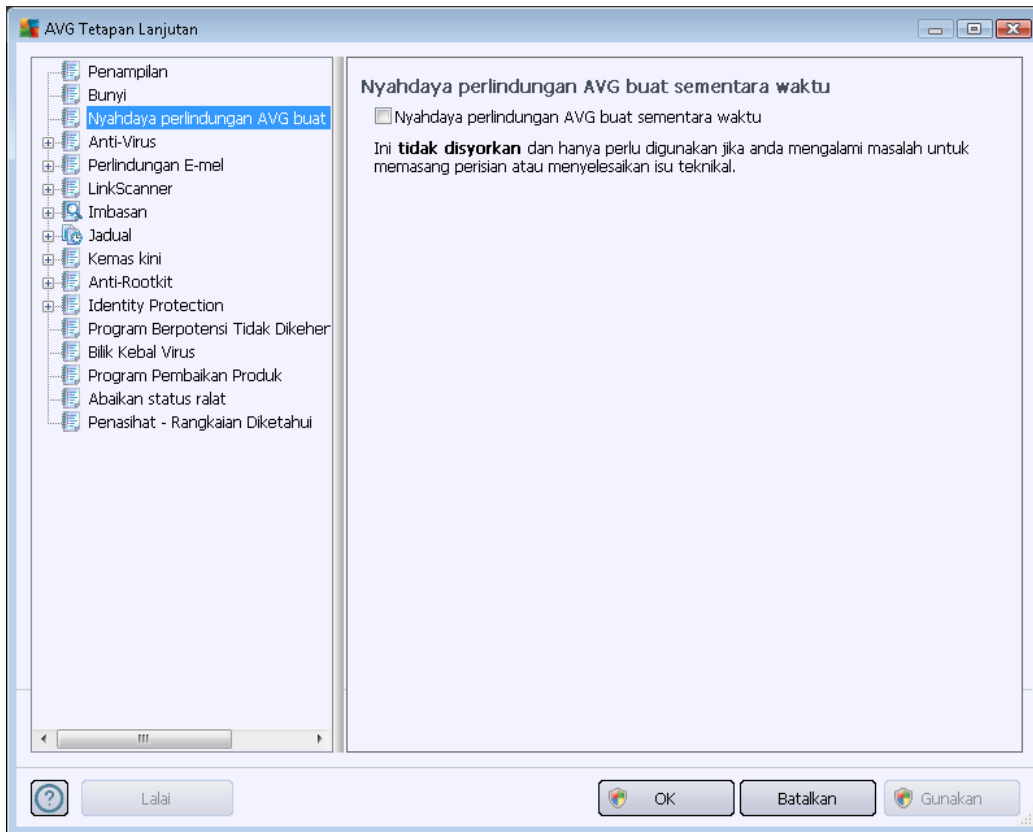
### Butang kawalan

- **Semak Imbas** – Memilih peristiwa masing-masing dari senarai, gunakan butang **Semak Imbas** untuk mencari cakera anda untuk fail bunyi yang dikehendaki yang anda ingin peruntukkan. (*Sila maklum bahawa hanya bunyi \*.wav disokong buat masa itu!*)
- **Main** – Untuk mendengar bunyi yang dipilih, serlahkan peristiwa dalam senarai dan tekan butang **Main**.
- **Padam** – Gunakan butang **Padam** untuk membuang bunyi yang diperuntukkan kepada peristiwa tertentu.

### 10.3. Menyahdayakan perlindungan AVG buat sementara waktu

Dalam dialog **Menyahdayakan perlindungan AVG buat sementara waktu** anda mempunyai pilihan untuk mematikan keseluruhan perlindungan yang dikawal oleh **AVG Internet Security 2012** anda sekali gus.

***Jangan lupa bahawa anda tidak seharusnya menggunakan opsiyen ini melainkan ia adalah benar-benar perlu!***

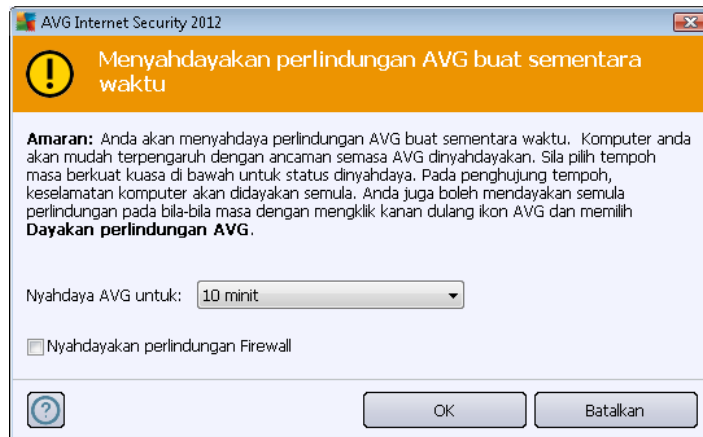


Dalam kebanyakan kes, adalah **tidak perlu** menyahdayakan **AVG Internet Security 2012** sebelum memasang perisian atau pemacu baharu, walaupun jika pemasang atau wizard perisian mencadangkan bahawa atur cara dan aplikasi yang dijalankan dimatikan dahulu untuk memastikan tiada gangguan yang tidak dikehendaki sewaktu proses pemasangan. Sekiranya anda benar-benar menghadapi masalah semasa pemasangan, cuba [menyahaktifkan perlindungan residen](#) (*Dayakan Resident Shield*) terlebih dahulu. Jika anda tidak mempunyai **AVG Internet Security 2012** yang dinyahdaya buat sementara waktu, anda hendaklah mendayakannya semula sebaik sahaja anda selesai. Jika anda bersambung ke Internet atau rangkaian semasa perisian antivirus anda dinyahdayakan, komputer anda terdedah kepada serangan.

### Bagaimana cara menyahdaya perlindungan AVG

- Tandakan kotak semakan **Nyahdaya perlindungan AVG buat sementara waktu**, dan sahkan pilihan anda dengan menekan butang **Guna**
- Dalam dialog **Nyahdaya perlindungan AVG buat sementara waktu** menentukan berapa lama anda ingin menyahdaya **AVG Internet Security 2012** anda. Secara lalai, perlindungan akan dimatikan selama 10 minit yang mencukupi untuk sebarang tugas umum seperti memasang perisian baharu dll. Sila maklum bahawa had masa permulaan yang berkemungkinan boleh ditetapkan ialah 15 minit, dan tidak boleh diganti mengikut nilai anda sendiri atas sebab keselamatan. Selepas tempoh masa yang ditentukan, semua komponen yang dinyahaktifkan akan diaktifkan semula secara automatik.



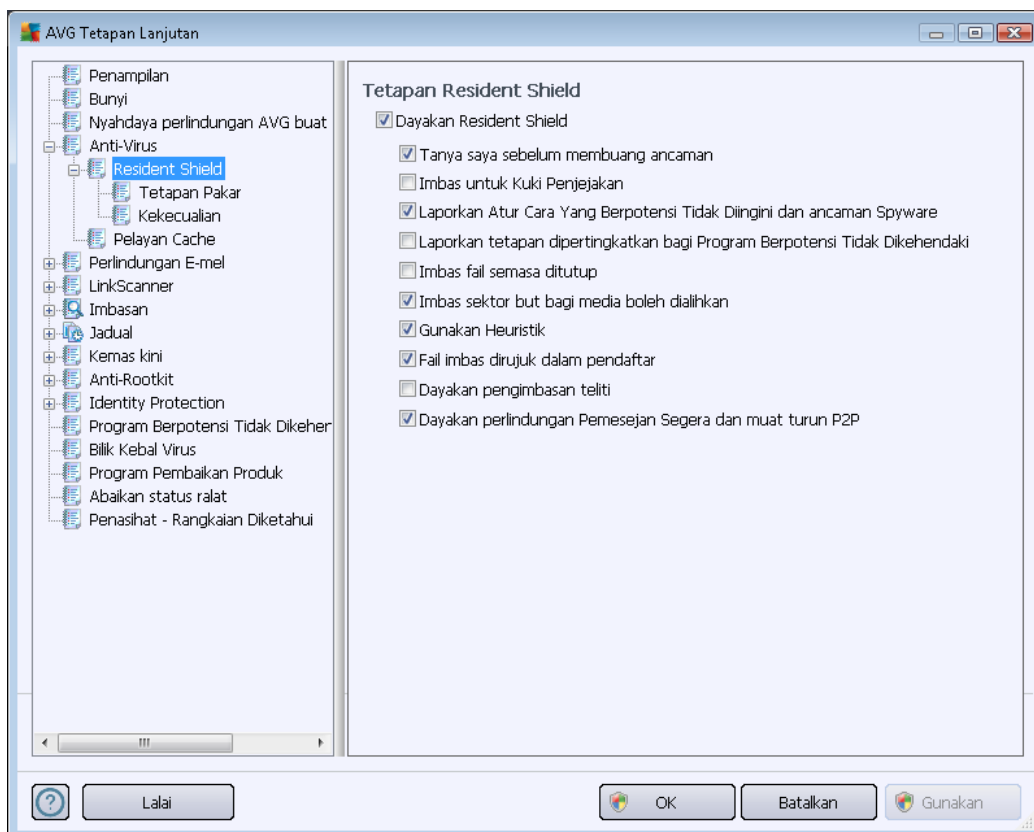


#### 10.4. AntiVirus

Komponen **AntiVirus** melindungi komputer anda secara berterusan dari semua jenis virus dan perisian pengintip yang diketahui (*termasuk yang dipanggil malware tidur dan tidak aktif, iaitu malware yang telah dimuat turun tetapi belum diaktifkan*).

### 10.4.1. Resident Shield

Resident Shield memberikan perlindungan langsung bagi fail dan folder daripada virus, perisian pengintip dan malware lain.



Dalam dialog **Tetapan Resident Shield** anda boleh mengaktifkan atau menyahaktifkan perlindungan Resident Shield sepenuhnya dengan menanda atau tidak menanda item **Dayakan Resident Shield** (*opsyen ini dihidupkan secara lalai*). Selain daripada itu, anda boleh memilih ciri bagi perlindungan residen yang perlu diaktifkan:

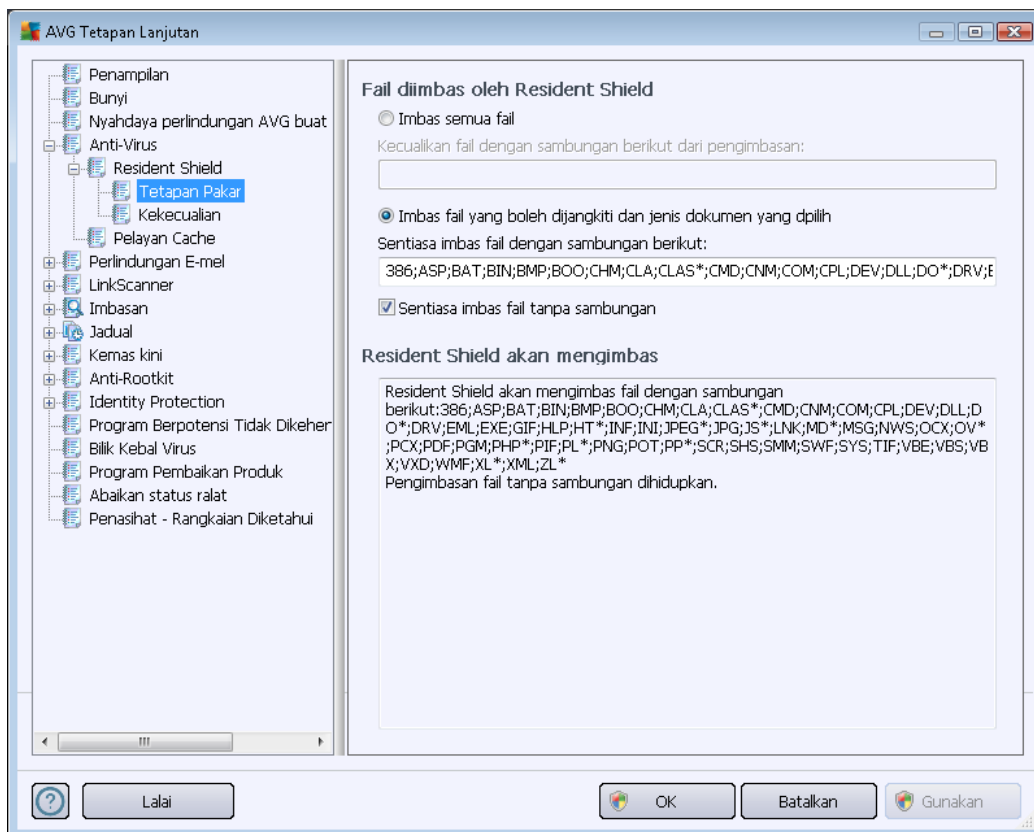
- **Tanya saya sebelum mengalih keluar ancaman** (*dihidupkan secara lalai*) – Tandakan untuk memastikan bahawa Resident Shield tidak akan melaksanakan sebarang tindakan secara automatik; sebagai ganti ia akan memaparkan dialog yang menerangkan ancaman yang dikesan, membolehkan anda memutuskan apa yang harus dilakukan. Jika anda membiarkan kotak tidak ditandakan, **AVG Internet Security 2012** akan memulihkan jangkitan secara automatik dan jika tidak dapat dipulihkan, objek itu akan dialihkan ke dalam [Bilik Kebal Virus](#).
- **Imbas untuk Kuki penjejakan** (*dimatikan secara lalai*) – Parameter ini menentukan bahawa kuki harus dikesan sewaktu pengimbasan. (*Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik.*)
- **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip** (*dibuka secara lalai*) – tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan



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

- **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki (dimatikan secara lalai)** – Tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat sesuai dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas fail semasa tutup (dimatikan secara lalai)** – 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 sophisticated.
- **Imbas sektor but bagi media boleh ditanggalkan (dibuka secara lalai)**
- **Gunakan Heuristik (dihidupkan secara lalai)** – [analisis heuristik](#) akan digunakan untuk pengesanan (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*).
- **Imbas fail yang dirujuk dalam pendaftar (dihidupkan secara lalai)** – Parameter ini mentakrifkan bahawa AVG akan mengimbas semua fail boleh laku yang ditambah ke pendaftar permulaan untuk mengelakkan jangkitan yang diketahui dilakukan pada permulaan komputer yang seterusnya.
- **Dayakan pengimbasan teliti (dimatikan secara lalai)** - dalam situasi khusus (*dalam keadaan kecemasan ekstrem*) anda boleh menandakan opsi ini untuk mengaktifkan algoritma yang paling teliti yang akan memeriksa semua objek yang berkemungkinan mengancam di bahagian dalam. Namun ingat bahawa kaedah ini agak mengambil masa.
- **Dayakan perlindungan Pemesejan Segera dan perlindungan muat turun P2P (dihidupkan secara lalai)** - Tandakan item ini jika anda ingin mengesahkan bahawa komunikasi pemesejan segera (*cth. ICQ, MSN Messenger, ...*) dan muat turun P2P bebas virus.

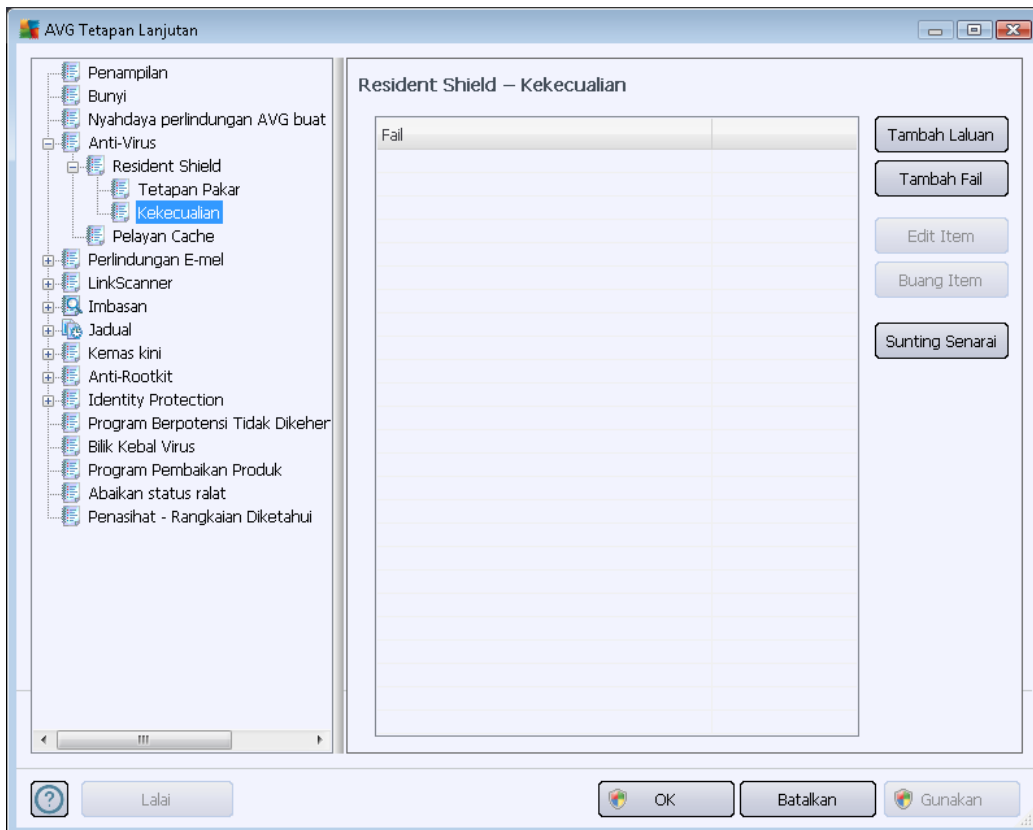
Dalam dialog **Fail yang diimbas oleh Resident Shield** dialog anda boleh mengkonfigurasi fail mana yang akan diimbas (oleh sambungan tertentu):



Tandakan kotak semakan masing-masing untuk memutuskan sama ada anda hendak **Imbas semua fail** atau **Imbas fail yang boleh dijangkiti dan jenis dokumen yang dipilih** sahaja. Jika anda memutuskan untuk opsi yang kedua, anda boleh seterusnya menentukan senarai sambungan yang menentukan fail yang perlu dikecualikan dari pengimbasan, dan juga senarai sambungan fail yang menentukan fail yang perlu diimbas di dalam semua keadaan.

Tandakan **Sentiasa imbas fail tanpa sambungan (dihidupkan secara lalai)** untuk memastikan bahawa fail yang tanpa sambungan dan dalam format tidak diketahui akan diimbas oleh Resident Shield. Kami mengesyorkan untuk membiarkan ciri ini dihidupkan, memandangkan fail tanpa sambungan adalah mencurigakan.

Seksyen di bawah yang dinamakan **Resident Shield akan mengimbas** meringkaskan lagi tetapan semasa, memaparkan gambaran keseluruhan terperinci tentang apa yang akan diimbas oleh **Resident Shield** sebenarnya.



Dialog **Resident Shield – Dialog yang dikecualikan** menawarkan kemungkinan mentakrifkan fail dan/atau folder yang harus dikecualikan dari pengimbasan **Resident Shield**.

***Jika ini tidak penting, kami sangat mengesyorkan untuk tidak mengecualikan sebarang item!***

### Butang kawalan

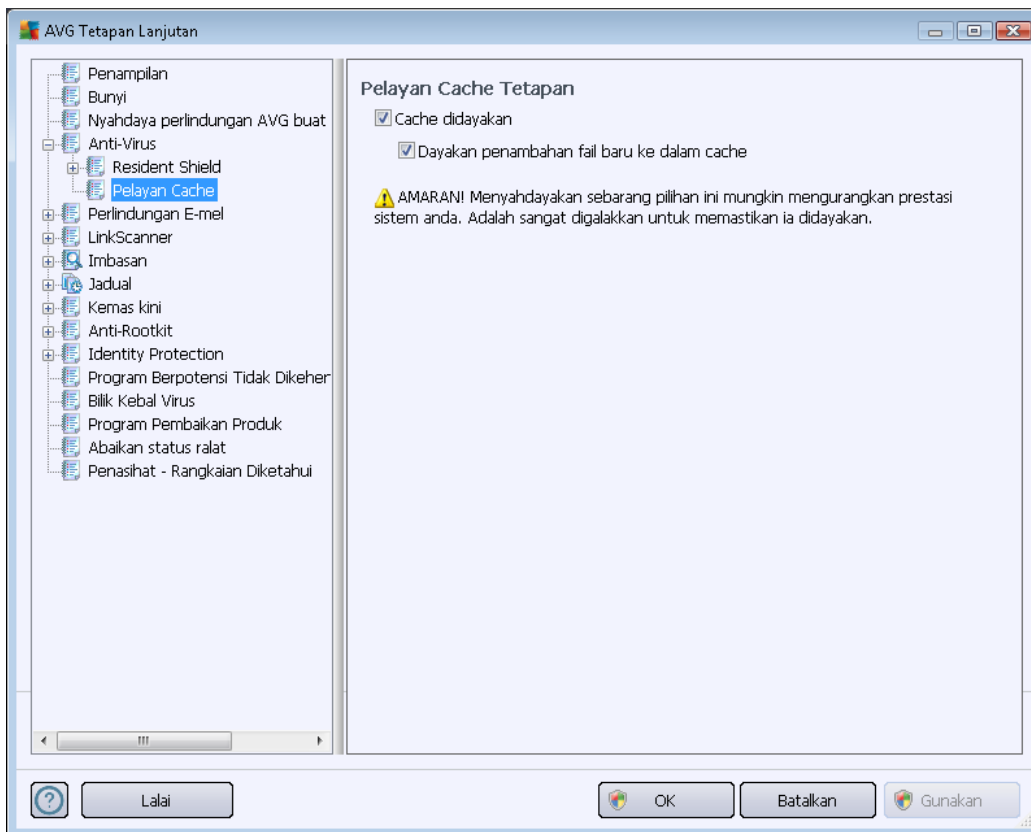
Dialog menyediakan butang kawalan berikut:

- **Tambah Laluan** – tentukan direktori untuk dikecualikan daripada imbasan dengan memilihnya satu persatu dari pohon navigasi cakera tempatan
- **Tambah Fail** – tentukan fail untuk dikecualikan daripada pengimbasan dengan memilihnya satu persatu daripada pohon navigasi cakera tempatan
- **Edit Item** – membenarkan anda mengedit laluan yang ditentukan kepada fail atau folder yang dipilih
- **Buang Item** – membenarkan anda memadam laluan ke item yang dipilih daripada senarai
- **Edit Senarai** – membenarkan anda mengedit seluruh senarai pengecualian yang ditakrifkan

dalam dialog baru yang berkelakuan seperti editor teks standard

### 10.4.2. Pelayan Cache

Dialog **Tetapan Pelayan Cache** merujuk kepada proses pelayan cache yang direka bentuk untuk mempercepatkan semua jenis imbasan **AVG Internet Security 2012**:



Pelayan cache mengumpul dan menyimpan maklumat bagi fail yang dipercayai (*fail dikira dipercayai jika ditandatangani dengan tandatangan digital bagi sumber yang dipercayai*). Fail-fail ini kemudiannya, secara automatik, dikira selamat, dan tidak perlu diimbas semula; oleh sebab itu, fail-fail ini dilangkau sewaktu pengimbasan.

Dialog **Tetapan Pelayan Cache** menawarkan opsiyen konfigurasi berikut:

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



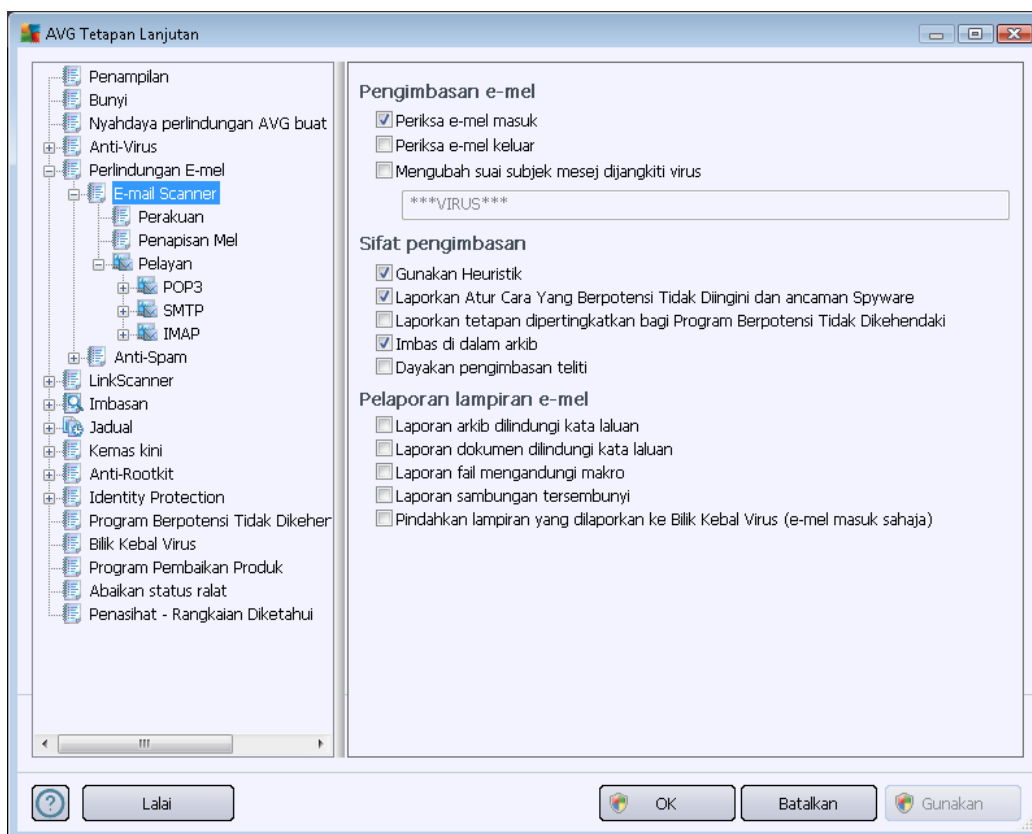
**Melainkan anda mempunyai sebab yang baik untuk mematikan pelayan cache, kami amat mengesyorkan anda menyimpan tetapan lalai dan membiarkan kedua-dua opsyen dihidupkan! Jika tidak, anda mungkin mengalami pengurangan ketara bagi kelajuan dan prestasi sistem anda.**

## 10.5. Perlindungan e-mel

Dalam seksyen **Perlindungan e-mel** anda boleh mengedit konfigurasi terperinci bagi [Pengimbas E-mel](#) dan [AntiSpam](#):

### 10.5.1. Pengimbas E-mel

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



### Pengimbasan e-mel

Dalam bahagian ini, anda boleh menetapkan asas ini untuk mesej e-mel masuk dan/atau keluar:

- **Semak e-mel masuk** (*buka secara lalai*) – tanda untuk buka/tutup opsyen bagi mengimbas semua mesej e-mel yang dihantar ke klien e-mel anda
- **Semak e-mel keluar** (*tutup secara lalai*) – tanda untuk buka/tutup opsyen bagi mengimbas semua mesej e-mel yang dihantar dari klien e-mel anda
- **Ubah suai subjek mesej dijangkiti virus** (*tutup secara lalai*) – jika anda ingin diberi



amaran mesej e-mel yang diimbis dikesan sebagai boleh berjangkit, tandakan item ini dan isikan teks yang diinginkan ke dalam medan teks. Teks ini kemudiannya akan ditambahkan ke medan "Subjek" setiap mesej e-mel yang dikesan untuk pengenalan dan penapisan yang lebih mudah. Nilai lalai ialah **\*\*\*VIRUS\*\*\*** yang kami syorkan untuk disimpan.

### Sifat pengimbasan

Dalam bahagian ini, anda boleh menentukan cara mesej e-mel akan diimbis:

- **Gunakan Heuristik (buka secara lalai)** – tandakan untuk menggunakan kaedah pengesanan heuristik semasa mengimbas mesej e-mel. Apabila opsi ini hidup, anda boleh menapis lampiran e-mel bukan sahaja dengan sambungan tetapi juga kandungan sebenar lampiran boleh dipertimbangkan. Penapisan boleh ditetapkan dalam dialog [Penapisan Mel](#).
- **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip (dibuka secara lalai)** – tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip](#) mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini (tutup secara lalai)** – tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas dalam arkib (buka secara lalai)** – tandakan untuk mengimbas kandungan arkib yang dilampirkan kepada mesej e-mel.
- **Dayakan pengimbasan menyeluruh (tutup secara lalai)** – dalam situasi khusus (*cth. syak komputer anda dijangkiti oleh virus atau eksploitasi*) anda boleh menandakan opsi ini untuk mengaktifkan algoritma pengimbasan menyeluruh yang akan turut mengimbas kawasan komputer anda yang sukar untuk dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.

### Pelaporan lampiran e-mel

Dalam seksyen ini, anda boleh menetapkan laporan tambahan mengenai fail yang berpotensi berbahaya atau mencurigakan. Sila maklum bahawa tiada dialog amaran yang akan dipaparkan, hanya teks perakuan akan ditambah ke penghujung mesej e-mel, dan semua laporan seumpamanya akan disenaraikan dalam dialog [pengesanan Pengimbas E-mel](#):

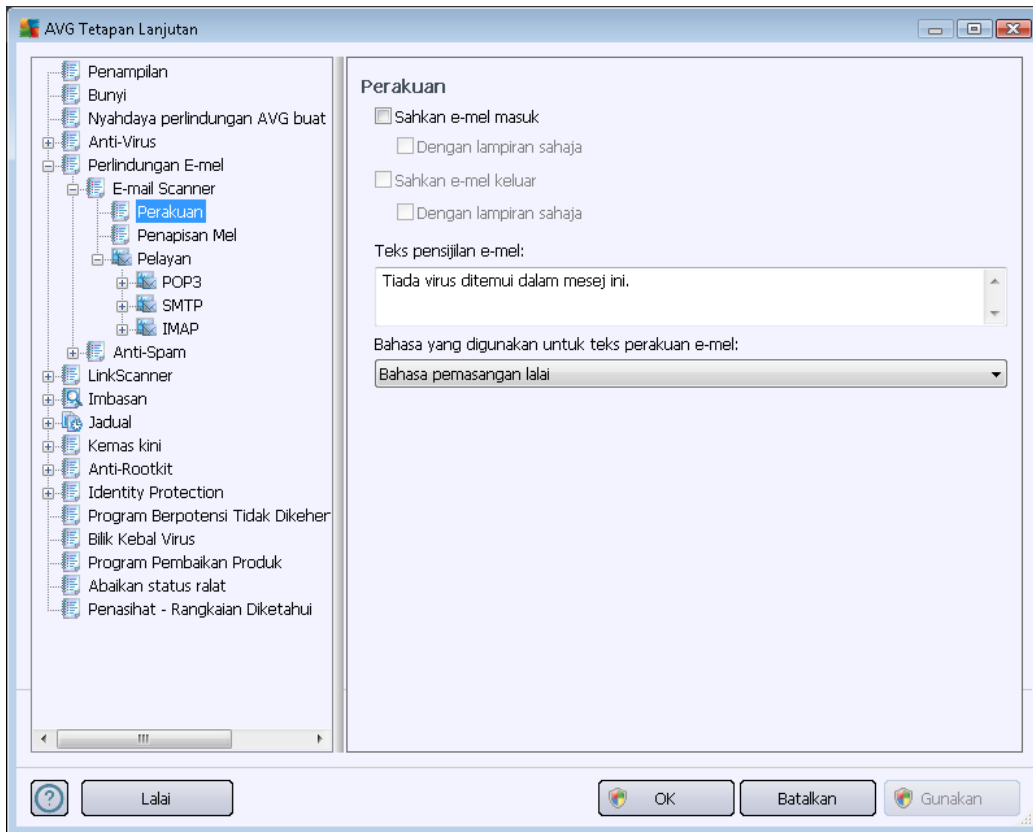
- **Laporkan arkib yang dilindungi kata laluan** – arkib (*ZIP, RAR dll.*) yang dilindungi oleh kata laluan adalah tidak mungkin diimbis untuk virus; tandakan kotak untuk melaporkan ini sebagai berpotensi berbahaya.





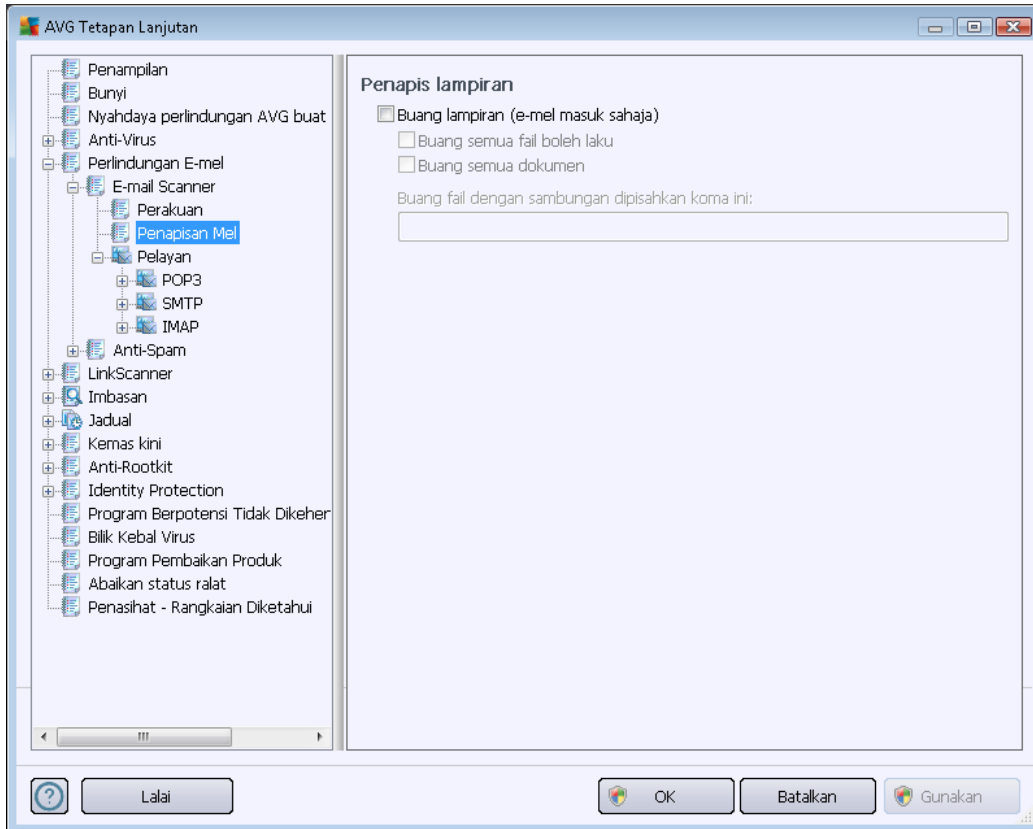
- **Laporkan dokumen yang dilindungi kata laluan** – dokumen dilindungi kata laluan tidak mungkin diimbis untuk virus; tandakan kotak untuk melaporkannya sebagai berpotensi berbahaya.
- **Laporkan fail mengandungi makro** – makro adalah urutan langkah yang dipraktikkan untuk menjadikan tugas tertentu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

Dalam dialog **Perakuan** anda boleh menanda kotak semakan tertentu untuk memutuskan sama ada anda hendak mengakui mel masuk anda (**Akui e-mel masuk**) dan/atau mel keluar (**Akui e-mel keluar**). Untuk setiap opsyen ini, anda boleh seterusnya, menentukan parameter **Dengan lampiran sahaja** supaya perakuan hanya ditambah pada mesej mel dengan lampiran:



Secara lalai, teks perakuan terdiri daripada hanya maklumat asas yang menyatakan *Tiada virus yang ditemui dalam mesej ini*. Walau bagaimanapun, maklumat ini boleh dilanjutkan atau ditukar mengikut keperluan anda: tulis teks perakuan yang dikehendaki ke dalam medan **Teks perakuan e-mel**. Dalam seksyen **Bahasa yang digunakan untuk teks perakuan e-mel** yang anda boleh seterusnya, mentakrifkan dalam bahasa apa bahagian perakuan yang dijana secara automatik (*Tiada virus yang ditemui dalam mesej ini*) perlu dipaparkan.

**Nota: Sila ingat bahawa hanya teks lalai akan dipaparkan dalam bahasa yang diminta, dan teks tersuai anda tidak akan diterjemah secara automatik!**



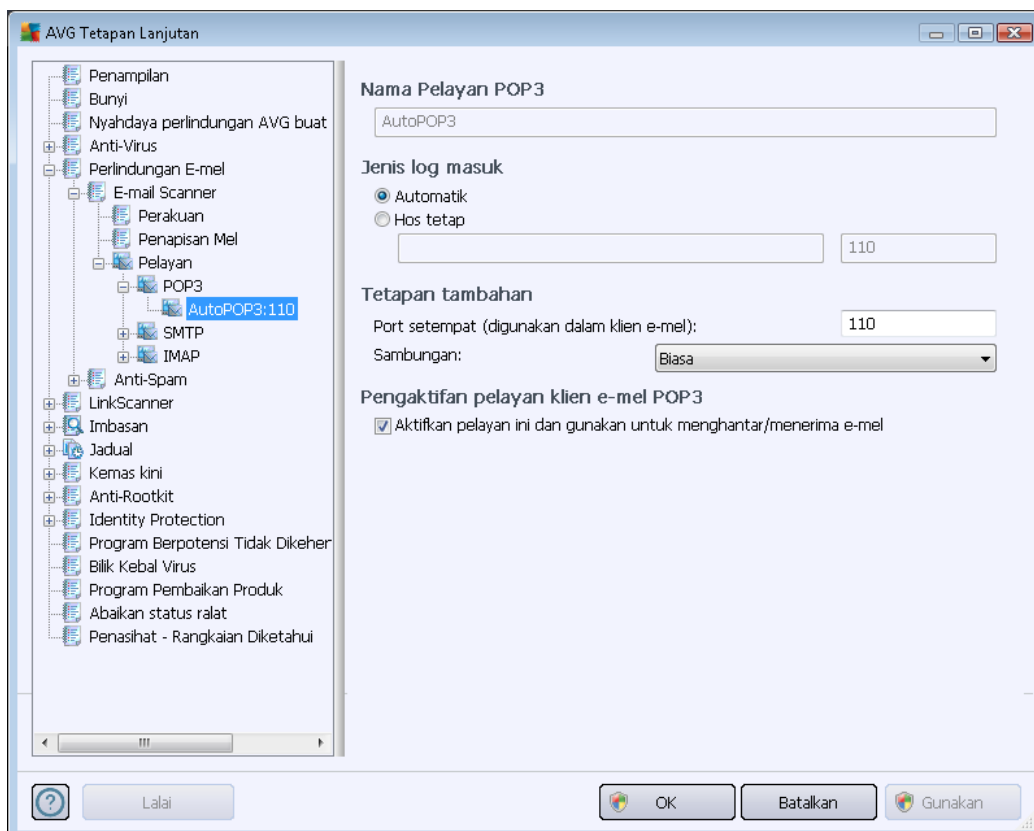
Dialog **Penapis lampiran** membenarkan anda menyediakan parameter untuk pengimbasan lampiran mesej e-mel. Secara lalainya, opsiyen **Buang lampiran** dimatikan. Jika anda memutuskan untuk mengaktifkannya, semua lampiran mesej e-mel yang dikesan sebagai berjangkit atau berpotensi berbahaya akan dibuang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

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

Dalam seksyen **Pelayan** anda boleh mengedit parameter bagi pelayan [Pengimbas E-mel](#):

- [Pelayan POP3](#)
- [Pelayan SMTP](#)
- [Pelayan IMAP](#)

Serta, anda boleh menentukan pelayan baru untuk mel masuk atau keluar, menggunakan butang **Tambah pelayan baharu**.

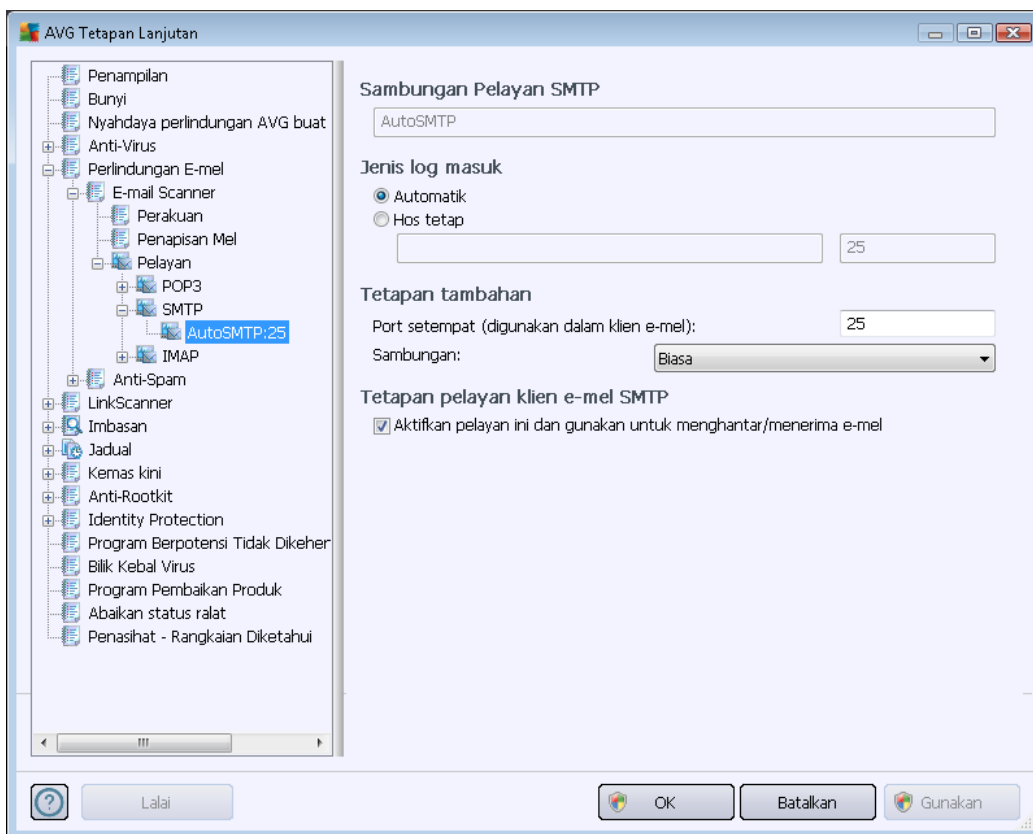


Dalam dialog ini (*dibuka melalui **Pelayan / POP3***) anda boleh menyediakan pelayan [Pengimbas E-mel](#) baharu menggunakan protokol POP3 untuk mel masuk:

- **Nama Pelayan POP3** – dalam medan ini anda boleh menentukan nama pelayan yang baru ditambah (*untuk menambah pelayan POP3, klik butang tetikus kanan di atas item POP3 di sebelah kiri menu navigasi*). Bagi pelayan "AutoPOP3" yang dibuat secara automatik medan ini dinyahaktifkan.
- **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.
  - **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.

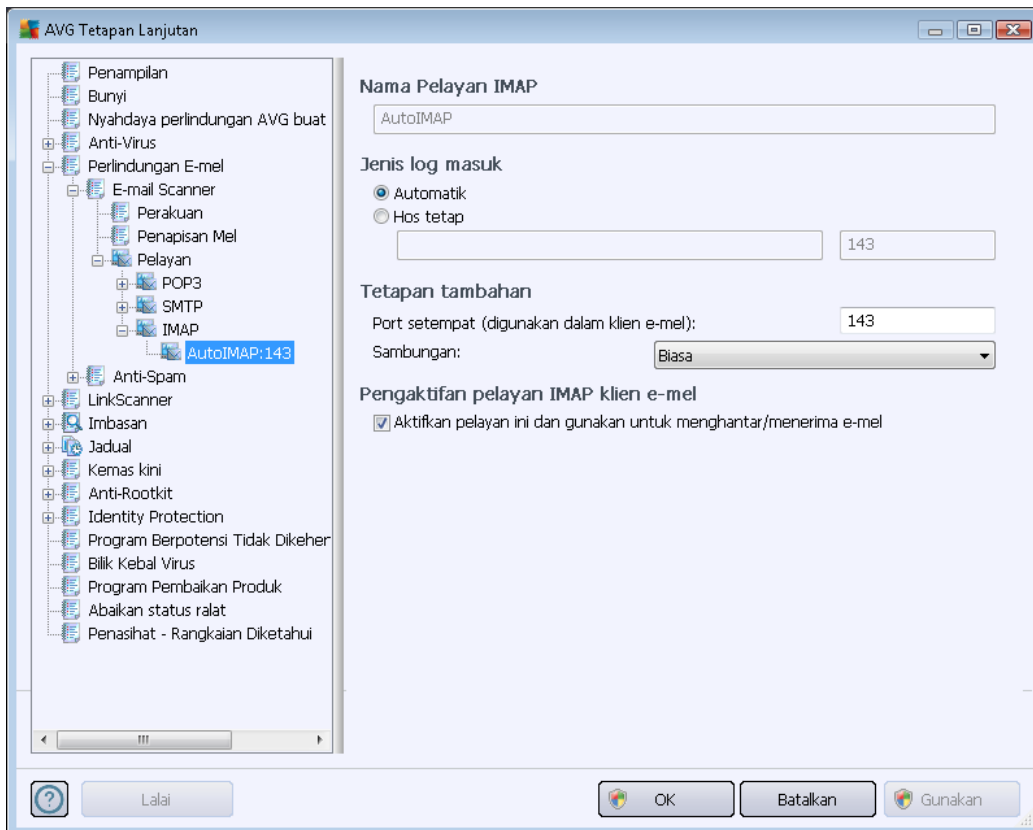
- **Tetapan tambahan** – menentukan parameter yang lebih terperinci:
  - **Port tempatan** – menentukan port di mana komunikasi dari aplikasi mel anda harus dijangka. Anda kemudiannya mesti menentukan dalam aplikasi mel anda port ini sebagai port untuk komunikasi POP3.
  - **Sambungan** – dalam menu 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** - tanda/buang tanda item ini untuk mengaktifkan atau menyahaktifkan pelayan POP3 yang ditentukan



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

- **Nama Pelayan SMTP** – dalam medan ini anda boleh menentukan nama pelayan yang baru ditambah (*untuk menambah pelayan SMTP, klik butang tetikus kanan di atas item SMTP di sebelah kiri menu navigasi*). Untuk pelayan "AutoSMTP" yang dibuat secara automatik medan ini dinyahaktifkan.

- **Jenis log masuk** - 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 penyemak imbas yang ditentukan di sini. Sila nyatakan alamat atau nama pelayan mel anda. Anda boleh menggunakan nama domain (sebagai contoh, smtp.acme.com) dan juga alamat IP (sebagai contoh, 123.45.67.89) sebagai nama. Jika pelayan mel menggunakan port tidak standard, anda boleh menaip port ini di belakang nama pelayan menggunakan noktah bertindih sebagai penentu hadnya (sebagai contoh, smtp.acme.com:8200). Port standard untuk komunikasi SMTP ialah 25.
- **Tetapan tambahan** – menentukan parameter yang lebih terperinci:
  - **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.
  - **Sambungan** – dalam menu jatuh ke 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 diselia oleh pihak ketiga. Ciri ini tersedia hanya apabila pelayan mel destinasi menyokongnya.
- **Pengaktifan pelayan SMTP klien e-mel** – tandakan/jangan tandakan kotak ini untuk mengaktifkan/menyahaktifkan pelayan SMTP yang ditentukan di atas



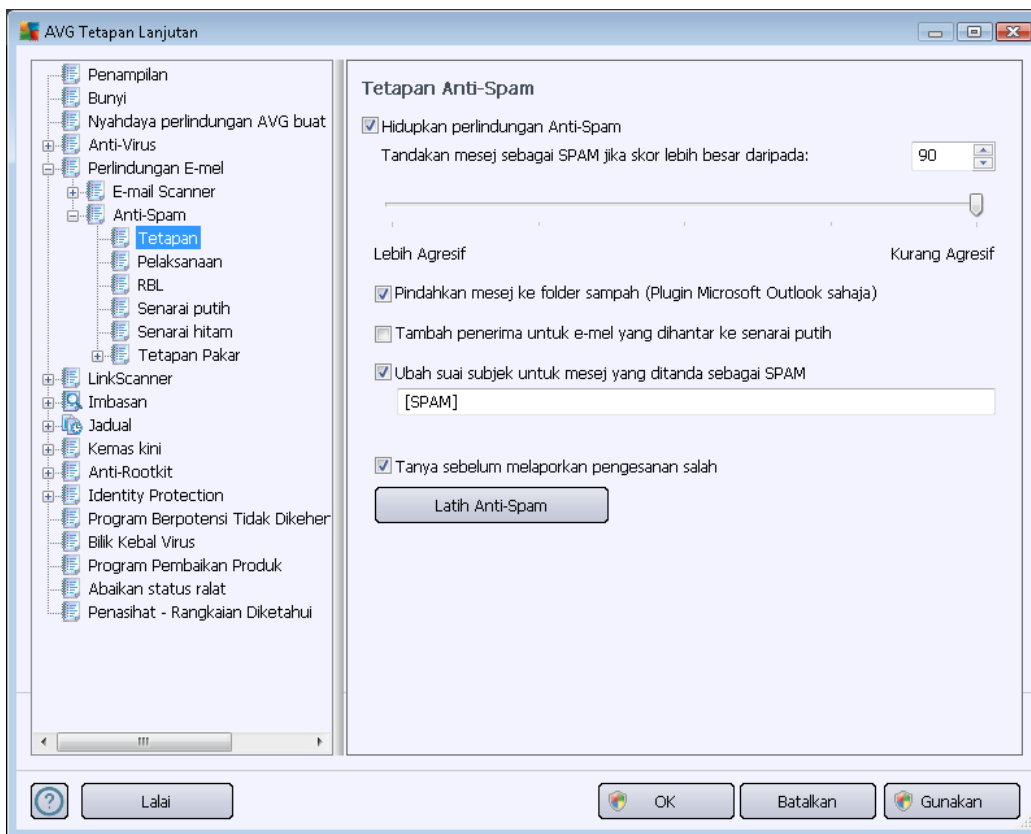
Dalam dialog ini (dibuka melalui **Pelayan / IMAP**) anda boleh menetapkan pelayan [Pengimbas E-mel](#) menggunakan protokol IMAP untuk mel keluar:

- **Nama Pelayan IMAP** – dalam medan ini anda boleh menentukan nama pelayan yang baru ditambah (*untuk menambah pelayan IMAP, klik butang tetikus kanan di atas item IMAP bagi menu navigasi kiri*). Bagi pelayan "AutoIMAP" yang dibuat secara automatik medan ini dinyahaktifkan.
- **Jenis log masuk** - 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 penyemak imbas 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 pengehad (*sebagai contoh, imap.acme.com:8200*). Port standard untuk komunikasi IMAP ialah 143.
- **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 IMAP.
  - **Sambungan** – dalam menu jatuh ke 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 diselia oleh pihak ketiga. Ciri ini tersedia hanya apabila pelayan mel destinasi menyokongnya.
- **Pengaktifan pelayan IMAP klien e-mel** – tandakan/jangan tandakan kotak ini untuk mengaktifkan/menyahaktifkan pelayan IMAP yang ditentukan di atas

## 10.5.2. AntiSpam



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

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





nilai atau dengan menggerakkan penggelongsor ke kiri atau kanan (*julat nilai adalah terhad kepada 50-90*).

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

- **Nilai 80-90** – Mesej e-mel berkemungkinan menjadi spam akan ditapis keluar. Sesetengah mesej bukan spam mungkin juga ditapis dengan tidak betul.
- **Nilai 60-79** – Dikira sebagai konfigurasi yang agak agresif. Mesej e-mel yang berkemungkinan spam akan ditapis keluar. Mesej bukan spam juga berkemungkinan ditangkap.
- **Nilai 50-59** – Konfigurasi yang sangat agresif. Mesej e-mel bukan spam berkemungkinan ditangkap sebagai mesej spam sebenar. Julat ambang ini tidak disarankan untuk penggunaan biasa.

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

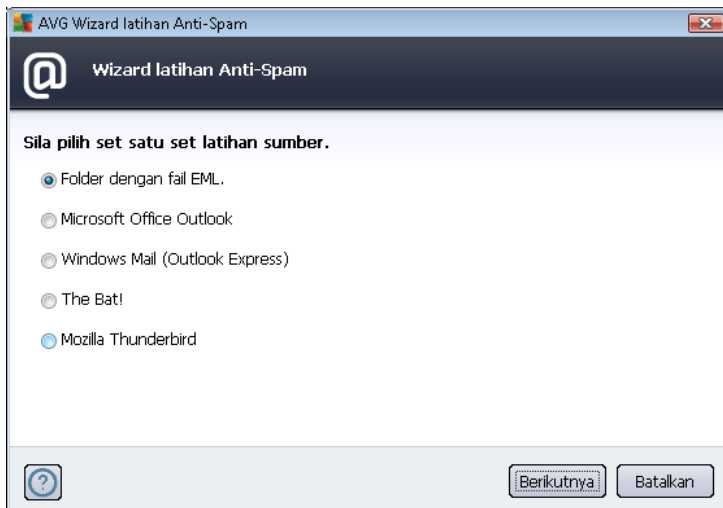
- **Alihkan mesej ke folder sarap** (*pasang masuk Microsoft Outlook sahaja*) - Tandakan kotak semakan ini untuk mentakrifkan bahawa setiap mesej spam yang dikesan harus dialihkan secara automatik ke folder sarap khusus dalam MS Outlook.e-mail client anda. Pada masa ini, ciri ini tidak disokong dalam klien mel lain.
- **Tambah penerima bagi e-mel yang dihantar ke [senarai putih](#)** - Tandakan kotak semakan ini untuk mengesahkan bahawa semua penerima bagi e-mel yang dihantar boleh dipercayai dan semua mesej e-mel yang datang dari akaun e-mel mereka boleh dihantar.
- **Ubah suai subjek untuk mesej yang ditandakan sebagai SPAM** - Tandakan kotak semakan ini jika anda mahu semua mesej yang dikesan sebagai spam ditandakan dengan perkataan atau aksara khusus dalam medan subjek e-mel; teks yang dikehendaki boleh ditaip dalam medan teks yang diaktifkan.
- **Tanya sebelum melaporkan pengesanan yang salah** – Dengan syarat semasa [proses pemasangan](#) anda bersetuju untuk menyertai [Program Pembaikan Produk](#). Jika benar, anda membenarkan pelaporan ancaman yang dikesan kepada AVG. Pelaporan ini dilakukan secara automatik. Walau bagaimanapun, anda boleh menandakan kotak semak ini untuk mengesahkan anda ingin ditanya sebelum sebarang spam yang dikesan dilaporkan kepada AVG untuk memastikan mesej ini benar-benar perlu diklasifikasikan sebagai spam.

## Butang kawalan

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



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



Terdapat opsiyen berikut untuk dipilih:

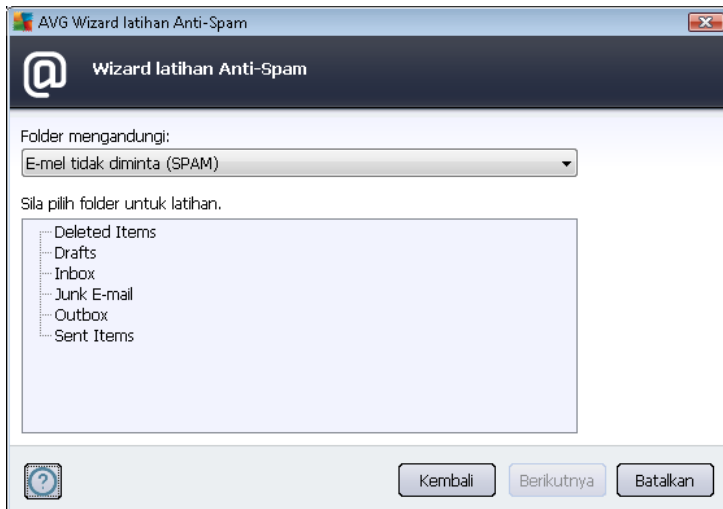
- **Klien e-mel khusus** – jika anda menggunakan salah satu klien e-mel yang disenaraikan ( *MS Outlook, Outlook Express, The Bat!*), hanya pilih opsiyen masing-masing
- **Folder dengan fail EML** – jika anda menggunakan sebarang atur cara e-mel, pertama sekali, anda harus menyimpan mesej ke folder khusus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

Untuk proses latihan yang lebih cepat dan murah, ia merupakan idea yang baik untuk menyusun e-mel dalam folder terlebih dahulu, agar folder yang anda akan gunakan untuk latihan mengandungi hanya mesej latihan (sama ada diingini, atau tidak diingini). Bagaimanapun, itu adalah tidak perlu, memandangkan anda akan boleh menapis e-mel kemudian nanti.

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

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

### **Folder dengan fail EML.**



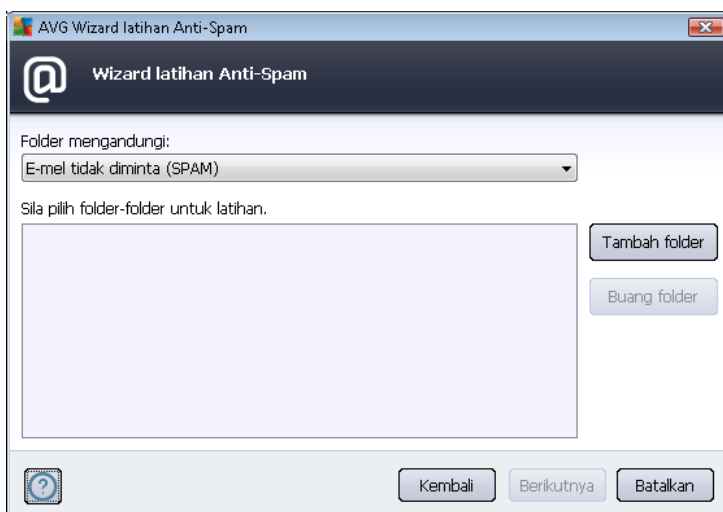
Dalam dialog ini, sila pilih folder dengan mesej yang anda hendak gunakan untuk latihan. Tekan butang **Tambah folder** untuk mencari folder dengan fail .eml (*mesej e-mel yang disimpan*). Folder terpilih akan kemudiannya dipaparkan dalam dialog.

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

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

## Klien e-mel khusus

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

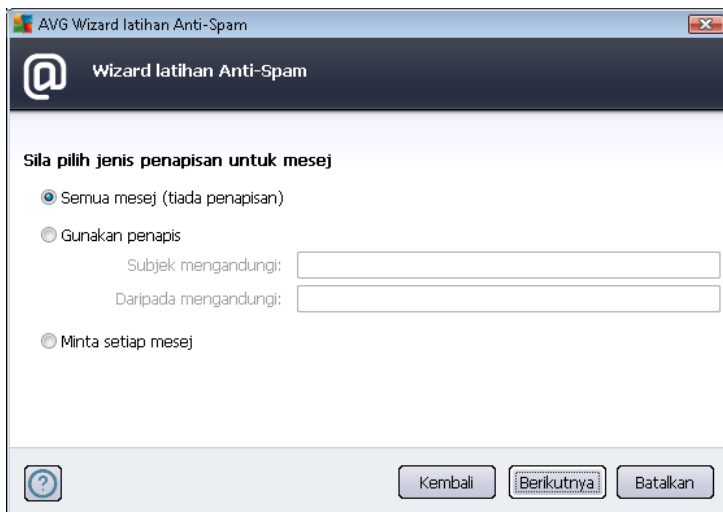




**Nota:** Dalam kes Microsoft Office Outlook, anda akan digesa untuk memilih profil MS Office Outlook dahulu.

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

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



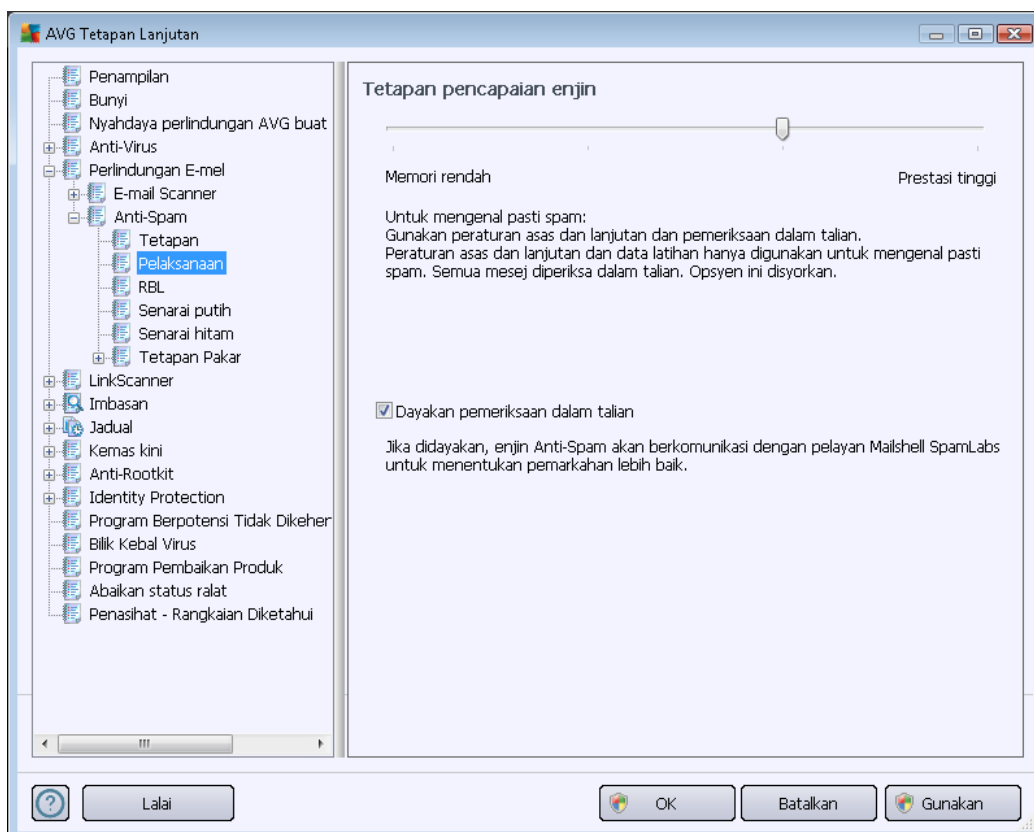
Dalam dialog ini, anda boleh menetapkan penapisan mesej e-mel.

- **Semua mesej (tiada penapisan)** – Jika anda pasti folder terpilih mengandungi cuma mesej yang anda ingin gunakan untuk latihan, pilih opsyen **Semua mesej (tiada penapisan)**.
- **Gunakan penapis** - Untuk penapisan lebih lanjut, pilih opsyen **Gunakan penapis**. Anda boleh mengisikan perkataan (*nama*), sebahagian perkataan atau perenggan untuk dicari dalam subjek e-mel dan/atau medan penghantar. Semua mesej yang sepadan dengan kriteria yang dimasukkan akan digunakan untuk latihan, tanpa penggesaan lanjut. Apabila anda mengisi kedua-dua medan teks, alamat yang sepadan dengan cuma satu dari dua keadaan itu akan digunakan, juga!
- **Tanya untuk setiap mesej** - Jika anda tidak pasti mengenai mesej yang terkandung dalam folder dan anda ingin wizard bertanya kepada anda mengenai setiap mesej (*supaya anda boleh menentukan sama ada untuk menggunakannya untuk latihan atau tidak*), pilih opsyen **Tanya bagi setiap mesej**.

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



Dialog **Tetapan prestasi enjin** (dipautkan melalui item **Prestasi** bagi navigasi kiri) menawarkan tetapan prestasi komponen **AntiSpam**:



Gerakkan gelangsar ke kiri atau kanan untuk menukar julat tahap prestasi pengimbasan di antara mod prestasi **memori Rendah / Tinggi**.

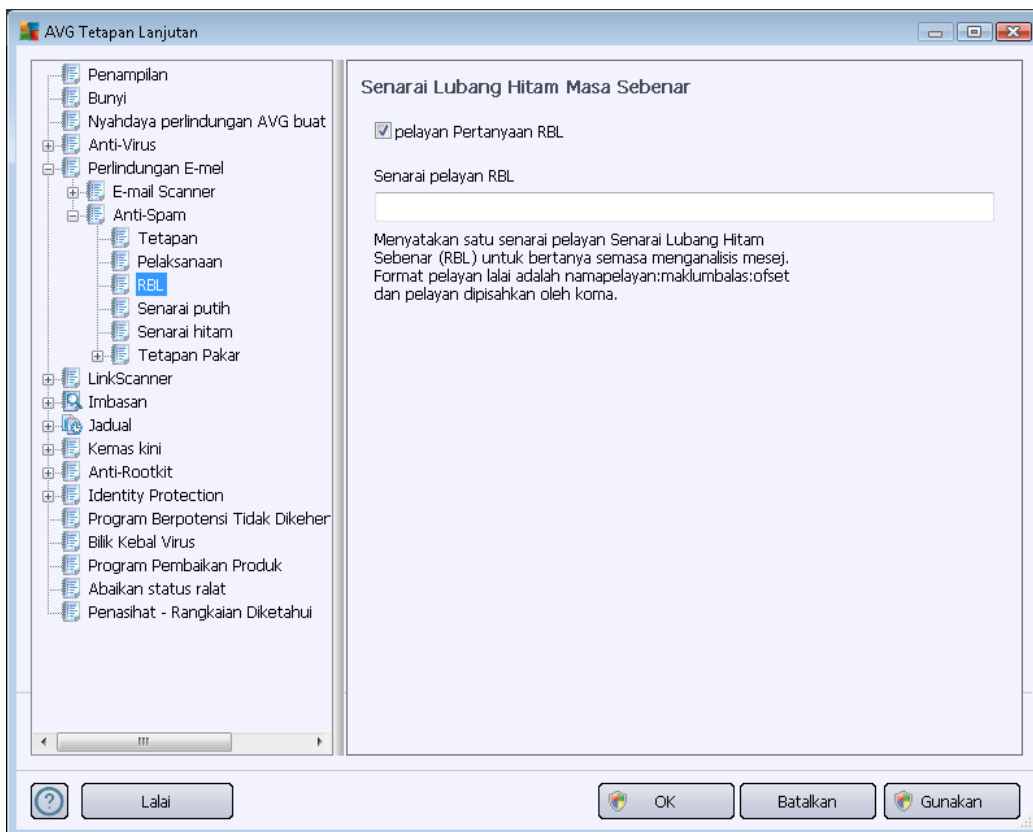
- **Memori rendah** – sewaktu proses pengimbasan untuk mengenal pasti spam, tiada peraturan yang akan digunakan. Hanya data latihan akan digunakan untuk pengenalanpastian. Mod ini tidak disyorkan untuk penggunaan biasa, melainkan perkakas komputer adalah sangat lemah.
- **Prestasi tinggi** - mod ini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

Item **Dayakan semakan dalam talian** dihidupkan secara lalai. Ia memberikan keputusan pengesanan spam yang lebih tepat melalui komunikasi dengan pelayan [Mailshell](#), cth. data yang diimbas akan dibandingkan dengan pangkalan data dalam talian [Mailshell](#).

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



Item **RBL** membuka dialog pengeditan yang dipanggil **Senarai Lubang Hitam Masa Nyata** yang anda boleh hidupkan/matikan fungsi **Tanya pelayan RBL**:

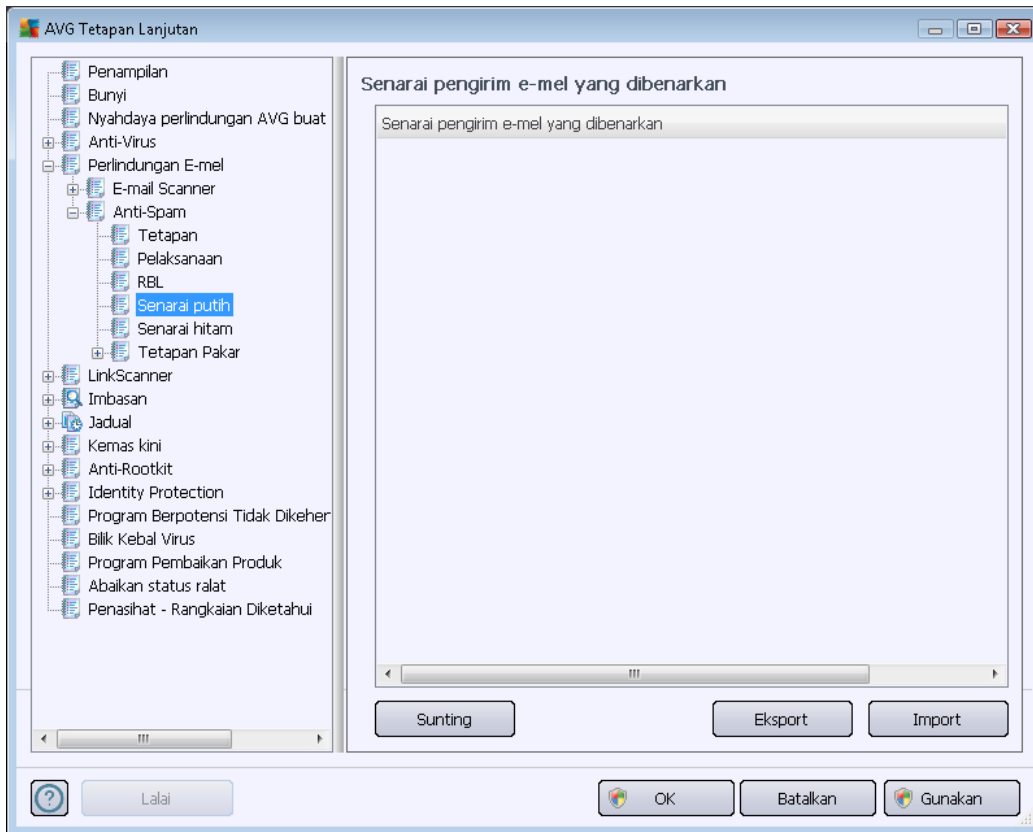


Pelayan RBL (*Senarai Lubang Hitam Masa Sebenar*) pelayan adalah pelayan DNS dengan pangkalan data meluas bagi penghantar spam yang diketahui. Apabila ciri ini dihidupkan, semua mesej e-mel akan disahkan dengan pangkalan data pelayan RBL dan ditanda sebagai spam jika sama dengan sebarang entri pangkalan data. Pangkalan data pelayan RBL mengandungi cap jari spam yang terkini untuk memberikan pengesanan spam yang terbaik dan paling tepat. Ciri ini berguna terutama sekali untuk pengguna yang menerima sejumlah besar spam yang tidak dikesan secara normal oleh enjin [AntiSpam](#).

**Senarai pelayan RBL** membenarkan anda menentukan lokasi pelayan RBL khusus (*sila maklum bahawa dengan mendayakan ciri ini, pada sesetengah sistem dan konfigurasi, melambatkan proses penerimaan e-mel, kerana setiap mesej perlu disahkan dengan pangkalan data pelayan RBL*).

**Tiada data peribadi yang dihantar ke pelayan!**

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



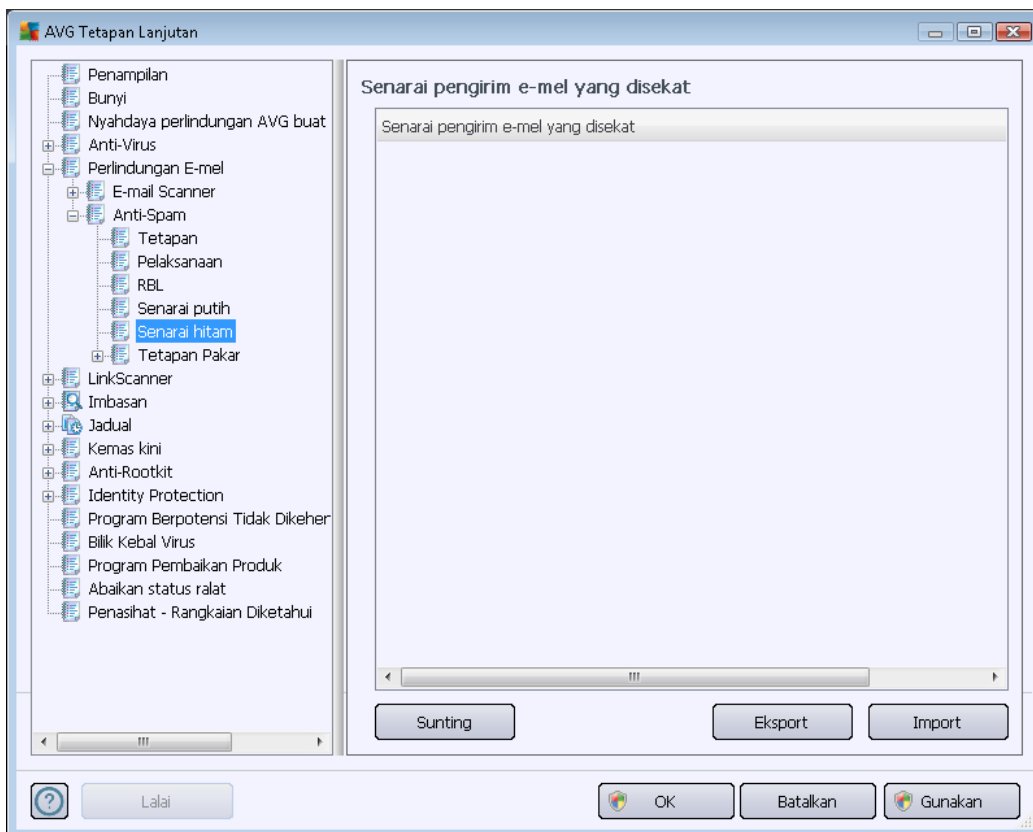
Dalam antara muka pengeditan, anda boleh mengumpulkan senarai penghantar yang anda pasti tidak akan menghantarkan anda mesej yang tidak diingini (spam). Anda juga boleh mengumpulkan senarai nama domain penuh (*cth. avg.com*), yang anda ketahui tidak menjana mesej spam. Sebaik sahaja anda mempunyai senarai penghantar seperti itu dan/atau nama domain disediakan, anda boleh memasukkannya melalui salah satu kaedah berikut: melalui entri terus setiap alamat e-mel atau dengan mengimport keseluruhan senarai alamat sekali.

### Butang kawalan

Butang kawalan berikut tersedia:

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

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



Dalam antara muka pengeditan, anda boleh mengumpulkan senarai penghantar yang anda jangkakan untuk menghantar mesej yang tidak diinginkan kepada anda (*spam*). Anda juga boleh mengumpulkan senarai nama domain penuh (*cth. spammingcompany.com*), yang anda jangkakan atau dari mana anda terima mesej. Semua e-mel daripada alamat/domain yang disenaraikan akan dikenal pasti sebagai spam. Sebaik sahaja anda mempunyai senarai penghantar seperti itu dan/atau nama domain disediakan, anda boleh memasukkannya melalui salah satu kaedah berikut: melalui entri terus setiap alamat e-mel atau dengan mengimport keseluruhan senarai alamat sekali.

### Butang kawalan

Butang kawalan berikut tersedia:

- **Edit** – tekan butang ini untuk membuka dialog, di mana anda boleh memasukkan senarai alamat secara manual (*anda juga boleh menggunakan salin dan tampal*). Masukkan satu item (*penghantar, nama domain*) bagi setiap baris.
- **Eksport** – jika anda bercadang untuk mengeksport rekod untuk tujuan tertentu, anda boleh melakukannya dengan menekan butang ini. Semua rekod akan disimpan ke fail teks kosong.





- **Import** – jika anda sudah mempunyai fail teks bagi alamat/nama domain e-mel yang disediakan, anda boleh mengimportnya dengan mudah dengan memilih butang ini.

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

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

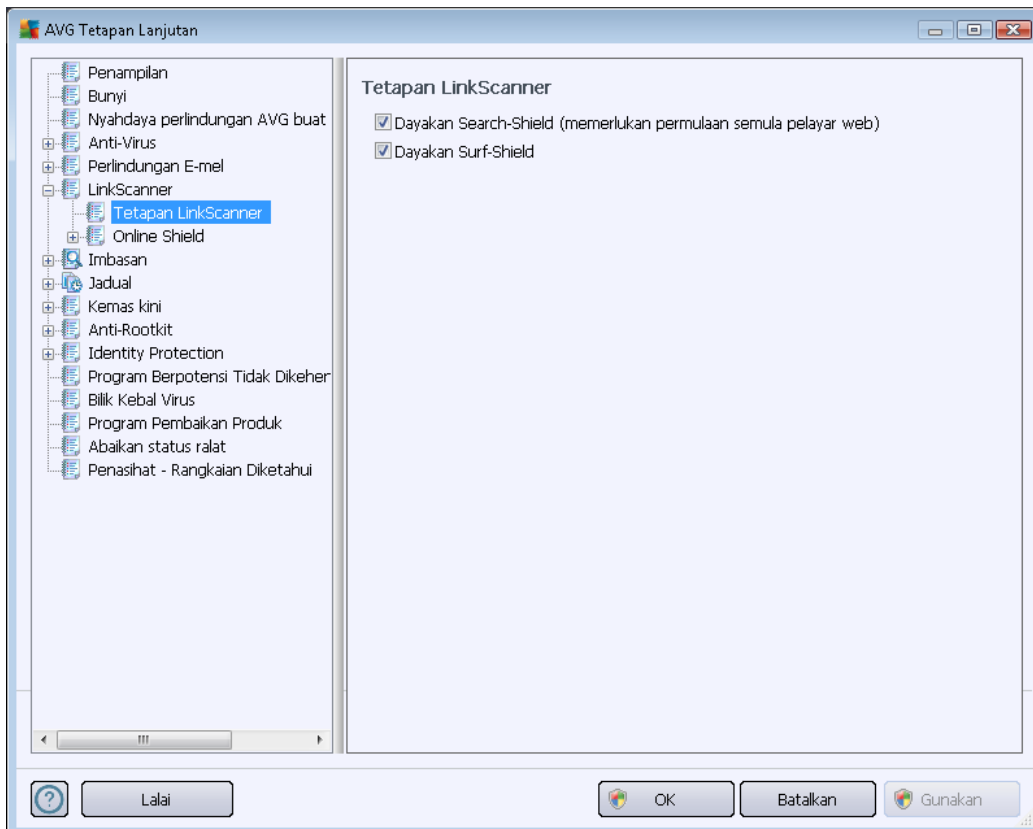
Jika anda masih perlu mengubah konfigurasi [AntiSpam](#) pada tahap yang sangat tinggi, sila ikuti arahan yang diberikan secara terus dalam antara muka pengguna. Secara umumnya, dalam setiap dialog anda akan menemui satu ciri khusus tunggal dan anda boleh mengeditnya – penerangannya sentiasa dimasukkan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

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

## **10.6. LinkScanner**

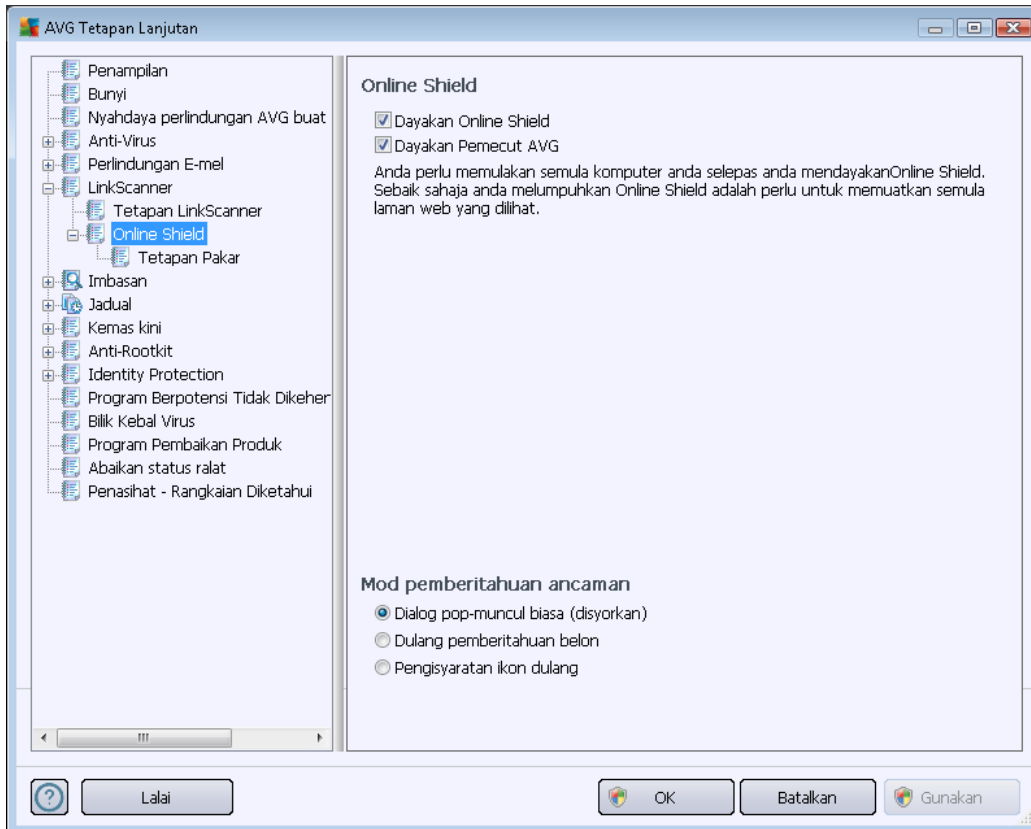
### 10.6.1. Tetapan LinkScanner

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



- **Dayakan Search-Shield** – (*dihidupkan secara lalai*): ikon pemberitahuan penasihat mengenai carian dilakukan dengan Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg atau SlashDot diperiksa kandungan tapak yang dikembalikan oleh enjin carian.
- **Dayakan 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*).

## 10.6.2. Online Shield

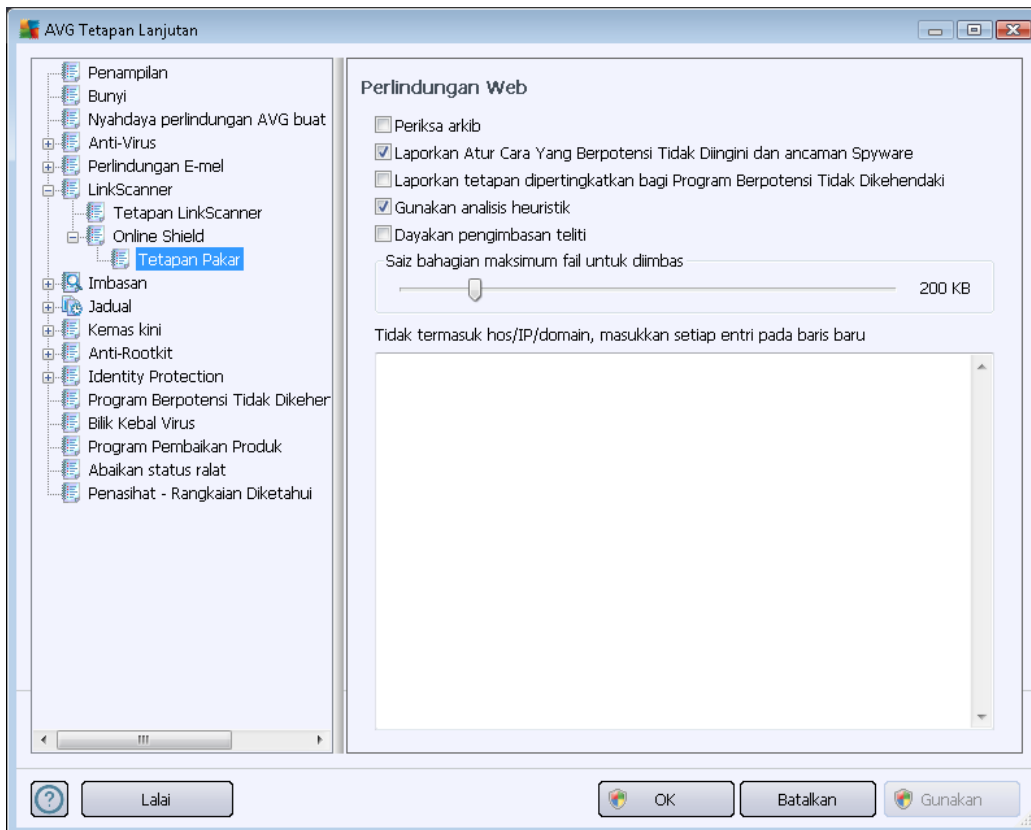


Dialog **Online Shield** menawarkan opsi berikut:

- **Dayakan Online Shield** (*dihidupkan secara lalai*) – Aktifkan/nyahaktifkan seluruh perkhidmatan **Online Shield**. Untuk tetapan lanjutan bagi **Online Shield** sila teruskan ke dialog berikutnya yang dipanggil [Perlindungan Web](#).
- **Dayakan Peningkat AVG** (*dihidupkan secara lalai*) - Aktifkan/Nyahaktifkan perkhidmatan **Peningkat AVG** yang membenarkan main balik video dalam talian yang lebih lancar dan membuatkan muat turun tambahan lebih mudah.

### Mod pemberitahuan ancaman

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.



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

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

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

- **Gunakan analisis heuristik** - (*dibuka secara lalai*): imbas kandungan halaman yang akan dipaparkan menggunakan kaedah [analisis heuristik](#) (*perlagakan dinamik arahan objek yang diimbis dalam persekitaran komputer maya*).
- **Dayakan pengimbasan teliti** (*ditutup secara lalai*) – dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsi ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa
- **Bahagian saiz fail maksimum untuk diimbis** – 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 bagi fail yang masih diimbis dengan **Perisai Dalam Talian**. Walaupun jika fail yang dimuat turun adalah lebih besar daripada yang ditentukan, dan oleh itu, tidak akan diimbis dengan Perisai Dalam Talian, anda masih dilindungi: jika fail dijangkiti, **Resident Shield** akan mengesannya dengan serta-merta.
- **Keluarkan hos/IP/domain** – ke dalam medan teks, anda boleh menaip nama sebenar bagi pelayan (*hos, alamat IP, alamat IP dengan topeng, atau URL*) atau domain yang harus diimbis oleh **Perisai Dalam Talian**. Oleh itu, hanya kecualikan hos yang anda betul-betul pasti tidak akan memberikan kandungan tapak web berbahaya.

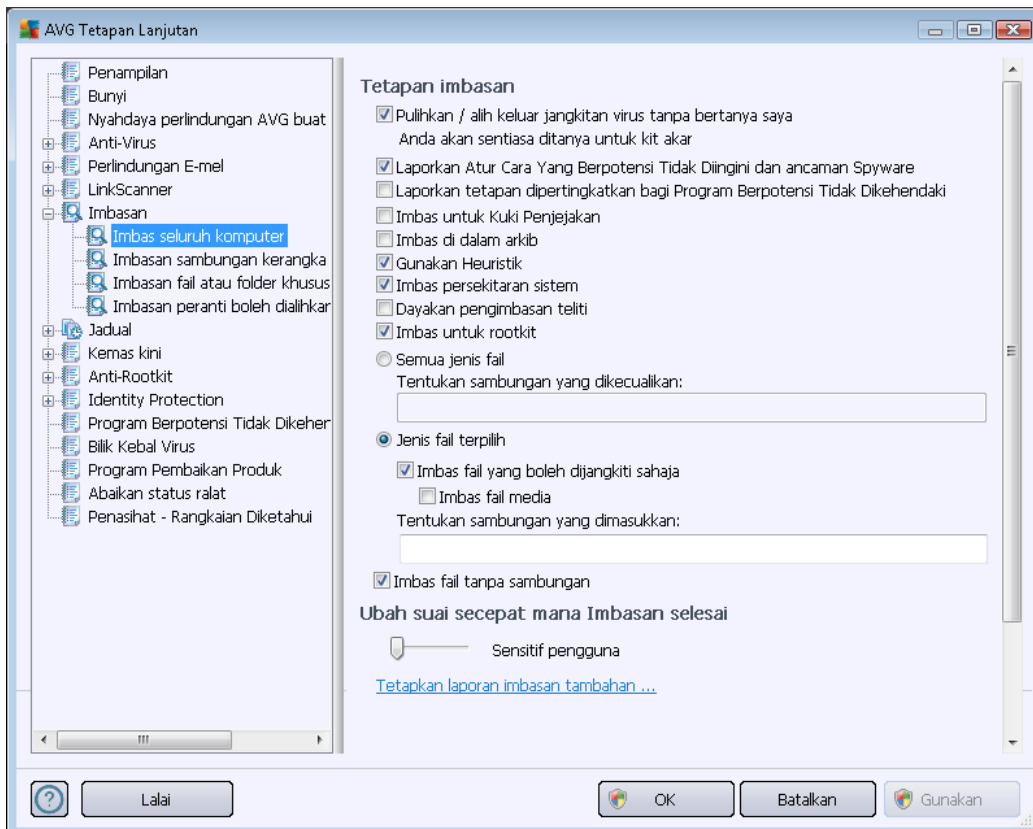
## 10.7. Imbasan

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

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

### 10.7.1. Imbasan seluruh komputer

Opsyen **Imbasan Seluruh Komputer** membenarkan anda mengedit parameter bagi salah satu imbasan yang dipraktakrifkan oleh vendor perisian, [Imbasan seluruh komputer](#):



#### Tetapan imbasan

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

- **Pulihkan / buang jangkitan virus tanpa bertanyakan saya** (*dihidupkan secara lalai*) – jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika cara mengatasinya tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
- **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip** (*dibuka secara lalai*) – tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki** (*ditutup*

*secara lalai*) – tandakan untuk mengesan pakej yang diluaskan bagi perisian pengintip: atur cara yang sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.

- **Imbas untuk Kuki Penjejakan** (*ditutup secara lalai*) – parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan; (*kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektroniknya*)
- **Imbas dalam arkib** (*ditutup secara lalai*) – parameter ini menentukan bahawa imbasan harus memeriksa semua fail yang disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** (*dibuka secara lalai*) – analisis heuristik (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan;
- **Imbas persekitaran sistem** (*dibuka secara lalai*) – imbasan juga akan memeriksa kawasan sistem komputer anda.
- **Dayakan pengimbasan teliti** (*ditutup secara lalai*) – dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.
- **Imbas untuk mengesan rootkit** (*dihidupkan secara lalai*) – imbasan [AntiRootkit](#) mencari kemungkinan terdapatnya rootkit di dalam komputer anda, cth. program dan teknologi yang boleh melakukan aktiviti malware dalam komputer anda. Jika rootkit dikesan, ini tidak semestinya bermaksud komputer anda dijangkiti. Dalam sesetengah kes, pemacu atau bahagian tertentu aplikasi biasa mungkin telah mengesan rootkit dengan salah.

Seterusnya, anda harus menentukan sama ada anda mahu mengimbas

- **Semua jenis fail** dengan kemungkinan pengecualian yang ditakrifkan daripada imbasan dengan memberikan senarai yang pemanjangan fail yang dipisahkan oleh koma (*apabila disimpan, koma bertukar kepada koma bertitik*) yang tidak harus diimbas;
- **Jenis fail yang dipilih** – anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio – jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
- Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** – opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan



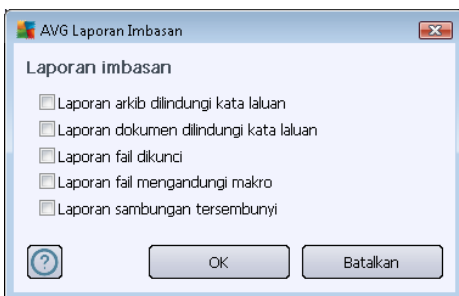
adalah lebih mencurigakan dan sepatutnya diimbis setiap masa.

### Laraskan berapa cepat Imbasan selesai

Dalam bahagian **Laraskan berapa cepat imbasan selesai** anda boleh menentukan selanjutnya kelajuan pengimbasan yang dikehendaki bergantung kepada penggunaan sumber sistem. Secara lalai, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi 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 ...

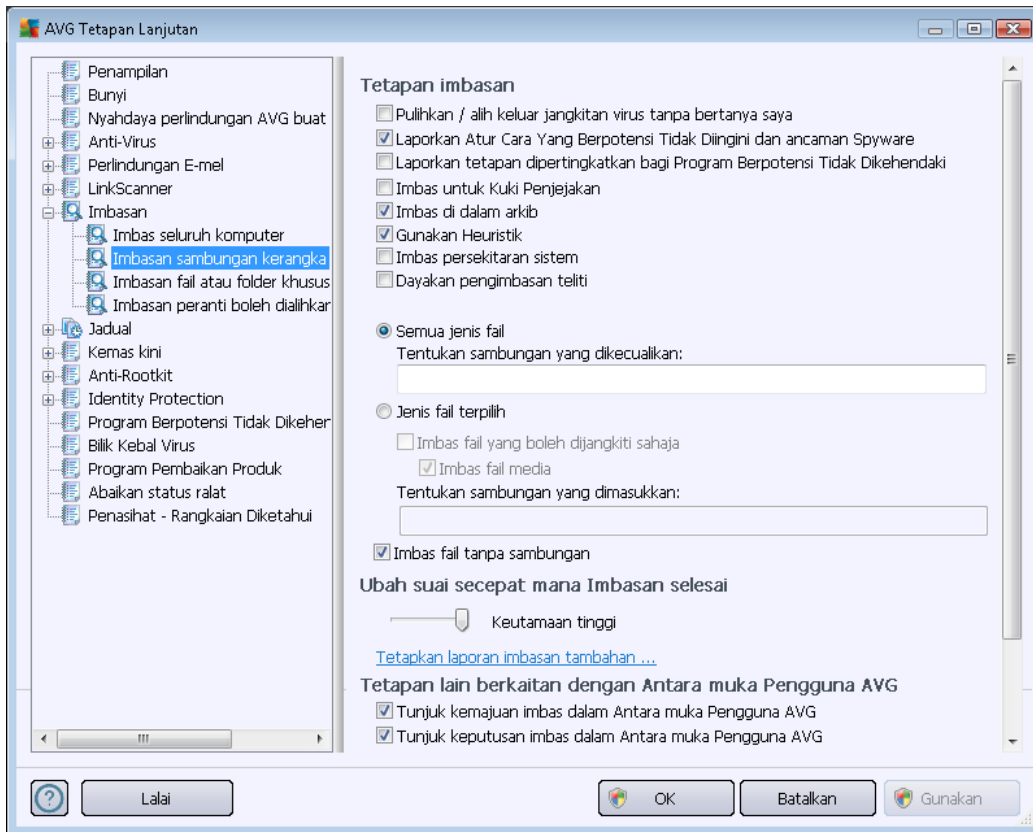
Klik pautan **Tetapkan laporan imbasan tambahan ...** untuk membuka tettingkap dialog tersendiri yang dipanggil **Laporan imbasan** di mana anda boleh menanda rait beberapa item untuk mentakrifkan penemuan imbasan yang harus dilaporkan:



### 10.7.2. Imbasan sambungan kerangka

Sama dengan item [Imbasan seluruh komputer](#) sebelumnya, item ini dinamakan **Imbasan sambungan kerangka** juga menawarkan beberapa opsyen untuk pengeditan imbasan yang dipraktifik 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](#):





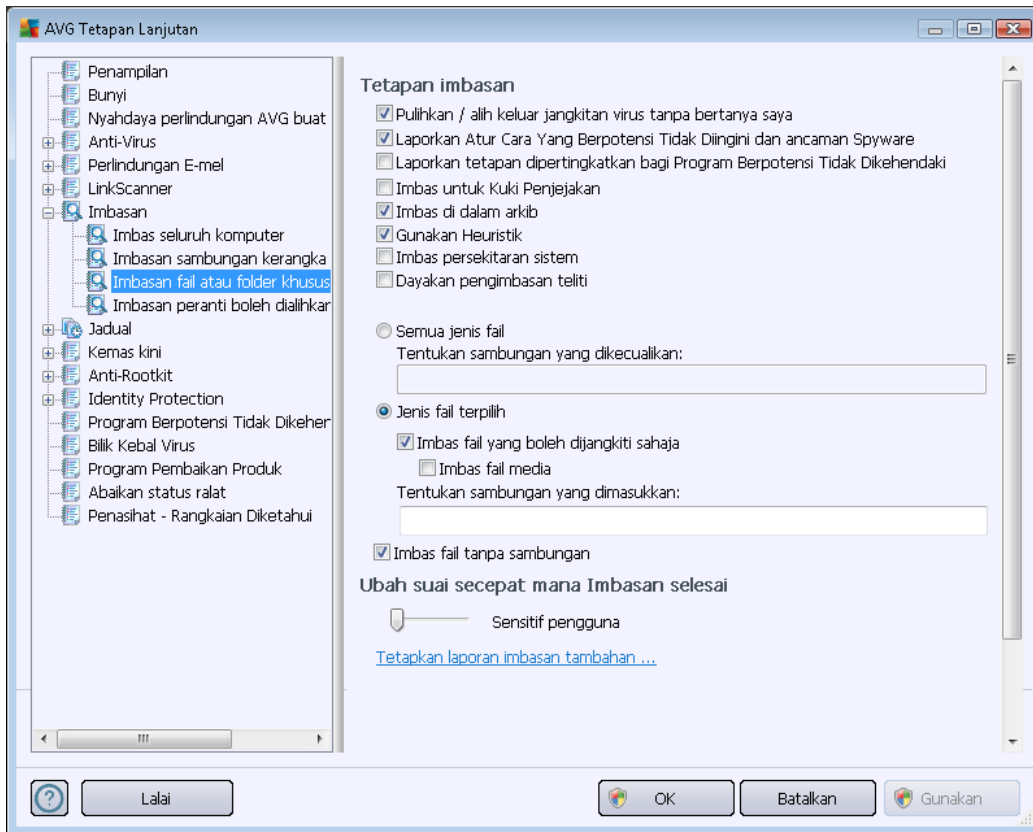
Senarai parameter adalah sama dengan yang tersedia untuk [Imbas seluruh komputer](#). Walau bagaimanapun, tetapan lalai berbeza (*contohnya, Imbasan Seluruh Komputer secara lalai tidak memeriksa arkib tetapi ia mengimbas persekitaran sistem, manakala dengan Imbasan Sambungan Kerangka ia adalah sebaliknya*).

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

Jika dibandingkan dengan dialog [Imbasan Seluruh Komputer](#), dialog **Imbasan sambungan kerangka** turut memasukkan bahagian yang dinamakan **Tetapan lain berkaitan Antara Muka Pengguna AVG**, di mana anda boleh menentukan sama ada anda mahu kemajuan imbasan dan keputusan imbasan boleh diakses dari antara muka pengguna AVG. Juga, anda boleh mentakrifkan bahawa keputusan imbasan hanya boleh dipaparkan jika jangkitan dikesan semasa pengimbasan.

### 10.7.3. Imbasan fail atau folder khusus

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](#):

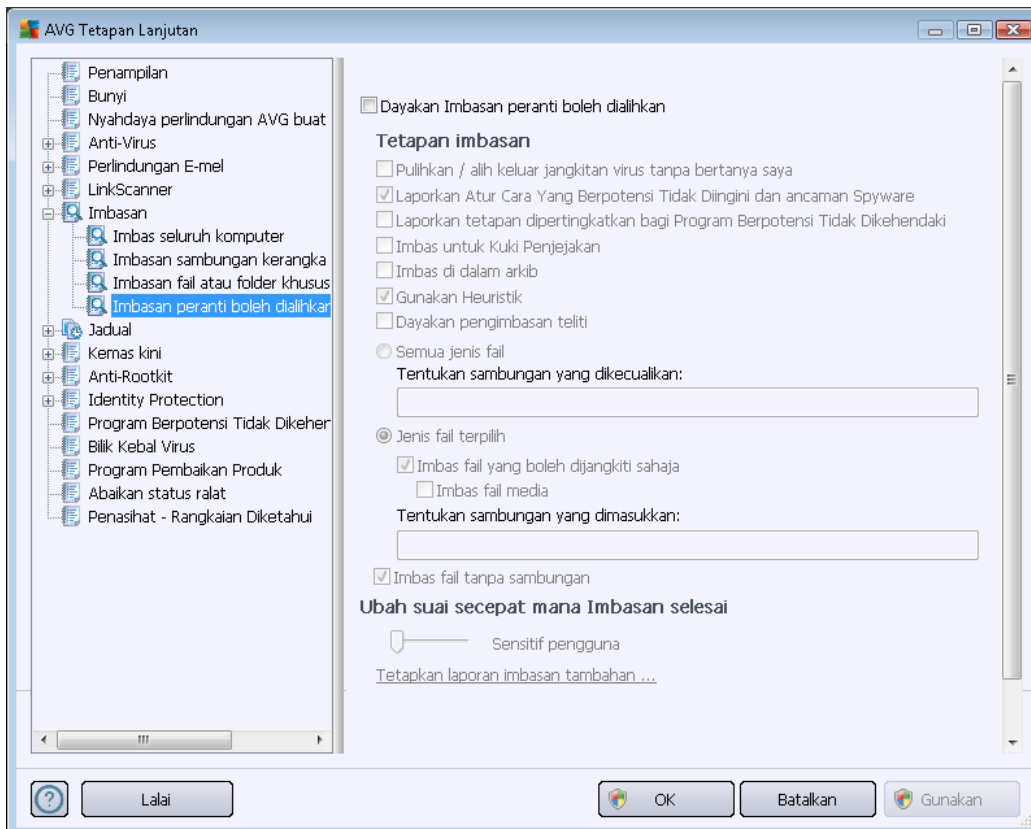


Semua parameter yang disediakan dalam dialog konfigurasi ini hanya digunakan pada kawasan yang dipilih untuk imbasan dengan [Imbas fail atau folder tertentu!](#)

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

#### 10.7.4. Imbasan peranti boleh dialihkan

Antara muka pengeditan untuk *Imbasan peranti boleh ditanggalkan* 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**.

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

#### 10.8. Jadual

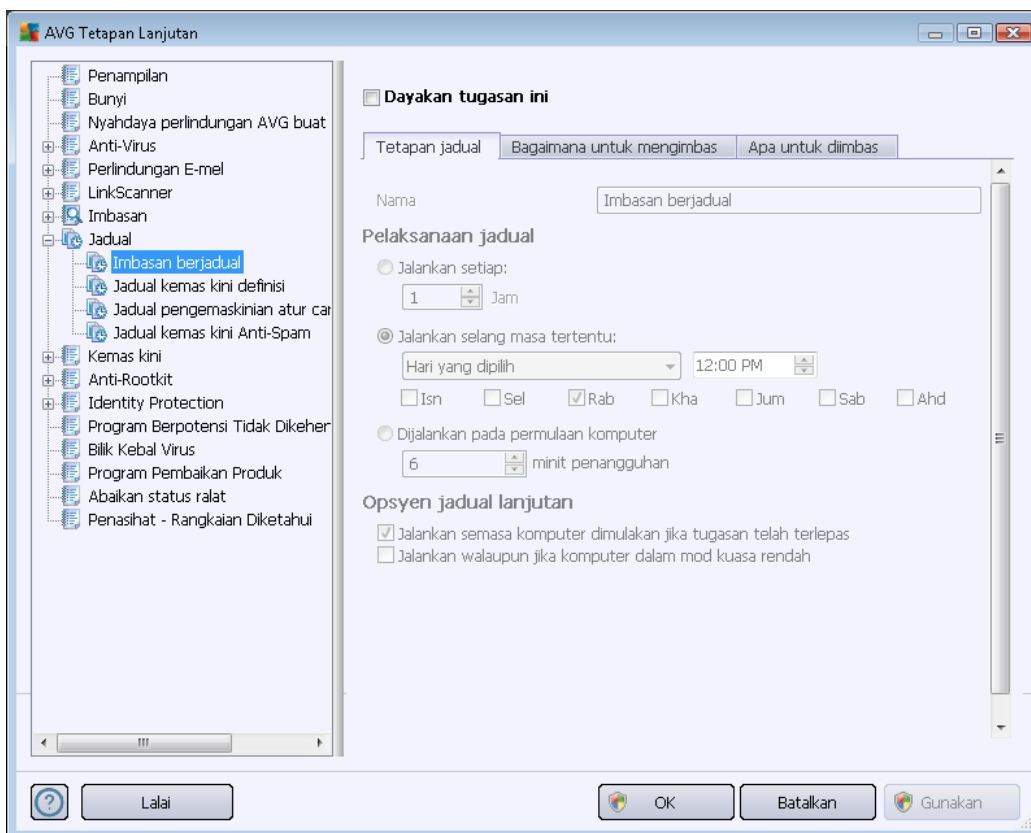
Dalam bahagian **Jadual** anda boleh mengedit tetapan lalai bagi:

- [Imbasan berjadual](#)
- [Jadual kemas kini definisi](#)
- [Jadual kemas kini atur cara](#)

- [Jadual kemas kini AntiSpam](#)

### 10.8.1. Imbasan yang Dijadualkan

Parameter bagi imbasan yang dijadualkan boleh diedit (*atau jadual baru disediakan*) pada tiga tab. Pada setiap tab, anda boleh menanda/tidak menanda dahulu item **Dayakan tugas ini** untuk menyahaktifkan ujian yang dijadualkan buat sementara waktu, dan menghidupkannya semula apabila perlu:



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

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



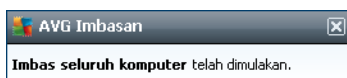
Di dalam dialog ini anda boleh menentukan lebih lanjut parameter imbasan yang berikut:

### Pelaksanaan jadual

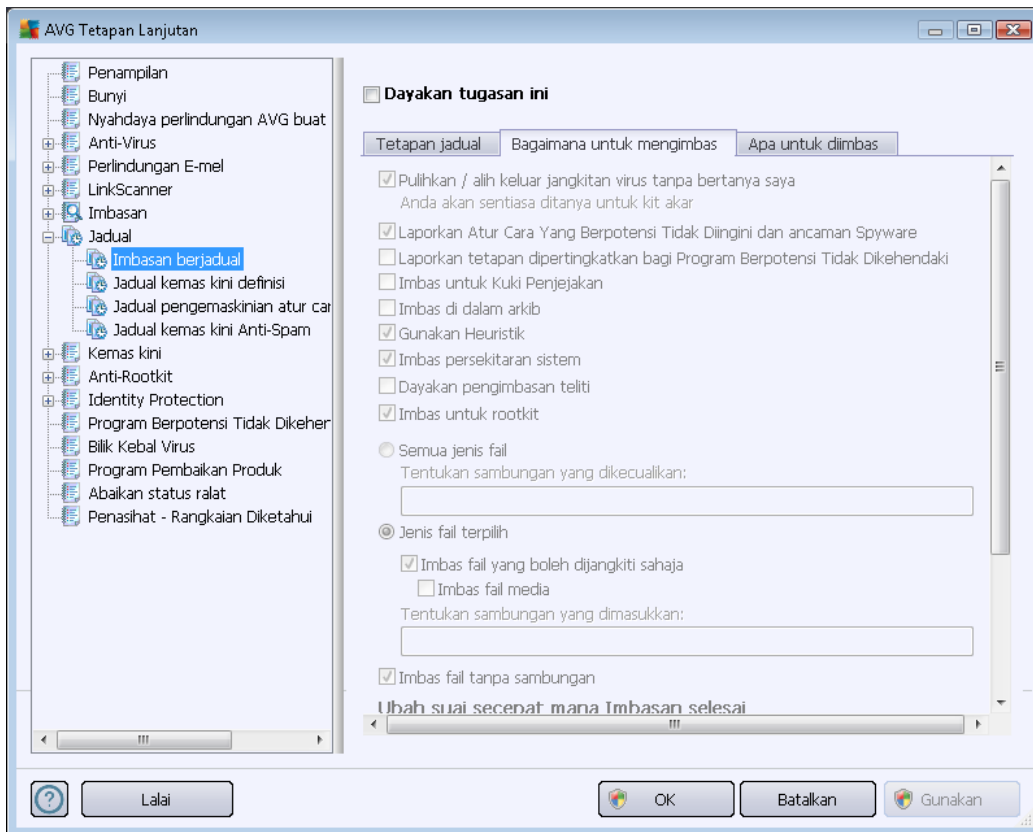
Di sini, anda boleh menentukan jarak waktu untuk pelancaran imbasan baru yang dijadualkan. Pemasaan boleh menjadi sama ada ditakrifkan oleh pelancaran imbasan berulang selepas satu tempoh masa tertentu (***Jalankan setiap ...***) atau dengan menentukan tarikh dan masa sebenar (***Jalankan pada jarak waktu khusus ...***), atau berkemungkinan dengan mentakrifkan peristiwa yang pelancaran imbasan harus dikaitkan dengan (***Jalankan 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 lampu suluh*) memberitahu imbasan yang dijadualkan sedang dijalankan. Klik kanan pada ikon AVG imbasan berjalan untuk membuka menu konteks di mana anda boleh membuat keputusan untuk menjeda atau malah menghentikan imbasan yang sedang berjalan, dan juga menukar prioriti imbasan yang sedang berjalan.



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 virus tanpa bertanyakan saya (dihidupkan secara lalai):** jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika terdapat cara mengatasinya. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
- **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip (dibuka secara lalai):** tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini (ditutup secara lalai):** tandakan untuk mengesan pakej yang diluaskan bagi perisian pengintip: atur cara yang sangat ok dan tidak berbahaya apabila diperoleh daripada pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi,



walaupun bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.

- **Imbas untuk Kuki Penjejakan (ditutup secara lalai):** parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan sewaktu imbasan; *kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektroniknya)*
- **Imbas dalam arkib (ditutup secara lalai):** parameter ini mentakrifkan imbasan harus memeriksa semua fail walaupun jika ia disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik (dibuka secara lalai):** analisis heuristik (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan;
- **Imbas persekitaran sistem (dibuka secara lalai):** imbasan juga akan memeriksa kawasan sistem komputer anda;
- **Dayakan pengimbasan menyeluruh (dimatikan secara lalai):** dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsiyen ini untuk mengaktifkan algoritma pengimbasan yang paling menyeluruh yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.
- **Imbas untuk mengesan rootkit (dihidupkan secara lalai):** *Imbasan [AntiRootkit](#) mencari kemungkinan terdapatnya rootkit di dalam komputer anda, cth. program dan teknologi yang boleh melakukan aktiviti malware dalam komputer anda. Jika rootkit dikesan, ini tidak semestinya bermaksud komputer anda dijangkiti. Dalam sesetengah kes, pemacu atau bahagian tertentu aplikasi biasa mungkin telah mengesan rootkit dengan salah.*

Seterusnya, anda harus menentukan sama ada anda mahu mengimbas

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

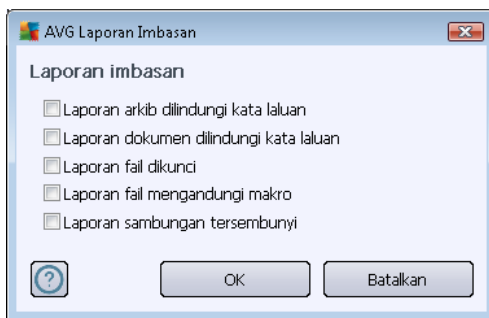
**Laraskan berapa cepat Imbasan selesai**



Dalam bahagian **Laraskan berapa cepat Imbasan selesai** anda boleh menentukan selanjutnya kelajuan pengimbasan yang dikehendaki bergantung kepada penggunaan sumber sistem. Secara lalai, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* 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.

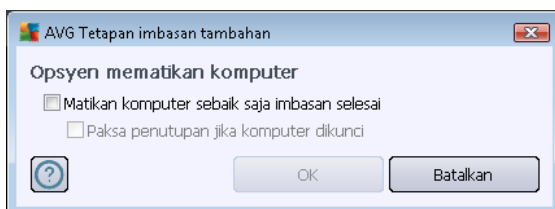
### Tetapkan laporan imbasan tambahan

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:

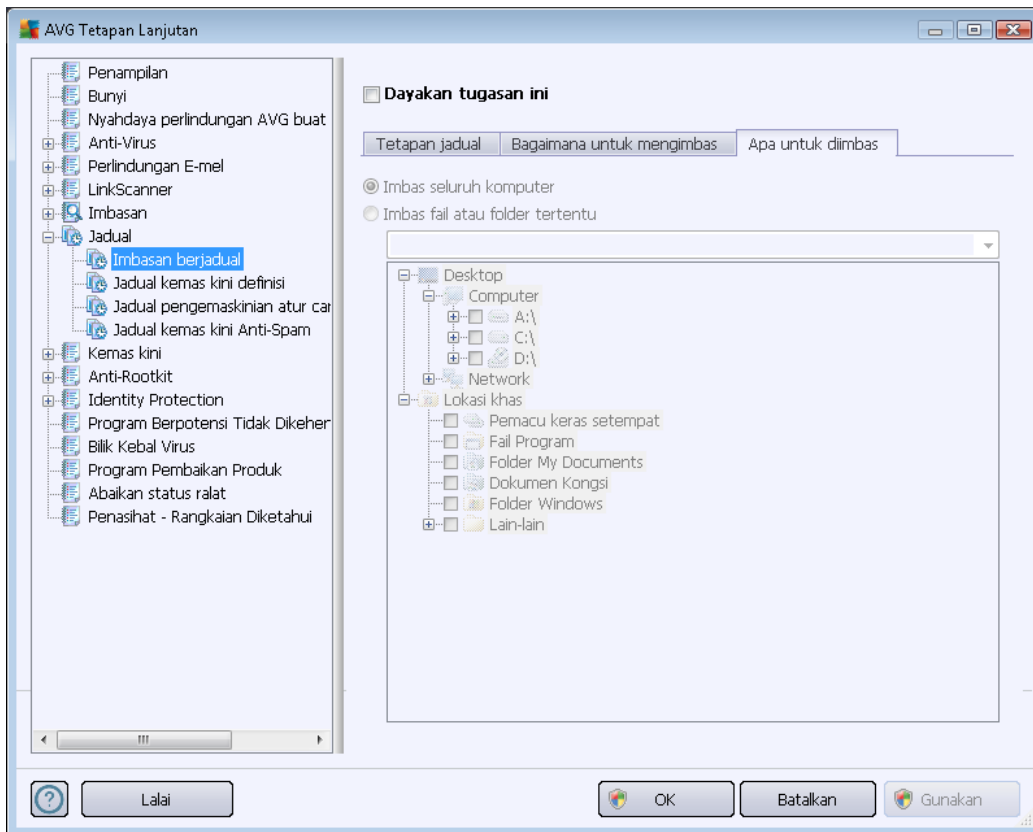


### Tetapan imbasan tambahan

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



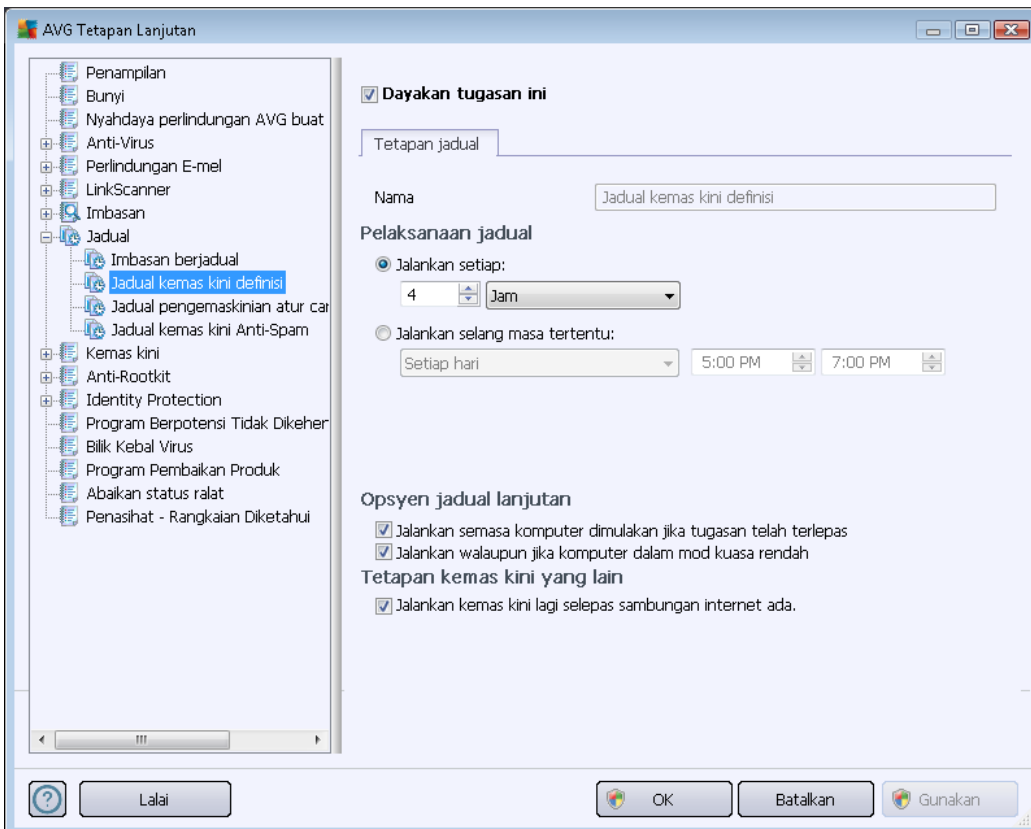




Pada tab ***Apa yang hendak diimbas*** anda boleh menentukan sama ada anda mahu menjadualkan [pengimbasan seluruh komputer](#) atau [pengimbasan fail atau folder tertentu](#). Jika anda memilih pengimbasan fail atau folder tertentu, dalam bahagian bawah dialog ini, struktur pepohonan yang dipaparkan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

### 10.8.2. Jadual Kemas Kini Definisi

Jika **benar-benar perlu**, anda boleh tidak menanda item **Dayakan tugas ini** untuk menyahaktifkan kemas kini atur cara buat sementara waktu, dan menghidupkannya semula pada waktu lain:



Dalam dialog ini, anda boleh menyediakan beberapa parameter terperinci mengenai jadual kemas kini definisi. Dalam medan teks yang dipanggil **Nama** (*nyahaktifkan semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.

#### Pelaksanaan jadual

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

#### Opsyen jadual lanjutan

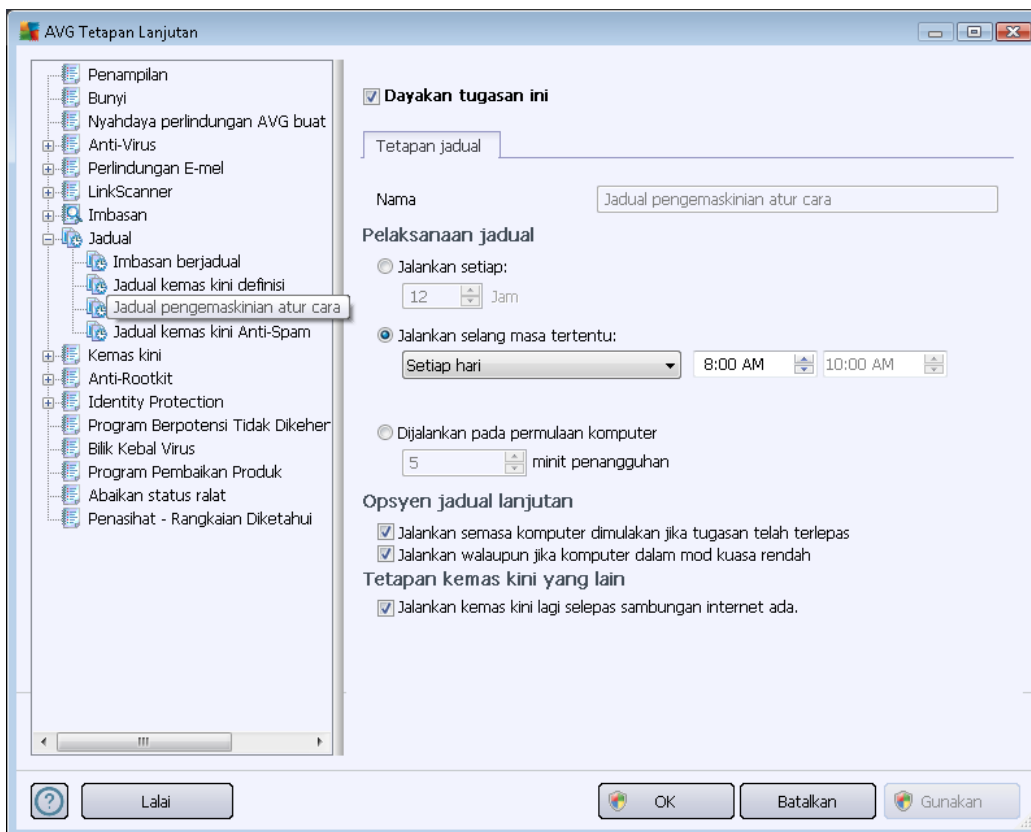
Seksyen ini membolehkan anda menentukan dalam keadaan apa kemas kini harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

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

### 10.8.3. Jadual Kemas Kini Atur Cara

Jika **benar-benar perlu**, anda boleh tidak menanda item **Dayakan tugas ini** untuk menyahaktifkan kemas kini atur cara buat sementara waktu, dan menghidupkannya semula pada waktu lain:



Dalam medan teks yang dipanggil **Nama** (*nyahaktifkan semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.

## Pelaksanaan jadual

Di sini, tentukan jarak waktu untuk 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.

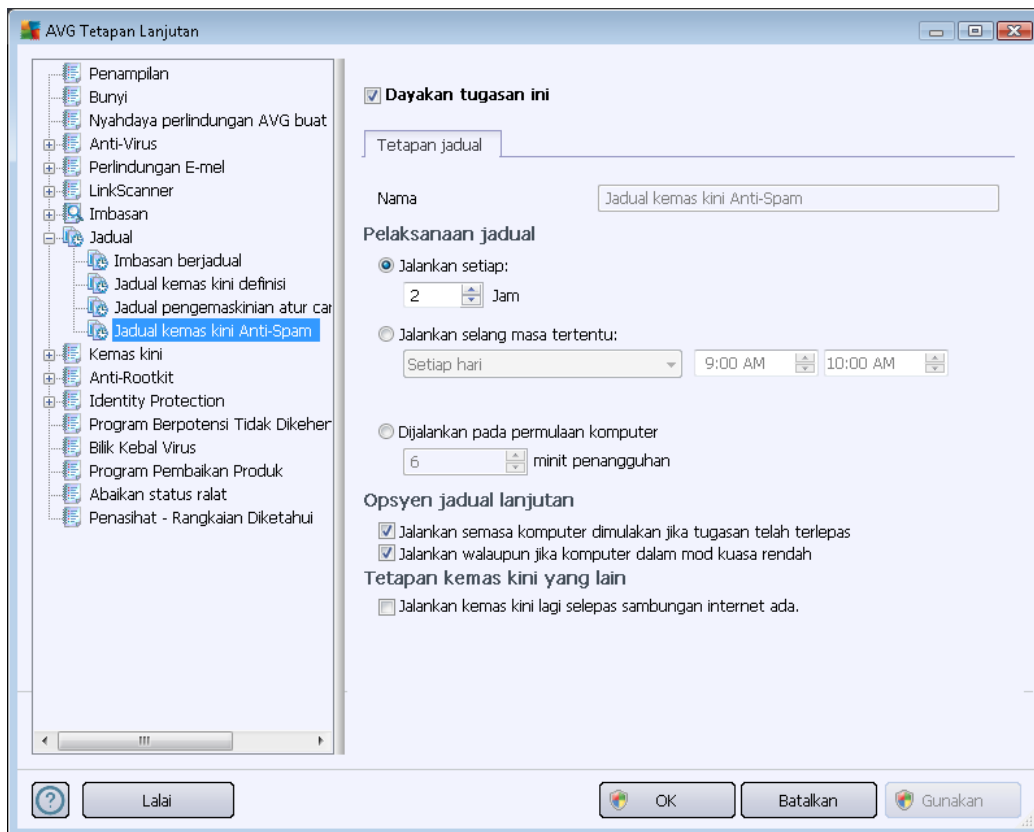
### **Tetapan kemas kini yang lain**

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](#)).

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

### **10.8.4. Jadual Kemas Kini AntiSpam**

Jika benar-benar perlu, anda boleh tidak menanda item ***Dayakan tugas ini*** untuk menyahaktifkan kemas kini [AntiSpam](#) yang dijadualkan buat sementara waktu, dan menghidupkannya semula pada waktu lain:



Dalam dialog ini, anda boleh menyediakan beberapa parameter terperinci bagi jadual kemas kini. Dalam medan teks yang dipanggil **Nama** (*nyahaktifkan semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.

### Pelaksanaan jadual

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

### Opsyen jadual lanjutan

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

### Tetapan kemas kini yang lain

Tandakan opsyen **Jalankan kemas kini semula sebaik sahaja sambungan Internet tersedia**

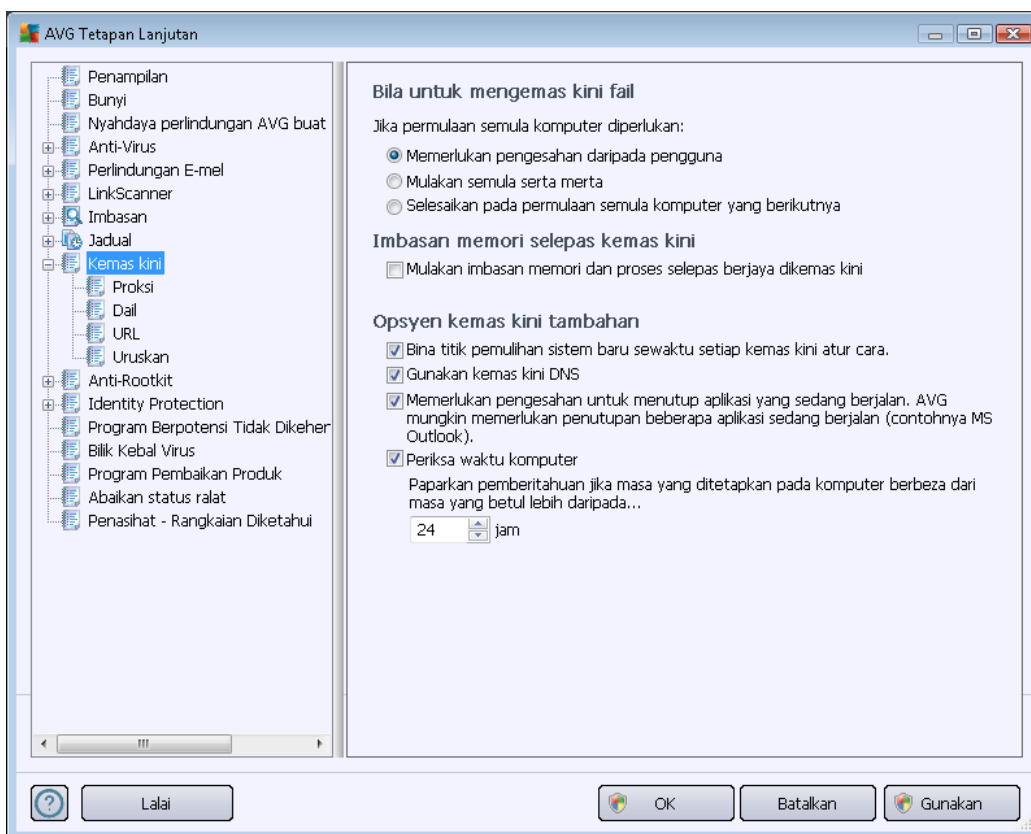


untuk memastikan jika sambungan internet rosak dan proses kemas kini [Anti-Spam](#) gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan internet disimpan semula.

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

## 10.9. 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 seksyen ini, anda boleh memilih daripada tiga pilihan alternatif untuk digunakan jika proses kemas kini memerlukan anda memulakan semula PC. Penyelesaian kemas kini boleh dijadualkan untuk mula semula PC seterusnya, atau anda boleh melancarkan mula semula dengan segera:

- **Memerlukan pengesahan dari pengguna (secara lalai)** – anda akan diminta untuk meluluskan mula 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

- **Lengkapkan mula semula komputer seterusnya** - pemuktamadan [proses kemas kini](#) akan ditangguh sehingga mula semula komputer seterusnya. Sila ingat bahawa pilihan ini hanya disyorkan jika anda pasti bahawa komputer dimulakan semula dengan kerap, sekurang-kurangnya sekali sehari!

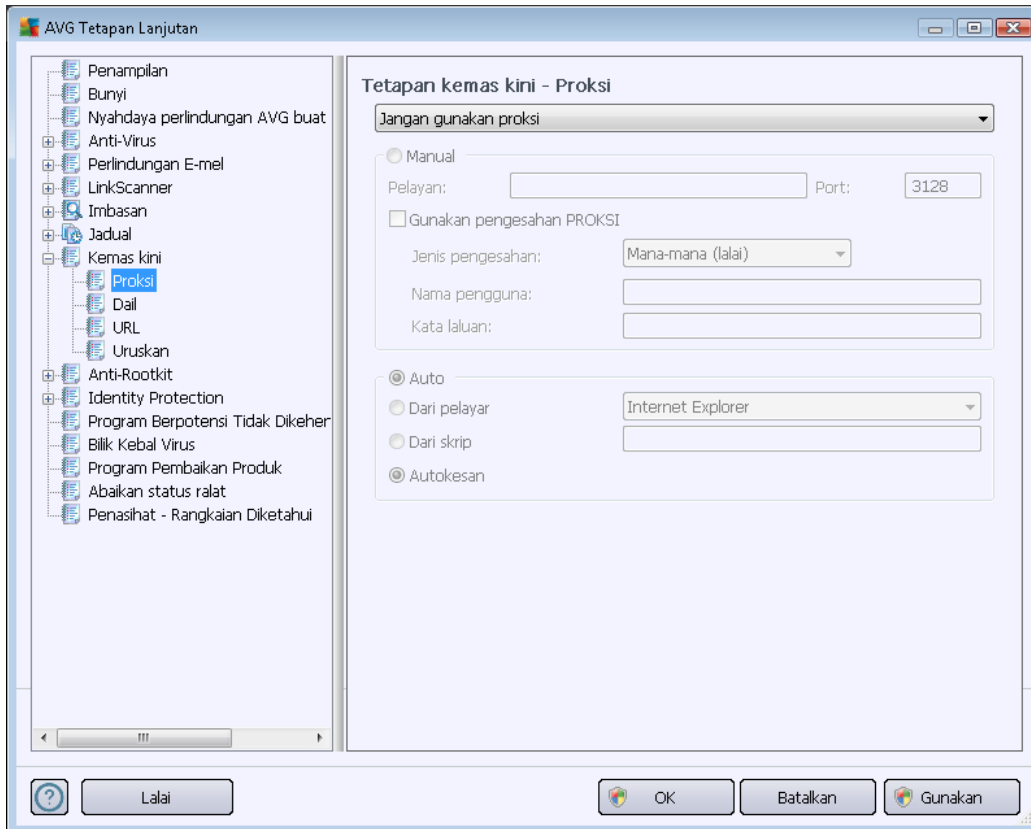
### Imbasan memori selepas kemas kini

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 (dihidupkan secara lalai)** – dengan item ini ditanda, sebaik sahaja kemas kini dilancarkan, **AVG Internet Security 2012** anda mencari maklumat mengenai versi pangkalan data virus terkini dan versi atur cara terkini pada pelayan DNS. Kemas kini fail terkecil yang amat diperlukan dimuat turun, dan digunakan. Dengan cara ini, jumlah amaun data yang dimuat turun diminimumkan, dan proses kemas kini berjalan dengan lebih cepat.
- **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 opsyen ini untuk mengesahkan bahawa anda mahu pemberitahuan ini dipaparkan jika masa komputer berbeza dari masa yang betul lebih daripada bilangan jam yang ditetapkan.

### 10.9.1. 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 proksi** – tetapan lalai
- **Cuba penyambungan menggunakan proksi dan jika ia gagal, sambungkan secara langsung**

Jika anda memilih sebarang opsi 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 opsi **Manual** untuk mengaktifkan bahagian dialog





*masing-masing*) anda perlu menentukan item berikut:

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

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

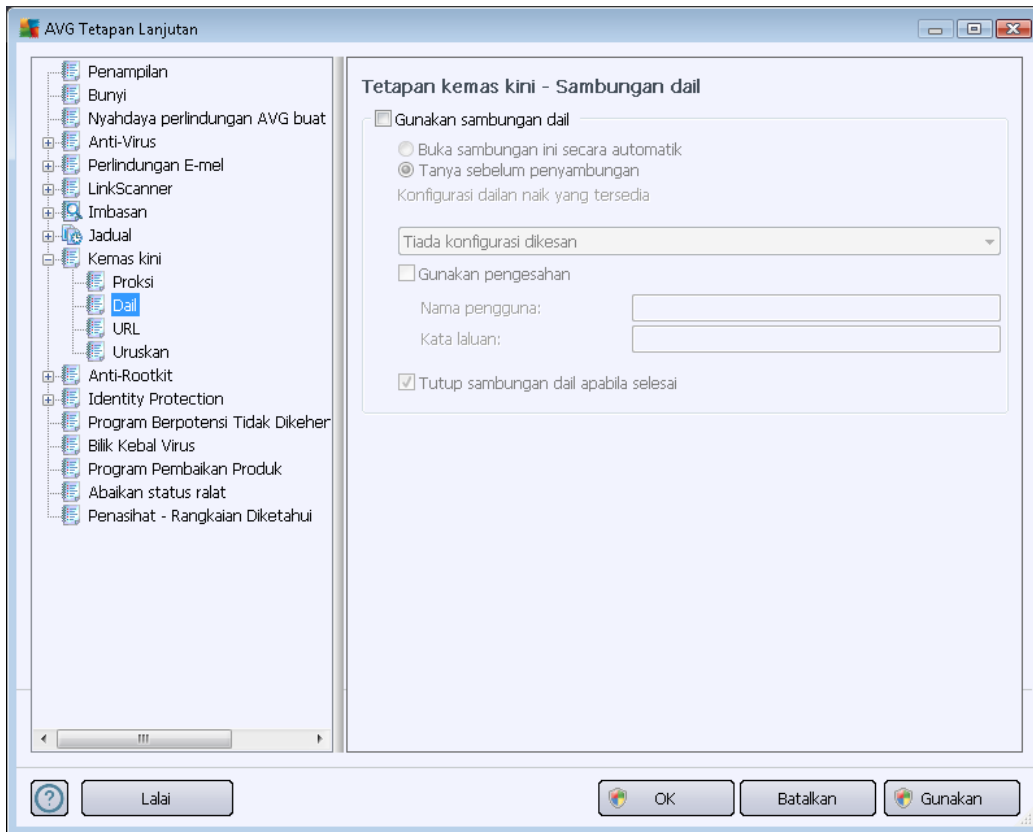
### **Konfigurasi automatik**

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

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

### **10.9.2. Dailan**

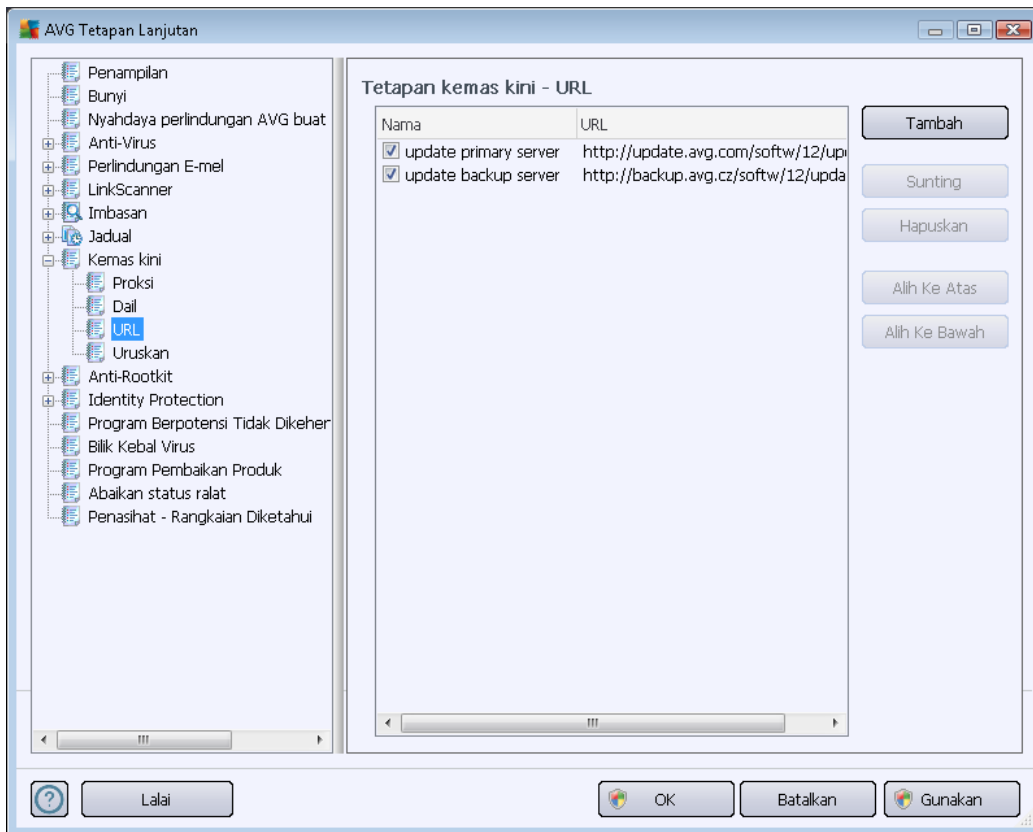
Semua parameter yang ditakrifkan secara pilihan dalam dialog **Kemas kini tetapan – sambungan Dailan** merujuk kepada sambungan dailan kepada Internet. Medan dialog adalah tidak aktif sehingga anda menandakan opsyen **Gunakan sambungan dailan** yang mengaktifkan medan:



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

### 10.9.3. URL

Dialog **URL** menawarkan senarai alamat Internet dari mana fail kemas kini dimuat turun:



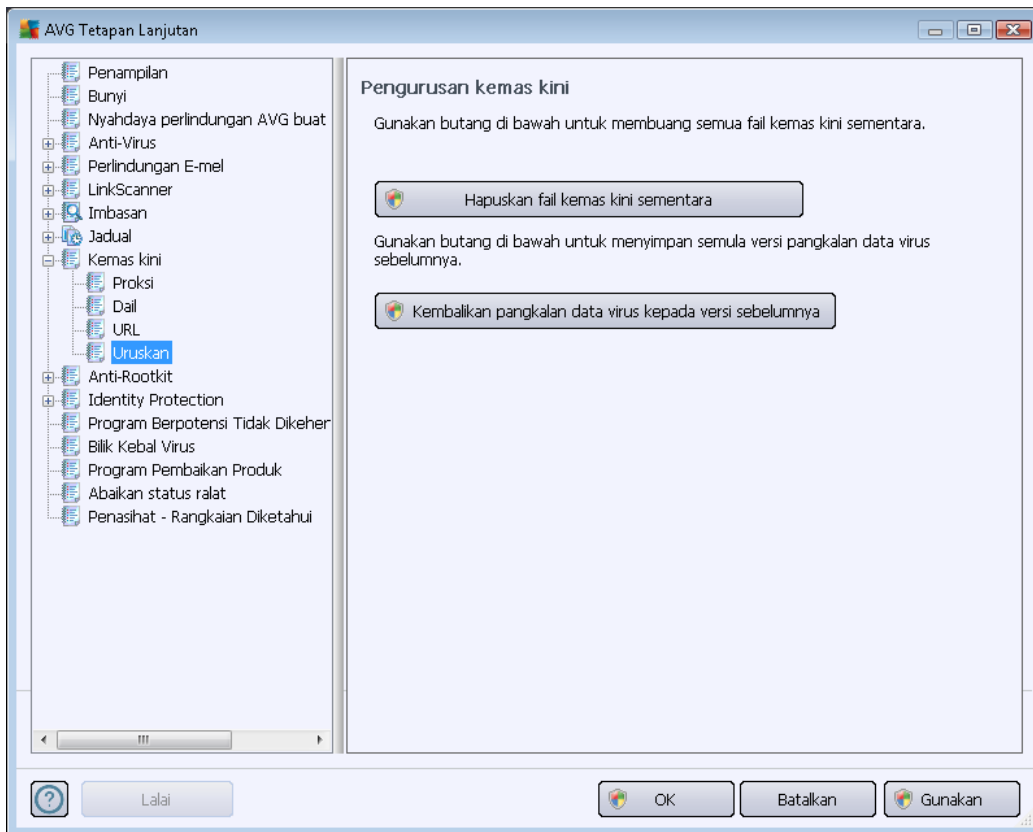
#### Butang kawalan

Senarai dan itemnya boleh diubah suai menggunakan butang kawalan berikut:

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

#### 10.9.4. Uruskan

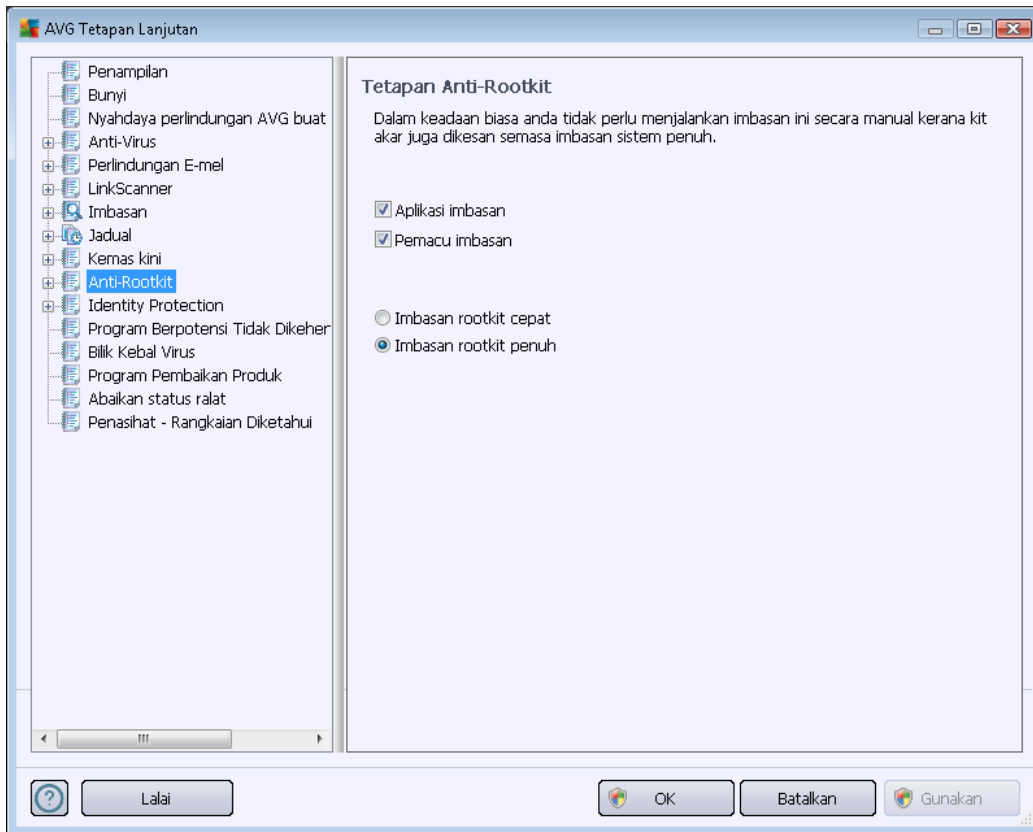
Dialog *Uruskan pengurusan* menawarkan dua opsyen yang boleh diakses melalui dua butang:



- **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 semula pangkalan data virus ke versi sebelumnya** – tekan butang ini untuk memadam versi pangkalan virus terkini daripada cakera keras anda, dan untuk kembali ke versi yang disimpan sebelum ini (*versi pangkalan virus baru akan menjadi sebahagian daripada kemas kini berikut*)

#### 10.10. AntiRootkit

Dalam dialog *Tetapan AntiRootkit* anda boleh mengedit konfigurasi komponen [AntiRootkit](#) dan parameter khusus pengimbasan antirootkit. Pengimbasan antirootkit adalah proses lalai yang disertakan dalam [Imbasan Seluruh Komputer](#):



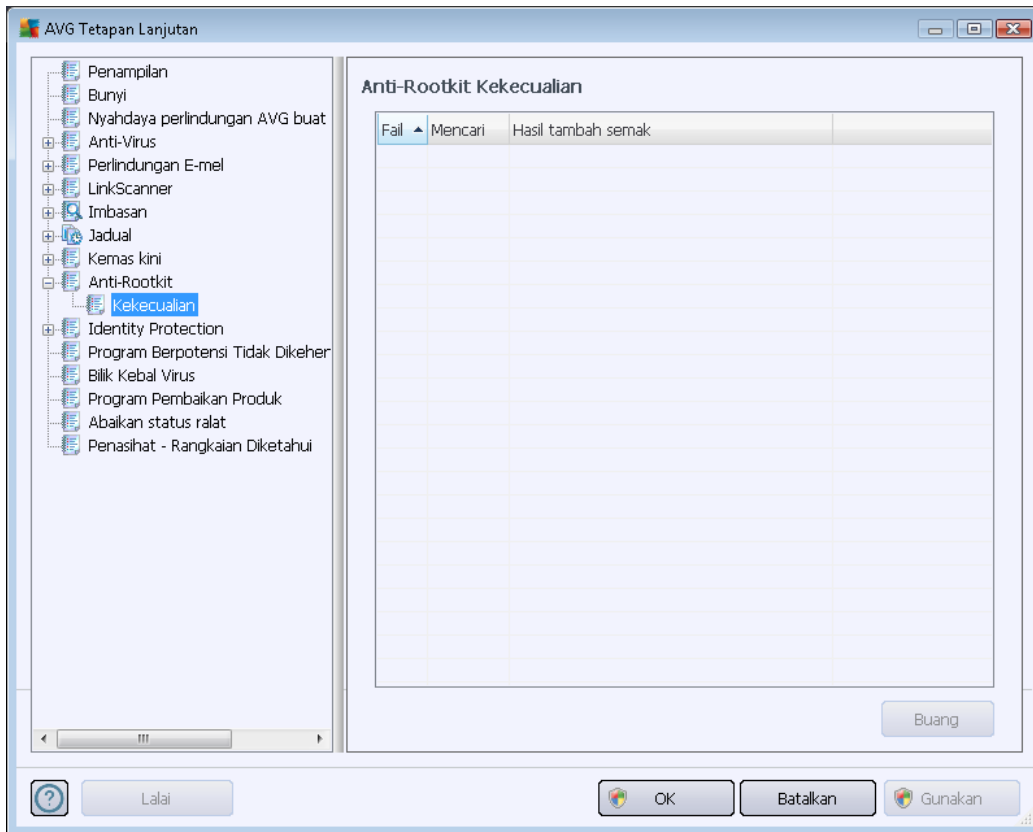
Mengedit semua fungsi komponen [AntiRootkit](#) seperti yang diberikan dalam dialog ini juga boleh diakses secara terus daripada [antara muka komponen AntiRootkit](#).

**Aplikasi imbasan** dan **Pemacu imbasan** membolehkan anda menentukan secara terperinci apa yang harus dimasukkan dalam imbasan antirootkit. Tetapan ini dimaksudkan untuk pengguna lanjutan; kami mengesyorkan untuk membiarkan semua opsi dihidupkan. Seterusnya, anda boleh memilih mod pengimbasan rootkit:

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

### 10.10.1. Kekecualian

Dalam dialog **Pengecualian AntiRootkit** anda boleh mentakrifkan fail khusus (*contohnya, sesetengah pemacu mungkin dikesan sebagai rootkit secara salah*) yang perlu dikecualikan dari pengimbasan ini:

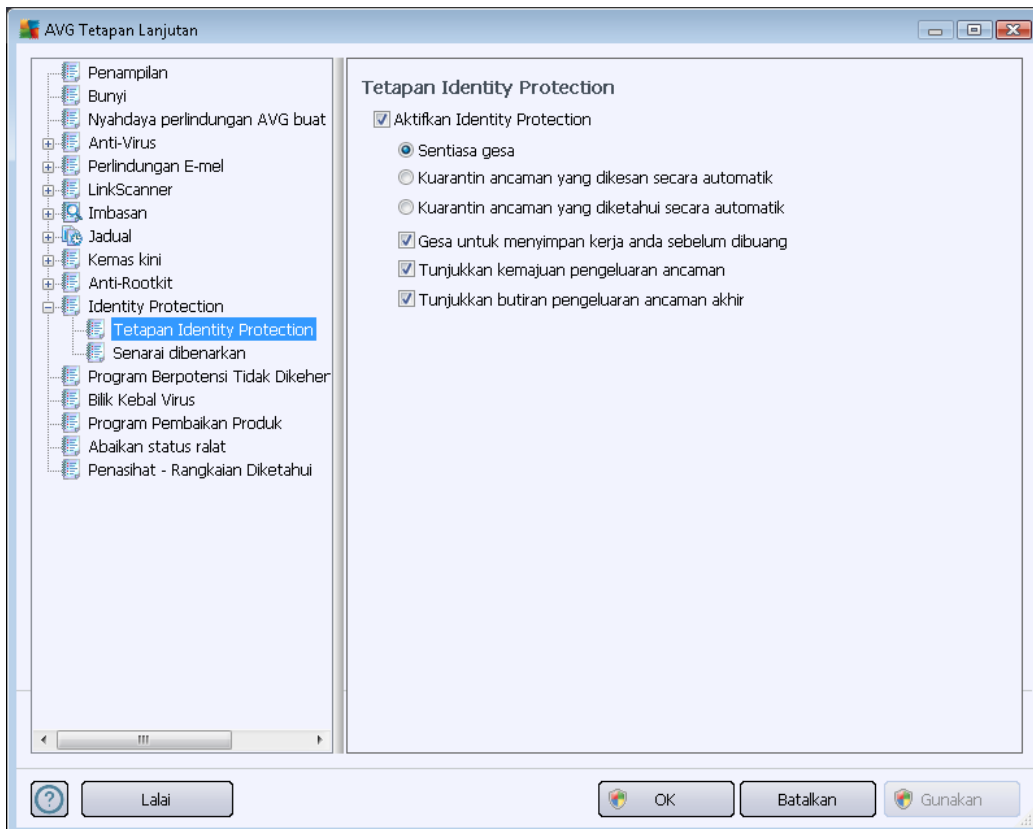


### 10.11. Identity Protection

**Identity Protection** adalah komponen antimalware yang melindungi anda daripada semua jenis malware (*perisian pengintip, bot, pencuri identiti, ...*) menggunakan teknologi kelakuan dan memberikan perlindungan hari sifar untuk virus baharu (*untuk penerangan terperinci bagi kefungsiannya komponen sila rujuk bab [Identity Protection](#)*).

### 10.11.1. Tetapan Identity Protection

Dialog **tetapan Identity Protection** membenarkan anda menghidupkan/mematikan ciri permulaan bagi komponen [Identity Protection](#):



**Aktifkan Identity Protection** (*dibuka secara lalai*) – jangan tanda untuk mematikan komponen [Identity Protection](#).

**Kami amat mengesyorkan jangan melakukan ini kecuali anda terpaksa!**

Apabila [Identity Protection](#) diaktifkan, anda boleh menentukan apa yang perlu dilakukan apabila ancaman dikesan:

- **Sentiasa gesa** (*dihidupkan secara lalai*) - apabila ancaman dikesan, anda akan ditanya sama ada ia harus dialihkan ke kuarantin untuk memastikan tiada aplikasi yang anda hendak jalankan dibuang.
- **Kuarantin ancaman dikesan secara automatik** – tandakan kotak semakan ini untuk mentakrifkan anda hendak semua kemungkinan ancaman dikesan dibuang ke tempat yang selamat bagi [Bilik Kebal Virus](#) dengan segera. Mengekalkan tetapan lalai apabila ancaman dikesan, anda akan ditanya sama ada ia harus dialihkan ke kuarantin untuk memastikan tiada aplikasi yang anda hendak jalankan dibuang.
- **Kuarantin ancaman diketahui secara automatik** – biarkan item ini ditanda jika anda hendak semua aplikasi dikesan sebagai kemungkinan malware untuk dialihkan secara



automatik dan dengan serta merta ke [Bilik Kebal Virus](#).

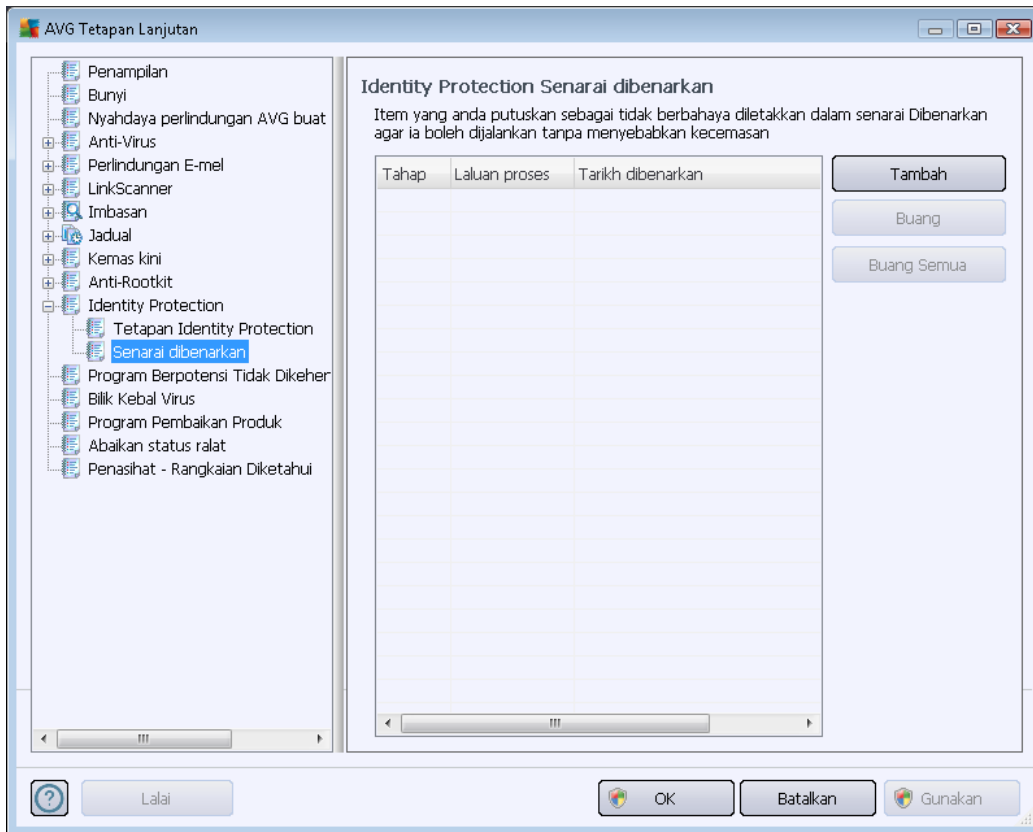
Seterusnya, anda boleh menguntukkan item tertentu untuk secara pilihan, mengaktifkan lebih kefungsiian [Identity Protection](#):

- **Gesa untuk menyimpan kerja anda sebelum pengeluaran** - (*dihidupkan secara lalai*) – pastikan item ini ditanda jika anda hendak diberi amaran sebelum aplikasi dikesan sebaik sahaja malware dikeluarkan ke kuarantin. Jika anda hanya bekerja dengan aplikasi tersebut, projek anda mungkin hilang dan anda perlu menyimpannya dahulu. sangat mengesyorkan.
- **Tunjukkan perkembangan pembuangan ancaman** - (*dihidupkan secara lalai*) – dengan item ini dihidupkan, sebaik sahaja kemungkinan malware dikesan, dialog baharu dibuka untuk memaparkan perkembangan malware yang sedang dibuang ke kuarantin.
- **Tunjukkan butiran pembuangan ancaman akhir** - (*dihidupkan secara lalai*) – dengan item ini dihidupkan, **Identity Protection** memaparkan maklumat terperinci terhadap setiap objek yang alihkan ke kuarantin (*tahap keseriusan, lokasi, dll.*).

### 10.11.2. Senarai dibenarkan

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





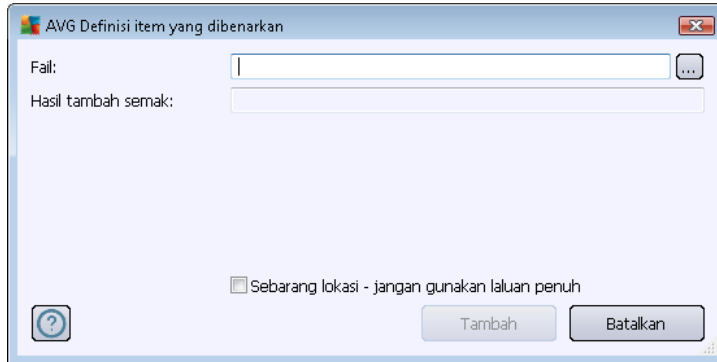
**Senarai dibenarkan Identity Protection** memberikan maklumat berikut pada setiap aplikasi:

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

### Butang kawalan

Butang kawalan yang tersedia dalam dialog **Senarai Identity Protection yang Dibenarkan** adalah seperti berikut:

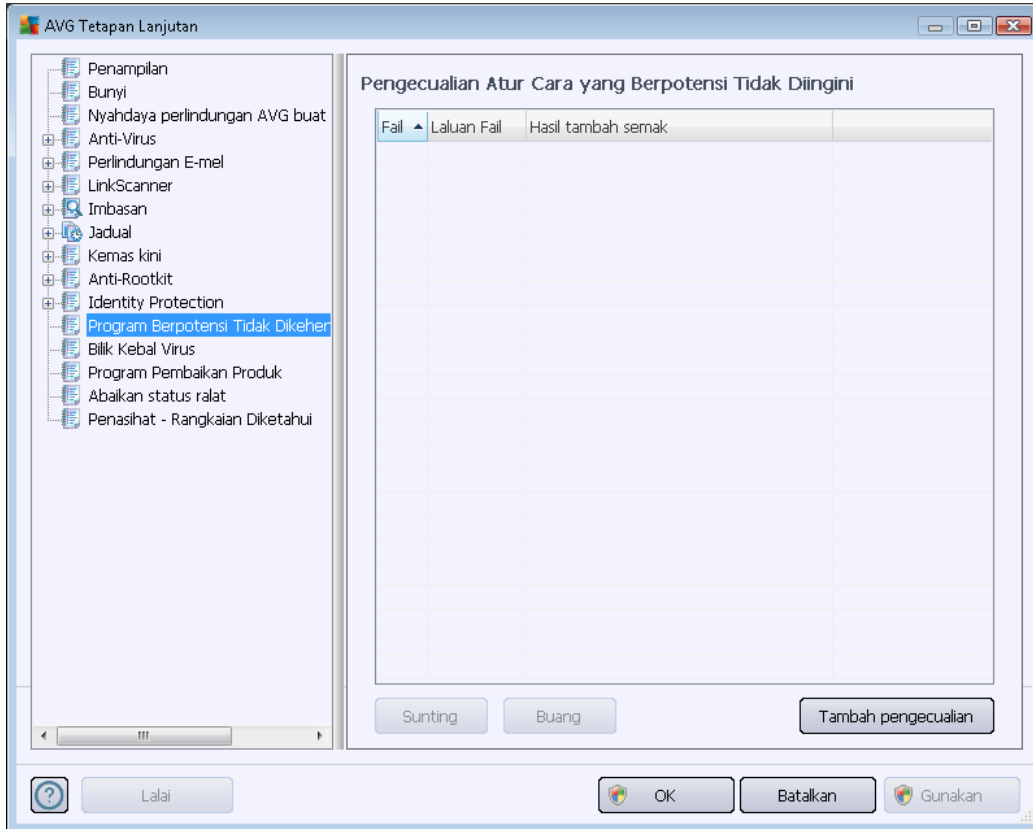
- **Tambah** - tekan butang ini untuk menambah aplikasi baharu ke senarai yang dibenarkan. Pop timbul dialog yang berikutnya:



- **Fail** – taipkan laluan penuh ke fail (*aplikasi*) yang anda hendak 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.
  - **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
- **Buang** - tekan untuk membuang aplikasi yang dipilih daripada senarai
  - **Buang semua** - tekan untuk membuang semua aplikasi yang disenaraikan

## 10.12. Atur Cara yang Berpotensi Tidak Diingini

**AVG Internet Security 2012** boleh menganalisis dan mengesan aplikasi boleh laku atau pustaka DLL yang berkemungkinan berpotensi tidak diingini dalam sistem. Dalam sesetengah kes, pengguna mungkin mahu mengekalkan atur cara yang tidak dikehendaki tertentu pada atur cara (komputer yang dipasang dengan sengaja). Sesetengah atur cara, terutama sekali yang percuma, termasuk adware. Adware seperti itu mungkin dikesan dan dilaporkan oleh **AVG Internet Security 2012** 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:



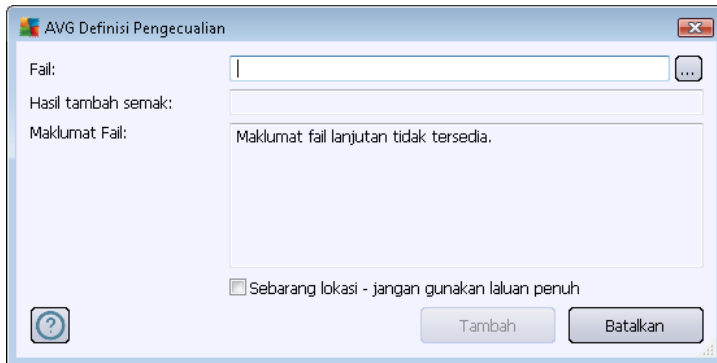
Dialog **Pengecualian Atur Cara Yang Berpotensi Tidak Dikehendaki** memaparkan senarai pengecualian yang telah ditentukan dan yang kini disahkan daripada atur cara yang berpotensi tidak dikehendaki. Anda boleh mengedit senarai, memadam item sedia ada atau menambah pengecualian baharu. Maklumat berikut boleh ditemui dalam senarai untuk setiap pengecualian tunggal:

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

### Butang kawalan

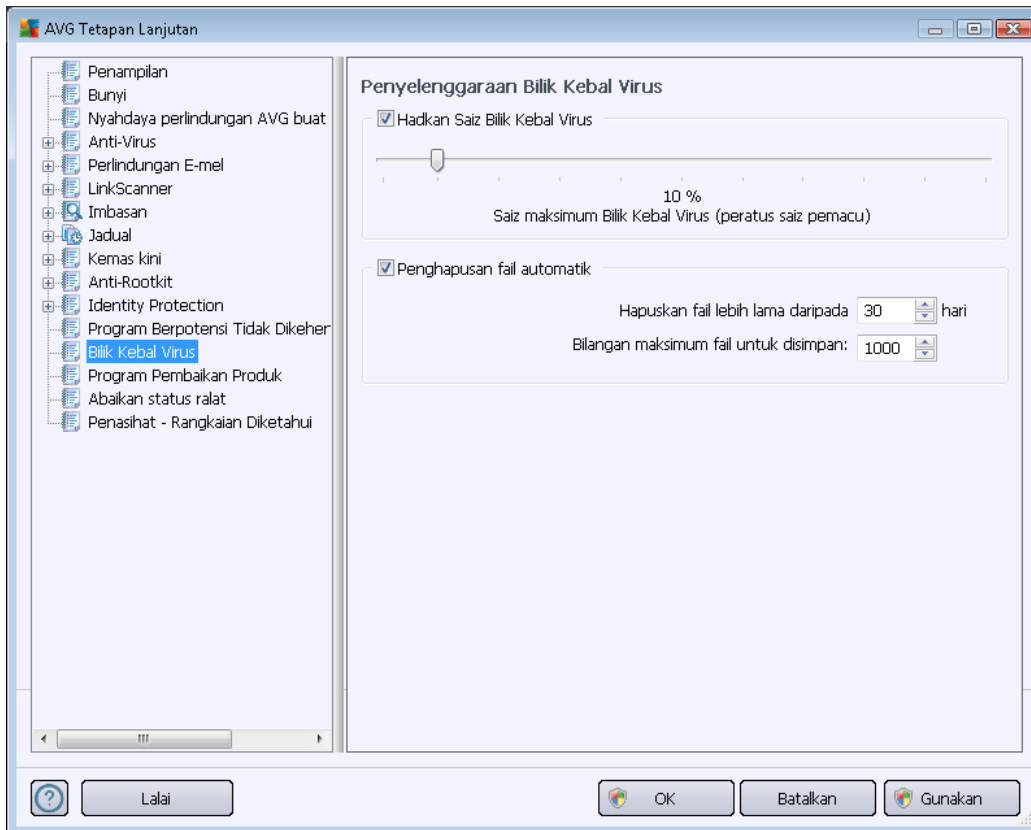
- **Edit** - membuka dialog pengeditan (*serupa dengan dialog untuk definisi pengecualian baharu, lihat di bawah*) bagi pengecualian yang sudah ditakrifkan di mana anda boleh mengubah parameter pengecualian
- **Buang** - memadam item yang dipilih dari senarai pengecualian
- **Tambah pengecualian** –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

parameter bagi pengecualian baharu untuk dicipta:



- **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. *Jika kotak semak ini bertanda, fail yang ditetapkan ditakrifkan sebagai pengecualian walau di mana ia berada (walau bagaimanapun, anda perlu mengisi laluan penuh ke fail ini juga; fail ini akan kemudiannya digunakan sebagai contoh unik bagi kemungkinan dua fail yang mempunyai nama yang sama muncul dalam sistem anda).*

### 10.13. Bilik Kebal Virus



Dialog **penyelenggaraan Bilik Kebal Virus** membenarkan anda menentukan beberapa parameter berkenaan pentadbiran objek yang disimpan dalam [Bilik Kebal Virus](#):

- **Hadkan saiz Bilik Kebal Virus** – Gunakan gelangsar untuk menyediakan saiz maksimum bagi [Bilik Kebal Virus](#). Saiz tersebut ditentukan mengikut perbandingan 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**).

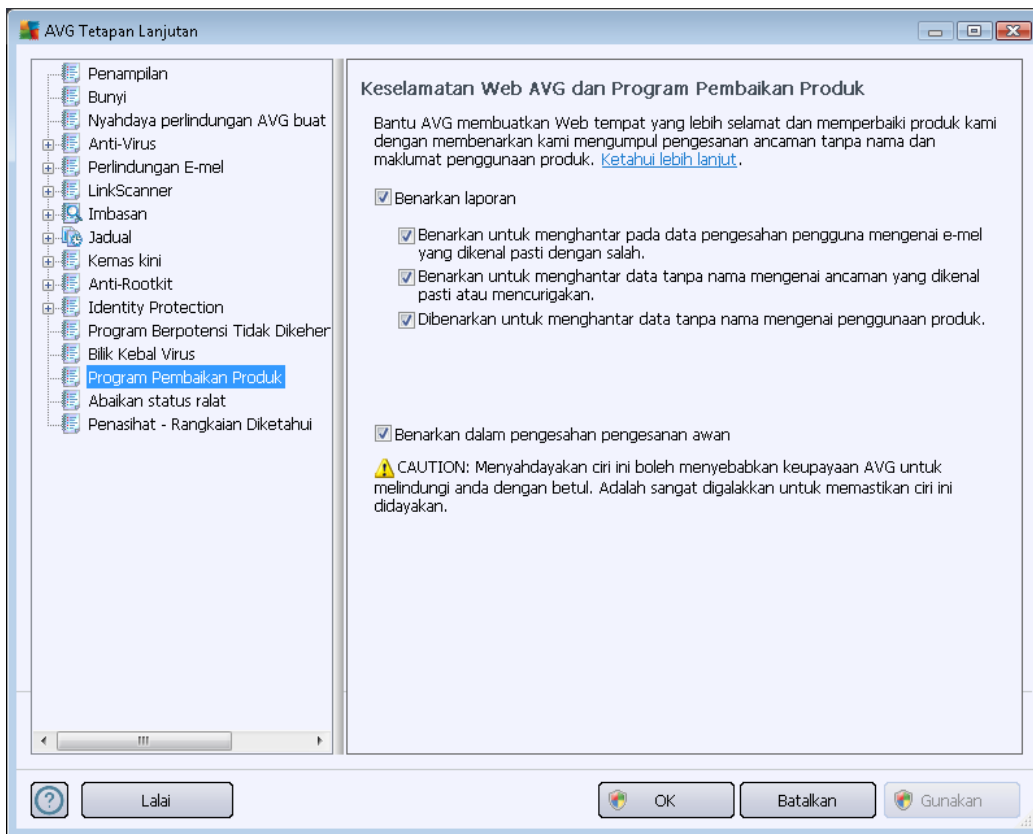
### 10.14. Program Pembaikan Produk

Dialog **Keselamatan Web AVG dan Program Pembaikan Produk** menjemput anda untuk menyertai pembaikan produk AVG, dan membantu kami meningkatkan tahap keselamatan Internet secara keseluruhan. Pastikan opsyen **Benarkan pelaporan** ditanda untuk mendayakan pelaporan ancaman yang dikesan kepada makmal AVG. Ini membantu kami mengumpulkan maklumat terbaru tentang ancaman terkini dari semua peserta di seluruh dunia, dan kami boleh sebagai balasan membaiki perlindungan untuk semua orang.

***Pelaporan diuruskan secara automatik, oleh itu tidak akan memberikan anda sebarang***



**masalah. Tiada data peribadi disertakan dalam laporan.** Melaporkan ancaman yang dikesan adalah pilihan, walau bagaimanapun, kami meminta anda terus hidupkan opsiyen ini. Ia membantu kami memperbaiki perlindungan untuk anda dan pengguna AVG lain.



Dalam dialog, opsiyen tetapan berikut tersedia:

- **Benarkan pelaporan (dihidupkan secara lalai)** - Jika anda mahu membantu kami memperbaiki **AVG Internet Security 2012** dengan lebih lanjut, biarkan kotak semak ditandakan. Ini akan membolehkan melaporkan semua ancaman yang dihadapi kepada AVG, maka kami akan dapat mengumpulkan maklumat yang terkini mengenai malware daripada semua peserta di seluruh dunia dan sebagai ganti, dapat memperbaiki perlindungan untuk semua orang. Pelaporan diuruskan secara automatik, oleh itu tidak akan memberikan anda sebarang kesulitan dan tiada data peribadi disertakan dalam laporan.
  - **Benarkan untuk menghantar data mengenai e-mel yang tidak dikenal pasti dengan betul setelah mendapat pengesahan pengguna (dihidupkan secara lalai)** – hantar maklumat mengenai mesej e-mel yang tidak dikenal pasti dengan betul sebagai spam, atau mengenai mesej spam yang tidak dikesan oleh komponen [Anti-Spam](#). Apabila menghantar maklumat jenis ini, anda akan diminta untuk pengesahan.
  - **Benarkan untuk menghantar data tanpa nama mengenai ancaman yang dikenal pasti atau mencurigakan (dihidupkan secara lalai)** – hantar maklumat



mengenai sebarang kod yang mencurigakan atau positif bahaya atau corak kelakuan (*boleh jadi virus, perisian pengintip atau halaman web berniat jahat yang anda sedang cuba akses*) dikesan pada komputer anda.

- **Benarkan untuk menghantar data tanpa nama mengenai penggunaan produk** (*dihidupkan secara lalai*) – hantar statistik asas mengenai penggunaan aplikasi, seperti bilangan pengesanan, imbasan yang dilancarkan, kemas kini yang berjaya atau gagal, dll.
- **Benarkan pengesahan awan untuk pengesanan** (*dihidupkan secara lalai*) – ancaman yang dikesan akan disemak jika benar-benar dijangkiti, untuk mengasingkan positif kesalahan.

### Ancaman paling biasa

Hari ini, terdapat lebih banyak ancaman di luar sana selain virus biasa. Penulis kod berniat jahat dan laman web merbahaya sangat berinovasi, dan ancaman jenis baharu muncul dengan kerap, dan sebahagian besarnya di Internet. Ini adalah beberapa yang paling biasa:

- **Virus** ialah kod berniat jahat yang menyalin dan menyebarkan dirinya sendiri, selalunya tidak disedari sehingga berlaku kerosakan. Sesetengah virus adalah ancaman serius, memadam atau sengaja mengubah fail dalam laluan mereka, manakala sesetengah virus melakukan sesuatu yang kelihatan tidak berbahaya, seperti memainkan muzik. Bagaimanapun, semua virus adalah berbahaya kerana keupayaan asasnya untuk berkembang – malah satu virus ringkas boleh memenuhi memori komputer sekelip mata, dan menyebabkan kerosakan.
- **Cecacing** ialah satu subkategori virus yang mana, tidak seperti virus normal, tidak memerlukan objek "pembawa" untuk melampirkannya; ia menghantar dirinya sendiri kepada komputer lain sendiri, selalunya melalui e-mel, dan hasilnya selalu melebihi bebas pelayan e-mel dan sistem rangkaian.
- **Perisian Pengintip** selalunya ditakrifkan sebagai kategori malware (*malware = sebarang perisian berniat jahat, termasuk virus*) atur cara melingkungi – biasanya kuda Trojan – disasarkan untuk mencuri maklumat peribadi, kata laluan, nombor kad kredit, atau mencerobohi komputer dan membenarkan penyerang mengawalnya dari jauh; sudah pasti, semuanya tanpa pengetahuan atau kebenaran pemilik komputer.
- **Program berpotensi tidak dikehendaki** adalah sejenis perisian pengintip yang boleh tetapi tidak semestinya merbahaya kepada komputer anda. Contoh khusus PUP adalah adware, perisian yang direka untuk mengedarkan pengiklanan, biasanya dengan memaparkan pop muncul iklan; mengganggu, tetapi tidak benar-benar berbahaya.
- **Kuki penjejakan** boleh dianggap sebagai sejenis perisian pengintip, memandangkan fail kecil ini, disimpan dalam penyemak imbas web dan dihantar secara automatik kepada laman web "induk" apabila anda melawatnya lagi, boleh mengandungi data seperti sejarah pelayaran anda dan maklumat serupa yang lain.
- **Eksplit** adalah kod berniat jahat yang cuba mengambil kesempatan dari kekurangan atau kelemahan dalam sistem pengendalian, penyemak imbas Internet, atau atur cara penting



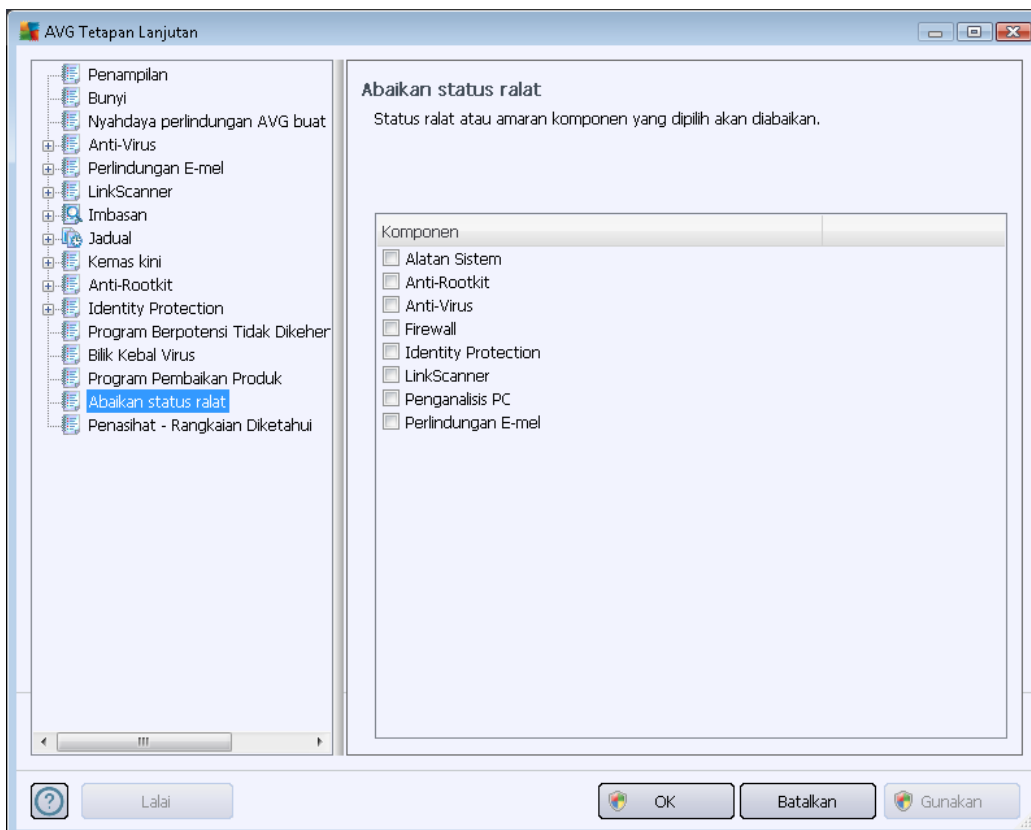
lain.

- **Pemancingan data** adalah percubaan untuk mendapatkan data peribadi sensitif dengan menyamar sebagai organisasi yang dipercayai dan terkenal. Biasanya, mangsa berpotensi dihubungi melalui e-mel palsu meminta mereka untuk cthnya. mengemas kini butiran akaun bank mereka. Untuk melakukan itu, mereka dijemput mengikuti pautan yang diberikan yang kemudiannya membawa kepada laman web palsu bank itu.
- **Penipuan adalah e-mel besar mengandungi maklumat berbahaya, merisaukan atau cuma mengganggu dan tidak berguna.** Kebanyakan daripada ancaman di atas menggunakan mesej e-mel palsu untuk disebarkan.
- **Laman web berniat jahat** adalah yang akan dengan sengaja memasang perisian berniat jahat pada komputer anda, dan laman yang digodam juga berbuat begitu, cuma ini adalah laman web sah yang telah dikompromi untuk menjangkiti pelawat.

**Untuk melindungi anda dari semua jenis ancaman berbeza ini, AVG Internet Security 2012 memasukkan komponen yang dikhususkan. Untuk penerangan ringkas mengenai perkara ini, sila rujuk bab [Gambaran Keseluruhan Komponen](#).**

## 10.15. Abaikan status ralat

Dalam dialog **Abaikan status ralat** anda boleh menanda komponen yang anda tidak mahu dimaklumkan:







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 (*Abaikan keadaan komponen*) juga tersedia untuk komponen khusus secara terus dari gambaran keseluruhan komponen [dalam tettingkap utama AVG](#).

## 10.16. Penasihat – Rangkaian Diketahui

[Penasihat AVG](#) menyertakan ciri yang mengawasi rangkaian yang anda sambungkan dan jika rangkaian baharu ditemui (*dengan nama rangkaian yang sudah digunakan, yang boleh menyebabkan kekeliruan*) ia akan memberitahu anda dan mengesyorkan supaya anda menyemak keselamatan rangkaian. Jika anda memutuskan bahawa rangkaian baharu itu adalah selamat untuk disambungkan, anda juga boleh menyimpannya pada senarai ini; [Penasihat AVG](#) kemudiannya akan mengingatkan atribut unik rangkaian tersebut (*terutamanya alamat MAC*) dan tidak akan memaparkan pemberitahuan kali berikutnya.

Dalam tettingkap dialog ini, anda boleh menyemak rangkaian mana yang telah anda simpan sebelum ini sebagai diketahui. Anda boleh memadam masukan individu dengan menekan butang **Keluarkan**; rangkaian yang berkenaan akan dianggap tidak diketahui dan berkemungkinan tidak selamat sekali lagi.

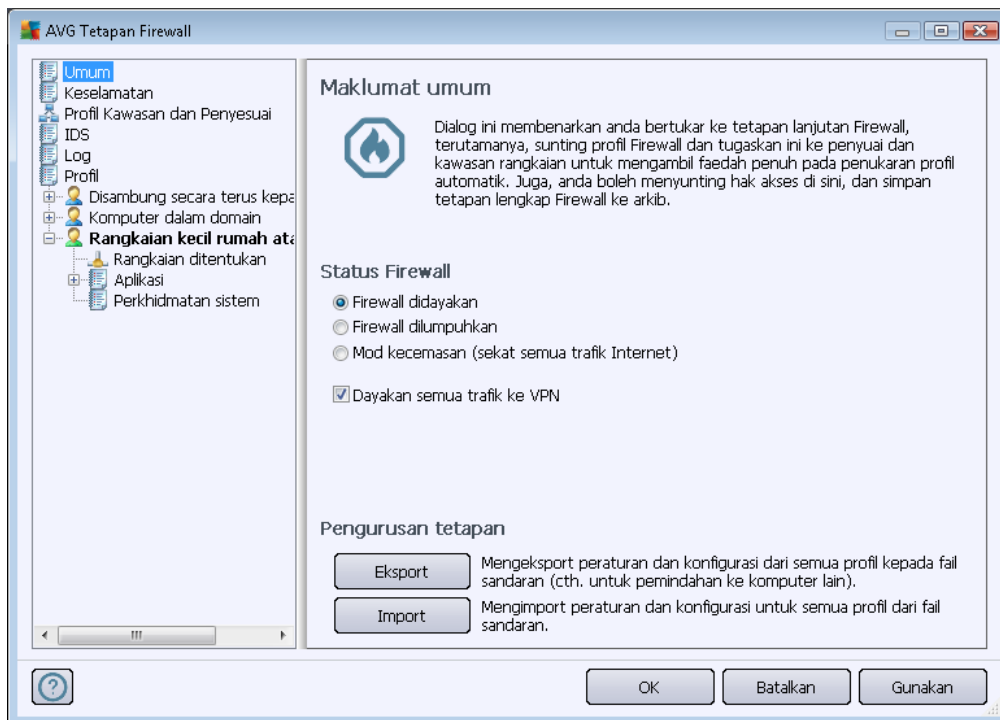
## 11. Tetapan Firewall

Konfigurasi [Firewall](#) membuka tettingkap baharu di mana beberapa dialog boleh menyediakan parameter yang sangat canggih bagi komponen.

**Walau bagaimanapun, vendor perisian telah menyediakan semua komponen AVG Internet Security 2012 untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi lalai. Sebarang pertukaran kepada tetapan harus dilakukan hanya oleh pengguna berpengalaman sahaja!**

### 11.1. Umum

Dialog *Maklumat umum* dibahagikan kepada dua bahagian:



### Status Firewall

Dalam bahagian *Status Firewall* anda boleh menukar status [Firewall](#) mengikut keperluan:

- **Firewall didayakan** – pilih opsiyen ini untuk membenarkan komunikasi kepada aplikasi tersebut yang diperuntukkan sebagai 'dibenarkan' dalam set peraturan yang ditakrifkan dalam [profil Firewall](#) yang dipilih.
- **Firewall dinyahdayakan** – pilihan ini mematikan [Firewall](#) sepenuhnya, semua lalu lintas rangkaian dibenarkan tetapi tidak diperiksa!
- **Mod kecemasan (sekat semua lalu lintas Internet)** – pilih opsiyen ini untuk menyekat



semua lalu lintas pada setiap port rangkaian tunggal; [Firewall](#) masih dijalankan tetapi semua lalu lintas rangkaian dihentikan.

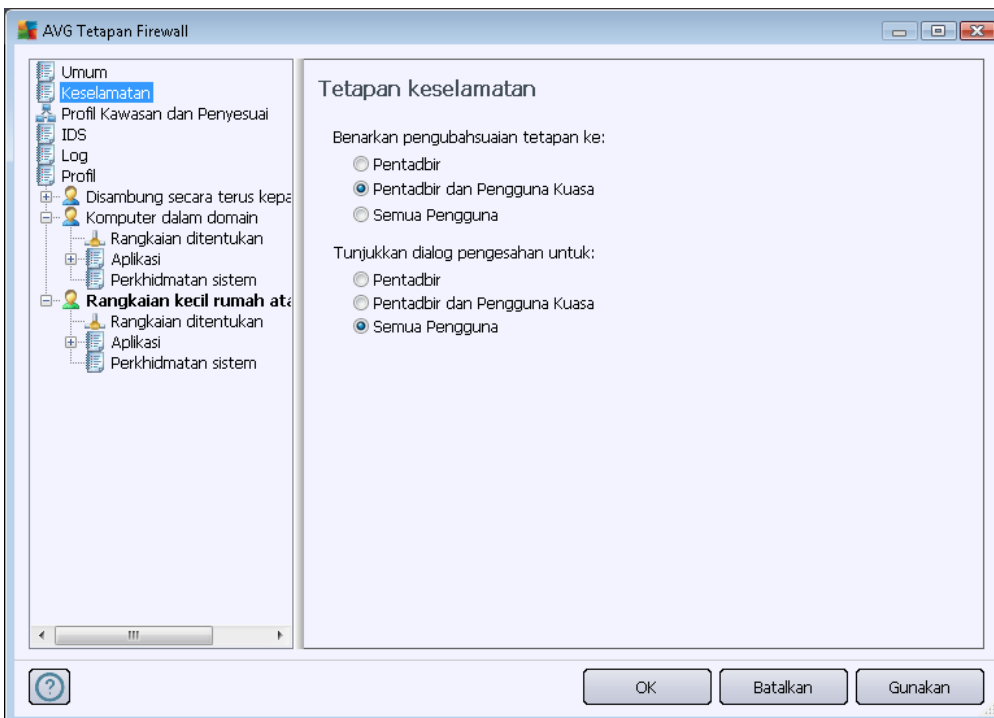
- **Dayakan semua lalu lintas ke VPN (dihidupkan secara lalai)** – jika anda menggunakan sambungan VPN (*Rangkaian Persendirian Maya*), cth. untuk menyambung ke pejabat anda dari rumah, kami mengesyorkan untuk menanda kotak. **AVG Firewall** akan mencari secara automatik melalui penyesuai rangkaian anda, cari yang digunakan untuk sambungan VPN, dan membenarkan semua aplikasi untuk menyambung ke rangkaian sasaran (*hanya digunakan pada aplikasi tanpa peraturan Firewall khusus diperuntukkan*) Pada sistem standard dengan penyesuai rangkaian biasa, langkah mudah ini sepatutnya menyelamatkan anda daripada perlu menyediakan peraturan terperinci untuk setiap aplikasi yang anda perlu gunakan pada VPN.

**Nota:** Untuk mendayakan sambungan VPN, anda perlu membenarkan komunikasi kepada protokol sistem berikut: GRE, ESP, L2TP, PPTP. Ia boleh dilakukan dalam dialog [Perkhidmatan sistem](#).

## Pengurusan tetapan

Dalam seksyen **Pengurusan tetapan** anda boleh **Eksport** atau **Import** konfigurasi [Firewall](#); iaitu eksport peraturan [Firewall](#) yang ditentukan dan tetapan kepada fail sandaran, atau sebaliknya, untuk mengimport seluruh fail sandaran.

## 11.2. Keselamatan



Dalam dialog **Tetapan keselamatan** anda boleh menentukan peraturan am bagi kelakuan [Firewall](#)



tidak kira profil yang dipilih:

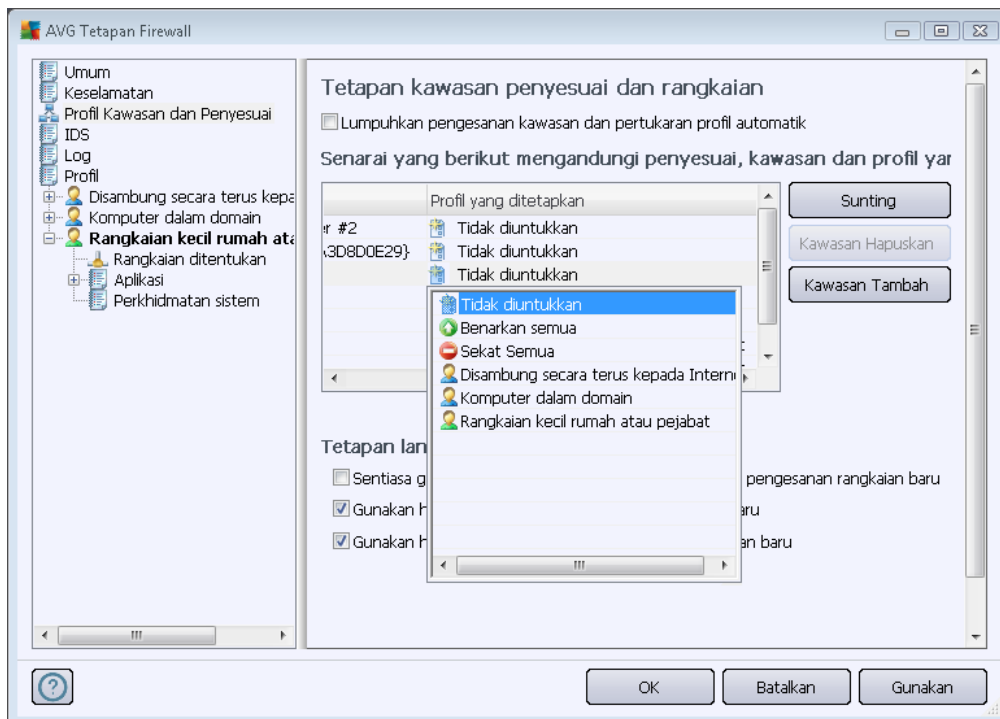
- **Benarkan pengubahsuaian kepada** – tentukan siapa dibenarkan untuk mengubah konfigurasi [Firewall](#).
- **Tunjukkan dialog pengesahan untuk** – tentukan kepada siapa dialog pengesahan (*dialog yang meminta keputusan dalam situasi yang tidak diliputi oleh peraturan [Firewall](#)*) harus dipaparkan.

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.
- **Pentadbir dan Pengguna Berkuasa** – pentadbir boleh menguntukkan mana-mana pengguna ke dalam kumpulan tertentu (*Pengguna Berkuasa*) dan menentukan kuat kuasa bagi ahli kumpulan.
- **Semua Pengguna** – pengguna lain tidak diperuntukkan ke dalam sebarang kumpulan tertentu.

### 11.3. Profil Kawasan dan Penyesuai

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



- **Nyahdaya pengesanan kawasan dan pertukaran profil automatik (dimatikan secara lalai)** - salah satu profil yang ditakrifkan boleh diperuntukkan kepada setiap jenis antara muka rangkaian kepada setiap kawasan masing-masing. Jika anda tidak mahu mentakrifkan profil khusus, satu profil sama 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 opsiyen **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 kiri item masing-masing dalam senarai penyesuai (*dalam lajur profil yang Diperuntukkan*), dan pilih profil dari menu konteks.

### Tetapan lanjutan

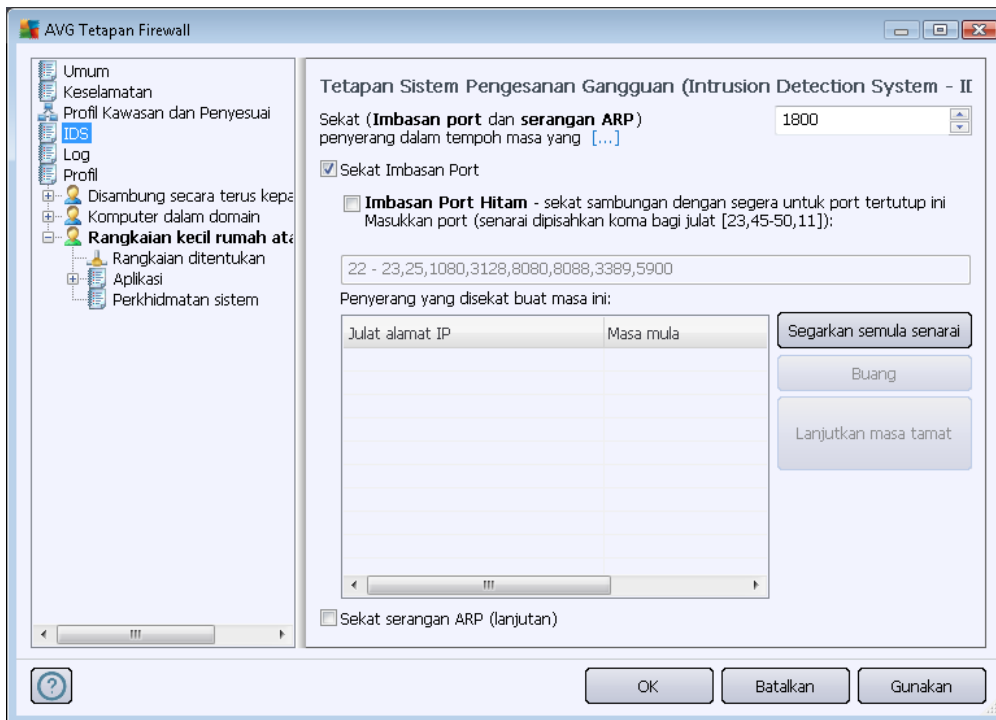
- **Sentiasa gunakan profil lalai dan jangan paparkan dialog pengesanan rangkaian baharu** – apabila komputer anda menyambung kepada rangkaian baharu, [Firewall](#) akan memberi amaran kepada anda dan memaparkan dialog yang menggesa anda untuk memilih jenis sambungan rangkaian, dan menguntukkannya [profil Firewall](#). Jika anda tidak mahu dialog dipaparkan, tandakan kotak ini.
- **Guna heuristik AVG untuk pengesanan rangkaian baharu** - Membolehkan pengumpulan maklumat mengenai rangkaian yang baharu dikesan dengan mekanisme AVG sendiri (*walaupun bagaimanapun, opsiyen ini hanya tersedia pada*

VISTA OS, dan lebih tinggi).

- o **Penggunaan heuristik Microsoft untuk pengesanan rangkaian baharu** - Membolehkan pengambilan maklumat mengenai rangkaian yang baru dikesan dari perkhidmatan Windows (opsyen ini hanya terdapat pada Windows Vista dan lebih tinggi).

#### 11.4. IDS

Sistem Pengesanan Gangguan adalah ciri analisis kelakuan khas yang direka bentuk untuk mengenal pasti dan menghalang cubaan komunikasi mencurigakan pada port khusus bagi komputer anda. Anda boleh mengkonfigurasi parameter IDS dalam dialog **tetapan Sistem Pengesanan Gangguan (IDS)** :



Dialog **tetapan Sistem Pengesanan Gangguan (IDS)** menawarkan opsi konfigurasi berikut:

- **Halang penyerang untuk tempoh masa yang ditentukan** – Di sini anda boleh menetapkan untuk berapa banyak saat sesuatu port harus dihalang, apabila cubaan komunikasi mencurigakan dikesan padanya. Secara lalai, selang masa ditetapkan ke 1800 saat (30 minit).
- **Halang Imbasan Port (dihidupkan secara lalai)** – Tandakan kotak untuk menghalang cubaan komunikasi pada semua port TCP dan UDP masuk ke komputer dari luar. Untuk sebarang sambungan tersebut, lima cubaan dibenarkan, dan yang ke-enam dihalang. Item dihidupkan secara lalai, dan adalah disyorkan untuk mengekalkan tetapan ini. Jika anda menghidupkan opsi **Halang Imbasan Port**, beberapa konfigurasi terperinci selanjutnya tersedia (jika tidak, item berikut akan dinyahaktifkan):

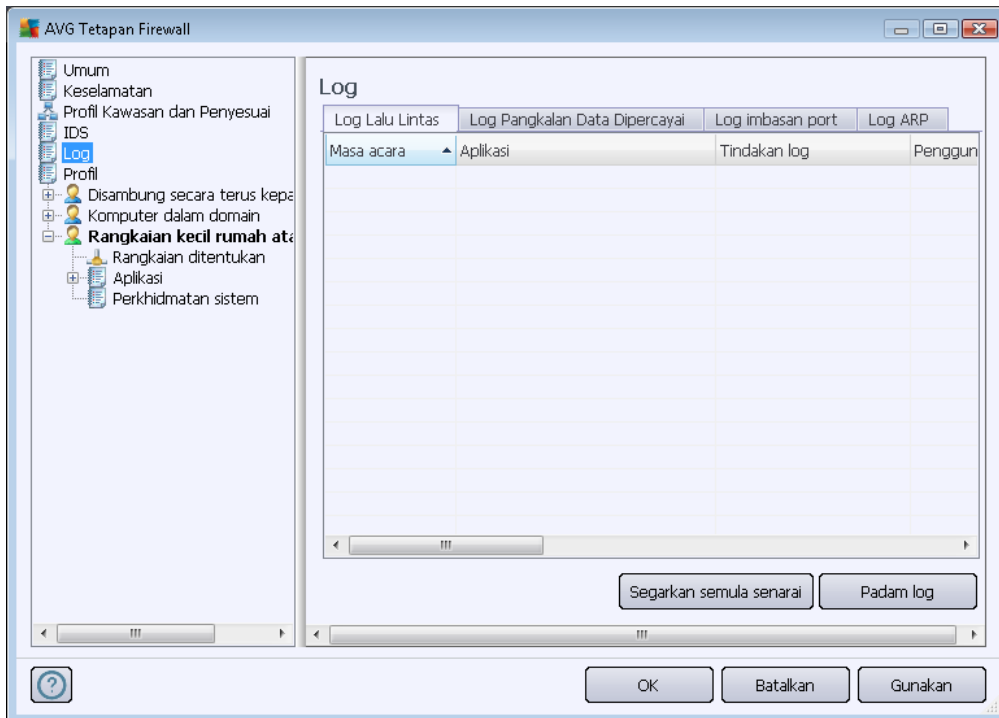


- **Imbasan Port Hitam** – Tandakan kotak untuk dengan serta-merta menghalang sebarang cubaan komunikasi pada port yang ditentukan dalam medan teks di bawah. Port individu atau julat port harus dibahagikan dengan koma. Terdapat senarai yang dipratetap bagi port yang disyorkan sekiranya anda hendak menggunakan ciri ini.
- Penyerang yang dihalang buat masa ini – Seksyen ini menyenaraikan sebarang cubaan komunikasi yang sedang dihalang oleh [Firewall](#). Sejarah lengkap bagi cubaan yang dihalang boleh dilihat dalam dialog [Log](#) (*tab Log imbasan Port*).
- **Halang serangan ARP (lanjutan) (dimatikan secara lalai)** - Tandakan pilihan ini untuk mengaktifkan halangan jenis khas cubaan komunikasi di dalam rangkaian setempat yang dikesan oleh **IDS** sebagai berkemungkinan berbahaya. Masa yang ditetapkan dalam **Halang penyerang dalam tempoh masa tertentu** digunakan. Kami mengesyorkan hanya pengguna lanjutan yang biasa dengan jenis dan tahap risiko bagi rangkaian tempatan mereka, menggunakan ciri ini.

### Butang kawalan

- **Segar semula senarai** – tekan butang ini untuk mengemas kini senarai (*untuk memasukkan sebarang cubaan dihalang yang terkini*)
- **Buang** - tekan untuk membatalkan halangan yang dipilih
- **Lanjutkan masa rehat** – tekan untuk memanjangkan tempoh masa di mana cubaan yang dipilih dihalang. Dialog baharu dengan opsi yang dilanjutkan akan muncul, membolehkan anda menetapkan masa dan tarikh tertentu, atau tempoh tanpa had.

## 11.5. Log



Dialog **Log** membenarkan anda untuk meneliti senarai semua tindakan **Firewall** yang dilog dan peristiwa dengan penerangan terperinci bagi parameter berkaitan (*waktu peristiwa, nama aplikasi, tindakan log masing-masing, nama pengguna, PID, arah lalu lintas, jenis protokol, bilangan port jauh dan tempatan, dll.*) pada empat 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 baharu 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.
- **Log imbasan port** – menyediakan log bagi semua aktiviti [Sistem Pengesanan Gangguan](#).
- **Log ARP** – maklumat log mengenai halangan jenis cubaan komunikasi istimewa di dalam rangkaian tempatan (opsyen [Halang serangan ARP](#)) yang dikesan oleh [Sistem Pengesanan Gangguan](#) sebagai berpotensi berbahaya.

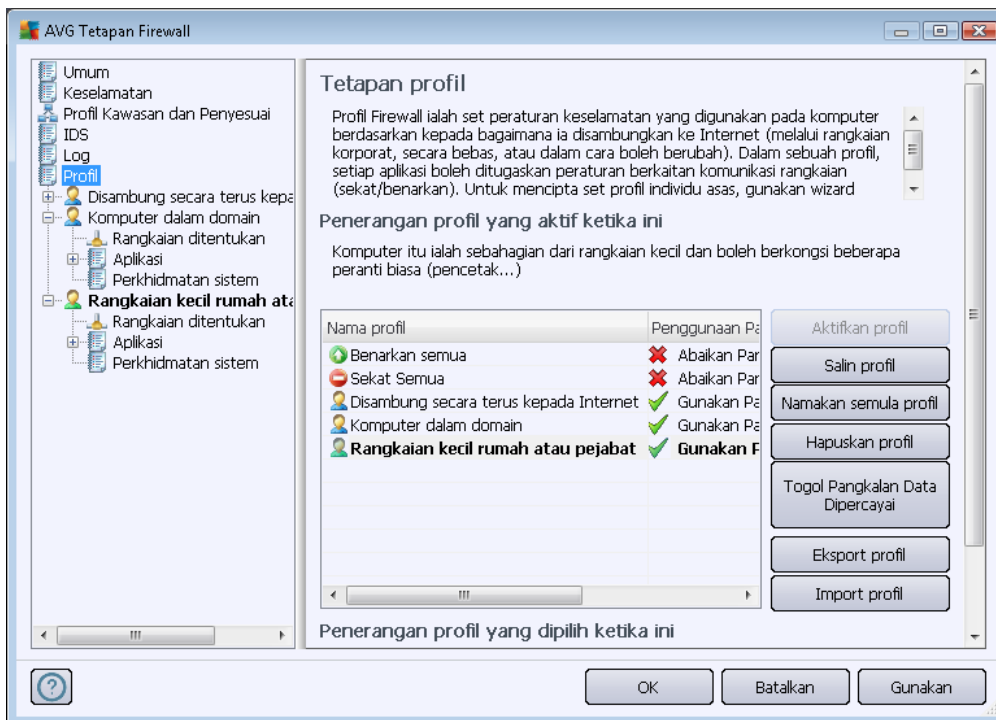


## Butang kawalan

- **Muat semula senarai** - semua parameter yang dilog boleh diatur mengikut atribut yang dipilih: mengikut kronologi (*tarikh*) atau mengikut abjad (*lajur lain*) – cuma klik pengepala lajur masing-masing. Guna butang **Muat semula senarai** untuk mengemas kini maklumat yang sedang dipaparkan.
- **Padam log** - Tekan untuk memadam semua entri dalam carta.

## 11.6. Profil

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



Profil sistem (*Benarkan semua, Halang semua*) tidak boleh diedit. Walau bagaimanapun, semua [profil](#) (*Secara terus, disambungkan ke Internet, Komputer dalam domain, Rangkaian rumah kecil atau pejabat*) kemudiannya, boleh diedit di 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 baharu berdasarkan pada salinan pendua asal.
- **Namakan semula profil** – Membenarkan anda menentukan nama yang baharu untuk profil

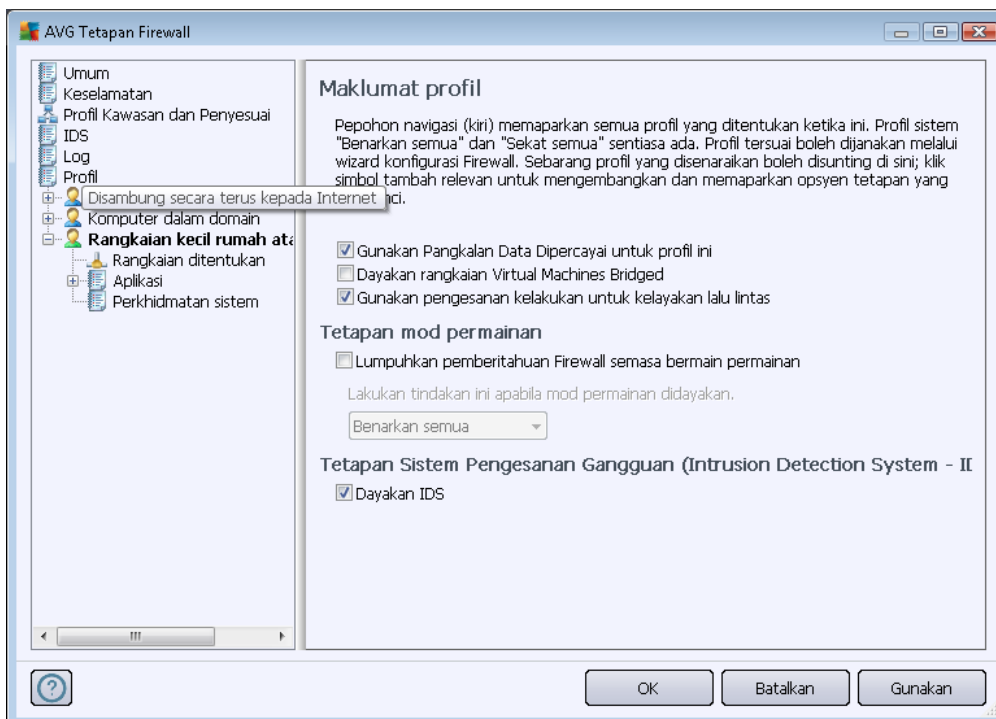
yang dipilih.

- **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 pangkalan data dalaman AVG yang mengumpulkan data mengenai aplikasi yang dipercayai dan diperakui yang sentiasa boleh dibenarkan untuk berkomunikasi dalam talian.*).
- **Eksport profil** – Merekod 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.

Dalam bahagian bawah dialog, anda boleh menemui penerangan profil yang dipilih dalam senarai di atas buat masa ini.

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

### 11.6.1. Maklumat Profil



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



- **Gunakan Pangkalan Data yang Dipercayai untuk profil ini** (dihidupkan secara lalai) – Tandakan opsi untuk mengaktifkan *Pangkalan Data yang Dipercayai* (iaitu pangkalan data dalaman AVG yang mengumpul maklumat mengenai aplikasi yang dipercayai dan diperakui yang berkomunikasi dalam talian. Jika tiada peraturan yang ditentukan untuk aplikasi tersebut lagi, adalah perlu untuk mengetahui sama ada aplikasi boleh diberikan akses kepada rangkaian. AVG mencari Pangkalan Data yang Dipercayai dan jika aplikasi disenaraikan, ia dikira selamat dan akan dibenarkan untuk berkomunikasi pada rangkaian. Jika tidak, anda akan dijemput untuk menentukan sama ada aplikasi harus dibenarkan untuk berkomunikasi pada rangkaian) untuk profil tersebut
- **Dayakan rangkaian Jejambat Mesin Maya** – (dimatikan secara lalai) – Tandakan item ini untuk membenarkan mesin maya dalam VMware menyambung secara terus ke rangkaian.
- **Gunakan pengesanan kelakuan untuk kelayakan lalu lintas** - (dihidupkan secara lalai) tandakan pilihan ini untuk membenarkan [Firewall](#) menggunakan kefungisian [Identity Protection](#) semasa menilai aplikasi – [Identity Protection](#) 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 memutuskan dan mengesahkan dengan menanda item masing-masing sama ada anda mahukan mesej maklumat [Firewall](#) dipaparkan walaupun semasa aplikasi skrin penuh sedang dijalankan pada komputer anda (*biasanya, ini adalah permainan, tetapi, digunakan pada sebarang aplikasi skrin penuh, cth. pembentangan PPT*), memandangkan mesej maklumat boleh menjadi agak mengganggu.

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.

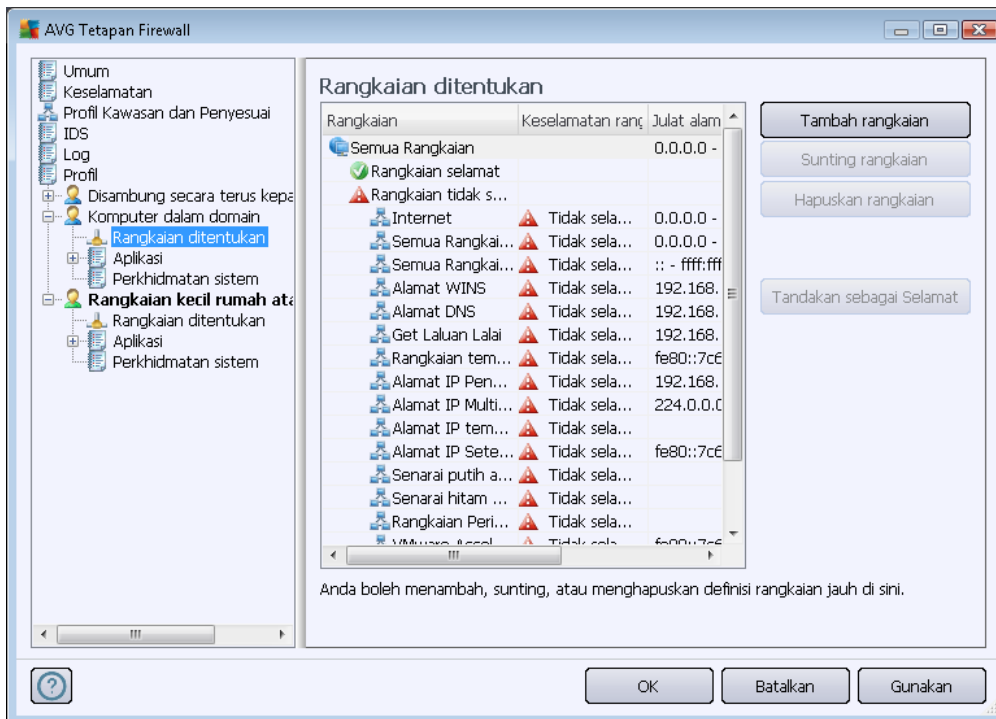
Dengan mod permainan dibuka, semua tugas yang dijadualkan (*imbasan, kemas kini*) ditangguhkan sehingga aplikasi ini ditutup.

### Tetapan Sistem Pengesanan Gangguan (Intrusion Detection System – IDS)

andakan kotak semak **Dayakan IDS** untuk mengaktifkan ciri analisis tingkah laku istimewa yang direka bentuk untuk mengenal pasti dan menghalang cubaan komunikasi mencurigakan melalui port tertentu komputer anda (*untuk butiran mengenai tetapan ciri ini rujuk bab [IDS](#) dokumentasi ini*).

## 11.6.2. Rangkaian yang Ditetapkan

Dialog *Rangkaian yang ditakrifkan* menawarkan senarai semua rangkaian yang komputer anda disambungkan.

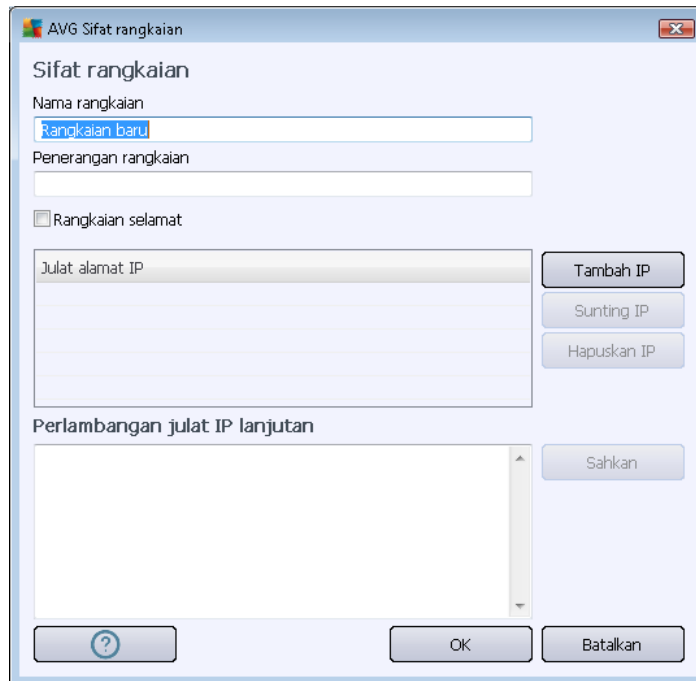


Senarai tersebut memberikan maklumat berikut pada setiap rangkaian yang dikesan:

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

### Butang kawalan

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

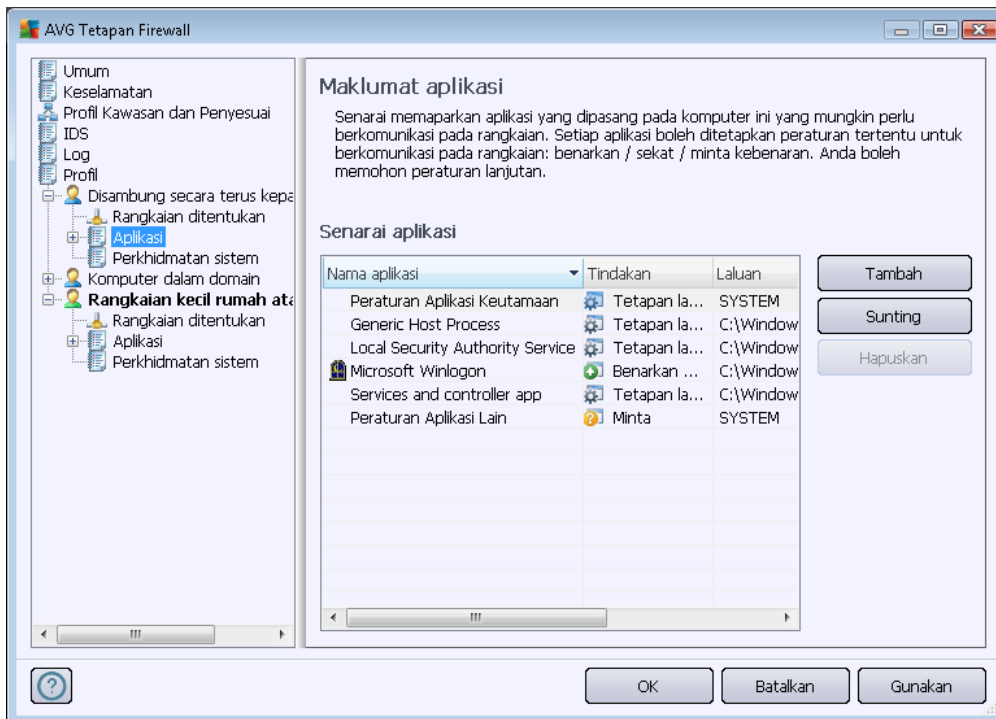


Dalam dialog ini, anda boleh menentukan ***Nama rangkaian***, berikan ***Penerangan rangkaian*** dan berkemungkinan peruntukkan rangkaian sebagai selamat. Rangkaian baharu boleh menjadi sama ada ditakrifkan secara manual dalam dialog persendirian yang dibuka melalui butang ***Tambah IP*** (secara alternatif ***Edit IP / Padam IP***), dalam dialog ini anda boleh menentukan rangkaian dengan memberikan julat atau topeng IP. Untuk sebilangan besar rangkaian yang harus ditakrifkan sebagai sebahagian daripada rangkaian yang baru dibuat, anda boleh menggunakan opsiyen ***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 baharu, lihat penerangan dalam perenggan sebelumnya*).
- ***Padam rangkaian*** – Membuang nota rangkaian yang dipilih daripada senarai rangkaian.
- ***Tandakan sebagai selamat*** – Secara lalai, semua rangkaian dikira tidak selamat, dan hanya jika anda pasti rangkaian masing-masing adalah selamat, anda boleh menggunakan butang ini untuk menguntukkannya (*dan sebaliknya, sebaik sahaja rangkaian diperuntukkan sebagai selamat, teks butang bertukar kepada "Tandakan sebagai tidak selamat"*).

### 11.6.3. Aplikasi

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



Aplikasi dalam **Senarai aplikasi** adalah yang dikesan pada komputer anda (*dan tindakan yang diuntukkan masing-masing*). Jenis tindakan berikut boleh digunakan:

-  - Benarkan komunikasi untuk semua rangkaian
-  - Benarkan komunikasi untuk rangkaian yang ditentukan sebagai Selamat sahaja
-  - Sekat komunikasi
-  - Paparkan dialog tanya (*pengguna akan dapat membuat keputusan sama ada untuk membenarkan atau menyekat komunikasi apabila aplikas cuba untuk berkomunikasi melalui rangkaian*)
-  - Tetapan lanjutan ditentukan

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



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

Selain dari aplikasi, senarai juga mengandungi dua item khas:

- **Keutamaan Peraturan Aplikasi** (di bahagian atas senarai) adalah keutamaan dan sentiasa digunakan sebelum peraturan bagi sebarang aplikasi individu.
- **Peraturan Aplikasi Lain** (di bahagian bawah senarai) digunakan sebagai "contoh terakhir", apabila tiada peraturan aplikasi khusus yang digunakan, cth. untuk aplikasi yang tidak diketahui dan tidak ditakrifkan. Pilih tindakan yang patut dicetuskan apabila aplikasi sedemikian cuba berkomunikasi melalui rangkaian:
  - *Halang* – komunikasi akan sentiasa dihalang.
  - *Benarkan* – komunikasi akan dibenarkan melalui sebarang rangkaian.
  - *Tanya* – anda akan dijemput untuk menentukan sama ada komunikasi harus dibenarkan atau dihalang.

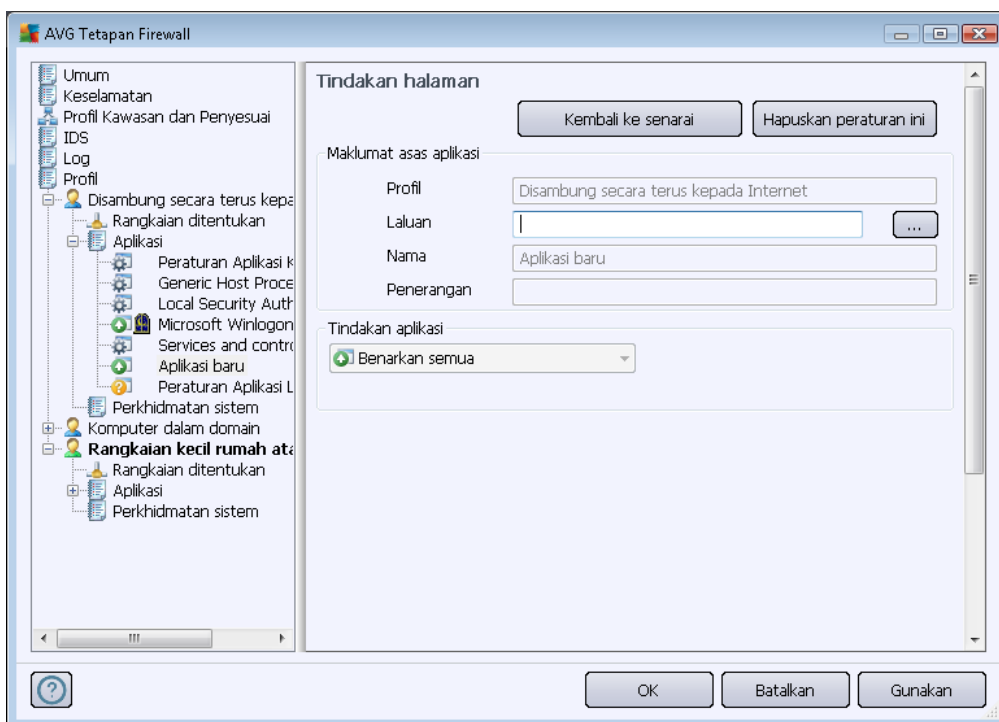
***Item ini mempunyai beberapa opsyen tetapan berbeza dari aplikasi biasa, dan hanya ditujukan untuk pengguna berpengalaman. Kami amat mengesyorkan untuk anda mengubah suai tetapan!***

### **Butang kawalan**

Senarai boleh diedit dengan menggunakan butang kawalan berikut:

- **Tambah** – Buka dialog [Tindakan Halaman](#) kosong untuk menentukan peraturan aplikasi baharu.
- **Edit** - Buka dialog [Tindakan Halaman](#) dengan data yang diberikan untuk pengeditan set peraturan aplikasi sedia ada.
- **Padam** - Membuang aplikasi yang dipilih daripada senarai.

Dalam dialog **Tindakan halaman**, anda boleh mentakrifkan tetapan untuk aplikasi tertentu secara terperinci:



### Butang kawalan

Dua butang kawalan tersedia di bahagian atas dialog:

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

### Maklumat asas aplikasi

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






### Tindakan aplikasi

Dalam menu jatuh bawah, anda boleh memilih peraturan [Firewall](#) untuk aplikasi, cth. apa [Firewall](#)





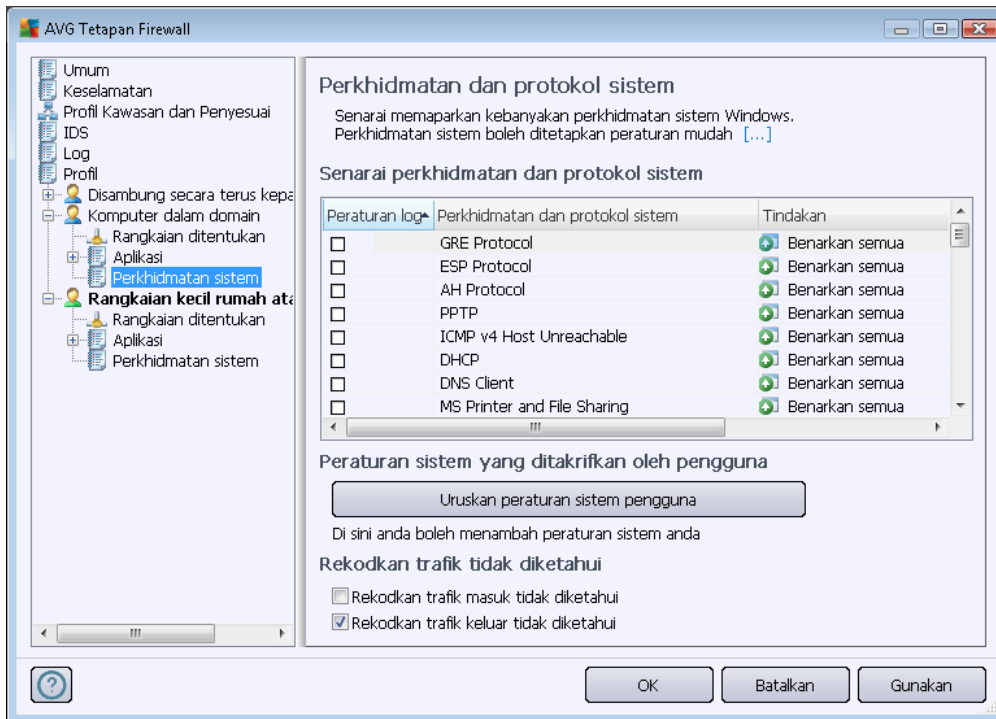
patut lakukan apabila aplikasi cuba berkomunikasi pada rangkaian:

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

#### 11.6.4. Perkhidmatan Sistem




***Sebarang pengeditan dalam dialog perkhidmatan dan protokol sistem yang bertujuan untuk PENGGUNA YANG BERPENGALAMAN SAHAJA!***

Dialog **Perkhidmatan dan protokol sistem** menyenaraikan perkhidmatan dan protokol piawai Windows yang mungkin diperlukan untuk berkomunikasi pada rangkaian:



## Senarai perkhidmatan dan protokol sistem

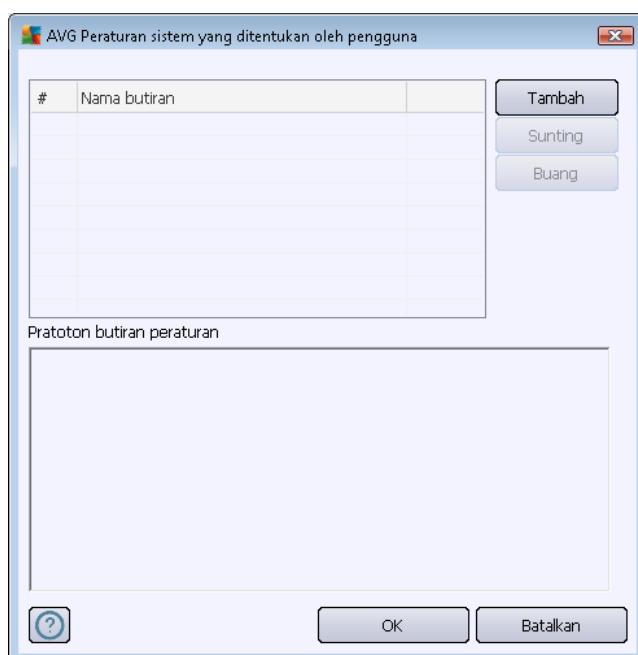
Carta terdiri daripada lajur berikut:

- **Tindakan peraturan log** – Kotak ini membolehkan anda menghidupkan rakaman setiap aplikasi peraturan dalam [log](#).
- **Perkhidmatan dan protokol sistem** – Lajur ini menunjukkan nama perkhidmatan sistem masing-masing.
- **Tindakan** – Lajur ini memaparkan ikon untuk tindakan yang diperuntukkan:
  -  Benarkan komunikasi untuk semua rangkaian
  -  Benarkan komunikasi untuk rangkaian yang ditentukan sebagai Selamat sahaja
  -  Sekat komunikasi
- **Rangkaian** - Lajur ini menyatakan pada rangkaian tertentu mana peraturan sistem digunakan

Untuk mengedit tetapan bagi sebarang item dalam senarai (*termasuk tindakan diperuntukkan*), klik kanan item dan pilih **Edit**. **Walau bagaimanapun, pengeditan peraturan sistem harus dilakukan oleh pengguna lanjutan sahaja; ia amat disyorkan untuk tidak mengedit peraturan sistem!**

### Peraturan sistem yang ditakrifkan oleh pengguna

Untuk membuka dialog baru untuk menentukan peraturan perkhidmatan sistem anda sendiri (*lihat gambar di bawah*), tekan butang **Uruskan peraturan sistem pengguna**. Bahagian atas bagi dialog **Peraturan sistem yang ditakrif pengguna** memaparkan gambaran keseluruhan bagi semua butiran bagi peraturan sistem yang diedit, bahagian bawah kemudiannya, memaparkan butiran yang dipilih. Butiran peraturan yang ditentukan pengguna boleh diedit, ditambah, atau dipadam dengan butang masing-masing; butiran ditentukan pengilang hanya boleh diedit:



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

### Rekodkan trafik tidak diketahui

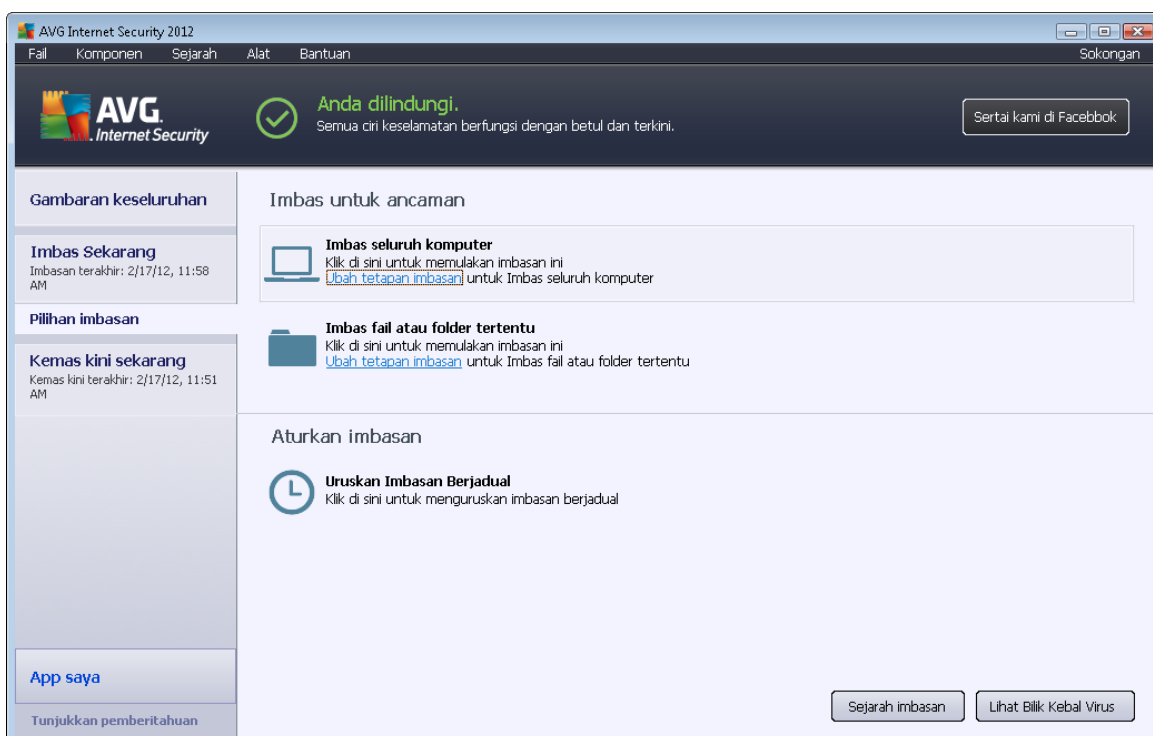
- **Log trafik masuk tidak diketahui (dimatikan secara lalai)** – Tandakan kotak ini untuk merekodkan dalam [Log](#) setiap percubaan tidak diketahui untuk menyambung ke komputer anda dari luar.
- **Log trafik masuk tidak diketahui (dihidupkan secara lalai)** – Tandakan kotak ini untuk merekodkan dalam [Log](#) setiap percubaan tidak diketahui dari komputer anda untuk menyambung ke lokasi luar.



## 12. Pengimbasan AVG

Secara lalai, **AVG Internet Security 2012** tidak menjalankan sebarang imbasan, seperti selepas yang permulaan, anda hendaklah dilindungi dengan sempurna oleh komponen residen bagi **AVG Internet Security 2012** yang sentiasa mengawal, dan tidak membenarkan sebarang kod berniat jahat memasuki komputer anda langsung. Sudah tentu, anda boleh [menjadualkan imbasan untuk dijalankan pada selang masa tetap, atau secara manual, melancarkan imbasan mengikut keperluan anda pada bila-bila masa.](#)

### 12.1. Antara Muka Pengimbasan



Antara muka pengimbasan AVG boleh diakses melalui [pautan pantas opsyen Imbasan](#). 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:
  - [Imbasan seluruh komputer](#)
  - [Imbas fail atau folder tertentu](#)
- [Bahagian](#) imbasan jadual – di mana anda boleh mentakrifkan ujian baru dan membuat jadual baru seperti yang diperlukan.



## Butang kawalan

Butang kawalan tersedia dalam antara muka pengujian adalah yang berikut:

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

## 12.2. Imbasan Pratakrif

Salah satu ciri utama bagi **AVG Internet Security 2012** adalah pengimbasan dalam permintaan. Ujian dalam permintaan direka bentuk untuk mengimbas pelbagai bahagian komputer anda apabila kecurigaan bagi kemungkinan jangkitan virus berlaku. Walau bagaimanapun, ia amat disarankan untuk menjalankan ujian seperti itu secara tetap walaupun jika anda merasakan tiada virus yang boleh ditemui pada komputer anda.

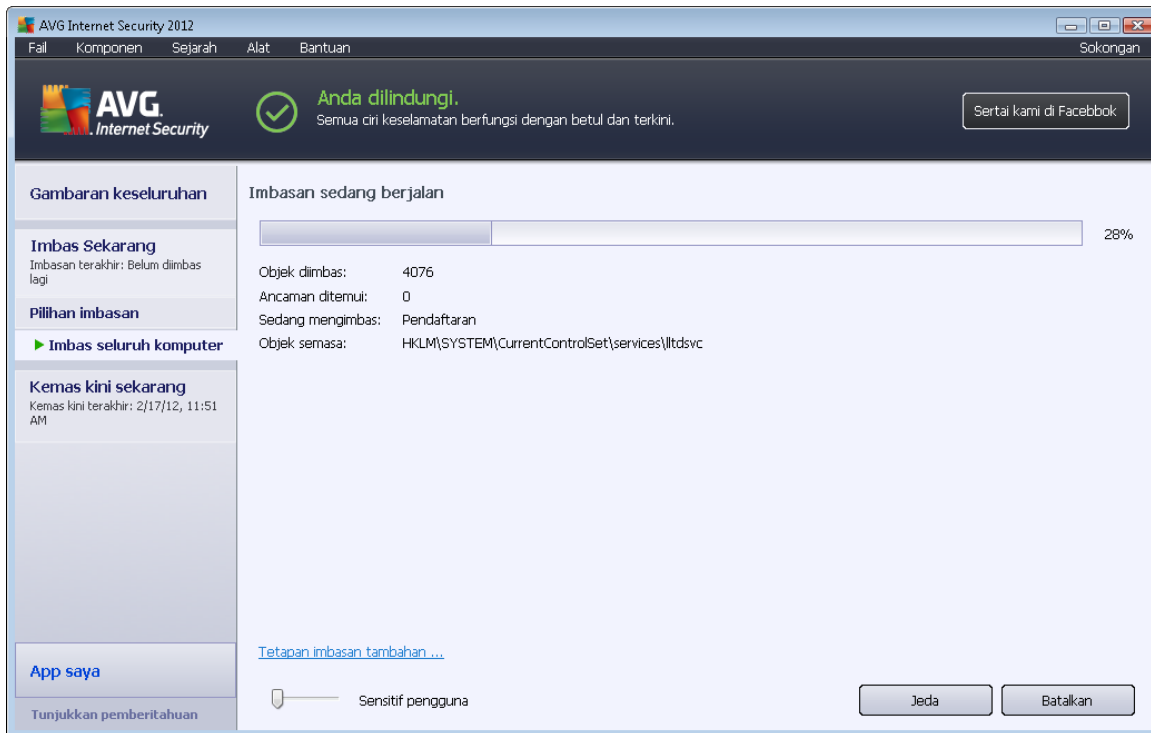
Dalam **AVG Internet Security 2012** anda akan menemui dua jenis pengimbasan yang dipratetapkan oleh vendor perisian:

### 12.2.1. Imbasan Seluruh Komputer

**Imbasan Seluruh Komputer** - mengimbas seluruh komputer anda untuk kemungkinan jangkitan dan/atau program berpotensi tidak dikehendaki. 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.

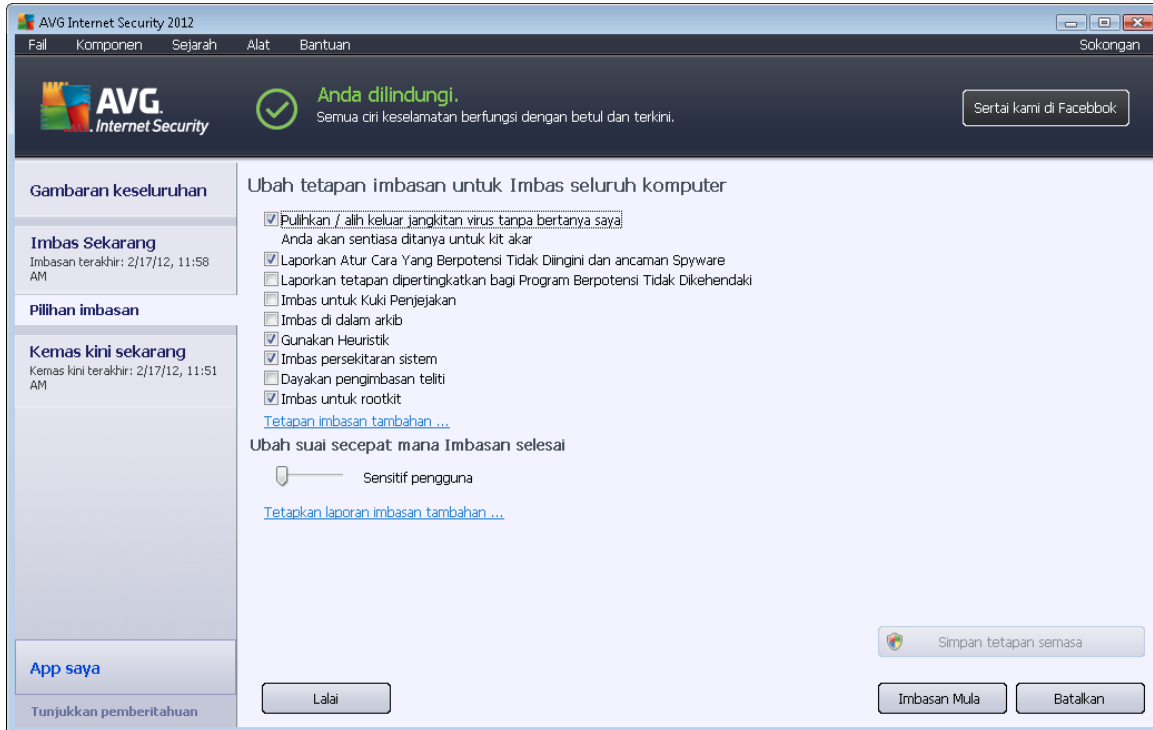
### Lancarkan imbasan

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



## Pengeditan konfigurasi imbasan

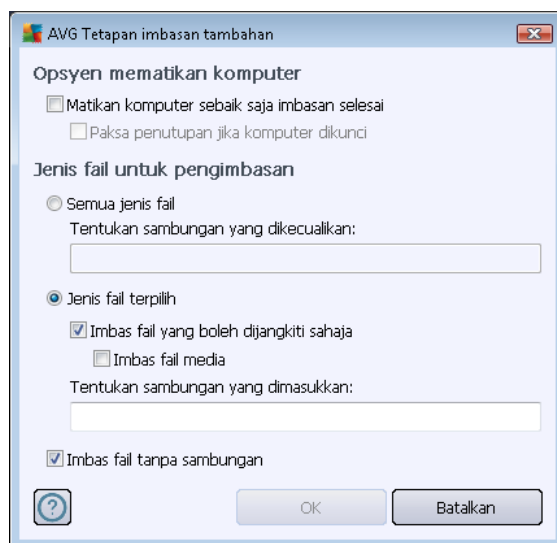
Anda mempunyai opsyen untuk menyunting tetapan lalai dipraktakrif untuk **Imbasan seluruh komputer**. Tekan pautan **Tukar tetapan imbasan** untuk pergi ke dialog **Tukar tetapan imbasan bagi Seluruh komputer** (boleh diakses dari [antara muka pengimbasan](#) melalui pautan **Tukar tetapan imbasan untuk Imbasan seluruh komputer**). **Adalah digalakkan untuk menyimpan tetapan lalai melainkan anda mempunyai alasan kukuh untuk menukarnya!**



- **Parameter imbasan** – dalam senarai parameter imbasan, anda boleh menghidupkan/mematikan parameter tertentu seperti yang diperlukan:
  - **Pulihkan / buang jangkitan virus tanpa bertanya saya (dihidupkan secara lalai)** – Jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika cara mengatasinya tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
  - **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip (dihidupkan secara lalai)** – Tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk mengesan perisian pengintip serta virus. Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
  - **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki ( dimatikan secara lalai)** – Tandakan untuk mengesan pakej yang diluaskan bagi perisian pengintip: atur cara yang sangat ok dan tidak berbahaya apabila diperoleh daripada pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
  - **Imbas untuk Kuki Penjejakan (dimatikan secara lalai)** – Parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan 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** (*dimatikan secara lalai*) – Parameter ini menentukan bahawa imbasan harus memeriksa semua fail yang disimpan dalam arkib, cth. ZIP, RAR, ...
  - **Gunakan Heuristik** (*dihidupkan secara lalai*) – Analisis heuristik (*pelagakan dinamik arahan objek yang diimbaskan dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan.
  - **Imbas persekitaran sistem** (*dihidupkan secara lalai*) – Imbasan juga akan menyemak kawasan sistem komputer anda.
  - **Dayakan pengimbasan menyeluruh** (*dimatikan secara lalai*) – Dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsiyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.
  - **Imbas untuk mengesan rootkit** (*dihidupkan secara lalai*) – imbasan [AntiRootkit](#) mencari kemungkinan terdapatnya rootkit di dalam komputer anda, cth. program dan teknologi yang boleh melakukan aktiviti malware dalam komputer anda. Jika rootkit dikesan, ini tidak semestinya bermaksud komputer anda dijangkiti. Dalam sesetengah kes, pemacu atau bahagian tertentu aplikasi biasa mungkin telah mengesan rootkit dengan salah.
- **Tetapan imbasan tambahan** – pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



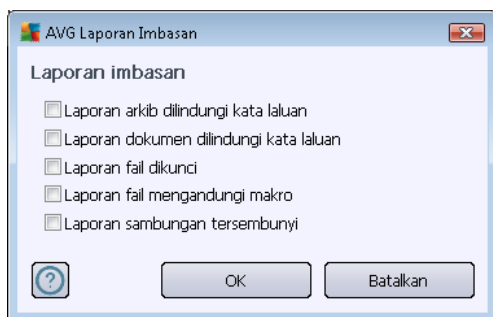
- **Opsyen mematikan komputer** – menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan





opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baharu membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).

- **Jenis fail untuk pengimbasan** – seterusnya, anda perlu memutuskan sama ada anda hendak mengimbas:
  - **Semua jenis fail** dengan kemungkinan bagi menentukan pengecualian daripada pengimbasan dengan memberikan senarai pemanjangan fail yang dipisahkan oleh koma yang tidak seharusnya diimbas;
  - **Jenis fail yang dipilih** – anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio – jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
  - Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** – opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.
- **Laraskan berapa cepat Imbasan selesai** - anda boleh menggunakan penggelongsor untuk menukar keutamaan proses pengimbasan. Secara lalai, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. 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 baharu 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 baharu anda sebagai konfigurasi*



lalui untuk digunakan untuk semua imbasan selanjutnya bagi seluruh komputer.

### 12.2.2. Imbas Fail atau Folder Tertentu

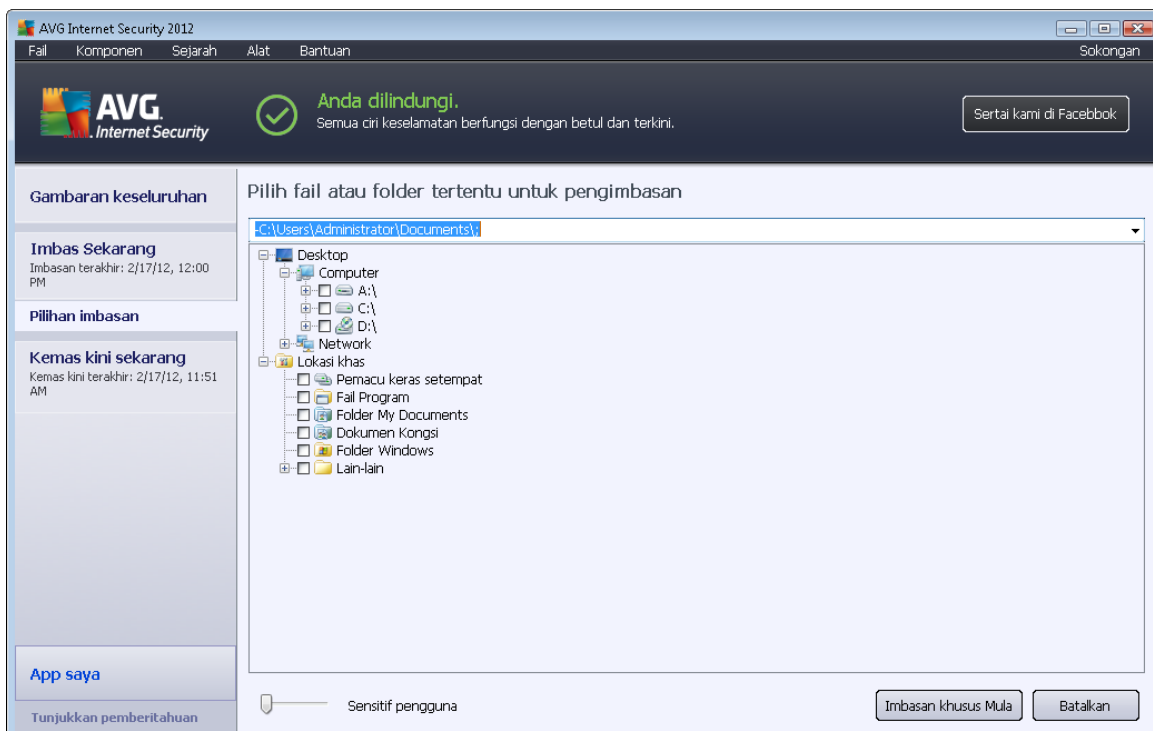
**Imbas fail atau folder tertentu** – mengimbas hanya kawasan komputer anda yang anda telah pilih untuk diimbas (*folder yang diimbas, cakera keras, cakera liut, CD, dll.*). Perkembangan imbasan jika pengesanan virus dan rawatannya adalah sama dengan imbas seluruh komputer: sebarang virus yang ditemui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

#### Lancarkan imbasan

**Imbas fail atau folder tertentu** boleh dilancarkan dari [pengimbasan antara muka](#) dengan mengklik pada ikon imbasan. Dialog baharu 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.

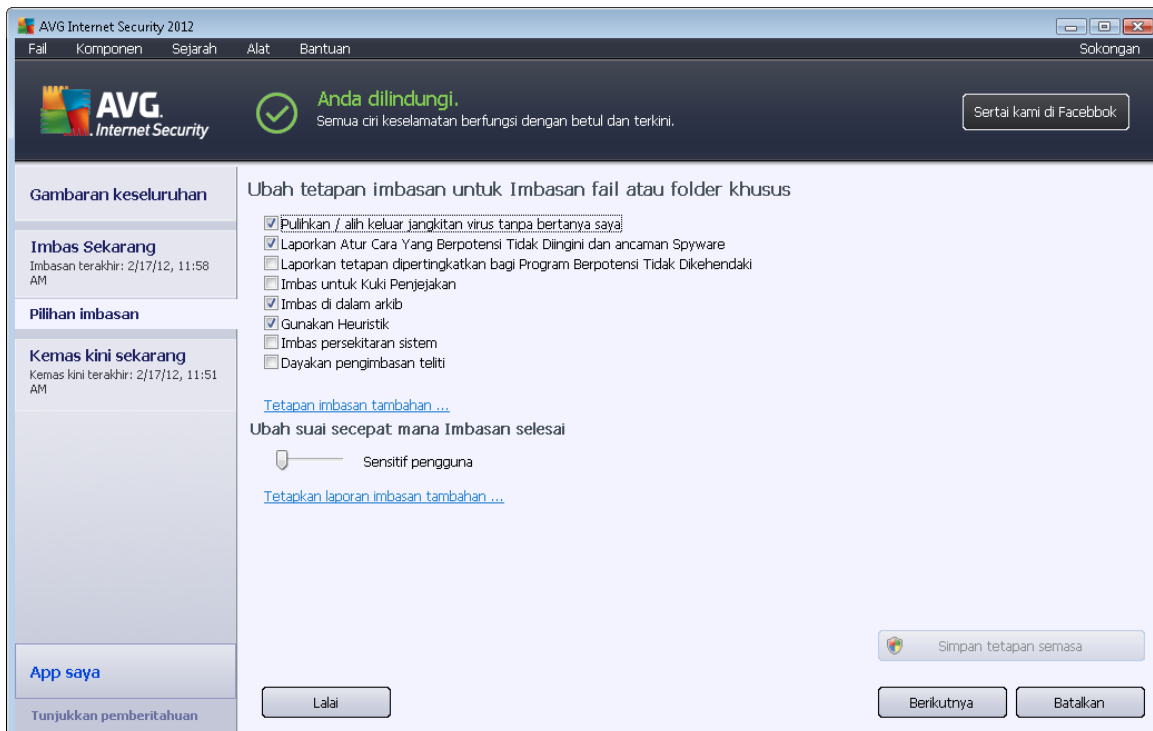
Terdapat juga kemungkinan mempunyai folder tertentu yang diimbas semasa semua subfoldernya tidak dimasukkan dalam imbasan ini, untuk melakukannya, tuliskan tanda tambah "-" di hadapan laluan yang dijana secara automatik (*lihat gambar skrin*). Untuk tidak memasukkan keseluruhan folder dari penggunaan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

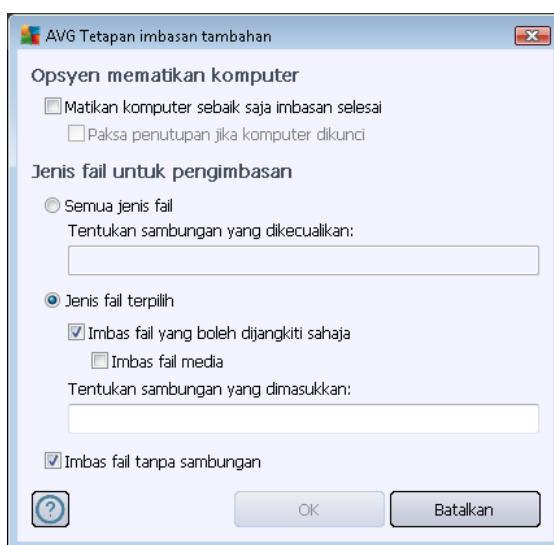
Anda mempunyai opsyen pengeditan bagi tetapan lalai yang dipratetapkan bagi **Imbasan fail atau folder tertentu**. Tekan pautan **Ubah tetapan imbasan** untuk pergi ke dialog **Ubah tetapan imbasan untuk Mengimbas fail atau folder tertentu**. **Adalah digalakkan untuk menyimpan tetapan lalai melainkan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



- **Parameter imbasan** – dalam senarai parameter imbasan, anda boleh menghidupkan/mematikan parameter tertentu seperti yang diperlukan:
  - **Pulihkan / buang jangkitan virus tanpa bertanyakan saya (dihidupkan secara lalai)** – jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika cara mengatasinya tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
  - **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip (dibuka secara lalai)** – tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
  - **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki (ditutup secara lalai)** – tandakan untuk mengesan pakej yang diluaskan bagi perisian pengintip: atur cara yang sangat ok dan tidak berbahaya apabila diperolehi dari

pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.

- **Imbas untuk Kuki Penjejakan** (*ditutup secara lalai*) – parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan; (*kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektroniknya*).
- **Imbas dalam arkib** (*dibuka secara lalai*) – parameter ini menentukan bahawa imbasan harus memeriksa semua fail yang disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** (*dihidupkan secara lalai*) – analisis heuristik (*pelagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan.
- **Imbas persekitaran sistem** (*ditutup secara lalai*) – imbasan juga akan memeriksa kawasan sistem komputer anda.
- **Dayakan pengimbasan teliti** (*ditutup secara lalai*) – dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.
- **Tetapan imbasan tambahan** – pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:

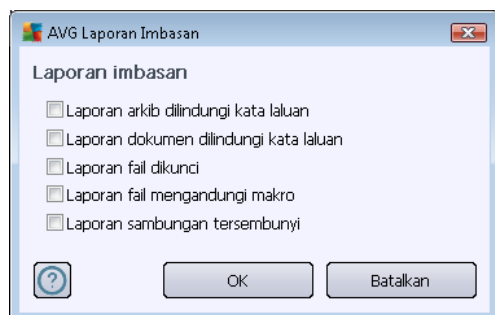


- **Opsyen mematikan komputer** – menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen



baharu membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).

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



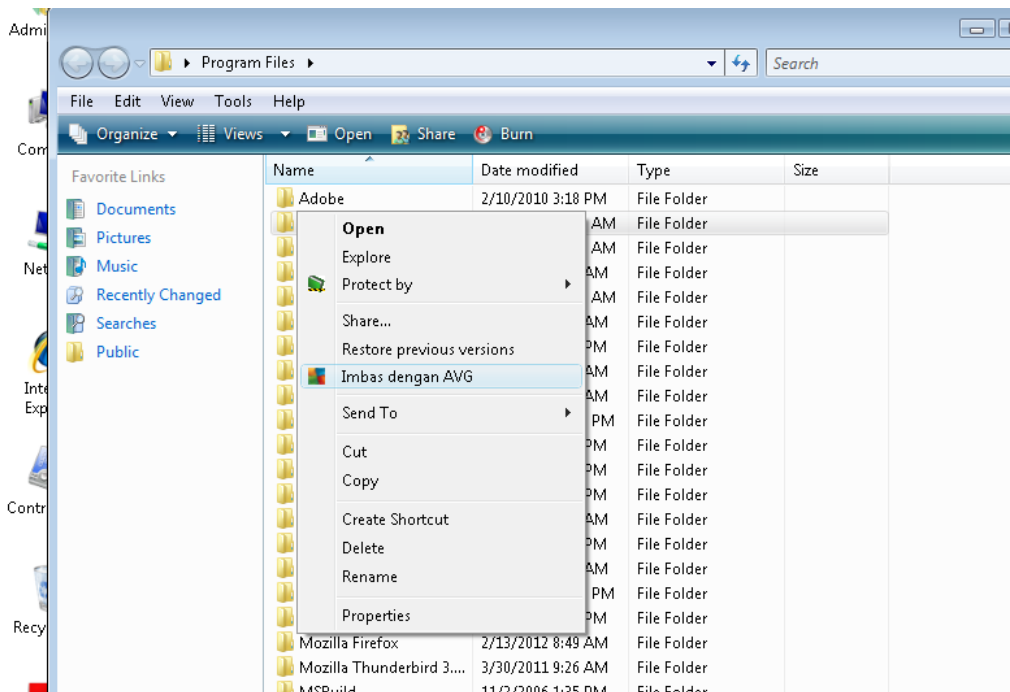
**Amaran:** *Tetapan imbasan ini adalah sama dengan parameter bagi imbasan yang baru ditakrifkan – seperti yang diterangkan dalam bab [Pengimbasan AVG / Penjadualan imbasan / Cara untuk Mengimbas](#). Sekiranya anda hendak memutuskan untuk mengubah konfigurasi lalai bagi **Imbas fail atau folder tertentu**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

### 12.3. Pengimbasan dalam Windows Explorer

Selain daripada imbasan dipratakrif yang dilancarkan untuk seluruh komputer atau kawasannya yang dipilih, **AVG Internet Security 2012** juga menawarkan pilihan bagi pengimbasan pantas bagi objek khusus secara terus dalam persekitaran Windows Explorer. Jika anda ingin membuka fail yang tidak diketahui dan anda tidak pasti mengenai kandungannya, anda mungkin mahu memeriksa dengan permintaan. Ikuti langkah-langkah ini:



- Dalam Windows Explorer, serlahkan fail (*atau folder*) yang anda hendak periksa
- Klik kanan tetikus anda pada objek untuk membuka menu konteks
- Pilih opsyen **Imbas dengan** supaya fail diimbas dengan **AVG Internet Security 2012**

### 12.4. Pengimbasan Garis Perintah

Dalam **AVG Internet Security 2012** terdapat pilihan bagi menjalankan imbasan daripada baris arahan. Anda boleh menggunakan opsyen ini contohnya pada pelayan atau semasa membuat skrip kelompok untuk dilancarkan secara automatik selepas but komputer. Daripada baris arahan, anda boleh melancarkan pengimbasan dengan paling banyak parameter yang ditawarkan dalam antara muka pegguna grafik AVG.

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



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

### Sintaks arahan

Sintaks arahan berikut:

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

### Parameter imbasan

Untuk memaparkan gambaran keseluruhan parameter sedia ada, taipkan arahan masing-masing bersama-sama parameter **/?** atau **/HELP** (cth. **avgscanx /?**). Satu-satunya parameter wajib adalah **/SCAN** untuk menentukan bahagian komputer yang harus 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.

#### 12.4.1. Parameter Imbasan CMD

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

- **/SCAN** [Imbas fail atau folder tertentu](#) **/SCAN=path;path** (e.g. **/SCAN=C:\;D:\**)
- **/COMP** [Imbasan 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
- **/LOG** Menjana fail keputusan imbasan
- **/MACROW** Laporkan makro
- **/PWDW** Laporkan fail yang dilindungi oleh kata laluan
- **/ARCBOMBSW** Laporkan bom arkib (*berulang kali memampatkan arkib*)
- **/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](#)
- **/PUPEXT** Laporkan set [Atur cara dipertingkatkan yang berkemungkinan tidak dikehendaki](#)
- **/REG** Imbas pendaftaran
- **/COO** Imbas kuki
- **/?** Memaparkan bantuan pada topik ini





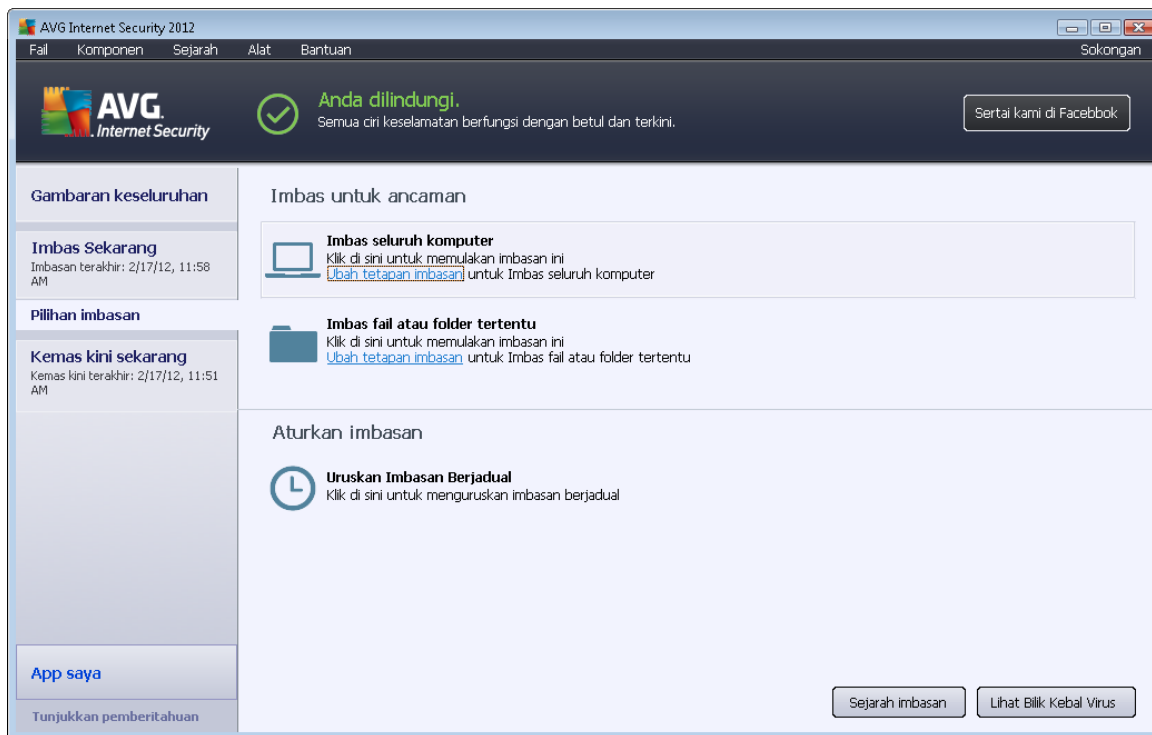
- **/HELP** Paparkan bantuan pada topik ini
- **/PRIORITY** Tetapkan keutamaan imbasan /Rendah, Auto, Tinggi/ (*lihat [Tetapan / Imbasan lanjutan](#)*)
- **/SHUTDOWN** Mematikan komputer apabila imbasan selesai
- **/FORCESHUTDOWN** Paksa komputer dimatikan apabila imbasan selesai
- **/ADS** Imbas Aliran Data Berganti-ganti (*NTFS sahaja*)
- **/HIDDEN** Laporkan fail dengan sambungan tersembunyi
- **/INFECTABLEONLY** Imbas fail dengan sambungan yang boleh dijangkiti sahaja
- **/THOROUGHSCAN** Dayakan pengimbasan menyeluruh
- **/CLOUDCHECK** Menyemak positif kesalahan
- **/ARCBOMBSW** Laporkan fail arkib yang dimampatkan semula

## 12.5. Penjadualan Imbasan

Dengan **AVG Internet Security 2012** anda boleh menjalankan imbasan dengan permintaan (contohnya, apabila anda mengesyaki jangkitan telah dibawa ke komputer anda) atau berasaskan perancangan yang dijadualkan. Ia amat disyorkan untuk menjalankan imbasan berdasarkan jadual: dengan cara ini, anda boleh memastikan komputer anda dilindungi dari sebarang kemungkinan daripada dijangkiti dan anda tidak perlu risau jika dan di mana untuk dilancarkan.

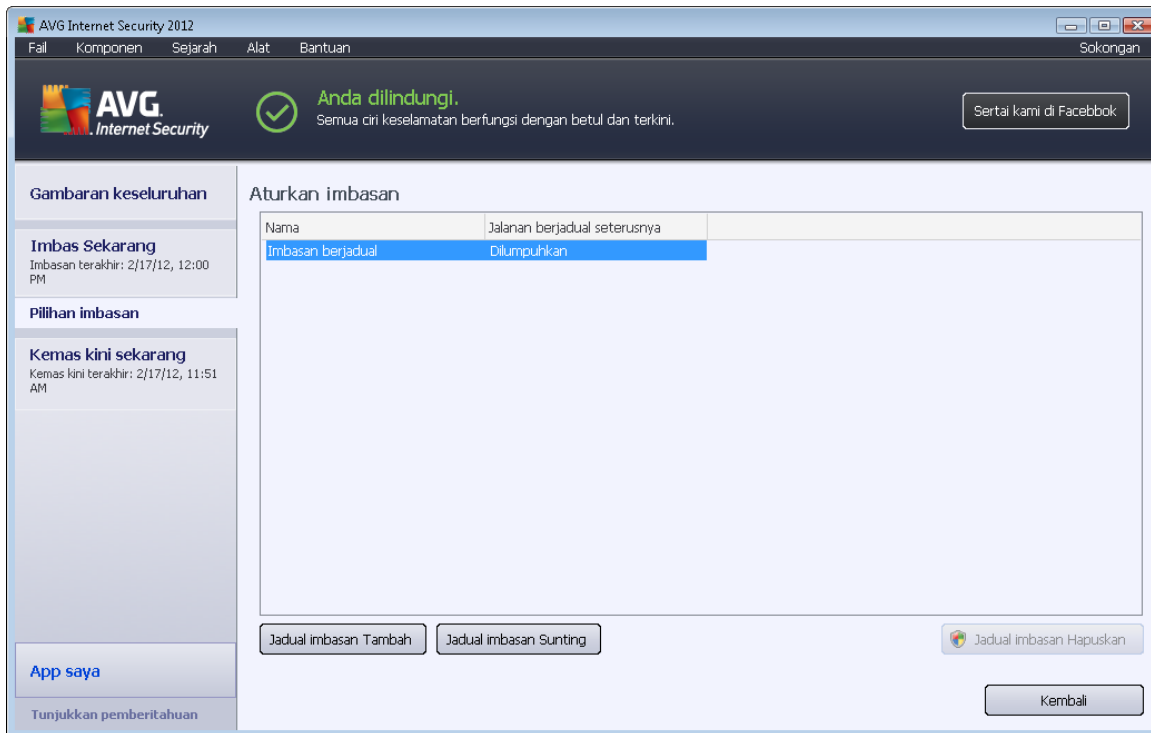
Anda harus melancarkan [imbasan Seluruh komputer](#) secara tetap, sekurang-kurangnya sekali seminggu. Walau bagaimanapun, jika boleh, lancarkan imbasan keseluruhan komputer anda setiap hari – seperti yang disediakan dalam konfigurasi lalai jadual imbasan. Jika komputer "sentiasa dihidupkan", kemudian, anda boleh menjadualkan imbasan di luar waktu bekerja. Jika komputer kadangkala dimatikan, maka jadualkan imbasan untuk berlaku [pada permulaan komputer semasa tugas telah terlepas](#).

Untuk membuat jadual imbasan baharu, lihat [antara muka imbasan AVG](#) dan cari bahagian bawah yang dipanggil **Jadualkan imbasan**:



## Jadualkan imbasan

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

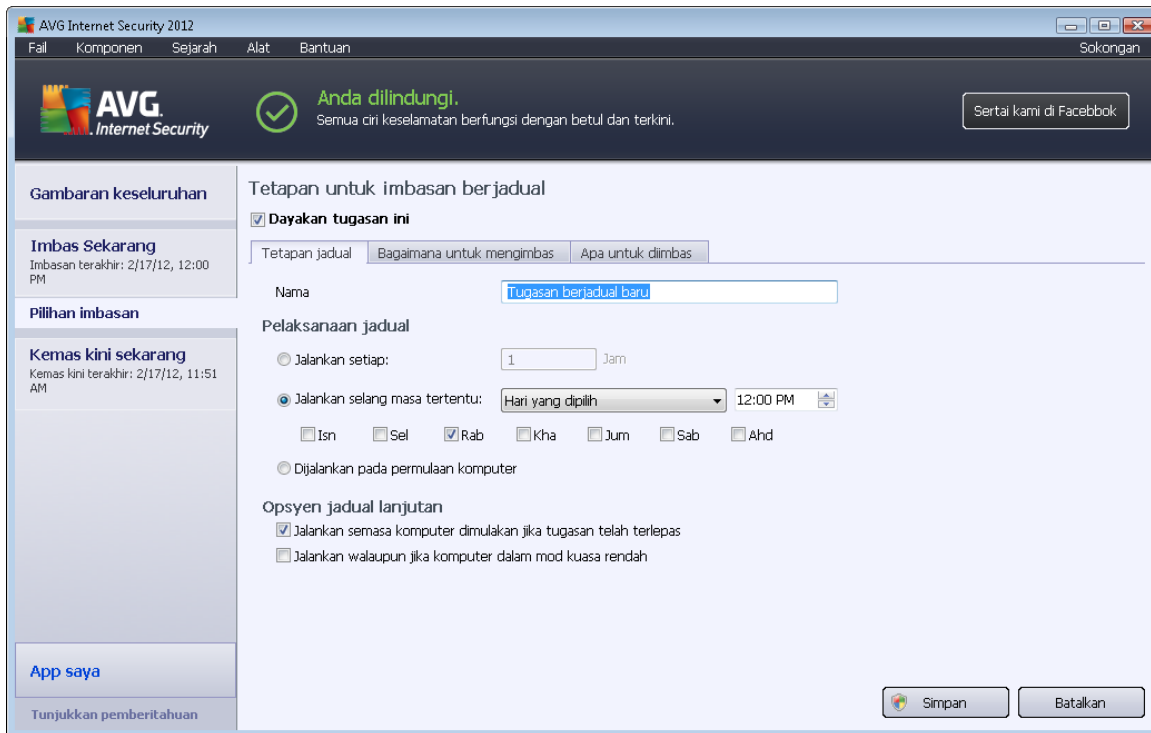


Anda boleh mengedit / menambah imbasan menggunakan butang kawalan berikut:

- **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 baharu 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 dipraktikkan dalam tetapan lalai tidak boleh dipadam.
- **Kembali** – kembali ke [antara muka pengimbasan AVG](#)

### 12.5.1. Tetapan Jadual

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



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

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

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

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

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

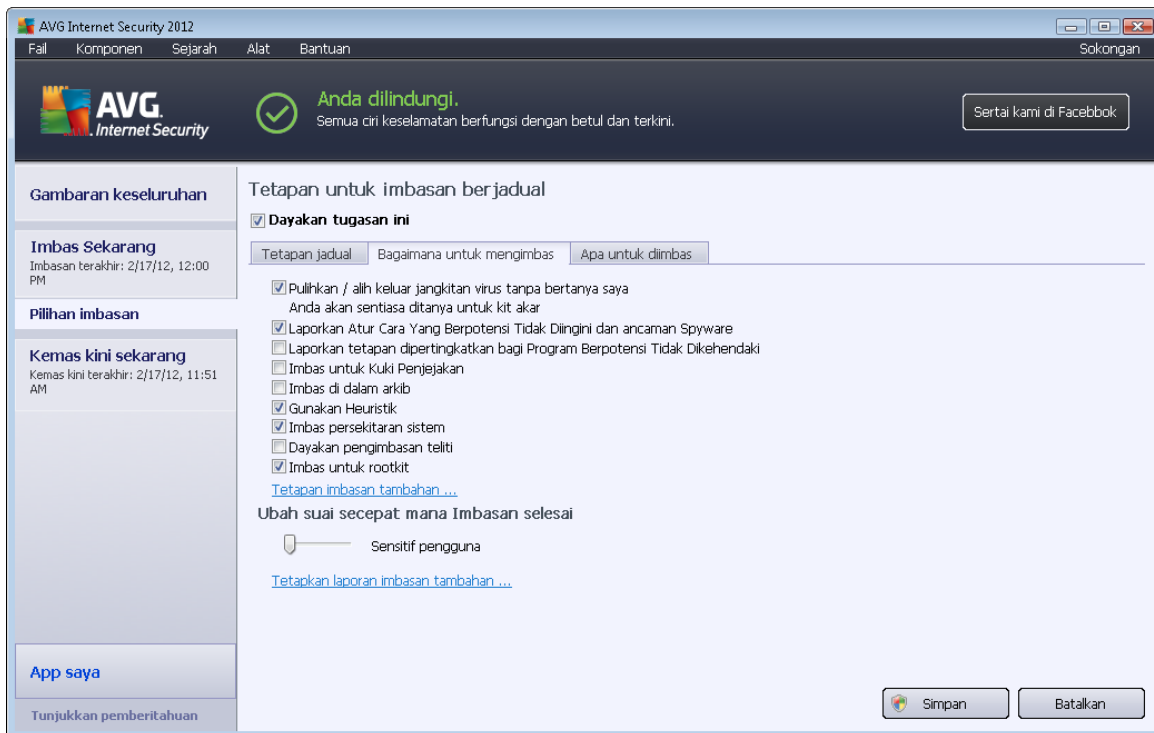


## Butang kawalan Tetapan untuk dialog imbasan berjadual

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

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

## 12.5.2. Bagaimana untuk Mengimbas



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

- **Pulihkan / buang jangkitan virus tanpa bertanya saya (dihidupkan secara lalai)**: jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika terdapat

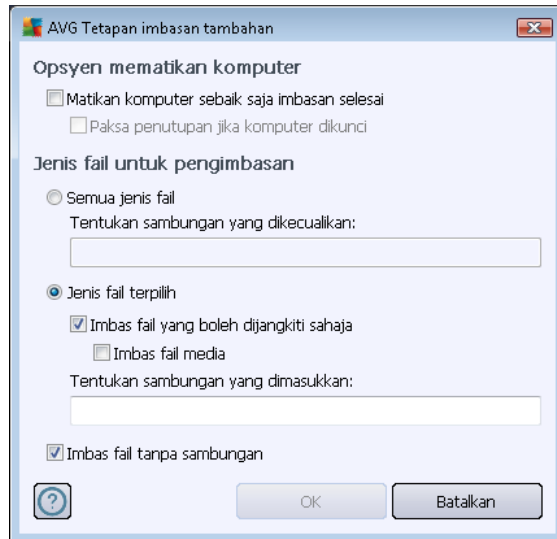


cara mengatasinya. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik atau jika anda memutuskan untuk mematikan pilihan ini, anda akan diberitahu mengenai pengesanan virus dan perlu memutuskan apa yang perlu dilakukan dengan jangkitan yang dikesan. Tindakan yang disarankan adalah untuk membuang fail yang dijangkiti ke [Bilik Kebal Virus](#).

- **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip (dibuka secara lalai):** tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta virus. Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini (ditutup secara lalai):** tandakan untuk mengesan pakej yang diluaskan bagi perisian pengintip: atur cara yang sangat ok dan tidak berbahaya apabila diperoleh daripada pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas untuk Kuki Penjejakan (ditutup secara lalai):** parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan sewaktu imbasan (*kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*).
- **Imbas dalam arkib (ditutup secara lalai):** parameter ini mentakrifkan bahawa pengimbasan harus memeriksa semua fail walaupun jika ia dibungkus dalam sejenis arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik (dibuka secara lalai):** analisis heuristik (*perlagakan dinamik bagi arahan objek yang diimbis dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan.
- **Imbas persekitaran sistem (dibuka secara lalai):** imbasan juga akan memeriksa kawasan sistem komputer anda.
- **Dayakan pengimbasan terperinci (ditutup secara lalai)** – dalam situasi tertentu (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsiyen ini untuk mengaktifkan algoritma pengimbasan yang paling terperinci yang akan mengimbas kawasan komputer anda yang tidak pernah dijangkiti, sekadar untuk memastikan sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa
- **Imbas untuk mengesan rootkit (dihidupkan secara lalai):** Imbasan [AntiRootkit](#) mencari kemungkinan terdapatnya rootkit di dalam komputer anda, cth. program dan teknologi yang boleh melakukan aktiviti malware dalam komputer anda. Jika rootkit dikesan, ini tidak semestinya bermaksud komputer anda dijangkiti. Dalam sesetengah kes, pemacu atau bahagian tertentu aplikasi biasa mungkin telah mengesan rootkit dengan salah.

Kemudian, anda boleh mengubah konfigurasi imbasan seperti berikut:

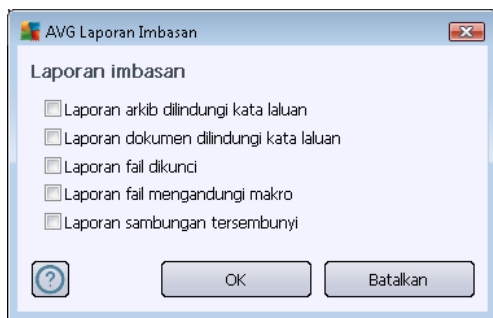
- **Tetapan imbasan tambahan** – pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



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

tahap *sensitif pengguna* bagi penggunaan sumber automatik. 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:



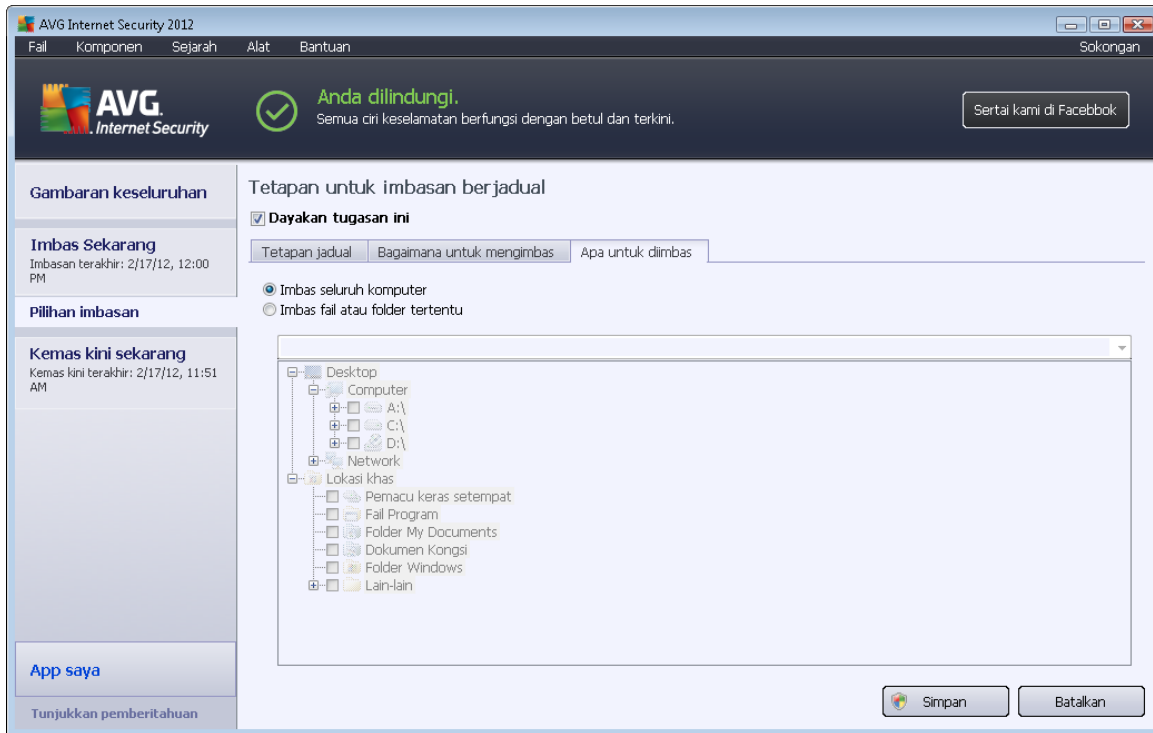
### Butang kawalan

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 kefungsiian yang sama tidak kira pada tab mana anda 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 mengkonfigurasikan 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](#).



### 12.5.3. Apa untuk Diimbas



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

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

Dalam struktur pepohon, anda juga boleh melihat dahan yang dipanggil **Lokasi khas**. Berikut, cari senarai lokasi yang akan diimbas sebaik sahaja kotak semakan masing-masing ditanda:

- **Pemacu keras tempatan** - semua pemacu keras bagi komputer anda
- **Fail Atur cara**
  - C:\Program Files\
  - dalam versi 64-bit C:\Program Files (x86)
- **Folder My Documents**



- o untuk Win XP: C:\Documents and Settings\Default User\My Documents\
- o untuk Windows Vista/7: C:\Users\user\Documents\

- **Dokumen Kongsi**

- o untuk Win XP: C:\Documents and Settings\All Users\Documents\
- o untuk Windows Vista/7: C:\Users\Public\Documents\

- **Folder Windows** – C:\Windows\

- **Lain-lain**

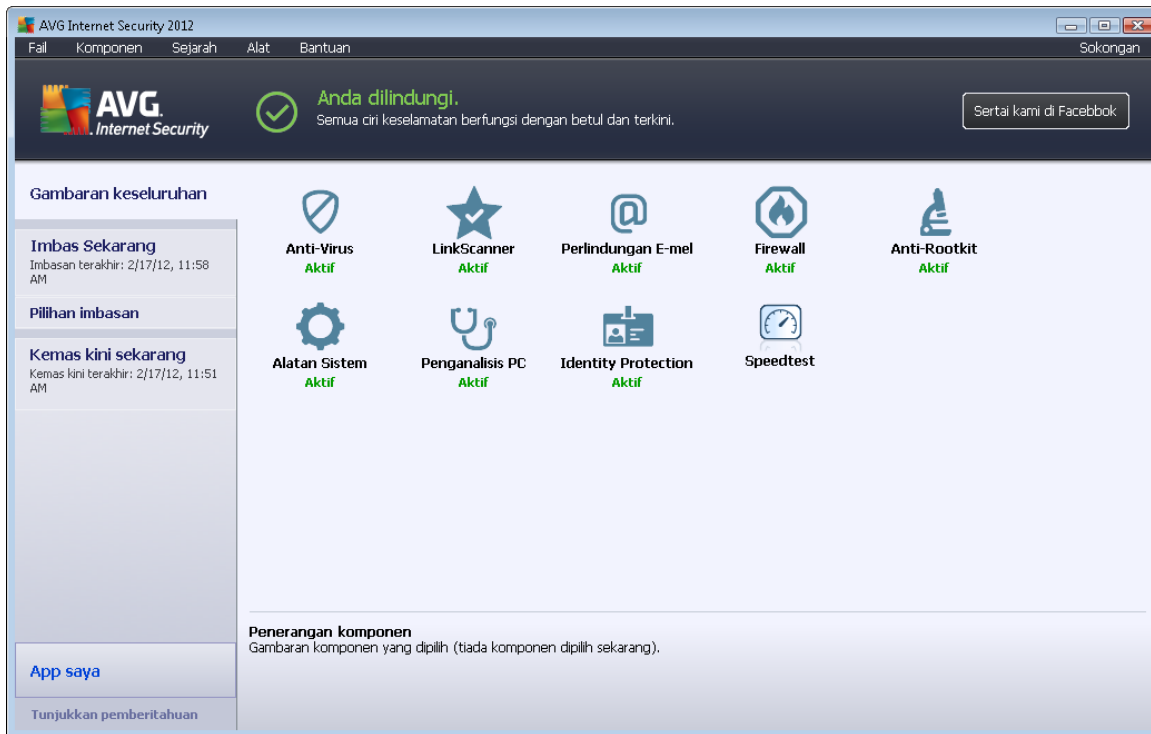
- o *Pemacu sistem* – pemacu keras di mana sistem pengendalian dipasang (biasanya C:)
- o *Folder sistem* – C:\Windows\System32\
- o *Folder Fail Sementara* – C:\Documents and Settings\User\Local\ (Windows XP); atau C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- o *Fail Internet Sementara* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); atau C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

## Butang kawalan

Dua butang kawalan yang sama tersedia pada semua ketiga-tiga tab bagi dialog **Tetapan untuk imbasan yang dijadualkan** ([Tetapan dijadualkan](#), [Bagaimana untuk mengimbas](#) dan [Apa hendak diimbas](#)):

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


## 12.6. Gambaran Keseluruhan Keputusan Imbasan




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

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

 – ikon hijau memberitahu tiada jangkitan yang dikesan sewaktu imbasan

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

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

Setiap ikon boleh menjadi sama ada tegar atau dipotong separuh – ikon tegar adalah untuk imbasan yang telah selesai dan yang diselesaikan dengan betul; ikon yang dipotong separuh bermaksud imbasan telah dibatalkan atau diganggu.

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

- **Masa mula** – tarikh dan masa semasa imbasan dilancarkan



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

### Butang kawalan

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

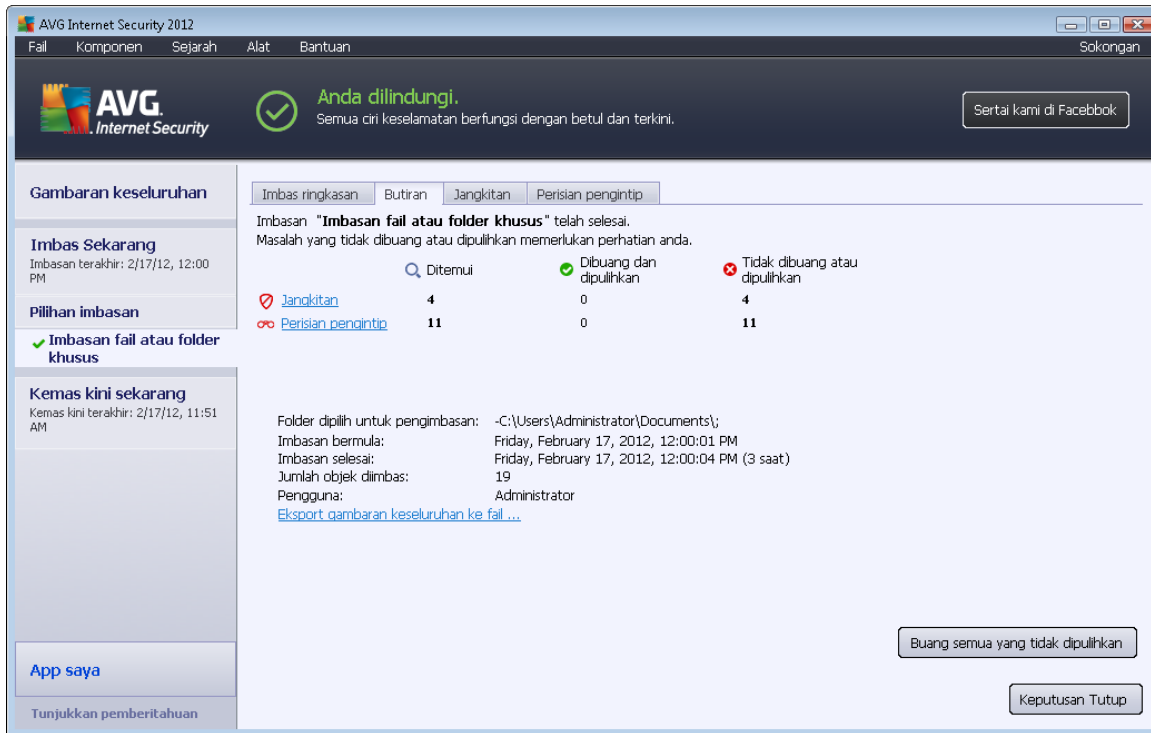
- **Lihat butiran** - tekannya untuk beralih ke dialog [Imbas keputusan](#) untuk melihat data terperinci bagi imbasan yang dipilih
- **Padam keputusan** - tekannya untuk membuang item yang dipilih daripada gambaran keseluruhan keputusan imbasan
- **Kembali** – mengalihkan semula ke dialog lalai bagi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

## 12.7. Butiran Keputusan Imbasan

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

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

### 12.7.1. Tab Gambaran Keseluruhan Keputusan



The screenshot shows the AVG Internet Security 2012 interface. The main window title is 'AVG Internet Security 2012'. The menu bar includes 'Fail', 'Komponen', 'Sejarah', 'Alat', and 'Bantuan'. The status bar at the top right says 'Sokongan'. The main area displays a green checkmark and the text 'Anda dilindungi. Semua ciri keselamatan berfungsi dengan betul dan terkini.' There is a 'Sertai kami di Facebook' button.

The left sidebar contains the following sections:

- Gambaran keseluruhan**
- Imbas Sekarang**: Imbasan terakhir: 2/17/12, 12:00 PM
- Pilihan imbasan**:
  - ✓ Imbasan fail atau folder khusus
- Kemas kini sekarang**: Kemas kini terakhir: 2/17/12, 11:51 AM
- App saya**
- Tunjukkan pemberitahuan

The main content area shows the results for the scan 'Imbasan fail atau folder khusus' which is completed. A message states: 'Masalah yang tidak dibuang atau dipulihkan memerlukan perhatian anda.' Below this is a table:

	Ditemui	Dibuang dan dipulihkan	Tidak dibuang atau dipulihkan
Jangkitan	4	0	4
Perisian pengintip	11	0	11

Additional details provided:

- Folder dipilih untuk pengimbasan: -C:\Users\Administrator\Documents\;
- Imbasan bermula: Friday, February 17, 2012, 12:00:01 PM
- Imbasan selesai: Friday, February 17, 2012, 12:00:04 PM (3 saat)
- Jumlah objek diimbas: 19
- Pengguna: Administrator

Buttons at the bottom right include 'Buang semua yang tidak dipulihkan' and 'Keputusan Tutup'.

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

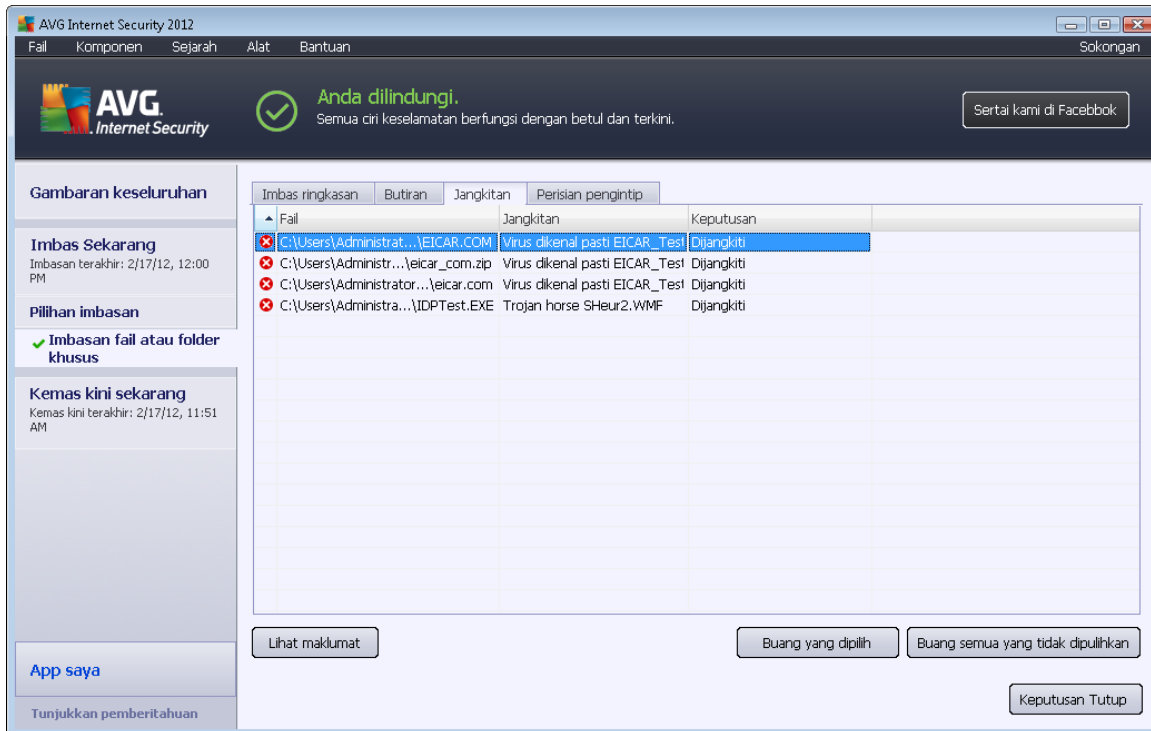
- jangkitan virus / perisian pengintip yang dikesan
- jangkitan virus / perisian pengintip yang dibuang
- bilangan jangkitan virus / perisian pengintip yang tidak boleh dibuang atau dipulihkan

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

#### Butang kawalan

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

## 12.7.2. Tab Jangkitan



Tab **Jangkitan** hanya dipaparkan dalam dialog **Imbas keputusan** jika jangkitan virus dikesan sewaktu pengimbasan. Tab ini dibahagikan kepada tiga bahagian menyediakan maklumat berikut:

- **Fail** – laluan penuh ke lokasi asal bagi objek yang dijangkiti
- **Jangkitan** – nama bagi virus yang dikesan (*untuk butiran mengenai virus khusus, sila rujuk kepada [Ensiklopedia Virus](#) dalam talian*)
- **Keputusan** – mentakrifkan status terkini bagi objek yang dijangkiti yang dikesan sewaktu imbasan:
  - **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 pada pengecualian PUP** – penemuan dinilai sebarai pengecualian dan ditambah pada senarai pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian](#)*)

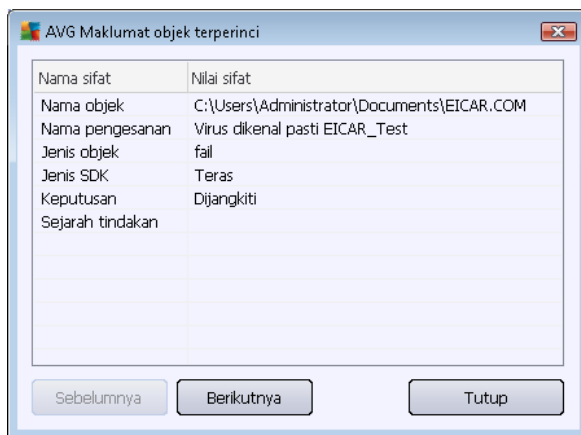
*[PUP](#) bagi tetapan lanjutan)*

- **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:

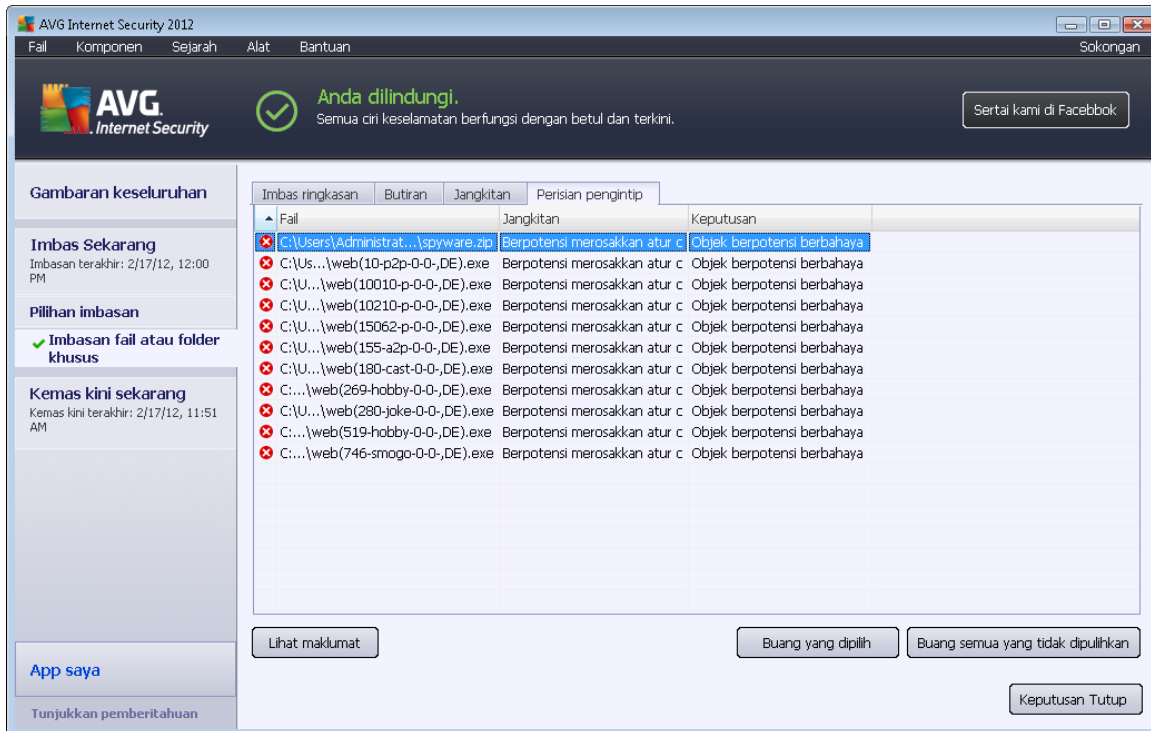
- **Lihat butiran** – butang ini membuka tettingkap dialog baru yang dinamakan **Maklumat objek terperinci**:



Dalam dialog ini anda boleh menemui maklumat terperinci mengenai objek boleh berjangkit yang dikesan (*cth. nama dan lokasi objek yang dijangkiti, jenis objek, jenis SDK, hasil pengesanan dan sejarah tindakan yang berkaitan dengan objek yang dikesan*). Menggunakan butang **Sebelumnya** / **Seterusnya** anda boleh melihat maklumat pada penemuan tertentu. Gunakan butang **Tutup** untuk menutup dialog ini.

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

### 12.7.3. Tab Perisian Pengintip



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

- **Fail** – laluan penuh ke lokasi asal bagi objek yang dijangkiti
- **Jangkitan** - nama yang dikesan perisian pengintip (*untuk butiran mengenai virus tertentu, sila rujuk [Ensiklopedia Virus](#) dalam talian*)
- **Keputusan** – mentakrif status objek semasa yang dikesan sewaktu imbasan:
  - **Dijangkiti** – objek yang dijangkiti dikesan dan dibiarkan 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 pada pengecualian PUP** – penemuan dinilai sebarai pengecualian dan ditambah pada senarai pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian PUP](#) bagi tetapan lanjutan*)

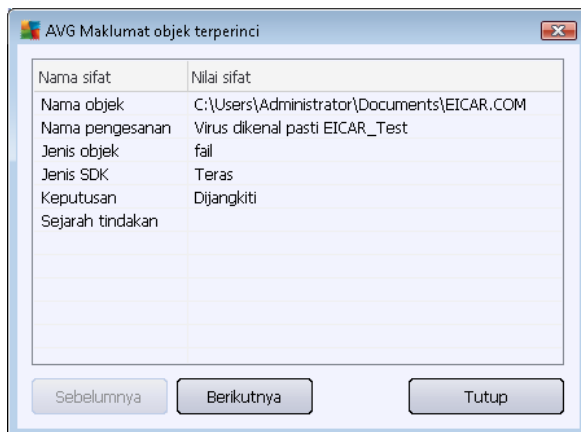


- **Fail yang dikunci – tidak diuji** – objek masing-masing dikunci dan oleh sebab itu, AVG tidak dapat mengimbasnya
- **Objek berpotensi berbahaya** – objek dikesan sebagai berpotensi berbahaya tetapi tidak dijangkiti (sebagai contoh, ia boleh mengandungi makro); maklumat adalah hanya amaran
- **But 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 anda dalam dialog ini:

- **Lihat butiran** – butang ini membuka tettingkap dialog baru yang dinamakan **Maklumat objek terperinci**:



Dalam dialog ini anda boleh menemui maklumat terperinci mengenai objek boleh berjangkit yang dikesan (*cth. nama dan lokasi objek yang dijangkiti, jenis objek, jenis SDK, hasil pengesanan dan sejarah tindakan yang berkaitan dengan objek yang dikesan*). Menggunakan butang **Sebelumnya** / **Seterusnya** anda boleh melihat maklumat pada penemuan tertentu. Gunakan butang **Tutup** untuk meninggalkan dialog ini.

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



#### 12.7.4. Tab Amaran

Tab **Amaran** memaparkan maklumat pada objek yang "disyaki" (*biasanya fail*) yang dikesan sewaktu pengimbasan. Apabila dikesan oleh Resident Shield, 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 dalam keputusan ujian, terdapat hanya Amaran yang dikesan oleh **AVG Internet Security 2012**, 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 Internet Security 2012** 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.

#### 12.7.5. Tab Rootkit

Tab **Rootkit** memaparkan maklumat mengenai rootkit yang dikesan semasa pengimbasan antirootkit yang disertakan dalam [Imbas Seluruh Komputer](#).

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

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

#### 12.7.6. Tab Maklumat

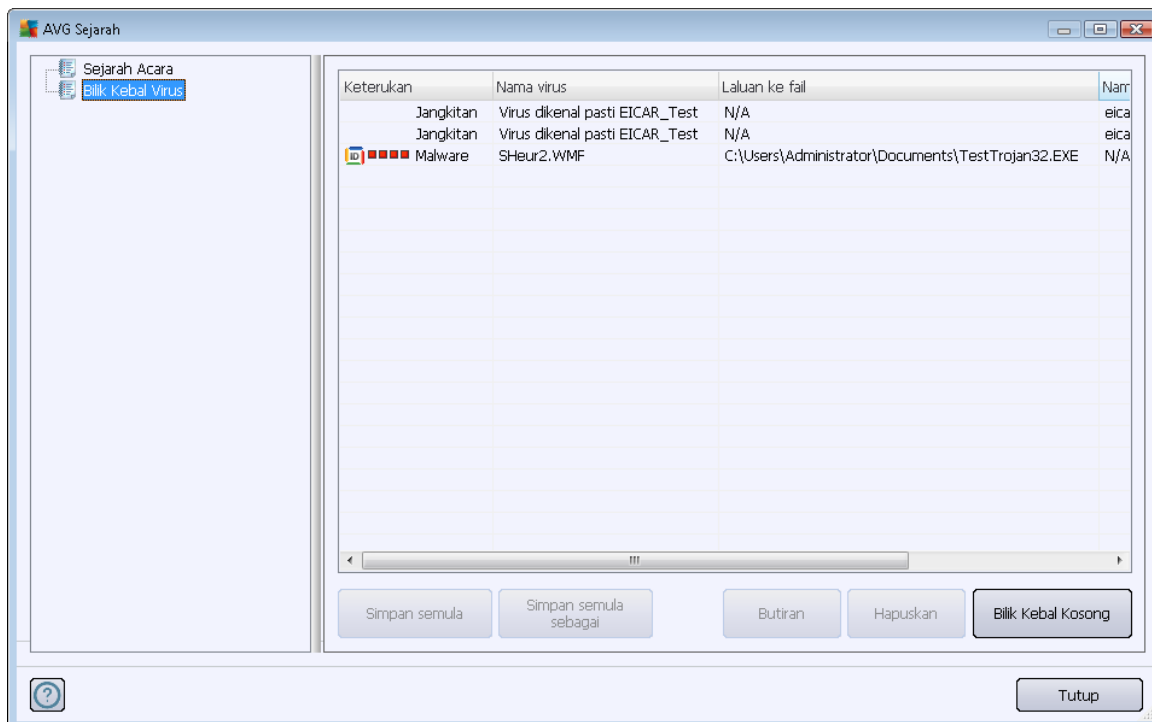
Tab **Maklumat** yang mengandungi data mengenai "penemuan" seperti itu yang tidak boleh dikategorikan sebagai jangkitan, perisian pengintip, dll. Ia boleh sama ada dilabel secara positif sebagai berbahaya tetapi ia masih berbaloi untuk perhatian anda. **AVG Internet Security 2012** imbasan boleh mengesan fail yang mungkin tidak dijangkiti, tetapi, mencurigakan. Fail ini dilaporkan sama ada sebagai [Amaran](#) atau sebagai Maklumat.



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

- **Masa jalan dipek** - Fail dipek dengan salah satu pembungkus masa jalan yang kurang biasa, yang mungkin menunjukkan cubaan untuk mengelakkan pengimbasan fail seperti itu. Walau bagaimanapun, bukan setiap laporan bagi fail seperti itu menunjukkan virus.
- **Rekursif jalan masa yang dipek** – Sama dengan yang di atas, walau bagaimanapun, kurang kerap di kalangan perisian biasa. Fail seperti itu adalah mencurigakan dan pembuangannya atau penghantarannya untuk analisis harus dipertimbangkan.
- **Arkib atau dokumen yang dilindungi kata laluan** - Fail yang dilindungi kata laluan tidak boleh diimbis oleh **AVG Internet Security 2012** (atau secara umumnya, 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 Internet Security 2012** 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), melaporkan percanggahan ini. **AVG Internet Security 2012** Dalam sesetengah kes, virus menggunakan nama bagi proses standard untuk membuatnya kurang ketara dalam sistem.
- **Fail dikunci** - Fail yang dilaporkan dikunci, seterusnya, tidak boleh diimbis oleh **AVG Internet Security 2012**. Ini biasanya bermaksud bahawa sesetengah fail digunakan oleh sistem secara berterusan (cth. *fail pertukaran*).

## 12.8. 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. Tujuan utama bagi **Bilik Kebal Virus** adalah untuk menyimpan sebarang fail yang dipadamkan untuk tempoh masa tertentu supaya anda boleh memastikan anda tidak memerlukan fail lagi dalam lokasi asalnya. Jika anda mendapati ketiadaan fail menyebabkan masalah, anda boleh menghantarkan fail yang dipersoalkan untuk analisis, atau menyimpannya semula ke lokasi asal.

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

- **Keterangan** – jika anda memutuskan untuk memasang komponen [Identity Protection](#) dalam **AVG Internet Security 2012**, pengenalan grafik bagi keterangan penemuan masing-masing pada skala empat tahap daripada yang tidak boleh dibantah (■□□□) sehingga kepada sangat berbahaya (■□■□) akan diberikan dalam bahagian ini; dan maklumat mengenai jenis jangkitan (*berdasarkan pada tahap jangkitannya – semua objek yang disenaraikan boleh menjadi secara positif atau berkemungkinan dijangkiti*)
- **Nama Virus** – menentukan nama jangkitan yang dikesan menurut [Ensiklopedia virus](#) (*dalam talian*)
- **Laluan ke fail** – laluan penuh ke lokasi asal bagi fail yang boleh dijangkiti dikesan

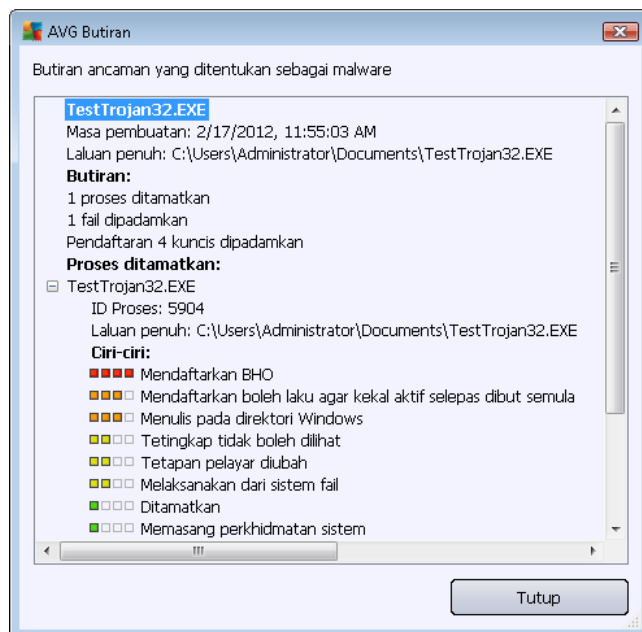


- **Nama objek asal** – semua objek yang dikesan yang disenaraikan dalam carta telah dilabel dengan nama standard yang diberikan oleh AVG sewaktu proses imbasan. Jika objek mempunyai nama asal khusus yang diketahui (*cth. nama lampiran e-mel yang tidak memberi respons kepada kandungan sebenar lampiran*), ia akan diberikan dalam 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** – mengalih fail yang dijangkiti ke folder yang dipilih
- **Butiran** – butang ini hanya digunakan pada ancaman yang dikesan oleh [Identity Protection](#). Dengan mengklik, ia memaparkan gambaran keseluruhan sinopsis gambaran keseluruhan bagi butiran ancaman (*apakah fail/proses yang telah dijangkiti, ciri-ciri proses dll.*). Sila maklum bahawa untuk semua item lain selain yang dikesan oleh IDP, butang ini berwarna kelabu dan tidak aktif!



- **Padam** – membuang fail yang dijangkiti daripada **Bilik Kebal Virus** sepenuhnya dan tidak boleh diundur
- **Kosongkan Bilik Kebal** – membuang semua **kandungan** Bilik Kebal Virus sepenuhnya. Dengan membuang fail dari **Bilik Kebal Virus**, fail ini dibuang tanpa boleh didapatkan kembali dari cakera ( bukan dialihkan ke tong kitar semula).



## 13. Kemas kini AVG

Tiada perisian keselamatan yang boleh menjamin perlindungan sebenar dari pelbagai jenis ancaman melainkan ia dikemas kini secara tetap! Penulis virus sentiasa mencari kecelaan baharu yang mereka boleh mengeksploitasi dalam perisian dan juga sistem pengendalian. Virus baharu, 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.

Mengambil kira semua ancaman komputer yang baru muncul, dan kelajuan yang ia sebarakan, ia sudah tentu penting untuk mengemas kini **AVG Internet Security 2012** anda secara tetap. Penyelesaian terbaik ialah kekal dengan tetapan lalai atur cara yang kemas kini automatik dikonfigurasi. Sila ingat bahawa jika pangkalan data virus bagi **AVG Internet Security 2012** anda tidak terkini, atur cara tidak dapat mengesan ancaman terkini!

***Adalah penting untuk mengemas kini AVG anda secara tetap! Kemas kini definisi virus penting patut dilakukan setiap hari, jika boleh. Kemas kini atur cara yang kurang penting boleh dilakukan setiap minggu.***

### 13.1. Pelancaran kemas kini

Untuk memberikan keselamatan maksimum yang tersedia, **AVG Internet Security 2012** adalah secara lalai, dijadualkan untuk mencari kemas kini baharu setiap empat jam. Memandangkan kemas kini AVG tidak dikeluarkan mengikut sebarang jadual yang dibetulkan tetapi dalam reaksi kepada amaran dan keseriusan ancaman baharu, semakan ini sangat penting untuk memastikan pangkalan data virus AVG dipastikan terkini setiap masa.

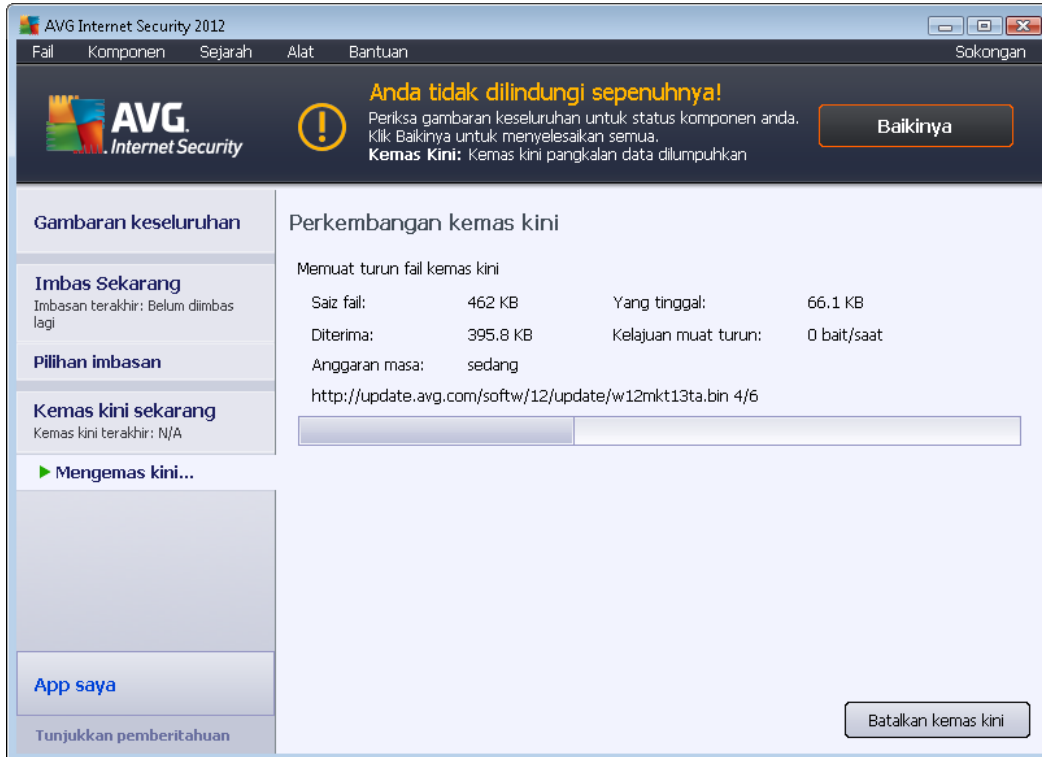
Sekiranya, anda ingin mengurangkan bilangan pelancaran kemas kini, anda boleh menyediakan parameter pelancaran kemas kini anda sendiri. Walau bagaimanapun, adalah amat disyorkan untuk melancarkan kemas kini sekali sehari! Konfigurasi boleh diedit dalam seksyen [Tetapan Lanjutan/Jadual](#), secara khusus, dalam dialog berikut:

- [Jadual kemas kini definisi](#)
- [Jadual kemas kini atur cara](#)
- [Jadual kemas kini AntiSpam](#)

Sekiranya, anda ingin memeriksa fail kemas kini baharu dengan segera, gunakan pautan pantas [Kemas kini sekarang](#) dalam antara muka pengguna utama. Pautan ini tersedia pada setiap masa dari sebarang dialog [antara muka pengguna](#).

### 13.2. Perkembangan kemas kini

Apabila anda memulakan kemas kini, pertama sekali, AVG akan mengenal pasti sama ada terdapat fail kemas kini baharu yang tersedia. Jika sedemikian, **AVG Internet Security 2012** memulakan muat turunnya dan melancarkan proses kemas kininya sendiri. Sewaktu proses kemas kini, anda akan dihalakan semula ke antara muka **Kemas kini** di mana anda boleh melihat perkembangan proses dalam persembahan grafiknya serta seperti dalam gambaran keseluruhan parameter statistik yang relevan (*kemas kini saiz fail, data yang diterima, kelajuan muat turun, masa berlalu, ...*):



**Nota:** Sebelum setiap pelancaran kemas kini atur cara AVG, titik pemulihan sistem dibuat. Sekiranya, proses kemas kini gagal dan sistem pengendalian anda rosak, anda boleh sentiasa menyimpan semula sistem pengendalian anda dalam konfigurasi asalnya dari titik ini. Opsyen ini boleh diakses melalui menu Windows: Start / All Programs / Accessories / System tools / System Restore. Disyorkan untuk pengguna berpengalaman sahaja!

### 13.3. Tahap kemas kini

AVG Internet Security 2012 memberikan dua tahap kemas kini untuk dipilih:

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

Apabila [menjadualkan kemas kini](#), adalah berkemungkinan untuk menentukan parameter tertentu untuk kedua-dua tahap kemas kini:

- [Jadual kemas kini definisi](#)
- [Jadual kemas kini atur cara](#)

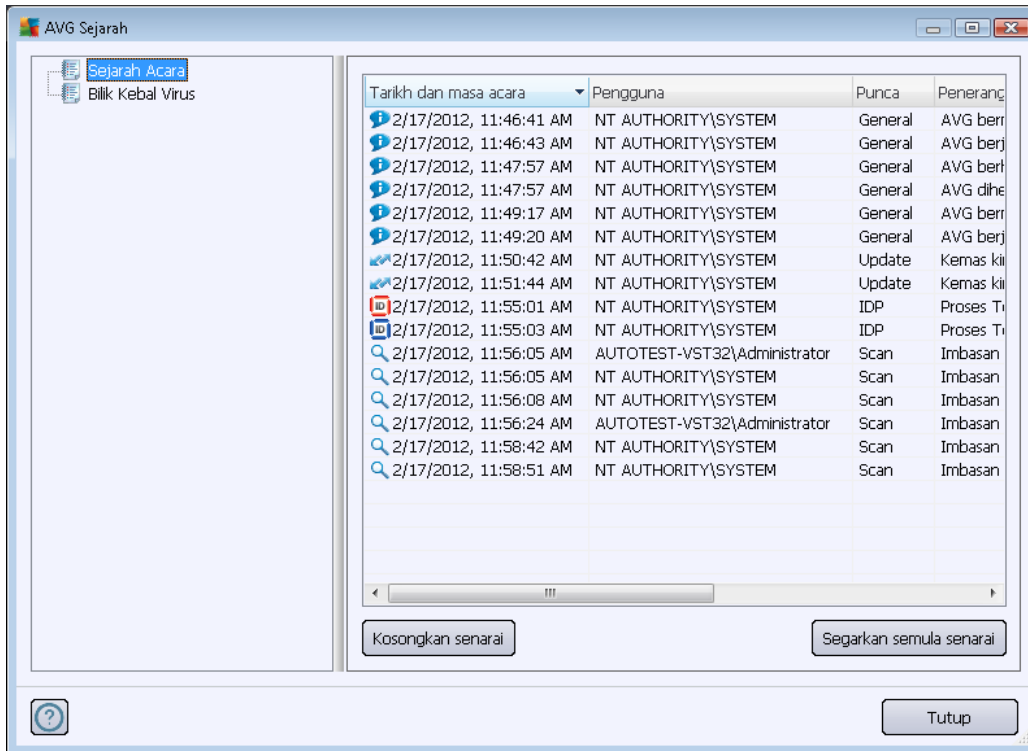
**Perhatian:** Jika persamaan masa bagi kemas kini atur cara yang dijadualkan dan imbasan yang



*dijadwalkan berlaku, proses kemas kini adalah lebih utama dan imbasan akan diganggu.*



## 14. Sejarah Acara



Dialog **Sejarah** boleh diakses dari [menu sistem](#) melalui item **Sejarah/Log Sejarah Acara**. Dalam dialog ini, anda boleh menemui ringkasan peristiwa penting yang berlaku sewaktu operasi **AVG Internet Security 2012**. **Sejarah** merekodkan jenis acara berikut:

- Maklumat mengenai kemas kini aplikasi AVG
- Maklumat pada pengimbasan bermula, tamat atau berhenti (*termasuk ujian yang dilakukan secara automatik*)
- Maklumat mengenai acara dihubungkan dengan pengesanan virus (*sama ada melalui [Resident Shield](#) atau [pengimbasan](#)*) termasuk lokasi kejadian
- Acara penting lain

Bagi setiap acara, maklumat berikut disenaraikan:

- **Tarikh dan masa acara** memberikan masa dan tarikh tepat acara berlaku
- **Pegguna** menyatakan nama pengguna yang sedang dilog masuk pada masa berlakunya acara
- **Sumber** memberikan maklumat mengenai komponen sumber atau bahagian lain sistem AVG yang mencetuskan acara
- **Penerangan acara** memberikan maklumat ringkas apa sebenarnya berlaku



### **Butang kawalan**

- ***Kosongkan senarai*** - tekan butang untuk memadam semua entri dalam senarai acara
- ***Muat semula senarai*** - tekan butang untuk mengemas kini semua entri dalam senarai acara

## 15. Soalan Lazim dan Sokongan Teknikal

Sekiranya, anda mempunyai sebarang masalah jualan atau teknikal dengan aplikasi **AVG Internet Security 2012** anda, terdapat beberapa cara untuk mendapatkan bantuan. Sila pilih dari opsyen berikut:

- **Dapatkan Sokongan:** Terus dalam aplikasi AVG anda boleh menghubungi halaman sokongan pelanggan khusus di laman web AVG (<http://www.avg.com/>). Pilih item menu utama **Bantuan / Dapatkan Sokongan** untuk dihalakan semula ke laman web AVG dengan saluran sokongan yang tersedia. Untuk teruskan, sila ikuti arahan dalam halaman web.
- **Sokongan (pautan menu utama):** Menu aplikasi AVG (*di atas antara muka pengguna utama*) termasuk pautan **Sokongan** yang membuka dialog baharu dengan semua jenis maklumat yang anda mungkin perlu cuba untuk mendapatkan bantuan. Dialog termasuk data asas mengenai atur cara AVG anda yang dipasang (*versi atur cara / pangkalan data*), butiran lesen, dan senarai pautan sokongan pantas:



- **Menyelesaikan masalah dalam fail bantuan:** Bahagian **Menyelesaikan masalah** baharu tersedia terus dalam fail bantuan yang disertakan dalam **AVG Internet Security 2012** (*untuk membuka fail bantuan, tekan kekunci F1 dalam mana-mana dialog dalam aplikasi*). Seksyen ini memberikan senarai situasi yang paling kerap berlaku semasa pengguna ingin mendapatkan bantuan profesional kepada isu teknikal. Sila pilih situasi yang terbaik menerangkan masalah anda, dan klik padanya untuk membuka arahan terperinci yang membawa kepada penyelesaian masalah.
- **Pusat Sokongan Laman Web AVG:** Secara alternatif, anda boleh mendapatkan penyelesaian kepada masalah anda pada laman web AVG (<http://www.avg.com/>). Dalam seksyen **Pusat Sokongan** anda boleh mendapatkan gambaran keseluruhan berstruktur



bagi kumpulan bertema yang berkaitan dengan isu jualan dan teknikal.

- **Soalan Lazim:** Pada laman web AVG (<http://www.avg.com/>) anda boleh mendapatkan seksyen berstruktur berasingan dan berhurafian bagi soalan lazim. Seksyen ini boleh diakses melalui opsyen menu **Pusat Sokongan / Soalan Lazim**. Sekali lagi, semua soalan dibahagikan dengan cara yang diatur dengan baik ke dalam kategori jualan, teknikal dan virus.
- **Mengenai virus & ancaman:** Bab khusus laman web AVG (<http://www.avg.com/>) dikhususkan untuk isu virus (*halaman web boleh diakses dari menu utama melalui opsyen Bantuan / Mengenai Virus dan Ancaman*). Dalam menu, pilih **Pusat Sokongan / Mengenai virus & ancaman** untuk memasukkan halaman yang memberikan gambaran keseluruhan berstruktur bagi maklumat berkaitan dengan ancaman dalam talian. Anda juga boleh mendapatkan arahan mengenai membuang virus, perisian pengintip dan nasihat mengenai cara untuk terus dilindungi.
- **Forum perbincangan:** Anda juga boleh menggunakan forum perbincangan pengguna AVG di <http://forums.avg.com>.