Nessus and Antivirus

January 31, 2014

(Revision 4)

Table of Contents

Introduction **3**
Standards and Conventions 3
Overview **3**
A Note on SCAP Audits 4
Microsoft Windows Defender **4**
Kaspersky Internet Security 2012 ..... **4**
AVG 2012 ..... **7**
Norton Internet Security 2012 ..... **10**
Norton 360 ..... **14**
Panda Internet Security 2012 ..... **18**
Trend Micro Titanium Maximum Security 2012 ..... **20**
Symantec Endpoint Protection **21**
Select a Policy 21
Review Scan Results 21
Review SEP Client Security Log 22
Find Intrusion Policy Signature 22
Research Intrusion Policy Signature Details 22
Consider Policy Change for the Signature 22
Hewlett-Packard NIC Teaming **22**
About Tenable Network Security **22**

Introduction

This document describes Tenable Network Security's Nessus vulnerability scanner and how it integrates with commercial antivirus solutions. Please email any comments and suggestions to support@tenable.com.

This document specifically covers Nessus integration with antivirus software. Installation, configuration, and management of Nessus is covered by other documents.

A basic understanding of Nessus functionality, antivirus software, and system administration is assumed.

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix **pwd** command:

```
# pwd
/opt/sc4/daemons
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Overview

By nature, security software typically is focused on restricting access to resources. To perform this and achieve a better security posture, products will seek to control all aspects of the system they are installed on, at the lowest level possible. This often has a side-effect of hindering legitimate programs as well. Whether it is through black-listing processes and an overly aggressive signature that matches an internal Windows program, or through white-listing and not including all legitimate services on a Unix system, the end result is an inconvenience for the user.

Vulnerability scanners utilize a series of checks to test for the presence of software errors that may lead to an unauthorized person gaining increased privileges. To do this, the checks must often perform part or all of an attack and gauge the server's response to determine success. As such, these vulnerability checks frequently look like the same attacks that a malicious person would use; therefore security software blocks the requests in an effort to protect the system.

This document outlines how several popular security software packages interact with Nessus, and provides tips or workarounds to allow the software to better co-exist without compromising your security or hindering your vulnerability scanning efforts.

The presence of antivirus software, regardless of configuration, may block some traffic generated by Nessus. Because the traffic is blocked quickly, Nessus will not necessarily receive a response indicating it was blocked. This may result in incomplete vulnerability scans. Further, the blocked or dropped traffic may give the appearance that Nessus actually runs faster in the presence of antivirus software. The presence of antivirus software does **not** enhance the speed of Nessus.

A Note on SCAP Audits

One audit, for SCAP compliance, requires sending an executable to the remote host. For systems that run security software (e.g., McAfee Host Intrusion Prevention or some Antivirus software), it may block or quarantine the executable required for auditing. For those systems, an exception must be made for the either the host or the executable sent.

Microsoft Windows Defender

Microsoft Defender (formerly Microsoft AntiSpyware) is a security product integrated into Microsoft Windows operating systems. It is designed to detect, prevent, and remove malware. Like many antivirus products, Microsoft Defender will frequently flag security software as suspicious. Based on Microsoft's implementation and policy for software classification, Microsoft Defender is **not well suited** to the presence and operation of Nessus 5.

With Nessus, scanning a remote system may prompt warnings that suggest a virus or malware is present:

```
Wed Jul 11 16:59:06 2012        3004    Microsoft-Windows-Windows Defender      N/A
N/A     Warning srv.name        None            Windows Defender Real-Time Protection
agent has detected changes. Microsoft recommends you analyze the software that made these
changes for potential risks. You can use information about how these programs operate to
choose whether to allow them to run or remove them from your computer.  Allow changes
only if you trust the program or the software publisher. Windows Defender can't undo
changes that you allow.   For more information please see the following:  Not Applicable
Scan ID: {61536928-ED69-482F-8E18-5BD623314F5C}    User: DOM\user    Name: Unknown    ID:
Severity ID:     Category ID:     Path Found:
process:pid:37220;service:tenable_mw_scan;file:C:\Windows\tenable_mw_scan_142a90001fb65e0
beb1751cc8c63edd0.exe    Alert Type: Unclassified software    Detection Type:       7931
```

Based on the Defender warnings, the Real Time Protection triggers on the actions taken by the executable (i.e., vulnerability scanning activity), not the executable itself. Unfortunately, Microsoft does not provide a mechanism to control executable properties or location via Group Policy. This can only be done if the software is upgraded from Defender to Forefront Client Security.

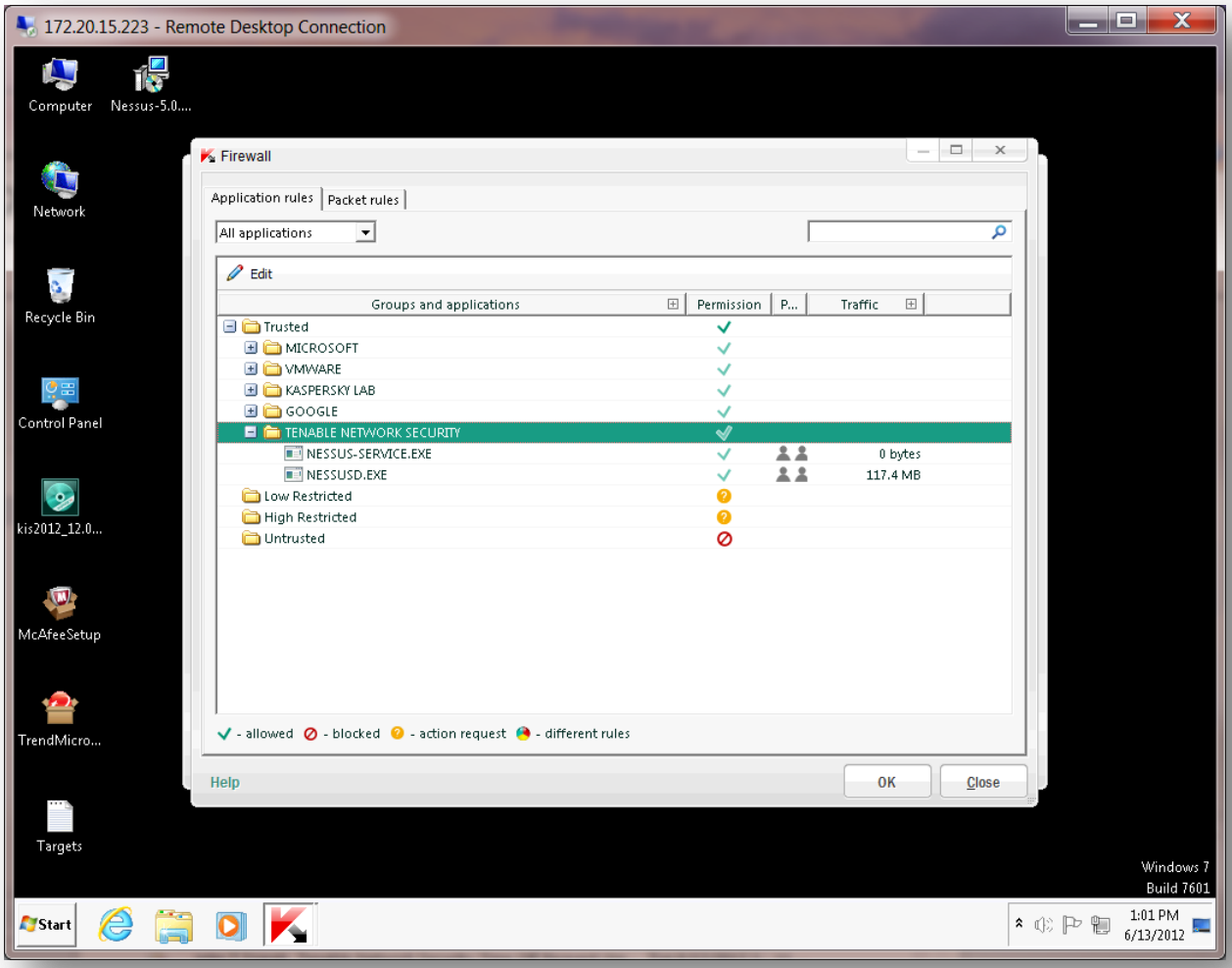
Microsoft KB 944019 and their Real-Time Protection FAQ have more information.

Kaspersky Internet Security 2012

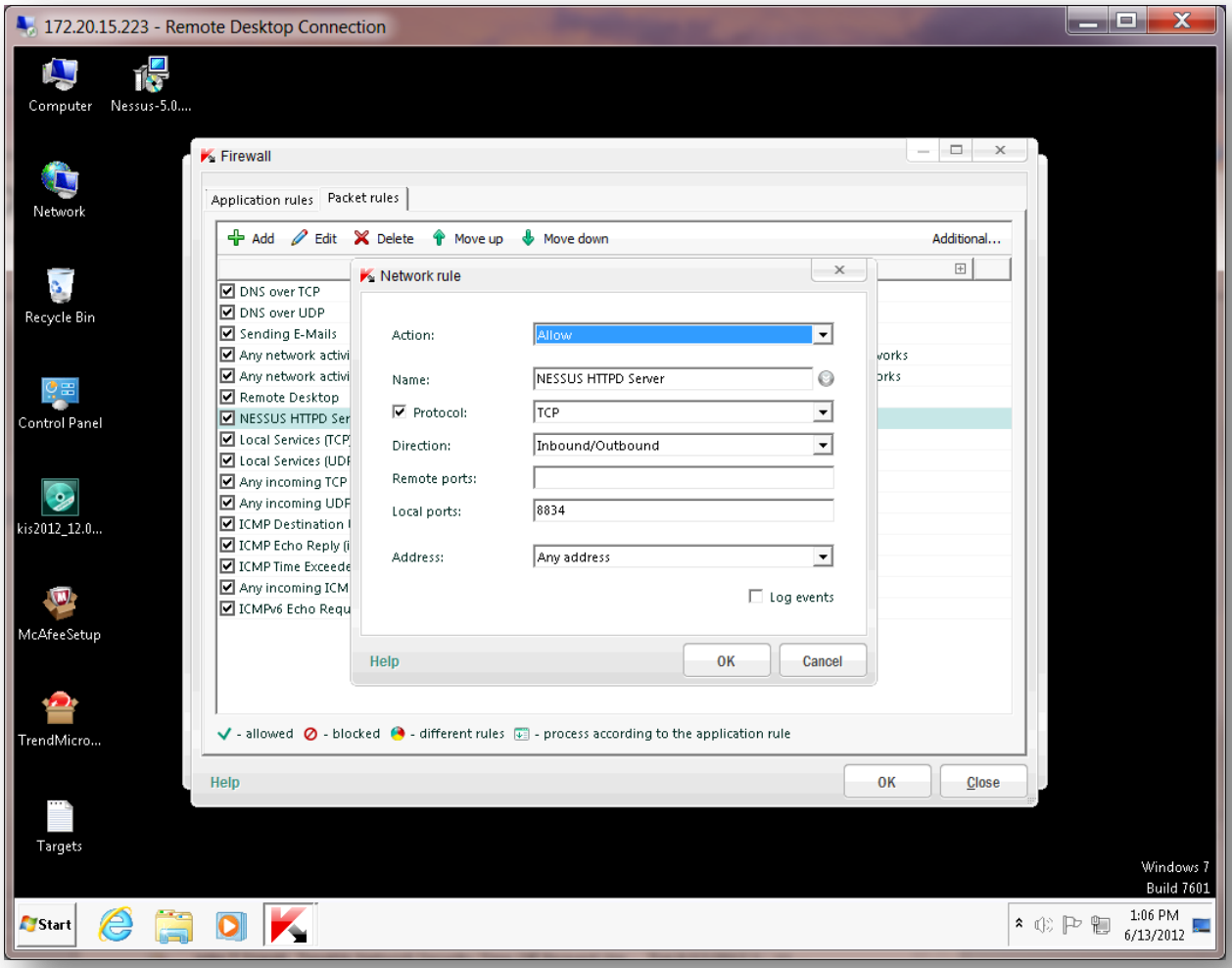
Kaspersky Internet Security (KIS) is a suite of tools from Kaspersky Labs that includes antivirus, a two-way firewall, information protection, parental controls, and more. The antivirus and firewall components of any security software have the potential to adversely affect vulnerability scanners, both in performance and by limiting select traffic.

Tenable's internal testing has determined that Kaspersky Internet Security 2012 **is well adapted** to the presence and operation of Nessus 5. Both programs can be installed, regardless of the order, and no modifications are required for either software to operate normally. The presence of KIS-2012 did not impact Nessus scan times.

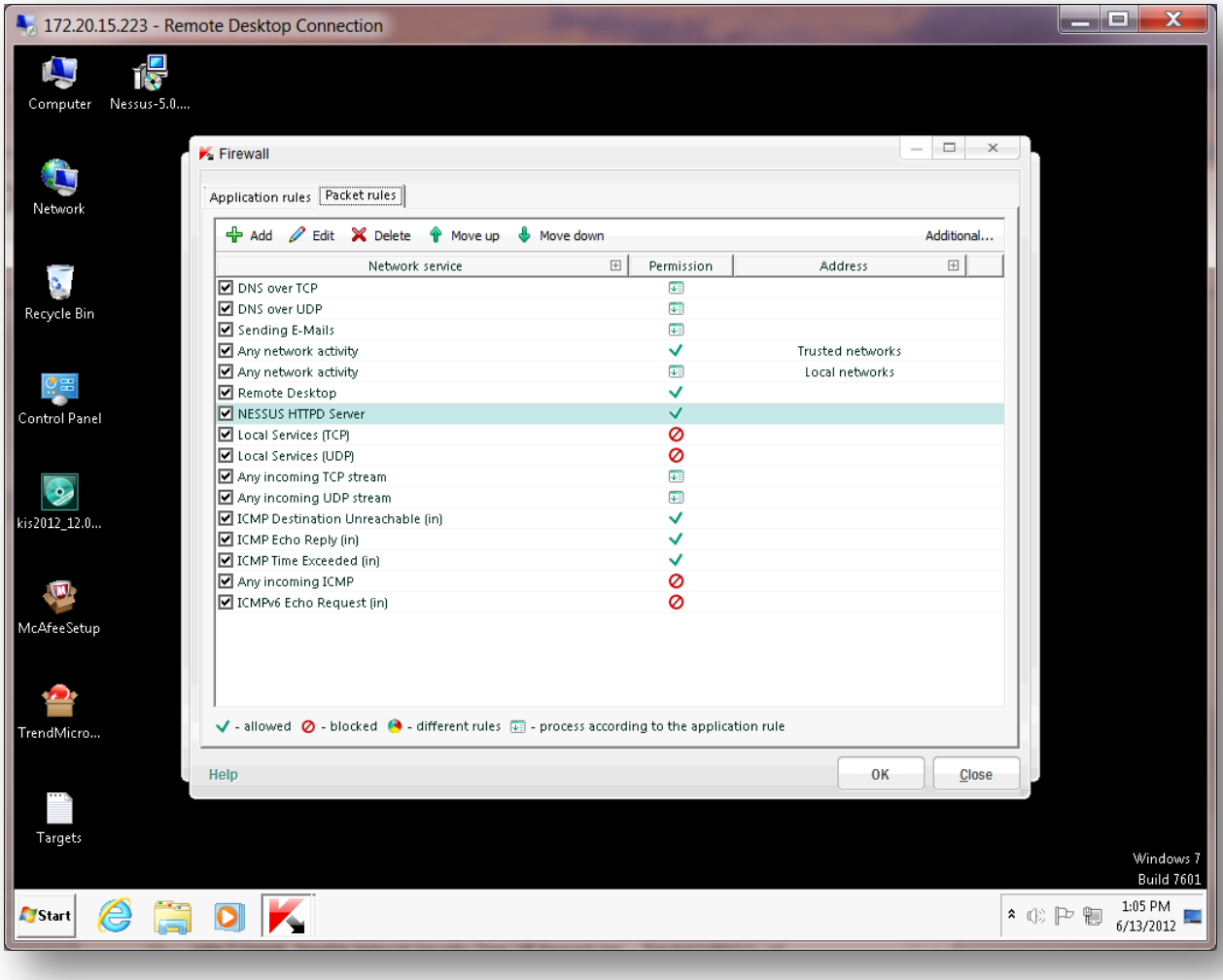
KIS-2012 creates rules to allow Nessus to operate. These special rules provide full network access to **`nessus.exe`** and **`nessus-service.exe`** in the 'Trusted' section of its Application Rules screen:



To allow remote access to Nessus, modify the Remote Desktop rules and add a rule for the Nessus web server on port 8834 (or an alternate port if configured differently). This will allow full access to the Nessus web server.



Once the rule is added, KIS-2012 will show the Nessus HTTPD server as allowed:

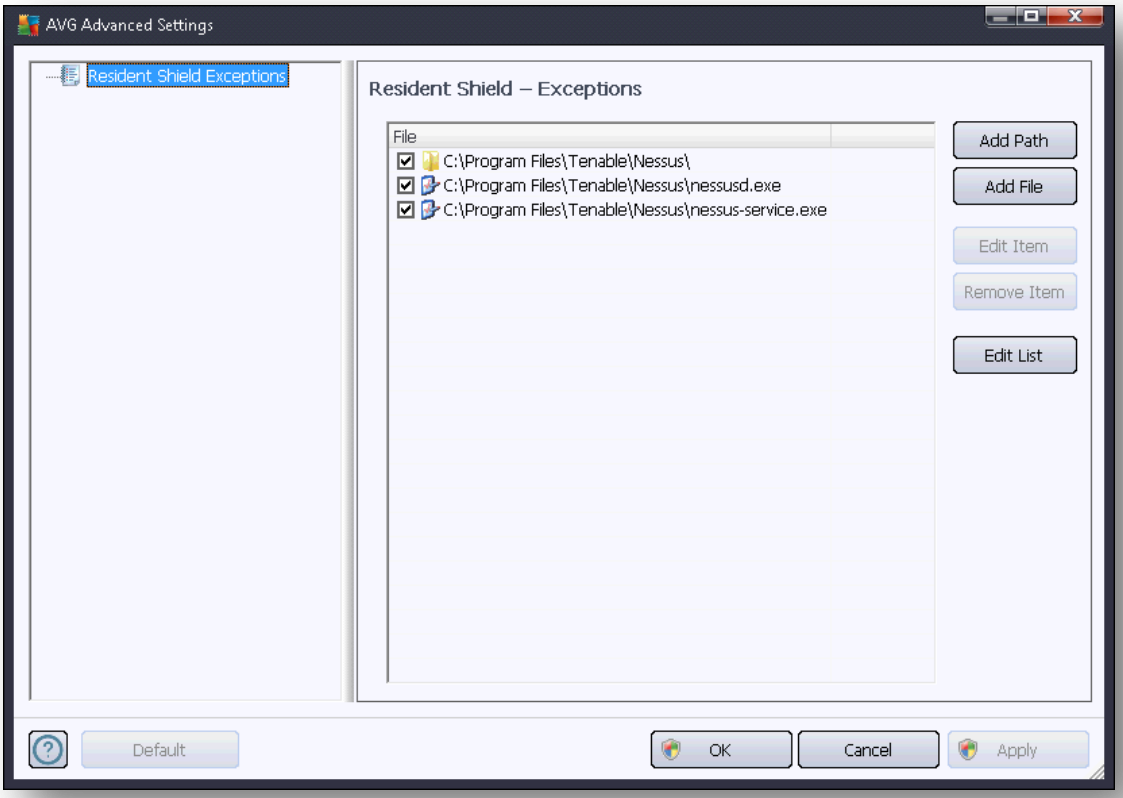


AVG 2012

AVG Internet Security 2012 (AVG-2012) is a suite of tools from AVG Technologies that includes antivirus, a firewall, and several tools designed to protect you while you use services on the Internet. The antivirus and firewall components of any security software have the potential to adversely affect vulnerability scanners, both in performance and by limiting select traffic.

Tenable's internal testing has determined that AVG-2012 is **not well suited** to the presence and operation of Nessus 5. Nessus scan durations increased by a factor ranging from 5 to 20 during initial testing, and coverage failed for detecting a wide range of issues.

Configuring AVG's "Resident Shield Exceptions" to allow the Nessus directory and binaries did not improve scan duration or vulnerability coverage.

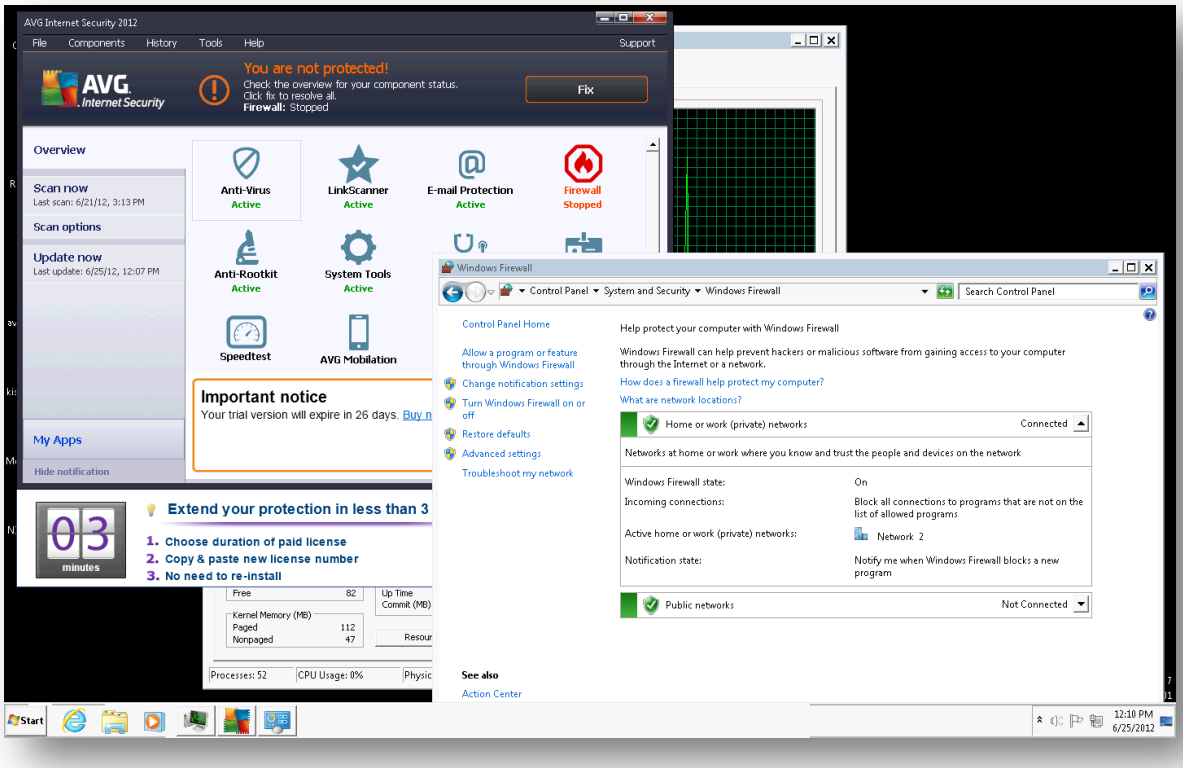


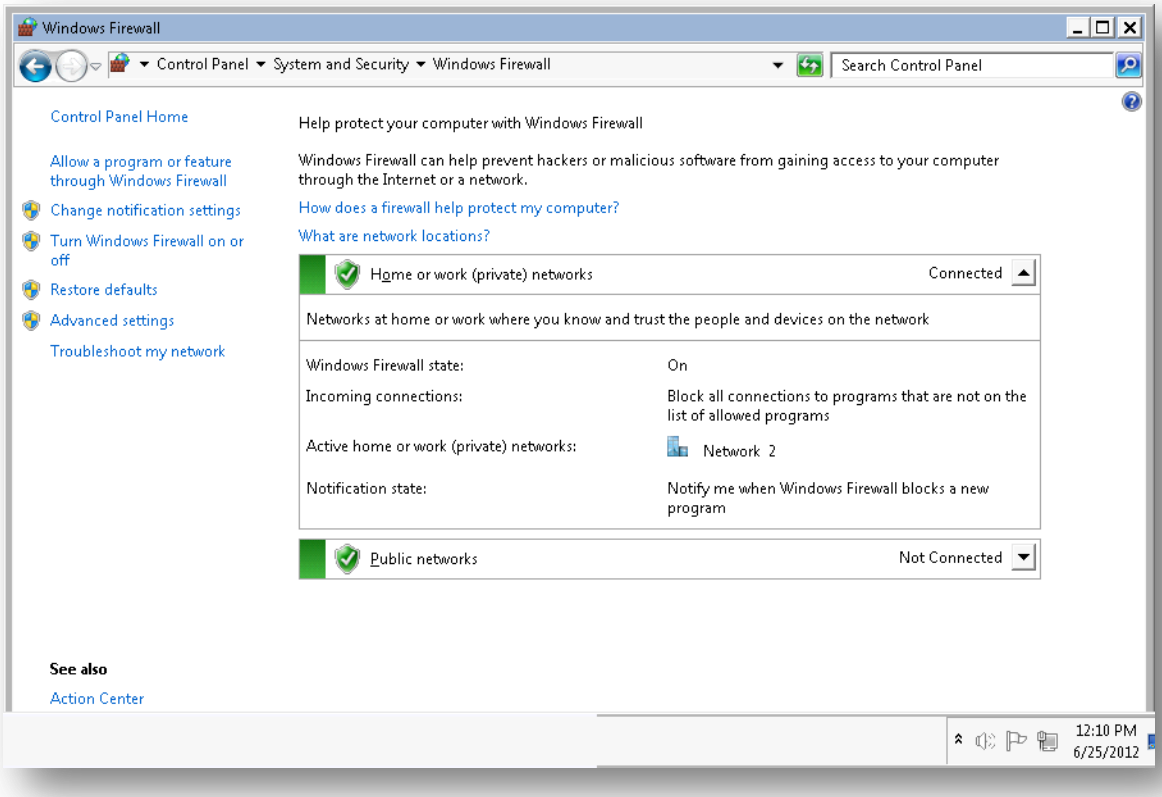
AVG Firewall logs recorded significant blocking of ICMP and UDP packets during scans. This caused the following plugins not to fire under AVG-2012:

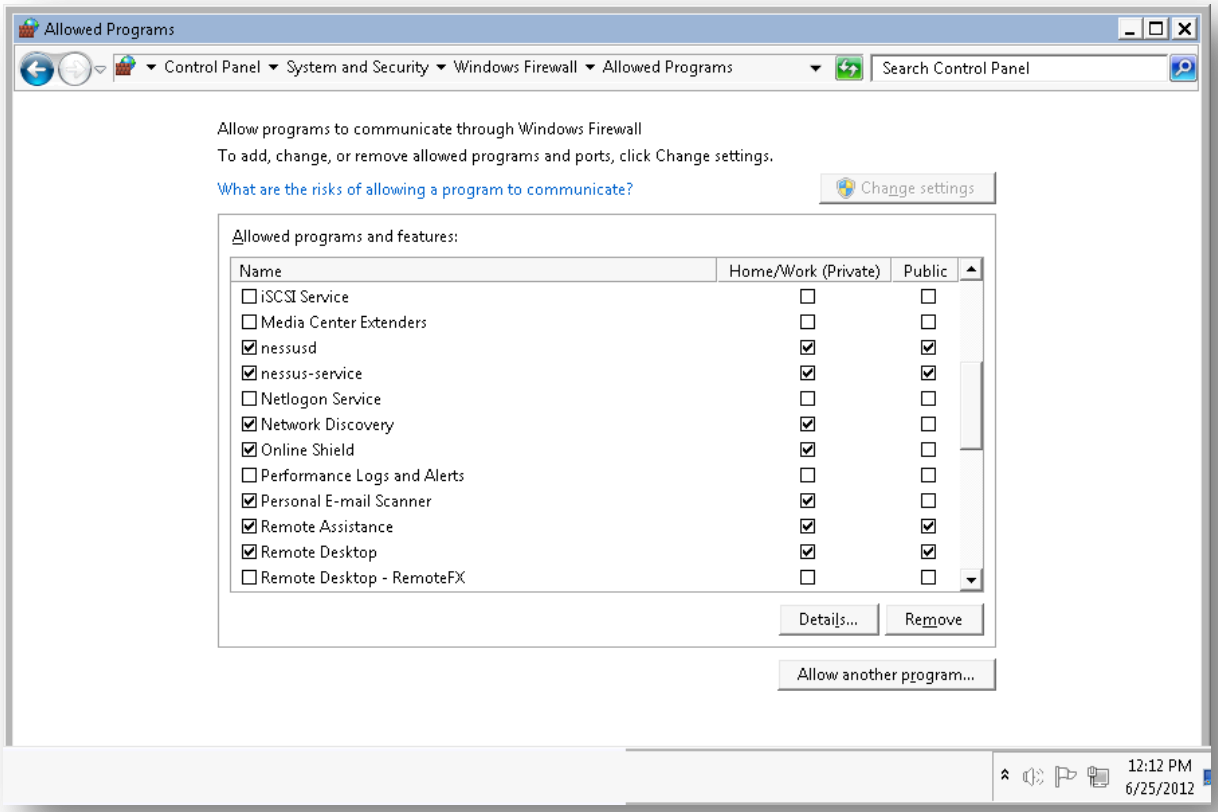
- 10114 (ICMP Timestamp)
- 10287 (UDP Traceroute)

No means were found within the software to moderate AVG Firewall interference with Nessus.

AVG/Windows Firewall settings below were necessary to achieve effective scan coverage and acceptable durations. With the Firewall settings below, Nessus under AVG-2012 matched baseline testing results. The following screenshots detail the AVG Firewall settings needed for Nessus 5 scanning:







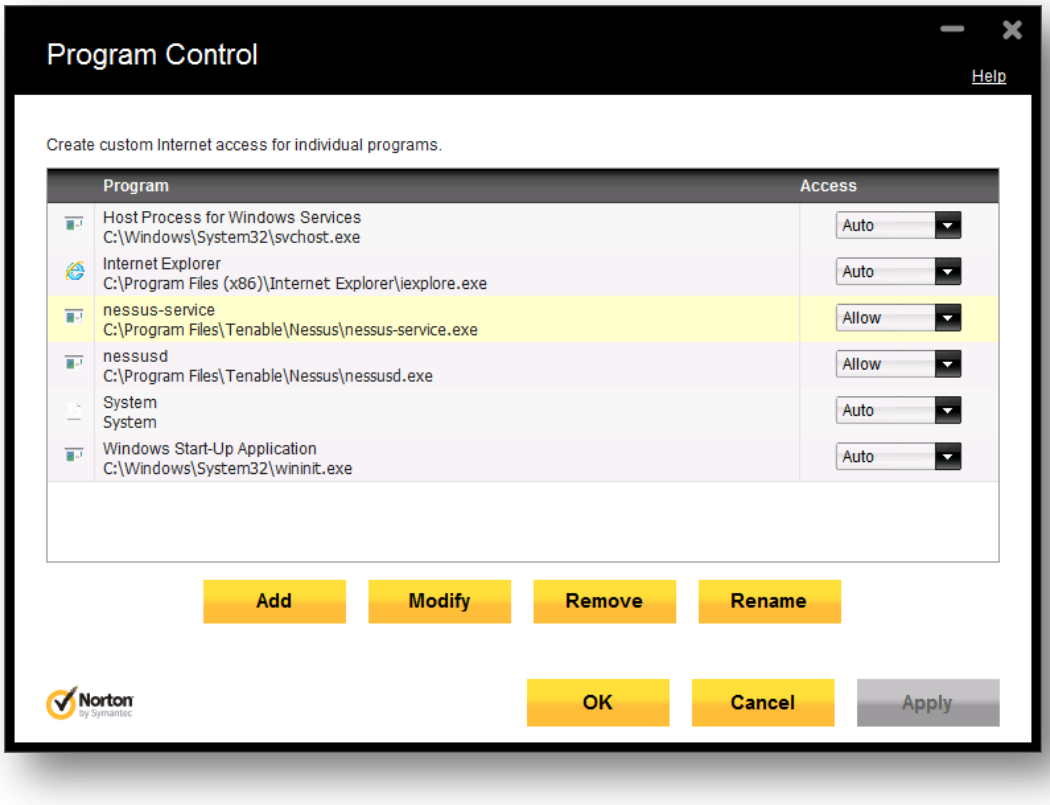
However, the presence of AVG-2012 continues to impact the default External Scan by increasing scan duration from 2 to 8 times the baseline measurements. Scans to all ports (1-65535) without credentials remain costly in time and CPU resources under AVG-2012.

Norton Internet Security 2012

Norton Internet Security 2012 (NIS-2012) is a suite of tools from Symantec that includes antivirus, a firewall, and several tools designed to protect you while you use services on the Internet. The antivirus and firewall components of any security software have the potential to adversely affect vulnerability scanners, both in performance and by limiting select traffic.

Tenable's internal testing has determined that NIS-2012 (version 19.7.1.5) can be configured to be **suitable** to the presence and operation of Nessus 5. The settings required to allow Nessus to run unhindered must be evaluated by the user or organization to determine if they are acceptable changes to NIS-2012.

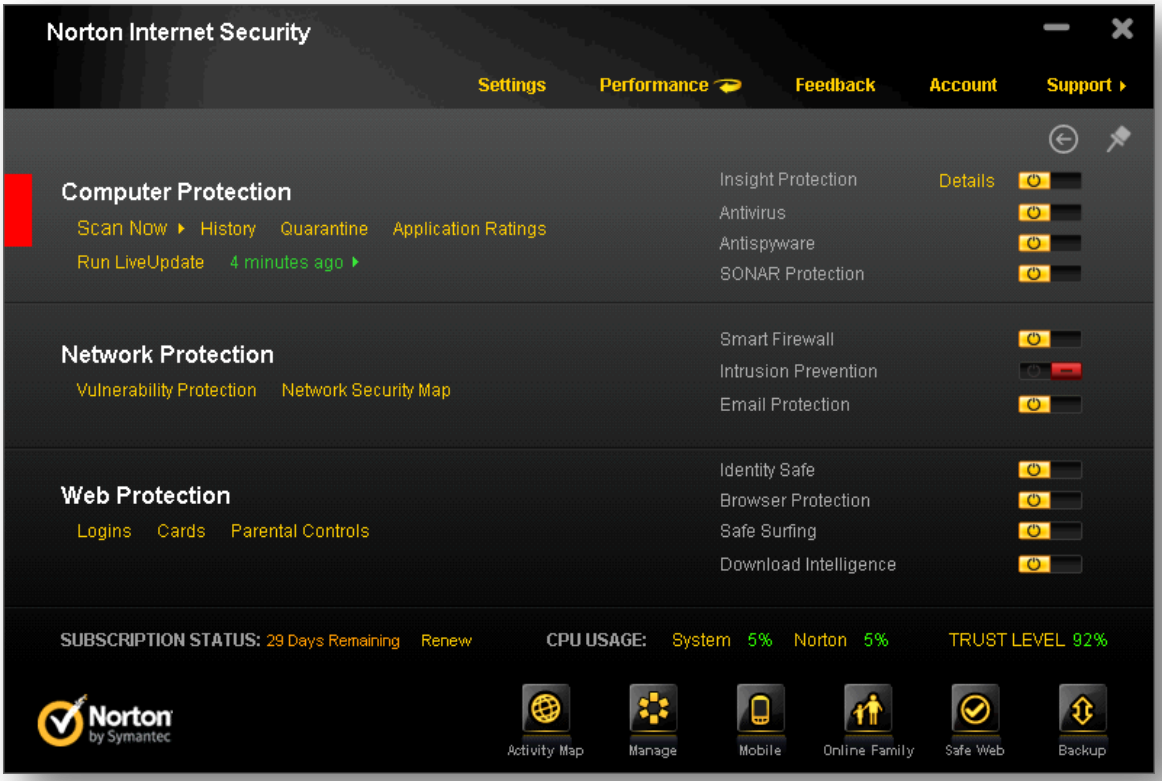
NIS-2012 recognizes Nessus during installation and creates a rule under "Program Control" to permit operation of **`nessusd.exe`** using an `AUTO` setting. You must also add a rule to cover the **`nessus-service.exe`** binary and give it `ALLOW` permission. This can be reached through the following path: NIS main screen → Settings → Network → Smart Firewall → Program Control → Configure.



These changes alone are not sufficient to create a “clear channel” for Nessus scans to operate at full effectiveness. With just these settings, NIS-2012 will display multiple alerts from the “Intrusion” module. Any Nessus scans launched with this configuration will result in both ICMP and UDP probes being blocked, and logged to the Firewall module as “active malware” running on the local machine.

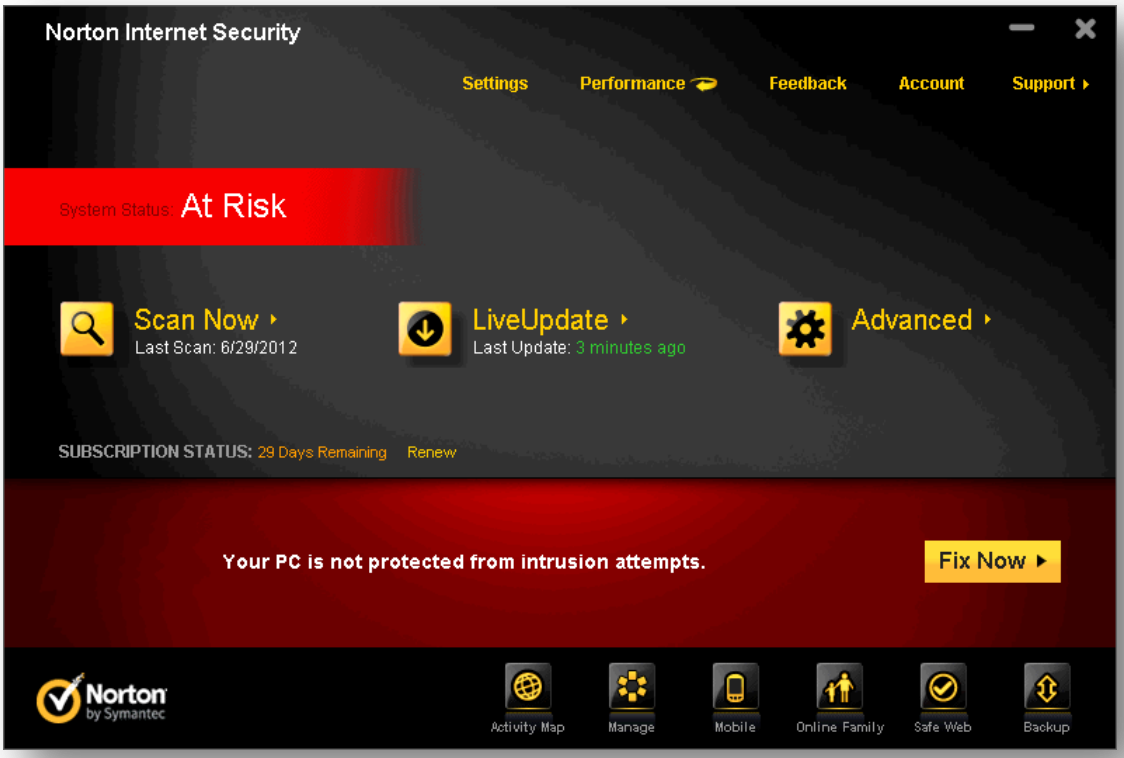
To enable unrestricted Nessus scans, the “Intrusion” module in NIS-2012 must be disabled. Once disabled, this will allow Nessus scans to perform at full capacity, and match baseline performance as far as thoroughness and speed.

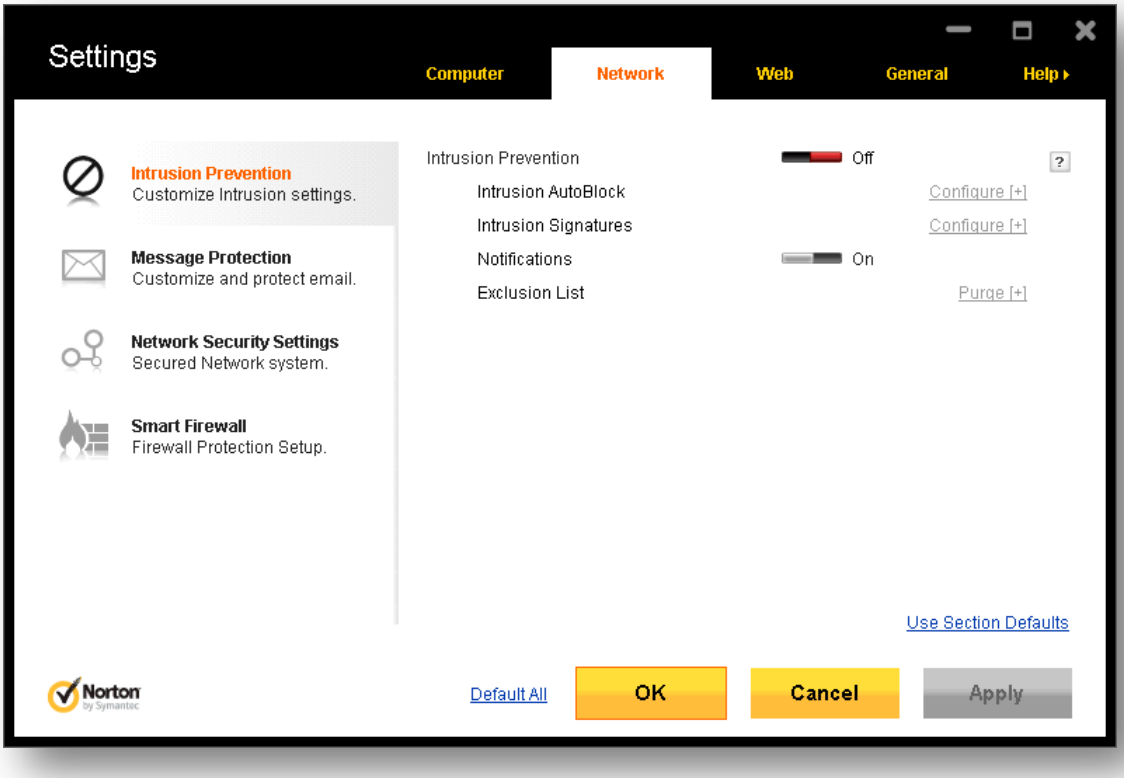
The attached message shows the configuration settings needed (along with the above) to operate Nessus under NIS-2012:



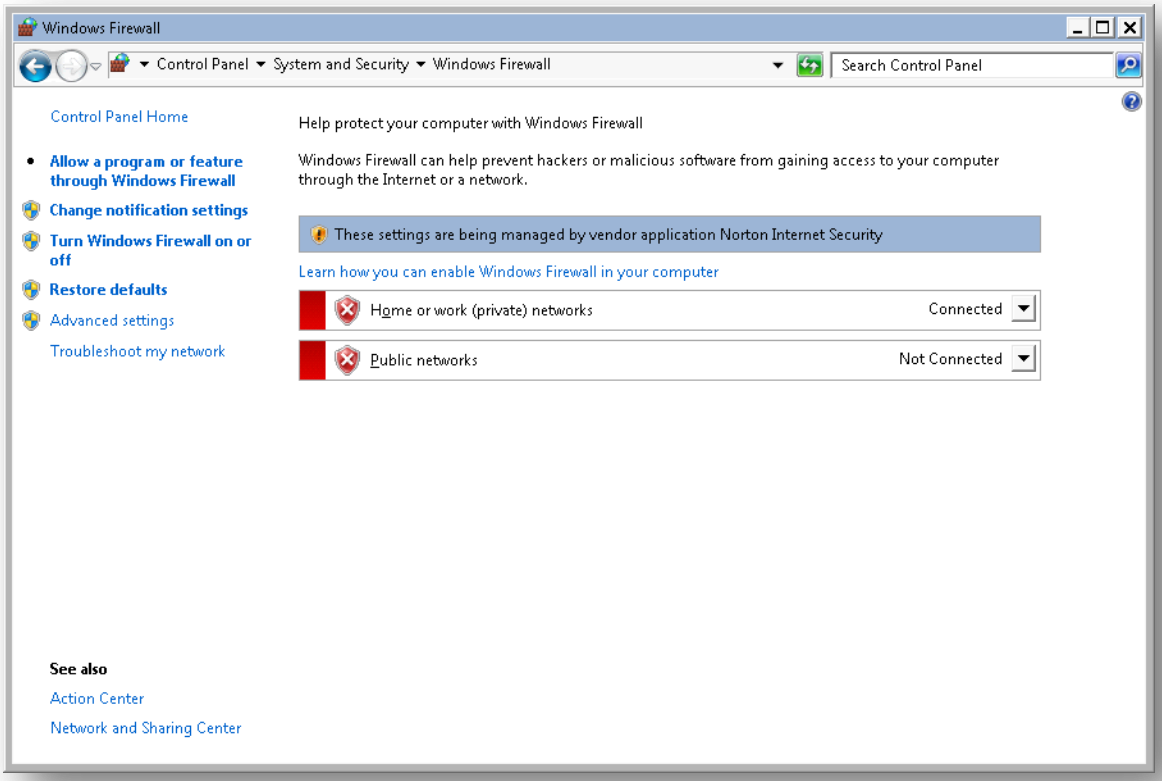
Ultimately, the following settings must be combined to allow effective operation of Nessus when Norton Internet Security 2012 is present:

1. Intrusion must be de-activated permanently
2. **`nessusd.exe`** and **`nessus-service.exe`** must be under Firewall/Program Control



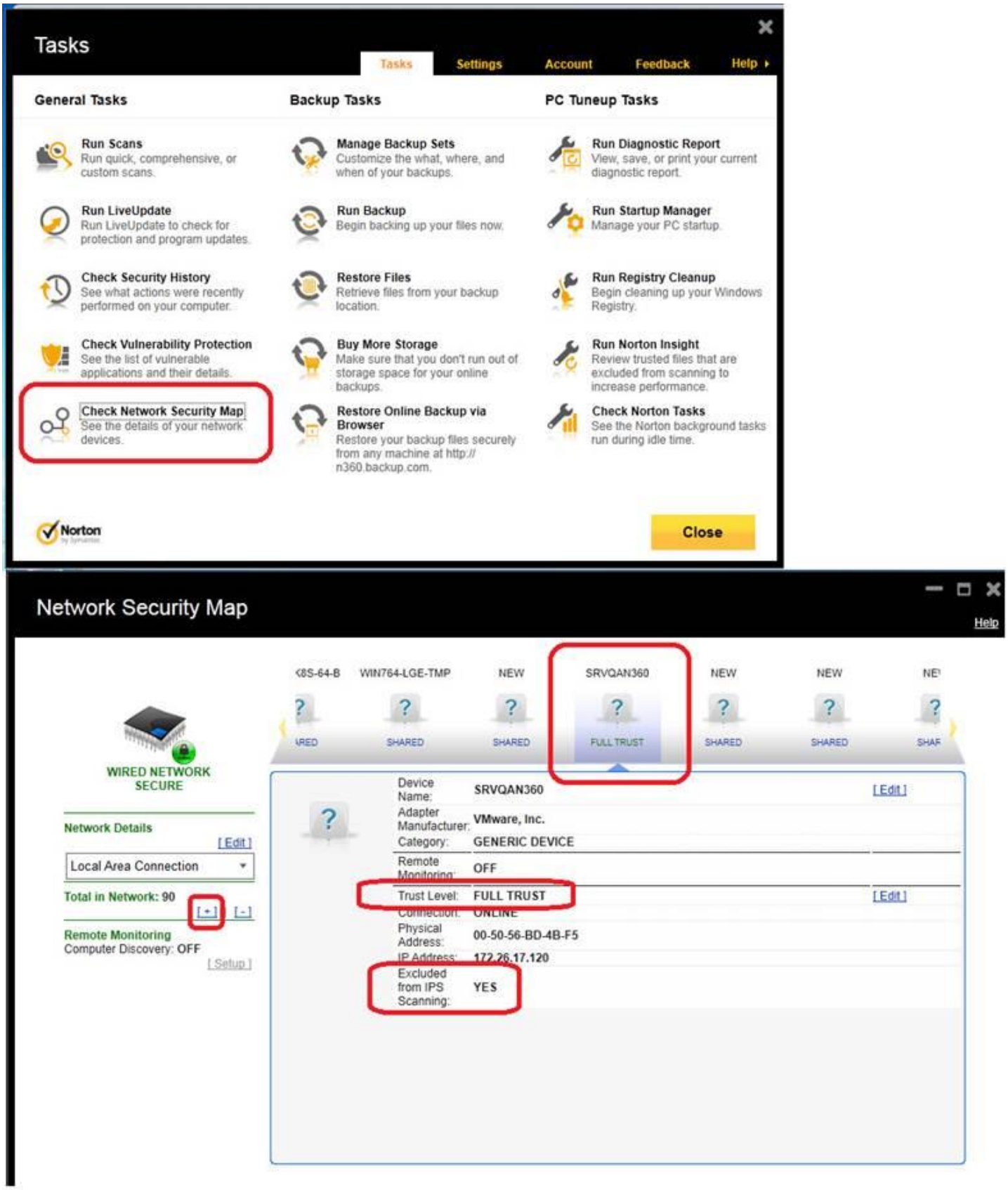


The settings above are in conjunction with the Windows Firewall yielding control of security to NIS-2012:



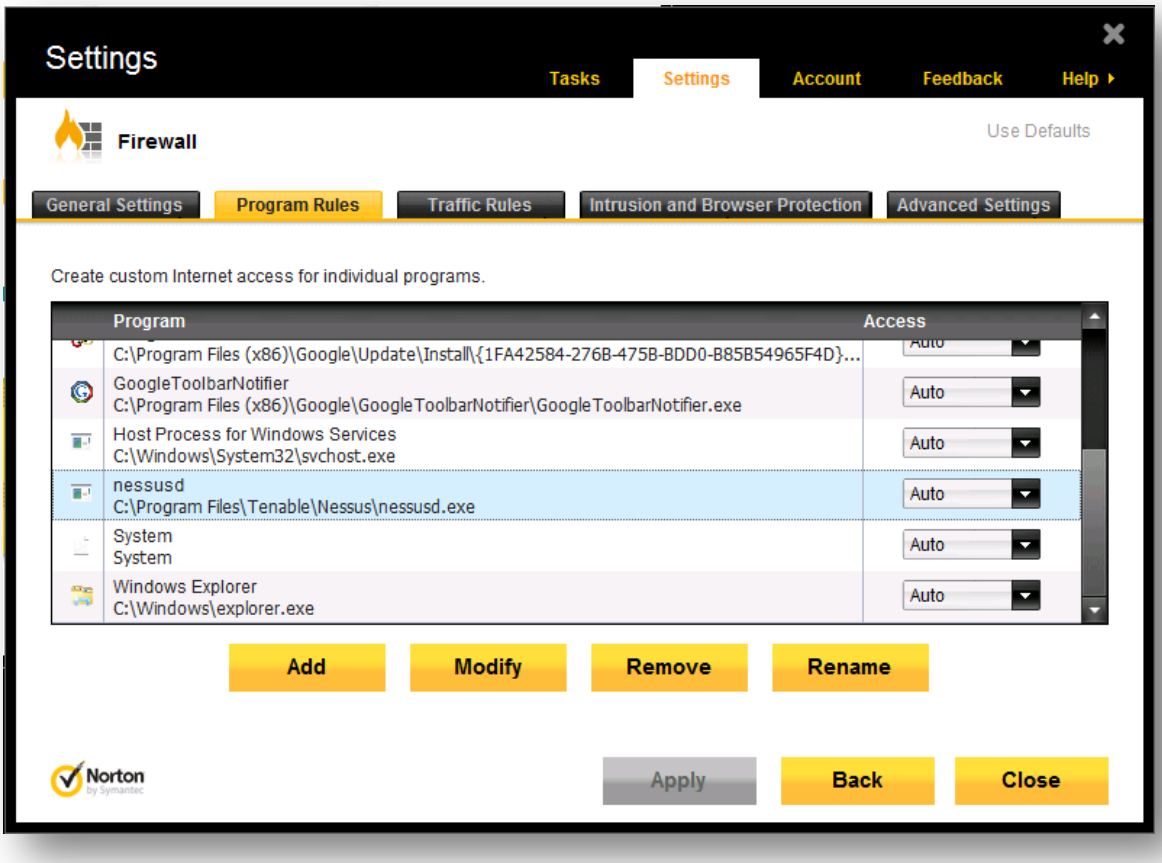
Norton 360

To allow a Nessus scanner full access to an operating system protected by Norton 360, it is necessary to establish a trust relationship between Norton 360 and the Nessus scanner. With Norton 360, this is accomplished by going to the Tasks area and selecting the “Check Network Security Map” area. From there, the Nessus scanner can be added manually (or edited if an entry already exists in the map). The Trust Level needs to be set to “Full Trust”, and the “Excluded From IPS” setting needs to be “YES”.

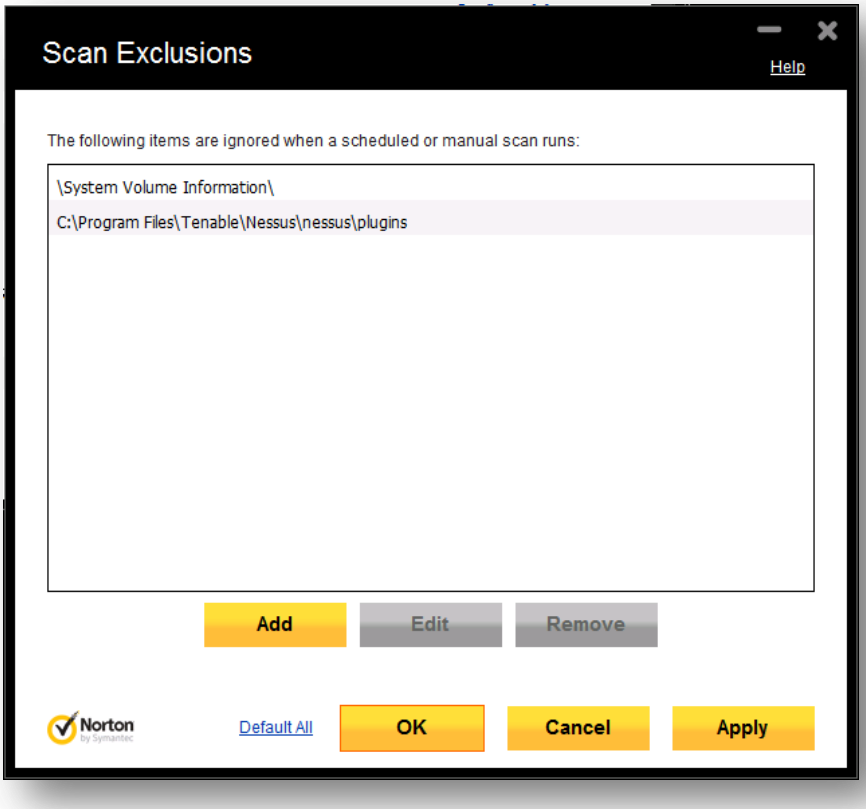


Norton 360 (N360) was tested in conjunction with Nessus 5 and responded very similarly to Norton Internet Security 2012 (NIS-2012) covered in the previous section. N360 recognizes and adapts to the installation of Nessus 5, but requires configuration changes. The settings required to allow Nessus to run unhindered must be evaluated by the user or organization to determine if they are acceptable changes to N360.

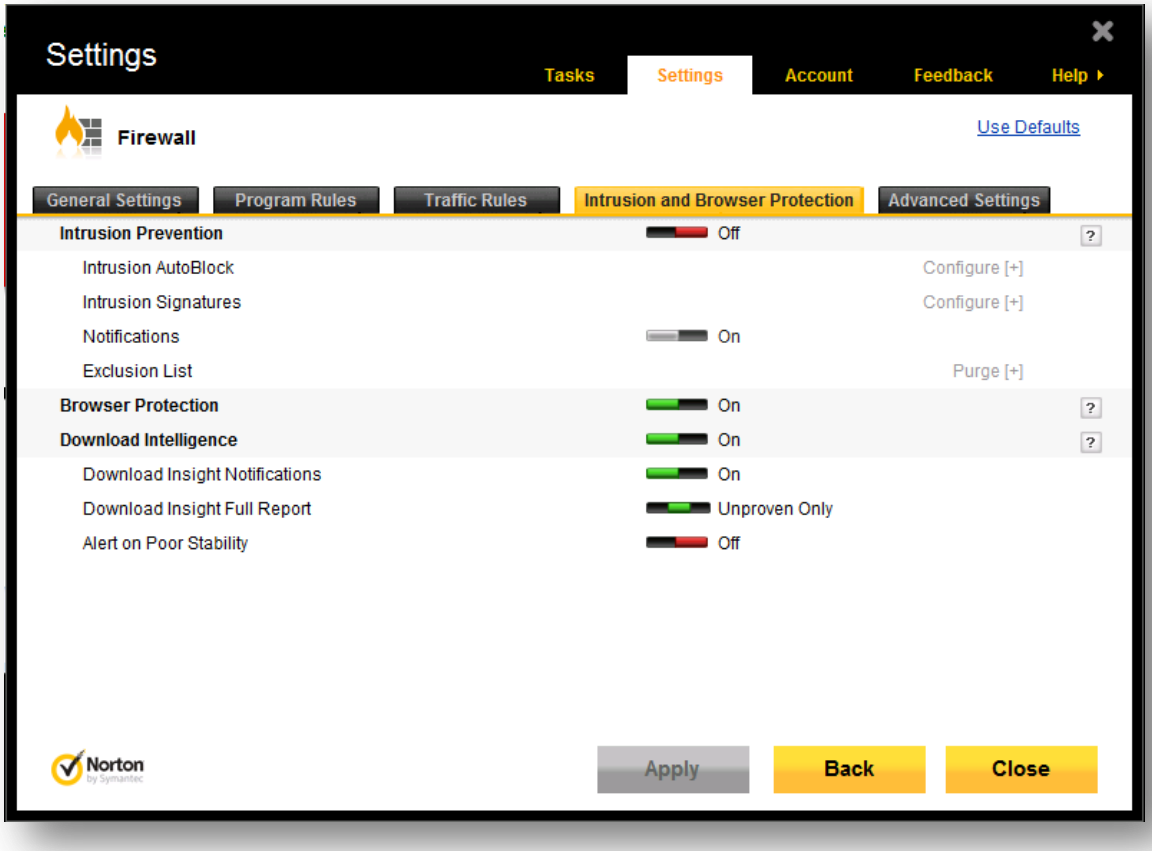
First, **`nessus-service.exe`** must be added to the Firewall:



Next, the Nessus plugin directory must be added to the exclusions for antivirus scanning:



Finally, N360 Intrusion Prevention must be **off** during Nessus scans to prevent the software blocking “attack” packets:



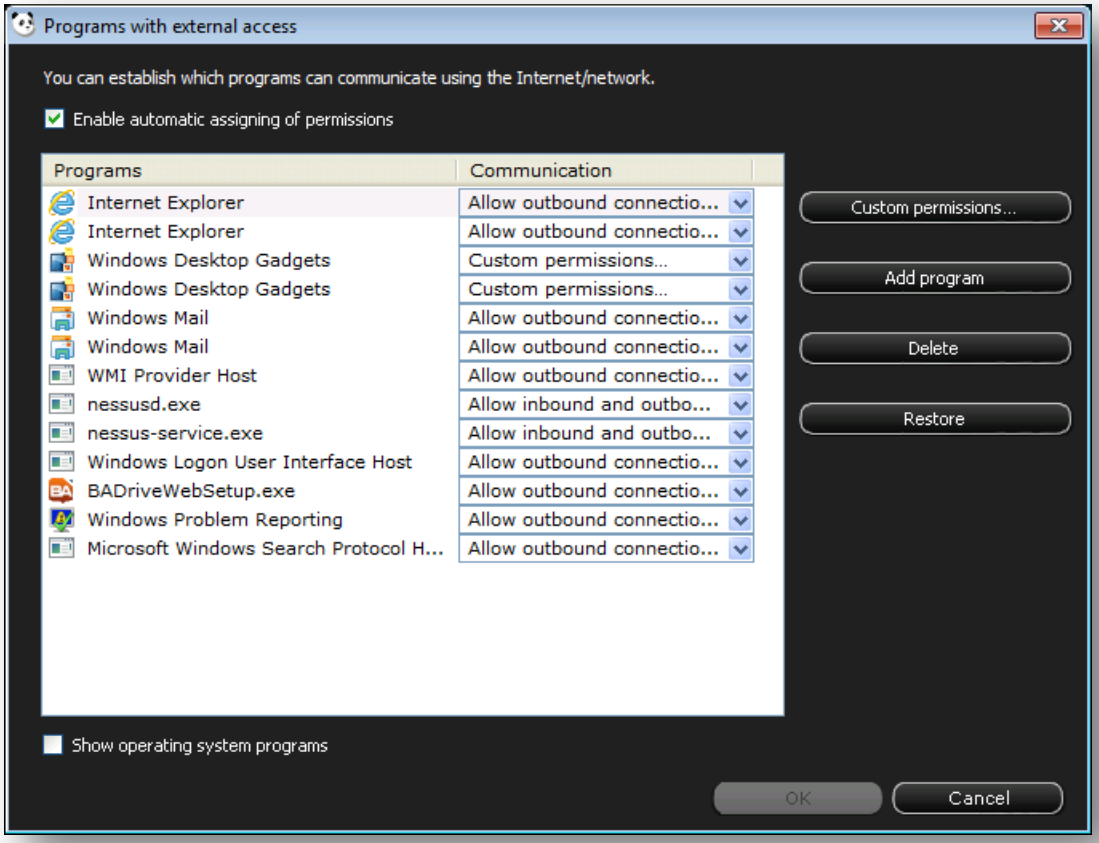
Once these configuration options have been set, users may still notice a slight degradation in Nessus scan times, but no impact to the actual vulnerability test coverage.

Panda Internet Security 2012

Panda Internet Security 2012 (NIS-2012) is a suite of tools from Panda Security that includes antivirus, a firewall, and several tools designed to protect you while you use services on the Internet. The antivirus and firewall components of any security software have the potential to adversely affect vulnerability scanners, both in performance and by limiting select traffic.

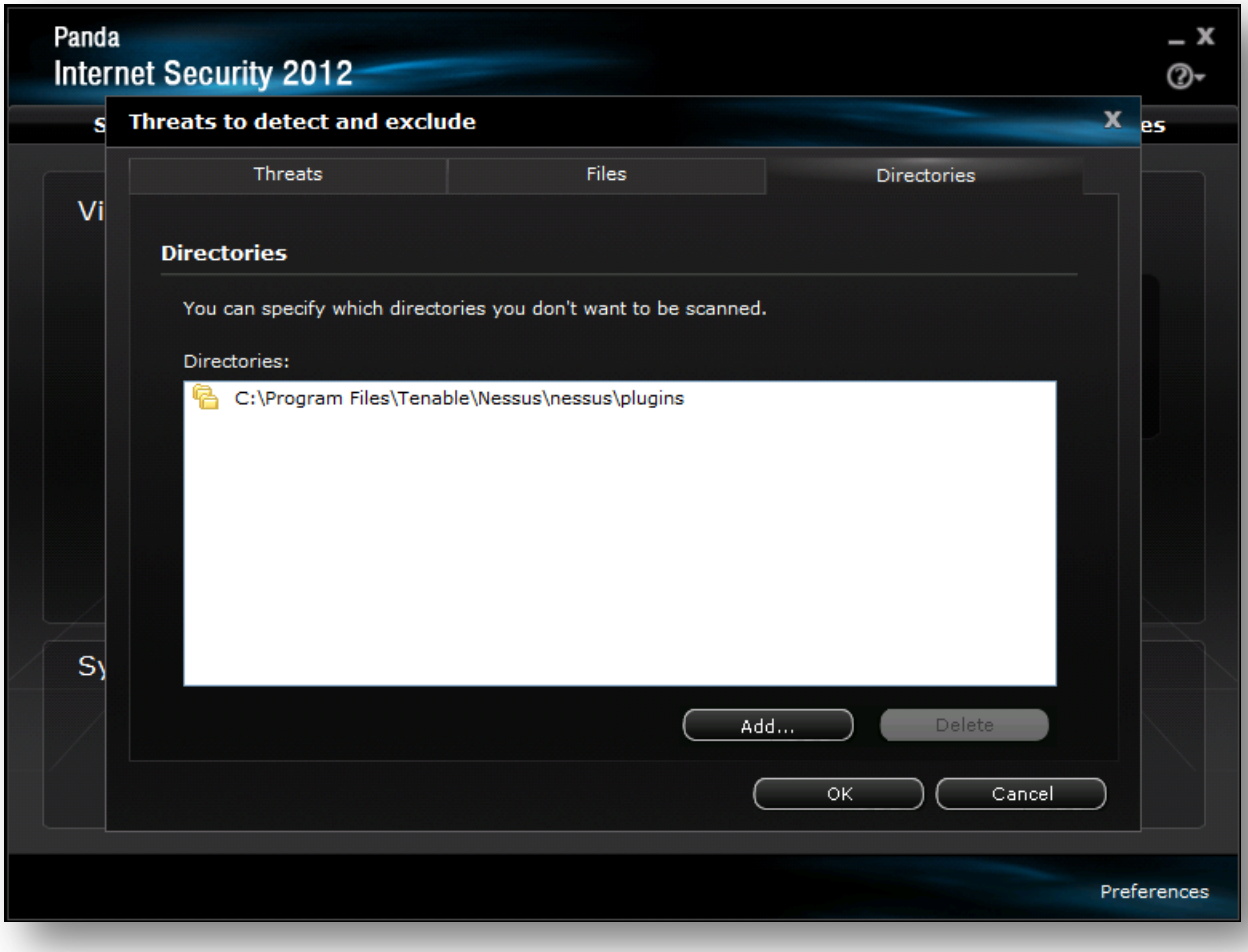
Tenable’s internal testing has determined that Panda 2012 can be configured to be **suitable** to the presence and operation of Nessus 5. The settings required to allow Nessus to run unhindered must be evaluated by the user or organization to determine if they are acceptable changes to Panda 2012. Once configured, Panda 2012 had no impact on Nessus scan duration and did not hinder plugins testing for vulnerabilities.

Tenable's testing was performed to simulate a user who acquires antivirus software after Nessus and Adobe products had already been installed. Once Panda 2012 is installed, it will not instantly recognize Nessus. You must create two Panda-based firewall rules that will allow Nessus traffic:



A rule must be created for both **`nessusd.exe`** and **`nessus-service.exe`** for Nessus to run properly.

In addition to configuring Panda to allow the Nessus executables, an exception must be added to instruct Panda not to scan the Nessus directory for viruses. If this is not done, Panda may flag and remove Nessus plugins (e.g., **`c99shell.nasl`**):



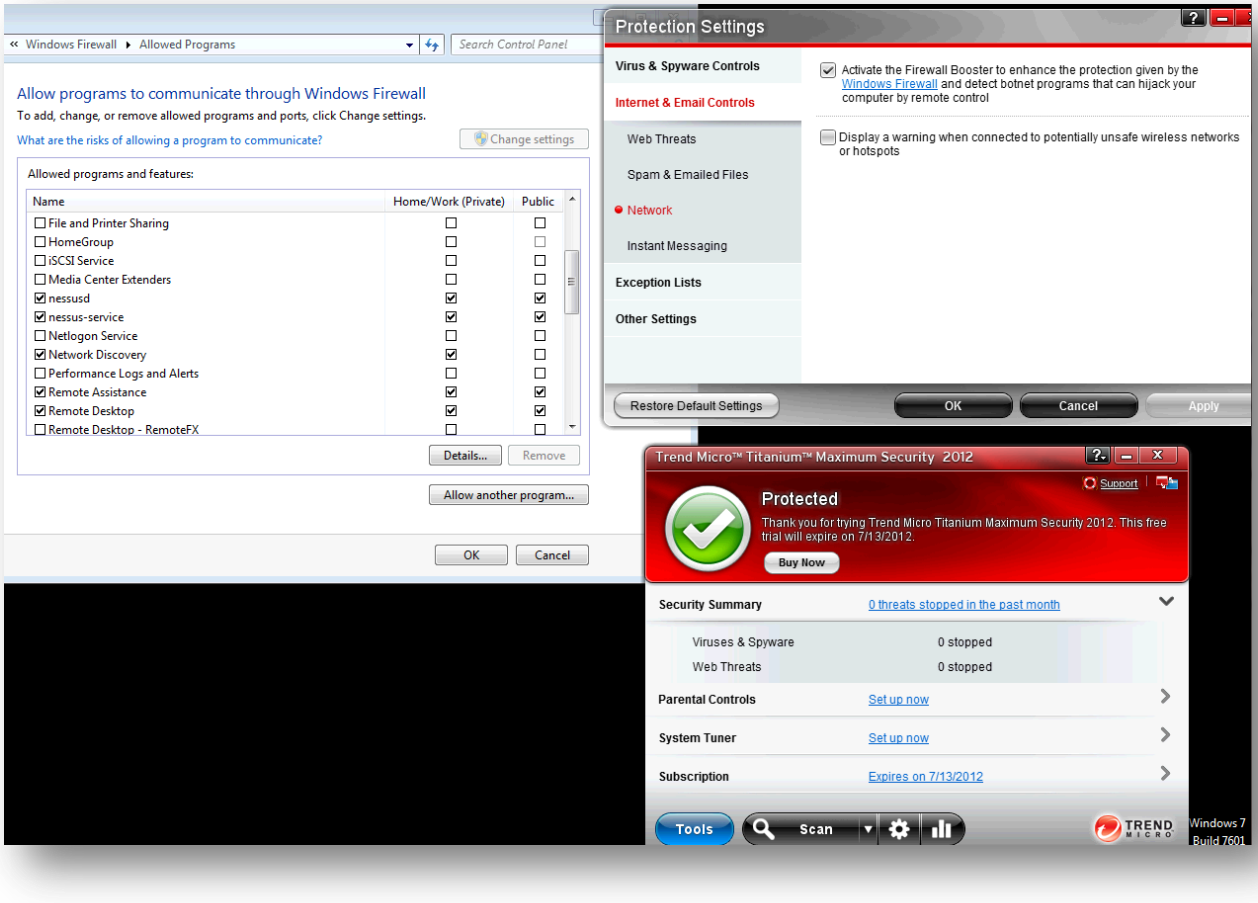
Trend Micro Titanium Maximum Security 2012

Trend Micro Titanium Maximum Security 2012 (TMS-2012) is a suite of tools from Trend Micro that includes cloud-based technology for protection and backup. The antivirus and firewall components of any security software have the potential to adversely affect vulnerability scanners, both in performance and by limiting select traffic.

Tenable's internal testing has determined that TMS-2012 can be configured to be **suitable** to the presence and operation of Nessus 5. The settings required to allow Nessus to run unhindered must be evaluated by the user or organization to determine if they are acceptable changes to Panda 2012. Once configured, TMS-2012 had no impact on Nessus scan duration and did not hinder plugins testing for vulnerabilities.

The settings displayed below allow Trend Micro to operate successfully with Nessus 5. Use of the Firewall Booster (default is ON) will generate detections of some Nessus probes (outbound) as inbound attacks. Turning the Firewall Booster off will avoid those alerts. Note that neither setting interferes with Nessus' operation.

Both Nessus executables (**`nessusd.exe`** and **`nessus-service.exe`**) must be added to the Windows Firewall as Trend Micro uses Windows Firewall as the first level of network protection:



Symantec Endpoint Protection

Symantec Endpoint Protection (SEP) is a suite of tools from Symantec that includes anti-malware monitoring via a variety of methods. The antivirus and firewall components of any security software have the potential to adversely affect vulnerability scanners, both in performance and by limiting select traffic.

Testing indicates that this product not only performs malware detection as the vendor states, but will potentially block suspicious network traffic including some of the tests generated by Nessus. To ensure scans are not interrupted or manipulated, SEP requires that a trust be set up between the Nessus scanner and all associated clients. Since SEP does this dynamically as it observes traffic, it must be configured based on a test scan. The steps below briefly outline the methodology required to configure SEP for subsequent scans. This method has been tested on SEP 12.1.3.

Select a Policy

Select a credential check policy that you will use in your environment (e.g., Malware Detection and Forensics Scan Configuration). Configure Nessus to scan a single host protected by SEP.

Review Scan Results

After performing the Malware Detection and Forensics scan, noting that network latency and host responsiveness may be a factor, there will be a number of plugin results missing including the Microsoft Windows AutoRun results. In addition, note the detailed results of plugin 10919, port open re-check, which will indicate ports that were open during the scan but were closed before the scan completed.

Review SEP Client Security Log

Use the SEP client on the SEP protected host to review the "Security Log" under "Client Management". Note the events that relate to the IP address of the Nessus server. Look at the details of the "Active Reponse" event type. This indicates the SEP client has blocked the Nessus server IP for a number of seconds. Next, look at the "Intrusion Prevention" event type. (At the time Tenable tested this approach, there was only one Intrusion Prevention event when using the SecurityCenter Malware Detection and Forensics scan.) The signature ID will be 21879 and the details will confirm the action to block traffic.

Find Intrusion Policy Signature

Use the SEP Manager to copy the current Intrusion Prevention Policy (copy and then paste it back to the Intrusion Prevention Policies list window), which can be deleted later. Rather than use the existing policy, using a copy is a safe strategy in case of any unintentional changes made whilst investigating the signatures through editing. Edit the copied Intrusion Prevention policy and choose to add an exception. Look for 21879 in the "Add Intrusion Prevention Exceptions" GUI window and note its name "OS Attack: MSRPC Workstation NetJoin BO" and then click "For more details for each signature, click here…", which will pop-up a browser window.

Research Intrusion Policy Signature Details

Locate "OS Attack:MSRPC Workstation NetJoin BO" and click on the attack signature to see the details. You can review the CVE-2006-4691 and Microsoft Security Bulletin MS06-070 references to understand the context of the attack signature. The signature is looking for an exploit attempt that applies to an old vulnerability in Microsoft Windows 2000 Service Pack 4 and Microsoft Windows XP Service Pack 2. During testing, this attack signature was triggered on a fully patched Windows 7 host. This does not negate the usefulness of the signature since we'd want to investigate what the source of the trigger was, but it is prohibiting the Nessus scan from completing all of the checks successfully. If you are comfortable with switching off the blocking action either temporarily or permanently, proceed to the next step.

Consider Policy Change for the Signature

Close the browser window you were using to research the details of the signature and ensure the signature is selected in the "Add Intrusion Prevention Exceptions" GUI window. Click "Next" to continue with modifying the signature and note its action is set to "Block". You can change the action to "Allow" but leave logging enabled. If the policy that is distributed to the SEP clients has the signature set to "Allow" as an exception, then the SecurityCenter Malware Detection and Forensics scan policy will work. At this point you are looking at a copied policy, but how you decide to distribute this particular policy change will be dictated by your in-house policies for modifying Symantec Endpoint Protection settings. You can use the third step to sanity check the change has been rolled out successfully if scanning fails on one or more hosts.

Hewlett-Packard NIC Teaming

Hewlett-Packard (HP) uses a technology called NIC teaming that groups several network interface cards into a single logical NIC. This technology has the potential to interfere with Nessus during packet forgery and sniffing packets.

It is recommended that Nessus be deployed on a system that does not utilize this technology, to ensure scans are not interrupted or adversely affected.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data.

Tenable is relied upon by more than 24,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments. We offer customers peace of mind thanks to the largest install base, the best expertise, and the ability to identify their biggest threats and enable them to respond quickly.

For more information, please visit tenable.com.