AVG Internet Security 2013

Manual Pengguna

Semakan dokumen 2013.11 (20.2.2013.)

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 libbzip2, Hak Cipta (c) 1996-2002 Julian R. Seward.

Kandungan

1. Pengenalan 5

2. Keperluan Pemasangan AVG 6

2.1 Sistem Pengendalian yang Disokong 6
2.2 Keperluan Minimum & Disyorkan HW 6

3. Proses Pemasangan AVG 7

3.1 Selamat datang: Pemilihan Bahasa 7
3.2 Selamat datang: Perjanjian Lesen 8
3.3 Aktifkan lesen anda 9
3.4 Pilih jenis pemasangan 10
3.5 Opsyen tersuai 12
3.6 Pasang AVG Security Toolbar 12
3.7 Perkembangan pemasangan 14
3.8 Pemasangan berjaya 15

4. Selepas Pemasangan 16

4.1 Pendaftaran produk 16
4.2 Akses ke antara muka pengguna 16
4.3 Mengimbas seluruh komputer 16
4.4 Ujian Eicar 16
4.5 Konfigurasi lalai AVG 17

5. Antara Muka Pengguna AVG 18

5.1 Navigasi Baris Atas 19
5.2 Maklumat Status Keselamatan 24
5.3 Gambaran keseluruhan Komponen 25
5.4 Aplikasi Saya 26
5.5 Pautan Pantas Imbas / Kemas Kini 26
5.6 Ikon Dulang Sistem 27
5.7 Alat AVG 29
5.8 Penasihat AVG 30
5.9 Pemecut AVG 31

6. Komponen AVG 32

6.1 Komputer 32
6.2 Pelayaran Web 33
6.3 Identiti 35

6.4 E-mel 37
6.5 Firewall 39
6.6 Quick Tune 42

7. AVG Security Toolbar 44

8. AVG Do Not Track 46

8.1 Antara muka AVG Do Not Track 46
8.2 Maklumat tentang proses penjejakan 48
8.3 Menyekat proses penjejakan 49
8.4 Tetapan AVG Do Not Track 49

9. Tetapan Lanjutan AVG 51

9.1 Penampilan 51
9.2 Bunyi 55
9.3 Menyahdayakan perlindungan AVG buat sementara waktu 56
9.4 Perlindungan Komputer 57
9.5 Pengimbas E-mel 63
9.6 Perlindungan Pelayaran Web 78
9.7 Identity Protection 81
9.8 Imbasan 82
9.9 Jadual 88
9.10 Kemas kini 97
9.11 Pengecualian 101
9.12 Bilik Kebal Virus 103
9.13 Perlindungan Diri AVG 104
9.14 Keutamaan Privasi 104
9.15 Abaikan status ralat 107
9.16 Penasihat – Rangkaian Diketahui 108

10. Tetapan Firewall 110

10.1 Umum 110
10.2 Aplikasi 112
10.3 Perkongsian fail dan pencetak 113
10.4 Tetapan lanjutan 115
10.5 Rangkaian ditentukan 116
10.6 Perkhidmatan sistem 117
10.7 Log 119

11. Pengimbasan AVG 121

11.1 Imbasan Pratakrif 122
11.2 Pengimbasan dalam Windows Explorer 130
11.3 Pengimbasan Garis Perintah 131
11.4 Penjadualan Imbasan 134
11.5 Keputusan Imbasan 141
11.6 Butiran keputusan imbasan 143

12. Bilik Kebal Virus 144

13. Sejarah 146

13.1 Keputusan imbasan 146
13.2 Pengesanan Resident Shield 147
13.3 Pengesanan Perlindungan E-mel 150
13.4 Penemuan Online Shield 151
13.5 Log sejarah acara 153
13.6 Log Firewall 154

14. Kemas kini AVG 156

14.1 Pelancaran kemas kini 156
14.2 Tahap kemas kini 156

15. Soalan Lazim dan Sokongan Teknikal 158

1. Pengenalan

Manual pengguna ini memberikan dokumentasi pengguna menyeluruh untuk **AVG Internet Security 2013**.

AVG Internet Security 2013 memberikan berbilang lapisan perlindungan untuk segala-gala yang anda lakukan dalam talian, yang bermaksud anda tidak perlu bimbang tentang 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 menerima perlindungan terbaik. Anda boleh membeli-belah dan menggunakan perkhidmatan bank dalam talian dengan selamat, menikmati kehidupan anda dalam rangkaian sosial atau melayari dan mencari dengan keyakinan menggunakan perlindungan masa nyata.

2. Keperluan Pemasangan AVG

2.1. Sistem Pengendalian yang Disokong

AVG Internet Security 2013 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)
- Windows 8 (x32 dan x64)

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

***Nota**: Komponen Identity tidak disokong pada Windows XP x64. Pada sistem pengendalian ini, anda boleh memasang AVG Internet Security 2013 tetapi hanya tanpa komponen IDP.*

2.2. Keperluan Minimum & Disyorkan HW

Keperluan perkakasan minimum untuk **AVG Internet Security 2013**:

- Intel Pentium CPU 1.5 GHz atau lebih cepat
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) memori RAM
- 1.3 GB ruang cakera keras kosong *(untuk tujuan pemasangan)*

Keperluan perkakasan disyorkan untuk **AVG Internet Security 2013**:

- Intel Pentium CPU 1.8 GHz atau lebih cepat
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) memori RAM
- 1.6 GB ruang cakera keras kosong *(untuk tujuan pemasangan)*

3. Proses Pemasangan AVG

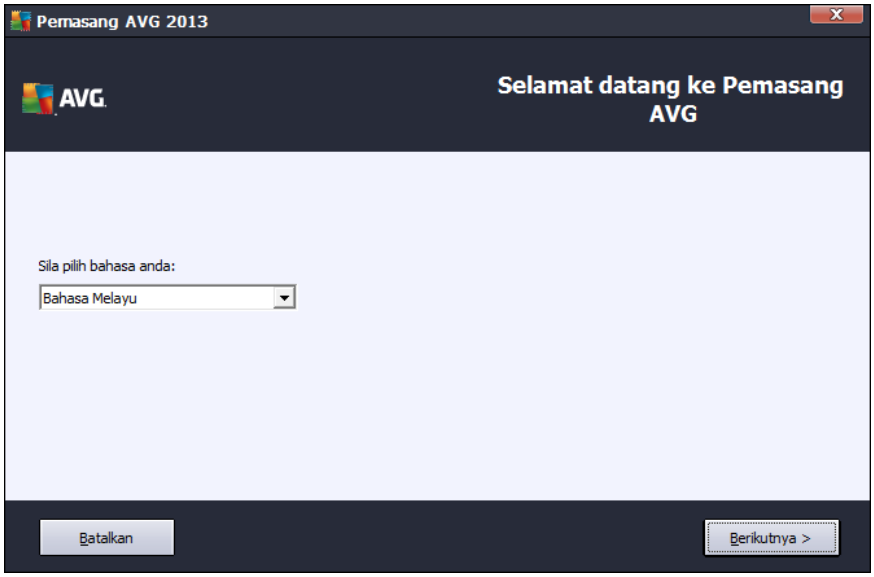
Untuk memasang **AVG Internet Security 2013** pada komputer anda, anda perlu mendapatkan fail pemasangan terkini. Untuk memastikan anda memasang versi terkini **AVG Internet Security 2013**, adalah disyorkan supaya anda memuat turun fail pemasangan daripada tapak web AVG (http://www.avg.com/). Bahagian ***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 dihala semula ke senarai lengkap bagi fail muat turun yang disuaikan untuk keperluan peribadi anda.

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. Kami menawarkan penerangan terperinci bagi setiap tetingkap dialog di bawah:

3.1. Selamat datang: Pemilihan Bahasa

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

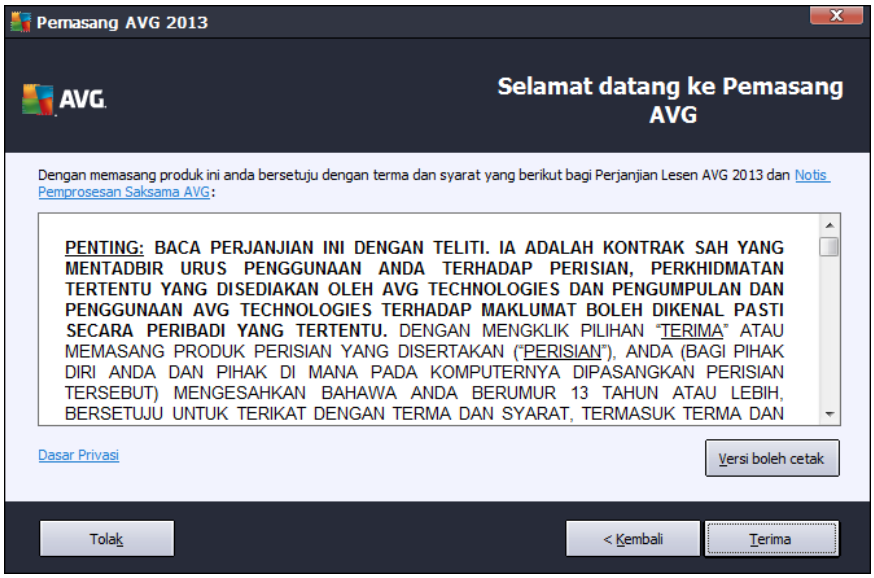


Dalam dialog ini anda boleh memilih bahasa yang digunakan untuk proses pemasangan. Klik kotak kombo untuk gulung bawah menu bahasa. Pilih bahasa yang dikehendaki, dan proses pemasangan akan meneruskan selanjutnya dalam bahasa pilihan anda.

Perhatian: Buat masa ini, anda hanya memilih bahasa bagi proses pemasangan. Aplikasi AVG Internet Security 2013 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 2013 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

Dialog ***Selamat Datang ke Pemasang AVG*** 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 menawarkan anda opsyen untuk mengetahui lebih lanjut mengenai ***Notis Pemprosesan Wajar AVG***, ***Pemeribadian AVG*** dan ***Dasar Privasi AVG*** *(semua fungsi yang dinyatakan dipaparkan di dalam dialog dalam bentuk hiperpautan aktif yang membawa anda ke tapak web khusus di mana anda boleh menemui maklumat terperinci)* . Klik pautan berkenaan untuk dihalakan semula ke tapak web AVG (http://www.avg.com/) di mana anda boleh menemui penerangan penuh pernyataan ini.

Butang kawalan

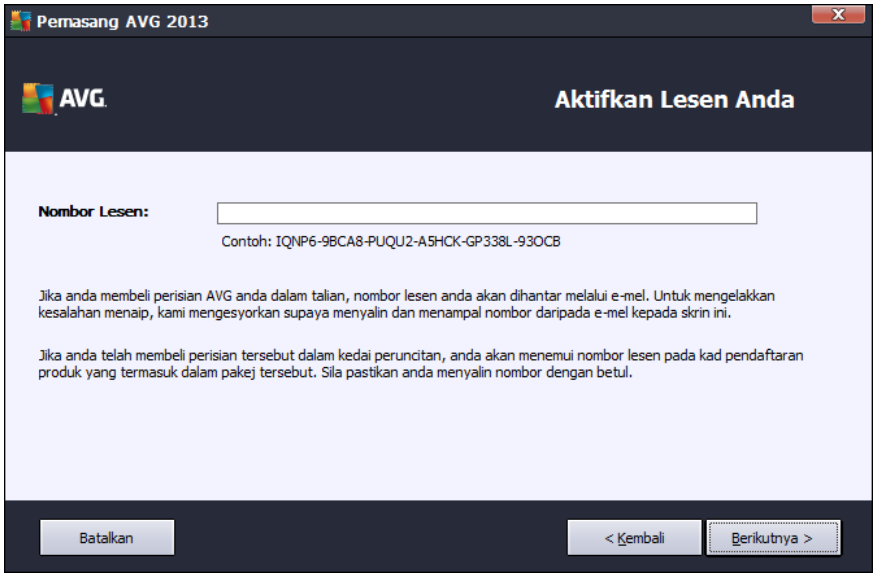
Daripada dialog persediaan pertama, terdapat hanya dua butang kawalan yang tersedia:

- ***Versi boleh cetak*** – Klik butang untuk memaparkan penerangan penuh perjanjian lesen AVG dalam antara muka web dan diatur untuk dicetak.
- ***Tolak*** – Klik untuk menolak perjanjian lesen. Proses persediaan akan berhenti dengan serta-merta. **AVG Internet Security 2013** 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 memasukkan nombor lesen anda ke dalam medan teks yang disediakan:



Di manakah untuk mencari nombor lesen

Nombor jualan boleh ditemui pada bungkusan CD dalam kotak **AVG Internet Security 2013** anda. Nombor lesen akan berada dalam e-mel pengesahan yang anda terima selepas membeli **AVG Internet Security 2013** anda dalam talian. Anda mesti menaip nombor betul-betul seperti yang ditunjukkan. Jika bentuk digital bagi nombor lesen tersedia (*dalam e-mel*), adalah disyorkan supaya anda menggunakan kaedah salin dan tampal untuk memasukkannya.

Bagaimana untuk menggunakan kaedah Salin & Tampal

Menggunakan kaedah ***Salin & Tampal*** untuk memasukkan nombor lesen **AVG Internet Security 2013** 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.

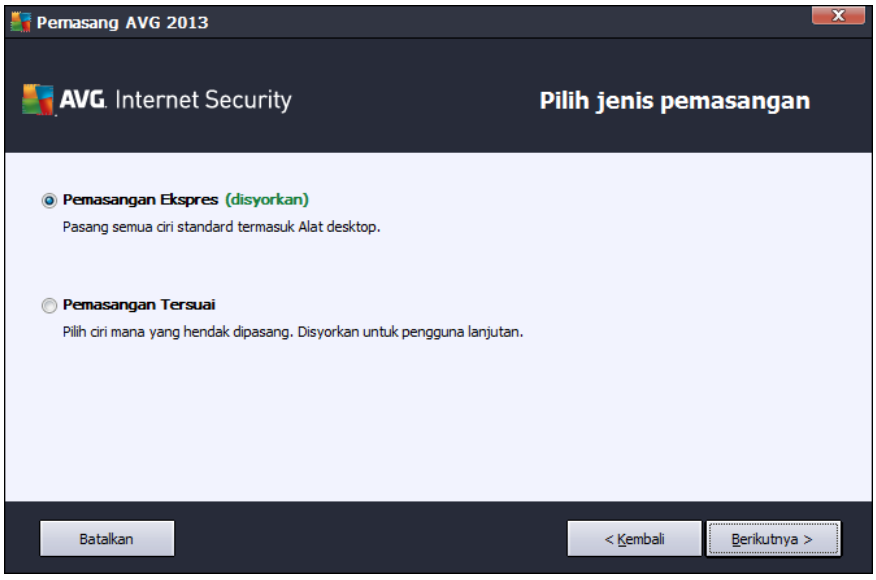
Butang kawalan

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

- ***Batal*** – klik untuk keluar daripada proses persediaan dengan serta-merta; **AVG Internet Security 2013** tidak akan dipasang!
- ***Undur*** – klik untuk kembali satu langkah ke belakang ke dialog persediaan sebelumnya.
- ***Seterusnya*** – klik untuk meneruskan pemasangan dan pergi satu langkah ke hadapan.

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 anda mengekalkan pemasangan ***Ekspres*** standard. Dengan cara ini anda memasang **AVG Internet Security 2013** dalam mod automatik sepenuhnya dengan tetapan yang dipratakrifkan oleh vendor atur cara, termasuk Alat AVG, AVG Security Toolbar dan mengkonfigurasikan AVG Secure Search sebagai pembekal carian lalai. Konfigurasi ini memberikan keselamatan maksimum yang digabungkan dengan penggunaan sumber yang optimum. Pada masa hadapan, jika terdapat keperluan untuk menukar konfigurasi, anda akan sentiasa mempunyai pilihan untuk melakukannya secara terus dalam aplikasi **AVG Internet Security 2013**.

Tekan butang ***Seterusnya*** untuk meneruskan ke dialog proses pemasangan berikut.

Pemasangan tersuai

Pemasangan Tersuai sepatutnya hanya digunakan oleh pengguna berpengalaman yang mempunyai alasan yang sah untuk memasang **AVG Internet Security 2013** 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 2013** harus dipasangkan. Secara lalainya, **AVG Internet Security 2013** 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.

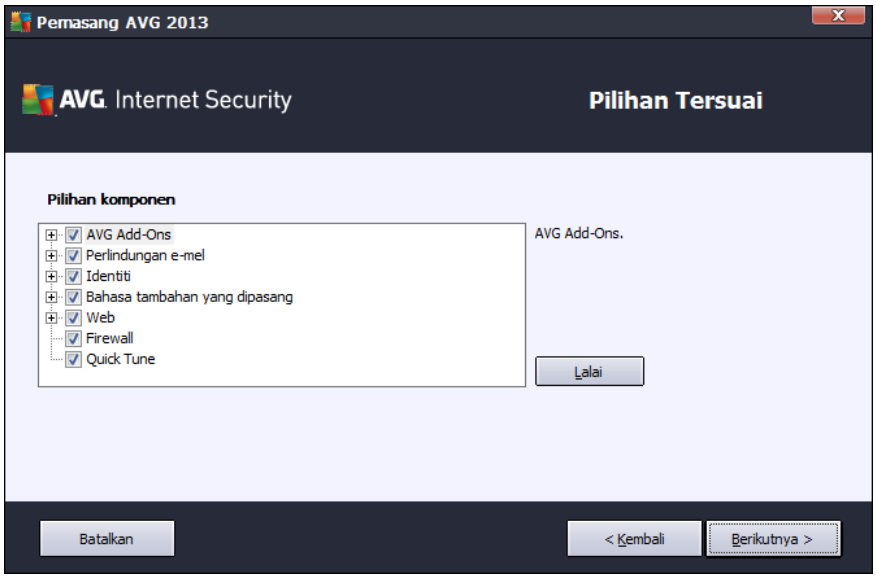
Butang kawalan

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

- ***Batal*** – klik untuk keluar daripada proses persediaan dengan serta-merta; **AVG Internet Security 2013** tidak akan dipasang!
- ***Undur*** – klik untuk kembali satu langkah ke belakang ke dialog persediaan sebelumnya.
- ***Seterusnya*** – klik untuk meneruskan pemasangan dan pergi satu langkah ke hadapan.

3.5. Opsyen tersuai

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



Seksyen ***Pemilihan Komponen*** menyediakan gambaran keseluruhan bagi semua komponen **AVG Internet Security 2013** 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 kefungsian 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 daripada proses persediaan dengan serta-merta; **AVG Internet Security 2013** tidak akan dipasang!
- ***Undur*** – klik untuk kembali satu langkah ke belakang ke dialog persediaan sebelumnya.
- ***Seterusnya*** – klik untuk meneruskan pemasangan dan pergi satu langkah ke hadapan.

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 pelayar Internet anda (*pelayar yang disokong buat masa ini ialah Microsoft Internet Explorer versi 6.0 atau lebih tinggi dan Mozilla Firefox versi 3.0 atau lebih tinggi*) dan untuk memberikan anda perlindungan dalam talian menyeluruh semasa melayari Internet. Buat masa ini,

pelayar Internet yang disokong ialah Internet Explorer (*versi 6.0 dan lebih tinggi*) dan/atau Mozilla Firefox (*versi 3.0 dan lebih tinggi*). Tiada pelayar lain yang disokong *(sekiranya anda menggunakan beberapa pelayar Internet alternatif, cth. Avant Browser, anda boleh mengalami kelakuan yang tidak dijangka).*

Dalam dialog itu anda mempunyai opsyen untuk memutuskan konfigurasi berikut:

- ***Tetapkan dan kekalkan AVG Secure Search sebagai pembekal carian lalai saya*** – biarkan ditanda untuk mengesahkan bahawa anda mahu menggunakan enjin AVG Secure Search yang bekerjasama dengan Link Scanner Surf Shield untuk keselamatan maksimum anda dalam talian.

- ***Pasang AVG Security Toolbar untuk meningkatkan perlindungan Internet saya*** – biarkan ditanda untuk memasang AVG Security Toolbar yang melindungi keselamatan maksimum anda semasa menyemak imbas Internet.

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

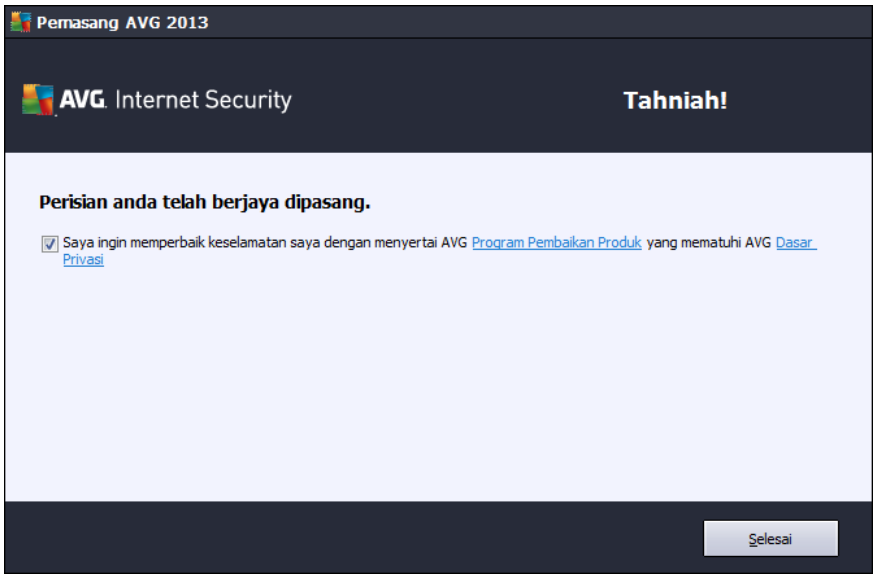
Terdapat dua butang kawalan tersedia dalam dialog ini:

- ***Minimumkan*** – Proses pemasangan boleh mengambil masa beberapa minit. Klik butang untuk meminimumkan tetingkap dialog kepada ikon yang boleh dilihat di bar sistem. Dialog akan muncul sekali lagi selepas pemasangan selesai.

- ***Batal*** – Butang ini hanya perlu digunakan jika anda ingin menghentikan proses pemasangan semasa. Sila ingat bahawa dalam hal sedemikian, **AVG Internet Security 2013** anda tidak akan dipasangkan!

3.8. Pemasangan berjaya

Dialog ***Pemasangan berjaya*** mengesahkan bahawa **AVG Internet Security 2013** anda telah dipasang dan dikonfigurasi sepenuhnya:



Program Pembaikan Produk dan Dasar Privasi

Di sini anda boleh memutuskan sama ada anda ingin menyertai dalam ***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. Semua data diperlakukan sebagai sulit dan mengikut Dasar Privasi AVG; klik pautan ***Dasar Privasi*** untuk dihalakan semula ke tapak web AVG (http://www.avg.com/) di mana anda boleh menemui penerangan penuh Dasar Privasi AVG. Jika anda bersetuju, sila biarkan opsyen ditandakan *(opsyen disahkan secara lalai)*.

Untuk menyelesaikan proses pemasangan tekan butang ***Selesai***.

4. Selepas Pemasangan

4.1. Pendaftaran produk

Setelah selesai melakukan pemasangan **AVG Internet Security 2013**, sila daftar produk anda dalam talian di tapak web AVG *(http://www.avg.com/)*. Selepas pendaftaran, anda akan mendapat akses penuh ke akaun pengguna AVG anda, surat berita Kemas Kinian 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 2013**. Sila pilih item navigasi baris atas / Opsyen / Daftar sekarang. Anda akan dihalakan semula ke halaman ***Pendaftaran*** di tapak web AVG *(http://www.avg.com/)*. Sila ikuti arahan yang diberikan pada halaman tersebut.

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 / AVG 2013***

4.3. Mengimbas seluruh komputer

Terdapat kemungkinan risiko bahawa virus komputer telah dihantar ke komputer anda sebelum pemasangan **AVG Internet Security 2013**. 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 supaya anda 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 2013** telah dipasang dengan betul, anda boleh melakukan ujian EICAR.

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

Cuba muat turun fail *eicar.com* dan simpannya pada cakera tempatan anda. Serta-merta selepas anda mengesahkan muat turun fail ujian, **AVG Internet Security 2013** anda akan bertindak balas padanya dengan amaran. Notis ini menunjukkan bahawa AVG dipasang dengan betul pada komputer anda.

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

4.5. Konfigurasi lalai AVG

Konfigurasi lalai (*cth. bagaimana aplikasi disediakan terus selepas pemasangan*) **AVG Internet Security 2013** ditetapkan oleh vendor perisian supaya semua komponen dan fungsi ditala untuk mencapai prestasi optimum. ***Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG! Perubahan pada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja.*** Jika anda mahu menukar konfigurasi AVG untuk disesuaikan dengan keperluan anda, pergi ke Tetapan Lanjutan AVG: pilih item menu utama *tetapan Opsyen/Lanjutan* dan sunting konfigurasi AVG dalam dialog Tetapan Lanjutan AVG yang baru dibuka.

5. Antara Muka Pengguna AVG

AVG Internet Security 2013 membuka tetingkap utama:

Tetingkap utama dibahagikan kepada beberapa bahagian:

- ***Navigasi baris atas*** terdiri daripada empat pautan aktif yang dibariskan dalam bahagian atas tetingkap utama *(Suka AVG, Laporan, Sokongan, Opsyen).* Butiran >>
- ***Maklumat Status Keselamatan*** memberikan maklumat asas mengenai status semasa **AVG Internet Security 2013** anda. Butiran >>
- ***Gambaran keseluruhan komponen yang dipasang*** boleh ditemui dalam jalur blok mendatar dalam bahagian tengah tetingkap utama. Komponen tersebut dipaparkan sebagai blok berwarna hijau cerah yang dilabelkan oleh ikon komponen masing-masing dan diberikan dengan maklumat mengenai status komponen. Butiran >>
- ***App Saya*** digambarkan secara grafik dalam jalur tengah sebelah bawah tetingkap utama dan menawarkan anda gambaran keseluruhan aplikasi pelengkap **AVG Internet Security 2013** yang sudah dipasang pada komputer anda atau disyorkan untuk pemasangan. Butiran >>
- ***Pautan pantas Imbas / Kemas Kini*** diletakkan dalam baris bawah blok dalam tetingkap utama. Butang ini membenarkan akses segera ke fungsi AVG paling penting dan paling kerap digunakan. Butiran >>

Di luar tetingkap utama **AVG Internet Security 2013**, terdapat lagi dua elemen kawalan yang anda boleh gunakan untuk mengakses aplikasi:

- ***Ikon dulang sistem*** terletak di penjuru kanan sebelah bawah monitor *(pada dulang sistem)*

dan menunjukkan status semasa **AVG Internet Security 2013**. Butiran >>

- ***Alat AVG*** boleh diakses dari bar sisi Windows (*disokong dalam OS Windows Vista/7/8 sahaja*), membenarkan akses pantas ke pengimbasan dan pengemas kinian di dalam **AVG Internet Security 2013**. Butiran >>

5.1. Navigasi Baris Atas

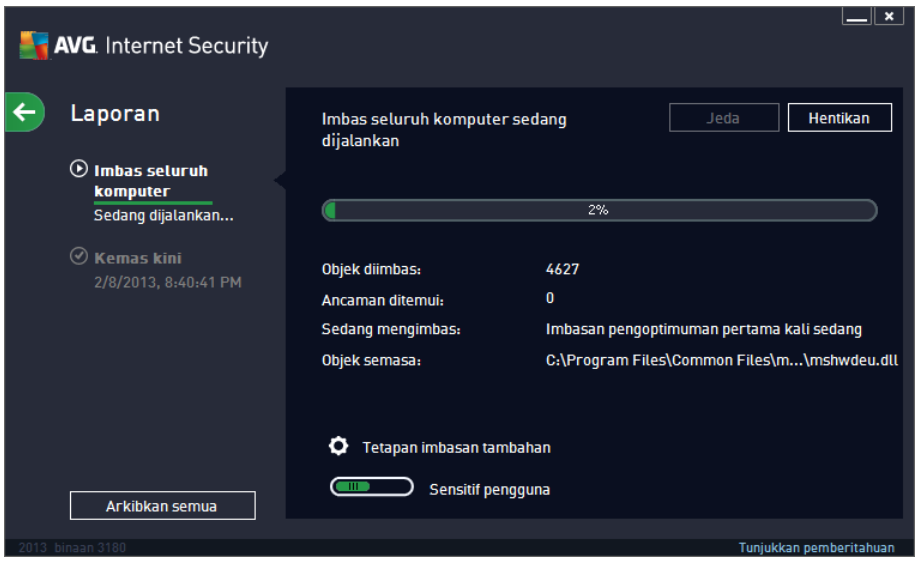
Navigasi baris atas terdiri daripada beberapa pautan aktif yang dibariskan dalam bahagian atas tetingkap utama. Navigasi termasuk butang yang berikut:

5.1.1. Suka AVG

Klik satu kali pada pautan untuk disambungkan ke komuniti Facebook AVG dan untuk berkongsi maklumat AVG terkini, berita, petua dan teknik untuk keselamatan internet maksimum anda.

5.1.2. Laporan

Membuka dialog ***Laporan*** baharu dengan gambaran keseluruhan semua laporan yang berkaitan mengenai imbasan dan proses kemas kini yang dilancarkan sebelum ini. Jika imbasan atau kemas kini sedang berjalan pada ketika ini, bulatan yang berputar akan dipaparkan bersebelahan teks ***Laporan*** dalam navigasi di sebelah atas antara muka pengguna utama. Klik bulatan ini untuk mendapatkan dialog yang menunjukkan kemajuan proses yang sedang berjalan:



5.1.3. Sokongan

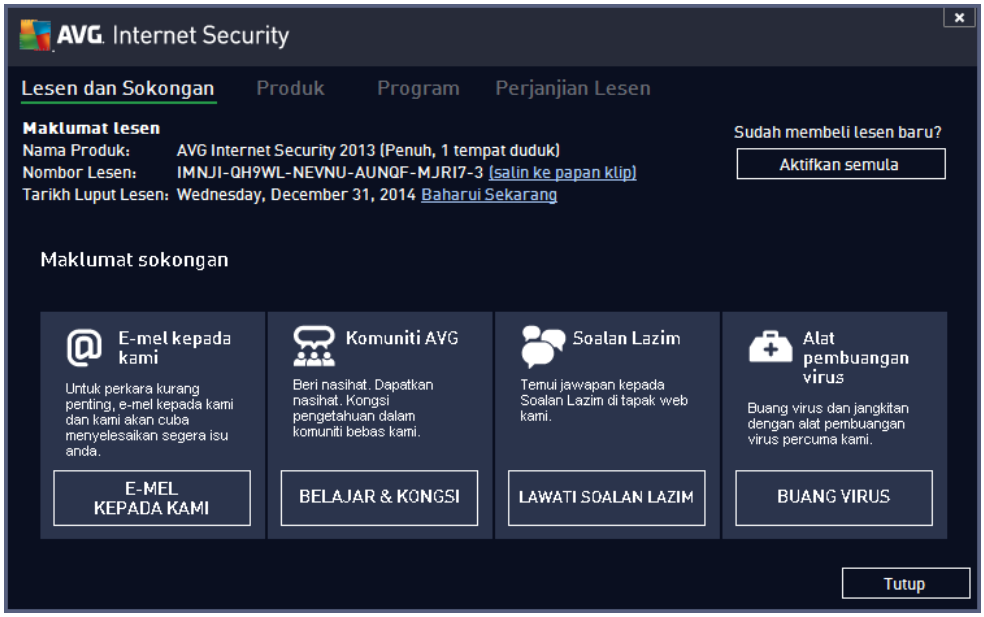
Membuka dialog baharu yang distrukturkan ke dalam empat tab di mana anda boleh menemui semua maklumat yang relevan mengenai **AVG Internet Security 2013**:

- ***Lesen dan Sokongan*** – Tab memberikan maklumat mengenai nama produk, nombor lesen dan tarikh tamat tempoh. Dalam bahagian di sebelah bawah dialog anda juga boleh menemui gambaran keseluruhan semua hubungan sokongan pelanggan yang tersedia yang disusun dengan jelas. Pautan aktif dan butang berikut tersedia dalam tab:

- *Aktifkan semula* – Klik untuk membuka dialog ***Aktifkan Perisian AVG*** baharu. Isikan nombor lesen anda ke dalam medan yang berkenaan untuk menggantikan nombor jualan anda *(yang anda gunakan semasa pemasanganAVG Internet Security 2013)* atau untuk menukar nombor lesen semasa anda dengan lesen lain *(cth. semasa menaik taraf kepada produk AVG yang lebih tinggi)*.

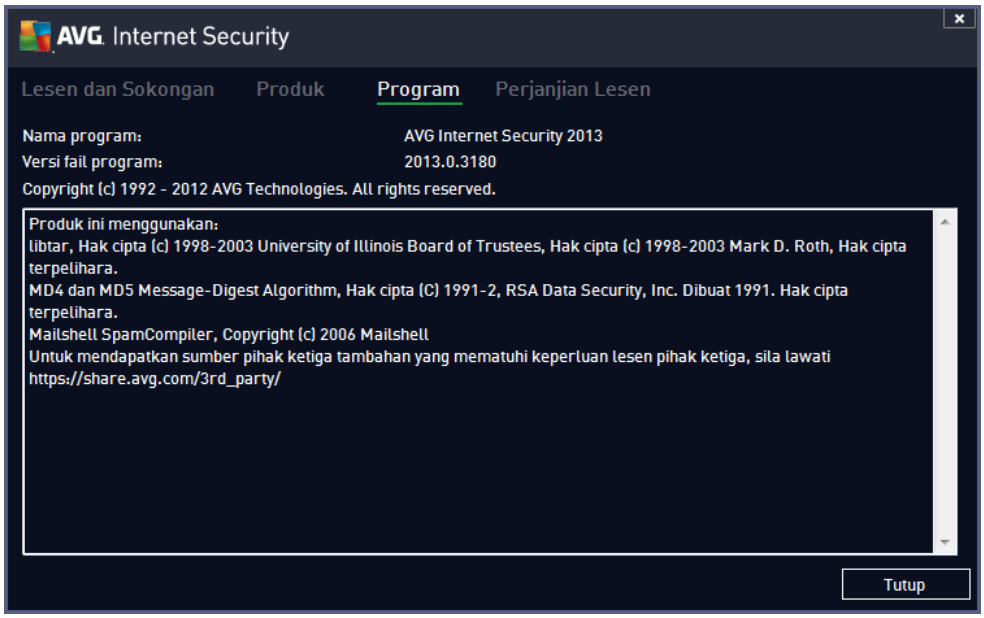
- *Salin ke papan klip* – Gunakan pautan ini untuk menyalin nombor lesen dan menampalnya di tempat yang diperlukan. Dengan cara ini anda boleh memastikan nombor lesen dimasukkan dengan betul.

- *Perbaharui Sekarang* – Kami mengesyorkan supaya anda membeli pembaharuan lesen **AVG Internet Security 2013** anda pada masa yang betul, sekurang-kurangnya sebulan sebelum penamatan tempoh lesen semasa anda. Anda akan dimaklumkan mengenai tarikh tamat tempoh yang semakin hampir. Klik pautan ini untuk dihalakan semula ke tapak web AVG *(http://www.avg.com/)* di mana anda menemui maklumat terperinci mengenai status lesen anda, tarikh tamat tempoh dan tawaran pembaharuan/naik taraf.



- ***Produk*** – Tab memberikan gambaran keseluruhan data teknikal **AVG Internet Security 2013** yang paling penting yang merujuk kepada maklumat produk, komponen yang dipasang, perlindungan e-mel yang dipasang dan maklumat sistem:

- ***Atur cara*** – Pada tab ini anda boleh menemui maklumat mengenai versi fail atur cara dan mengenai kod pihak ketiga yang digunakan dalam produk:



- ***Perjanjian Lesen*** – Tab menawarkan penerangan penuh perjanjian lesen antara anda dan AVG Technologies:

5.1.4. Opsyen

Penyelenggaraan **AVG Internet Security 2013** boleh diakses melalui item ***Opsyen***. Klik anak panah untuk membuka menu gulung bawah:

- ***Imbas komputer*** melancarkan imbasan seluruh komputer.
- ***Imbas folder dipilih...*** – Menukar kepada 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 atas permintaan ke atas satu fail khusus. Klik opsyen ini untuk membuka tetingkap baharu dengan struktur pepohon cakera anda. Pilih fail yang diingini dan sahkan pelancaran imbasan.
- ***Kemas kini*** – Melancarkan proses kemas kini secara automatik untuk **AVG Internet Security 2013**.
- ***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 diputuskan sambungan dari Internet; komputer anda disambungkan ke rangkaian yang tiada akses kepada Internet, dll.). Dalam tetingkap yang baru dibuka, pilih folder di mana anda telah meletakkan fail kemas kini sebelum ini dan melancarkan proses kemas kini.
- ***Bilik Kebal Virus*** – Membuka antara muka pada ruang kuarantin, Bilik Kebal Virus, di mana AVG membuang semua jangkitan yang dikesan yang tidak boleh dipulihkan secara automatik atas beberapa sebab. Di dalam kuarantin ini, fail yang dijangkiti dipencilkan, keselamatan komputer anda dijamin dan pada masa yang sama, fail yang dijangkiti disimpan untuk kemungkinan pembaikan pada masa hadapan.
- ***Sejarah*** – Menawarkan opsyen submenu khusus yang lebih lanjut:

- *Keputusan imbasan* – Membuka dialog yang memberikan gambaran keseluruhan keputusan pengimbasan.
- *Pengesanan Resident Shield* – Membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh Resident Shield.
- *Pengesanan Identity Protection* – Membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh Identity Protection.
- *Pengesanan Perlindungan E-mel* – Membuka dialog dengan gambaran keseluruhan bagi lampiran mesej mel yang dikesan sebagai berbahaya oleh komponen Perlindungan E-mel.
- *Penemuan Online Shield* – Membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh Online Shield.
- *Log sejarah acara* – Membuka antara muka log sejarah dengan gambaran keseluruhan semua **AVG Internet Security 2013** tindakan
- *Log Firewall* – Membuka dialog dengan gambaran keseluruhan terperinci bagi tindakan Firewall.

- ***Tetapan lanjutan...*** – Membuka dialog tetapan lanjutan AVG di mana anda boleh menyunting konfigurasi **AVG Internet Security 2013**. Secara umum, adalah disyorkan supaya anda mengekalkan tetapan lalai bagi aplikasi seperti yang ditakrifkan oleh vendor perisian.
- ***Tetapan firewall...*** – Membuka dialog kendiri untuk konfigurasi lanjutan bagi komponen Firewall.
- ***Kandungan bantuan*** – Membuka fail bantuan AVG.
- ***Dapatkan sokongan*** – Membuka tapak web AVG *(http://www.avg.com/)* di halaman pusat sokongan pelanggan.
- ***Web AVG Anda*** – Membuka tapak web AVG *(http://www.avg.com/).*
- ***Tentang Virus dan Ancaman*** – Membuka ensiklopedia virus dalam talian di mana anda boleh mencari maklumat terperinci mengenai virus yang dikenal pasti.
- ***Aktifkan (Semula)*** – Membuka dialog ***Aktifkan AVG*** dengan data yang telah anda berikan semasa proses pemasangan. Dalam dialog ini, anda boleh memasukkan nombor lesen anda sama ada dengan menggantikan nombor jualan (*yang anda telah pasangkan AVG*), atau untuk menggantikan nombor lesen lama (*cth. semasa menaik taraf ke produk AVG baharu*).
- ***Daftar sekarang / Akaun Saya*** – Menyambung ke halaman pendaftaran tapak web AVG (http://www.avg.com/). Sila isikan data pendaftaran anda; hanya pelanggan yang mendaftarkan produk AVG mereka boleh menerima sokongan teknikal percuma. Jika menggunakan versi percubaan **AVG Internet Security 2013**, dua item yang muncul kemudian sebagai ***Beli sekarang*** dan ***Aktifkan***, membolehkan anda membeli versi penuh atur cara dengan serta-merta. Untuk **AVG Internet Security 2013** yang dipasang dengan nombor jualan, item dipaparkan sebagai ***Daftar*** dan ***Aktifkan***.

- ***Tentang AVG*** – Membuka dialog baharu dengan empat tab yang memberikan data mengenai lesen anda yang telah dibeli dan sokongan yang boleh diakses, maklumat produk dan atur cara serta pernyataan penuh perjanjian lesen.

5.2. Maklumat Status Keselamatan

Seksyen ***Maklumat Status Keselamatan*** terletak di bahagian atas tetingkap utama **AVG Internet Security 2013**. Dalam bahagian ini, anda akan sentiasa mendapatkan maklumat mengenai status keselamatan terkini bagi **AVG Internet Security 2013** anda. Sila lihat gambaran keseluruhan ikon yang berkemungkinan bertindih dalam bahagian ini dan maksudnya:

– ikon berwarna hijau menunjukkan bahawa ***AVG Internet Security 2013 anda berfungsi sepenuhnya***. Komputer anda dilindungi sepenuhnya, terkini dan semua komponen dipasang berfungsi dengan betul.

– ikon berwarna kuning memberi amaran bahawa ***satu atau lebih komponen dikonfigurasi dengan salah*** dan anda harus menyemak tetapan/sifatnya. Tiada masalah kritikal dalam **AVG Internet Security 2013** dan anda mungkin telah memutuskan untuk mematikan komponen atas sebab tertentu. Anda masih dilindungi! Walau bagaimanapun, sila berikan perhatian kepada tetapan masalah komponen! Komponen yang dikonfigurasi dengan salah akan dipaparkan dengan amaran berjalur oren dalam antara muka pengguna utama.

Ikon kuning juga muncul jika atas sebab tertentu, anda telah memutuskan untuk mengabaikan status ralat komponen. Opsyen ***Abaikan status ralat*** boleh diakses dalam cabang Tetapan lanjutan / Abaikan status ralat. Di sana anda mempunyai pilihan untuk menyatakan anda menyedari tentang keadaan ralat komponen tetapi atas sebab tertentu anda hendak menyimpan **AVG Internet Security 2013** dan anda tidak mahu diberi amaran mengenainya. Anda mungkin perlu menggunakan opsyen ini dalam situasi tertentu tetapi amat disyorkan supaya anda mematikan opsyen ***Abaikan status ralat*** secepat mungkin!

Selain itu, ikon berwarna kuning juga akan dipaparkan jika **AVG Internet Security 2013** anda memerlukan komputer supaya dimulakan semula (***Mula semula diperlukan***). Sila beri perhatian kepada amaran ini dan mulakan semula PC anda.

– ikon berwarna oren menunjukkan bahawa ***AVG Internet Security 2013 berada dalam status kritikal***! Satu atau lebih komponen tidak berfungsi dengan betul dan **AVG Internet Security 2013** 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 2013 tidak ditetapkan ke prestasi optimum, butang baharu yang dipanggil Klik untuk baiki (secara alternatif Klik untuk baikinya semua jika masalah berkenaan melibatkan lebih daripada satu komponen) muncul di sebelah maklumat status keselamatan. Tekan butang ini untuk melancarkan proses automatik semakan dan konfigurasi atur cara. Ini adalah cara mudah untuk menetapkan AVG Internet Security 2013 kepada 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 2013 juga boleh diperoleh pada bila-bila masa daripada ikon dulang sistem.*

5.3. Gambaran keseluruhan Komponen

Gambaran keseluruhan komponen yang dipasang boleh ditemui dalam jalur blok mendatar dalam bahagian tengah tetingkap utama. Komponen tersebut dipaparkan sebagai blok berwarna hijau cerah yang dilabelkan oleh ikon komponen masing-masing. Setiap blok memberikan maklumat mengenai status perlindungan semasa. Jika komponen dikonfigurasi dengan betul dan berfungsi sepenuhnya, maklumat tersebut dinyatakan dalam huruf berwarna hijau. Jika komponen dihentikan, kefungsiannya terhad atau komponen berada dalam keadaan ralat, anda akan dimaklumkan oleh teks amaran yang dipaparkan dalam medan teks berwarna oren. ***Adalah amat disyorkan supaya anda memberi perhatian kepada tetapan komponen masing-masing!***

Gerakkan tetikus di atas komponen untuk memaparkan teks pendek di bahagian bawah tetingkap utama. Teks memberikan pengenalan asas kepada kefungsian komponen. Juga, ia memaklumkan mengenai status semasa komponen dan menentukan perkhidmatan komponen mana yang tidak dikonfigurasi dengan betul.

Senarai komponen yang dipasang

Dalam **AVG Internet Security 2013** bahagian ***Gambaran Keseluruhan Komponen*** mengandungi maklumat mengenai komponen berikut:

- ***Komputer*** – Komponen ini meliputi dua perkhidmatan: ***AntiVirus Shield*** mengesan virus, spyware, cecacing, trojan, fail boleh laku yang tidak dikehendaki atau pustaka di dalam sistem anda dan melindungi anda daripada adware yang berniat jahat manakala ***Anti-Rootkit*** mengimbas rootkit berbahaya yang tersembunyi di dalam aplikasi, pemacu atau pustaka. Butiran >>
- ***Pelayaran Web*** – Melindungi anda dari serangan berasaskan web semasa anda mencari dan melayari Internet. Butiran >>
- ***Identiti*** – Komponen tersebut menjalankan perkhidmatan ***Identity Shield*** yang sentiasa melindungi aset digital anda daripada ancaman baharu dan tidak diketahui di Internet. Butiran >>
- ***E-mel*** – Menyemak mesej e-mel masuk anda untuk mengesan SPAM dan menyekat virus, serangan pemalsuan data atau ancaman lain. Butiran >>
- ***Firewall*** – Mengawal semua komunikasi pada setiap port rangkaian, melindungi anda daripada serangan berniat jahat dan menyekat semua cubaan gangguan. Butiran >>

Tindakan boleh diakses

- ***Gerakkan tetikus pada sebarang ikon komponen*** untuk menyerlahkannya dalam gambaran keseluruhan komponen. Pada masa yang sama, penerangan kefungsian asas komponen muncul di bahagian bawah antara muka pengguna.
- ***Ikon komponen sekali klik*** untuk membuka antara muka komponen itu sendiri dengan

maklumat mengenai status semasa komponen dan mengakses konfigurasi dan data statistiknya.

5.4. Aplikasi Saya

Dalam kawasan ***App Saya*** *(baris blok hijau di bawah set komponen)* anda boleh menemui gambaran keseluruhan aplikasi AVG tambahan yang telah dipasang pada komputer anda atau disyorkan untuk pemasangan. Blok dipaparkan secara bersyarat dan boleh mewakili sebarang aplikasi berikut:

- ***Perlindungan mudah alih*** adalah aplikasi yang melindungi telefon bimbit anda daripada virus dan malware. Ia juga memberikan anda keupayaan untuk menjejak telefon pintar anda dari jauh jika anda terpisah daripadanya.

- ***LiveKive*** adalah khusus untuk sandaran data dalam talian pada pelayan yang terjamin. 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 yang didayakan web, termasuk peranti iPhones dan Android.

- ***Family Safety*** membantu anda melindungi anak anda daripada tapak web, kandungan media dan carian dalam talian yang tidak sesuai serta 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 membolehkan anda menetapkan tahap perlindungan yang sesuai untuk setiap anak anda dan memantaunya secara berasingan melalui log masuk unik.

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

- ***MultiMi*** mengumpulkan semua e-mel dan akaun sosial anda di satu tempat yang selamat, menjadikannya mudah untuk kekal berhubung dengan keluarga dan rakan anda, untuk menyemak imbas Internet, berkongsi foto, video dan fail. MultiMi mengandungi perkhidmatan LinkScanner yang melindungi anda daripada ancaman di web yang semakin meningkat dengan menganalisis halaman web disebalik semua pautan pada sebarang halaman web yang sedang anda lihat dan memastikan ia selamat.

- ***AVG Toolbar*** tersedia secara langsung dalam pelayar Internet anda dan mengawal keselamatan maksimum anda semasa menyemak imbas Internet.

Untuk maklumat terperinci mengenai sebarang aplikasi ***App Saya*** klik blok yang berkenaan. Anda akan dihalakan semula ke halaman web AVG khusus, di mana anda juga boleh memuat turun komponen dengan serta-merta.

5.5. Pautan Pantas Imbas / Kemas Kini

Pautan pantas terdapat di barisan butang di sebelah bawah dalam antara muka pengguna **AVG Internet Security 2013**. Pautan ini membenarkan anda untuk mengakses ciri yang paling penting dan paling kerap digunakan bagi aplikasi dengan segera, iaitu pengimbasan dan kemas kini. Pautan

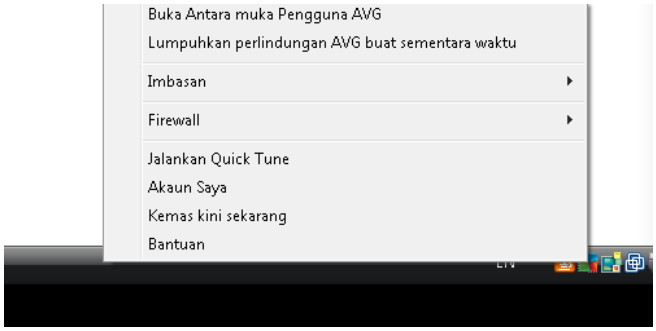
pantas boleh diakses dari semua dialog antara muka pengguna:

- ***Imbas sekarang*** – Butang dibahagikan secara grafik kepada dua bahagian. Ikuti pautan ***Imbas sekarang*** untuk melancarkan Imbas Seluruh Komputer dengan serta-merta dan melihat kemajuan dan keputusannya dalam tetingkap Laporan yang dibuka secara automatik. Butang ***Opsyen*** membuka dialog ***Opsyen Imbasan*** di mana anda boleh menguruskan imbasan berjadual dan menyunting parameter Imbas Seluruh Komputer / Imbas Fail atau Folder Tertentu. *(Untuk butiran, lihat bab Pengimbasan AVG)*

- ***Kemas kini sekarang*** – Tekan butang untuk melancarkan kemas kini produk dengan serta-merta. Anda akan dimaklumkan mengenai keputusan kemas kini dalam dialog slaid pada ikon dulang sistem AVG. *(Untuk butiran, lihat bab Kemas Kini AVG)*

5.6. Ikon Dulang Sistem

Ikon Dulang Sistem AVG *(pada bar tugas Windows anda, penjuru bawah sebelah kanan monitor anda)* menunjukkan status semasa bagi **AVG Internet Security 2013** anda. Ia boleh dilihat pada setiap masa dalam dulang sistem anda, tidak kira sama ada antara muka pengguna bagi **AVG Internet Security 2013** anda dibuka atau ditutup:



Paparan Ikon Dulang Sistem AVG

- Dalam warna penuh dengan tiada elemen ditambah, ikon menunjukkan bahawa semua komponen **AVG Internet Security 2013** 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. *(Dengan mengesahkan opsyen 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 seruan menandakan bahawa komponen *(atau malahan, lebih banyak komponen)* berada dalam keadaan ralat. Sentiasa beri perhatian kepada amaran sedemikian dan cuba selesaikan 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 berwarna penuh dengan anak panah bermaksud bahawa salah satu daripada imbasan **AVG Internet Security 2013** sedang dijalankan sekarang.

Maklumat Ikon Dulang Sistem AVG

Ikon Dulang Sistem AVG juga memberitahu mengenai aktiviti semasam dalam **AVG Internet Security 2013** anda dan mengenai kemungkinan perubahan status dalam atur cara (*cth. pelancaran automatik bagi imbasan atau kemas kini berjadual, bertukar profil Firewall, perubahan status komponen, perulangan status ralat, ...*) melalui tetingkap timbul yang dibuka daripada 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 2013**, 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 2013**.

- ***Lumpuhkan perlindungan AVG buat sementara waktu*** – opsyen ini membolehkan anda untuk mematikan keseluruhan perlindungan yang dilindungi oleh **AVG Internet Security 2013** 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 2013** sebelum memasang perisian atau pemacu baharu, walaupun jika pemasang 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 2013** 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..

- ***Imbasan*** – klik untuk membuka menu konteks untuk imbasan dipratakrif (*Imbas Seluruh Komputer* dan *Imbas Fail atau Folder Tertentu*) 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 kemudiannya boleh menetapkan prioritinya, secara alternatif menghentikan atau menjeda imbasan yang sedang berjalan. Tindakan berikut juga boleh diakses: *Tetapkan keutamaan untuk semua imbasan, Jeda semua imbasan* atau *Hentikan semua imbasan*.

- ***Jalankan Penganalisis PC*** – klik untuk melancarkan komponen Penganalisis PC

- ***Akaun Saya*** – Membuka halaman utama Akaun Saya di mana anda boleh menguruskan produk langganan anda, membeli perlindungan tambahan, memuat turun fail pemasangan,

menyemak pesanan dan invois anda sebelum ini dan menguruskan maklumat peribadi anda.

- ***Kemas kini sekarang*** – melancarkan kemas kini segera.
- ***Bantuan*** – membuka fail bantuan pada halaman mula.

5.7. Alat AVG

Alat AVG dipaparkan pada desktop Windows (*Bar Sisi Windows*). Aplikasi ini hanya disokong dalam sistem pengendalian Windows Vista dan Windows 7/8. ***Alat AVG*** menawarkan akses segera kepada fungsi **AVG Internet Security 2013** yang paling penting, iaitu pengimbasan dan pengemaskinian**:**

Kawalan alat AVG

Jika diperlukan, alat AVG membenarkan anda melancarkan imbasan atau kemas kini dengan serta-merta; juga memberikan pautan pantas yang menyambungkan anda ke rangkaian sosial utama dan menawarkan pencarian pantas:

- ***Imbas sekarang*** – klik pautan ***Imbas sekarang*** untuk memulakan imbasan seluruh komputer terus. Anda boleh melihat kemajuan imbasan dalam antara muka pengguna alternatif 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 imbasan. 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*****AVG Internet Security 2013** untuk melancarkan kemas kini secara terus dari dalam alat:

- ***Pautan Twitter*** – membuka antara muka ***alat AVG*** baharu yang memberikan gambaran keseluruhan suapan AVG terkini yang dikirimkan ke Twitter. Ikuti pautan ***Lihat semua suapan AVG Twitter*** untuk membuka pelayar Internet anda dalam tetingkap baharu dan anda akan dihalakan semula terus ke tapak web Twitter, khususnya ke halaman yang dikhususkan bagi berita AVG:

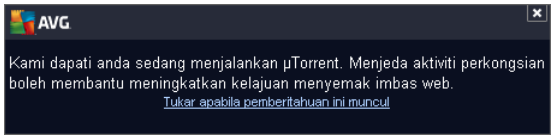
- ***Pautan Facebook*** – membuka pelayar Internet anda di tapak web Facebook, khususnya di halaman ***komuniti AVG***.

- ***Kotak carian*** – taipkan kata kunci dan dapatkan keputusan carian dengan serta-merta dalam tetingkap yang baru dibuka dengan penyemak imbas web lalai anda.

5.8. Penasihat AVG

Penasihat AVG telah direka bentuk untuk mengesan masalah yang mungkin memperlahankan komputer anda atau memberinya risiko dan untuk mengesyorkan tindakan bagi menyelesaikan situasi ini. Jika anda mengalami kelambatan komputer secara tiba-tiba *(menyemak imbas Internet, prestasi keseluruhan)*, ia tidak selalunya jelas apa sebenarnya puncanya dan seterusnya, cara untuk menyelesaikan masalah itu. Masa itulah ***Penasihat AVG*** akan membantu: Ia akan memaparkan pemberitahuan dalam dulang sistem yang memberitahu anda kemungkinan masalah itu dan mencadangkan bagaimana untuk membaikinya. ***Penasihat AVG*** 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 gelongsor timbul di atas dulang sistem:



Secara khususnya, ***Penasihat AVG*** mengawasi yang berikut:

- ***Keadaan mana-mana pelayar web yang dibuka buat masa ini***. Pelayar web boleh menyaratkan memori, terutamanya jika berbilang tab atau tetingkap telah dibuka untuk beberapa lama dan menggunakan terlalu banyak sumber sistem. mis. melambatkan komputer anda. Dalam situasi sebegini, memulakan semula pelayar web biasanya boleh membantu.

- ***Menjalankan sambungan Rakan Ke Rakan***. Selepas menggunakan protokol P2P untuk berkongsi fail, sambungan tersebut kadangkala kekal aktif, menggunakan jumlah tertentu lebar jalur anda. Hasilnya, anda boleh melihat kelambatan menyemak imbas.

- ***Rangkaian tidak diketahui dengan nama biasa***. Ini biasanya hanya terpakai kepada pengguna yang menyambung kepada berbagai rangkaian, lazimnya dengan komputer mudah alih: Jika rangkaian baharu yang tidak diketahui mempunyai nama yang sama seperti rangkaian diketahui yang kerap digunakan *(cth. Rumah atau WifiSaya)*, kekeliruan boleh berlaku dan anda boleh menyambung kepada rangkaian yang tidak diketahui sama sekali dan berkemungkinan tidak selamat secara tidak sengaja. ***Penasihat AVG*** boleh menghalang perkara ini dengan memberi amaran kepada anda bahawa nama yang diketahui itu sebenarnya mewakili rangkaian baharu. Sudah semestinya, jika anda memutuskan bahawa rangkaian yang tidak diketahui itu adalah selamat, anda boleh menyimpannya pada senarai rangkaian yang diketahui ***AVG Advisor*** supaya ia tidak dilaporkan lagi pada masa hadapan.

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.

Pelayar web yang disokong

Ciri ini berfungsi dengan pelayar web berikut: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.9. Pemecut AVG

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 tetingkap timbul dulang sistem.

6. Komponen AVG

6.1. Komputer

Komponen ***Komputer*** meliputi dua perkhidmatan keselamatan utama: ***AntiVirus*** dan ***Anti-Rootkit***:

- ***AntiVirus*** terdiri daripada enjin pengimbasan yang mengawal semua fail, kawasan sistem komputer dan media boleh dialihkan *(cakera kilat dsb.)* dan mengimbas virus yang diketahui. Sebarang virus yang dikesan akan disekat daripada melakukan sebarang tindakan dan kemudiannya akan dibersihkan atau dikuarantin dalam Bilik Kebal Virus. Anda tidak akan menyedari proses tersebut semasa perlindungan residen berjalan "dalam latar belakang". AntiVirus juga menggunakan imbasan heuristik, di mana fail diimbas untuk mengesan ciri virus yang lazim. Ini bermaksud bahawa AntiVirus boleh mengesan virus yang baharu dan tidak diketahui, jika virus baharu itu mengandungi beberapa ciri lazim yang terdapat pada virus sedia ada. **AVG Internet Security 2013** juga boleh menganalisis dan mengesan aplikasi boleh laku atau pustaka DLL yang berpotensi tidak diingini dalam sistem *(berbagai jenis spyware, adware dsb.)*. Tambahan pula, AntiVirus mengimbas pendaftar sistem anda untuk mengesan entri yang mencurigakan, fail Internet sementara dan membolehkan anda memperlakukan semua item berpotensi berbahaya dengan cara yang sama seperti sebarang jangkitan lain.

- ***Anti-Rootkit*** ialah alat khusus yang mengesan dan membuang rootkit berbahaya, mis. atur cara dan teknologi yang boleh menyamar kehadiran perisian berniat jahat pada komputer anda. Rootkit direka bentuk untuk melakukan kawalan asas sistem komputer tanpa kebenaran daripada pemilik sistem dan pengurus yang sah. Anti-Rootkit boleh mengesan rootkit berdasarkan pada set peraturan yang diprataktif. Jika Anti-Rootkit menemui rootkit, ia tidak semestinya bermaksud rootkit tersebut telah dijangkiti. Kadangkala, rootkit digunakan sebagai pemacu atau ia adalah sebahagian daripada aplikasi yang betul.

Kawalan dialog

Untuk bertukar antara kedua-dua bahagian dialog, anda boleh mengklik di mana-mana dalam panel perkhidmatan yang berkenaan. Panel tersebut kemudiannya diserlahkan dengan warna biru cerah. Dalam kedua-dua bahagian dialog anda boleh menemui kawalan berikut. Kefungsian mereka adalah serupa sama ada ia dimiliki oleh satu perkhidmatan keselamatan atau *(AntiVirus atau Anti-Rootkit)* yang lain:

Didayakan / Dilumpuhkan – Butang tersebut boleh mengingatkan anda kepada lampu isyarat, dari segi penampilan dan kefungsian. Klik satu kali untuk bertukar antara dua posisi. Warna hijau bermaksud ***Didayakan***, yang bermakna perkhidmatan keselamatan AntiVirus diaktifkan dan berfungsi sepenuhnya. Warna merah mewakili status ***Dilumpuhkan***, cth. perkhidmatan dinyahaktifkan. Jika anda tidak mempunyai sebarang sebab yang kukuh untuk menyahaktifkan perkhidmatan, kami amat mengesyorkan supaya anda mengekalkan tetapan lalai untuk semua konfigurasi keselamatan. Tetapan lalai menjamin prestasi aplikasi yang optimum dan keselamatan maksimum anda. Jika atas sebab tertentu anda berhasrat untuk menyahaktifkan perkhidmatan, anda akan diberi amaran mengenai risiko yang boleh berlaku dengan serta-merta dengan tanda ***Amaran*** merah dan maklumat bahawa anda tidak dilindungi sepenuhnya pada masa ini. ***Sila ingat bahawa anda seharusnya mengaktifkan perkhidmatan semula secepat mungkin!***

Tetapan – Klik butang untuk dihalakan semula ke antara muka tetapan lanjutan. Dengan tepat lagi, dialog berkenaan dibuka dan anda akan dapat mengkonfigurasi perkhidmatan yang dipilih, cth. AntiVirus atau Anti-Rootkit. Dalam antara muka tetapan lanjutan, anda boleh menyunting semua konfigurasi bagi setiap perkhidmatan keselamatan dalam **AVG Internet Security 2013** tetapi sebarang konfigurasi boleh disyorkan kepada pengguna berpengalaman sahaja!

Statistik – Klik butang untuk dihalakan semula ke halaman khusus pada tapak web AVG (http://www.avg.com/). Pada halaman ini, anda boleh menemui gambaran keseluruhan statistik terperinci bagi semua aktiviti **AVG Internet Security 2013** yang dilakukan pada komputer anda dalam tempoh masa tertentu dan secara keseluruhan.

Butiran – Klik butang dan penerangan ringkas perkhidmatan yang diserlahkan muncul di bahagian bawah dialog.

– Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke antara muka pengguna utama dengan gambaran keseluruhan komponen.

Dalam bahagian Anti-Rootkit, anda juga akan menemui butang ***Imbas rootkit*** khusus yang boleh anda gunakan untuk melancarkan terus imbasan rootkit bebas *(namun, imbasan rootkit adalah bahagian Imbas seluruh komputer yang terselindung)*.

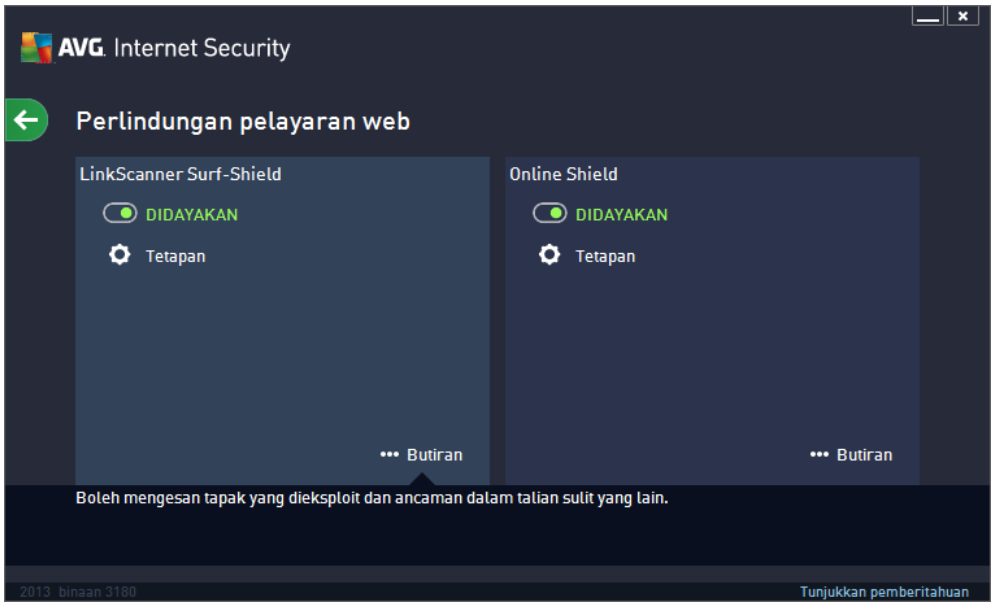
6.2. Pelayaran Web

Perlindungan pelayaran web terdiri daripada dua perkhidmatan: ***LinkScanner Surf-Shield*** dan ***Online Shield***:

- ***LinkScanner Surf-Shield*** 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 laman berkenaan lebih daripada 24 jam. LinkScanner melindungi anda dengan menganalisis halaman web di sebalik semua pautan

pada mana-mana halaman web yang anda sedang lihat dan memastikan ia selamat pada satu-satunya masa yang paling penting – semasa anda akan mengklik pautan berkenaan. ***LinkScanner Surf-Shield bukan bertujuan untuk perlindungan platform pelayan!***

- ***Online Shield*** adalah sejenis perlindungan residen masa nyata; ia mengimbas kandungan halaman web yang dilawati (dan kemungkinan fail yang dimasukkan di dalamnya) sebelum ini dipaparkan dalam pelayar web anda atau dimuat turun ke komputer anda. Online Shield mengesan halaman yang anda akan lawati menyertakan beberapa javascript berbahaya dan menghalang halaman daripada dipaparkan. Serta, ia mengenal pasti malware yang terkandung dalam halaman dan menghentikan muat turunnya dengan serta-merta supaya ia tidak dapat masuk ke komputer anda. Perlindungan yang berkuasa ini akan menyekat sebarang kandungan halaman web yang berniat jahat yang anda cuba buka dan menghalangnya daripada dimuat turun ke komputer anda. Dengan ciri ini didayakan, mengklik pautan atau menaip dalam URL ke tapak berbahaya akan menghalang anda daripada membuka halaman web secara automatik, dengan itu, melindungi anda daripada dijangkiti secara tidak sengaja. Adalah penting untuk mengingati bahawa halaman web yang dieksploitasi boleh menjangkiti komputer anda hanya dengan melawati tapak yang terjejas. ***Online Shield bukan bertujuan untuk perlindungan platform pelayan!***



Kawalan dialog

Untuk bertukar antara kedua-dua bahagian dialog, anda boleh mengklik di mana-mana dalam panel perkhidmatan yang berkenaan. Panel tersebut kemudiannya diserlahkan dengan warna biru cerah. Dalam kedua-dua bahagian dialog anda boleh menemui kawalan berikut. Kefungsiannya adalah serupa sama ada ia dimiliki oleh satu perkhidmatan keselamatan atau *(LinkScanner Surf-Shield atau Online Shield)* yang lain:

Didayakan / Dilumpuhkan – Butang tersebut boleh mengingatkan anda kepada lampu isyarat, dari segi penampilan dan kefungsian. Klik satu kali untuk bertukar antara dua posisi. Warna hijau bermaksud ***Didayakan***, yang bermakna perkhidmatan keselamatan LinkScanner Surf-Shield / Online Shield diaktifkan dan berfungsi sepenuhnya. Warna merah mewakili status ***Dilumpuhkan***, cth. perkhidmatan dinyahaktifkan. Jika anda tidak mempunyai

sebarang sebab yang kukuh untuk menyahaktifkan perkhidmatan, kami amat mengesyorkan supaya anda mengekalkan tetapan lalai untuk semua konfigurasi keselamatan. Tetapan lalai menjamin prestasi aplikasi yang optimum dan keselamatan maksimum anda. Jika atas sebab tertentu anda berhasrat untuk menyahaktifkan perkhidmatan, anda akan diberi amaran mengenai risiko yang boleh berlaku dengan serta-merta dengan tanda ***Amaran*** merah dan maklumat bahawa anda tidak dilindungi sepenuhnya pada masa ini. ***Sila ingat bahawa anda seharusnya mengaktifkan perkhidmatan semula secepat mungkin!***

Tetapan – Klik butang untuk dihalakan semula ke antara muka tetapan lanjutan. Dengan tepat lagi, dialog berkenaan dibuka dan anda akan dapat mengkonfigurasi perkhidmatan yang dipilih, cth. LinkScanner Surf-Shield atau Online Shield. Dalam antara muka tetapan lanjutan, anda boleh menyunting semua konfigurasi bagi setiap perkhidmatan keselamatan dalam **AVG Internet Security 2013** tetapi sebarang konfigurasi boleh disyorkan kepada pengguna berpengalaman sahaja!

Statistik – Klik butang untuk dihalakan semula ke halaman khusus pada tapak web AVG (http://www.avg.com/). Pada halaman ini, anda boleh menemui gambaran keseluruhan statistik terperinci bagi semua aktiviti **AVG Internet Security 2013** yang dilakukan pada komputer anda dalam tempoh masa tertentu dan secara keseluruhan.

Butiran – Klik butang dan penerangan ringkas perkhidmatan yang diserlahkan muncul di bahagian bawah dialog.

– Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke antara muka pengguna utama dengan gambaran keseluruhan komponen.

6.3. Identiti

Komponen ***Identity protection*** menjalankan perkhidmatan ***Identity Shield*** yang sentiasa melindungi aset digital anda daripada ancaman baharu dan tidak diketahui di Internet:

- ***Identity Protection*** adalah perkhidmatan anti-malware yang melindungi anda daripada semua jenis malware (*spyware, bot, kecurian identiti, ...*) menggunakan teknologi kelakuan dan memberikan perlindungan hari sifar untuk virus baharu. Identity Protection memberi tumpuan kepada menghalang pencuri identiti daripada mencuri kata laluan, butiran akaun bank, nombor kad kredit anda dan barangan digital peribadi yang lain yang bernilai daripada semua jenis perisian berniat jahat *(malware)* yang mensasarkan 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 secara 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 yang tersembunyi)* proses dan lebih daripada 285 corak kelakuan berbeza dan boleh menentukan jika sesuatu yang 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 daftaran, pembukaan port dll)*. Anda tidak perlu memulakan imbasan untuk dilindungi. Teknologi adalah sangat proaktif, jarang sekali memerlukan kemas kini dan

sentiasa melindungi.

Kawalan dialog

Di dalam dialog, anda boleh menemui kawalan berikut:

Didayakan / Dilumpuhkan – Butang tersebut boleh mengingatkan anda kepada lampu isyarat, dari segi penampilan dan kefungsian. Klik satu kali untuk bertukar antara dua posisi. Warna hijau bermaksud ***Didayakan***, yang bermakna perkhidmatan keselamatan Identity Protection diaktifkan dan berfungsi sepenuhnya. Warna merah mewakili status ***Dilumpuhkan*** , cth. perkhidmatan dinyahaktifkan. Jika anda tidak mempunyai sebarang sebab yang kukuh untuk menyahaktifkan perkhidmatan, kami amat mengesyorkan supaya anda mengekalkan tetapan lalai untuk semua konfigurasi keselamatan. Tetapan lalai menjamin prestasi aplikasi yang optimum dan keselamatan maksimum anda. Jika atas sebab tertentu anda berhasrat untuk menyahaktifkan perkhidmatan, anda akan diberi amaran mengenai risiko yang boleh berlaku dengan serta-merta dengan tanda ***Amaran*** merah dan maklumat bahawa anda tidak dilindungi sepenuhnya pada masa ini. ***Sila ingat bahawa anda seharusnya mengaktifkan perkhidmatan semula secepat mungkin!***

Tetapan – Klik butang untuk dihalakan semula ke antara muka tetapan lanjutan. Dengan tepat lagi, dialog berkenaan dibuka dan anda akan dapat mengkonfigurasi perkhidmatan yang dipilih, cth. Identity Protection. Dalam antara muka tetapan lanjutan, anda boleh menyunting semua konfigurasi bagi setiap perkhidmatan keselamatan dalam **AVG Internet Security 2013** tetapi sebarang konfigurasi boleh disyorkan kepada pengguna berpengalaman sahaja!

Butiran – Klik butang dan penerangan ringkas perkhidmatan yang diserlahkan muncul di bahagian bawah dialog.

– Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke antara muka pengguna utama dengan gambaran keseluruhan komponen.

Malangnya, dalam **AVG Internet Security 2013** perkhidmatan Identity Alert tidak disertakan. Jika anda ingin menggunakan perlindungan jenis ini, ikuti butang ***Naik taraf atau Aktifkan*** untuk dihalakan semula ke halaman web khusus di mana anda boleh membeli lesen Identity Alert.

Harap maklum bahawa walaupun dengan edisi AVG Premium Security, perkhidmatan Identity Alert pada masa ini hanya tersedia dalam rantau yang terpilih sahaja: AS, United Kingdom, Kanada dan Ireland.

6.4. E-mel

Komponen ***Perlindungan e-mel*** meliputi dua perkhidmatan keselamatan berikut: ***Pengimbas E-mel*** dan ***Anti-Spam***:

- ***Pengimbas E-mel***: Satu daripada sumber virus dan trojan yang paling biasa adalah melalui e-mel. Pemancingan data dan spam menjadikan e-mel sumber risiko yang lebih besar. Akaun e-mel percuma lebih berkemungkinan untuk menerima e-mel berniat jahat sedemikian *(kerana ia jarang menggunakan teknologi anti-spam)* dan pengguna rumah agak terlalu bergantung pada e-mel sedemikian. Pengguna rumah juga 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 anti-spam dsb, 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 itu juga boleh menapis keluar jenis lampiran e-mel tertentu dan menambah teks perakuan pada mesej bebas jangkitan. ***Pengimbas E-mel tidak dimaksudkan untuk platform pelayan!***

- ***Anti-Spam*** menyemak semua mesej e-mel masuk dan menandakan e-mel yang tidak dikehendaki sebagai spam *(Spam merujuk kepada e-mel yang tidak diminta, kebanyakannya pengiklanan produk atau perkhidmatan yang dihantar kepada bilangan alamat e-mel yang besar pada masa yang sama, mengisi peti mel penerima. Spam tidak merujuk kepada e-mel komersial sah yang mana telah mendapat kebenaran pengguna.)*. Anti-Spam boleh mengubah suai subjek e-mel *(yang telah dikenal pasti sebagai spam)* dengan menambah rentetan teks khas. Anda kemudiannya boleh menapis e-mel anda dalam klien e-mel anda dengan mudah. Komponen Anti-Spam menggunakan beberapa kaedah analisis untuk memproses setiap mesej e-mel, menawarkan perlindungan semaksimum mungkin daripada mesej e-mel yang tidak dikehendaki. Anti-Spam menggunakan pangkalan data yang dikemas kini dengan kerap untuk pengesanan spam. Adalah berkemungkinan untuk menggunakan pelayan RBL *(pangkalan data awam bagi alamat e-mel "penghantar spam yang diketahui")* dan untuk menambah alamat e-mel secara manual ke Senarai putih anda *(jangan sesekali tandakan sebagai spam)* dan Senarai hitam *(sentiasa tandakan sebagai spam)*.

Kawalan dialog

Untuk bertukar antara kedua-dua bahagian dialog, anda boleh mengklik di mana-mana dalam panel perkhidmatan yang berkenaan. Panel tersebut kemudiannya diserlahkan dengan warna biru cerah. Dalam kedua-dua bahagian dialog anda boleh menemui kawalan berikut. Kefungsiannya adalah serupa sama ada ia dimiliki oleh satu perkhidmatan keselamatan atau *(Pengimbas E-mel atau Anti-Spam)* yang lain:

Didayakan / Dilumpuhkan – Butang tersebut boleh mengingatkan anda kepada lampu isyarat, dari segi penampilan dan kefungsian. Klik satu kali untuk bertukar antara dua posisi. Warna hijau bermaksud ***Didayakan***, yang bermakna perkhidmatan keselamatan diaktifkan dan berfungsi sepenuhnya. Warna merah mewakili status ***Dilumpuhkan***, cth. perkhidmatan dinyahaktifkan. Jika anda tidak mempunyai sebarang sebab yang kukuh untuk menyahaktifkan perkhidmatan, kami amat mengesyorkan supaya anda mengekalkan tetapan lalai untuk semua konfigurasi keselamatan. Tetapan lalai menjamin prestasi aplikasi yang optimum dan keselamatan maksimum anda. Jika atas sebab tertentu anda berhasrat untuk menyahaktifkan perkhidmatan, anda akan diberi amaran mengenai risiko yang boleh berlaku dengan serta-merta dengan tanda ***Amaran*** merah dan maklumat bahawa anda tidak dilindungi sepenuhnya pada masa ini. ***Sila ingat bahawa anda seharusnya mengaktifkan perkhidmatan semula secepat mungkin!***

Dalam bahagian Pengimbas E-mel anda boleh melihat dua butang "lampu isyarat". Dengan cara ini anda boleh menentukan secara berasingan sama ada anda mahu Pengimbas E-mel menyemak mesej masuk, keluar atau kedua-duanya. Secara lalainya, pengimbasan dihidupkan untuk mesej masuk sementara dimatikan untuk mel keluar di mana risiko jangkitan adalah agak rendah.

Tetapan – Klik butang untuk dihalakan semula ke antara muka tetapan lanjutan. Dengan tepat lagi, dialog berkenaan dibuka dan anda akan dapat mengkonfigurasi perkhidmatan yang dipilih, cth. Pengimbas E-mel atau Anti-Spam. Dalam antara muka tetapan lanjutan, anda boleh menyunting semua konfigurasi bagi setiap perkhidmatan

keselamatan dalam **AVG Internet Security 2013** tetapi sebarang konfigurasi boleh disyorkan kepada pengguna berpengalaman sahaja!

Statistik – Klik butang untuk dihalakan semula ke halaman khusus pada tapak web AVG (http://www.avg.com/). Pada halaman ini, anda boleh menemui gambaran keseluruhan statistik terperinci bagi semua aktiviti **AVG Internet Security 2013** yang dilakukan pada komputer anda dalam tempoh masa tertentu dan secara keseluruhan.

Butiran – Klik butang dan penerangan ringkas perkhidmatan yang diserlahkan muncul di bahagian bawah dialog.

– Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke antara muka pengguna utama dengan gambaran keseluruhan komponen.

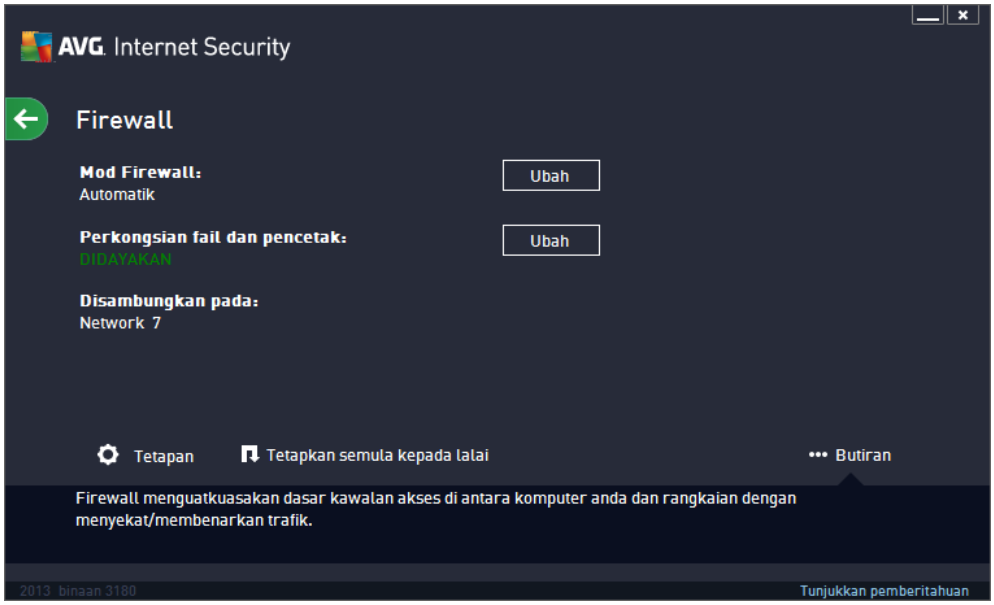
6.5. Firewall

Firewall adalah sistem yang menguatkuasakan dasar kawalan akses antara dua atau lebih rangkaian dengan menyekat/membenarkan trafik. 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 tersebut dan tidak membenarkan penceroboh mengakses komputer. Firewall dikonfigurasi untuk membenarkan atau menolak komunikasi dalaman/luaran *(kedua-dua cara, masuk dan keluar)* 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 pelayar lain akan disekat. melindungi maklumat peribadi anda yang boleh dikenal pasti daripada dihantar dari komputer anda tanpa kebenaran anda. Ia mengawal cara komputer anda bertukar data dengan komputer lain di Internet atau rangkaian setempat. Dalam organisasi, Firewall juga melindungi komputer individu daripada serangan yang dimulakan oleh pengguna dalaman pada komputer lain dalam rangkaian.

Dalam **AVG Internet Security 2013**, ***Firewall*** mengawal semua trafik 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 Internet/rangkaian setempat)* atau aplikasi yang mendekati komputer anda dari luar yang cuba menyambung ke PC anda. Untuk setiap aplikasi ini Firewall kemudiannya sama ada membenarkan atau melarang komunikasi pada port rangkaian. Secara lalainya, jika aplikasi tidak diketahui *(cth. tidak mempunyai peraturan Firewall yang ditakrifkan)*, Firewall akan bertanya anda jika anda mahu membenarkan atau menyekat percubaan komunikasi.

AVG Firewall bukan bertujuan untuk perlindungan platform pelayan!

Disyorkan: *Secara umumnya, adalah tidak disyorkan anda 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.*



Mod Firewall tersedia

Firewall membenarkan anda mentakrifkan peraturan keselamatan tertentu berdasarkan pada sama ada komputer anda terletak pada domain, komputer kendiri mahupun mungkin komputer bimbit. Setiap opsyen ini memerlukan perlindungan tahap berbeza dan setiap tahap dilindungi oleh mod masing-masing. Secara ringkasnya, mod Firewall adalah konfigurasi khusus komponen Firewall dan anda boleh menggunakan sejumlah konfigurasi yang dipratakrifkan.

- ***Automatik*** – Dalam mod ini, Firewall mengendalikan semua trafik rangkaian secara automatik. Anda tidak akan dijemput untuk membuat sebarang keputusan. Firewall akan membenarkan sambungan untuk setiap aplikasi yang diketahui dan pada masa yang sama, satu peraturan akan dicipta untuk aplikasi yang menentukan bahawa aplikasi tersebut sentiasa boleh menyambung pada masa akan datang. Untuk aplikasi lain, Firewall akan memutuskan sama ada sambungan tersebut harus dibenarkan atau disekat berdasarkan pada kelakuan aplikasi. Namun, dalam situasi sedemikian, peraturan tidak akan dicipta dan aplikasi akan disemak semula semasa ia cuba untuk menyambung. Mod automatik ini agak tidak mengganggu dan disyorkan untuk kebanyakan pengguna.

- ***Interaktif*** – mod ini berguna jika anda mahu mengawal sepenuhnya semua trafik rangkaian ke dan dari komputer anda. Firewall akan mengawasinya untuk anda dan memaklumkan kepada anda setiap percubaan untuk berkomunikasi atau memindahkan data, membolehkan anda membenarkan atau menyekat percubaan itu mengikut kemahuan anda. Disyorkan untuk pengguna lanjutan sahaja.

- ***Sekat akses ke Internet*** – Sambungan Internet disekat sepenuhnya, anda tidak boleh mengakses Internet dan tiada sesiapa pun dari luar boleh mengakses komputer anda. Untuk penggunaan khas dan masa yang singkat sahaja.

- ***Matikan perlindungan Firewall*** – melumpuhkan Firewall akan mendayakan semua trafik rangkaian ke dan dari komputer anda. Akibatnya, ini akan menjadikannya terdedah kepada serangan penggodam. Sila sentiasa pertimbangkan opsyen ini dengan berhati-hati.

Sila maklum bahawa terdapat mod automatik khusus yang juga tersedia dalam Firewall. Mod ini diaktifkan secara senyap jika sama ada komponen Komputer atau Identity protection dimatikan dan komputer anda dengan itu, lebih mudah terdedah. Dalam hal sedemikian, Firewall akan hanya membenarkan secara automatik aplikasi yang diketahui dan benar-benar selamat. Untuk hal lain, ia akan meminta keputusan anda. Ini akan menggantikan komponen perlindungan yang dinyahaktifkan dan untuk memastikan komputer anda selamat.

Kawalan dialog

Dialog ini memberikan gambaran keseluruhan maklumat asas mengenai status komponen Firewall:

- ***Mod Firewall*** – Memberikan maklumat mengenai mod Firewall yang dipilih buat masa ini. Gunakan butang ***Tukar*** yang terletak bersebelahan maklumat yang diberikan untuk bertukar kepada antara muka tetapan Firewall jika anda mahu menukar mod semasa kepada mod lain *(untuk penerangan dan cadangan mengenai penggunaan profil Firewall, sila lihat perenggan terdahulu)*.

- ***Perkongsian fail dan pencetak*** – Memaklumkan sama ada perkongsian fail dan pencetak *(dalam kedua-dua arah)* dibenarkan pada masa ini. Perkongsian fail dan pencetak sebenarnya bermaksud berkongsi sebarang fail atau folder yang anda tandakan sebagai "Dikongsi" dalam Windows, unit cakera biasa, pencetak, pengimbas dan semua peranti yang serupa. Perkongsian item sedemikian hanya wajar dalam rangkaian yang boleh dianggap selamat *(contohnya di rumah, di tempat kerja atau di sekolah)*. Namun, jika anda disambungkan ke rangkaian awam *(seperti Wi-Fi lapangan terbang atau kafe Internet)*, anda mungkin tidak mahu berkongsi apa-apa.

- ***Disambungkan ke*** – Memberikan maklumat mengenai nama rangkaian yang anda disambungkan buat masa ini. Dengan Window XP, nama rangkaian memberi respons kepada gelaran yang anda pilih untuk rangkaian tertentu semasa anda mula-mula disambungkan padanya. Dengan Windows Vista atau lebih tinggi, nama rangkaian diambil secara automatik daripada Network and Sharing Center.

Dialog ini mengandungi kawalan berikut:

Tukar - Butang tersebut membenarkan anda menukar status parameter yang berkenaan. Untuk butiran proses pertukaran, sila lihat penerangan parameter khusus dalam perenggan di atas.

Tetapan – Klik butang untuk dihalakan semula ke antara muka tetapan Firewall di mana anda boleh menyunting semua konfigurasi Firewall. Sebarang konfigurasi harus dilakukan oleh pengguna berpengalaman sahaja!

Tetapkan semula kepada lalai – Tekan butang ini untuk menulis ganti konfigurasi Firewall semasa dan untuk mengembalikan semula konfigurasi lalai berdasarkan kepada pengesanan automatik.

Butiran – Klik butang dan penerangan ringkas perkhidmatan yang diserlahkan muncul di bahagian bawah dialog.

– Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk

kembali ke antara muka pengguna utama dengan gambaran keseluruhan komponen.

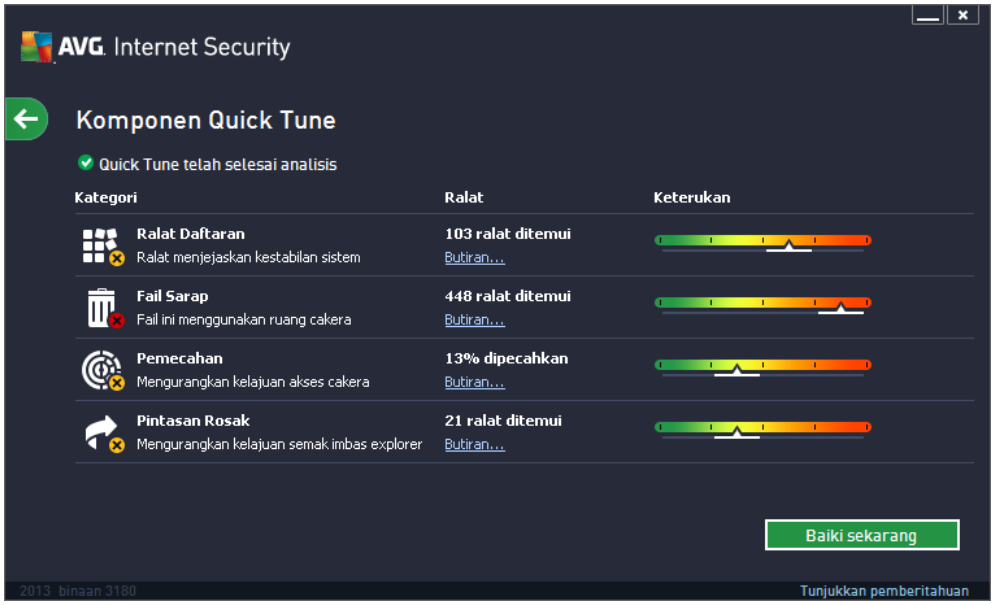
6.6. Quick Tune

Komponen ***Quick Tune*** ialah alat lanjutan untuk analisis sistem terperinci dan pembetulan mengenai bagaimana kelajuan dan prestasi keseluruhan komputer anda dapat dipertingkatkan:

Kategori berikut boleh dianalisis dan dibaiki: ralat daftaran, fail sarap, pemecahan dan pintasan rosak:

- ***Ralat Daftaran*** akan memberikan anda bilangan ralat dalam Daftaran Windows yang mungkin melambatkan komputer anda atau menyebabkan mesej ralat muncul.
- ***Fail Sarap*** akan memberikan anda bilangan fail yang menggunakan ruang cakera anda dan berkemungkinan besar boleh dihapuskan. Biasanya, ia adalah pelbagai jenis fail sementara dan fail dalam Tong Kitar Semula.
- ***Pemecahan*** akan mengira peratusan cakera keras anda yang dipecahkan, iaitu yang digunakan untuk tempoh yang lama oleh itu, kebanyakan fail kini berserak di seluruh bahagian yang berlainan pada cakera fizikal.
- ***Pintasan Rosak*** akan mencari 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:



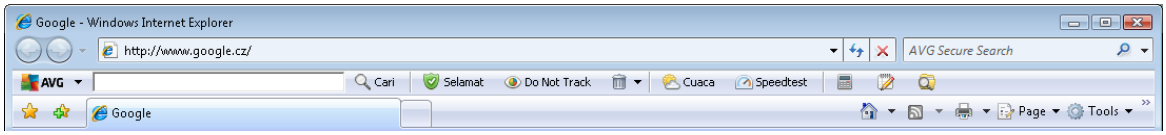
Gambaran keseluruhan keputusan memberikan bilangan masalah sistem yang dikesan (***Ralat***) yang dikelaskan mengikut kategori berkenaan yang telah diuji. Keputusan analisis juga akan dipaparkan secara grafik pada paksi dalam lajur ***Keterukan***.

Butang kawalan

- ***Analisis sekarang*** (*dipaparkan sebelum analisis bermula*) – tekan butang ini untuk melancarkan analisis segera komputer anda
- ***Baiki sekarang*** *(dipaparkan sebaik sahaja analisis selesai*) – tekan butang untuk membaiki semua ralat yang ditemui. Anda akan mendapat gambaran keseluruhan keputusan sebaik sahaja proses pembetulan selesai.
- ***Batal*** – tekan butang ini untuk hentikan menjalankan analisis, atau untuk kembali ke antara dialog utama AVG lalai (*gambaran keseluruhan komponen*) sebaik sahaja analisis selesai

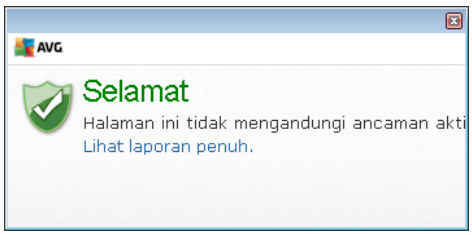
7. AVG Security Toolbar

AVG Security Toolbar ialah alat yang berfungsi bersama dengan perkhidmatan LinkScanner Surf-Shield dan mengawal keselamatan maksimum anda semasa menyemak imbas Internet. Dalam **AVG Internet Security 2013**, 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 pelayar lain yang disokong *(sekiranya anda menggunakan beberapa pelayar Internet alternatif, cth. Avant Browser, anda boleh mengalami kelakuan yang tidak dijangka).*



AVG Security Toolbar terdiri daripada yang berikut:

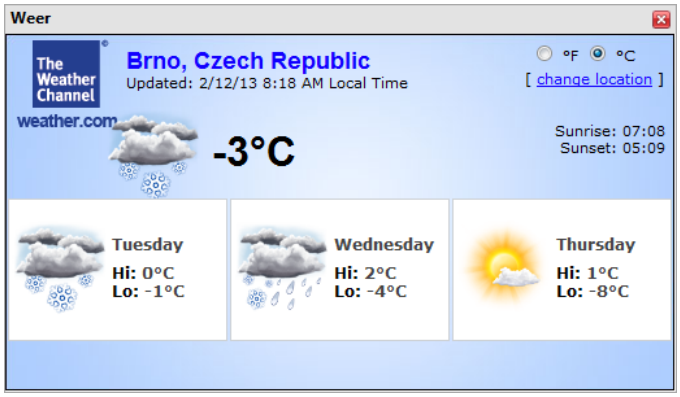
- ***Logo AVG*** dengan menu jatuh ke bawah:
    - ***Tahap Ancaman Semasa*** – membuka halaman web makmal virus dengan paparan grafik bagi tahap ancaman semasa pada web.
    - ***Makmal Ancaman AVG*** – membuka tapak web ***Makmal Ancaman AVG*** khusus *(di http://www.avgthreatlabs.com)* di mana anda boleh menemui maklumat tentang berbagai keselamatan tapak web dan tahap ancaman semasa dalam talian.
    - ***Bantuan Toolbar*** – membuka bantuan dalam talian yang meliputi semua kefungsian ***AVG Security Toolbar***.
    - ***Serahkan maklum balas Produk*** – membuka halaman web dengan borang yang anda boleh isikan dan memberitahu kami pendapat anda mengenai ***AVG Security Toolbar***.
    - ***Nyahpasang AVG Security Toolbar*** – membuka halaman web yang memberikan penerangan terperinci mengenai cara untuk menyahaktifkan ***AVG Security Toolbar*** dalam setiap pelayar web yang disokong.
    - ***Tentang...*** – membuka tetingkap baharu dengan maklumat mengenai versi ***AVG Security Toolbar*** yang dipasang buat masa ini.
- ***Medan carian*** – cari di Internet menggunakan ***AVG Security Toolbar*** untuk memastikan benar-benar selamat dan selesa 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)*.
- ***Keselamatan Tapak*** – butang ini membuka dialog baharu yang memberikan maklumat mengenai tahap ancaman semasa (*Selamat buat masa ini*) bagi halaman yang baru sahaja anda lawati. Gambaran ringkas ini boleh dikembangkan dan dipaparkan dengan butiran penuh semua aktiviti keselamatan yang berkaitan dengan halaman tersebut terus di dalam tetingkap pelayar (*Lihat laporan lengkap*):



- ***Do Not Track*** – perkhidmatan DNT membantu anda mengenal pasti tapak web yang mengumpulkan data mengenai aktiviti dalam talian anda dan memberikan anda pilihan untuk membenarkannya atau tidak membenarkannya. Butiran >>

- ***Hapuskan*** – butang 'tong sampah' memberikan menu gulung bawah di mana anda boleh memilih sama ada anda mahu hapuskan maklumat mengenai penyemakan lalu, muat turun, borang dalam talian anda atau hapuskan semua sejarah carian anda sekali gus.

- ***Cuaca*** – butang ini membuka dialog baharu yang memberikan maklumat mengenai cuaca semasa di lokasi anda dan ramalan cuaca untuk dua hari akan datang. Maklumat ini 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***.

- ***Ujian kelajuan*** – Butang ini menghalakan anda semula ke aplikasi dalam talian yang boleh membantu anda mengesahkan kualiti sambungan internet anda *(ping)* dan kelajuan muat turun serta muat naik anda.

- Butang pintasan untuk akses pantas kepada aplikasi ini: ***Kalkulator***, ***Pad Nota***, ***Windows Explorer***.

8. AVG Do Not Track

AVG Do Not Track membantu anda mengenal pasti laman web yang mengumpulkan data mengenai aktiviti dalam talian anda. ***AVG Do Not Track*** yang merupakan sebahagian daripada AVG Security Toolbar menunjukkan tapak web atau pengiklan yang mengumpul 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, kefungsian ***AVG Do Not Track*** disokong dalam penyemak imbas Mozilla Firefox, Chrome dan Internet Explorer.

8.1. 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. Dalam hal sedemikian, ikon ***AVG Do Not Track*** yang terdapat pada AVG Security Toolbar menukar penampilannya, nombor kecil kelihatan pada ikon yang memberikan maklumat mengenai beberapa perkhidmatan pengumpulan data yang dikesan:

Klik ikon untuk melihat dialog berikut:

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

- ***Web Analytics*** *(dibenarkan secara lalai):* Perkhidmatan yang digunakan untuk memperbaik 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.

- ***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.

- ***Social Buttons*** *(dibenarkan secara lalai):* Elemen yang direka bentuk untuk memperbaik 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.

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.*

Kawalan dialog

- ***Apakah penjejakan?*** – Klik pautan ini di bahagian atas dialog untuk dihalakan semula ke laman web yang dikhususkan untuk memberi penerangan terperinci terhadap prinsip penjejakan dan huraian jenis penjejakan tertentu.

- ***Sekat Semua*** – Klik butang yang terdapat di bahagian bawah dialog bagi menyatakan bahawa anda tidak mahu sebarang aktiviti pengumpulan data sama sekali *(untuk butiran lihat bab Menyekat proses penjejakan).*

- ***Tetapan Do Not Track*** – Klik butang ini di bahagian bawah dialog untuk dihalakan semula ke laman 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)*

8.2. 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.

8.3. 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 kefungsian 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 memperbaik 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.

8.4. Tetapan AVG Do Not Track

Dialog ***Opsyen Do Not Track*** menawarkan opsyen konfigurasi berikut:

- ***Do Not Track didayakan*** – Secara lalainya, perkhidmatan DNT adalah aktif *(HIDUP)*. Untuk melumpuhkan perkhidmatan ini, gerakkan suis kepada kedudukan MATI.

- Dalam bahagian tengah dialog anda boleh melihat kotak dengan senarai perkhidmatan pengumpulan data yang diketahui yang boleh dikelaskan sebagai Ad Networks. Secara lalainya, ***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. Atau, anda boleh menggunakan butang ***Lalai*** untuk membatalkan semua perubahan tetapan yang telah dilakukan dan untuk kembali kepada konfigurasi asal.

- ***Maklumkan tapak web...*** – Dalam bahagian ini anda boleh menghidupkan/mematikan opsyen ***Maklumkan tapak web bahawa saya tidak mahu dijejak*** *(dihidupkan secara lalai).* Biarkan opsyen ini ditandakan untuk mengesahkan bahawa anda mahu ***Do Not Track*** memaklumkan pembekal perkhidmatan pengumpulan data yang dikesan bahawa anda tidak mahu dijejak.

9. Tetapan Lanjutan AVG

Dialog konfigurasi lanjutan **AVG Internet Security 2013** terbuka dalam tetingkap baharu 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 mana konfigurasinya ingin anda tukar (*atau bahagian tertentunya*) untuk membuka dialog penyuntingan dalam bahagian kanan tetingkap.

9.1. Penampilan

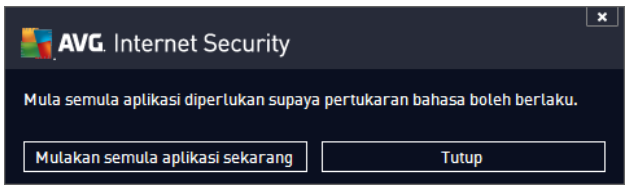
Item pertama pepohon navigasi, ***Penampilan***, merujuk kepada tetapan umum antara muka pengguna AVG Internet Security 2013 dan memberikan beberapa opsyen asas bagi kelakukan aplikasi:

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 2013**. Menu jatuh bawah hanya menawarkan bahasa yang anda pilih sebelum ini untuk dipasang semasa proses pemasangan serta bahasa Inggeris (*secara lalainya, bahasa Inggeris sentiasa dipasang secara automatik*). Untuk selesai menukar **AVG Internet Security 2013** 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 2013**
- Tekan butang ***Mula semula aplikasi sekarang*** untuk bersetuju dengan mula semula atur cara, dan tunggu beberapa saat untuk pertukaran bahasa dilakukan:

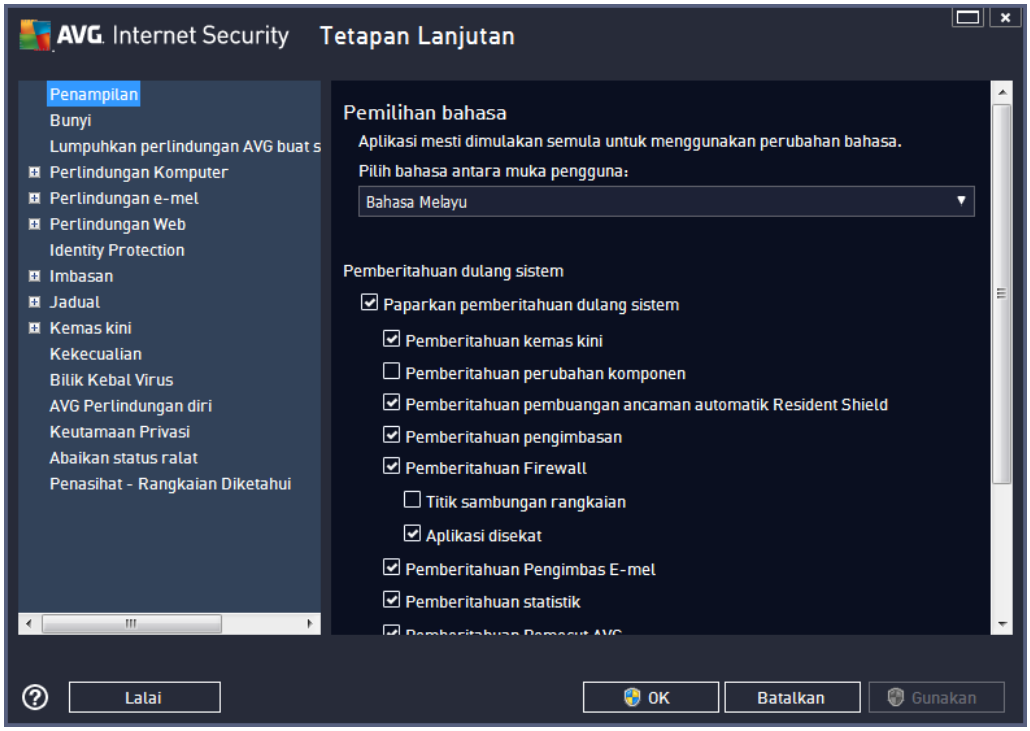


Pemberitahuan dulang sistem

Dalam bahagian ini, anda boleh menyekat daripada memaparkan pemberitahuan dulang sistem pada status aplikasi **AVG Internet Security 2013**. Secara lalai, pemberitahuan sistem dibenarkan untuk dipaparkan. Adalah amat disyorkan supaya anda mengekalkan konfigurasi ini! Pemberitahuan sistem memberikan maklumat, contohnya tentang melancarkan pengimbasan atau proses kemas kini atau tentang perubahan status komponen **AVG Internet Security 2013**. Anda seharusnya memberi perhatian kepada pemberitahuan ini!

Walau bagaimanapun, jika atas sebab tertentu anda memutuskan bahawa anda tidak mahu diberitahu dengan cara ini atau anda hanya inginkan pemberitahuan tertentu sahaja *(berkaitan dengan komponen AVG Internet Security 2013 khusus)* dipaparkan, anda boleh mentakrifkan dan menentukan keutamaan anda dengan menanda/tidak menanda opsyen berikut:

- ***Paparkan pemberitahuan dulang sistem*** *(dihidupkan secara lalai)* – secara lalainya, 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:



- ***Pemberitahuan** kemas kini (dihidupkan secara lalai)* - tentukan sama ada maklumat mengenai **AVG Internet Security 2013** pelancaran, kemajuan dan pemuktamadan proses kemas kini harus dipaparkan.

- ***Pemberitahuan perubahan keadaan komponen** (dimatikan secara lalai)* - tentukan sama ada maklumat berkenaan keaktifan/ketidakaktifan komponen atau kemungkinan masalahnya harus dipaparkan. Apabila melaporkan status kerosakan komponen, opsyen ini adalah bersamaan dengan fungsi bermaklumat ikon dulang sistem yang melaporkan masalah dalam sebarang **AVG Internet Security 2013** komponen.

- ***Pemberitahuan pembuangan ancaman automatik Resident Shield** (dihidupkan secara lalai)* - tentukan sama ada maklumat berkenaan proses penyimpanan, penyalinan dan pembukaan harus dipaparkan atau disekat (*konfigurasi ini hanya kelihatan jika opsyen auto pulih Resident Shield dihidupkan*).

- ***Pemberitahuan** imbasan (dihidupkan secara lalai)* - tentukan sama ada maklumat selepas pelancaran automatik bagi imbasan yang dijadualkan, kemajuannya dan hasilnya harus dipaparkan.

- ***Pemberitahuan Firewall** (dihidupkan secara lalai)* - tentukan sama ada maklumat berkenaan status dan proses Firewall, cth. amaran pengaktifan/penyahaktifan komponen, sekatan trafik yang mungkin berlaku dsb. harus dipaparkan. Item ini memberikan dua lagi opsyen pilihan khusus *(untuk penerangan terperinci bagi setiap satunya, sila rujuk bab Firewall dokumen ini)*:

  - ***Titik sambungan rangkaian**(dimatikan secara lalai)*- semasa bersambung kepada rangkaian, Firewall memaklumkan sama ada ia mengenali rangkaian tersebut dan bagaimana perkongsian fail dan pencetak akan ditetapkan.

- ***Aplikasi disekat*** *(dihidupkan secara lalai)* - semasa aplikasi yang tidak diketahui atau mencurigakan mencuba untuk bersambung ke rangkaian, Firewall menyekat percubaan itu dan memaparkan pemberitahuan. Ini adalah berguna supaya anda sentiasa dimaklumkan, oleh kerana itu kami mengesyorkan supaya ciri ini sentiasa menghidupkan.

- ***Pemberitahuan*** *Pengimbas E-mel* *(dihidupkan secara lalai)* - tentukan sama ada maklumat mengenai pengimbasan semua mesej e-mel masuk dan keluar harus dipaparkan.

- ***Pemberitahuan statistik*** *(dihidupkan secara lalai)* - biarkan opsyen sentiasa ditandakan untuk membenarkan pemberitahuan semakan statistik tetap dipaparkan dalam dulang sistem.

- ***Pemberitahuan Pemecut AVG*** *(dihidupkan secara lalai)* - tentukan sama ada maklumat mengenai aktiviti ***Pemecut AVG*** harus dipaparkan. Perkhidmatan ***Pemecut AVG*** membenarkan main balik video dalam talian yang lebih lancar dan membuatkan muat turun tambahan lebih mudah.

- ***Pemberitahuan peningkatan masa but*** *(dimatikan secara lalai)* - tentukan sama ada anda ingin dimaklumkan mengenai pemecutan masa but komputer anda.

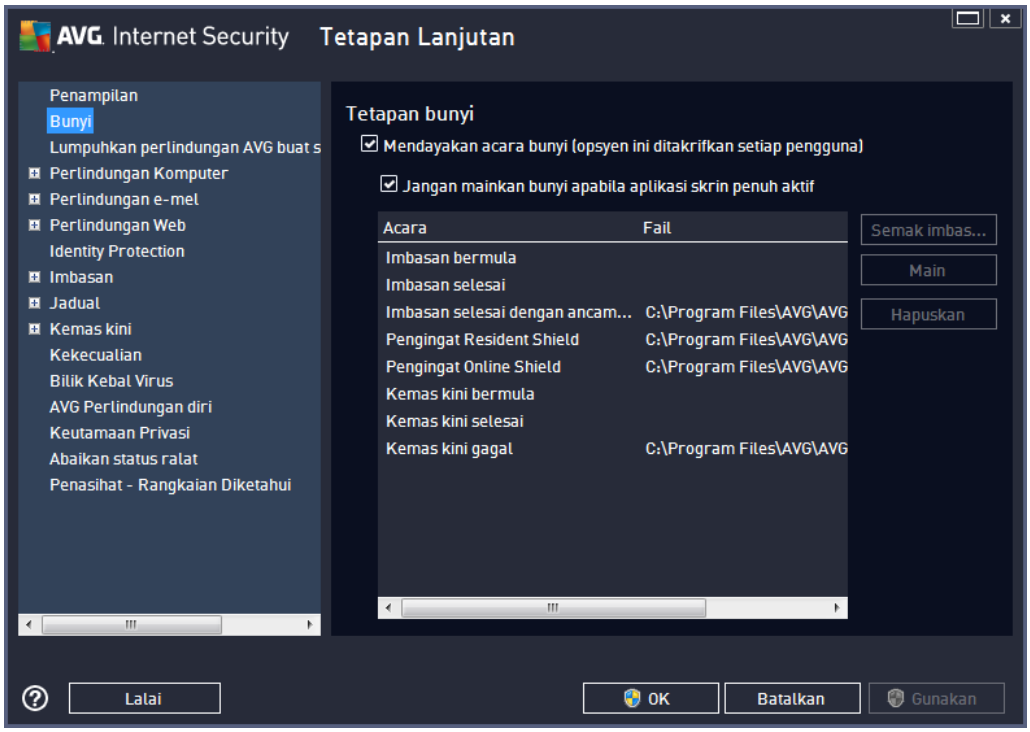
- ***Pemberitahuan Penasihat AVG*** *(dihidupkan secara lalai)* - tentukan sama ada maklumat selepas aktiviti Penasihat AVG harus dipaparkan dalam panel gelangsar pada dulang sistem.

Mod permainan

Fungsi AVG ini direka bentuk untuk aplikasi skrin penuh di mana sebarang belon maklumat AVG (*dipaparkan cth. apabila imbasan berjadual dimulakan*) akan mengganggu (*ia boleh meminimumkan aplikasi atau merosakkan grafiknya*). Untuk mengelakkan situasi ini, biarkan kotak semak untuk opsyen ***Dayakan mod permainan semasa aplikasi skrin penuh dilakukan*** ditandakan (*tetapan lalai*).

9.2. Bunyi

Dalam dialog ***Bunyi*** anda boleh menentukan sama ada anda ingin dimaklumkan mengenai tindakan **AVG Internet Security 2013** 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 opsyen ***Dayakan peristiwa bunyi*** ditanda (*opsyen dihidupkan, secara lalai*) untuk mengaktifkan senarai bagi semua tindakan yang berkaitan. Anda juga mungkin ingin menandakan opsyen ***Jangan mainkan bunyi semasa aplikasi skrin penuh sedang aktif*** untuk menyekat pemberitahuan bunyi dalam situasi di mana ia mungkin mengganggu *(lihat juga bahagian mod Permainan bab Tetapan lanjutan/Penampilan dalam dokumen ini)*.

Butang kawalan

- ***Semak imbas*** – Dengan memilih acara masing-masing daripada senarai, gunakan butang ***Semak imbas*** untuk mencari fail bunyi yang diingini pada cakera anda yang ingin anda peruntukkan. *(Sila maklum bahawa hanya bunyi *.wav disokong pada masa ini!)*

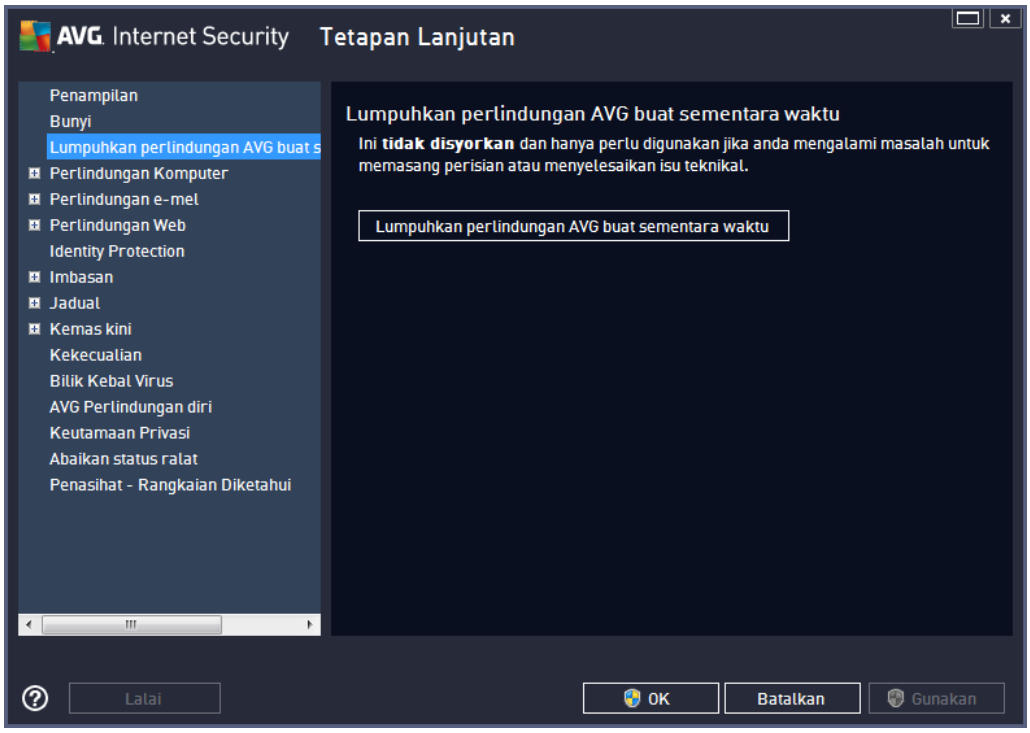
- ***Main*** – untuk mendengar bunyi yang dipilih, serlahkan acara dalam senarai dan tekan butang ***Main***.

- ***Hapuskan*** – gunakan butang ***Hapuskan*** untuk mengalih keluar bunyi yang diperuntukkan kepada acara tertentu.

9.3. Menyahdayakan perlindungan AVG buat sementara waktu

Dalam dialog ***Menyahdaya perlindungan AVG buat sementara waktu*** anda mempunyai pilihan untuk mematikan keseluruhan perlindungan yang dikawal oleh **AVG Internet Security 2013** anda sekali gus.

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

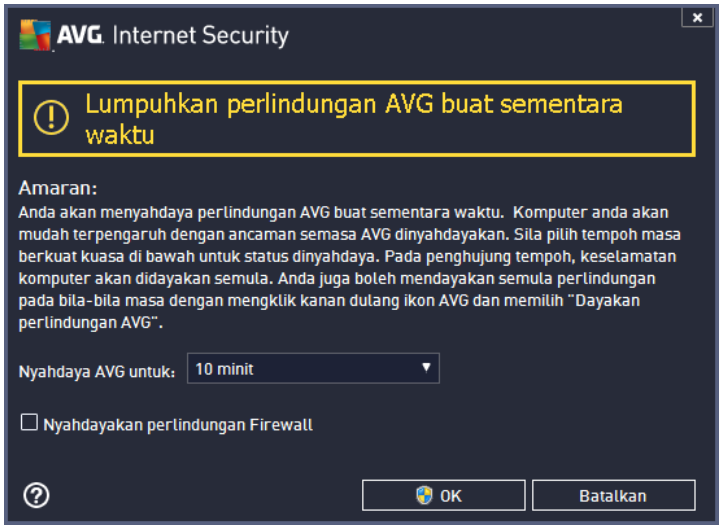


Dalam kebanyakan kes, adalah ***tidak perlu*** menyahdayakan **AVG Internet Security 2013** sebelum memasang perisian atau pemacu baharu, walaupun jika pemasang atau wizard perisian mencadangkan bahawa atur cara dan aplikasi yang dijalankan dimatikan dahulu untuk memastikan tiada gangguan yang tidak dikehendaki sewaktu proses pemasangan. Sekiranya anda benar-benar mengalami masalah semasa pemasangan, cuba menyahaktifkan perlindungan residen terlebih dahulu (*Dayakan Resident Shield*). Jika anda perlu menyahdayakan **AVG Internet Security 2013** buat sementara waktu, anda hendaklah mendayakannya semula sebaik sahaja anda selesai. Jika anda disambungkan ke Internet atau rangkaian semasa perisian antivirus anda dilumpuhkan, komputer anda terdedah kepada serangan.

Bagaimana hendak menyahdayakan perlindungan AVG

Tandakan kotak semak ***Lumpuhkan perlindungan AVG buat sementara waktu*** dan sahkan pilihan anda dengan menekan butang ***Guna***. Dalam dialog ***Lumpuhkan perlindungan AVG buat sementara waktu*** yang baru dibuka, tentukan berapa lama anda ingin melumpuhkan **AVG Internet Security 2013** anda. Secara lalai, perlindungan akan dimatikan selama 10 minit yang seharusnya mencukupi untuk sebarang tugasan biasa seperti memasang perisian baharu dll. Anda boleh

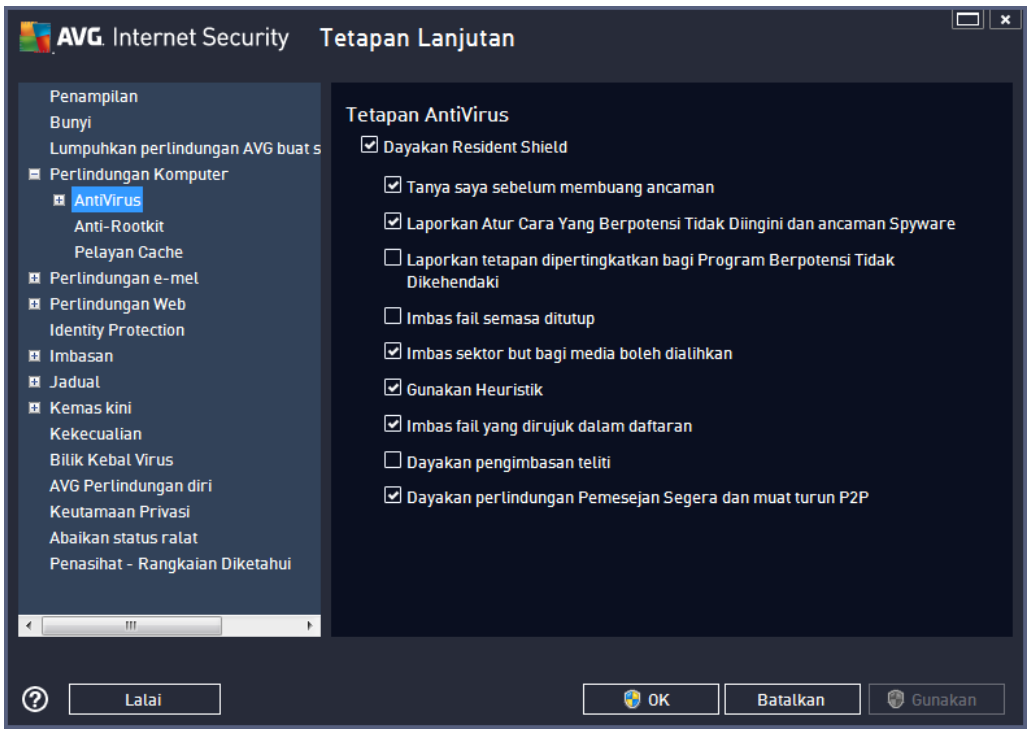
menentukan tempoh masa yang lebih lama, namun opsyen ini tidak disyorkan jika tidak benar-benar diperlukan. Selepas itu, semua komponen yang dinyahaktifkan akan diaktifkan semula secara automatik. Paling lama, anda boleh melumpuhkan perlindungan AVG hingga komputer dimulakan semula seterusnya. Opsyen berbeza untuk mematikan komponen ***Firewall*** terdapat dalam dialog ***Lumpuhkan perlindungan AVG buat sementara waktu***. Tandakan ***Lumpuhkan perlindungan Firewall*** untuk melakukannya.



9.4. Perlindungan Komputer

9.4.1. AntiVirus

AntiVirus bersama dengan ***Resident Shield*** melindungi komputer anda secara berterusan dari semua jenis virus, spyware dan malware yang diketahui secara umumnya *(termasuk yang dipanggil malware tidur dan tidak aktif, iaitu malware yang telah dimuat turun tetapi belum diaktifkan)*.



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

- ***Tanya saya sebelum membuang 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 2013** akan memulihkan jangkitan secara automatik dan jika tidak dapat dipulihkan, objek itu akan dialihkan ke dalam Bilik Kebal Virus.

- ***Laporkan Atur Cara Yang Berpotensi Tidak Diingini dan ancaman Spyware*** (*dihidupkan secara lalai*) – tandakan untuk mengaktifkan imbasan Spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- ***Laporkan tetapan dipertingkatkan bagi Atur Cara Yang Berpotensi Tidak Diingini*** (*dimatikan secara lalai*) – tandakan untuk mengesan pakej spyware lanjutan: atur cara yang sangat baik 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 fail semasa ditutup*** (*dimatikan secara lalai*) – pengimbasan se masa ditutup memastikan AVG mengimbas objek aktif (cth. aplikasi, dokumen ...) semasa ia dibuka dan

juga semasa ia ditutup; ciri ini membantu melindungi komputer anda daripada beberapa jenis virus canggih.

- ***Imbas sektor but bagi media boleh ditanggalkan*** (*dihidupkan secara lalai*)

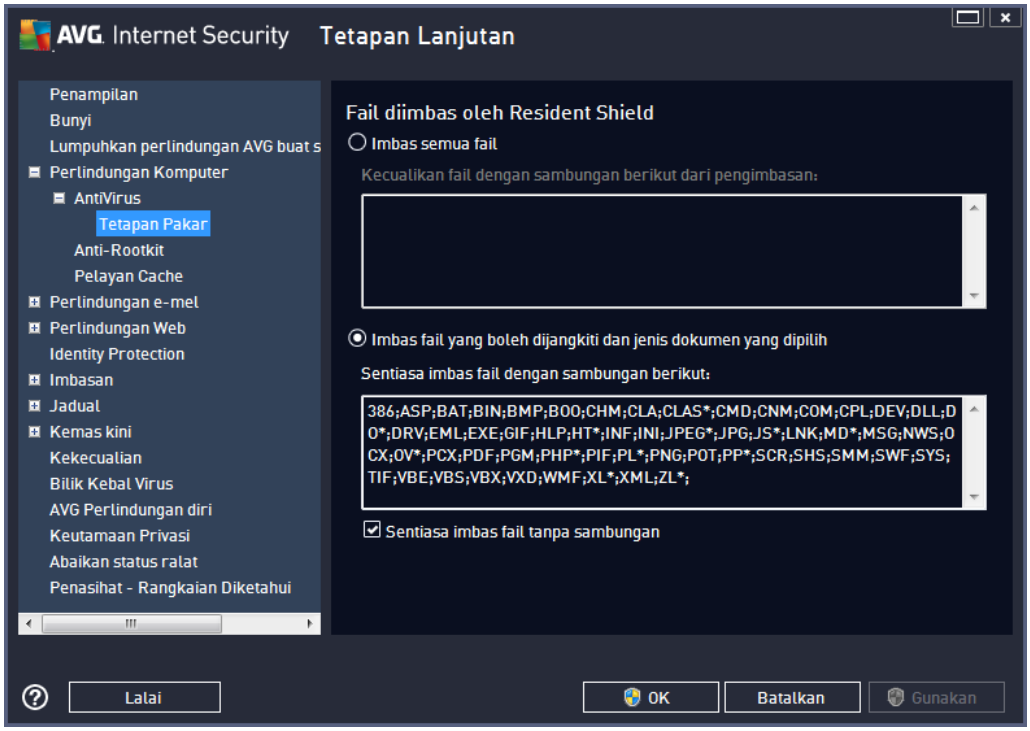
- ***Gunakan Heuristik*** – (*dihidupkan secara lalai*) – analisis heuristik akan digunakan untuk pengesanan (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*).

- ***Imbas fail yang dirujuk dalam pendaftar*** (*dihidupkan secara lalai*) – parameter ini mentakrifkan bahawa AVG akan mengimbas semua fail boleh laku yang ditambah pada pendaftar permulaan untuk mengelakkan jangkitan yang diketahui berlaku semasa permulaan komputer yang seterusnya.

- ***Dayakan pengimbasan teliti*** (*dimatikan secara lalai*) – dalam situasi khusus (*dalam keadaan kecemasan melampau*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma yang paling teliti yang akan menyemak semua objek yang berkemungkinan memberi ancaman secara mendalam. 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. AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...*) dan data yang dimuat turun dalam rangkaian Rakan kepada Rakan *(rangkaian yang membenarkan sambungan terus antara klien, tanpa pelayan, yang berpotensi berbahaya; lazimnya digunakan untuk berkongsi fail muzik)* adalah bebas virus.

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

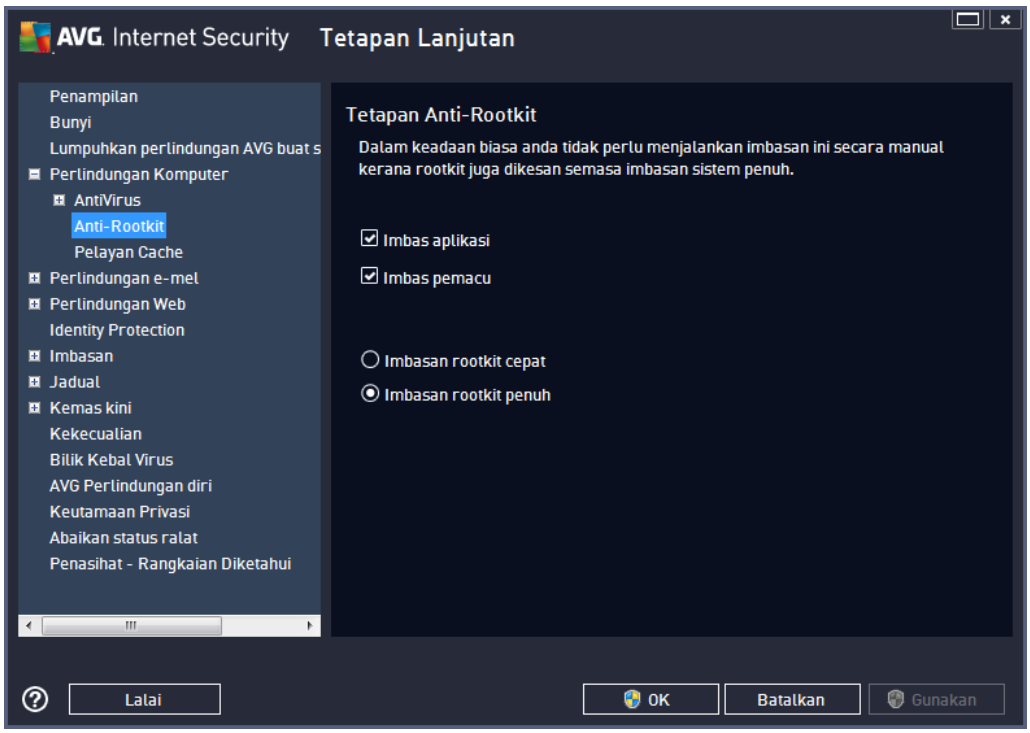


Tandakan kotak semak masing-masing untuk memutuskan sama ada anda hendak ***Imbas semua fail*** atau ***Imbas fail yang boleh dijangkiti dan jenis dokumen yang dipilih*** sahaja. Untuk mempercepatkan pengimbasan dan memberikan tahap perlindungan maksimum pada masa yang sama, kami mengesyorkan supaya anda mengekalkan tetapan lalai. Dengan cara ini, hanya fail yang boleh dijangkiti sahaja akan diimbas. Dalam bahagian dialog yang berkenaan, anda juga boleh menemui senarai sambungan boleh disunting yang mentakrifkan fail yang disertakan dalam pengimbasan.

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

9.4.2. Anti-Rootkit

Dalam dialog ***Tetapan Anti-Rootkit*** anda boleh menyunting konfigurasi perkhidmatan ***Anti-Rootkit*** dan parameter khusus pengimbasan anti-rootkit. Pengimbasan anti-rootkit adalah proses lalai yang disertakan dalam Imbas Seluruh Komputer:

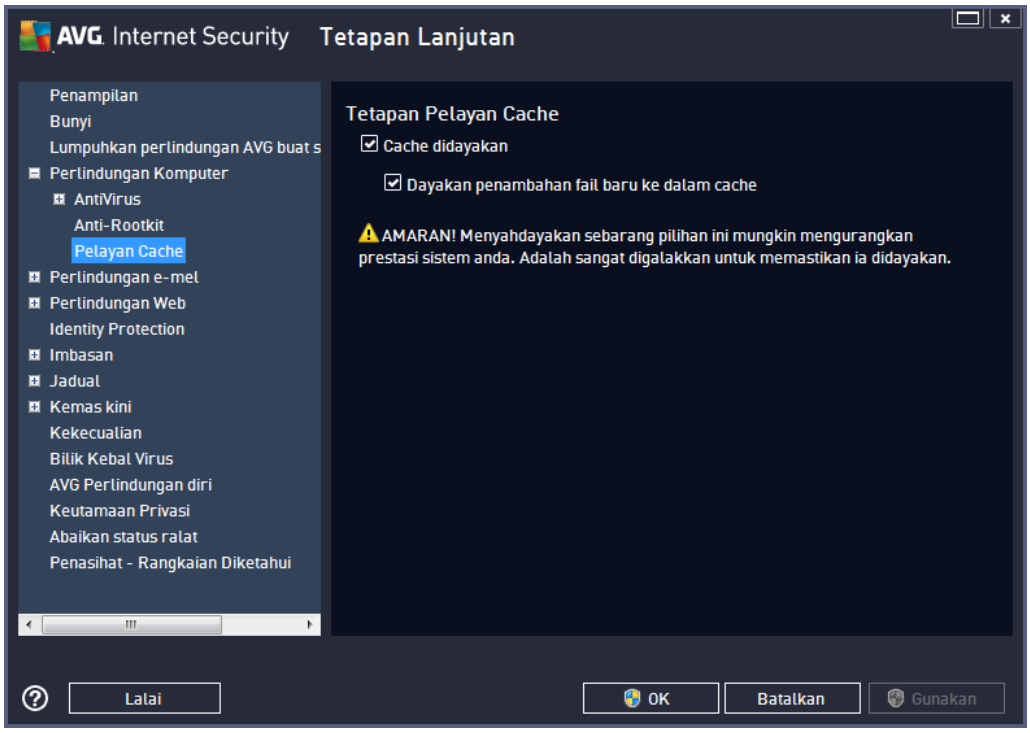


Imbas aplikasi dan ***Imbas pemacu*** membolehkan anda menentukan secara terperinci apa yang harus dimasukkan dalam imbasan antirootkit. Tetapan ini adalah untuk pengguna lanjutan; kami mengesyorkan supaya anda membiarkan semua opsyen dihidupkan. Anda juga boleh memilih mod pengimbasan rootkit:

- ***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*)

9.4.3. Pelayan Cache

Dialog ***Tetapan Pelayan Cache*** merujuk kepada proses pelayan cache yang direka bentuk untuk mempercepatkan semua jenis imbasan **AVG Internet Security 2013**:



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

Dialog ***Tetapan Pelayan Cache*** menawarkan opsyen berikut untuk konfigurasi:

- ***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 spyware dahulu.

- ***Dayakan penambahan fail baharu ke dalam cache*** (*dihidupkan secara lalai*) – jangan tanda kotak untuk hentikan 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.

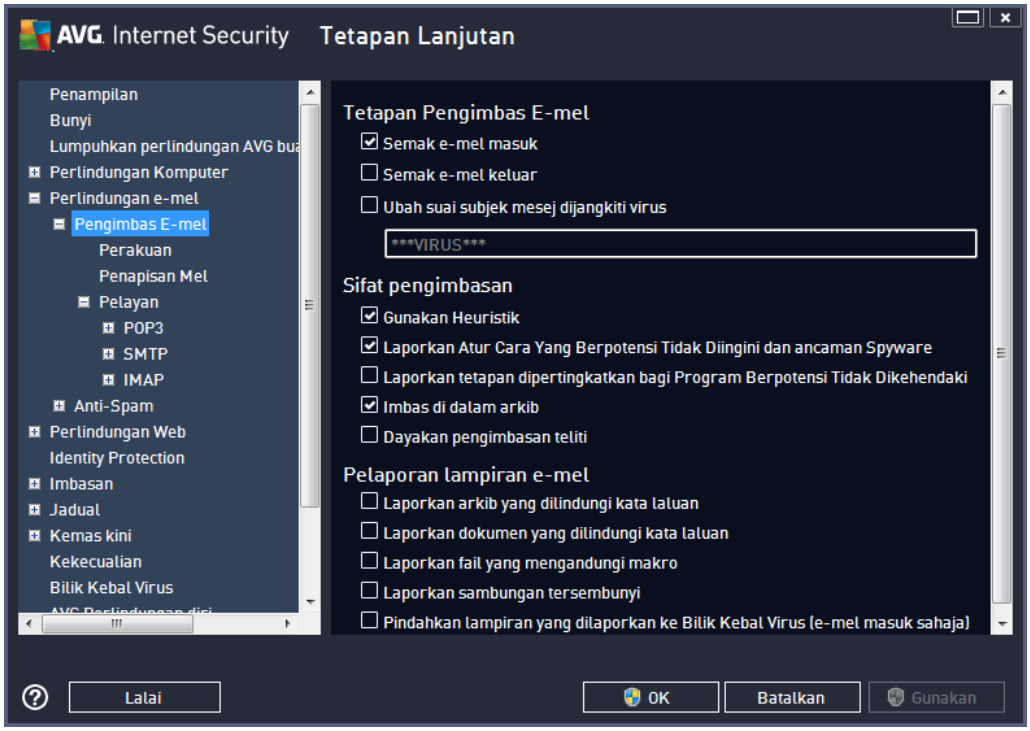
Melainkan anda mempunyai alasan yang kukuh untuk mematikan pelayan cache, kami amat mengesyorkan supaya anda mengekalkan tetapan lalai dan membiarkan kedua-dua opsyen dihidupkan! Jika tidak, anda mungkin mengalami penurunan yang ketara dalam kelajuan dan prestasi sistem anda.

9.5. Pengimbas E-mel

Dalam bahagian ini anda boleh menyunting konfigurasi terperinci Pengimbas E-mel dan Anti-Spam:

9.5.1. 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*** (*dihidupkan secara lalai*) – tandakan untuk menghidupkan/ mematikan opsyen bagi mengimbas semua mesej e-mel yang dihantar ke klien e-mel anda
- ***Semak e-mel keluar*** (*dimatikan secara lalai*) – tandakan untuk menghidupkan/mematikan opsyen bagi mengimbas semua e-mel yang dihantar dari akaun anda
- ***Ubah suai subjek mesej yang dijangkiti virus*** (*dimatikan secara lalai*) – jika anda ingin diberi amaran bahawa mesej e-mel yang diimbas dikesan sebagai dijangkiti, tandakan item ini dan isikan teks yang diinginkan ke dalam medan teks. Teks ini kemudiannya akan ditambahkan ke medan "Subjek" untuk setiap mesej e-mel yang dikesan untuk pengenalan dan penapisan yang lebih mudah. Nilai lalai ialah ***VIRUS*** yang kami syorkan supaya anda kekalkan.

Sifat pengimbasan

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

- ***Gunakan Heuristik*** (*dihidupkan secara lalai*) – tandakan untuk menggunakan kaedah pengesanan heuristik semasa mengimbas mesej e-mel. Apabila opsyen ini dihidupkan, anda boleh menapis lampiran e-mel bukan sahaja melalui sambungan tetapi kandungan sebenar lampiran juga akan dipertimbangkan. Penapisan boleh ditetapkan dalam dialog Penapisan Mel.

- ***Laporkan Atur Cara Yang Berpotensi Tidak Diingini dan ancaman Spyware*** (*dihidupkan secara lalai*) – tandakan untuk mengaktifkan imbasan spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- ***Laporkan tetapan dipertingkatkan bagi Atur Cara Yang Berpotensi Tidak Diingini*** (*dimatikan secara lalai*) – tandakan untuk mengesan pakej spyware lanjutan: 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 di dalam arkib*** (*dihidupkan secara lalai*) – tandakan untuk mengimbas kandungan arkib yang dilampirkan pada mesej e-mel.

- ***Dayakan pengimbasan teliti*** (*dimatikan secara lalai*) – dalam situasi khusus (*cth. kecurigaan komputer anda telah dijangkiti oleh virus atau serangan*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan paling teliti 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; teks perakuan hanya akan ditambah pada penghujung mesej e-mel dan semua laporan seumpamanya akan disenaraikan dalam dialog pengesanan Perlindungan E-mel:

- ***Laporkan arkib yang dilindungi kata laluan*** – arkib (*ZIP, RAR dll.*) yang dilindungi oleh kata laluan tidak boleh diimbas untuk mengesan virus; tandakan kotak untuk melaporkannya sebagai berpotensi berbahaya.

- ***Laporkan dokumen yang dilindungi kata laluan*** – dokumen yang dilindungi kata laluan tidak boleh diimbas untuk mengesan virus; tandakan kotak untuk melaporkannya sebagai berpotensi berbahaya.

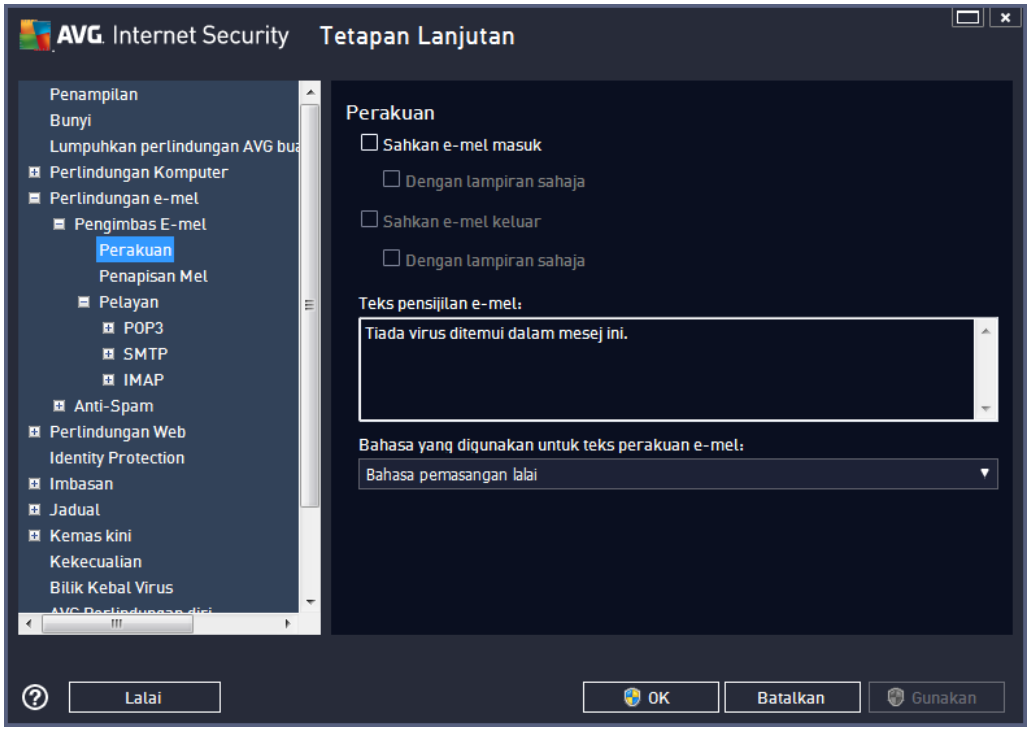
- ***Laporkan fail mengandungi makro*** – makro adalah urutan langkah yang dipratakrifkan untuk menjadikan tugasan tertentu lebih mudah untuk pengguna (*makro MS Word dikenali ramai*). Dengan itu, makro boleh mengandungi arahan berpotensi berbahaya dan anda mungkin ingin menandakan kotak untuk memastikan 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 "sesuatu. txt" yang tidak berbahaya; tandakan kotak untuk melaporkannya sebagai berpotensi berbahaya.

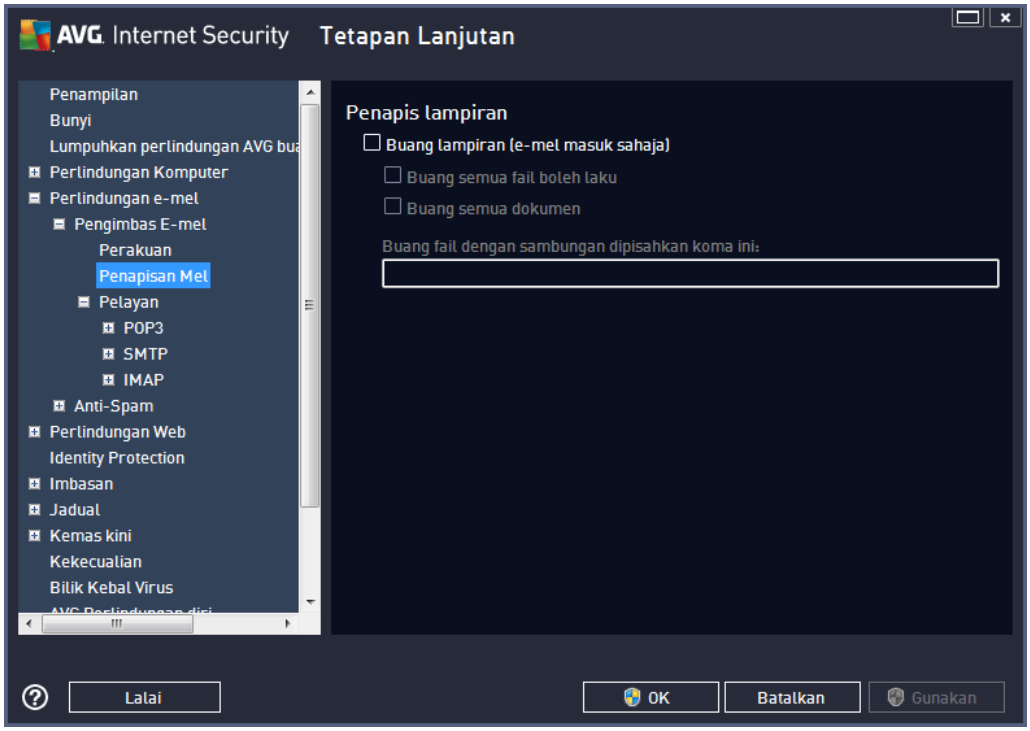
- ***Alihkan lampiran yang dilaporkan ke Bilik Kebal Virus*** – tentukan sama ada anda hendak diberitahu melalui e-mel mengenai arkib yang dilindungi kata laluan, dokumen yang dilindungi kata laluan, fail yang mengandungi makro dan/atau fail dengan sambungan tersembunyi dikesan sebagai lampiran pada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

Dalam dialog ***Perakuan*** yang boleh menandakan kotak semak khusus untuk memutuskan sama ada anda mahu memperakui mel masuk (***Perakui e-mel masuk***) dan/atau mel keluar anda (***Perakui e-mel keluar***). Untuk setiap opsyen ini, anda boleh seterusnya, menentukan parameter ***Dengan lampiran sahaja*** supaya perakuan hanya ditambah pada mesej e-mel dengan lampiran:



Secara lalai, teks perakuan mengandungi 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 bahagian ***Bahasa yang digunakan untuk teks perakuan e-mel*** , anda boleh seterusnya mentakrifkan dalam bahasa apa bahagian perakuan yang dijana secara automatik (*Tiada virus yang ditemui dalam mesej ini*) harus dipaparkan.

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



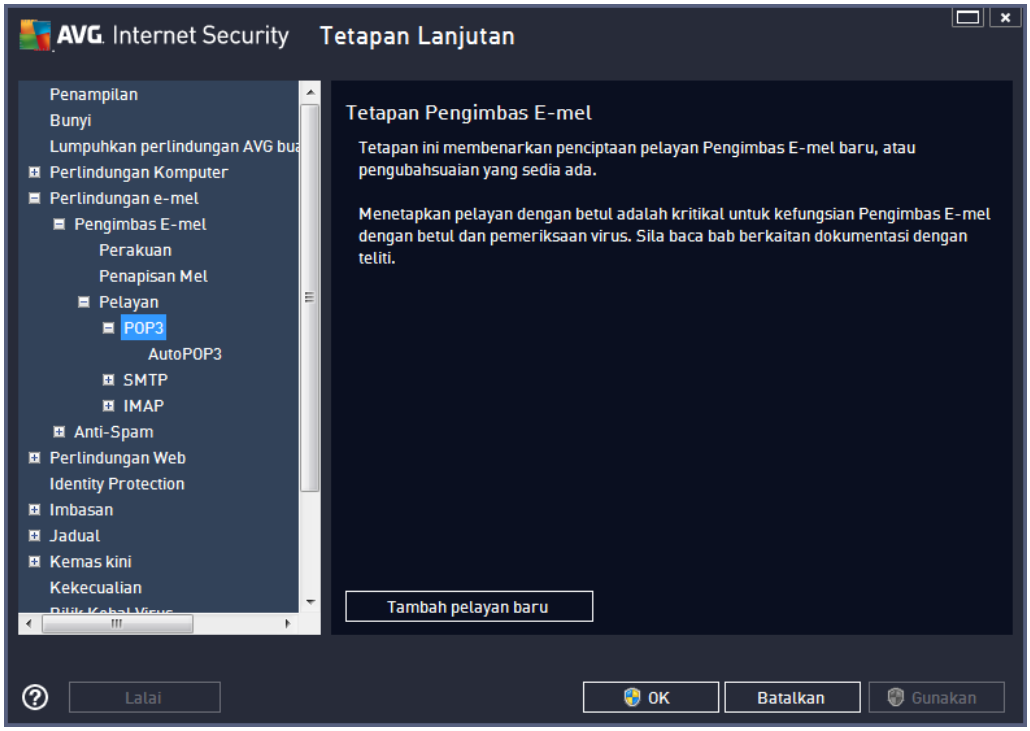
Dialog ***Penapis lampiran*** membenarkan anda menyediakan parameter untuk pengimbasan lampiran mesej e-mel. Secara lalainya, opsyen ***Alih keluar lampiran*** dimatikan. Jika anda memutuskan untuk mengaktifkannya, semua lampiran mesej e-mel yang dikesan sebagai dijangkiti atau berpotensi berbahaya akan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

- ***Buang semua fail boleh laku*** – semua fail *.exe akan dihapuskan
- ***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

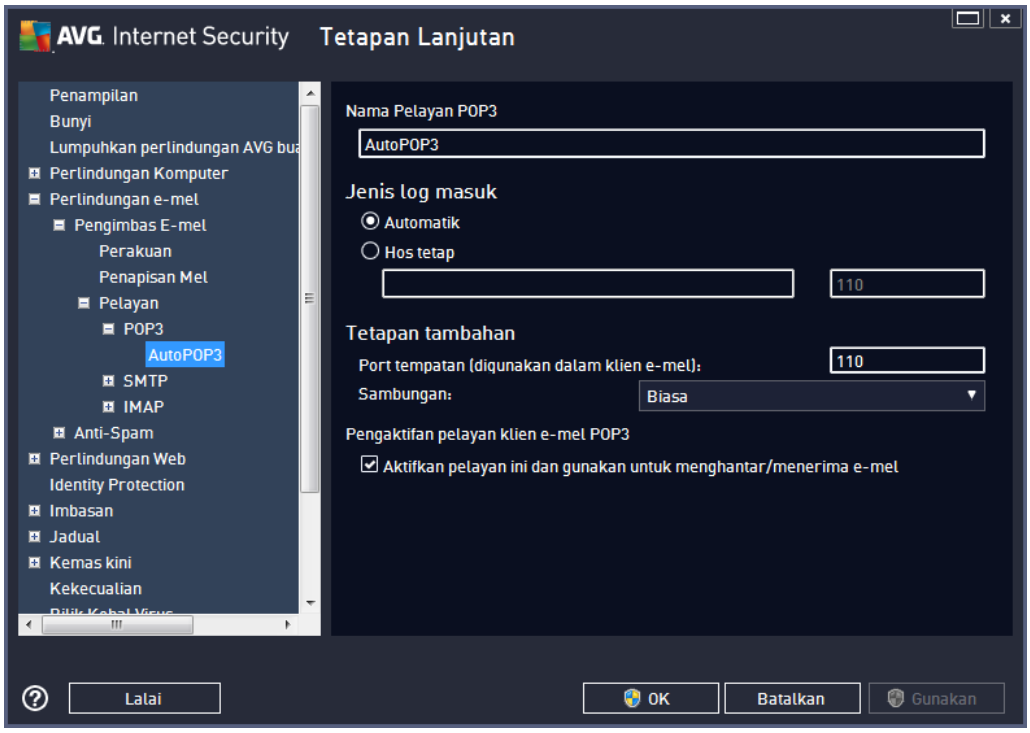
Dalam bahagian ***Pelayan*** anda boleh menyunting parameter untuk pelayan Pengimbas E-mel:

- Pelayan POP3
- Pelayan SMTP
- Pelayan IMAP

Anda juga boleh mentakrifkan pelayan baharu untuk mel masuk atau keluar menggunakan butang ***Tambah pelayan baharu***.



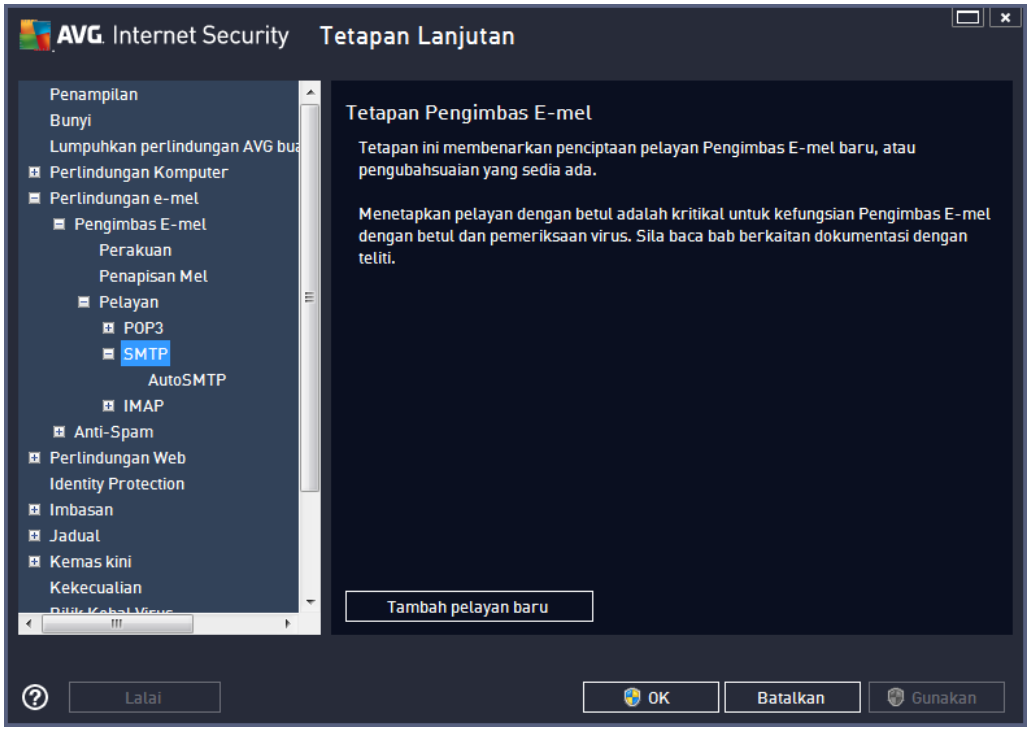
Dalam dialog ini anda boleh menetapkan pelayan Pengimbas E-mel baharu menggunakan protokol POP3 untuk mel masuk:



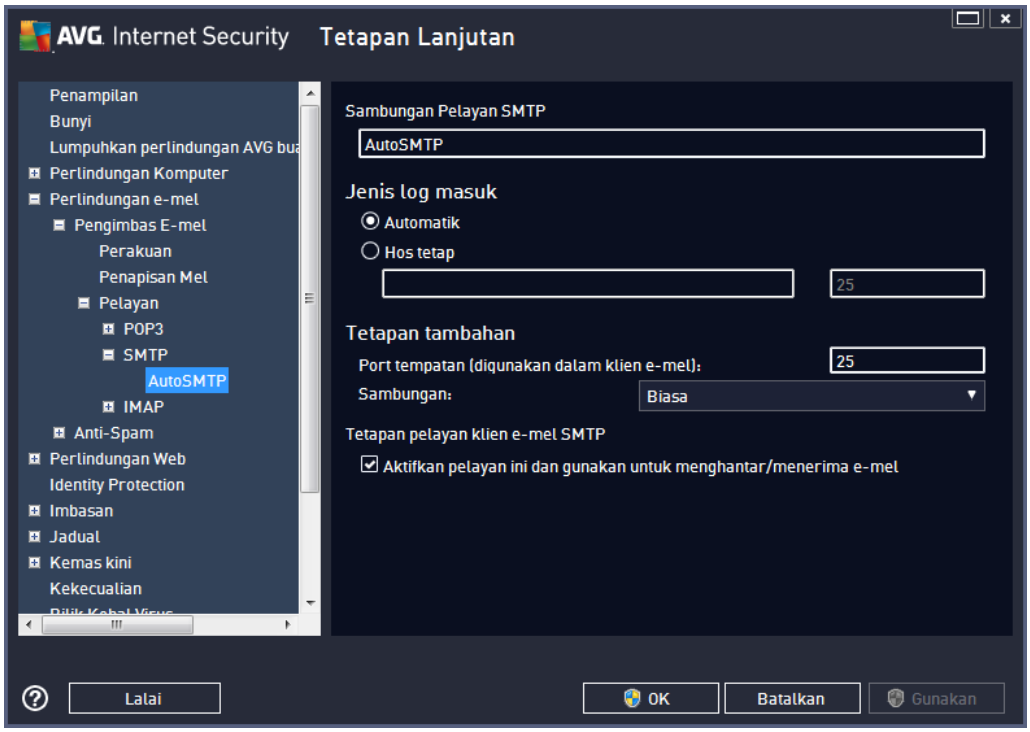
- ***Nama Pelayan POP3*** – dalam medan ini anda boleh menentukan nama pelayan yang baru

ditambah (*untuk menambah pelayan POP3, klik butang tetikus kanan di atas item POP3 di sebelah kiri menu navigasi*). Bagi pelayan "AutoPOP3" yang dicipta 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 hal ini, atur cara akan sentiasa menggunakan pelayan yang ditentukan 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 menyatakan 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



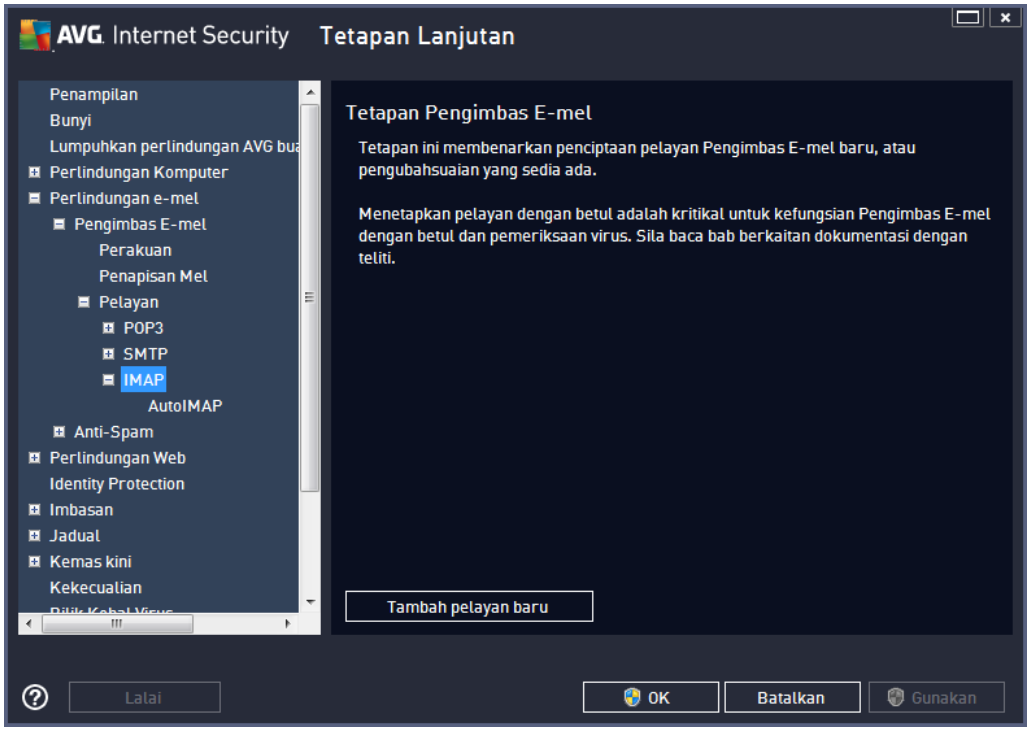
Dalam dialog ini anda boleh menetapkan pelayan Pengimbas E-mel baharu menggunakan protokol SMTP untuk mel keluar:



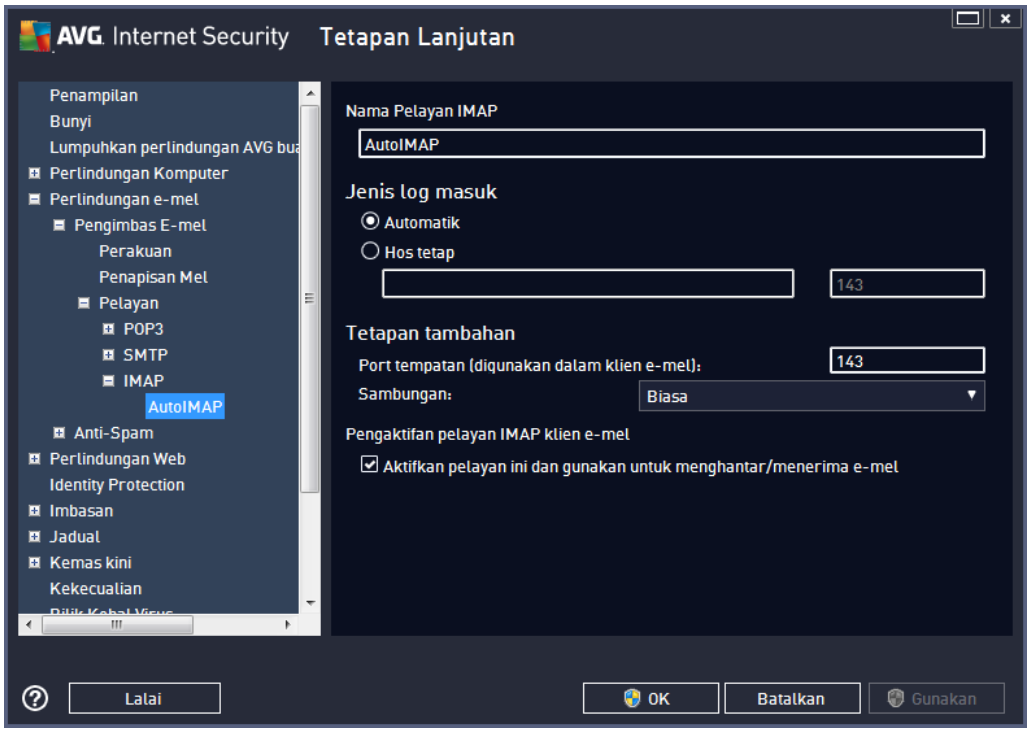
- ***Nama Pelayan SMTP*** – dalam medan ini anda boleh menentukan nama pelayan yang baru

ditambah (*untuk menambah pelayan SMTP, klik butang tetikus kanan di atas item SMTP di sebelah kiri menu navigasi*). Untuk pelayan "AutoSMTP" yang dicipta 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 disokong oleh pelayan mel destinasi.
- ***Pengaktifan pelayan SMTP klien e-mel*** – tandakan/nyahtandakan kotak ini untuk mengaktifkan/menyahaktifkan pelayan SMTP yang dinyatakan di atas



Dalam dialog ini anda boleh menetapkan pelayan Pengimbas E-mel baharu menggunakan protokol IMAP untuk mel keluar:

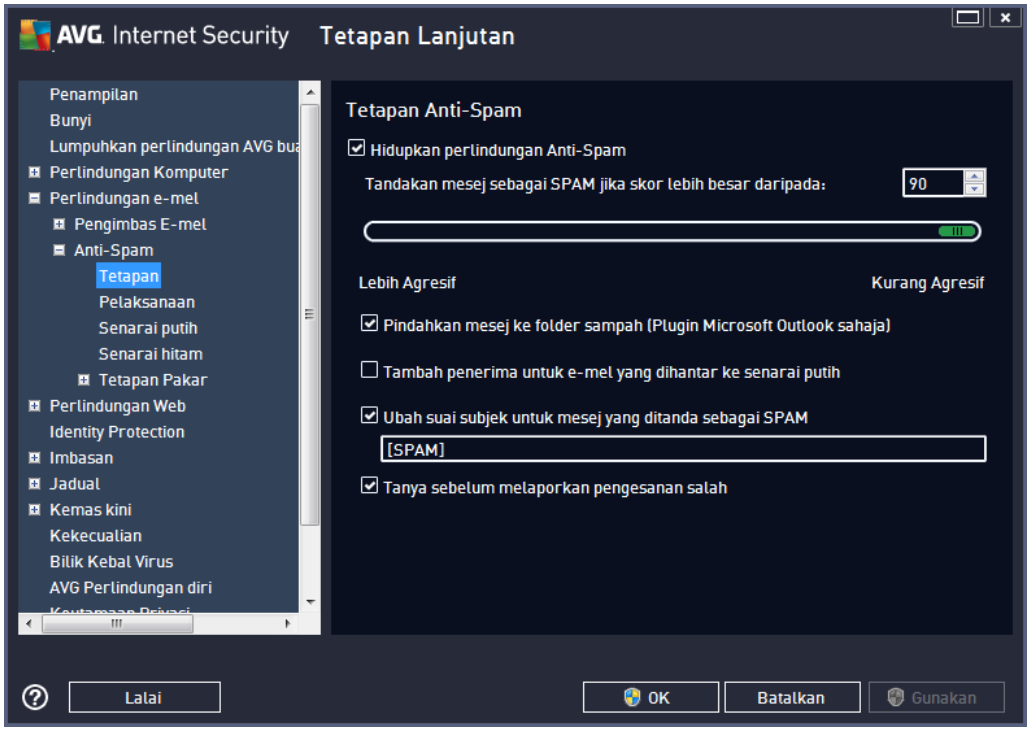


- ***Nama Pelayan IMAP*** – dalam medan ini anda boleh menentukan nama pelayan yang baru

ditambah (*untuk menambah pelayan IMAP, klik butang tetikus kanan di atas item IMAP bagi menu navigasi kiri*). Bagi pelayan "AutoIMAP" yang dicipta secara automatik, medan ini dinyahakifkan.

- ***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 diawasi oleh pihak ketiga. Ciri ini tersedia hanya apabila pelayan mel destinasi menyokongnya.
- ***Pengaktifan pelayan IMAP klien e-mel*** – tandakan/nyahtandakan kotak ini untuk mengaktifkan/menyahaktifkan pelayan IMAP yang dinyatakan di atas

9.5.2. AntiSpam



Dalam dialog ***tetapan Anti-Spam*** anda boleh menanda/tidak menanda kotak semak ***Hidupkan perlindungan Anti-Spam*** untuk membenarkan/melarang pengimbasan anti-spam bagi komunikasi e-mel. Opsyen ini dihidupkan secara lalai dan seperti biasa, adalah disyorkan supaya anda mengekalkan konfigurasi ini melainkan anda mempunyai sebab sebenar untuk menukarnya.

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 yang berkemungkinan adalah spam akan ditapis keluar. Sesetengah mesej bukan spam juga mungkin ditapis secara tidak betul.
- ***Nilai 60-79*** – dianggap 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 Anti-Spam*** anda boleh seterusnya mentakrifkan cara mesej e-mel spam yang dikesan akan diperlakukan:

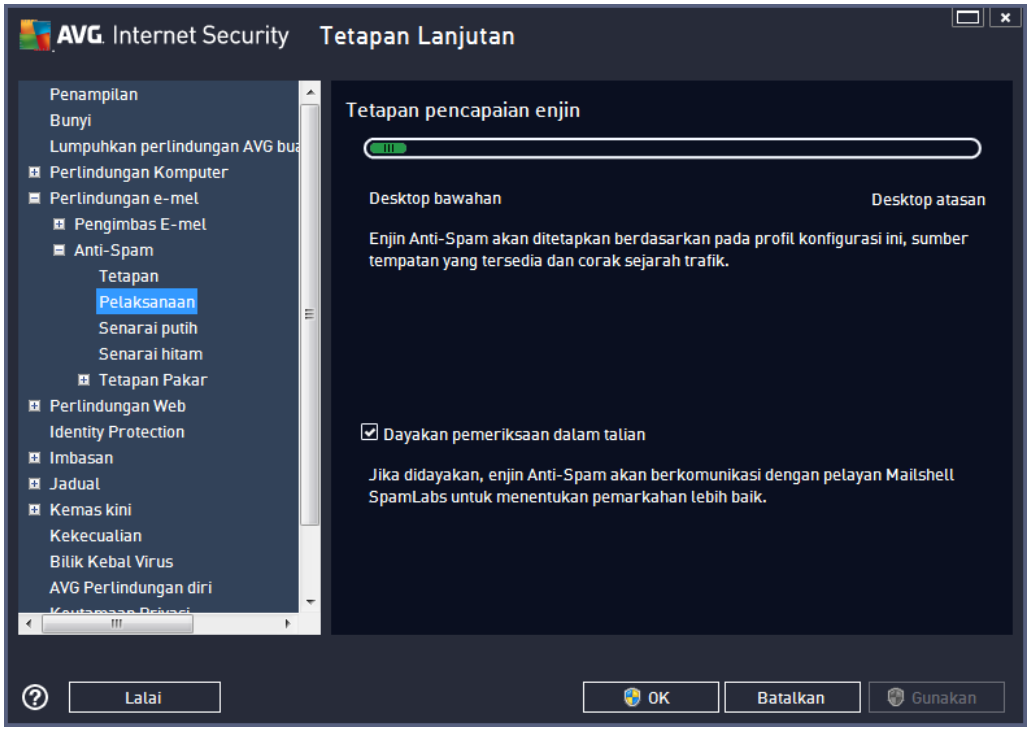
- ***Alihkan mesej ke folder sampah*** *(plugin Microsoft Outlook sahaja)* – tandakan kotak semak ini untuk menentukan bahawa setiap mesej spam yang dikesan harus dialihkan secara automatik ke folder sampah khusus dalam klien e-mel MS Outlook anda. Pada masa ini, ciri ini tidak disokong dalam klien mel lain.

- ***Tambah penerima bagi e-mel yang dihantar ke senarai putih*** – tandakan kotak semak 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 semak 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 projek Keutamaan Privasi. Jika benar, anda membenarkan pelaporan ancaman yang dikesan kepada AVG. Laporan ini dibuat 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.

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



Gerakkan gelangsar ke kiri atau kanan untuk menukar tahap prestasi pengimbasan antara ***Desktop bawahan*** / ***Desktop atasan***.

- ***Desktop bawahan*** – semasa proses pengimbasan untuk mengenal pasti spam, tiada

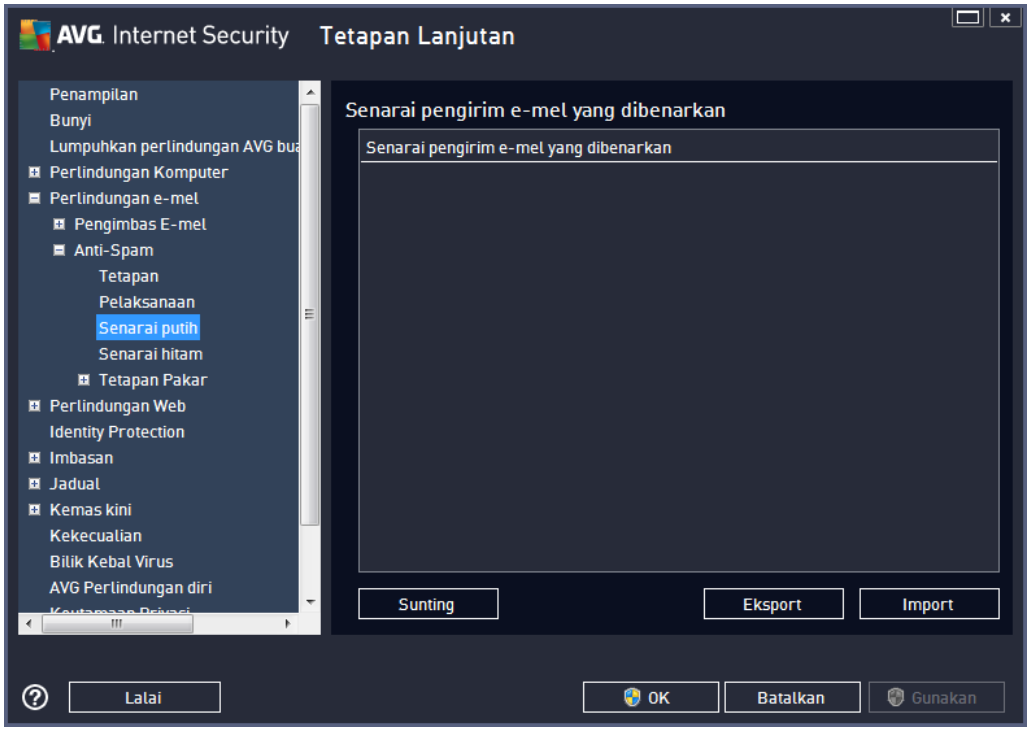
peraturan yang akan digunakan. Hanya data latihan akan digunakan untuk pengenalpastian. Mod ini tidak disyorkan untuk penggunaan biasa, melainkan perkakas komputer adalah sangat lemah.

- ***Desktop atasan*** – mod ini akan menggunakan jumlah memori yang besar. Semasa proses pengimbasan untuk mengenal pasti spam, ciri berikut akan digunakan: cache pangkalan data peraturan dan spam, peraturan asas dan lanjutan, alamat IP penghantar spam dan pangkalan data penghantar 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 umumnya, adalah disyorkan supaya anda mengekalkan tetapan lalai dan hanya menukarnya jika anda mempunyai sebab yang kukuh untuk melakukannya. Sebarang perubahan kepada konfigurasi ini harus dibuat oleh pengguna yang pakar sahaja!

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.



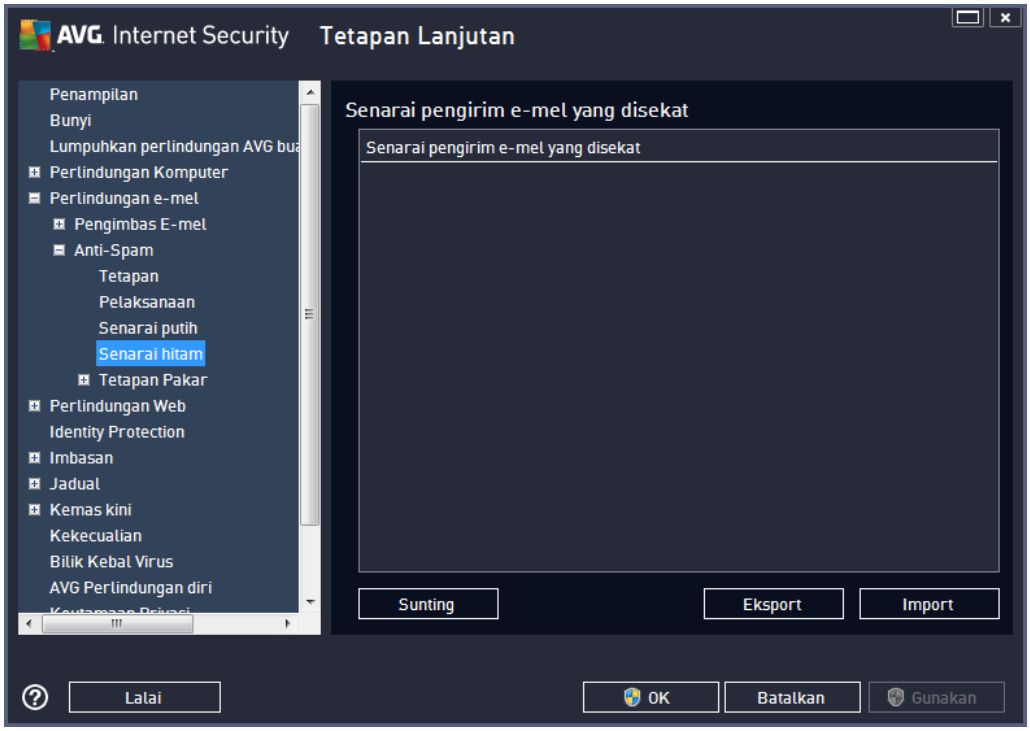
Dalam antara muka pengeditan, anda boleh mengumpulkan senarai penghantar yang anda pasti tidak akan menghantarkan anda mesej yang tidak diingini (spam). Anda juga boleh mengumpulkan senarai nama domain penuh (*cth. avg.com*), yang anda ketahui tidak menjana mesej spam. Selepas anda menyediakan senarai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

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 diingini kepada anda *(spam)*. Anda juga boleh mengumpulkan senarai nama domain penuh (*cth. spammingcompany.com*), yang anda jangkakan atau dari mana anda terima mesej. Semua e-mel daripada alamat/domain yang disenaraikan akan dikenal pasti sebagai spam. Selepas anda menyediakan senarai penghantar dan/atau domain, anda boleh memasukkannya dengan satu daripada kaedah berikut: dengan memasukkan terus setiap alamat e-mel atau dengan mengimport keseluruhan senarai alamat sekali gus.

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.

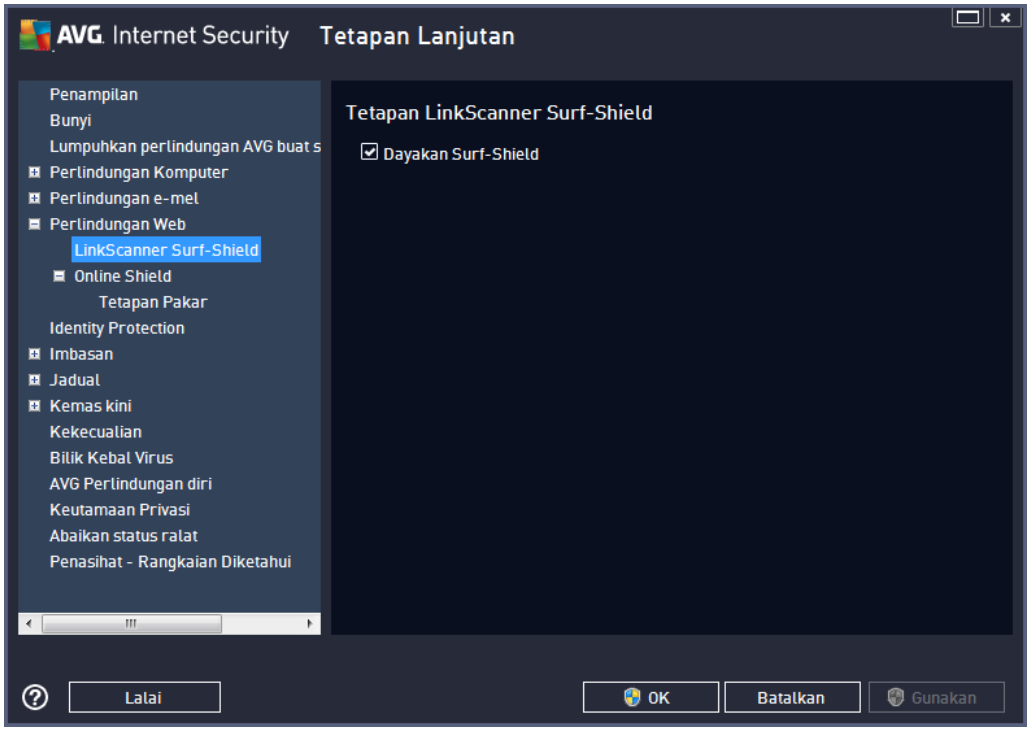
Cabang Tetapan Pakar mengandungi opsyen tetapan yang luas untuk ciri Anti-Spam. Tetapan ini bertujuan secara eksklusif untuk pengguna berpengalaman, biasanya pentadbir rangkaian yang perlu mengkonfigurasikan perlindungan antispam dalam perincian penuh untuk perlindungan terbaik pelayan e-mel. Atas sebab ini, tiada bantuan tambahan tersedia untuk dialog individu; namun, terdapat penerangan ringkas untuk setiap opsyen secara langsung dalam antara muka pengguna. Kami amat mengesyorkan untuk tidak menukar sebarang tetapan melainkan anda sangat biasa dengan tetapan lanjutan untuk Spamcatcher (MailShell Inc.). Sebarang perubahan yang tidak sesuai boleh menyebabkan prestasi menjadi buruk atau kefungsian komponen yang tidak betul.

Jika anda percaya anda masih perlu mengubah konfigurasi AntiSpam pada tahap yang sangat tinggi, sila ikuti arahan yang diberikan terus dalam antara muka pengguna. Secara umumnya, dalam setiap dialog anda akan menemui satu ciri khusus yang boleh anda sunting. Penerangannya sentiasa disertakan dalam dialog itu sendiri. Anda boleh menyunting parameter berikut:

- ***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

9.6. Perlindungan Pelayaran Web

Dialog ***tetapan LinkScanner*** membolehkan anda menandakan/nyahtandakan ciri berikut:



- ***Dayakan Surf-Shield*** – (*dihidupkan secara lalai*): perlindungan (*masa nyata*) aktif terhadap tapak eksploitatif semasa tapak tersebut diakses. Sambungan tapak yang diketahui berniat jahat dan kandungannya yang eksploitatif disekat semasa tapak tersebut diakses oleh pengguna melalui pelayar web (*atau sebarang aplikasi lain yang menggunakan HTTP*).

- ***Tambah 'Dijamin oleh LinkScanner'...*** – (*dimatikan secara lalai*): sahkan opsyen ini untuk memastikan supaya semua mesej yang dihantar daripada rangkaian sosial Facebook / MySpace yang mengandungi hiperpautan aktif akan diperakui sebagai disemak oleh LinkScanner.

9.6.1. Online Shield

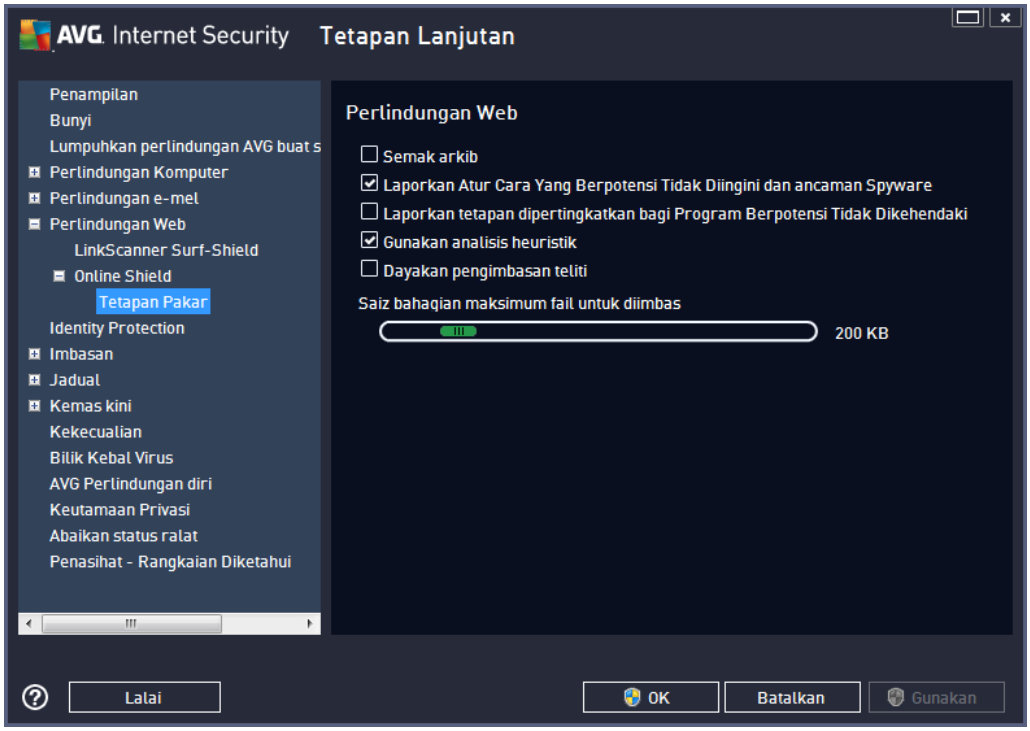
Dialog ***Online Shield*** menawarkan opsyen berikut:

- ***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 Pemecut AVG*** *(dihidupkan secara lalai)* – Aktifkan/nyahaktifkan perkhidmatan Pemecut AVG. Pemecut AVG membenarkan main balik video dalam talian yang lebih lancar dan membuatkan muat turun tambahan lebih mudah. Apabila proses pemecutan video sedang dijalankan, anda akan dimaklumkan melalui tetingkap timbul dulang sistem:

Mod pemberitahuan ancaman

Di bahagian bawah dialog, pilih kaedah yang mana anda ingin dimaklumkan mengenai potensi ancaman yang dikesan: melalui dialog 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*** – opsyen ini mengesahkan bahawa ***Online Shield*** harus melaksanakan imbasan pada kandungan halaman www. Dengan syarat opsyen ini dihidupkan (*secara lalai*), anda juga boleh menukar item ini kepada hidup/mati:

    - ***Periksa arkib*** – (*dimatikan secara lalai*): imbas kandungan arkib yang berkemungkinan dimasukkan dalam halaman www untuk dipaparkan.

    - ***Laporkan Atur Cara Yang Berpotensi Tidak Diingini dan ancaman Spyware*** – (*dihidupkan secara lalai*): tandakan untuk mengaktifkan imbasan spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

    - ***Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki*** – (*dimatikan secara lalai*): tandakan untuk mengesan pakej lanjutan bagi spyware: atur cara yang sememangnya baik dan tidak berbahaya apabila diperoleh dari pengilang secara terus tetapi boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan lagi keselamatan komputer anda, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.

    - ***Gunakan analisis heuristik*** – (*dihidupkan secara lalai*): imbas kandungan halaman yang akan dipaparkan menggunakan kaedah analisis heuristik (*perlagakan dinamik*

arahan objek yang diimbas dalam persekitaran komputer maya).

- ***Dayakan pengimbasan teliti*** (*dimatikan secara lalai*) – dalam situasi khusus (*kecurigaan tentang komputer anda dijangkiti*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang jarang dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.

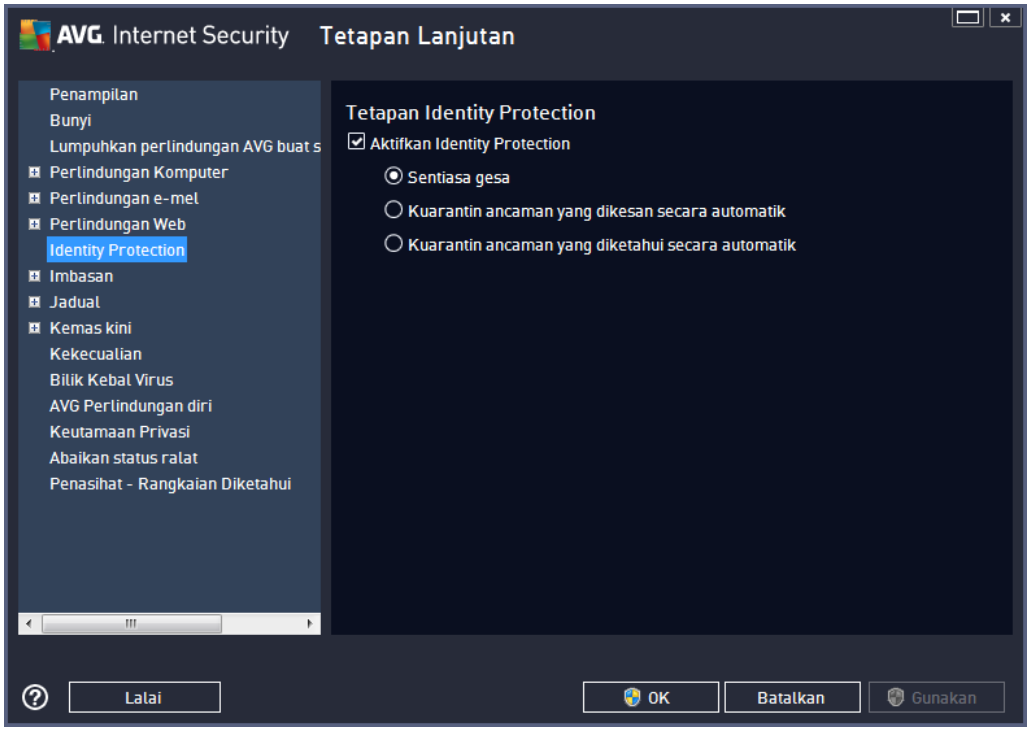
- ***Bahagian saiz fail maksimum untuk diimbas*** – jika fail yang dimasukkan terdapat dalam halaman yang dipaparkan, anda juga boleh mengimbas kandungannya sebelum ia dimuat turun ke komputer anda. Walau bagaimanapun, pengimbasan fail besar mengambil sedikit masa dan muat turun laman web mungkin menjadi perlahan. Anda boleh menggunakan bar gelangsar untuk menentukan saiz maksimum bagi fail yang masih diimbas dengan ***Perisai Dalam Talian***. Walaupun jika fail yang dimuat turun bersaiz lebih besar daripada yang dinyatakan, maka tidak akan diimbas dengan Online Shield, anda masih dilindungi: jika fail itu dijangkiti, ***Resident Shield*** akan mengesannya dengan serta-merta.

- ***Kecualikan hos/IP/domain*** – anda boleh menaip nama sebenar pelayan (*hos, alamat IP, alamat IP dengan topeng atau URL*) atau domain yang tidak harus diimbas oleh ***Online Shield*** ke dalam medan teks. Oleh itu, hanya kecualikan hos yang anda betul-betul pasti tidak akan memberikan kandungan tapak web berbahaya.

9.7. Identity Protection

Identity Protection ialah komponen anti-malware yang melindungi anda daripada semua jenis malware (*spyware, bot, kecurian identiti, ...*) menggunakan teknologi kelakuan dan memberikan perlindungan hari sifar untuk virus baharu *(untuk penerangan terperinci bagi kefungsian komponen sila rujuk bab Identity*).

Dialog ***tetapan Identity Protection*** membenarkan anda menghidupkan/mematikan ciri asas bagi komponen Identity Protection:



Aktifkan Identity Protection (*dihidupkan secara lalai*) – jangan tanda untuk mematikan komponen Identity.

Kami amat mengesyorkan agar tidak melakukan ini kecuali jika anda benar-benar perlu!

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 yang dikesan secara automatik*** – tandakan kotak semak ini untuk menentukan bahawa anda ingin semua ancaman yang mungkin dikesan dialihkan ke tempat selamat 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 yang diketahui secara automatik*** – biarkan item ini ditandakan jika anda ingin semua aplikasi yang dikesan sebagai kemungkinan malware untuk dialihkan secara automatik dan dengan serta-merta ke Bilik Kebal Virus.

9.8. Imbasan

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

- ***Imbas seluruh komputer*** – imbasan dipratakrif standard bagi seluruh komputer

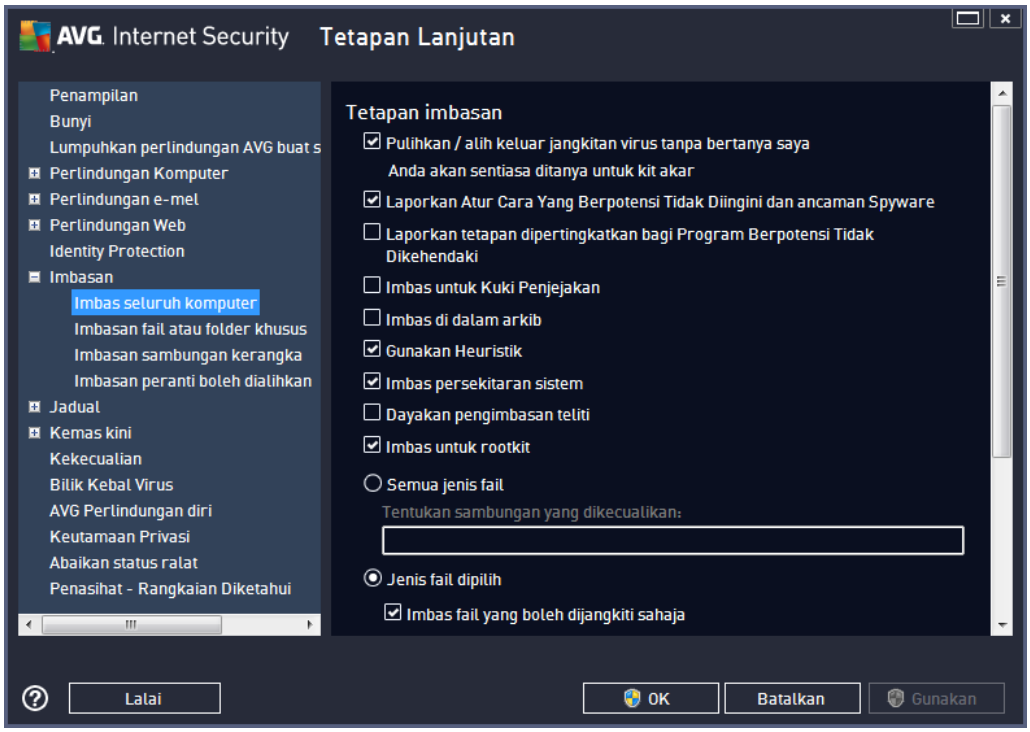
- ***Imbasan sambungan kerangka*** – imbasan khusus objek yang dipilih terus daripada persekitaran Windows Explorer

- ***Imbas fail atau folder tertentu*** – imbasan dipratakrif standard bagi kawasan yang dipilih pada komputer anda

- ***Imbasan peranti boleh dialihkan*** – imbasan khusus bagi peranti boleh dialihkan yang dipasang pada komputer anda

9.8.1. Imbasan seluruh komputer

Opsyen ***Imbas Seluruh Komputer*** membenarkan anda mengedit parameter bagi salah satu imbasan yang dipratakrifkan 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 Atur Cara Yang Berpotensi Tidak Diingini dan ancaman Spyware*** (*dihidupkan secara lalai*) – tandakan untuk mengaktifkan imbasan spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami

mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- ***Laporkan tetapan dipertingkatkan bagi Atur Cara Yang Berpotensi Tidak Diingini*** (*dimatikan secara lalai*) – tandakan untuk mengesan pakej spyware lanjutan: 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 Kuki Penjejakan*** (*dimatikan secara lalai*) – parameter ini menentukan supaya kuki harus dikesan ; (*kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*)

- ***Imbas di dalam arkib*** (*dimatikan secara lalai*) – parameter ini menentukan bahawa imbasan harus menyemak 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*** (*dimatikan secara lalai*) – dalam situasi khusus (*kecurigaan tentang komputer anda dijangkiti*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang jarang 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.

Anda juga harus menentukan sama ada anda mahu mengimbas

- ***Semua jenis fail*** dengan opsyen mentakrifkan pengecualian daripada imbasan dengan memberikan senarai sambungan fail yang dipisahkan koma (*selepas disimpan, koma bertukar kepada koma bertitik*) yang tidak harus diimbas;

- ***Jenis fail dipilih*** – anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang boleh dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya fail teks biasa atau fail tidak boleh laku yang lain*), termasuk fail media (*fail video, audio – jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa imbasan kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan melalui sambungan fail mana yang seharusnya sentiasa diimbas.

- Secara pilihan, anda boleh menentukan anda hendak ***Imbas fail tanpa sambungan*** –

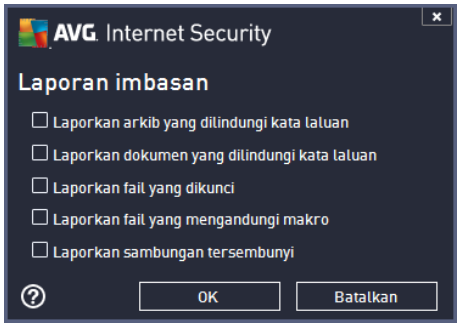
opsyen ini dihidupkan secara lalai dan adalah disyorkan supaya anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan seharusnya diimbas setiap masa.

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 imbasan dijalankan dengan lebih cepat, ia akan mengambil masa yang kurang tetapi penggunaan sumber sistem akan meningkat dengan ketara semasa 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 sumber sistem yang digunakan dengan menambah tempoh pengimbasan.

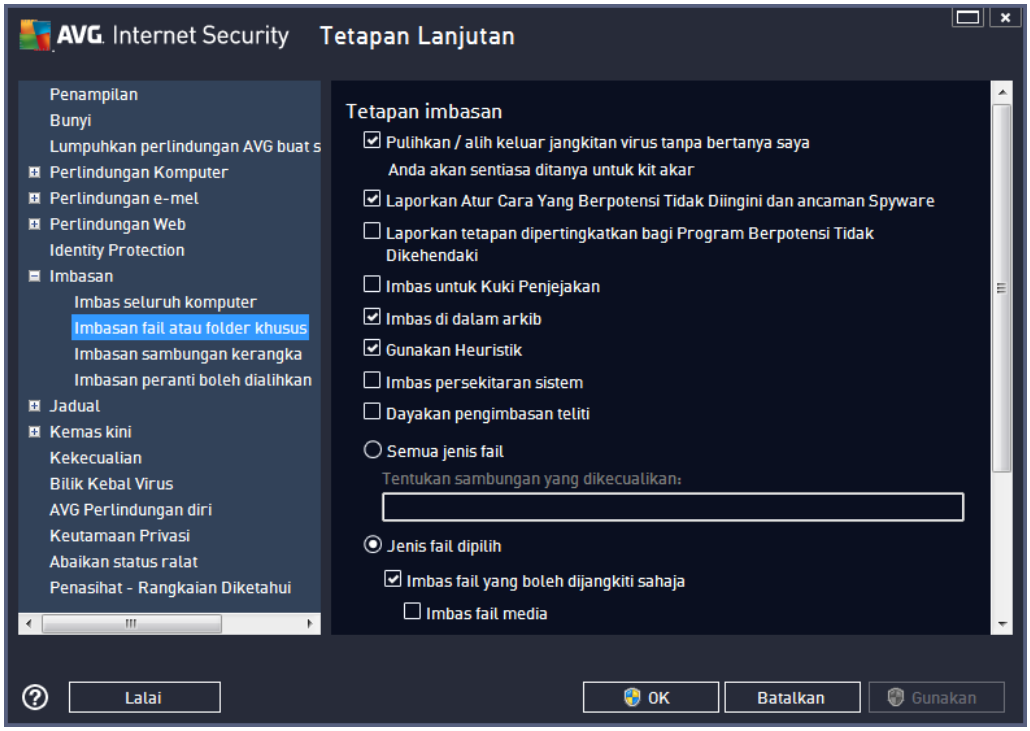
Tetapkan laporan imbasan tambahan ...

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



9.8.2. Imbasan fail atau folder khusus

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

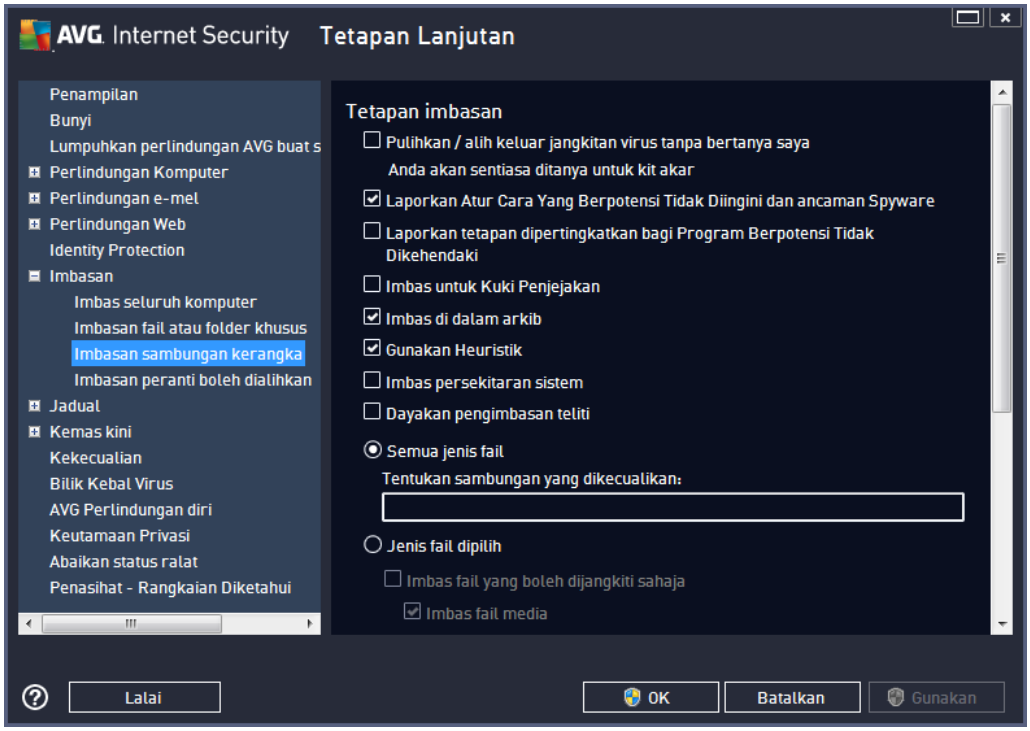


Semua parameter yang disediakan dalam dialog konfigurasi ini hanya digunakan pada kawasan yang dipilih untuk imbasan dengan Imbas fail atau folder tertentu!

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

9.8.3. Imbasan sambungan kerangka

Sama dengan item Imbasan seluruh komputer sebelumnya, item ini dinamakan ***Imbasan sambungan kerangka*** juga menawarkan beberapa opsyen untuk pengeditan imbasan yang dipratakrif oleh vendor perisian. Kali ini konfigurasi adalah berkaitan dengan persekitaran mengimbas objek tertentu yang dilancarkan terus daripada Windows Explorer (*sambungan kerangka*), lihat bab Mengimbas dalam Windows Explorer:



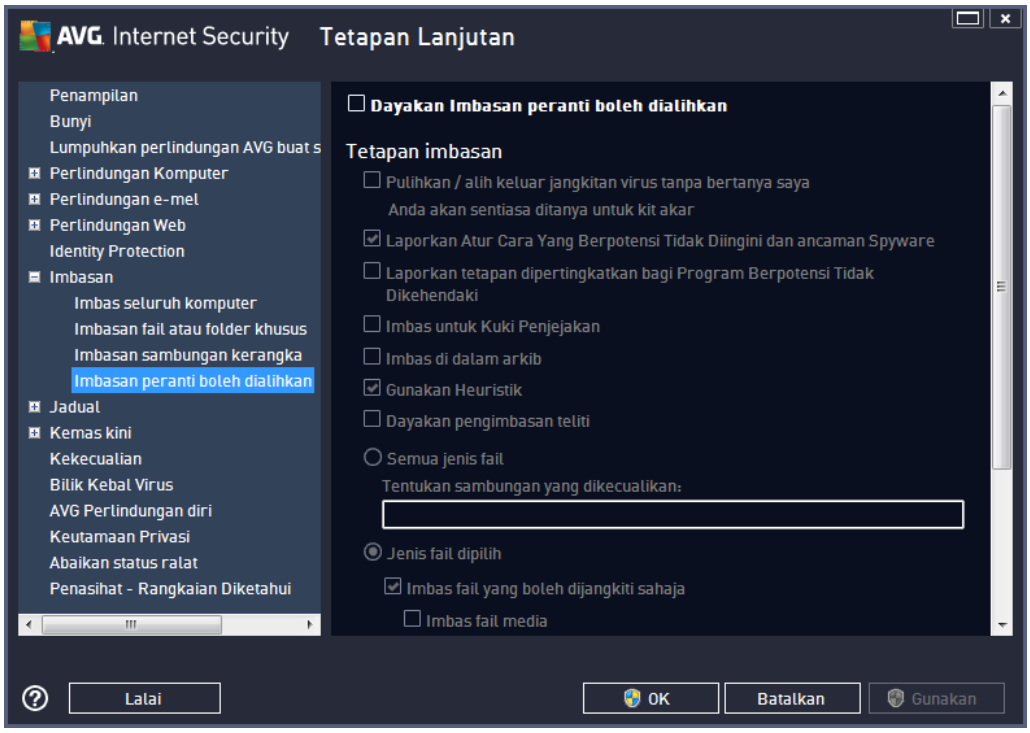
Senarai parameter adalah sama dengan senarai yang tersedia untuk Imbas seluruh komputer. Walau bagaimanapun, tetapan lalai berbeza (*contohnya, Imbas Seluruh Komputer secara lalainya tidak menyemak arkib tetapi ia mengimbas persekitaran sistem, bertentangan dengan Imbasan Sambungan Kerangka*).

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

Dibandingkan dengan dialog Imbas Seluruh Komputer, dialog ***Imbas sambungan kerangka*** juga menyertakan bahagian yang dipanggil ***Tetapan lain yang berkaitan dengan Antara Muka Pengguna AVG***, di mana anda boleh menentukan sama ada anda mahu kemajuan imbasan dan keputusan imbasan untuk menjadi boleh diakses daripada antara muka pengguna AVG. Anda juga boleh menentukan bahawa keputusan imbasan hanya harus dipaparkan sekiranya jangkitan dikesan semasa pengimbasan.

9.8.4. 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 memasangkan sebarang peranti boleh dialihkan pada komputer anda. Secara lalainya, imbasan ini dimatikan. Walau bagaimanapun, adalah penting untuk mengimbas peranti boleh dialihkan untuk mengesan kemungkinan ancaman memandangkan ini adalah sumber jangkitan utama. Untuk menyediakan dan melancarkan imbasan ini secara automatik apabila diperlukan, tanda opsyen ***Dayakan Imbasan peranti boleh dialihkan***.

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

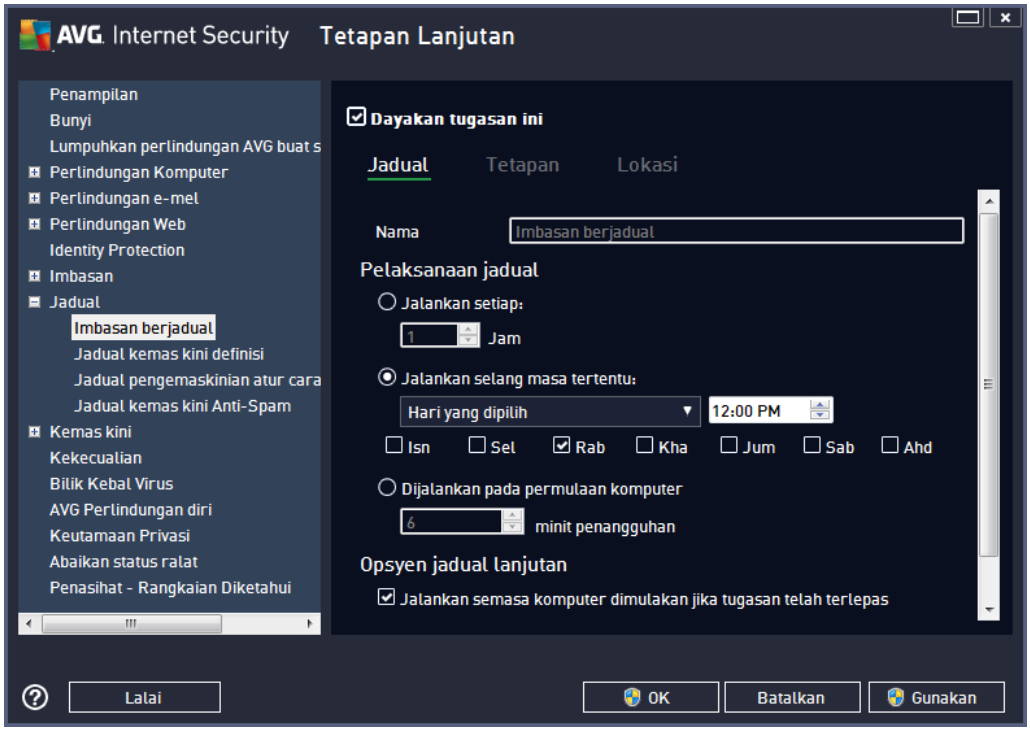
9.9. Jadual

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

- Imbasan berjadual
- Jadual kemas kini definisi
- Jadual kemas kini atur cara
- Jadual kemas kini AntiSpam

9.9.1. Imbasan Berjadual

Parameter imbasan berjadual boleh disunting (*atau persediaan jadual baharu*) pada tiga tab. Pada setiap tab, anda boleh menanda/tidak menanda dahulu item ***Dayakan tugasan ini*** untuk menyahaktifkan ujian yang dijadualkan buat sementara waktu dan menghidupkannya semula apabila diperlukan:



Seterusnya, medan teks yang dipanggil ***Nama*** (*dinyahaktifkan untuk semua jadual lalai*) menyatakan nama yang diperuntukkan untuk jadual ini oleh vendor atur cara. Untuk jadual yang baru ditambah (*anda boleh menambah jadual baharu dengan mengklik kanan item* ***Imbasan berjadual*** *dalam pepohon navigasi kiri*) anda boleh menentukan nama anda sendiri dan dalam hal itu, medan teks tersebut akan terbuka untuk penyuntingan. Cuba sentiasa gunakan nama yang ringkas, deskriptif dan sesuai untuk imbasan bagi menjadikannya lebih mudah untuk dibezakan daripada imbasan lain kemudiannya.

Contoh: *Adalah tidak sesuai untuk menamakan imbasan itu "Imbasan baharu" atau "Imbasan saya" memandangkan nama-nama ini tidak merujuk kepada apa yang sebenarnya disemak oleh imbasan itu. Sebaliknya, contoh nama deskriptif yang baik adalah "Imbasan kawasan sistem" dsb. Ia juga tidak perlu untuk menyatakan nama imbasan sama ada ia adalah imbasan seluruh komputer atau hanya imbasan fail atau folder yang dipilih – imbasan anda sendiri sentiasa akan menjadi versi khusus imbasan fail atau folder yang dipilih.*

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

Pelaksanaan jadual

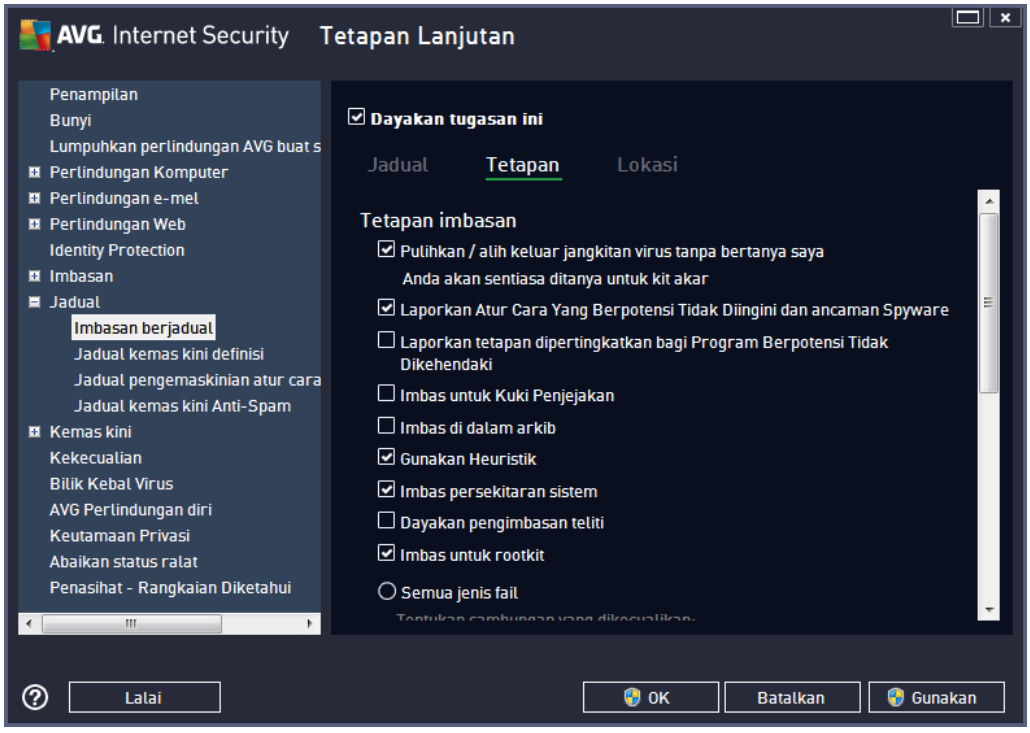
Di sini, anda boleh menentukan jarak waktu untuk pelancaran imbasan yang baru dijadualkan.

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 tetingkap timbul pada ikon dulang sistem AVG.

Kemudian, Ikon dulang sistem AVG yang baharu 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 ***Tetapan*** anda akan menemui senarai parameter pengimbasan yang boleh dihidupkan/ dimatikan secara pilihan. Secara lalai, kebanyakan parameter dihidupkan dan kefungsiannya akan digunakan semasa pengimbasan. ***Melainkan anda mempunyai alasan yang sah untuk menukar tetapan ini, kami mengesyorkan supaya anda mengekalkan konfigurasi yang dipratakrifkan 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 Atur Cara Yang berpotensi Tidak Diingini dan ancaman Spyware*** *(dihidupkan secara lalai):* tandakan untuk mengaktifkan imbasan spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- ***Laporkan tetapan dipertingkatkan Atur Cara Yang Berpotensi Tidak Diingini*** (*dimatikan secara lalai*): tandakan untuk mengesan pakej lanjutan spyware: 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 Kuki Penjejakan*** (*dimatikan secara lalai*): parameter ini menentukan bahawa kuki harus dikesan semasa mengimbas; (*Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*)

- ***Imbas di dalam arkib*** (*dimatikan secara lalai*): parameter ini menentukan bahawa pengimbasan harus menyemak semua fail walaupun jika ia disimpan di 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*** (*dimatikan secara lalai):* dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsyen 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 Anti-Rootkit mencari kemungkinan terdapatnya rootkit di dalam komputer anda, cth. atur cara 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.

Anda juga harus menentukan sama ada anda mahu mengimbas

- ***Semua jenis fail*** dengan opsyen mentakrifkan pengecualian daripada imbasan dengan memberikan senarai sambungan fail yang dipisahkan koma (*selepas disimpan, koma bertukar kepada koma bertitik*) yang tidak harus diimbas;

- ***Jenis fail dipilih*** – anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang boleh dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya fail*

teks biasa atau fail tidak boleh laku yang lain), termasuk fail media *(fail video, audio – jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa imbasan kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus)*. Sekali lagi, anda boleh menentukan melalui sambungan fail mana yang seharusnya sentiasa diimbas.

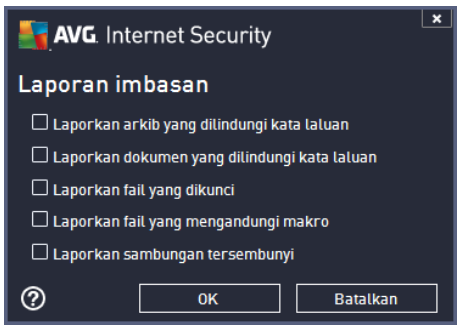
- Secara pilihan, anda boleh menentukan anda hendak ***Imbas fail tanpa sambungan*** – opsyen ini dihidupkan secara lalai dan adalah disyorkan supaya anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan seharusnya diimbas setiap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

Laraskan berapa cepat imbasan selesai

Dalam bahagian ini anda boleh menentukan dengan lebih lanjut kelajuan imbasan yang diingini bergantung kepada penggunaan sumber sistem. Secara lalainya, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Jika anda mahu imbasan dijalankan dengan lebih cepat, ia akan mengambil masa yang kurang tetapi penggunaan sumber sistem akan meningkat dengan ketara semasa 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 sumber sistem yang digunakan dengan melanjutkan tempoh pengimbasan.

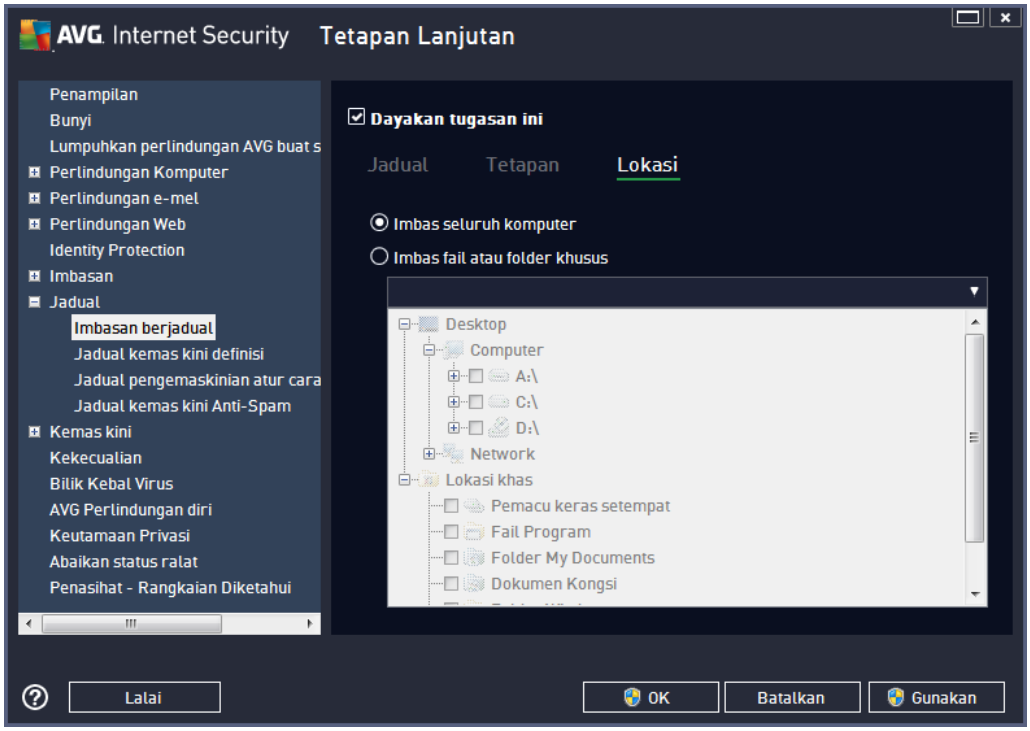
Tetapkan laporan imbasan tambahan

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



Opsyen mematikan komputer

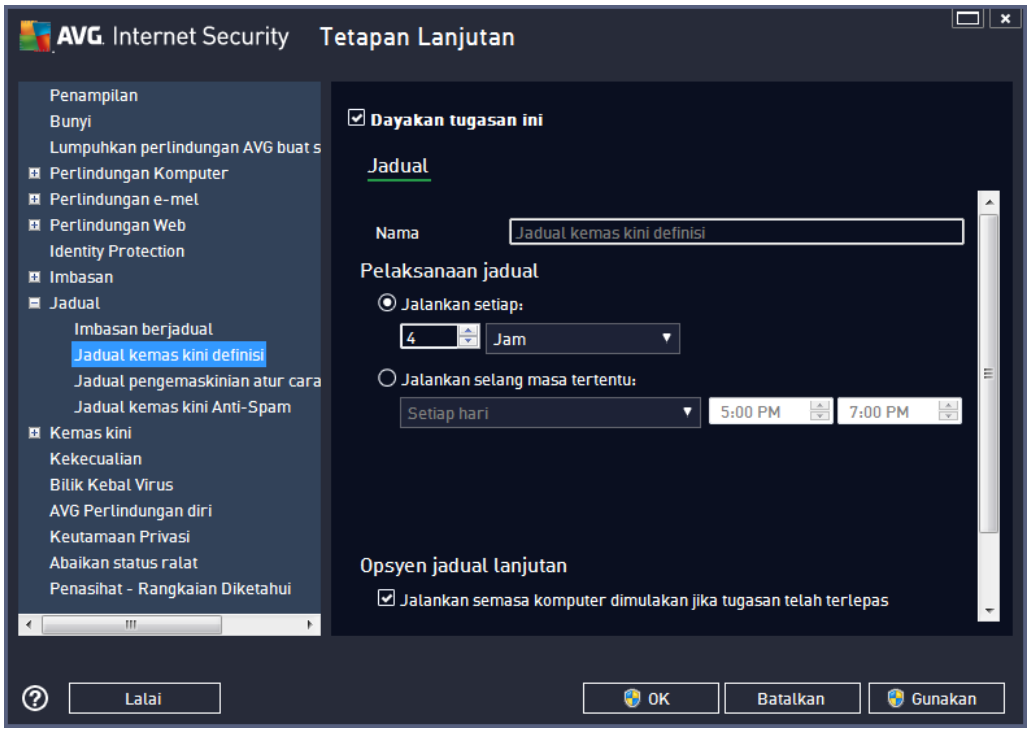
Dalam bahagian ***Opsyen penutupan komputer*** anda boleh menentukan sama ada komputer harus ditutup secara automatik sebaik saja imbasan yang sedang berjalan selesai. Dengan mengesahkan opsyen ini (***Matikan komputer sebaik sahaja imbasan selesai***), opsyen baharu diaktifkan yang membenarkan komputer dimatikan walaupun jika ia sedang dikunci (***Paksa penutupan jika komputer dikunci***).



Pada tab ***Lokasi*** anda boleh menentukan sama ada anda mahu menjadualkan pengimbasan seluruh komputer atau pengimbasan fail atau folder tertentu. Jika anda memilih pengimbasan fail atau folder tertentu, dalam bahagian bawah dialog ini, struktur pepohon yang dipaparkan diaktifkan dan anda boleh menentukan folder untuk diimbas.

9.9.2. 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 untuk jadual kemas kini definisi. Medan teks yang dipanggil ***Nama*** (*dinyahaktifkan untuk semua jadual lalai*) menunjukkan nama yang diperuntukkan untuk jadual ini oleh vendor atur cara.

Menjalankan 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

Bahagian ini membenarkan anda untuk mentakrifkan di mana kemas kini definisi harus/tidak harus dilancarkan jika komputer di dalam mod kuasa rendah atau dimatikan sepenuhnya.

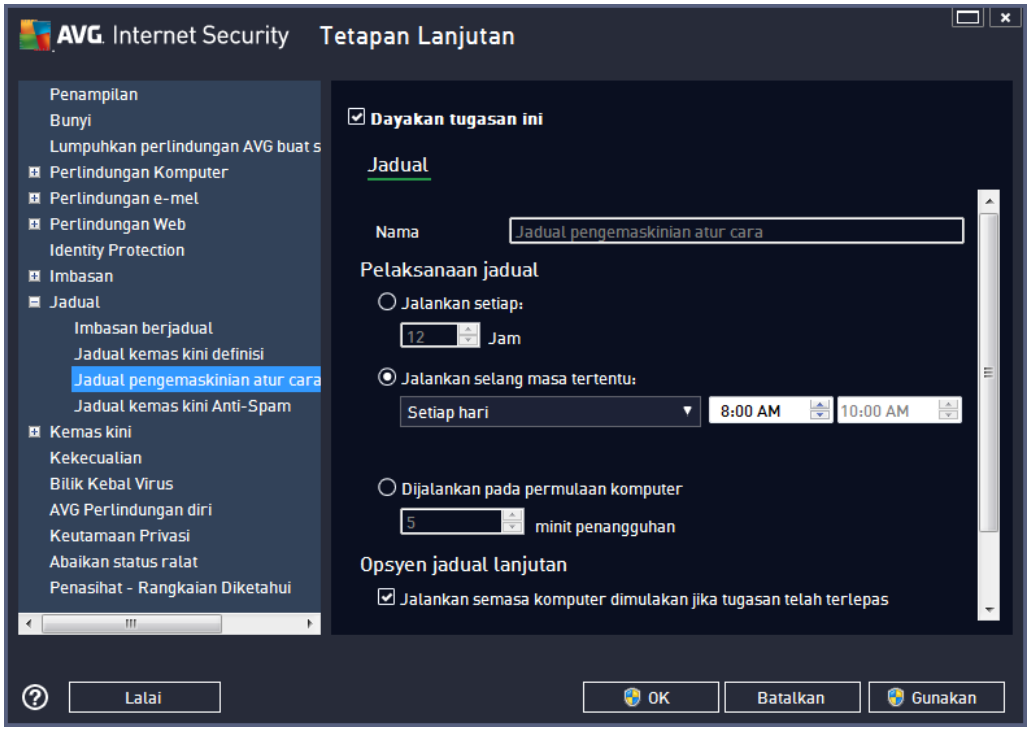
Tetapan kemas kini yang lain

Akhir sekali, tandakan opsyen ***Jalankan kemas kini semula sebaik sahaja sambungan Internet tersedia*** untuk memastikan bahawa jika sambungan Internet terganggu dan proses kemas kini gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan Internet dipulihkan.

Sebaik sahaja kemas kini berjadual dilancarkan pada masa yang anda telah tentukan, anda akan diberitahu mengenai hal ini melalui tetingkap timbul yang terbuka di atas ikon dulang sistem AVG (*dengan syarat anda telah menyimpan konfigurasi lalai dialog Tetapan Lanjutan/Penampilan*).

9.9.3. 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:



Medan teks yang dipanggil ***Nama*** (*dinyahaktifkan untuk semua jadual lalai*) menunjukkan nama yang diperuntukkan untuk 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.

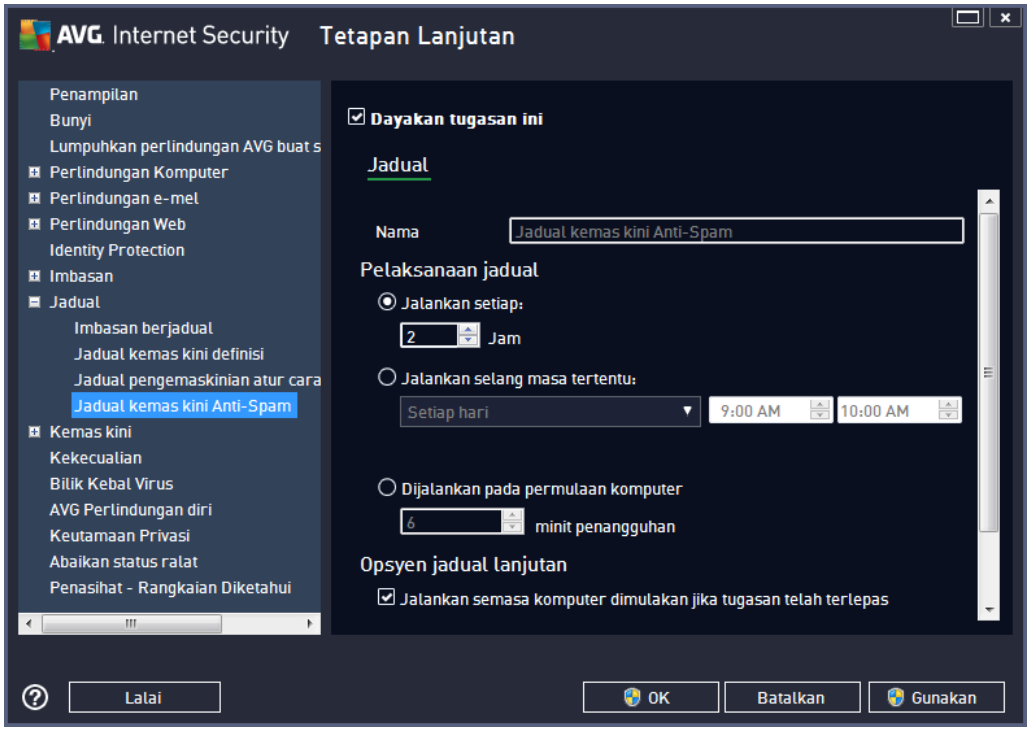
Tetapan kemas kini yang lain

Tandakan opsyen ***Jalankan kemas kini semula sebaik sahaja sambungan Internet tersedia*** untuk memastikan bahawa jika sambungan Internet terganggu dan proses kemas kini gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan Internet dipulihkan. Sebaik sahaja kemas kini berjadual dilancarkan pada masa yang anda telah tentukan, anda akan diberitahu mengenai hal ini melalui tetingkap timbul yang terbuka di atas ikon dulang sistem AVG (*dengan syarat anda telah menyimpan konfigurasi lalai dialog Tetapan Lanjutan/Penampilan*).

Nota: *Jika masa bagi kemas kini atur cara berjadual dan imbasan berjadual berlaku serentak, proses kemas kini adalah lebih utama dan imbasan akan terganggu.*

9.9.4. 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. Medan teks yang dipanggil ***Nama*** (*dinyahaktifkan untuk semua jadual lalai*) menyatakan nama yang diperuntukkan untuk jadual ini oleh vendor atur cara.

Menjalankan jadual

Di sini, tentukan jarak waktu untuk pelancaran kemas kini Anti-Spam yang baru dijadualkan. Pemasaan boleh ditentukan sama ada oleh pelancaran kemas kini Anti-Spam selepas tempoh masa tertentu (***Dijalankan setiap ...***) atau dengan menentukan tarikh dan masa sebenar (

Dijalankan dalam jarak masa tertentu), atau berkemungkinan dengan menentukan acara yang harus dikaitkan dengan pelancaran kemas kini (***Tindakan berdasarkan permulaan komputer***).

Opsyen jadual lanjutan

Bahagian ini membolehkan anda menentukan dalam apa 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 terganggu dan proses kemas kini Anti-Spam gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan Internet dipulihkan.

Sebaik sahaja imbasan berjadual dilancarkan pada masa yang anda telah tentukan, anda akan diberitahu mengenai hal ini melalui tetingkap timbul yang terbuka di atas ikon dulang sistem AVG (*dengan syarat anda telah menyimpan konfigurasi lalai dialog Tetapan Lanjutan/Penampilan).*

9.10. Kemas kini

Item navigasi ***Kemas Kini*** membuka dialog baharu di mana anda boleh menentukan parameter umum berkenaan kemas kini AVG:

Bila untuk mengemas kini fail

Dalam bahagian ini, anda boleh memilih tiga opsyen alternatif untuk digunakan jika proses kemas kini memerlukan anda memulakan semula PC. Penyelesaian kemas kini boleh dijadualkan kepada permulaan semula PC berikutnya atau anda boleh melancarkan permulaan 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 opsyen ini hanya disyorkan jika anda pasti untuk memulakan semula komputer anda dengan kerap, sekurang-kurangnya sekali sehari!

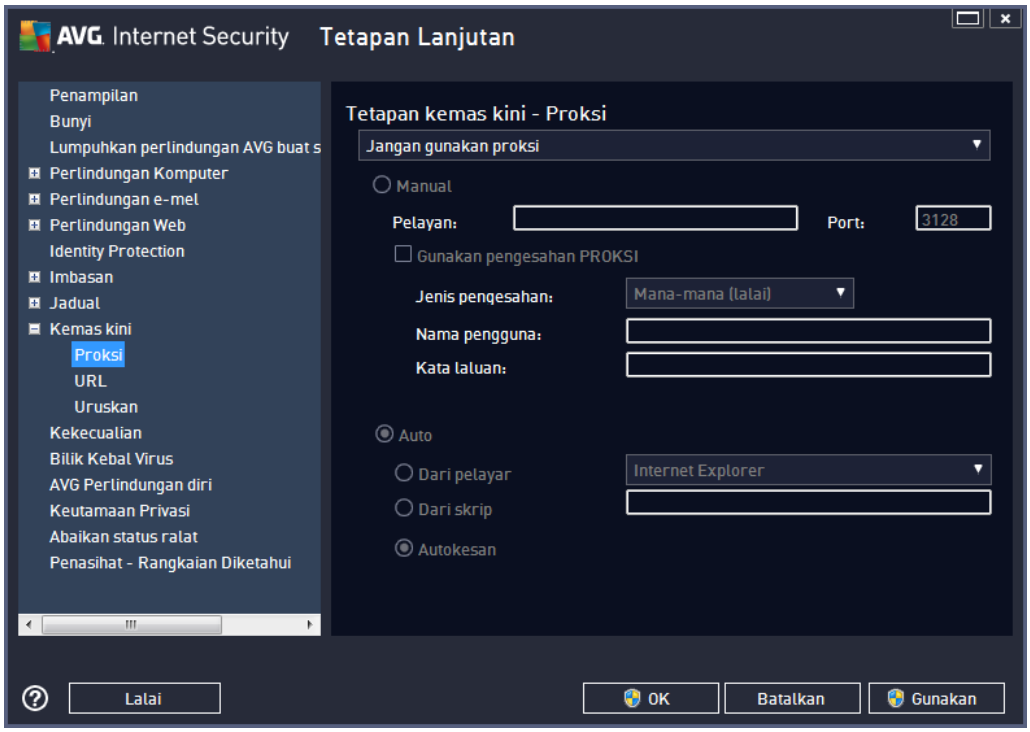
Imbasan memori selepas kemas kini

Tandakan kotak semak ini untuk menentukan bahawa anda hendak melancarkan imbasan memori baharu selepas setiap kemas kini yang berjaya diselesaikan. Kemas kini terkini yang dimuat turun mungkin mengandungi definisi virus baharu dan ini boleh digunakan dalam pengimbasan dengan serta-merta.

Opsyen kemas kini tambahan

- ***Bina titik pemulihan sistem baharu semasa 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 ranap, anda sentiasa boleh memulihkan OS anda kepada konfigurasi asalnya dari titik ini. Opsyen ini boleh diakses melalui Start / All Programs / Accessories / System tools / System Restore, tetapi sebarang perubahan hanya boleh disyorkan kepada pengguna berpengalaman sahaja! Pastikan kotak semakan ini ditandakan jika anda hendak menggunakan kefungsian ini.
- ***Gunakan kemas kini DNS*** (*dihidupkan secara lalai*) – dengan item ini ditandakan, sebaik sahaja kemas kini dilancarkan, **AVG Internet Security 2013** 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*) hal ini akan membantu anda memastikan tiada aplikasi yang sedang dijalankan yang akan ditutup tanpa kebenaran anda – jika diperlukan untuk proses kemas kini diselesaikan.
- ***Semak 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.

9.10.1. 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:

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

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

Konfigurasi manual

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

- ***Pelayan*** – menentukan alamat IP pelayan atau nama pelayan
- ***Port*** – menentukan bilangan port yang mendayakan akses Internet (*secara lalai, nombor ini*

ditetapkan kepada 3128 tetapi boleh ditetapkan secara berbeza – jika anda tidak pasti, hubungi pentadbir rangkaian anda)

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

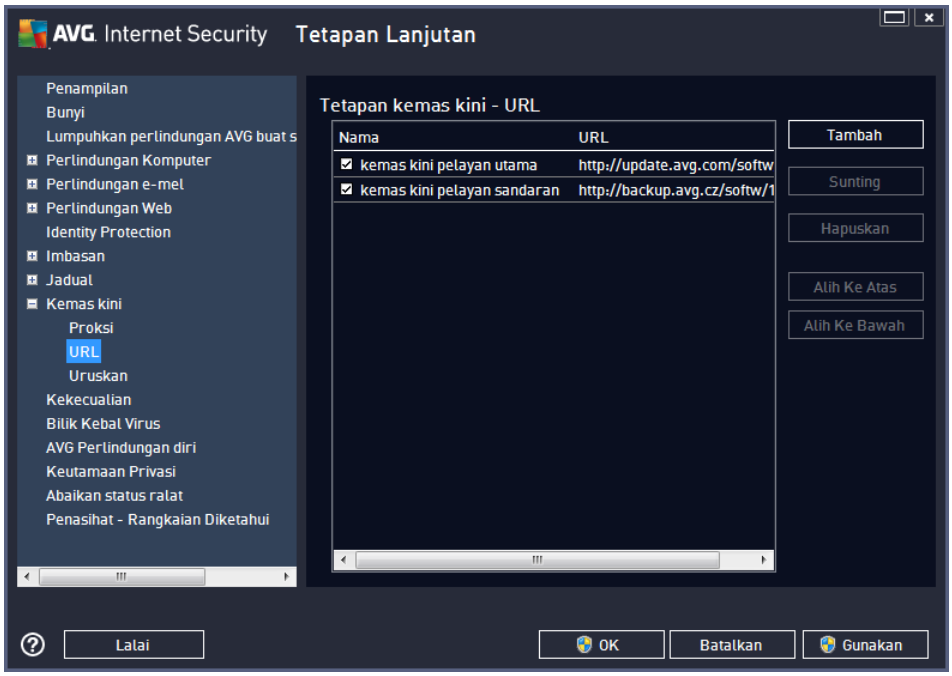
Konfigurasi automatik

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

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

9.10.2. 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 baharu untuk ditambah

ke senarai

- ***Edit*** – membuka dialog di mana anda boleh mengedit parameter URL yang dipilih
- ***Hapuskan*** – hapuskan URL yang dipilih dari senarai
- ***Alih ke Atas*** – mengalihkan URL yang dipilih ke satu kedudukan atas dalam senarai
- ***Alih ke Bawah*** – mengalihkan URL yang dipilih ke satu kedudukan ke bawah dalam senarai

9.10.3. Uruskan

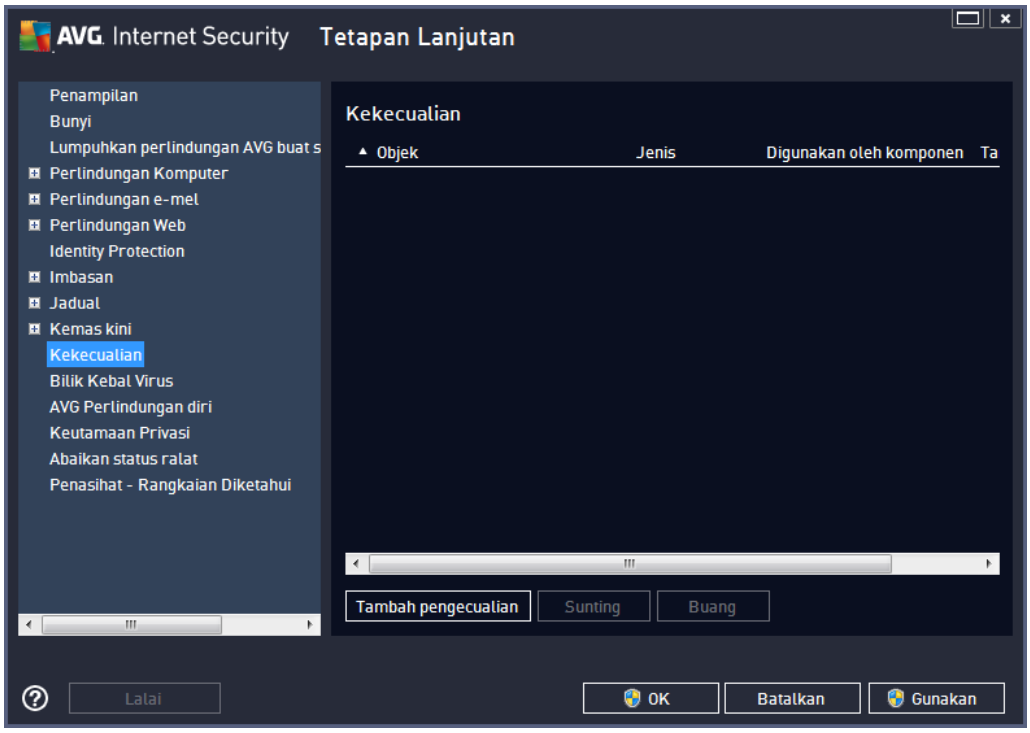
Dialog ***Uruskan pengurusan*** menawarkan dua opsyen yang boleh diakses melalui dua butang:

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

9.11. Pengecualian

Dalam dialog ***Pengecualian*** anda boleh mentakrifkan pengecualian, iaitu, item yang **AVG Internet Security 2013** akan abaikan. Biasanya, anda perlu mentakrifkan pengecualian jika AVG terus mengesan atur cara atau fail sebagai ancaman atau menyekat tapak web yang selamat sebagai berbahaya. Tambahkan fail atau tapak web sedemikian pada senarai pengecualian ini dan AVG tidak akan melaporkan atau menyekatnya lagi.

Sila sentiasa pastikan bahawa fail, atur cara atau tapak web yang dipersoalkan benar-benar selamat!



Carta dalam dialog memaparkan senarai pengecualian, jika terdapat pengecualian yang telah ditakrifkan. Setiap item mempunyai kotak semak di sebelahnya. Jika kotak semak ditandakan, maka pengecualian berkuat kuasa; jika tidak, maka pengecualian hanya ditentukan tetapi tidak digunakan buat masa ini. Dengan mengklik pengepala lajur, anda boleh mengisih item yang dibenarkan mengikut kriteria masing-masing.

Butang kawalan

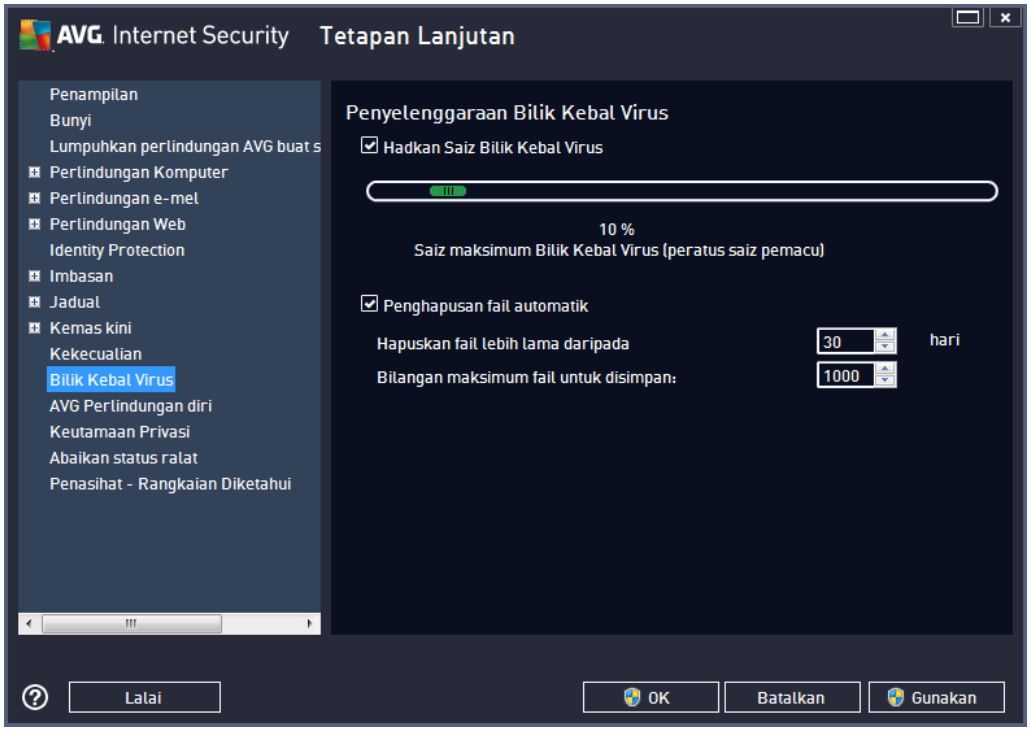
- ***Tambah pengecualian*** – Klik untuk membuka dialog baharu di mana anda boleh menentukan item yang harus dikecualikan daripada pengimbasan AVG. Pertama sekali, anda akan dijemput untuk mentakrifkan jenis objek, cth. sama ada ia adalah fail, folder atau URL. Kemudian, anda perlu menyemak imbas cakera anda untuk memberikan laluan ke objek berkenaan atau taipkan URL. Akhir sekali, anda boleh memilih ciri AVG mana yang harus mengabaikan objek yang dipilih *(Resident Shield, Identiti, Imbasan, Anti-Rootkit)*.

- ***Sunting*** – Butang ini hanya aktif jika beberapa pengecualian telah ditakrifkan dan disenaraikan dalam carta. Kemudian, anda boleh menggunakan butang untuk membuka dialog pengeditan pada pengecualian yang dipilih dan mengkonfigurasi parameter pengecualian.

- ***Buang*** – Gunakan butang ini untuk membatalkan pengecualian yang ditakrifkan sebelum ini. Anda boleh sama ada membuang satu per satu atau menyerlahkan satu blok pengecualian dalam senarai dan membatalkan pengecualian yang ditakrifkan. Dengan membatalkan pengecualian, fail, folder atau URL yang berkenaan akan disemak semula oleh AVG. Sila maklum bahawa hanya pengecualian akan dibuang, bukan fail atau folder itu

sendiri!

9.12. Bilik Kebal Virus

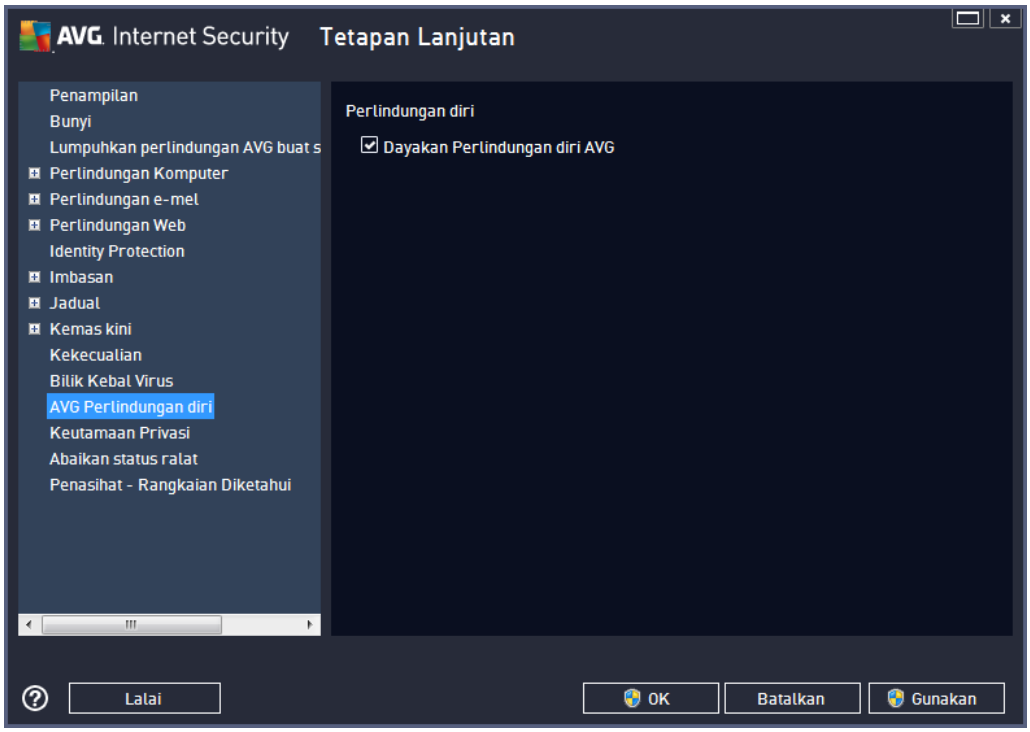


Dialog ***penyelenggaraan Bilik Kebal Virus*** membenarkan anda menentukan beberapa parameter berkenaan pentadbiran objek yang disimpan dalam Bilik Kebal Virus:

- ***Hadkan saiz Bilik Kebal Virus*** – gunakan gelangsar untuk menyediakan saiz maksimum bagi Bilik Kebal Virus. Saiz tersebut ditentukan mengikut perkadaran dibandingkan dengan saiz cakera setempat anda.

- ***Pemadaman fail automatik*** – dalam bahagian ini menentukan tempoh masa maksimum bagi objek yang patut disimpan dalam Bilik Kebal Virus (***Hapuskan fail yang lebih lama daripada ... hari***), dan bilangan fail maksimum untuk disimpan dalam Bilik Kebal Virus (***Bilangan fail maksimum untuk disimpan***).

9.13. Perlindungan Diri AVG

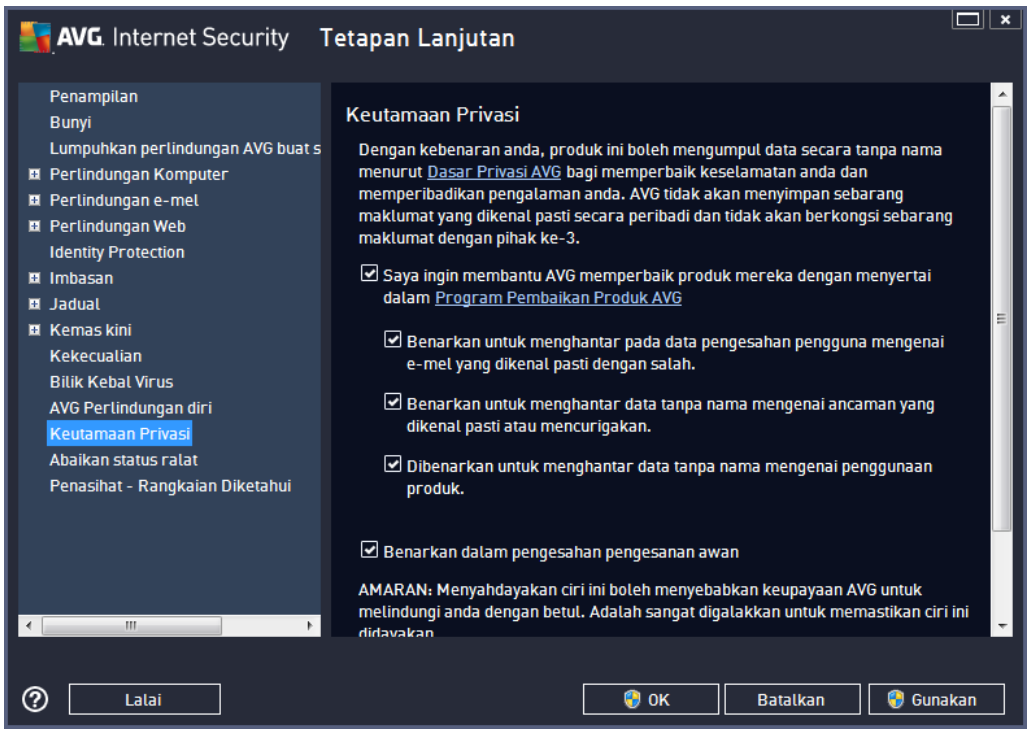


Perlindungan Diri AVG membolehkan **AVG Internet Security 2013** untuk melindungi prosesnya sendiri, fail, kekunci daftaran dan pemacu daripada ditukar atau dinyahaktifkan. Sebab utama untuk jenis perlindungan ini adalah kerana sesetengah ancaman yang canggih cuba untuk mematikan perlindungan antivirus dan kemudian bebas mengakibatkan kerosakan pada komputer anda.

Kami mengesyorkan supaya ciri ini sentiasa dihidupkan!

9.14. Keutamaan Privasi

Dialog ***Keutamaan Privasi*** menjemput anda untuk mengambil bahagian dalam pembaikan produk AVG dan untuk membantu kami meningkatkan tahap keseluruhan keselamatan Internet. Laporan anda membantu kami mengumpul maklumat terkini tentang ancaman terbaru daripada semua peserta di seluruh dunia dan sebagai ganti, kami dapat memperbaiki perlindungan untuk semua orang. Pelaporan tersebut dibuat secara automatik dan oleh itu, tidak menyebabkan sebarang kesulitan kepada anda. Tiada data peribadi disertakan dalam laporan ini. Melaporkan ancaman yang dikesan adalah pilihan, walau bagaimanapun, kami meminta anda untuk membiarkan opsyen ini dihidupkan. Ia membantu kami memperbaiki perlindungan untuk anda dan pengguna AVG lain.



Dalam dialog, opsyen tetapan berikut tersedia:

- ***Saya ingin membantu AVG memperbaik produk mereka dengan mengambil bahagian dalam Program Pembaikan Produk AVG*** *(dihidupkan secara lalai)* – Jika anda ingin membantu kami memperbaik lebih lanjut **AVG Internet Security 2013**, tandakan kotak semak. Ini akan membolehkan semua ancaman yang dihadapi dilaporkan 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 tersebut dibuat secara automatik dan oleh itu, tidak menyebabkan sebarang kesulitan kepada anda 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 perkhidmatan 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, spyware 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.

- ***Saya mahu AVG memperibadikan pengalaman saya dengan menghidupkan Pemeribadian AVG*** – ciri ini menganalisis kelakuan atur cara dan aplikasi yang dipasang pada PC anda secara tanpa nama. Berdasarkan pada analisis ini AVG boleh menawarkan kepada anda perkhidmatan yang disasarkan terus kepada keperluan anda, untuk menjamin keselamatan maksimum anda.

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 melebihkan bebas pelayan e-mel dan sistem rangkaian.

- ***Spyware*** 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.

- ***Atur cara yang berpotensi tidak diingini*** adalah sejenis spyware yang boleh tetapi tidak semestinya berbahaya kepada komputer anda. Contoh khusus PUP adalah adware, perisian yang direka untuk mengedarkan pengiklanan, biasanya dengan memaparkan iklan timbul; mengganggu, tetapi tidak benar-benar berbahaya.

- ***Kuki penjejakan*** boleh dianggap sebagai sejenis spyware, 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.

- ***Eksploit*** 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, potensi mangsa dihubungi melalui e-mel pukal yang meminta mereka untuk cthnya. mengemas kini butiran akaun bank mereka. Untuk melakukan perkara tersebut, mereka dijemput mengikuti pautan yang diberikan yang kemudiannya membawa kepada laman web palsu bank itu.

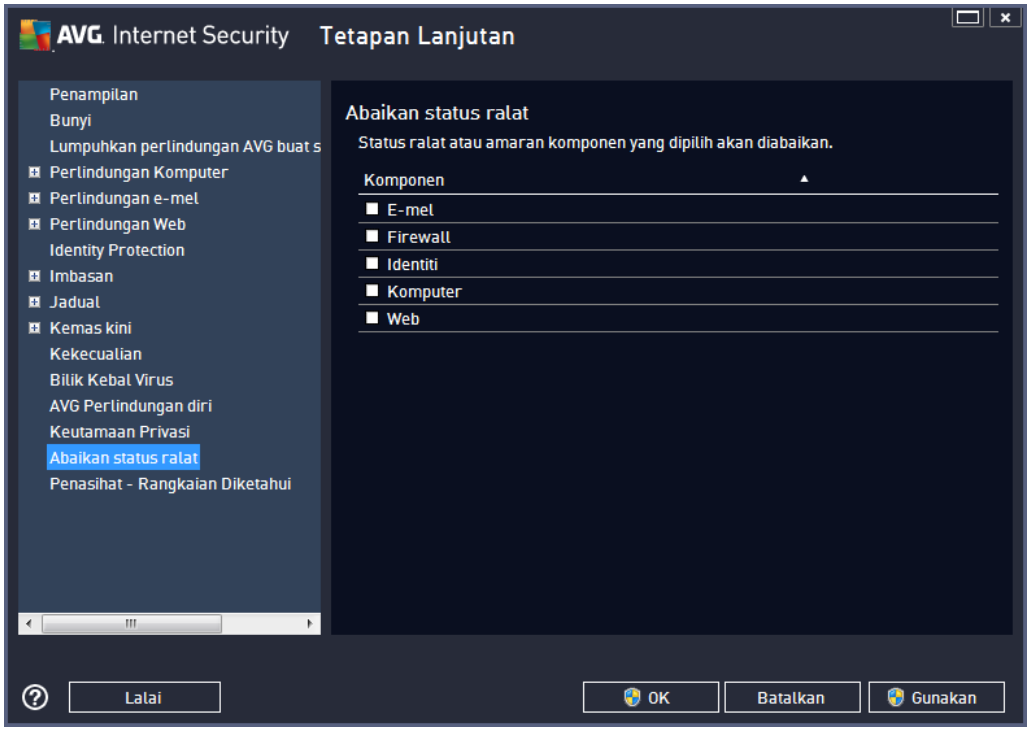
- ***Palsu*** ialah e-mel pukal yang mengandungi maklumat berbahaya, merisaukan atau cuma mengganggu dan tidak berguna. Kebanyakan dari ancaman di atas menggunakan mesej e-mel palsu untuk disebarkan.

- ***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 2013 memasukkan komponen yang dikhususkan. Untuk penerangan ringkas mengenai perkara ini, sila rujuk bab Gambaran Keseluruhan Komponen.

9.15. 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 diberikan 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 tetingkap utama AVG

Mungkin terdapat situasi di mana atas sebab tertentu anda perlu mematikan komponen tersebut buat sementara waktu. ***Ini tidak disyorkan, anda seharusnya cuba memastikan supaya semua***

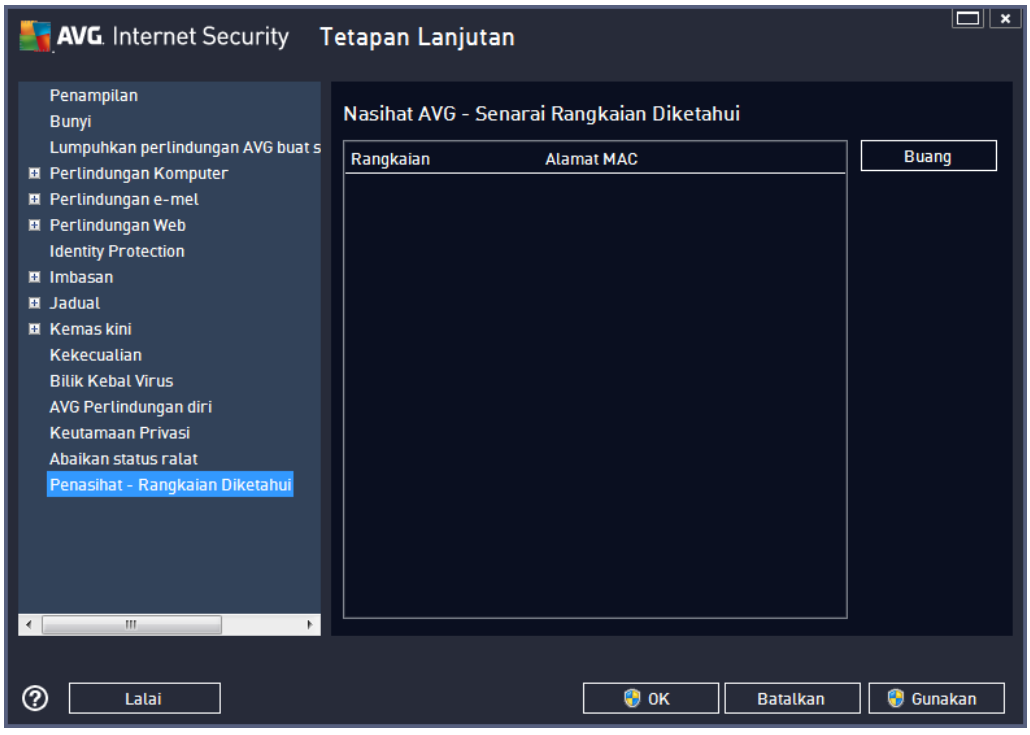
komponen dihidupkan secara kekal dan dalam konfigurasi lalai tetapi hal ini boleh berlaku. Dalam hal ini, ikon dulang sistem secara automatik melaporkan status ralat komponen. Walau bagaimanapun, dalam kes ini, kita tidak dapat bercakap mengenai ralat sebenar memandangkan anda telah mencetuskannya dengan 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 ***Abaikan status ralat*** anda boleh memilih komponen yang mungkin berada dalam keadaan ralat (*atau dimatikan*) dan anda tidak mahu menerima maklumat mengenainya. Tekan butang ***OK*** untuk mengesahkan.

9.16. 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 *(Melalui pautan yang diberikan dalam dulang pemberitahuan Penasihat AVG yang menggelangsar di atas dulang sistem sebaik sahaja rangkaian yang tidak diketahui dikesan. Untuk butiran sila lihat bab Penasihat AVG)*. Penasihat AVG kemudiannya akan mengingati atribut unik rangkaian tersebut *(khususnya alamat MAC)* dan tidak akan memaparkan pemberitahuan pada masa akan datang. Setiap rangkaian di mana anda disambungkan akan dianggap sebagai rangkaian diketahui secara automatik dan ditambahkan pada senarai. Anda boleh hapuskan masukan individu dengan menekan butang ***Keluarkan***; rangkaian yang berkenaan akan dianggap tidak diketahui dan berkemungkinan tidak selamat lagi.

Dalam tetingkap dialog ini, anda boleh menyemak rangkaian mana yang dianggap sebagai diketahui:



Nota: *Ciri rangkaian diketahui di dalam Penasihat AVG tidak disokong pada Windows XP 64 bit.*

10. Tetapan Firewall

Konfigurasi Firewall dibuka dalam tetingkap baharu di mana di dalam beberapa dialog anda boleh menyediakan parameter lanjutan untuk komponen. Konfigurasi Firewall dibuka dalam tetingkap baharu di mana anda boleh menyunting parameter lanjutan komponen dalam beberapa dialog konfigurasi. Konfigurasi boleh dipaparkan secara alternatif dalam sama ada mod asas atau pakar. Semasa anda mula-mula masuk ke dalam tetingkap konfigurasi, ia membuka versi asas yang memberikan penyuntingan bagi parameter berikut:

- Umum
- Aplikasi
- Perkongsian Fail dan Pencetak

Di bahagian bawah dialog anda akan menemui butang ***Mod pakar***. Tekan butang tersebut untuk memaparkan selanjutnya item dalam navigasi dialog untuk konfigurasi Firewall lanjutan:

- Tetapan lanjutan
- Rangkaian ditakrifkan
- Perkhidmatan sistem
- Log

Walau bagaimanapun, vendor perisian telah menyediakan semua komponen AVG Internet Security 2013 untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi lalai. Sebarang perubahan kepada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja!

10.1. Umum

Dialog ***Maklumat umum*** memberikan gambaran keseluruhan semua mod Firewall yang tersedia. Pilihan semasa bagi mod Firewall boleh ditukar dengan memilih mod lain daripada menu.

Walau bagaimanapun, vendor perisian telah menyediakan semua komponen AVG Internet Security 2013 untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi lalai. Sebarang perubahan kepada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja!

Firewall membenarkan anda mentakrifkan peraturan keselamatan tertentu berdasarkan pada sama ada komputer anda terletak pada domain, komputer kendiri mahupun mungkin komputer bimbit. Setiap opsyen ini memerlukan perlindungan tahap berbeza dan setiap tahap dilindungi oleh mod masing-masing. Secara ringkasnya, mod Firewall adalah konfigurasi khusus komponen Firewall dan anda boleh menggunakan sejumlah konfigurasi yang dipratakrifkan:

- ***Automatik*** – Dalam mod ini, Firewall mengendalikan semua trafik rangkaian secara automatik. Anda tidak akan dijemput untuk membuat sebarang keputusan. Firewall akan membenarkan sambungan untuk setiap aplikasi yang diketahui dan pada masa yang sama, satu peraturan akan dicipta untuk aplikasi yang menentukan bahawa aplikasi tersebut sentiasa boleh menyambung pada masa akan datang. Untuk aplikasi lain, Firewall akan memutuskan sama ada sambungan tersebut harus dibenarkan atau disekat berdasarkan pada kelakuan aplikasi. Namun, dalam situasi sedemikian, peraturan tidak akan dicipta dan aplikasi akan disemak semula semasa ia cuba untuk menyambung. ***Mod automatik ini agak tidak mengganggu dan disyorkan untuk kebanyakan pengguna.***

- ***Interaktif*** – mod ini berguna jika anda mahu mengawal sepenuhnya semua trafik rangkaian ke dan dari komputer anda. Firewall akan mengawasinya untuk anda dan memaklumkan kepada anda setiap percubaan untuk berkomunikasi atau memindahkan data, membolehkan anda membenarkan atau menyekat percubaan itu mengikut kemahuan anda. Disyorkan untuk pengguna lanjutan sahaja.

- ***Sekat akses ke Internet*** – Sambungan Internet disekat sepenuhnya, anda tidak boleh mengakses Internet dan tiada sesiapa pun dari luar boleh mengakses komputer anda. Untuk penggunaan khas dan masa yang singkat sahaja.

- ***Matikan perlindungan Firewall*** – melumpuhkan Firewall akan mendayakan semua trafik rangkaian ke dan dari komputer anda. Akibatnya, ini akan menjadikannya terdedah kepada serangan penggodam. Sila sentiasa pertimbangkan opsyen ini dengan berhati-hati.

Sila maklum bahawa terdapat mod automatik khusus yang juga tersedia dalam Firewall. Mod ini

diaktifkan secara senyap jika sama ada komponen Komputer atau Identity protection dimatikan dan komputer anda dengan itu, lebih mudah terdedah. Dalam hal sedemikian, Firewall akan hanya membenarkan secara automatik aplikasi yang diketahui dan benar-benar selamat. Untuk hal lain, ia akan meminta keputusan anda. Ini akan menggantikan komponen perlindungan yang dinyahaktifkan dan untuk memastikan komputer anda selamat.

10.2. Aplikasi

Dialog ***Aplikasi*** menyenaraikan semua aplikasi yang telah mencuba untuk berkomunikasi melalui rangkaian setakat ini 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
- – sekat komunikasi
- – tetapan lanjutan ditakrifkan

Sila maklum bahawa hanya aplikasi yang telah dipasang sahaja yang boleh dikesan. Secara lalai, apabila aplikasi baharu cuba menyambung melalui rangkaian untuk kali pertama, Firewall akan mencipta peraturan untuknya secara automatik mengikut pangkalan data yang dipercayai atau bertanyakan kepada anda sama ada anda ingin membenarkan atau menyekat komunikasi. Dalam kes kedua, 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. ***Peraturan Aplikasi Utama*** (*di*

bahagian atas senarai) adalah diutamakan dan sentiasa digunakan sebelum peraturan untuk 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 harus dicetuskan apabila aplikasi sedemikian mencuba untuk berkomunikasi melalui rangkaian: Sekat *(komunikasi akan sentiasa disekat)*, Benarkan *(komunikasi akan dibenarkan melalui sebarang rangkaian)*, Tanya *(anda akan dijemput untuk memutuskan sama ada komunikasi harus dibenarkan atau disekat)*. ***Item ini mempunyai opsyen tetapan berbeza daripada aplikasi biasa dan hanya ditujukan untuk pengguna berpengalaman. Kami amat mengesyorkan untuk anda mengubah suai tetapan!***

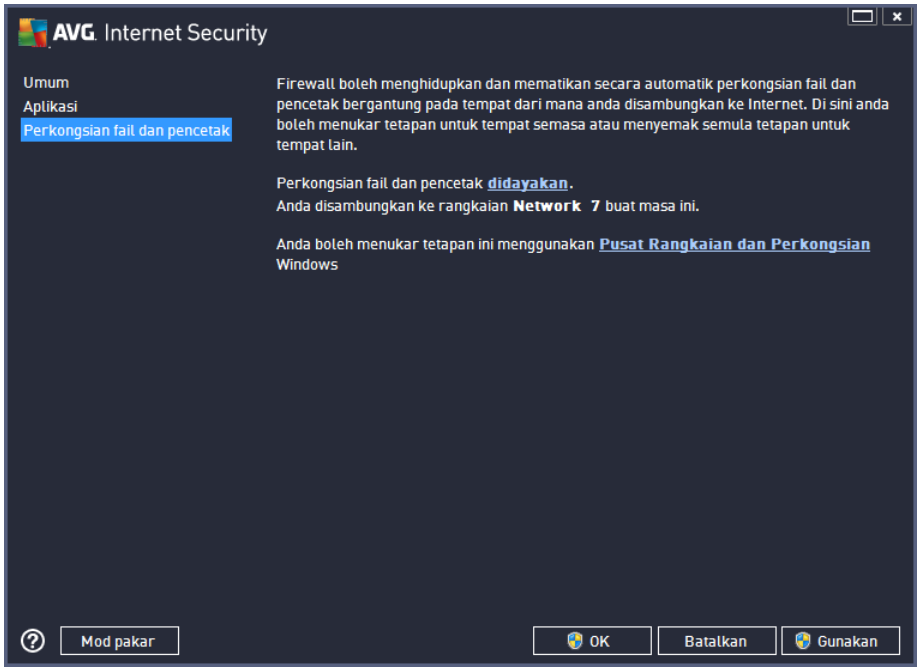
Butang kawalan

Senarai boleh diedit dengan menggunakan butang kawalan berikut:

- ***Tambah*** – membuka dialog kosong untuk mentakrifkan peraturan aplikasi baharu.
- ***Sunting*** – membuka dialog yang sama dengan data yang diberikan untuk menyunting set peraturan aplikasi sedia ada.
- ***Hapuskan*** – membuang aplikasi yang dipilih dari senarai.

10.3. Perkongsian fail dan pencetak

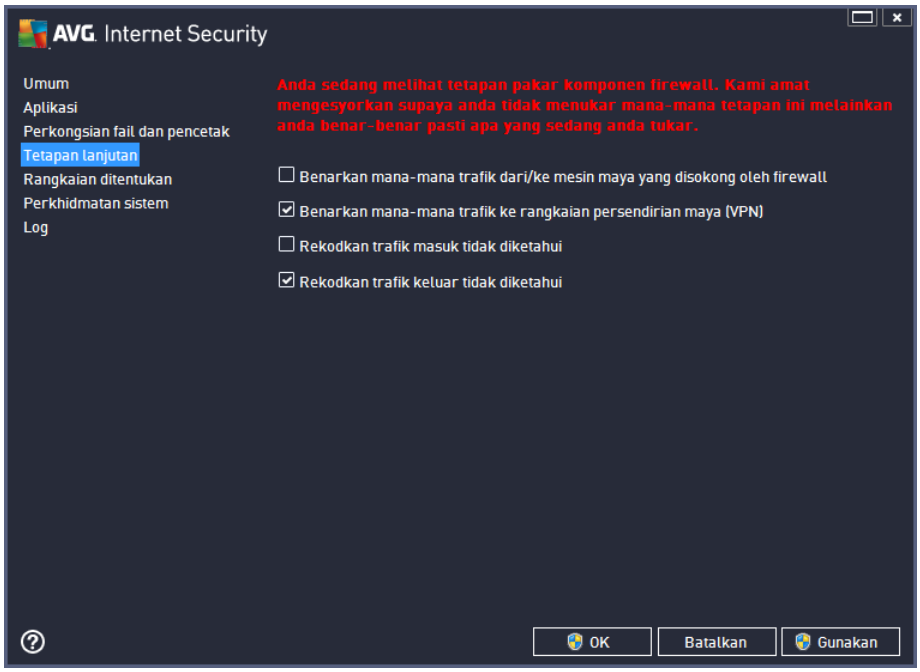
Perkongsian fail dan pencetak sebenarnya bermaksud berkongsi sebarang fail atau folder yang anda tandakan sebagai "Dikongsi" dalam Windows, unit cakera biasa, pencetak, pengimbas dan semua peranti yang serupa. Perkongsian item sedemikian hanya wajar dalam rangkaian yang boleh dianggap selamat *(contohnya di rumah, di tempat kerja atau di sekolah)*. Namun, jika anda disambungkan ke rangkaian awam *(seperti Wi-Fi lapangan terbang atau kafe Internet)*, anda mungkin tidak mahu berkongsi apa-apa. AVG Firewall boleh menyekat atau membenarkan perkongsian dengan mudah dan membolehkan anda menyimpan pilihan anda untuk rangkaian yang telah dilawati.



Dalam dialog ***Perkongsian Fail dan Pencetak*** anda boleh menyunting konfigurasi perkongsian fail dan pencetak serta rangkaian yang disambungkan buat masa ini. Dengan Window XP, nama rangkaian memberi respons kepada gelaran yang anda pilih untuk rangkaian tertentu semasa anda mula-mula disambungkan padanya. Dengan Windows Vista atau lebih tinggi, nama rangkaian diambil secara automatik daripada Network and Sharing Center.

10.4. Tetapan lanjutan

Sebarang penyuntingan di dalam dialog Tetapan lanjutan adalah untuk PENGGUNA BERPENGALAMAN SAHAJA!



Dialog ***Tetapan lanjutan*** membolehkan anda untuk memilih/tidak memilih parameter Firewall berikut:

- ***Membenarkan sebarang trafik dari/ke mesin maya yang disokong oleh firewall*** – sokongan untuk sambungan rangkaian dalam mesin maya seperti VMWare.
- ***Benarkan sebarang trafik ke rangkaian persendirian maya (VPN)*** – sokongan untuk sambungan VPN *(digunakan untuk menyambung kepada komputer jauh)*.
- ***Log trafik masuk/keluar yang tidak diketahui*** – semua percubaan komunikasi *(masuk/keluar)* oleh aplikasi yang tidak diketahui akan direkodkan dalam log Firewall.

10.5. Rangkaian ditentukan

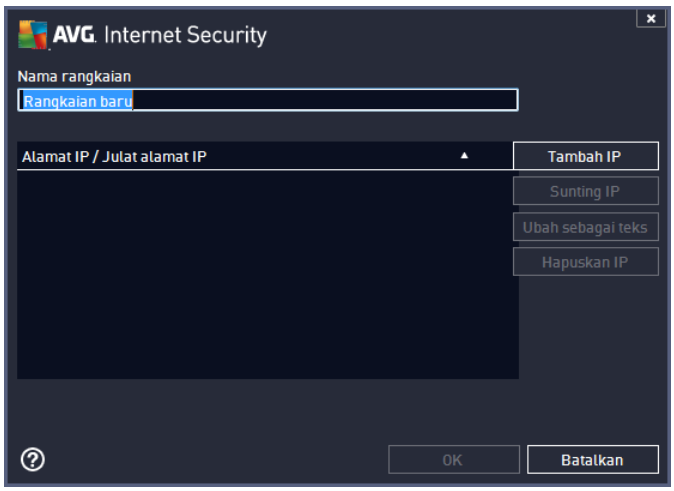
Sebarang penyuntingan di dalam dialog Rangkaian ditentukan adalah untuk PENGGUNA BERPENGALAMAN SAHAJA!

Dialog ***Rangkaian ditentukan*** menawarkan senarai semua rangkaian yang bersambung dengan komputer anda. Senarai tersebut memberikan maklumat berikut pada setiap rangkaian yang dikesan:

- ***Rangkaian*** – memberikan senarai nama semua rangkaian di mana komputer disambungkan kepadanya.
- ***Julat alamat IP*** – setiap rangkaian akan dikesan secara automatik dan ditentukan dalam bentuk julat alamat IP.

Butang kawalan

- ***Tambah rangkaian*** – membuka tetingkap dialog baharu di mana anda boleh menyunting parameter untuk rangkaian yang baru ditentukan, cth. untuk memberikan ***Nama rangkaian*** dan menentukan ***julat alamat IP***:

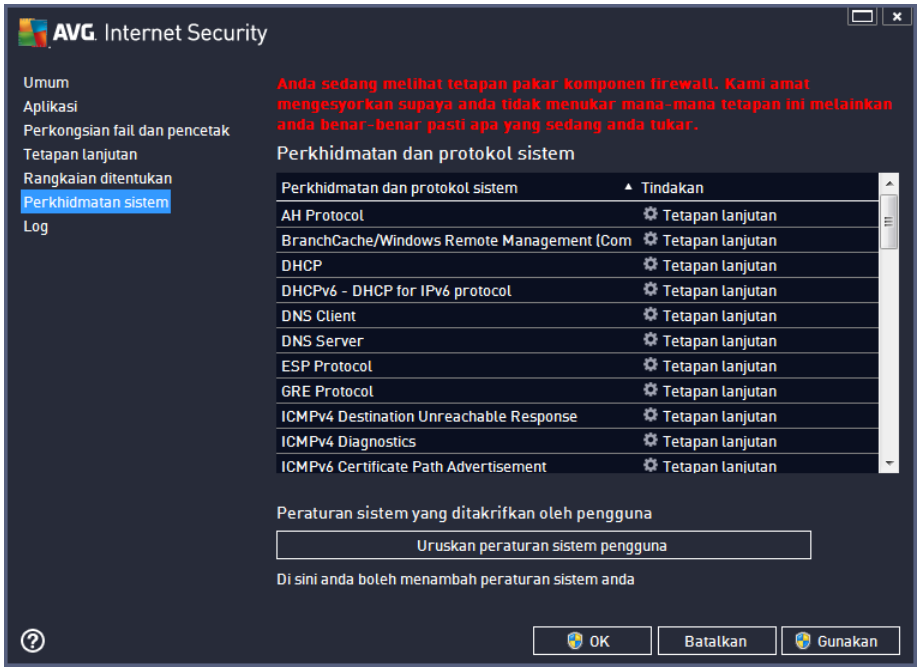


- ***Sunting rangkaian*** – membuka tetingkap dialog ***Sifat rangkaian*** (*lihat di atas*) di mana anda boleh menyunting parameter bagi rangkaian yang telah ditakrifkan (*dialog adalah sama dengan dialog untuk menambah rangkaian baharu, lihat penerangan dalam perenggan sebelumnya*).

- ***Hapuskan rangkaian*** – membuang rujukan kepada rangkaian yang dipilih daripada senarai rangkaian.

10.6. Perkhidmatan sistem

Sebarang penyuntingan dalam dialog perkhidmatan dan protokol sistem adalah ditujukan untuk PENGGUNA YANG BERPENGALAMAN SAHAJA!



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

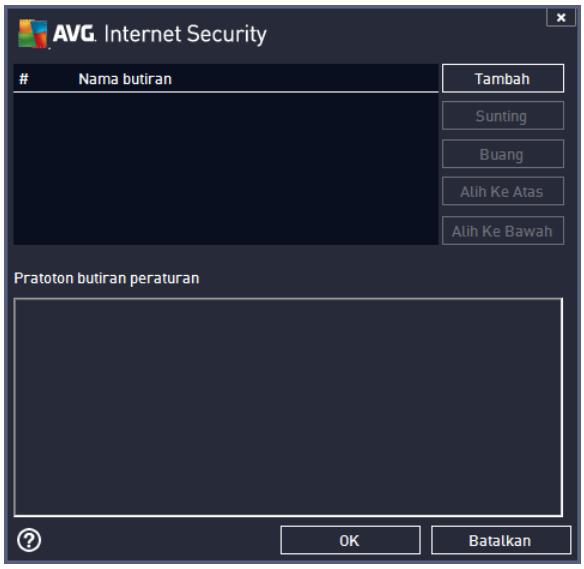
berikut:

- ***Perkhidmatan dan protokol sistem*** – Lajur ini menunjukkan nama perkhidmatan sistem berkenaan.
- ***Tindakan*** – Lajur ini memaparkan ikon untuk tindakan yang diperuntukkan:
  - o Benarkan komunikasi untuk semua rangkaian
  - o Sekat komunikasi

Untuk menyunting tetapan bagi sebarang item dalam senarai (*termasuk tindakan yang diperuntukkan*), klik kanan item dan pilih ***Sunting***. ***Walau bagaimanapun, penyuntingan peraturan sistem harus dilakukan oleh pengguna lanjutan sahaja dan adalah amat disyorkan supaya anda tidak menyunting peraturan sistem!***

Peraturan sistem yang ditakrifkan oleh pengguna

Untuk membuka dialog baharu untuk menentukan peraturan perkhidmatan sistem anda sendiri (*lihat gambar di bawah*), tekan butang ***Uruskan peraturan sistem pengguna***. Dialog yang sama dibuka jika anda memutuskan untuk menyunting konfigurasi sebarang item sedia ada di dalam senarai perkhidmatan dan protokol sistem. Bahagian atas dialog ini memaparkan gambaran keseluruhan bagi semua butiran peraturan sistem yang disunting buat masa ini, bahagian bawah kemudiannya memaparkan butiran yang dipilih. Butiran peraturan boleh disunting, ditambah atau dihapuskan melalui butang masing-masing:



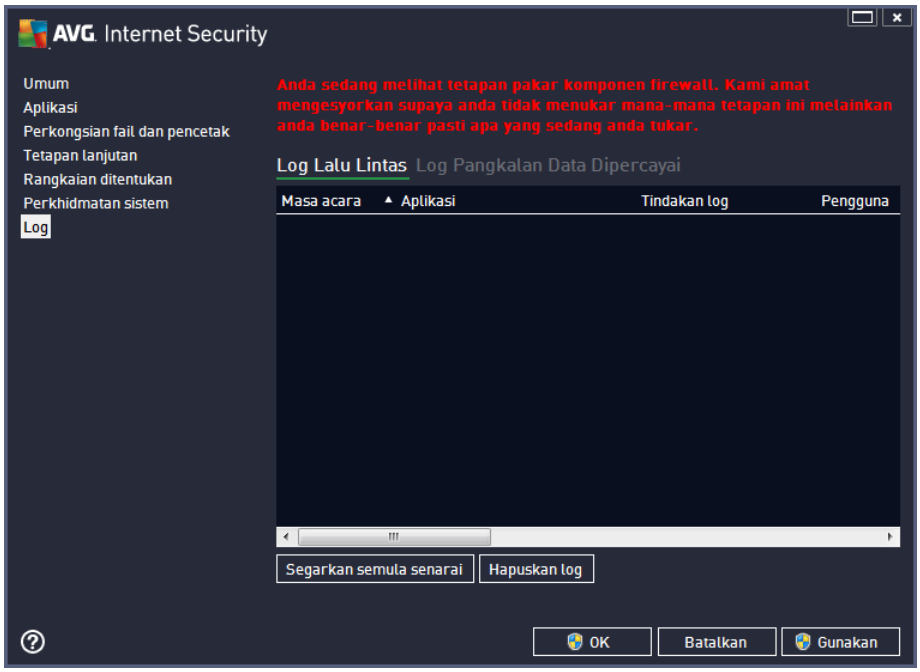
Sila ingat bahawa tetapan peraturan terperinci adalah lanjutan dan khusus ditujukan untuk pentadbir rangkaian yang memerlukan kawalan penuh ke atas konfigurasi Firewall. Jika anda tidak biasa dengan jenis protokol komunikasi, nombor port rangkaian, definisi alamat IP dll., harap jangan ubah suai tetapan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

10.7. Log

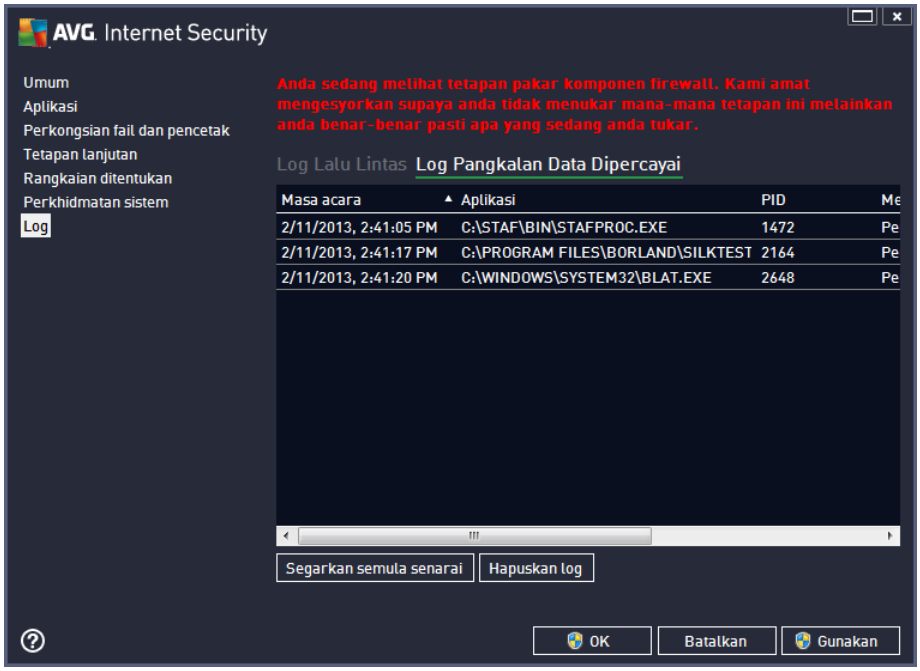
Sebarang penyuntingan di dalam dialog Log adalah untuk PENGGUNA BERPENGALAMAN SAHAJA!

Dialog ***Log*** membenarkan anda menyemak semula senarai semua tindakan dan acara Firewall yang dilog dengan penerangan terperinci bagi parameter berkaitan yang dipaparkan pada dua tab:

- ***Log Trafik*** – Tab ini menawarkan maklumat mengenai aktiviti oleh semua aplikasi yang telah cuba menyambung ke rangkaian. Untuk setiap item, anda akan menemui maklumat mengenai masa acara, nama aplikasi, tindakan log yang berkenaan, nama pengguna, PID, arak trafik, jenis protokol, bilangan port jauh dan setempat serta maklumat mengenai alamat IP setempat dan jauh.



- ***Log Pangkalan Data Dipercayai*** – *Pangkalan data dipercayai* adalah pangkalan data dalaman AVG untuk mengumpul maklumat 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 peraturan firewall yang ditentukan untuk aplikasi ini lagi*), adalah perlu untuk mengetahui sama ada komunikasi rangkaian harus dibenarkan untuk aplikasi berkenaan. Pertama sekali, AVG mencari *Pangkalan data yang dipercayai*dan jika aplikasi disenaraikan, ia akan diberikan akses kepada rangkaian secara automatik. Hanya selepas itu, dengan syarat tiada maklumat mengenai aplikasi yang tersedia dalam pangkalan, anda akan ditanya dalam dialog kendiri sama ada anda ingin membenarkan aplikasi mengakses rangkaian.



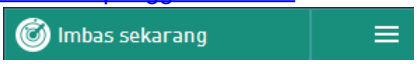
Butang kawalan

- ***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 baru dipaparkan.

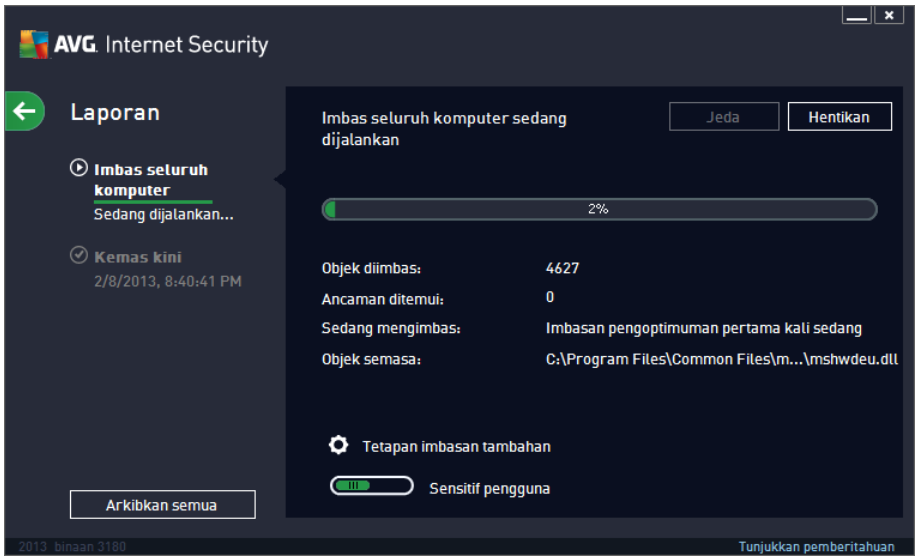
- ***Hapuskan log*** – tekan untuk hapuskan semua entri dalam carta.

11. Pengimbasan AVG

Secara lalai, **AVG Internet Security 2013** tidak menjalankan sebarang imbasan, seperti selepas imbasan awal *(di mana anda dijemput untuk melancarkan*), anda seharusnya dilindungi dengan sempurna oleh komponen residen **AVG Internet Security 2013** yang sentiasa mengawal dan tidak membenarkan sebarang kod berniat jahat memasuki komputer anda. Sudah tentu, anda boleh menjadualkan imbasan untuk dijalankan pada selang masa tetap, atau secara manual, melancarkan imbasan mengikut keperluan anda pada bila-bila masa.

Antara muka pengimbasan AVG boleh diakses dari antara muka pengguna utama melalui butang yang dibahagikan secara grafik ke dalam dua bahagian: 

- ***Imbas sekarang*** – Tekan butang tersebut untuk memaut ke lancarkan Imbas Seluruh Komputer dengan serta-merta dan melihat kemajuan dan keputusannya dalam tetingkap Laporan yang dibuka secara automatik:



- ***Opsyen*** – Pilih butang ini *(dipaparkan secara grafik sebagai tiga garis mendatar dalam medan hijau)* untuk membuka dialog ***Opsyen Imbasan*** di mana anda boleh menguruskan imbasan berjadual dan menyunting parameter Imbas Seluruh Komputer / Imbas Fail atau Folder Tertentu:

Dalam ***Opsyen Imbasan***, anda boleh melihat tiga bahagian konfigurasi imbasan utama:

- ***Uruskan imbasan berjadual*** – Klik opsyen ini untuk membuka dialog baharu dengan gambaran keseluruhan semua jadual imbasan. Sebelum anda mentakrifkan imbasan anda sendiri, anda hanya akan dapat melihat satu imbasan berjadual yang dipratakrifkan oleh vendor perisian yang disenaraikan dalam carta. Imbasan dimatikan secara lalai. Untuk menghidupkannya, klik kanan padanya dan pilih opsyen *Dayakan tugasan* dari menu konteks. Setelah imbasan berjadual didayakan, anda boleh menyunting konfigurasinya melalui butang *Sunting jadual imbasan*. Anda juga boleh mengklik butang *Tambah jadual imbasan* untuk mencipta jadual imbasan baharu anda sendiri.

- ***Imbas seluruh komputer / Tetapan*** – Butang ini dibahagikan kepada dua bahagian. Klik opsyen *Imbas seluruh komputer* untuk melancarkan serta-merta pengimbasan keseluruhan komputer anda *(untuk butiran mengenai imbasan seluruh komputer, sila lihat bab berkenaan yang dipanggil Imbasan pratakrif / Imbas seluruh komputer)*. Mengklik bahagian *Tetapan* di bawah akan membawa anda ke dialog konfigurasi bagi imbas seluruh komputer.

- ***Imbas fail atau folder tertentu / Tetapan*** – Sekali lagi, butang ini dibahagikan kepada dua bahagian. Klik opsyen *Imbas fail atau folder tertentu* untuk melancarkan dengan serta-merta pengimbasan kawasan tertentu komputer anda *(untuk butiran mengenai imbasan fail atau folder terpilih, sila lihat bab berkenaan yang dipanggil Imbasan pratakrif / Imbas fail atau folder tertentu)*. Mengklik bahagian *Tetapan* di bawah akan membawa anda ke dialog konfigurasi bagi imbasan fail atau folder tertentu.

11.1. Imbasan Pratakrif

Salah satu ciri utama bagi **AVG Internet Security 2013** adalah pengimbasan dalam permintaan. Ujian dengan permintaan direka bentuk untuk mengimbas pelbagai bahagian komputer anda apabila terdapat kecurigaan bagi kemungkinan jangkitan virus. Bagaimanapun, adalah amat disyorkan supaya anda menjalankan ujian sedemikian secara tetap walaupun jika anda merasakan tiada virus yang boleh ditemui pada komputer anda.

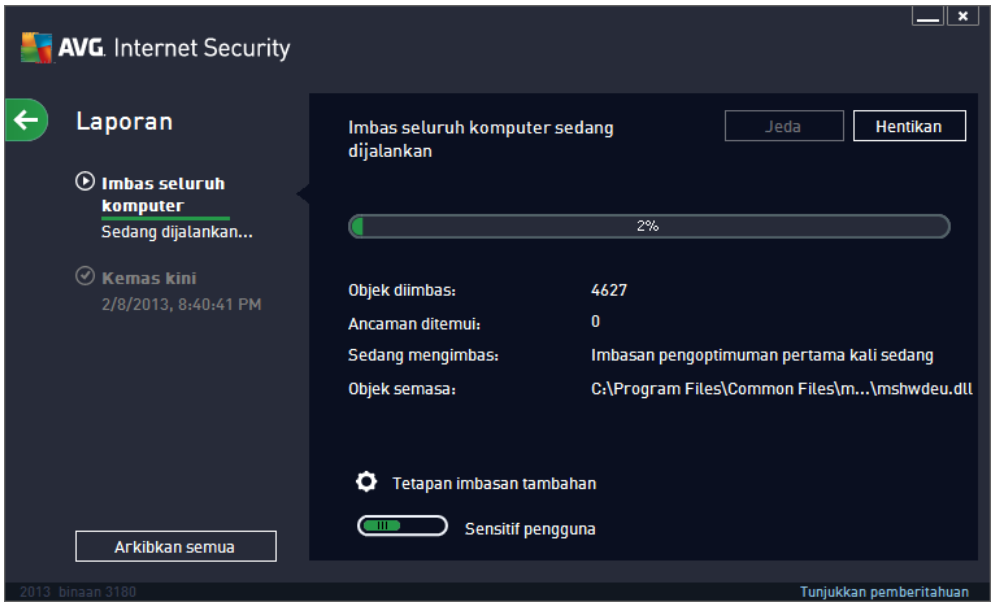
Dalam **AVG Internet Security 2013** anda akan menemui jenis pengimbasan berikut yang dipratetapkan oleh vendor perisian:

11.1.1. Imbas seluruh komputer

Imbas seluruh komputer mengimbas seluruh komputer anda untuk kemungkinan jangkitan dan/ atau atur cara yang berpotensi tidak diingini. Ujian ini akan mengimbas semua pemacu keras pada 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 komputer anda sekurang-kurangnya sekali seminggu.

Lancarkan imbasan

Imbas seluruh komputer boleh dilancarkan secara terus daripada antara muka pengguna utama dengan mengklik butang ***Imbas sekarang***. Tiada tetapan khusus lanjut perlu dikonfigurasikan untuk jenis imbasan ini; imbasan akan bermula dengan serta-merta. Dalam dialog ***Imbas seluruh komputer dalam kemajuan*** (*lihat tangkapan skrin*) anda boleh melihat kemajuan dan keputusannya. Imbasan boleh diganggu buat sementara waktu (***Jeda***) atau dibatalkan (***Berhenti***) jika perlu.



Penyuntingan konfigurasi imbasan

Anda boleh menyunting konfigurasi ***Imbas seluruh komputer*** dalam dialog ***Imbas seluruh komputer – Tetapan*** *(dialog boleh diakses melalui pautan Tetapan untuk Imbas seluruh komputer dalam dialog Opsyen imbasan).* ***Adalah disyorkan supaya anda mengekalkan tetapan lalai melainkan anda mempunyai alasan kukuh untuk menukarnya!***

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 Atur Cara Yang Berpotensi Tidak Diingini dan ancaman Spyware*** *(dihidupkan secara lalai)* – Tandakan untuk mengaktifkan imbasan spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- ***Laporkan tetapan dipertingkatkan bagi Atur Cara Yang Berpotensi Tidak Diingini*** *(dimatikan secara lalai)* – tandakan untuk mengesan pakej spyware lanjutan: 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 Kuki Penjejakan*** *(dimatikan secara lalai)* – Parameter ini menentukan supaya kuki harus dikesan; *(kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka)*.

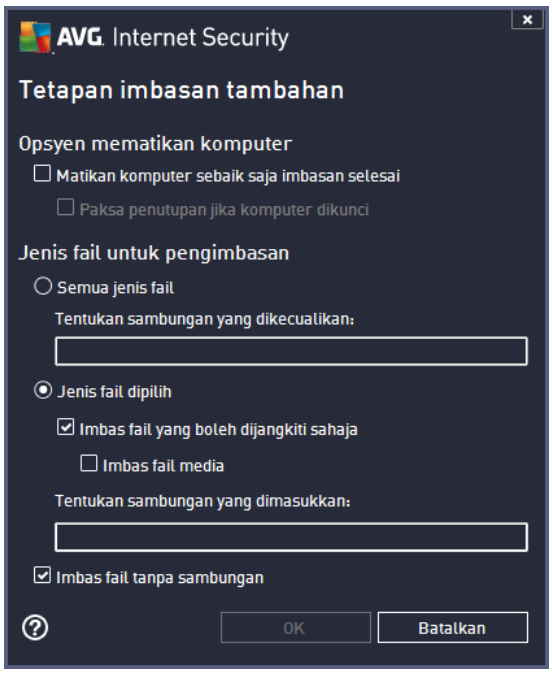
- ***Imbas di dalam arkib*** *(dimatikan secara lalai)* – Parameter ini menentukan bahawa imbasan harus menyemak semua fail yang disimpan di dalam arkib, cth. ZIP, RAR, ...

- ***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*** *(dihidupkan secara lalai)* – Imbasan juga akan menyemak kawasan sistem komputer anda.

- ***Dayakan pengimbasan teliti*** *(dimatikan secara lalai)* – Dalam situasi khusus *(kecurigaan tentang komputer anda dijangkiti)* anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang jarang dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.

- ***Tetapan imbasan tambahan*** – pautan membuka dialog Tetapan imbasan tambahan baharu 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*** – anda juga harus memutuskan sama ada anda hendak mengimbas:

    - ***Semua jenis fail*** dengan opsyen menentukan pengecualian daripada pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan koma yang tidak seharusnya diimbas;

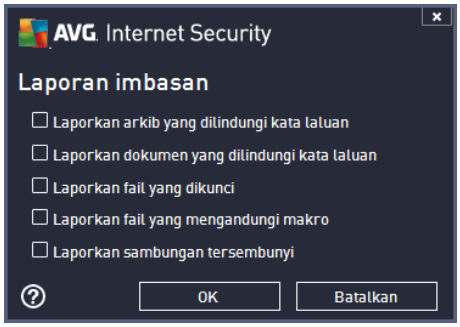
    - ***Jenis fail dipilih*** – anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang boleh dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya fail teks biasa atau fail tidak boleh laku yang lain*), termasuk fail media (*fail video, audio – jika anda membiarkan kotak ini tidak ditandakan, ia akan mengurangkan lebih banyak masa imbasan kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali

lagi, anda boleh menentukan melalui sambungan fail mana yang seharusnya sentiasa diimbas.

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

- ***Laraskan berapa cepat imbasan selesai*** – anda boleh menggunakan gelangsar untuk menukar keutamaan proses pengimbasan. Secara lalainya, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud beban sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama masa diambil untuk mengimbas*) atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).

- ***Tetapkan laporan imbasan tambahan*** – pautan membuka dialog ***Laporan imbasan*** baharu di mana anda boleh memilih jenis kemungkinan penemuan yang harus dilaporkan:



Amaran: *Tetapan imbasan ini adalah sama dengan parameter untuk imbasan yang baru ditakrifkan – seperti yang diterangkan dalam bab Pengimbasan AVG / Penjadualan imbasan / Cara untuk Mengimbas. Sekiranya anda memutuskan untuk menukar konfigurasi lalai* ***Imbas seluruh komputer****, anda kemudiannya boleh menyimpan tetapan baharu anda sebagai konfigurasi lalai untuk digunakan bagi semua imbasan selanjutnya untuk seluruh komputer.*

11.1.2. Imbas fail atau folder khusus

Imbas fail atau folder khusus – 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 seperti semasa mengimbas 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 terus daripada dialog Opsyen imbasan dengan mengklik pada butang **Imbas fail atau folder tertentu**. Dialog baharu yang dipanggil ***Pilih fail atau folder tertentu 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 semak di bahagian atas dialog ini. Terdapat juga opsyen untuk mengimbas folder tertentu sementara semua subfoldernya dikecualikan daripada dalam imbasan ini, untuk melakukannya, tuliskan tanda tolak "**-**" di hadapan laluan yang dijana secara automatik (*lihat gambar skrin*). Untuk tidak memasukkan keseluruhan folder dari imbasan, gunakan parameter "**!**". Akhir sekali, untuk melancarkan imbasan, tekan butang ***Mulakan imbasan***; proses pengimbasan itu sendiri adalah secara asasnya sama dengan Imbas Seluruh komputer.

Penyuntingan konfigurasi imbasan

Anda boleh menyunting konfigurasi ***Imbas fail atau folder tertentu*** dalam dialog ***Imbas fail atau folder tertentu – Tetapan*** *(dialog boleh diakses melalui pautan Tetapan untuk Imbas fail atau folder tertentu dalam dialog Opsyen imbasan).* ***Adalah disyorkan supaya anda mengekalkan tetapan lalai melainkan anda mempunyai alasan kukuh untuk menukarnya!***

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 semasa 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 Atur Cara Yang berpotensi Tidak Diingini dan ancaman Spyware*** *(dihidupkan secara lalai)*: Tandakan untuk mengaktifkan imbasan spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.

- ***Laporkan tetapan dipertingkatkan Atur Cara Yang Berpotensi Tidak Diingini*** *(dimatikan secara lalai)*: Tandakan untuk mengesan pakej lanjutan spyware: 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 Kuki Penjejakan*** *(dimatikan secara lalai)*: Parameter ini menentukan bahawa kuki harus dikesan; *(kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka)*.

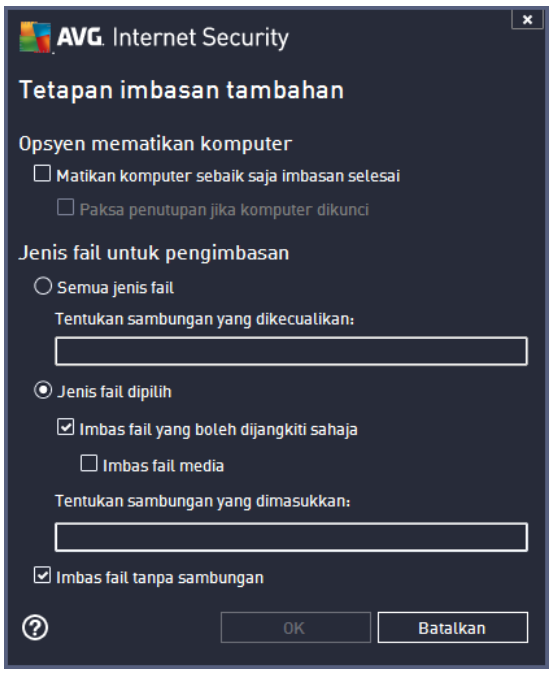
- ***Imbas di dalam arkib*** *(dihidupkan secara lalai)*: Parameter ini menentukan bahawa imbasan harus menyemak semua fail yang disimpan dalam arkib, cth. ZIP, RAR, ...

- ***Gunakan Heuristik*** *(dihidupkan secara lalai)*: Analisis heuristik *(pelagakan dinamik arahan objek yang dikesan dalam persekitaran komputer maya)* akan menjadi salah satu daripada kaedah yang digunakan untuk pengesanan virus semasa imbasan.

- ***Imbas persekitaran sistem*** *(dimatikan secara lalai)*: Pengimbasan juga akan menyemak kawasan sistem komputer anda.

- ***Dayakan pengimbasan teliti*** *(dimatikan secara lalai)*: Dalam situasi khusus *(kecurigaan tentang komputer anda dijangkiti)* anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang jarang dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.

- ***Tetapan imbasan tambahan*** – Pautan membuka dialog ***Tetapan imbasan tambahan*** baharu 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*** – anda juga harus memutuskan sama ada anda hendak mengimbas:

  - ***Semua jenis fail*** dengan opsyen menentukan pengecualian daripada pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan koma yang tidak seharusnya diimbas;

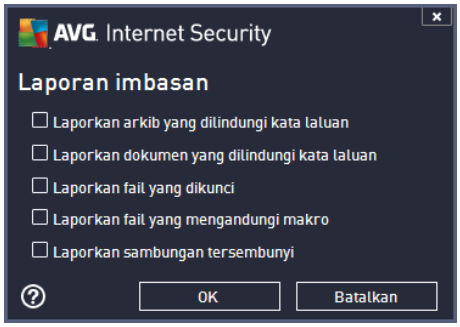
  - ***Jenis fail dipilih*** – anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang boleh dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya fail teks biasa atau fail tidak boleh laku yang lain*), termasuk fail media (*fail video, audio – jika anda membiarkan kotak ini tidak ditandakan, ia akan mengurangkan lebih banyak masa imbasan kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan melalui sambungan fail mana yang seharusnya sentiasa diimbas.

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

- ***Laraskan berapa cepat imbasan selesai*** – anda boleh menggunakan gelangsar untuk menukar keutamaan proses pengimbasan. Secara lalainya, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Secara alternatif,

anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud beban 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*).

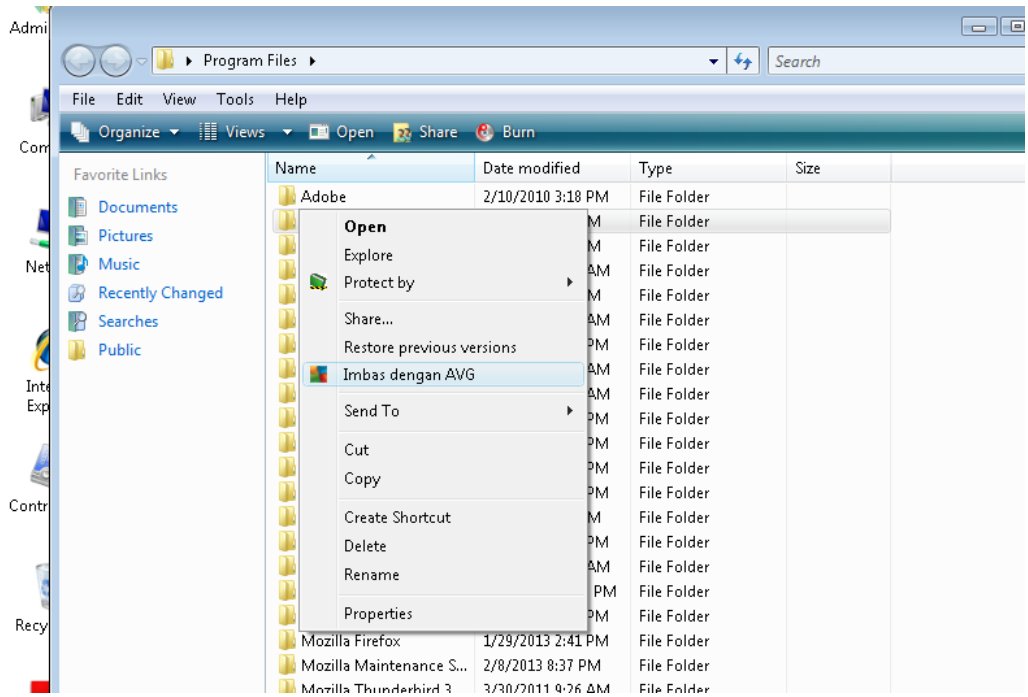
- ***Tetapkan laporan imbasan tambahan*** – pautan membuka dialog ***Laporan Imbasan*** baharu di mana anda boleh memilih jenis kemungkinan penemuan yang harus dilaporkan:



Amaran: *Tetapan imbasan ini adalah sama dengan parameter untuk 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 khusus*** *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 dijadualkan (semua imbasan yang dijadualkan adalah berdasarkan pada konfigurasi semasa Imbasan fail atau folder yang dipilih).*

11.2. Pengimbasan dalam Windows Explorer

Selain daripada imbasan dipratakrif yang dilancarkan untuk seluruh komputer atau kawasannya yang dipilih, **AVG Internet Security 2013** 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 2013**

11.3. Pengimbasan Garis Perintah

Dalam **AVG Internet Security 2013** 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 perintah, anda boleh melancarkan imbasan dengan kebanyakan parameter seperti yang ditawarkan dalam antara muka pengguna grafik AVG.

Untuk melancarkan imbasan AVG daripada baris perintah, 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 berbilang parameter, ini harus dibariskan dalam barisan dan dipisahkan dengan ruang dan aksara garis condong

- jika parameter memerlukan nilai khusus yang diberikan (cth. parameter ***/scan*** yang memerlukan maklumat mengenai kawasan terpilih komputer anda yang akan diimbas dan anda perlu memberikan laluan sebenar ke bahagian yang dipilih), nilai dipisahkan oleh 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 mengimbas anda boleh menghentikan proses menggunakan ***Ctrl+C*** atau ***Ctrl+Pause***.

Pengimbasan CMD dilancarkan daripada antara muka grafik

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

Memandangkan dialog ini hanya boleh diakses dalam Windows Safe Mode, untuk penerangan terperinci bagi dialog ini, sila rujuk fail bantuan yang boleh dibuka terus daripada dialog.

11.3.1. Parameter Imbasan CMD

Berikut terdapat senarai semua parameter yang tersedia untuk pengimbasan baris perintah:

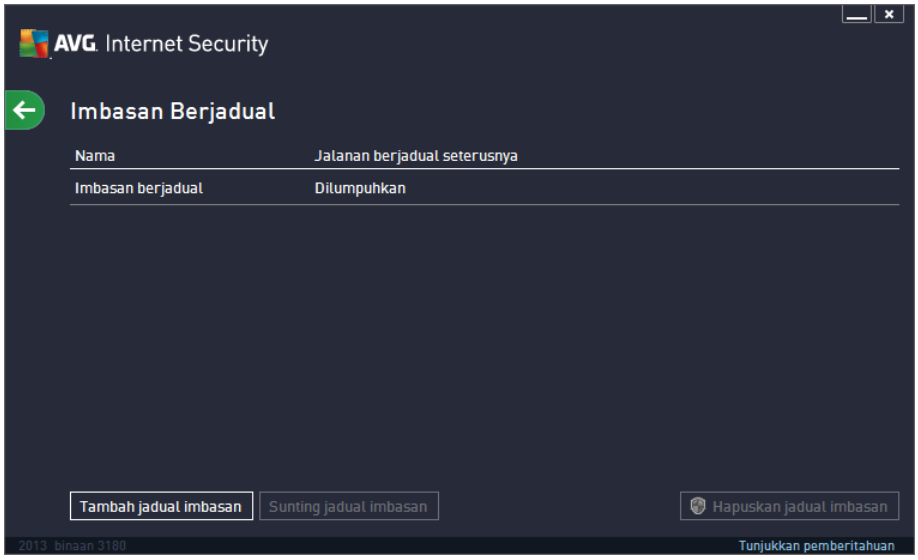
- /SCAN Imbas fail atau folder tertentu /SCAN=laluan;laluan *(cth. /SCAN=C:\;D:\)*
- /COMP Imbasan Seluruh Komputer
- /HEUR Gunakan analisis heuristik
- /EXCLUDE Kecualikan laluan atau fail daripada imbasan
- /@ Fail perintah /nama fail/
- /EXT Imbas sambungan ini /contohnya EXT=EXE,DLL/
- /NOEXT Jangan imbas sambungan ini /contohnya NOEXT=JPG/
- /ARC Imbas arkib
- /CLEAN Bersihkan 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 kata laluan
- /ARCBOMBSW Laporkan bom arkib *(memampatkan arkib berulang kali)*
- /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 untuk menghenti paksa
- /BOOT Dayakan semakan MBR/BOOT
- /PROC Imbas proses aktif
- /PUP Laporkan Atur cara yang berpotensi tidak diingini
- /PUPEXT Laporkan tetapan dipertingkatkan Atur cara yang berpotensi tidak diingini
- /REG Imbas daftaran
- /COO Imbas kuki
- /? Memaparkan bantuan pada topik ini
- /HELP Paparkan bantuan mengenai topik ini
- /PRIORITY Tetapkan keutamaan imbasan /Rendah, Auto, Tinggi/ *(lihat Tetapan lanjutan / Imbasan)*
- /SHUTDOWN Menutup komputer apabila imbasan selesai
- /FORCESHUTDOWN Paksa penutupan komputer apabila imbasan selesai
- /ADS Imbas Aliran Data Gantian *(NTFS sahaja)*
- /HIDDEN Laporkan fail dengan sambungan tersembunyi
- /INFECTABLEONLY Imbas fail dengan sambungan yang boleh dijangkiti sahaja
- /THOROUGHSCAN Dayakan pengimbasan teliti
- /CLOUDCHECK Semak positif palsu
- /ARCBOMBSW Laporkan fail arkib yang dimampatkan semula

11.4. Penjadualan Imbasan

Dengan **AVG Internet Security 2013** anda boleh menjalankan imbasan dengan permintaan *(contohnya, apabila anda mengesyaki jangkitan telah menembusi komputer anda)* atau berasaskan perancangan berjadual. Adalah amat disyorkan supaya anda menjalankan imbasan berasaskan jadual: dengan cara ini anda boleh memastikan komputer anda dilindungi daripada sebarang kemungkinan dijangkiti dan anda tidak perlu bimbang mengenai jika dan bila hendak melancarkan imbasan. Anda harus melancarkan Imbas 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.

Jadual imbasan boleh dicipta / disunting dalam dialog ***Imbasan berjadual*** yang boleh diakses melalui butang ***Uruskan imbasan berjadual*** di dalam dialog Opsyen imbasan. Dalam dialog ***Imbasan Berjadual*** baharu anda boleh melihat gambaran keseluruhan lengkap bagi semua imbasan berjadual buat masa ini:



Sebelum anda mentakrifkan imbasan anda sendiri, anda hanya akan dapat melihat satu imbasan berjadual yang dipratakrifkan oleh vendor perisian yang disenaraikan dalam carta. Imbasan dimatikan secara lalai. Untuk menghidupkannya, klik kanan padanya dan pilih opsyen ***Dayakan tugasan*** dari menu konteks. Setelah imbasan berjadual didayakan, anda boleh menyunting konfigurasinya melalui butang ***Sunting jadual imbasan***. Anda juga boleh mengklik butang ***Tambah jadual imbasan*** untuk mencipta jadual imbasan baharu anda sendiri. Parameter imbasan berjadual boleh disunting (*atau persediaan jadual baharu*) pada tiga tab:

- Jadual
- Tetapan
- Lokasi

Pada setiap tab anda boleh menukar butang "lampu isyarat" untuk menyahaktifkan ujian

berjadual buat sementara waktu dan menghidupkannya semula apabila perlu:

11.4.1. Jadual

Dalam bahagian atas tab ***Jadual*** anda boleh menemui medan teks di mana anda boleh menentukan nama jadual imbasan yang ditakrifkan buat masa ini. Cuba sentiasa gunakan nama yang ringkas, deskriptif dan sesuai untuk imbasan bagi menjadikannya lebih mudah untuk dibezakan daripada imbasan lain kemudiannya. Contohnya, adalah tidak sesuai untuk menamakan imbasan itu "Imbasan baharu" atau "Imbasan saya" memandangkan nama-nama ini tidak merujuk kepada apa yang sebenarnya disemak oleh imbasan itu. Sebaliknya, contoh nama deskriptif yang baik adalah "Imbasan kawasan sistem" dsb.

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 yang baru dijadualkan. Masa boleh 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 mungkin dengan mentakrifkan acara yang harus dikaitkan dengan pelancaran imbasan *(Jalankan pada permulaan komputer)*.

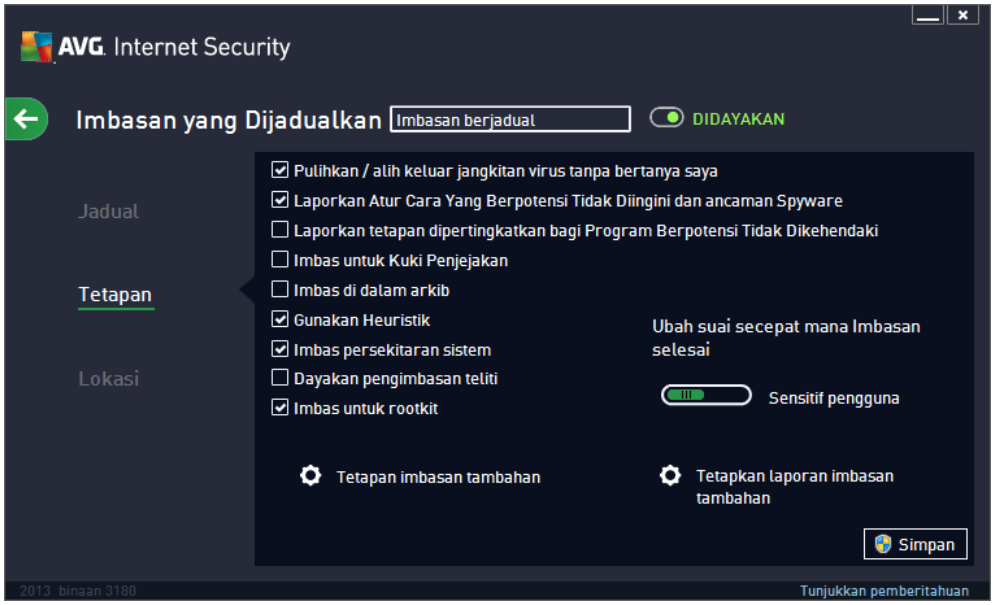
- ***Opsyen jadual lanjutan*** – Bahagian ini membenarkan anda menentukan di bawah syarat mana imbasan harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya. Apabila imbasan berjadual dilancarkan pada masa yang anda tentukan, anda akan diberitahu mengenai perkara ini melalui tetingkap timbul pada ikon dulang sistem AVG. Ikon dulang sistem AVG baharu kemudiannya muncul (dalam warna penuh dengan lampu suluh) memberitahu imbasan berjadual sedang berjalan. Klik kanan pada ikon menjalankan imbasan AVG untuk membuka menu konteks di mana anda boleh membuat keputusan untuk menjeda atau menghentikan imbasan yang sedang berjalan dan juga menukar prioriti imbasan yang sedang berjalan.

Kawalan dalam dialog

- ***Simpan*** – Menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain pada dialog ini dan menukar kembali ke gambaran keseluruhan Imbasan berjadual. Oleh itu, jika anda ingin mengkonfigurasikan parameter ujian pada semua tab, tekan butang untuk menyimpannya hanya selepas anda telah menentukan semua keperluan anda.

- – Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke gambaran keseluruhan Imbasan berjadual.

11.4.2. Tetapan



Dalam bahagian atas tab ***Tetapan*** anda boleh menemui medan teks di mana anda boleh menentukan nama jadual imbasan yang ditakrifkan buat masa ini. Cuba sentiasa gunakan nama yang ringkas, deskriptif dan sesuai untuk imbasan bagi menjadikannya lebih mudah untuk dibezakan daripada imbasan lain kemudiannya. Contohnya, adalah tidak sesuai untuk menamakan imbasan itu "Imbasan baharu" atau "Imbasan saya" memandangkan nama-nama ini tidak merujuk kepada apa yang sebenarnya disemak oleh imbasan itu. Sebaliknya, contoh nama deskriptif yang baik adalah "Imbasan kawasan sistem" dsb.

Pada tab ***Tetapan*** anda akan menemui senarai parameter pengimbasan yang boleh dihidupkan/ dimatikan secara pilihan. ***Melainkan anda mempunyai alasan yang sah untuk menukar tetapan ini, kami mengesyorkan supaya anda mengekalkan konfigurasi yang dipratakrifkan 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 Atur Cara Yang berpotensi Tidak Diingini dan ancaman Spyware*** *(dihidupkan secara lalai):* tandakan untuk mengaktifkan imbasan spyware serta virus. Spyware mewakili kategori malware yang dipersoalkan, walaupun ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat. Kami mengesyorkan supaya anda membiarkan ciri ini diaktifkan kerana ia meningkatkan

keselamatan komputer anda.

- ***Laporkan tetapan dipertingkatkan Atur Cara Yang Berpotensi Tidak Diingini*** (*dimatikan secara lalai*): tandakan untuk mengesan pakej lanjutan spyware: 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 Kuki Penjejakan*** (*dimatikan secara lalai*): parameter ini menentukan bahawa kuki harus dikesan semasa mengimbas; (*Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*)

- ***Imbas di dalam arkib*** (*dimatikan secara lalai*): parameter ini menentukan bahawa pengimbasan harus menyemak semua fail walaupun jika ia disimpan di 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;

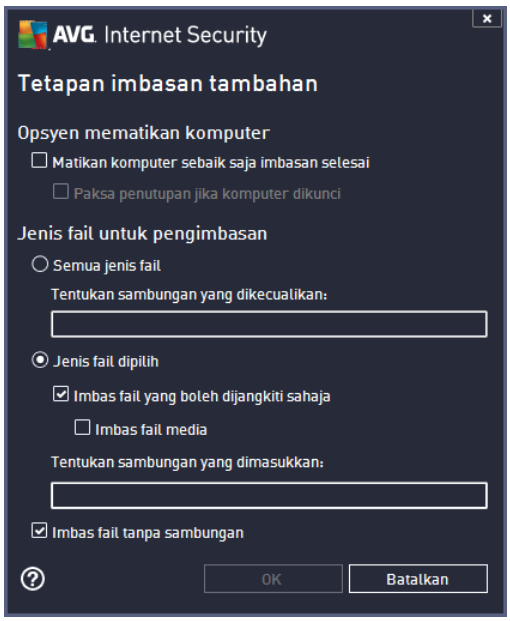
- ***Imbas persekitaran sistem*** (*dibuka secara lalai*): imbasan juga akan memeriksa kawasan sistem komputer anda;

- ***Dayakan pengimbasan teliti*** (*dimatikan secara lalai):* dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsyen 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 Anti-Rootkit mencari kemungkinan terdapatnya rootkit di dalam komputer anda, cth. atur cara 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*** baharu di mana anda boleh menentukan parameter berikut:



- ***Opsyen mematikan komputer*** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan yang sedang berjalan selesai. Dengan mengesahkan opsyen ini *(Matikan komputer sebaik sahaja imbasan selesai)*, pengaktifan opsyen baharu yang membenarkan komputer ditutup walaupun jika ia sedang dikunci *(Paksa penutupan jika komputer dikunci)*.

- ***Jenis fail untuk pengimbasan*** – anda juga harus memutuskan sama ada anda hendak mengimbas:

    - ***Semua jenis fail*** dengan opsyen menentukan pengecualian daripada pengimbasan dengan memberikan senarai sambungan fail yang dipisahkan koma yang tidak seharusnya diimbas;

    - ***Jenis fail dipilih*** – anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang boleh dijangkiti *(fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya fail teks biasa atau fail tidak boleh laku yang lain)*, termasuk fail media *(fail video, audio – jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa imbasan kerana fail ini biasanya agak besar dan kurang berkemungkinan dijangkiti virus)*. Sekali lagi, anda boleh menentukan melalui sambungan fail mana yang seharusnya sentiasa diimbas.

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

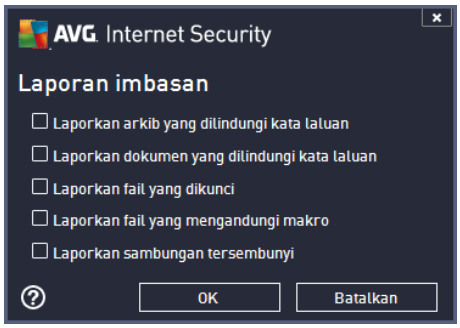
Laraskan berapa cepat imbasan selesai

Dalam bahagian ini anda boleh menentukan dengan lebih lanjut kelajuan imbasan yang diingini bergantung kepada penggunaan sumber sistem. Secara lalainya, nilai opsyen ini ditetapkan kepada

tahap *sensitif pengguna* bagi penggunaan sumber automatik. Jika anda mahu imbasan dijalankan dengan lebih cepat, ia akan mengambil masa yang kurang tetapi penggunaan sumber sistem akan meningkat dengan ketara semasa 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 sumber sistem yang digunakan dengan melanjutkan tempoh pengimbasan.

Tetapkan laporan imbasan tambahan

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

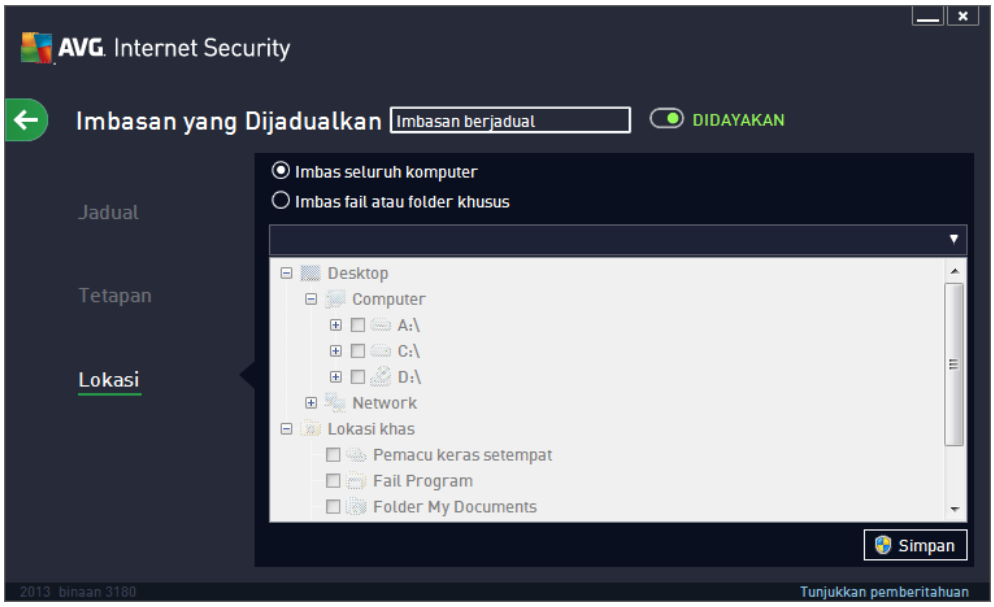


Kawalan dalam dialog

- ***Simpan*** – Menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain pada dialog ini dan menukar kembali ke gambaran keseluruhan Imbasan berjadual. Oleh itu, jika anda ingin mengkonfigurasikan parameter ujian pada semua tab, tekan butang untuk menyimpannya hanya selepas anda telah menentukan semua keperluan anda.

- – Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke gambaran keseluruhan Imbasan berjadual.

11.4.3. Lokasi



Pada tab ***Lokasi*** 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, di bahagian bawah dialog ini, struktur pepohon yang dipaparkan diaktifkan 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 menandakan pada kotak yang berkenaan. Folder yang dipilih akan muncul dalam medan teks di bahagian atas dialog dan menu jatuh bawah akan menyimpan sejarah imbasan terpilih anda untuk digunakan kemudian. 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 jarak tambahan*).

Dalam struktur pepohon, anda juga boleh melihat cabang yang dipanggil ***Lokasi khas***. Di bawah, terdapat senarai lokasi yang akan diimbas selepas kotak semak yang berkenaan ditandakan:

- ***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***
    - *untuk Win XP:* C:\Documents and Settings\Default User\My Documents\
    - *untuk Windows Vista/7*: C:\Users\user\Documents\
- ***Dokumen Kongsi***
    - *untuk Win XP*: C:\Documents and Settings\All Users\Documents\

- *untuk Windows Vista/7*: C:\Users\Public\Documents\

- ***Folder Windows*** – C:\Windows\

- ***Lain-lain***

  - *Pemacu sistem* – pemacu keras di mana sistem pengendalian dipasang (biasanya C:)

  - *Folder sistem* – C:\Windows\System32\

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

  - *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*)

Kawalan dalam dialog

- ***Simpan*** – Menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain pada dialog ini dan menukar kembali ke gambaran keseluruhan Imbasan berjadual. Oleh itu, jika anda ingin mengkonfigurasikan parameter ujian pada semua tab, tekan butang untuk menyimpannya hanya selepas anda telah menentukan semua keperluan anda.

- – Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke gambaran keseluruhan Imbasan berjadual.

11.5. Keputusan Imbasan

Dialog ***Gambaran keseluruhan keputusan imbasan*** memberikan senarai keputusan semua imbasan yang telah dilaksanakan setakat ini. Carta tersebut memberikan maklumat berikut pada setiap keputusan imbasan:

- ***Ikon*** – Lajur pertama memaparkan ikon maklumat yang menerangkan status imbasan:
  - Tiada jangkitan ditemui, imbasan telah selesai.
  - Tiada jangkitan ditemui, imbasan diganggu sebelum selesai
  - Jangkitan ditemui dan tidak dipulihkan, imbasan selesai
  - Jangkitan ditemui dan tidak dirawat, imbasan diganggu sebelum selesai
  - Jangkitan ditemui dan semua telah dirawat atau dibuang, imbasan selesai
  - Jangkitan ditemui dan semua telah dirawat atau dibuang, imbasan diganggu sebelum selesai
- ***Nama*** – Lajur memberikan nama imbasan yang berkaitan. Sama ada ia adalah satu daripada dua imbasan yang dipratakrifkan atau imbasan berjadual anda sendiri.
- ***Masa mula*** – Memberikan tarikh dan masa sebenar imbasan dilancarkan.
- ***Masa tamat*** – Memberikan tarikh dan masa sebenar imbasan selesai, dijeda atau terganggu.
- ***Objek diuji*** – Memberikan jumlah bilangan semua objek yang diimbas.
- ***Jangkitan*** – Memberikan bilangan jangkitan yang dibuang/jumlah jangkitan yang ditemu.
- ***Tinggi / Sederhana / Rendah*** – Tiga lajur berikutnya memberikan bilangan jangkitan keterukan tinggi, sederhana dan rendah yang ditemui masing-masing.
- ***Rootkit*** – Memberikan jumlah keseluruhan rootkit yang ditemui semasa pengimbasan.

Kawalan dialog

Lihat butiran – Klik butang untuk melihat maklumat terperinci mengenai imbasan yang dipilih *(diserlahkan dalam carta di atas)*.

Hapuskan keputusan – Klik butang untuk membuang maklumat keputusan imbasan yang dipilih daripada carta.

– Gunakan anak panah berwarna hijau dalam bahagian atas sebelah kiri dialog untuk kembali ke antara muka pengguna utama dengan gambaran keseluruhan komponen.

11.6. Butiran keputusan imbasan

Untuk membuka gambaran keseluruhan bagi maklumat terperinci pada keputusan imbasan yang dipilih, klik butang ***Lihat butiran*** yang boleh diakses dalam dialog Gambaran keseluruhan keputusan imbasan. Anda akan dihalakan semula ke antara muka dialog yang sama yang menerangkan secara terperinci maklumat mengenai keputusan imbasan berkenaan. Maklumat tersebut dibahagikan kepada tiga tab:

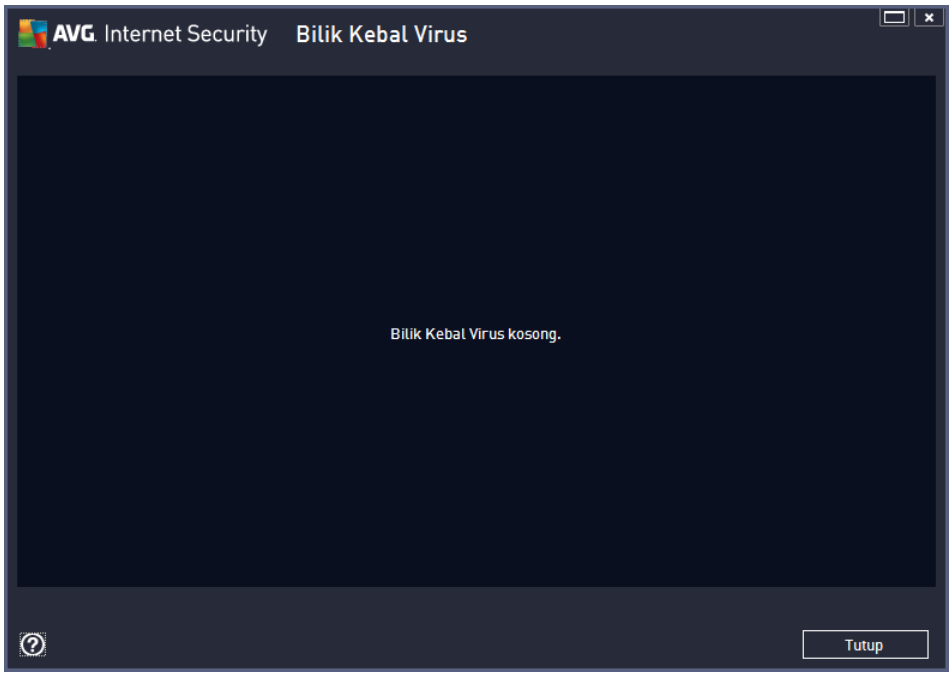
- ***Ringkasan*** – Tab memberikan maklumat asas mengenai imbasan: Jika ia berjaya diselesaikan, jika sebarang ancaman ditemui dan apa yang terjadi padanya.
- ***Butiran*** – Tab memaparkan semua maklumat mengenai imbasan, termasuk butiran mengenai sebarang ancaman yang dikesan. Eksport gambaran keseluruhan ke fail membolehkan anda menyimpannya sebagai fail .csv.
- ***Pengesanan*** – Tab ini hanya dipaparkan jika terdapat sebarang ancaman dikesan semasa imbasan dan memberikan maklumat terperinci mengenai ancaman tersebut:

  Keseriusan rendah: maklumat atau amaran, bukan ancaman sebenar. Biasanyan dokumen yang mengandungi makro, dokumen atau arkib yang dilindungi kata laluan, fail dikunci, dsb.

  Keterukan sederhana: biasanya PUP *(atur cara yang berpotensi tidak diingini, seperti adware)* atau kuki penjejakan

  Keterukan tinggi: ancaman serius seperti virus, Trojan, eksploitasi, dsb. Juga objek yang dikesan oleh kaedah pengesanan Heuristik, mis. ancaman yang belum lagi diterangkan dalam pangkalan data virus.

12. 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 dihapuskan 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 dianalisis atau memulihkannya ke lokasi asal.

Antara muka ***Bilik Kebal Virus*** dibuka dalam tetingkap berasingan dan menawarkan gambaran keseluruhan maklumat mengenai objek dijangkiti yang dikuarantin:

- ***Tarikh simpanan*** – Memberikan tarikh dan masa fail yang disyaki tersebut dikesan dan dibuang ke Bilik Kebal Virus.
- ***Keterukan*** – Jika anda memutuskan untuk memasang komponen Identity dalam **AVG Internet Security 2013** anda, pengenalpastian grafik bagi keterukan penemuan masing-masing pada skala empat tahap daripada yang tidak boleh dibantah *(tiga titik hijau)* sehingga kepada sangat berbahaya *(tiga titik merah)* 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 Pengesanan*** – Menentukan nama jangkitan yang dikesan menurut ensiklopedia virus dalam talian.
- ***Sumber*** – Menentukan komponen **AVG Internet Security 2013** mana yang telah mengesan ancaman berkenaan.

- ***Mesej*** – Dalam situasi yang jarang berlaku, beberapa nota boleh kelihatan dalam lajur ini dengan memberikan komen terperinci terhadap ancaman berkenaan yang dikesan.

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*** – untuk maklumat terperinci mengenai ancaman tertentu yang dikuarantin dalam ***Bilik Kebal Virus*** serlahkan item yang dipilih dalam senarai dan klik butang ***Butiran*** untuk memanggil dialog baharu dengan penerangan mengenai ancaman yang dikesan.
- ***Hapuskan*** – membuang fail yang dijangkiti daripada ***Bilik Kebal Virus*** sepenuhnya dan tidak boleh dibalikkan.
- ***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. Sejarah

Bahagian ***Sejarah*** termasuk maklumat mengenai semua acara yang lalu *(seperti kemas kini, imbasan, pengesanan, dsb.)* dan laporan mengenai acara ini. Bahagian ini boleh diakses daripada antara muka pengguna utama melalui item ***Opsyen / Sejarah***. Seterusnya, sejarah semua acara yang direkodkan dibahagikan kepada bahagian berikut:

- Keputusan imbasan
- Pengesanan Resident Shield
- Pengesanan Perlindungan E-mel
- Penemuan Online Shield
- Log sejarah acara
- Log Firewall

13.1. Keputusan imbasan

Dialog ***Gambaran keseluruhan keputusan imbasan*** boleh diakses melalui item menu ***Opsyen / Sejarah / Keputusan imbasan*** dalam navigasi baris atas tetingkap utama **AVG Internet Security 2013**. Dialog memberikan senarai semua imbasan yang dilancarkan sebelum ini dan maklumat mengenai 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
- ***Tinggi / Sederhana*** / ***Rendah*** – lajur ini memberikan bilangan jangkitan dibuang/jumlah jangkitan yang ditemui mengikut turutan keterukan tinggi, sederhana dan rendah
- ***Maklumat*** – maklumat berkaitan dengan perjalanan imbasan dan keputusan *(biasanya mengenai penyelesaian atau gangguannya)*
- ***Rootkit*** – bilangan rootkit

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
- ***Hapuskan keputusan*** – tekannya untuk membuang item yang dipilih daripada gambaran keseluruhan keputusan imbasan
- – untuk bertukar kepada dialog utama AVG lalai *(gambaran keseluruhan komponen)*, gunakan anak panah di penjuru kiri sebelah atas dialog ini

13.2. Pengesanan Resident Shield

Perkhidmatan ***Resident Shield*** adalah sebahagian daripada komponen ***Komputer*** dan 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 maklumat mengenai objek yang telah dikesan dan diperuntukkan sebagai dijangkiti (*Nama*) dan beberapa fakta deskriptif mengenai jangkitan yang dikenali (*Penerangan*). Pautan Tunjukkan butiran akan menghalakan anda semula ke ensiklopedia virus dalam talian di mana anda boleh menemui maklumat terperinci mengenai jangkitan yang dikesan, jika jangkitan ini diketahui. Dalam dialog tersebut, anda juga akan melihat gambaran keseluruhan penyelesaian yang tersedia mengenai cara untuk mengendalikan ancaman yang dikesan. Salah satu alternatif akan dilabelkan sebagai disyorkan: ***Lindungi Saya (disyorkan). Jika boleh, anda seharusnya sentiasa memilih opsyen ini!***

Nota: *Kemungkinan terdapat saiz objek yang dikesan melebihi had ruang kosong dalam Bilik Kebal Virus. Jika yang demikian, mesej amaran akan muncul dengan memaklumkan anda mengenai isu semasa anda cuba mengalihkan objek yang dijangkiti ke Bilik Kebal Virus. Walau bagaimanapun, saiz Bilik Kebal Virus boleh diubah suai. 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 opsyen 'Had saiz Bilik Kebal Virus'.*

Dalam bahagian bawah dialog anda boleh menemui pautan ***Tunjukkan butiran***. Klik padanya untuk membuka tetingkap baharu dengan maklumat terperinci mengenai proses yang sedang berjalan semasa jangkitan dikesan dan pengenalan proses.

Satu senarai untuk semua pengesanan Resident Shield tersedia untuk tinjauan menyeluruh di dalam dialog ***pengesanan Resident Shield***. Dialog ini boleh diakses melalui item menu ***Opsyen / Sejarah / pengesanan Resident Shield*** dalam navigasi baris atas tetingkap utama **AVG Internet Security 2013**. Dialog menawarkan gambaran keseluruhan objek yang dikesan oleh resident shield yang dinilai sebagai berbahaya dan sama ada telah dipulihkan atau dialihkan ke Bilik Kebal Virus.

Untuk setiap objek yang dikesan, maklumat berikut disediakan:

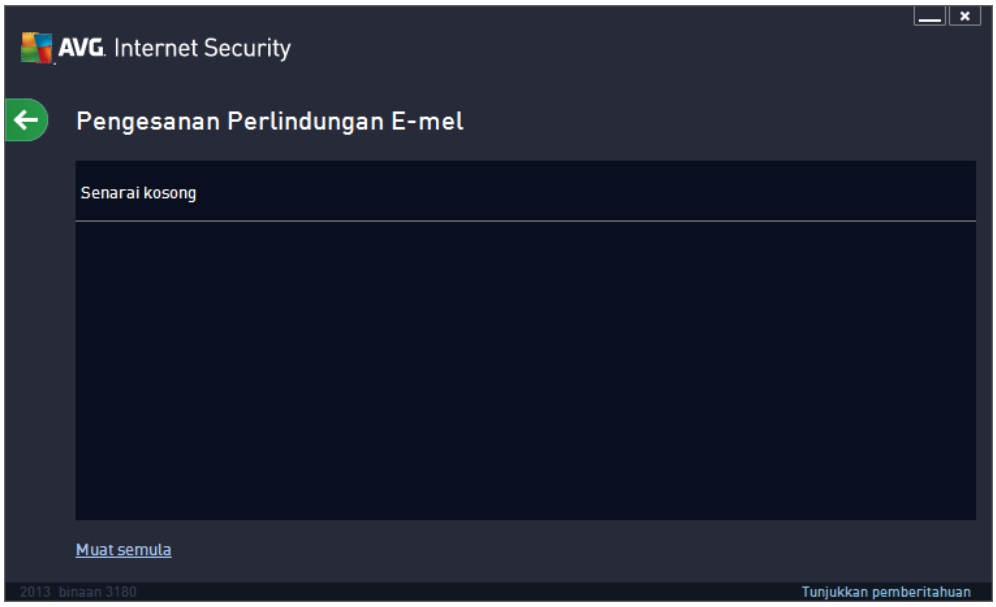
- ***Nama pengesanan*** – penerangan (*mungkin juga nama*) objek yang dikesan dan lokasinya
- ***Keputusan*** – tindakan dilakukan dengan objek yang dikesan
- ***Pengesanan masa*** – tarikh dan masa ancaman dikesan dan disekat
- ***Jenis Objek*** – jenis objek yang dikesan
- ***Proses*** – tindakan apa yang dilakukan untuk memanggil objek berpotensi berbahaya supaya ia boleh dikesan

Butang kawalan

- ***Muat semula*** – kemas kini senarai penemuan yang dikesan oleh ***Online Shield***
- ***Eksport*** – eksport keseluruhan senarai objek yang dikesan ke dalam fail
- ***Buang yang dipilih*** – di dalam senarai anda boleh menyerlahkan rekod yang dipilih dan menggunakan butang ini untuk hapuskan item yang dipilih ini sahaja
- ***Buang semua ancaman*** – gunakan butang untuk hapuskan semua rekod yang disenaraikan dalam dialog ini
- – untuk bertukar kepada dialog utama AVG lalai *(gambaran keseluruhan komponen)*, gunakan anak panah di penjuru kiri sebelah atas dialog ini

13.3. Pengesanan Perlindungan E-mel

Dialog ***Pengesanan Perlindungan E-mel*** boleh diakses melalui menu item ***Opsyen / Sejarah / Pengesanan Perlindungan E-mel*** dalam baris navigasi sebelah atas tetingkap utama **AVG Internet Security 2013**.



Dialog tersebut memberikan senarai semua penemuan yang dikesan melalui komponen E-mel. Untuk setiap objek yang dikesan, maklumat berikut disediakan:

- ***Nama pengesanan*** – penerangan (*(mungkin juga nama)* objek yang dikesan dan sumbernya
- ***Keputusan*** – tindakan dilakukan dengan objek yang dikesan
- ***Masa pengesanan*** – tarikh dan masa objek mencurigakan 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. Anda juga boleh mengeksport keseluruhan senarai objek yang dikesan dalam fail (***Eksport senarai ke fail***) dan hapuskan semua entri pada objek yang dikesan (***Kosongkan senarai***).

Butang kawalan

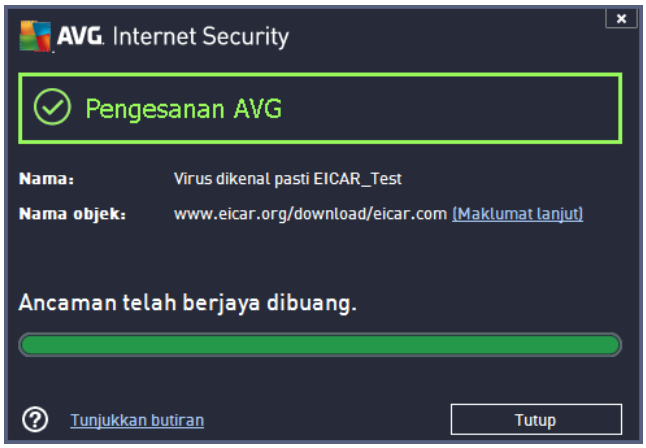
Butang kawalan tersedia dalam antara muka ***pengesanan Pengimbas E-mel*** adalah seperti berikut:

- ***Muat semula senarai*** – mengemas kini senarai ancaman yang dikesan.

- – untuk bertukar kepada dialog utama AVG lalai *(gambaran keseluruhan komponen),* gunakan anak panah di penjuru kiri sebelah atas dialog ini

13.4. Penemuan 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:

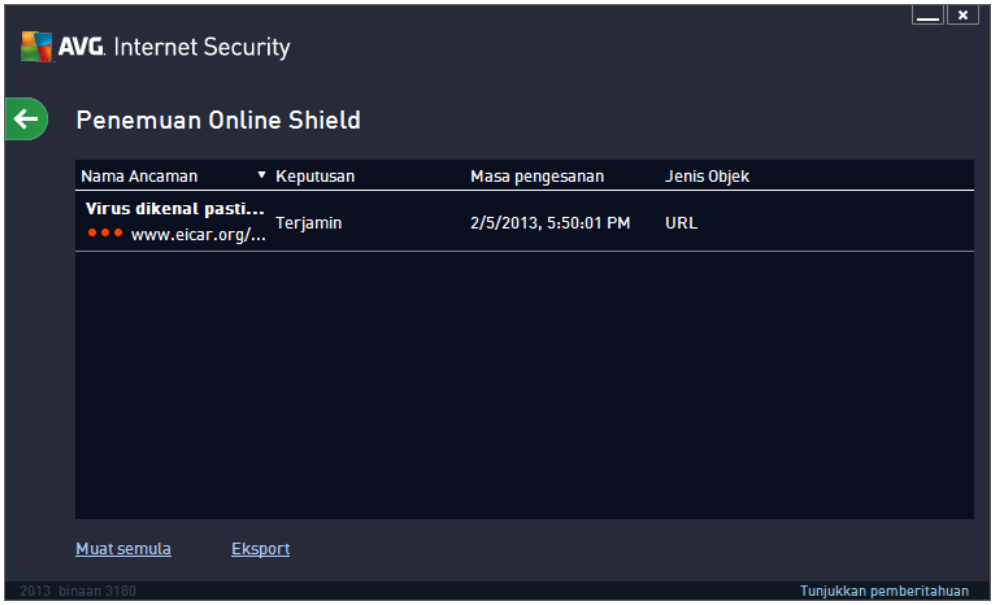


Dalam dialog amaran ini anda akan menemui maklumat mengenai objek yang telah dikesan dan diperuntukkan sebagai dijangkiti (*Nama*) dan beberapa fakta deskriptif mengenai jangkitan yang dikenali (*Penerangan*). Pautan Tunjukkan butiran akan menghalakan anda semula ke ensiklopedia virus dalam talian di mana anda boleh menemui maklumat terperinci mengenai jangkitan yang dikesan, jika jangkitan ini diketahui. Dialog menyediakan elemen kawalan berikut:

- ***Tunjukkan butiran*** – klik pautan untuk membuka tetingkap timbul baharu di mana anda boleh menemui maklumat mengenai proses yang berjalan semasa jangkitan dikesan dan pengenalan proses.

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

Halaman web yang mencurigakan tidak akan dibuka dan pengesanan ancaman akan dilog dalam senarai ***penemuan Online Shield***. Gambaran keseluruhan bagi ancaman yang dikesan ini boleh diakses melalui item menu ***Opsyen / Sejarah / penemuan Online Shield*** dalam navigasi baris atas tetingkap utama **AVG Internet Security 2013**.



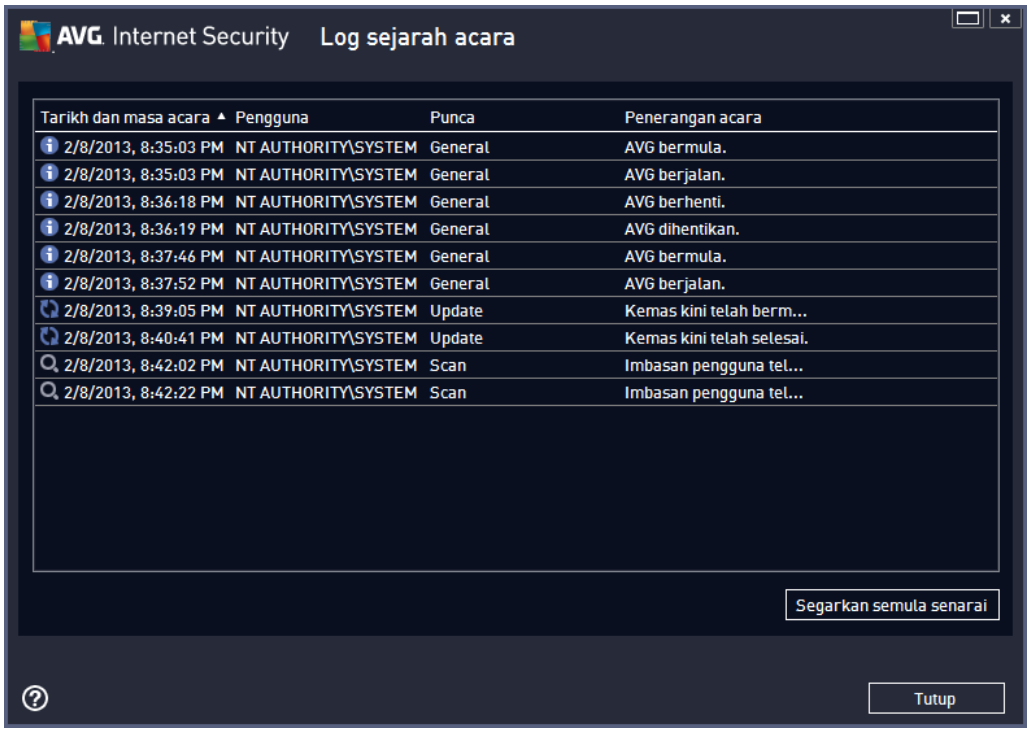
Untuk setiap objek yang dikesan, maklumat berikut disediakan:

- ***Nama pengesanan*** – penerangan (*mungkin juga nama*) objek yang dikesan dan sumbernya (*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

Butang kawalan

- ***Muat semula*** – kemas kini senarai penemuan yang dikesan oleh ***Online Shield***
- ***Eksport*** – eksport keseluruhan senarai objek yang dikesan ke dalam fail
- – untuk bertukar kepada dialog utama AVG lalai *(gambaran keseluruhan komponen),* gunakan anak panah di penjuru kiri sebelah atas dialog ini

13.5. Log sejarah acara



Dialog ***Log sejarah acara*** boleh diakses melalui menu item ***Opsyen / Sejarah / Log sejarah acara*** dalam baris navigasi sebelah atas tetingkap utama **AVG Internet Security 2013**. Dalam dialog ini, anda boleh menemui ringkasan acara penting yang berlaku sewaktu operasi **AVG Internet Security 2013**. Dialog memberikan rekod jenis acara berikut: maklumat mengenai kemas kini aplikasi AVG; maklumat mengenai imbasan mula, tamat atau berhenti (*termasuk ujian yang dilakukan secara automatik*); maklumat mengenai acara yang berhubung dengan pengesanan virus (*sama ada oleh resident shield atau pengimbasan*) termasuk lokasi kejadian; dan acara penting lain.

Untuk setiap acara, maklumat berikut disenaraikan:

- ***Tarikh dan masa acara*** memberikan tarikh dan masa yang tepat acara itu berlaku.
- ***Pengguna*** menyatakan nama pengguna yang sedang dilog masuk pada masa acara itu berlaku.
- ***Sumber*** memberikan maklumat mengenai komponen sumber atau bahagian lain sistem AVG yang mencetuskan acara tersebut.
- ***Penerangan acara*** memberikan rumusan ringkas mengenai perkara sebenar yang berlaku.

Butang kawalan

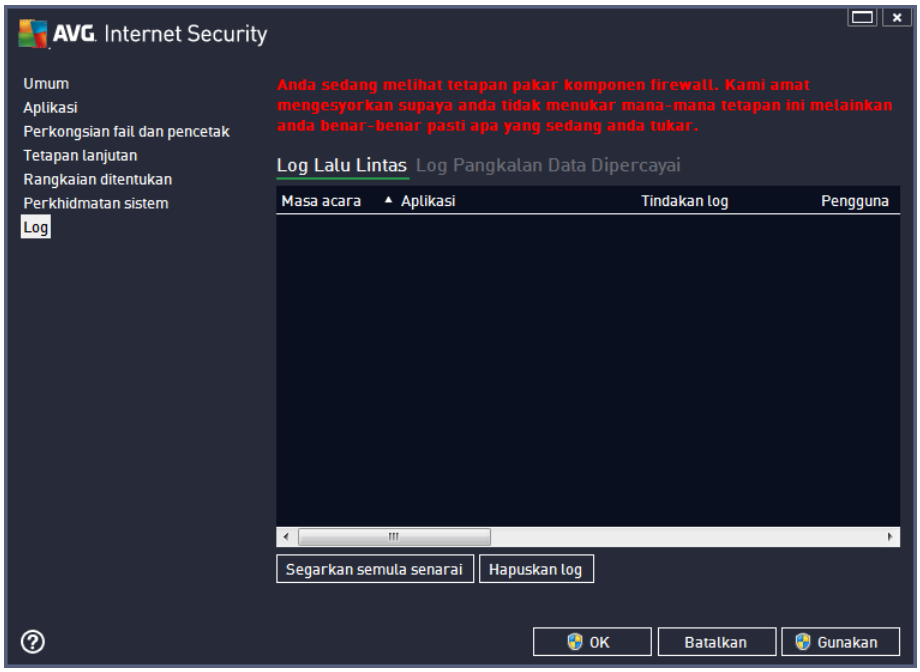
- ***Muat semula senarai*** – tekan butang untuk mengemas kini semua entri dalam senarai acara
- ***Tutup*** – tekan butang untuk kembali ke **AVG Internet Security 2013** tetingkap utama

13.6. Log Firewall

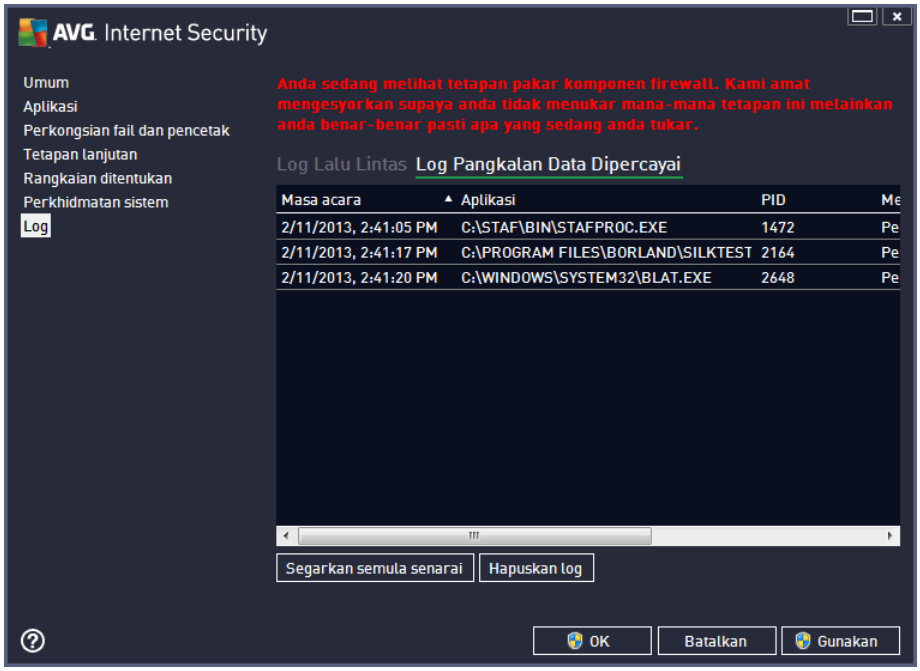
Dialog ini bertujuan untuk konfigurasi pakar dan kami mengesyorkan supaya anda tidak menukar sebarang tetapan melainkan anda benar-benar pasti tentang perubahan tersebut!

Dialog ***Log*** membenarkan anda menyemak semula senarai semua tindakan dan acara Firewall yang dilog dengan penerangan terperinci bagi parameter berkaitan yang dipaparkan pada dua tab:

- ***Log Trafik*** – Tab ini menawarkan maklumat mengenai aktiviti oleh semua aplikasi yang telah cuba menyambung ke rangkaian. Untuk setiap item, anda akan menemui maklumat mengenai masa acara, nama aplikasi, tindakan log yang berkenaan, nama pengguna, PID, arak trafik, jenis protokol, bilangan port jauh dan setempat serta maklumat mengenai alamat IP setempat dan jauh.



- ***Log Pangkalan Data Dipercayai*** – *Pangkalan data dipercayai* adalah pangkalan data dalaman AVG untuk mengumpul maklumat 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 peraturan firewall yang ditentukan untuk aplikasi ini lagi*), adalah perlu untuk mengetahui sama ada komunikasi rangkaian harus dibenarkan untuk aplikasi berkenaan. Pertama sekali, AVG mencari *Pangkalan data yang dipercayai*dan jika aplikasi disenaraikan, ia akan diberikan akses kepada rangkaian secara automatik. Hanya selepas itu, dengan syarat tiada maklumat mengenai aplikasi yang tersedia dalam pangkalan, anda akan ditanya dalam dialog kendiri sama ada anda ingin membenarkan aplikasi mengakses rangkaian.



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 baru dipaparkan.

- ***Hapuskan log*** – tekan untuk hapuskan semua entri dalam carta.

14. 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 baharu, serangan penggodam baharu 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 ia disebarkan, adalah amat penting untuk mengemas kini **AVG Internet Security 2013** anda secara tetap. Penyelesaian terbaik ialah dengan mengekalkan tetapan lalai atur cara di mana kemas kini automatik dikonfigurasikan. Sila ingat bahawa jika pangkalan data virus bagi **AVG Internet Security 2013** anda tidak dikemas kini, atur cara tidak akan 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.

14.1. Pelancaran kemas kini

Untuk memberikan keselamatan maksimum yang tersedia, **AVG Internet Security 2013** secara lalainya dijadualkan untuk mencari kemas kinian pangkalan data virus baharu setiap empat jam. Memandangkan kemas kini AVG tidak dikeluarkan mengikut sebarang jadual yang ditetapkan tetapi dalam respons kepada jumlah dan keterukan ancaman baharu, semakan ini sangat penting untuk memastikan pangkalan data virus AVG anda terkini setiap masa.

Jika anda ingin menyemak 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. Apabila anda memulakan kemas kini, pertama sekali, AVG akan mengenal pasti sama ada terdapat fail kemas kini baharu yang tersedia. Jika demikian, **AVG Internet Security 2013** mula memuat turunnya dan melancarkan proses kemas kini dengan sendirinya. Anda akan dimaklumkan mengenai hasil kemas kini dalam dialog slaid pada ikon dulang sistem AVG.

Sekiranya anda ingin mengurangkan bilangan pelancaran kemas kini, anda boleh menyediakan parameter pelancaran kemas kini anda sendiri. Walau bagaimanapun, ***adalah amat disyorkan supaya anda melancarkan kemas kini sekurang-kurangnya sekali sehari!*** Konfigurasi boleh diedit dalam bahagian Tetapan Lanjutan/Jadual, secara khusus dalam dialog berikut:

- Jadual kemas kini definisi
- Jadual kemas kini atur cara
- Jadual kemas kini AntiSpam

14.2. Tahap kemas kini

AVG Internet Security 2013 memberikan dua tahap kemas kini untuk dipilih:

- ***Kemas kini definisi*** mengandungi perubahan yang diperlukan untuk perlindungan antivirus, anti-spam dan anti-malware 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

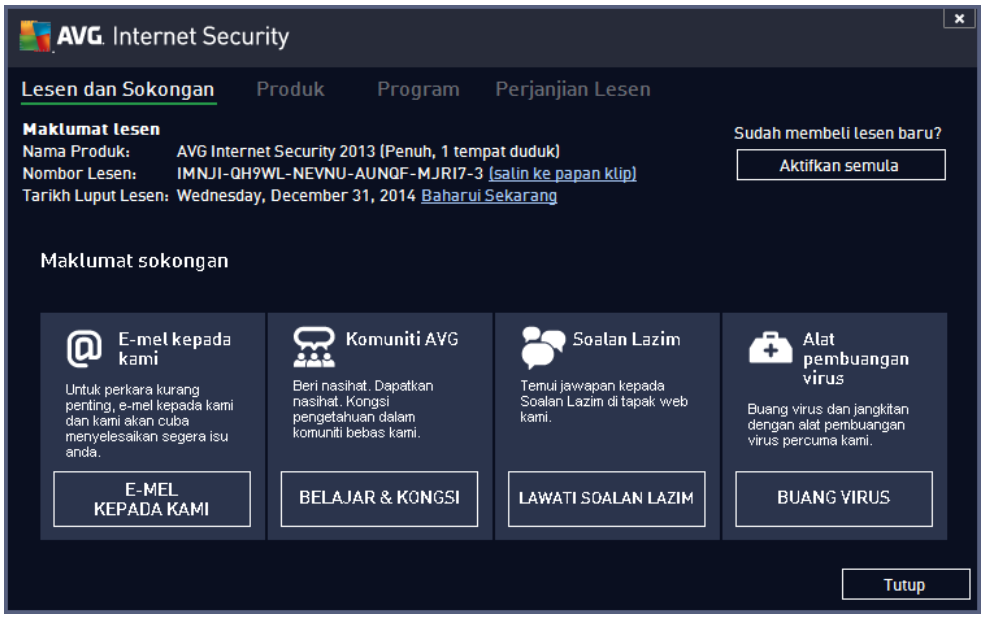
Nota: *Jika kemas kini atur cara berjadual dan imbasan berjadual berlaku serentak, proses kemas kini adalah lebih utama dan imbasan akan terganggu.*

15. Soalan Lazim dan Sokongan Teknikal

Sekiranya anda mempunyai sebarang masalah jualan atau teknikal dengan aplikasi **AVG Internet Security 2013** anda, terdapat beberapa cara untuk mendapatkan bantuan. Sila pilih daripada opsyen berikut:

- ***Dapatkan Sokongan***: Terus dalam aplikasi AVG, anda boleh menghubungi halaman sokongan pelanggan khusus di tapak web AVG (http://www.avg.com/). Pilih item menu utama ***Bantuan / Dapatkan Sokongan*** untuk dihalakan semula ke tapak web AVG dengan saluran sokongan yang tersedia. Untuk meneruskan, sila ikuti arahan pada 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 dengan **AVG Internet Security 2013** *(untuk membuka fail bantuan, tekan kekunci F1 dalam mana-mana dialog dalam aplikasi)*. Bahagian ini memberikan senarai situasi yang paling kerap berlaku semasa pengguna ingin mendapatkan bantuan profesional untuk isu teknikal. Sila pilih situasi yang paling tepat menggambarkan masalah anda dan klik padanya untuk membuka arahan terperinci yang membawa kepada penyelesaian masalah.

- ***Pusat Sokongan tapak web AVG***: Secara alternatif, anda boleh mendapatkan penyelesaian kepada masalah anda di tapak 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 berhuraian bagi soalan lazim. Bahagian ini boleh diakses melalui opsyen menu ***Pusat Sokongan / Soalan Lazim***. Sekali lagi, semua

soalan dibahagikan dengan cara yang teratur ke dalam kategori jualan, teknikal dan virus.

- ***Mengenai virus & ancaman***: Bahagian khusus tapak 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 memasuki halaman yang memberikan gambaran keseluruhan berstruktur bagi maklumat berkaitan dengan ancaman dalam talian. Anda juga boleh mendapatkan arahan mengenai membuang virus, spyware dan nasihat mengenai cara untuk terus dilindungi.

- ***Forum perbincangan***: Anda juga boleh menggunakan forum perbincangan pengguna AVG di http://forums.avg.com.