



Firewall Test

comparatives

Firewall protection in public networks

Commissioned by CHIP

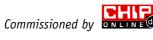
Language: English

Last Revision: 11th April 2014

www.av-comparatives.org

Contents

Test setup3Test procedure for each product.4Tested products.5Results overview.6Detailed results7Agnitum Outpost Pro 9.0.4527.670.1937 [standalone firewall program]8AhnLab V3 Internet Security 8.0.8.2.15348avast! Internet Security 2014.9.0.20119AVG Internet Security 2014.0.42599Bitdefender Internet Security 14.0.276.110BullGuard Internet Security 14.0.276.110Emsisoft Online Armor 7.0.0.1866 [standalone firewall program]11eScan Internet Security 2014 14.0.0.465112Kaspersky Internet Security 2014 14.0.0.465112Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 20142014 21.0.201Agnetarine Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	Firewall protection in public networks	3
Tested products.5Results overview.6Detailed results.7Agnitum Outpost Pro 9.0.4527.670.1937 [standalone firewall program].8AhnLab V3 Internet Security 8.0.8.2.1534.8avast! Internet Security 2014.9.0.2011.9AVG Internet Security 2014.0.4259.9Bitdefender Internet Security 14.0.276.1.0BullGuard Internet Security 14.0.1400.1507.11eScan Internet Security 2014 14.0.0.4651.12Kaspersky Internet Security 2014 14.0.0.4651.12McAfee Internet Security 2014 12.9.134.13Microsoft Windows 7 SP1 Firewall (integrated into operating system).13Symantec Norton Internet Security 2014 21.1.0.18.14ThreatTrack VIPRE Internet Security 2014.11And Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report.17	Test setup	3
Results overview	Test procedure for each product	4
Detailed results.7Agnitum Outpost Pro 9.0.4527.670.1937 [standalone firewall program].8AhnLab V3 Internet Security 8.0.8.2.1534.8avast! Internet Security 2014.9.0.2011.9AVG Internet Security 2014.0.4259.9Bitdefender Internet Security 2014 17.24.0.1033.10BullGuard Internet Security 14.0.276.1.10Emsisoft Online Armor 7.0.0.1866 [standalone firewall program].11eScan Internet Security 14.0.1400.1507.11ESET Smart Security 70.302.26.12Kaspersky Internet Security 2014 12.9.134.13Microsoft Windows 7 SP1 Firewall (integrated into operating system).13Symantec Norton Internet Security 2014 21.1.0.18.14ThreatTrack VIPRE Internet Security 2014.11Areat Free Firewall 12.0.118.000 [standalone firewall program].15Conclusion.16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	Tested products	5
Agnitum Outpost Pro 9.0.4527.670.1937 [standalone firewall program]	Results overview	6
AhnLab V3 Internet Security 8.0.8.2.15348avast! Internet Security 2014.9.0.20119AVG Internet Security 2014.0.42599Bitdefender Internet Security 2014 17.24.0.103310BullGuard Internet Security 14.0.276.110Emsisoft Online Armor 7.0.0.1866 [standalone firewall program]11eScan Internet Security 14.0.1400.150711ESET Smart Security 7.0.302.2612Kaspersky Internet Security 2014 14.0.0.465112McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201420142014 I2.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	Detailed results	7
avast! Internet Security 2014.9.0.20119AVG Internet Security 2014.0.42599Bitdefender Internet Security 2014 17.24.0.103310BullGuard Internet Security 14.0.276.110Emsisoft Online Armor 7.0.0.1866 [standalone firewall program]11eScan Internet Security 14.0.1400.150711ESET Smart Security 7.0.302.2612Kaspersky Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201411.1.0.18Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	Agnitum Outpost Pro 9.0.4527.670.1937 [standalone firewall program]	8
AVG Internet Security 2014.0.4259.9Bitdefender Internet Security 2014 17.24.0.1033.10BullGuard Internet Security 14.0.276.1.10Emsisoft Online Armor 7.0.0.1866 [standalone firewall program].11eScan Internet Security 14.0.1400.1507.11ESET Smart Security 7.0.302.26.12Kaspersky Internet Security 2014 14.0.0.4651.12McAfee Internet Security 2014 12.9.134.13Microsoft Windows 7 SP1 Firewall (integrated into operating system).13Symantec Norton Internet Security 2014 21.1.0.18.14ThreatTrack VIPRE Internet Security 2014.14Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program].15Conclusion.16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report.17	AhnLab V3 Internet Security 8.0.8.2.1534	8
Bitdefender Internet Security 2014 17.24.0.103310BullGuard Internet Security 14.0.276.110Emsisoft Online Armor 7.0.0.1866 [standalone firewall program]11eScan Internet Security 14.0.1400.150711ESET Smart Security 7.0.302.2612Kaspersky Internet Security 2014 14.0.0.465112McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201414Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	avast! Internet Security 2014.9.0.2011	9
BullGuard Internet Security 14.0.276.1.10Emsisoft Online Armor 7.0.0.1866 [standalone firewall program].11eScan Internet Security 14.0.1400.150711ESET Smart Security 7.0.302.2612Kaspersky Internet Security 2014 14.0.0.465112McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201411Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report.17	AVG Internet Security 2014.0.4259	9
Emsisoft Online Armor 7.0.0.1866 [standalone firewall program]11eScan Internet Security 14.0.1400.150711ESET Smart Security 7.0.302.2612Kaspersky Internet Security 2014 14.0.0.465112McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201411Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	Bitdefender Internet Security 2014 17.24.0.1033	10
eScan Internet Security 14.0.1400.150711ESET Smart Security 7.0.302.2612Kaspersky Internet Security 2014 14.0.0.465112McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201414Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	BullGuard Internet Security 14.0.276.1	10
ESET Smart Security 7.0.302.2612Kaspersky Internet Security 2014 14.0.0.465112McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201414Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	Emsisoft Online Armor 7.0.0.1866 [standalone firewall program]	11
Kaspersky Internet Security 2014 14.0.0.465112McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201414Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	eScan Internet Security 14.0.1400.1507	11
McAfee Internet Security 2014 12.9.13413Microsoft Windows 7 SP1 Firewall (integrated into operating system)13Symantec Norton Internet Security 2014 21.1.0.1814ThreatTrack VIPRE Internet Security 201414Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	ESET Smart Security 7.0.302.26	12
Microsoft Windows 7 SP1 Firewall (integrated into operating system)	Kaspersky Internet Security 2014 14.0.0.4651	12
Symantec Norton Internet Security 2014 21.1.0.18	McAfee Internet Security 2014 12.9.134	13
ThreatTrack VIPRE Internet Security 201414Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]15Conclusion16Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report17	Microsoft Windows 7 SP1 Firewall (integrated into operating system)	13
Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]	Symantec Norton Internet Security 2014 21.1.0.18	14
Conclusion	ThreatTrack VIPRE Internet Security 2014	14
Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report	Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]	15
	Conclusion	16
Annual 2. Contraction of a standing terms	Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report	17
Appendix 2: Explanation of networking terms	Appendix 2: Explanation of networking terms	17







Firewall protection in public networks

These days, laptops are very popular as home computers, as they take up little space and can easily be moved from room to room. Many home users will enable file sharing, in order to e.g. stream digital music to their hi-fi systems or digital photos to their TVs. Many of these users take their laptops to a public location, e.g. their local coffee house, and connect to the Internet using the establishment's WLAN. They will reasonably expect that if they define the network as public when prompted, that their computers will be secured against intrusion by other users in the public network. Business users who use a laptop as their one and only work computer may find themselves in a similar situation, with the additional possibility that their machines may have been configured to allow remote control using Microsoft's Remote Desktop.

The purpose of this test is to determine whether common third-party firewalls, both standalone and integrated into Internet security suites, actually provide basic inbound access control for laptop users who switch between private and public networks. Please note that the scope of the test is obviously very limited, and that a good score here does not by any means indicate that a product provides perfect network security.

The test was conducted in January 2014, using product versions available as at 13th January 2014. This test was not sponsored in any way. It was commissioned by CHIP magazine¹.

We hope that the weaknesses uncovered in this test will be rectified by the respective manufacturers of the affected products as soon as possible. Unfortunately, we have to point out that a similar test, conducted as part of AV-Comparatives' 2012 Summary Report, found similar weaknesses, which have still not been improved. Please see Appendix 1 for details.

NB: for readers less familiar with networking terms, these are explained in Appendix 2.

Test setup

The test device is a Lenovo ThinkPad Twist running a fully up-to-date Microsoft Windows 7 Professional SP1 64-bit. The base image, without any third-party security software, is configured to allow file sharing and Remote Desktop access in private networks, but not public ones. This means that in a private network, i.e. defined as "Home" or "Work" in Windows Network and Sharing Center (WNSC), it is possible to do the following:

- Ping the test PC using both its hostname and IP address, with both IPv4 and IPv6;
- Access a shared folder, using both the hostname and IPv4 address, then open, edit and save a document in it;
- Remotely control the test PC via Remote Desktop, using the hostname, IPv4 address and IPv6 address.

However, if the network type is set to Public in WNSC, all the forms of access noted above are blocked by Windows Firewall.

¹ <u>http://www.chip.de/artikel/Firewall-Test-Kostenlose-und-kostenpflichtige-Tools-fuer-Windows_32878576.html</u>



Test procedure for each product

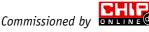
The test PC is connected to the WLAN/Internet using a connection that is defined as Work in WNSC. The test version of each product, available as at 13th January 2014, is installed using default settings, and the test PC restarted. If the product itself prompts the user to define the current network type, the Private/Trusted option is chosen. If the product has an update function, this is run. We check to see that the product has registered in Windows Action Center as the system firewall, and that both Action Center and the product itself show it as working properly. From a second PC, we then check for connectivity in the existing private network as follows:

Ping hostname -4 Ping hostname -6 Ping IPv4 address Ping IPv6 address File share hostname File share IPv4 address Remote Desktop (RDP) hostname Remote Desktop (RDP) IPv4 address Remote Desktop (RDP) IPv6 address

We would expect all forms of access to be possible, to allow maximum control and functionality of the test PC in the private network. We then shut down the PC, switch off the WLAN router to which it had been connected, and then start the PC again. Once it is running, we connect it to a different WLAN, which we define as Public in WNSC, using the dialog box shown below:



If the product displays its own prompt for the network type, we set this to the equivalent, e.g. "Public" or "Untrusted". However, we do not make any other changes to the product's configuration.





This procedure simulates the average laptop user moving from a home/office environment to a public network in a café, airport or hotel. Once the PC is connected to the new, public WLAN, we run the same connectivity tests as for the private network. This time, we would expect all connection attempts to fail, as the computer should be protected from all outside external detection and access in the public network. One of the problems we have found with some of the firewalls tested is that they require proactive manual configuration by the user in order to provide suitable protection in public networks. That is to say, when the Windows network connection prompt asks the user to define the network as Home, Work or Public, the firewall neither adopts these settings automatically nor displays its own prompt. In this case, the firewall stays set to private mode and allows pinging, file sharing and Remote Desktop access to continue. In cases where this happens, we change the firewall's own settings manually (where possible), and test again, to see if this protects the computer appropriately.

We note how the firewall software reacts when the new network is joined. In some cases, it will automatically adopt the same setting that the user chooses in the WNSC prompt; we find this ideal, as it configures the firewall correctly without any additional user action being necessary. Alternatively, the firewall may display its own similar prompt for the user to define the network type, which we find perfectly acceptable. In some cases, however, the firewall displays neither its own prompt nor coordinates with the WNSC prompt; the only way the user can ensure appropriate protection in a public network is by proactively manually changing the firewall's own settings. We feel this is entirely unsuitable for an Internet security suite designed for use by non-experts. Finally, having connected to a network and defined it as Work in WNSC (and at the firewall's own prompt, if there is one), we then change the setting to Public in WNSC, to simulate a situation in which the user makes a mistake by clicking the wrong button when connecting, and then immediately rectifies it by changing the network type in WNSC. Ideally, the firewall should either change automatically, or again display its own prompt. Readers should note that Windows can and should be configured to demand a username and password before allowing file-sharing or Remote Desktop access. However, even if this is the case, a lack of firewall protection makes it much quicker and easier for an attacker to gain access to the PC.

Tested products

Two additional products were tested specifically for CHIP and their results can be seen in the CHIP article². The products included in this test report are:

- Agnitum Outpost Pro 9.0
- AhnLab V3 Internet Security 8.0
- avast! Internet Security 2014
- AVG Internet Security 2014
- Bitdefender Internet Security 2014
- BullGuard Internet Security 14.0
- Emsisoft Online Armor 7.0
- eScan Internet Security 14.0

- ESET Smart Security 7.0
- Kaspersky Internet Security 2014
- McAfee Internet Security 2014
- Microsoft Windows 7 SP1
- Symantec Norton Internet Security 2014
- ThreatTrack VIPRE Internet Security 2014
- Zone Alarm Free Firewall 12.0

² <u>http://www.chip.de/artikel/Firewall-Test-Kostenlose-und-kostenpflichtige-Tools-fuer-Windows_32878576.html</u>



Results overview



Please note that these results refer only to this particular test, and not to any other indicators of firewall security. The table shows how the product behaves without proactive manual configuration.

Product	Protection provided in public networks:		
Floduct	Ping	File Sharing	Remote Desktop
Agnitum Outpost Pro 9.0	++	+	_
AhnLab V3 Internet Security 8.0	-	-	_
avast! Internet Security 2014	++	++	++
AVG Internet Security 2014	++	++	++
Bitdefender Internet Security 2014	++	++	+
BullGuard Internet Security 14.0	++	++	++
Emsisoft Online Armor 7.0	_	-	_
eScan Internet Security 14.0	-	-	-
ESET Smart Security 7.0	+	++	+
Kaspersky Internet Security 2014	++	++	++
McAfee Internet Security 2014	++	++	++
Microsoft Windows 7 SP1	++	++	++
Symantec Norton Internet Security 2014	+	+	+
ThreatTrack VIPRE Internet Security 2014	+	+	+
Zone Alarm Free Firewall 12.0	+	+	+

Key to ratings

++ : Complete protection. The product protects the computer completely against all three forms of access, regardless of whether the computer name, IPv4 address or IPv6 address is used.

+ : Partial protection. The product protects the computer only in some cases. For example, it may protect against attempted access when the computer name is used, but not if an IP address is used.

- : No protection. The product allows access using computer name, IPv4 address and IPv6 address.

Notes

Being able to **ping** a computer over the network does not in itself allow an attacker to steal data or control the computer in any way. However, it does allow the attacker to identify the computer on the network, which is an important first step in the process of hacking into it.

If hackers can access a computer's **file share** in a public network, they can read, copy and possibly even delete any files in the shared folder. It is obviously very important that a file share be protected against outside access in a public network.

Remote Desktop allows remote control of a computer over the network. An attacker with Remote Desktop access effectively has complete control of the computer, so it is very important to prevent this. However, it should be noted that the feature is only available in Business/Professional versions of Windows (not the Home/Standard versions), and that it is disabled by default.



Detailed results

The reports for individual products show in detail which forms of access (if any) were allowed in both private and public networks. Ideally, a firewall should allow all forms of access in private networks, but none in public networks. Some products blocked some forms of access, typically Ping, in private networks, which we consider to be an irritation. One product prompts the user to state whether incoming access should be allowed; we regard this as fine for computer enthusiasts and professionals, but not ideal for typical users, who may not understand what is happening, and will thus not be able to answer appropriately.

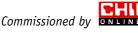
For all products, there is a column in the results table entitled *Public (Windows)*. This shows how the product reacts without proactive manual configuration of the product's settings. As noted in the methodology above, we select Public in the Windows Network and Sharing Center prompt when joining the new network; if the product additionally displays its own prompt for network type, we also select Public or equivalent here. For some products, a third and possibly even a fourth column is shown, with the name in quotes, e.g. "NetBIOS blocked". In the event that the firewall does not automatically provide complete protection, we attempt to manually configure the program for a public network, and then test again to see if it then protects more effectively. In one case, there were two possible settings which seemed suitable, so we tried both. Some other programs had only one possible setting, and in others there were no options available at all. The column heading shown in quotes represents the network type defined in the product itself.

Key to colour coding in tables

FAIL: Product fails to protect the computer in public network	PROMPT: Product asks user whether to allow access	IRRITATION: product blocks access in private network	PASS: product behaves exactly as it should do
---	---	--	--

The tests described here are very basic inbound-firewall tests and can easily be repeated and verified by anyone with two laptops and access to a public and a private network.

Since the report was first published on the CHIP website, some of the manufacturers have admitted to the issues with their firewalls as described here, and have taken steps to rectify them in future releases.





	Private	Public (Windows)	"NetBIOS blocked"
Ping hostname -4	IRRITATION	PASS	PASS
Ping hostname -6	IRRITATION	PASS	PASS
Ping IPv4 address	IRRITATION	PASS	PASS
Ping IPv6 address	IRRITATION	PASS	PASS
File share hostname	PASS	PASS	FAIL
File share IPv4 address	PASS	FAIL	PASS
RDP hostname	PASS	FAIL	FAIL
RDP IPv4 address	PASS	FAIL	FAIL
RDP IPv6 address	PASS	FAIL	FAIL

Agnitum Outpost Pro 9.0.4527.670.1937 [standalone firewall program]

Agnitum's firewall may prove a minor irritation to advanced users by blocking all forms of ping in private networks. More importantly, it allows both file sharing and Remote Desktop access in public networks, even when the setting "NetBIOS blocked" is selected in the program's own configuration options.

A screen video of the test can be seen at http://youtu.be/XsUaQ7GkK74

	Private	Public (Windows)	"Mobile (Wireless LAN)"	"Direct (No firewall)"
Ping hostname -4	PASS	FAIL	PASS	PASS
Ping hostname -6	PASS	FAIL	FAIL	FAIL
Ping IPv4 address	PASS	FAIL	PASS	PASS
Ping IPv6 address	PASS	FAIL	FAIL	PASS
File share hostname	PASS	FAIL	FAIL	FAIL
File share IPv4 address	PASS	FAIL	FAIL	FAIL
RDP hostname	PASS	FAIL	FAIL	FAIL
RDP IPv4 address	PASS	FAIL	FAIL	FAIL
RDP IPv6 address	PASS	FAIL	PASS	PASS

AhnLab V3 Internet Security 8.0.8.2.1534

After installation, AhnLab's firewall correctly allowed all types of access in the existing private network. On connection to a public network, it neither co-ordinated with the WNSC setting nor produced its own prompt, leaving the computer exposed. Even when we manually changed the firewall's own configuration, both of the two possible settings still allowed file-sharing and Remote Desktop access. We note that the suite's setup wizard makes installation of the firewall optional, and that even if it is installed, it is disabled by default and Windows Firewall is used instead.

A screen video of the test can be seen at <u>http://youtu.be/g2_YV0gqo7Q</u>





	Private	Public (Windows)
Ping hostname -4	PASS	PASS
Ping hostname -6	PASS	PASS
Ping IPv4 address	PASS	PASS
Ping IPv6 address	PASS	PASS
File share hostname	PASS	PASS
File share IPv4 address	PASS	PASS
RDP hostname	PASS	PASS
RDP IPv4 address	PASS	PASS
RDP IPv6 address	PASS	PASS

avast! Internet Security 2014.9.0.2011

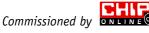
By default, avast! Internet Security does not disable Windows Firewall, and so both firewalls run in parallel. In this configuration, all forms of access are allowed in private networks and blocked in public networks, which is exactly as it should be.

We also tested Avast's firewall on its own, with Windows Firewall disabled, and found the results to be identical. Users should however note that in this case, if the network type is changed in Windows Network and Sharing Center, this also needs to be changed manually in the Avast Firewall settings.

	Private	Public (Windows)
Ping hostname -4	PASS	PASS
Ping hostname -6	PASS	PASS
Ping IPv4 address	PASS	PASS
Ping IPv6 address	PASS	PASS
File share hostname	PASS	PASS
File share IPv4 address	PASS	PASS
RDP hostname	PASS	PASS
RDP IPv4 address	PASS	PASS
RDP IPv6 address	PASS	PASS

AVG Internet Security 2014.0.4259

In our test, AVG's firewall performed identically to Windows Firewall, allowing all forms of access in private networks but blocking them all in public LANs. Co-ordination with Windows Network and Sharing Center is perfect; if the network type is changed in WNSC, AVG's settings automatically follow, and vice versa.





Bitdefender Internet Security 2014 17.24.0.1033

	Private	Public (Windows)
Ping hostname -4	PASS	PASS
Ping hostname -6	PASS	PASS
Ping IPv4 address	PASS	PASS
Ping IPv6 address	PASS	PASS
File share hostname	PASS	PASS
File share IPv4 address	PASS	PASS
RDP hostname	PASS	PASS
RDP IPv4 address	PASS	FAIL
RDP IPv6 address	PASS	PASS

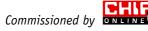
Bitdefender's firewall performed perfectly in almost all aspects of the test, and co-ordinated its settings perfectly with those of Windows Network and Sharing Center. However, in a public network, it allowed Remote Desktop access using the IPv4 address.

A screen video of the test can be seen at <u>http://youtu.be/KLU5CPzz9_g</u>

BullGuard Internet Security 14.0.276.1

	Private	Public (Windows)
Ping hostname -4	IRRITATION	PASS
Ping hostname -6	IRRITATION	PASS
Ping IPv4 address	IRRITATION	PASS
Ping IPv6 address	IRRITATION	PASS
File share hostname	PASS	PASS
File share IPv4 address	PASS	PASS
RDP hostname	PASS	PASS
RDP IPv4 address	PASS	PASS
RDP IPv6 address	IRRITATION	PASS

In the public network, BullGuard correctly blocked all forms of access. It was in fact a little overprotective, as it also blocked all forms of pinging, and Remote Desktop access using IPv6 address, in private networks too. However, this would be very unlikely to affect standard users. We note that changes to the network type in Windows Network and Sharing Center are perfectly co-ordinated with BullGuard's own firewall settings.





	Private	Public (Windows)
Ping hostname -4	IRRITATION	FAIL
Ping hostname -6	PASS	FAIL
Ping IPv4 address	IRRITATION	FAIL
Ping IPv6 address	PASS	FAIL
File share hostname	IRRITATION	FAIL
File share IPv4 address	IRRITATION	FAIL
RDP hostname	PASS	FAIL
RDP IPv4 address	PASS	FAIL
RDP IPv6 address	PASS	FAIL

Emsisoft Online Armor 7.0.0.1866 [standalone firewall program]

In our test, Emsisoft Online Armor failed to prevent any form of access in our public network, despite the fact that it showed its own connection dialog box, with which we were able to confirm that the LAN concerned should not be trusted.

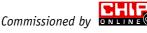
A screen video of the test can be seen at http://youtu.be/vStwd1XZtfl

	Private	Public (Windows)	"Blocked"
Ping hostname -4	PASS	FAIL	PASS
Ping hostname -6	PASS	FAIL	FAIL
Ping IPv4 address	PASS	FAIL	PASS
Ping IPv6 address	PASS	FAIL	FAIL
File share hostname	PASS	FAIL	FAIL
File share IPv4 address	PASS	FAIL	PASS
RDP hostname	PASS	FAIL	FAIL
RDP IPv4 address	PASS	FAIL	PASS
RDP IPv6 address	PASS	FAIL	FAIL

eScan Internet Security 14.0.1400.1507

eScan's firewall correctly allowed all forms of access in our private network. However, when we connected to a public network, it neither co-ordinated with Windows Network and Sharing Center nor displayed its own prompt, leaving the computer unprotected. Even when we manually changed the network type to "Blocked" in the suite's own settings, file-sharing and Remote Desktop access were still possible.

A screen video of the test can be seen at http://youtu.be/yo7DX3U7TQA





	Private	Public (Windows)
Ping hostname -4	PASS	PASS
Ping hostname -6	IRRITATION	PASS
Ping IPv4 address	PASS	PASS
Ping IPv6 address	PASS	FAIL
File share hostname	PASS	PASS
File share IPv4 address	PASS	PASS
RDP hostname	PASS	PASS
RDP IPv4 address	PASS	PASS
RDP IPv6 address	PASS	FAIL

ESET Smart Security 7.0.302.26

We found two minor ping-related flaws in ESET's firewall in our test: pinging the hostname with IPv6 in a private network is not possible, while pinging the IPv6 address in a public network does work. Additionally, Remote Desktop access using the IPv6 address is possible in a public network. We note that it is possible to completely deactivate the ESET firewall in the suite's settings, neatly removing it from the program interface, and allowing Windows firewall to be used without any alerts or error messages.

A screen video of the test can be seen at http://youtu.be/RhWQW_sLwNM

	Private	Public (Windows)
Ping hostname -4	PASS	PASS
Ping hostname -6	PASS	PASS
Ping IPv4 address	PASS	PASS
Ping IPv6 address	PASS	PASS
File share hostname	PASS	PASS
File share IPv4 address	PASS	PASS
RDP hostname	PASS	PASS
RDP IPv4 address	PASS	PASS
RDP IPv6 address	PASS	PASS

Kaspersky Internet Security 2014 14.0.0.4651

Kaspersky Lab's firewall was exemplary when it came to allowing access in private networks but blocking it in public LANs. Users should be aware that if the network type is changed in Windows Network and Sharing Center, it also needs to be changed manually in the suite's settings.





	Private	Public (Windows)	
Ping hostname -4	IRRITATION	PASS	
Ping hostname -6	IRRITATION	PASS	
Ping IPv4 address	IRRITATION	PASS	
Ping IPv6 address	IRRITATION	PASS	
File share hostname	PASS	PASS	
File share IPv4 address	PASS	PASS	
RDP hostname	PASS	PASS	
RDP IPv4 address	PASS	PASS	
RDP IPv6 address	PASS	PASS	

McAfee Internet Security 2014 12.9.134³

The firewall in McAfee Internet Security co-ordinates perfectly with Windows Network and Sharing Center, so setting or changing the network type in one automatically configures the same setting in the other. All forms of access were blocked in our public network, as they should be. There is one very minor flaw, namely that no form of ping will work in a private network, although this would not affect standard users.

Microsoft Windows 7 SP1 Firewall (integrated into operating system)

	Private	Public (Windows)	
Ping hostname -4	PASS	PASS	
Ping hostname -6	PASS	PASS	
Ping IPv4 address	PASS	PASS	
Ping IPv6 address	PASS	PASS	
File share hostname	PASS	PASS	
File share IPv4 address	PASS	PASS	
RDP hostname	PASS	PASS	
RDP IPv4 address	PASS	PASS	
RDP IPv6 address	PASS	PASS	

Microsoft's Windows Firewall, built into Windows 7, allows all forms of access in private networks, but blocks them all in public networks. We find it simple and effective, and it represents the baseline against which third-party firewalls are measured.



³ Firewall version: 13.8.706

Symantec Norton Internet Security 2014 21.1.0.18

	Private	Public (Windows)	
Ping hostname -4	IRRITATION	PASS	
Ping hostname -6	PASS	FAIL	
Ping IPv4 address	IRRITATION	PASS	
Ping IPv6 address	PASS	FAIL	
File share hostname	PASS	FAIL	
File share IPv4 address	PASS	PASS	
RDP hostname	PASS	FAIL	
RDP IPv4 address	PASS	PASS	
RDP IPv6 address	PASS	FAIL	

In our test, Norton's firewall would not allow pinging with IPv4 in a private network. More importantly, it did not prevent file-sharing or Remote Desktop access in our public network.

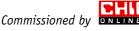
A screen video of the test can be seen at <u>http://youtu.be/mfuX-JYZGgs</u>

	Private	Public (Windows)	
Ping hostname -4	PASS	PASS	
Ping hostname -6	PASS	FAIL	
Ping IPv4 address	PASS	PASS	
Ping IPv6 address	PASS	FAIL	
File share hostname	PASS	FAIL	
File share IPv4 address	PASS	PASS	
RDP hostname	PASS	FAIL	
RDP IPv4 address	IRRITATION	PASS	
RDP IPv6 address	PASS	FAIL	

ThreatTrack VIPRE Internet Security 2014

VIPRE's firewall exhibits one minor inconvenience for business users, in that Remote Desktop access is not possible using an IPv4 address in a private network. It also has two major flaws, in that both file sharing and Remote Desktop access are possible in public networks.

A screen video of the test can be seen at <u>http://youtu.be/LSVjge_wsCk</u>





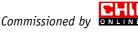


	Private	Public (Windows)	"Public" (Zone Alarm)
Ping hostname -4	PASS	PASS	PASS
Ping hostname -6	PASS	PASS	FAIL
Ping IPv4 address	PASS	PASS	PASS
Ping IPv6 address	PASS	FAIL	FAIL
File share hostname	PASS	FAIL	FAIL
File share IPv4 address	PASS	PASS	PASS
RDP hostname	PASS	FAIL	PASS
RDP IPv4 address	PASS	PASS	PASS
RDP IPv6 address	PASS	FAIL	FAIL

Zone Alarm Free Firewall 12.0.118.000 [standalone firewall program]

Zone Alarm Free Firewall correctly allowed all forms of access in a private network. When we connected to a public network, it did block some forms of access, including file share and Remote Desktop using IPv4 address. However, both the file share and Remote Desktop could still be accessed using the hostname. Changing the network type in the suite's own settings blocked two further types of access, but still allowed file sharing using hostname and Remote Desktop using IPv6 address.

A screen video of the test can be seen at http://youtu.be/2wqFS92X6iY



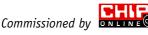


Conclusion

Of twelve Internet security suites tested, only five provided full protection in public networks. Another two allowed Remote Desktop connections to be made using IP addresses; whilst this does not affect users with Home editions of Windows, it could represent a significant security risk to business users with Professional, Business or Enterprise versions of Windows. One further suite can provide full protection if it is manually configured (and the PC restarted after connecting to the network), but this can only be done by advanced users with an understanding of TCP/IP networking. For the average user, the suite's firewall effectively allows all forms of access in public networks. The remaining four allow both file sharing and Remote Desktop access in public networks, even in cases where the LAN has been registered as public in the suite's own settings.

Six out of the seven manufacturers whose suites fail to provide complete protection make a standalone antivirus program without firewall, which can usually be purchased more cheaply than the corresponding full Internet security suite. However, most manufacturers claim in their advertising that the more expensive suite will protect the user's computer better than the simple antivirus program. This test indicates that half of the security vendors are actually charging more money for a product that may provide significantly less security in some situations, and that users would do better to buy the simple antivirus program and rely on Windows Firewall to prevent unauthorised intrusion. We note that a number of major vendors are nowadays not including their own firewalls in their security suites, but relying on Windows Firewall instead, as this provides suitable protection and is easy to configure.

In the case of the four standalone firewalls, all allowed both file sharing and Remote Desktop access in public networks, even in cases where the network has been set to Public/Untrusted in the program itself. We would suggest that enthusiasts who use such programs should consider whether the advanced features provided in these programs make up for the lack of basic protection in public networks.





Appendix 1: Firewall problems noted in AV-Comparatives' 2012 Summary Report

- **Bitdefender**: Very similar problem reported, with Remote Desktop possible using IPv6 address.
- **eScan**: A smaller problem was reported, Remote Desktop using IP address possible.
- ThreatTrack VIPRE: Very similar problem, all forms of access possible with IPv6.

Appendix 2: Explanation of networking terms

Ping is a command made using Windows' Command Prompt. It essentially sends a message along the lines of "can you hear me" from one computer to another over a network (which could be a local area network or the Internet). If the receiving computer is online and configured to respond, it will send back a message which means "receiving you loud and clear". An example is shown below:

C:\Windows\system32>ping user-pc
Pinging user-pc [10.1.43.12] with 32 bytes of data:
Reply from 10.1.43.12: bytes=32 time<1ms TTL=128
Reply from 10.1.43.12: bytes=32 time<1ms TTL=128
Reply from 10.1.43.12: bytes=32 time<1ms TTL=128
Reply from 10.1.43.12: bytes=32 time=2ms TTL=128
Ping statistics for 10.1.43.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = Oms, Maximum = 2ms, Average = Oms
Hiniman Choy Haximan Zhoy Hvorago Cho

In the example above, the computer being pinged has the hostname (or Computer Name in Windows jargon) "user-pc". It sends back 4 replies (the standard), showing that it is online and configured to reply to ping requests. This is an important diagnostic tool in network configuration.

The reply includes the IPv4 address, a unique identifying number for the computer on the network, which in this case is 10.1.43.12. It is possible to ping a computer using the hostname, IPv4 address or IPv6 address (e.g. fe80::6905:ec41:ad0e:22ec%3). Windows Vista, 7 and 8 operating systems use both IPv4 and IPv6, so a computer running such an OS will typically have both an IPv4 and an IPv6 address in a local area network.

Both the IPv4 and IPv6 addresses can be used to ping a computer, i.e. the command can be "Ping user-pc", "ping 10.1.43.12" or "ping fe80::6905:ec41:ad0e:22ec%3". Alternatively, the hostname alone can be specified ("ping user-pc"); or the hostname can be used, and the version of the Internet Protocol specified ("ping user-pc -4" or "ping user-pc -6).

File sharing allows a file (e.g. document, picture, video or music file) on one computer to be opened/read/viewed/played on another computer on the same network. File sharing can be configured so that shared files can also be edited or deleted from another computer.

Remote Desktop is a feature available in Business/Professional/Enterprise versions of Windows XP, Vista, 7 and 8, which allows the computer to be remotely controlled from another computer on the local area network, or even over the Internet. It allows the remote user to do anything that a local user can do with a mouse and keyboard, including printing and shutting down the computer.



Copyright and Disclaimer

This publication is Copyright © 2014 by AV-Comparatives ®. Any use of the results, etc. in whole or in part, is ONLY permitted if the explicit written agreement of the management board of AV-Comparatives, is given prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (April 2014)

