Kaspersky Internet Security from Kaspersky Lab (Moscow, Russia) is a suite of impressive security products built around an extremely secure two-way Windows firewall. The product's approach to security is inventive and comprehensive. Kaspersky Internet Security includes a firewall software module that has accumulated an impressive list of awards and acquitted itself well in comparative tests at multiple independent research centers. Eugene Kaspersky, founder, studied mathematics and physics at Moscow State University when he was a high school student. The inspiration for the Kaspersky Lab business stems from Eugene's discovery of a virus that infected his computer. He analyzed the virus and then wrote a disinfection utility.

The point of getting a security suite rather than a collection of individual security components is to have all elements of your security protection working together. Kaspersky Internet Security smoothly combines antivirus, firewall, phishing protection, antispam, parental control, and more. The components all do a good job; no slackers in this bunch!

Firewall Performance : 8/10

The market for third-party personal firewall software for Windows stems from the early days of Windows XP, which included a firewall to protect from incoming traffic only. The Windows Vista

firewall filters incoming and outgoing traffic and Windows 7 and 8 include a two-way firewall with lots of good features and configuration options. In order to compete with Microsoft's ever-improving built-in Windows security, third-party vendors of firewalls for Windows are creating security suites with firewall and additional security modules. The standalone Windows firewall software market is morphing into a security-suite market. Vendors who continue to market standalone Windows firewall software products are addressing XP and Vista users as well as any Windows 7 and 8 users who haven't yet realized that the Windows 7 and 8 firewalls are perfectly good alternatives to firewall products from third-party vendors. A firewall, however, is not a complete security solution.

In keeping with the current evolution of the security market, Kaspersky Internet Security is a two-way firewall and more. The firewall monitors every network connection to the computer. When the product detects a new network, the user can assign a status based on whether it is a public network such as the internet, a local network at home or in a corporation where access to files and printers is required, or a trusted network where it is safe to allow all traffic to flow unchallenged.

Virtually every third-party firewall follows the lead of the built-in Windows Firewall by placing all of the system's ports in stealth mode. For some years now, Kaspersky has marched to a different drummer. My Kaspersky contact explained that stealthing ports "essentially slows down the operation" and caused problems for some users. "You want to ports closed," he continued. "That is where we are preventing brute force attacks."

Indeed, when I ran my usual port scans and other Web-based attacks, none actually penetrated security. It did seem odd to me, finding all ports closed but not stealthed. However, the firewall overall is advanced enough that I tend to believe Kaspersky's contention that stealthing the ports wouldn't add more security.

The firewall itself is tough. Every attempt I made to disable it using techniques that could be replicated in a malicious program was met with "Access denied." It also did a better job than most when I attacked it with 30-plus exploits generated by the Core IMPACT penetration tool. None of the exploits penetrated security, and it actively blocked over 60 percent of them, identifying many by name.

Kaspersky takes a different approach to program control than many firewall tools. Where the less-advanced firewalls query the user in order to decide which programs should have Internet

access, Kaspersky uses a system of trust levels. Known good programs from their immense database get a Trusted rating and are permitted full access to resources. Known bad programs receive an Untrusted rating and can't even launch. Unknowns are rated Low Restricted or High Restricted, depending on their behavior, with corresponding limits on access to system resources.

I saw this system in action when I tried launching a collection of leak test utilities. These utilities use the same sneaky techniques found in malware that attempts to evade program control. The antivirus component blocked one, and a couple managed to connect despite Kaspersky's protection, but most simply failed in their attempts to connect with the Internet.

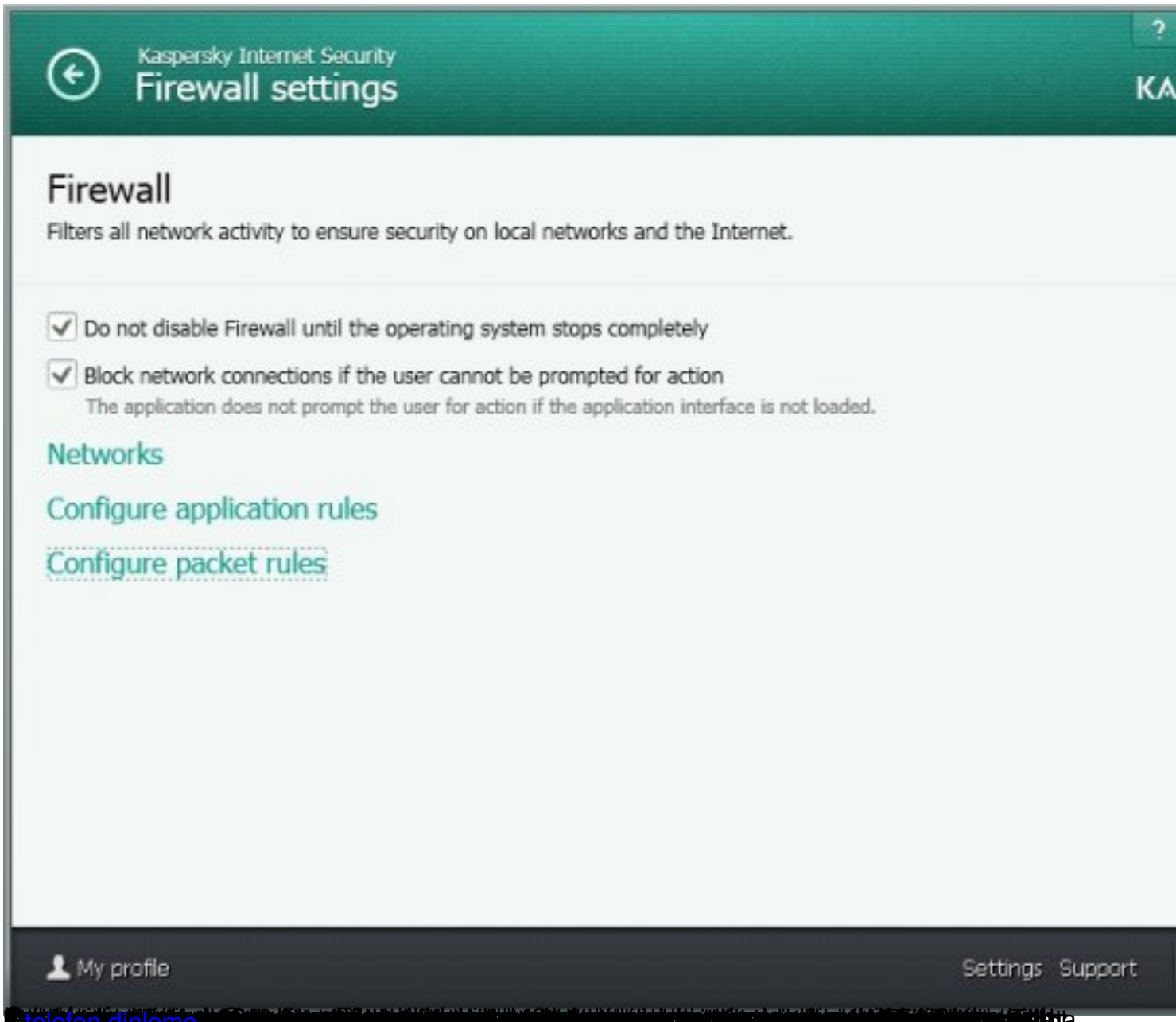
By default, the suite simply handles security events without bothering the user. I put it into Interactive mode and re-ran the leak tests; this time I got multiple very detailed reports on just what sneaky tricks the firewall detected.

I'm impressed with this firewall. It manages to fend off exploits and handle program control without bombarding the user with popup queries. Norton's firewall accomplishes the same success in its own way; few other firewalls can boast this level of built-in intelligence.


Kaspersky Internet Security
KA
Computer is protected
Threats: none
Protection components: main components enabled
Databases: up to date
License: 361 days remaining
Scan
Update
Safe Money
Reports
My profile
Settings
Support


Kaspersky Internet Security
KA
Computer is protected
Scan
Update
Safe Money
Reports
Parental Control
Network Monitor
Quarantine
Tools
Application Control
Virtual Keyboard
My profile
Settings
Support

sch.



telefon dinleme