Software firewalls

S-38.153 Security of communication protocols

Jari Huttunen

Software firewalls

- Definition (loose):

  - An implementation as software that can be run on a personal computer to offer basic defense from outside (and inside) attacks

Software firewalls (cont)

How does it differ from hardware firewalls?

- Based on application level differentation

  - Differentiation between traffic sent by different programs (vs packet per packet filtering)

Software firewalls (cont)

- Easier to set up?
- More difficult in use? (annoying pop up messages)
- Running on end-user machine

  - memory consumption

Software firewalls (cont)

- A software firewall does NOT replace the need for anti-virus software (or vice versa)
- What happens when a software firewall crashes?

  - Usually just lets all the traffic through

Software firewalls (cont)

- So, when should you use a software firewall instead of hardware fw?

  - Only one (or few) end user(s)
- To get the safest result use both sw and hw firewall!

Let’s examine some common commercial software firewalls

There are though some freeware software available that do the same job…

Norton Personal Firewall 2003

- List price $49.95
- Part of Symantec's Norton Internet Security 2003
- Intrusion detection

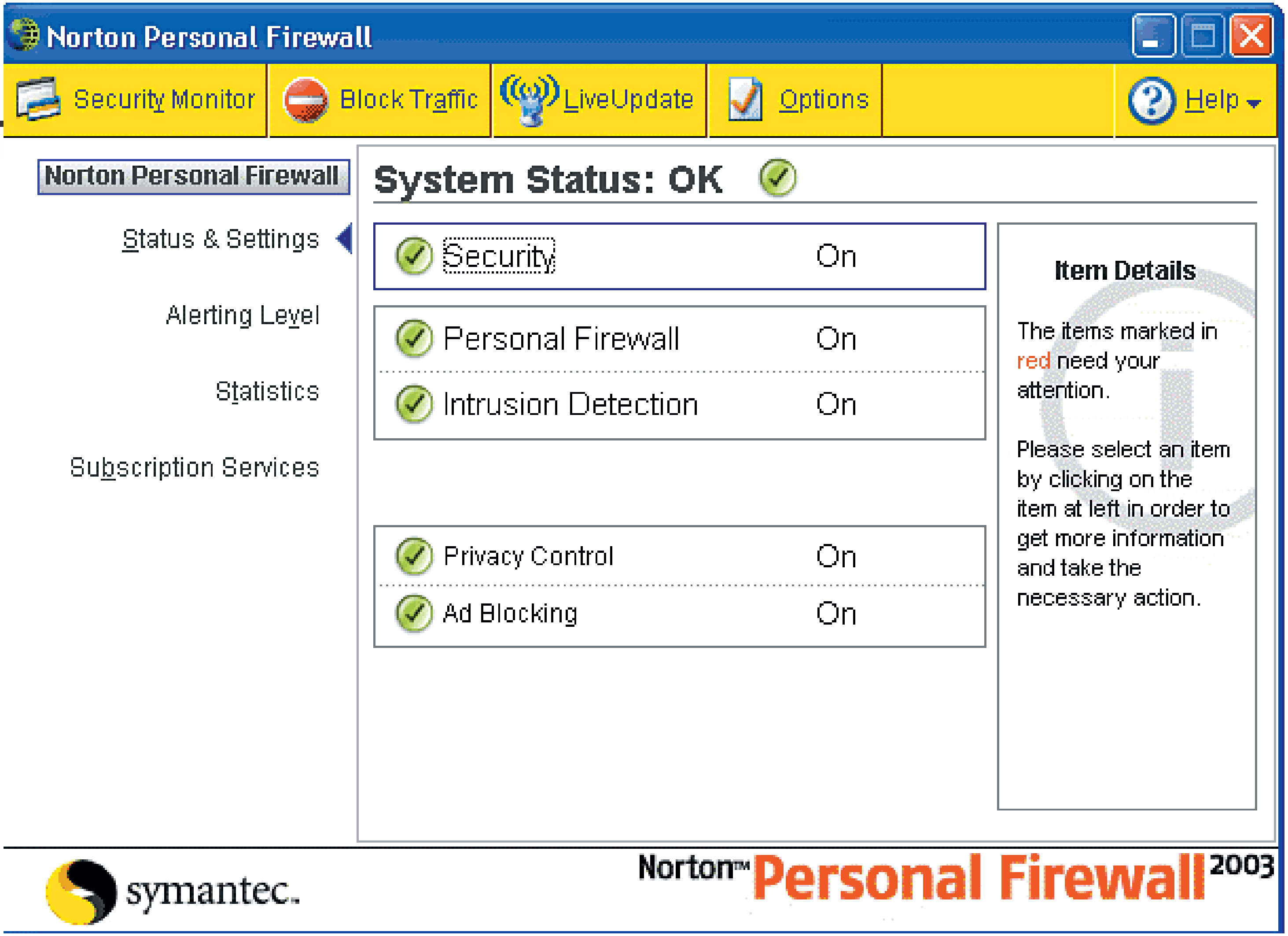
  - can e.g. detect and block port scans
- Automatic program control

  - determines which programs can safely connect to the Internet

Norton Personal Firewall 2003 (cont)

- Alert Assistant

  - provides detailed information to help you choose the best course of action
- Live update
- Easy to use but still powerful



System Status: OK ✓

✓	Security	On
✓	Personal Firewall	On
✓	Intrusion Detection	On
✓	Privacy Control	On
✓	Ad Blocking	On

Item Details

The items marked in red need your attention.

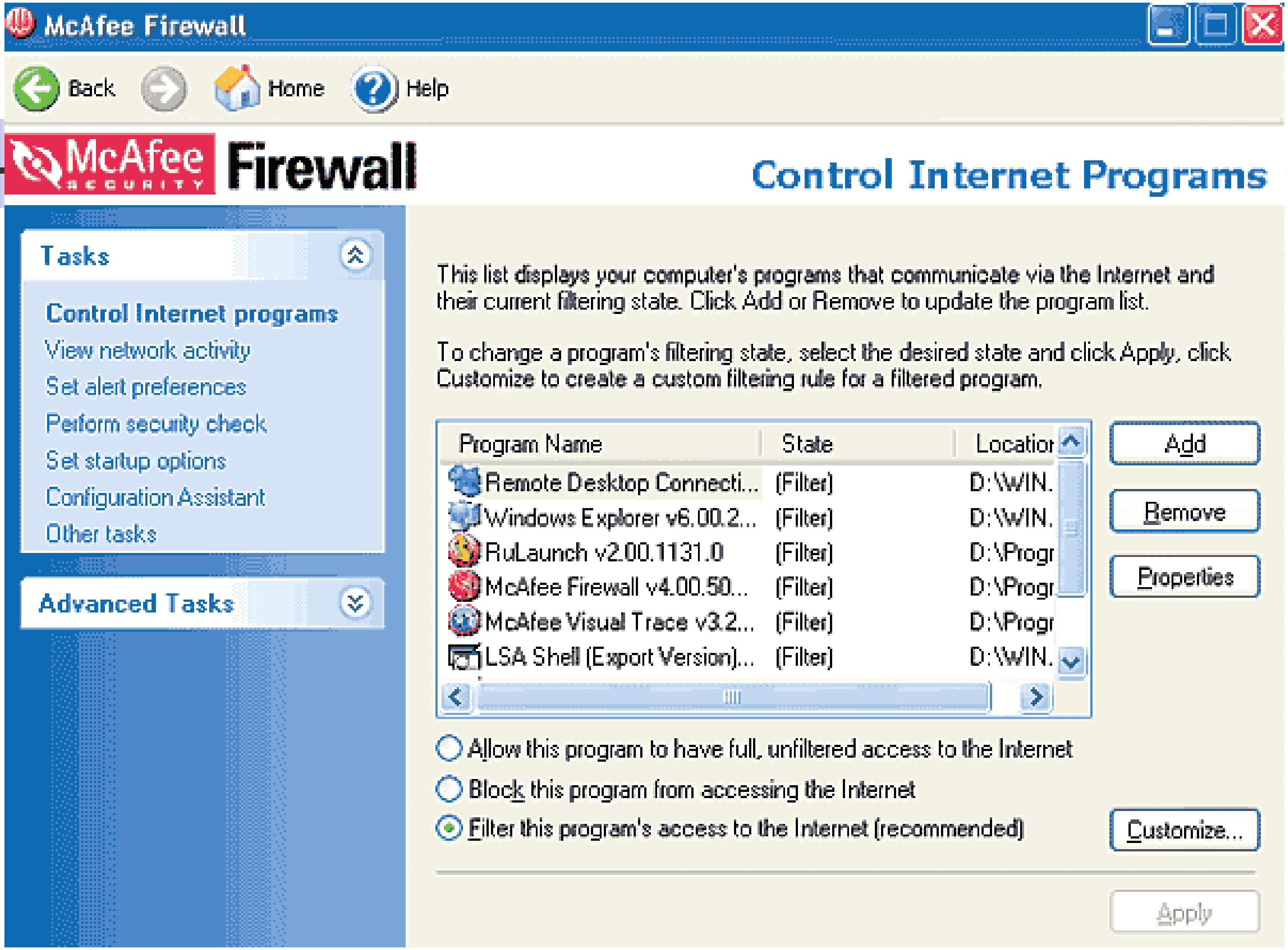
Please select an item by clicking on the item at left in order to get more information and take the necessary action.

McAfee Firewall 4.0

- List price $39.95
- Not the same as McAfee Personal Firewall Plus 4.1
- Enhanced Hacker Tracing
- Application Scan
- Firewall Settings Security Check
- Intrusion Detection System

McAfee Firewall 4.0 (cont)

- Password protection



Control Internet Programs

This list displays your computer's programs that communicate via the Internet and their current filtering state. Click Add or Remove to update the program list.

To change a program's filtering state, select the desired state and click Apply, click Customize to create a custom filtering rule for a filtered program.

Program Name	State	Locatior
Remote Desktop Connecti...	(Filter)	D:\WIN.
Windows Explorer v6.00.2...	(Filter)	D:\WIN.
RuLaunch v2.00.1131.0	(Filter)	D:\Progr
McAfee Firewall v4.00.50...	(Filter)	D:\Progr
McAfee Visual Trace v3.2...	(Filter)	D:\Progr
LSA Shell (Export Version)...	(Filter)	D:\WIN.

○ Allow this program to have full, unfiltered access to the Internet

○ Block this program from accessing the Internet

● Filter this program's access to the Internet (recommended)

Sygate Personal Firewall PRO 5.0

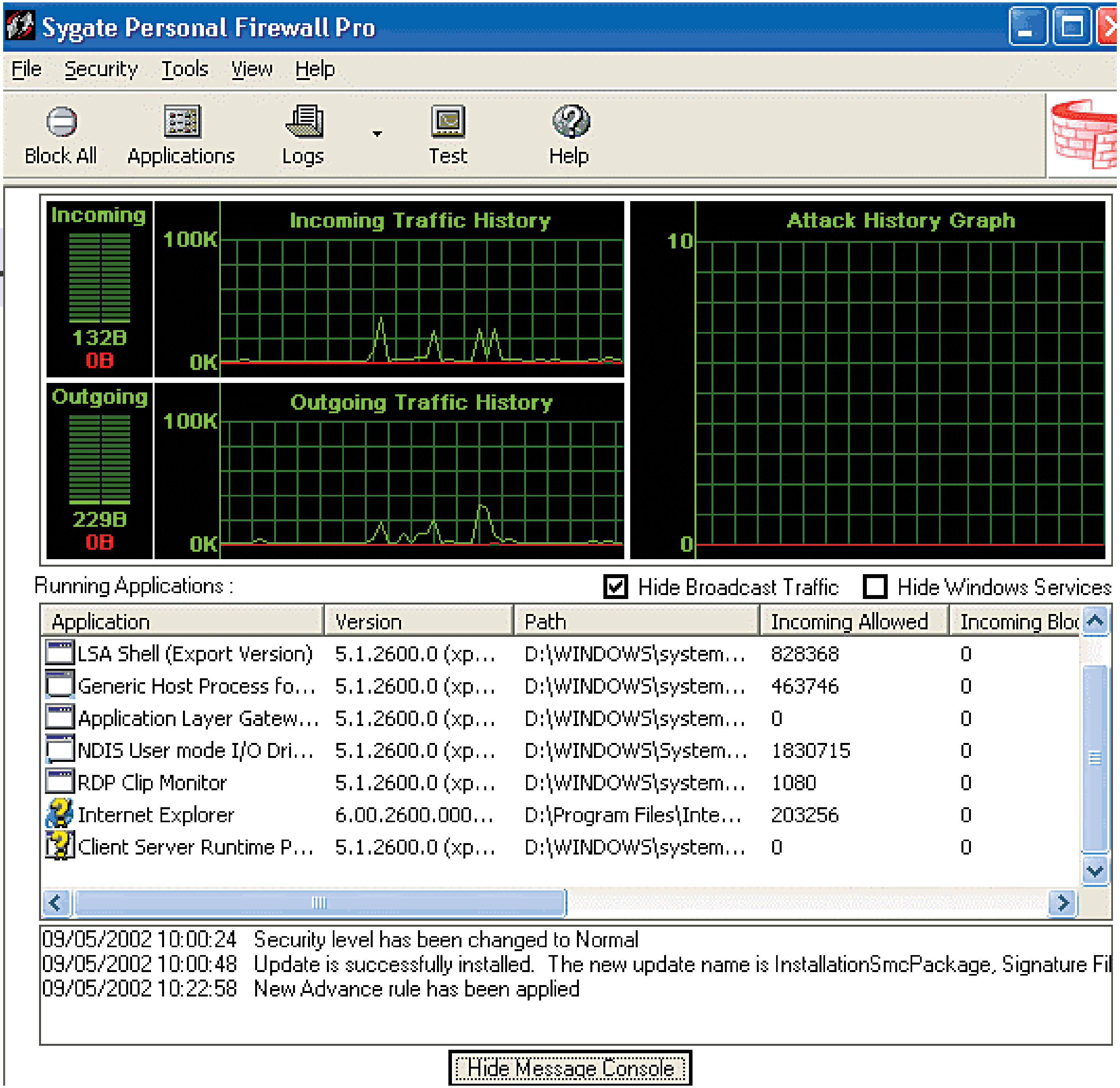
- List price $39.95
- Intrusion detection
- Anti-IP & Anti-MAC Spoofing
- Component Integrity

  - Fingerprint (MD5 checksum)

  - Application DLL Authentication

Sygate Personal Firewall PRO 5.0 (cont)

- Firewall Termination Prevention



Running Applications :

☑ Hide Broadcast Traffic □ Hide Windows Services

Application	Version	Path	Incoming Allowed	Incoming Bloc
LSA Shell (Export Version)	5.1.2600.0 (xp…	D:\WINDOWS\system…	828368	0
Generic Host Process fo…	5.1.2600.0 (xp…	D:\WINDOWS\system…	463746	0
Application Layer Gatew…	5.1.2600.0 (xp…	D:\WINDOWS\system…	0	0
NDIS User mode I/O Dri…	5.1.2600.0 (xp…	D:\WINDOWS\System…	1830715	0
RDP Clip Monitor	5.1.2600.0 (xp…	D:\WINDOWS\system…	1080	0
Internet Explorer	6.00.2600.000…	D:\Program Files\Inte…	203256	0
Client Server Runtime P…	5.1.2600.0 (xp…	D:\WINDOWS\system…	0	0

```
09/05/2002 10:00:24   Security level has been changed to Normal
09/05/2002 10:00:48   Update is successfully installed.  The new update name is InstallationSmcPackage, Signature Fil
09/05/2002 10:22:58   New Advance rule has been applied
```

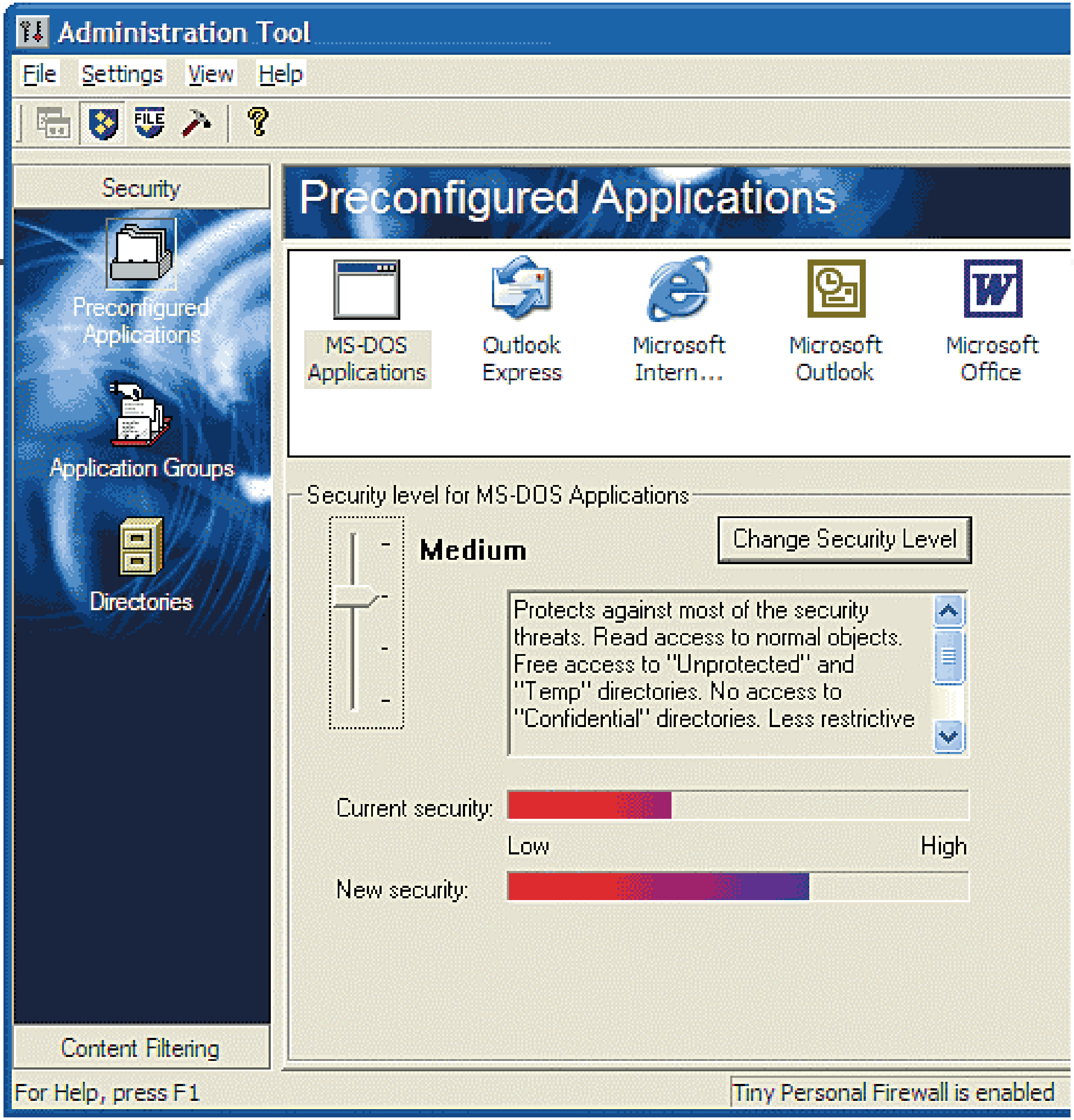
Tiny Personal Firewall 3.0

- List price $39
- A lot of flexibility in making rules

  -> not so easy to use
- Intrusion Detection (rules from SNORT.ORG)
- Learning mode
- Windows Security

Tiny Personal Firewall 3.0 (cont)

- Block or admit traffic on specific ports at specific times of day
- File Access Guard



Security level for MS-DOS Applications

Medium

Protects against most of the security threats. Read access to normal objects. Free access to "Unprotected" and "Temp" directories. No access to "Confidential" directories. Less restrictive

Current security:

New security:

For Help, press F1

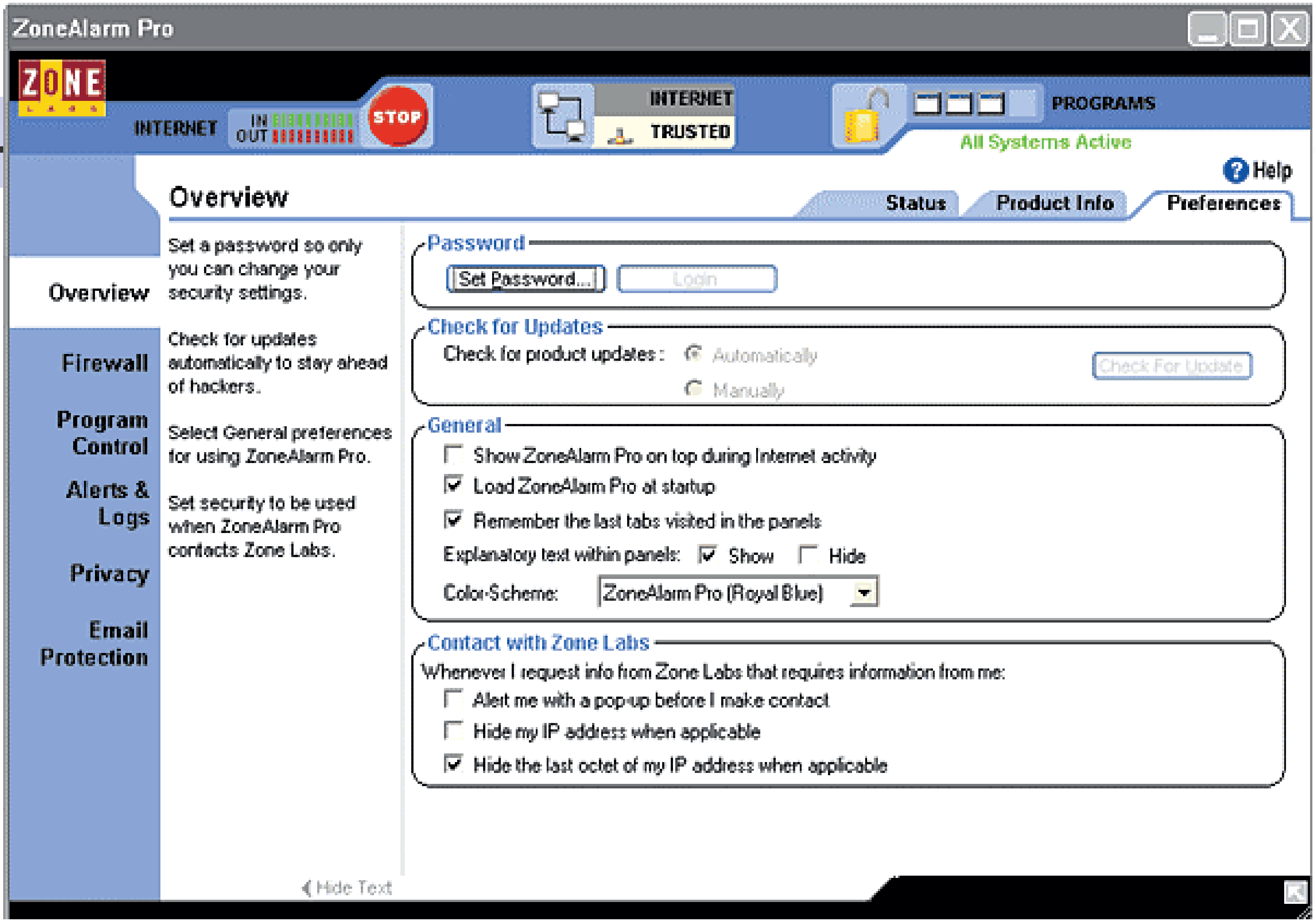
Tiny Personal Firewall is enabled

ZoneAlarm Pro 3.1

- List price $49.95
- The regular version of ZoneAlarm is available free to individuals and nonprofit organizations
- Simple and easy to use

ZoneAlarm Pro 3.1 (cont)

- Automatic Intrusion Blocking
- Hacker Tracking
- Pop-up Ad Control + cookie control
- Automatic Network Detection
- Advanced MailSafe e-mail attachment protection
- Stealth Mode to make your PC invisible on the Internet



Overview

Set a password so only you can change your security settings.

Check for updates automatically to stay ahead of hackers.

Select General preferences for using ZoneAlarm Pro.

Set security to be used when ZoneAlarm Pro contacts Zone Labs.

Password

Check for Updates

Check for product updates : ● Automatically ○ Manually

General

□ Show ZoneAlarm Pro on top during Internet activity

☑ Load ZoneAlarm Pro at startup

☑ Remember the last tabs visited in the panels

Explanatory text within panels: ☑ Show □ Hide

Color Scheme: ZoneAlarm Pro (Royal Blue)

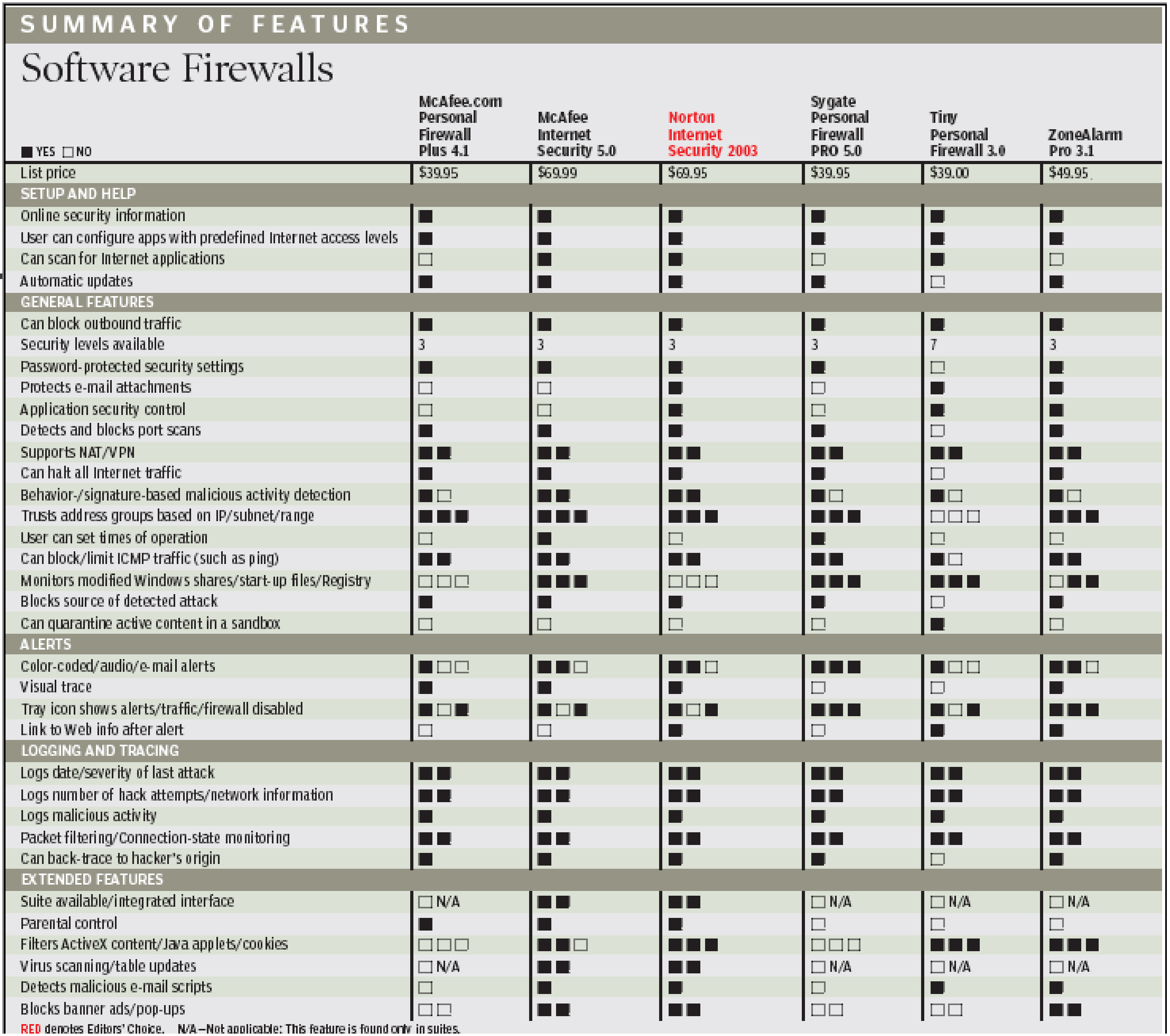
Contact with Zone Labs

Whenever I request info from Zone Labs that requires information from me:

□ Alert me with a pop-up before I make contact

□ Hide my IP address when applicable

☑ Hide the last octet of my IP address when applicable



SUMMARY OF FEATURES

Software Firewalls

■ YES □ NO	McAfee.com Personal Firewall Plus 4.1	McAfee Internet Security 5.0	Norton Internet Security 2003	Sygate Personal Firewall PRO 5.0	Tiny Personal Firewall 3.0	ZoneAlarm Pro 3.1
List price	$39.95	$69.99	$69.95	$39.95	$39.00	$49.95
SETUP AND HELP						
Online security information	■	■	■	■	■	■
User can configure apps with predefined Internet access levels	■	■	■	■	■	■
Can scan for Internet applications	□	■	■	□	■	□
Automatic updates	■	■	■	■	□	■
GENERAL FEATURES						
Can block outbound traffic	■	■	■	■	■	■
Security levels available	3	3	3	3	7	3
Password-protected security settings	■	■	■	■	□	■
Protects e-mail attachments	□	□	■	□	■	■
Application security control	□	□	■	□	■	■
Detects and blocks port scans	■	■	■	■	□	■
Supports NAT/VPN	■ ■	■ ■	■ ■	■ ■	■ ■	■ ■
Can halt all Internet traffic	■	■	■	■	□	■
Behavior-/signature-based malicious activity detection	■ □	■ ■	■ ■	■ □	■ □	■ □
Trusts address groups based on IP/subnet/range	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	□ □ □	■ ■ ■
User can set times of operation	□	■	□	■	□	□
Can block/limit ICMP traffic (such as ping)	■ ■	■ ■	■ ■	■ ■	■ □	■ ■
Monitors modified Windows shares/start-up files/Registry	□ □ □	■ ■ ■	□ □ □	■ ■ ■	■ ■ ■	□ ■ ■
Blocks source of detected attack	■	■	■	■	□	■
Can quarantine active content in a sandbox	□	□	□	□	■	□
ALERTS						
Color-coded/audio/e-mail alerts	■ □ □	■ ■ □	■ ■ □	■ ■ ■	■ □ □	■ ■ □
Visual trace	■	■	■	□	□	■
Tray icon shows alerts/traffic/firewall disabled	■ □ ■	■ □ ■	■ □ ■	■ ■ ■	■ □ ■	■ ■ ■
Link to Web info after alert	□	□	■	□	■	■
LOGGING AND TRACING						
Logs date/severity of last attack	■ ■	■ ■	■ ■	■ ■	■ ■	■ ■
Logs number of hack attempts/network information	■ ■	■ ■	■ ■	■ ■	■ ■	■ ■
Logs malicious activity	■	■	■	■	■	■
Packet filtering/Connection-state monitoring	■ ■	■ ■	■ ■	■ ■	■ ■	■ ■
Can back-trace to hacker's origin	■	■	■	■	□	■
EXTENDED FEATURES						
Suite available/integrated interface	□ N/A	■ ■	■ ■	□ N/A	□ N/A	□ N/A
Parental control	■	■	■	□	□	□
Filters ActiveX content/Java applets/cookies	□ □ □	■ ■ □	■ ■ ■	□ □ □	■ ■ ■	■ ■ ■
Virus scanning/table updates	□ N/A	■ ■	■ ■	□ N/A	□ N/A	□ N/A
Detects malicious e-mail scripts	□	■	■	□	■	■
Blocks banner ads/pop-ups	□ □	■ ■	■ ■	□ □	□ □	■ ■

RED denotes Editors' Choice. N/A—Not applicable: This feature is found only in suites.

Source: http://common.ziffdavisinternet.com/download/0/1715/softwarefirewalls.pdf

That’s all folks!

Any questions?