Network Performance Test

Business Security Software

Language: English
August 2016

Last Revision: 11th October 2016

www.av-comparatives.org

Test commissioned by the vendor

Introduction

This report, commissioned by ESET, considers six major business anti-virus solutions with regard to resource management. In total, four individual tests were carried out. The first two tests measure the amount of network traffic caused by the products. Test One was a long-term test conducted without any user interaction, while Test Two was a shorter-term test with simulated user operations. Test Three considers the size of the client-side virus definitions. The last test, Test Four, looks at the machine load (CPU, RAM) during a single update of the client.

Tested Products

The test included the following security products:

- ESET Endpoint Security 6.4
- Kaspersky Endpoint Security 10.2
- McAfee Endpoint Security 10.2
- Sophos Endpoint Security and Control 10.6
- Symantec Endpoint Protection 12.1
- Trend Micro OfficeScan 11.0

Machine Setup

A total of seven server-client test systems were set up for the test: one for each product, plus an additional server-client system with no antivirus installed as a control. For each server-client test system, we use one Windows Server machine and one Windows client machine. A domain is created on the Windows Server, and the client machine is joined to this domain. An appropriate server configuration is used for all seven servers, and an appropriate client configuration is used for all seven clients. The respective configurations are as follows:

Server: Standard installation of Windows Server 2012 R2 64 Bit with 4GB of RAM. The following changes were made:

- Disabled the Windows Update service
- Installed the Windows Assessment and Deployment Toolkit 8.59.25584
- Installed WinPCAP 4.1.3

Client: Standard installation of Windows 7 Professional 64 Bit with 3GB of RAM. The following changes were made:

- Disabled the Windows Update service
- Installed the Windows Assessment and Deployment Toolkit 8.59.25584
- Installed WinPCAP 4.1.3
- Installed Java 8 Update 66

For each of the six server-client test systems with AV products installed, the product's management console is installed on the server using default settings. Some products require the installation of additional Microsoft Software, such as .NET Framework or SQL Server, so we install the respective components on those machines where it is required; we regard the additional software as being part of the product itself for the purposes of this test. The relevant endpoint security product is then installed on the client, also using default settings. We check that the client software is registered in the management console, that communication between AV client and console is working as expected, and that the AV client can update virus definitions successfully. No antivirus software is installed on the server itself. Each server-client system is assigned an independent VLAN, which is completely isolated from network traffic in the other VLANs. The machines are configured to keep the basic network load as low as possible, e.g. by disabling Windows Updates. It has to be pointed out that those measures cannot prevent the machine from sending any data on the network, however. The server and the client in each test system are allowed to connect the Internet at any time.

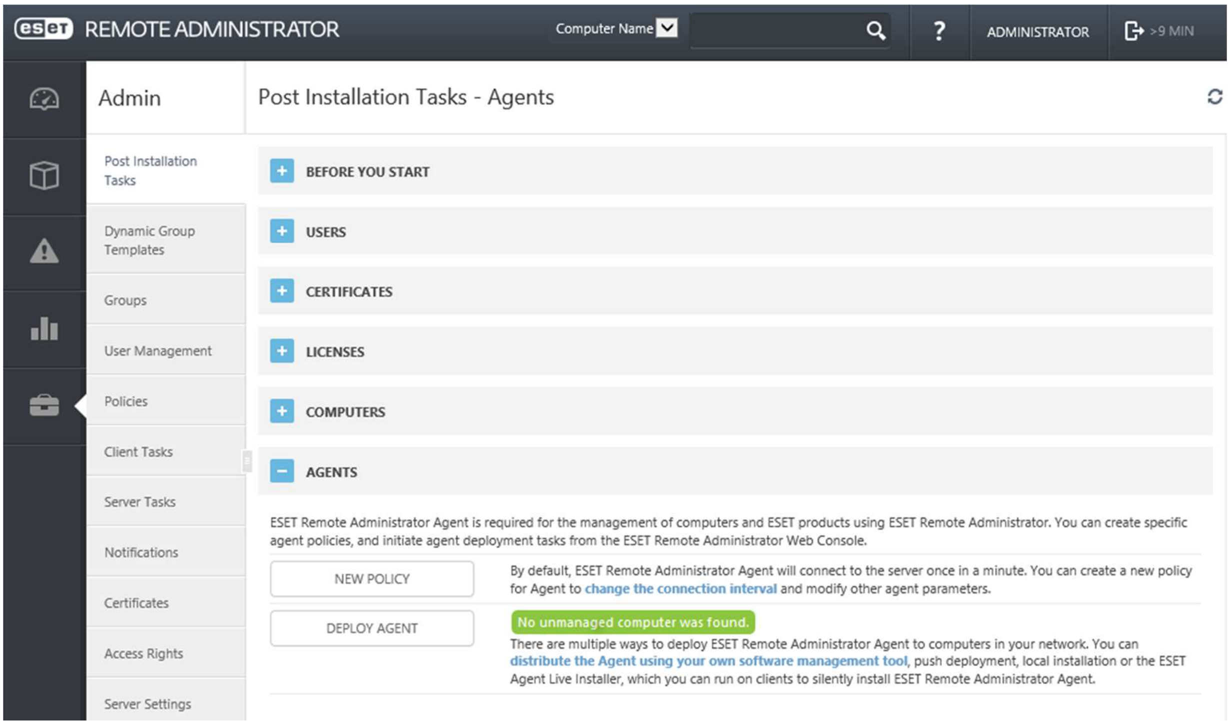
Settings Used

All products (except ESET) were tested using default settings.

By default, the ESET client connects to the server once every minute. This shorter update interval is only recommended for setup purposes, because adding computers, pushing policies, and checking the status of protected computers is easier for the administrator using nearly real-time updates.

As shown in the screenshot below, the ESET Administration Console recommends setting the update interval to 20 minutes or more for productive use. In accordance to this recommendation, we changed the default settings to let clients only connect to the server once every 20 minutes.

ESET informed us that they are working on an improvement for this situation. In the future their product will provide a setup policy with a limited time validity – automatically changing the initial update interval after a predefined amount of time. Until these "limited time validity" policies are implemented, ESET is sticking with the recommendation shown in the screenshot.



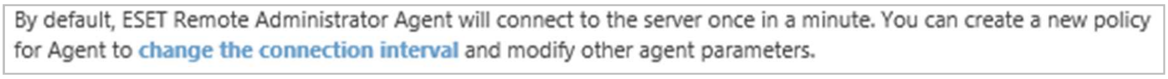
Post Installation Tasks - Agents

ESET Remote Administrator Agent is required for the management of computers and ESET products using ESET Remote Administrator. You can create specific agent policies, and initiate agent deployment tasks from the ESET Remote Administrator Web Console.

By default, ESET Remote Administrator Agent will connect to the server once in a minute. You can create a new policy for Agent to change the connection interval and modify other agent parameters.

No unmanaged computer was found.

There are multiple ways to deploy ESET Remote Administrator Agent to computers in your network. You can distribute the Agent using your own software management tool, push deployment, local installation or the ESET Agent Live Installer, which you can run on clients to silently install ESET Remote Administrator Agent.


By default, ESET Remote Administrator Agent will connect to the server once in a minute. You can create a new policy for Agent to change the connection interval and modify other agent parameters.

Test One: Long-Term Network Load Test (Idle)

Methodology

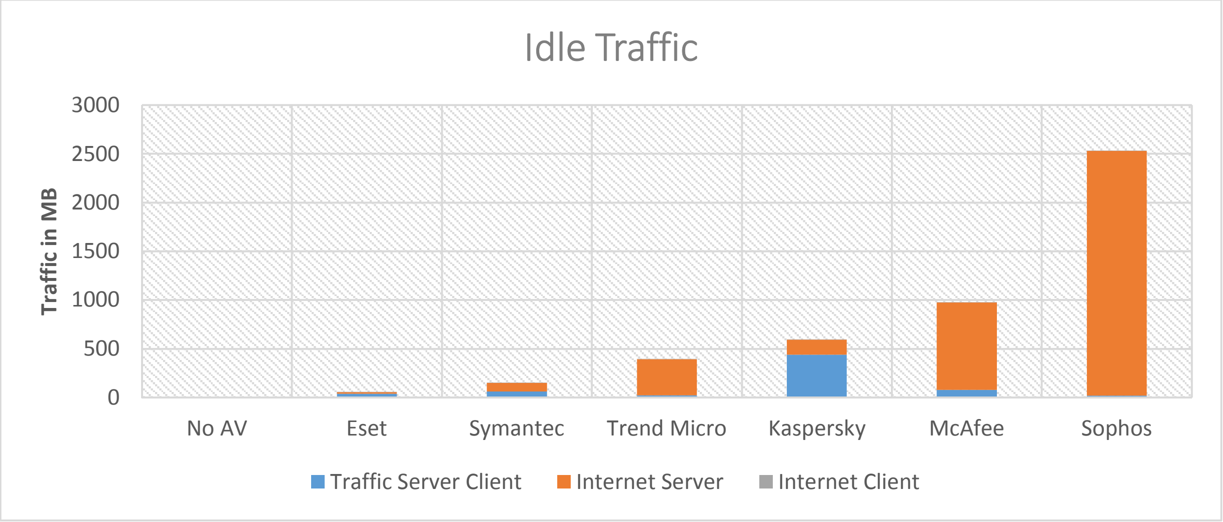
The goal of this test is to compare the participating products in terms of the network load they generate during the course of one week. The test does not involve any user input, therefore all the machines simply idle for one week (7 days – from 1st to 7th October). The network traffic is captured using WinPCAP. The resulting *.pcap files are analysed after the test is completed. The analysis distinguishes between three major components: network load between server and client; network load between server and Internet; network load between client and Internet. All values are treated independently.

Each machine is restarted before the test runs. After the restart, each machine is allowed to idle for at least three hours before the test starts. This allows triggered actions (such as "Update after restart") to be performed without being captured. The network traffic is captured for both machines, i.e. server and client, for each server-client test system.

Results

All values in the following table are given in Megabytes (MB).

	Traffic LAN (Server <> Client)	Traffic WAN (Server)	Traffic WAN (Client)
No AV	0	0	0.1
ESET	38	19	1.0
Symantec	63	89	1.2
Trend Micro	22	370	0.6
Kaspersky Lab	441	152	2.1
McAfee	78	898	1.2
Sophos	18	2,514	1.2



Test Two: Network Load Test (User Action)

Methodology

This test is similar to the long-term network load test. The machine setup and the testing methodology are the same. Whilst in the previous test no user action was simulated, in this test we perform automated actions using the Windows Assessment and Deployment Toolkit (ADK). The actions include:

- Archiving files on local disk:
  - MS Office, 297 MB, 335 files
  - PDF, 440 MB, 289 files
  - PE, 930 MB, 2,328 files

- Copying Files on local disk
  - MS Office, 297 MB, 335 files
  - PDF, 440 MB, 289 files
  - PE, 930 MB, 2,328 files
  - ZIP, 353 MB, 4 files

- Installation of four well-known applications

The test files are copied to the machine in Safe Mode without any antivirus software present. Therefore none of the performed actions and included files can be whitelisted before the actual test starts. The analysis of the network traffic starts before the ADK operations start, and ends after the ADK operations are completed.

Results

The results table contains the overall network load (LAN and WAN) on the client side. All values are in Megabytes (MB).

Product	Total Client-Side Network Load
No AV	0.0 MB
ESET	0.2 MB
Symantec	0.4 MB
Kaspersky Lab	0.4 MB
Sophos	0.8 MB
McAfee	2.6 MB
Trend Micro	23.8 MB

Test Three: Size of Client-Side Definitions

Methodology

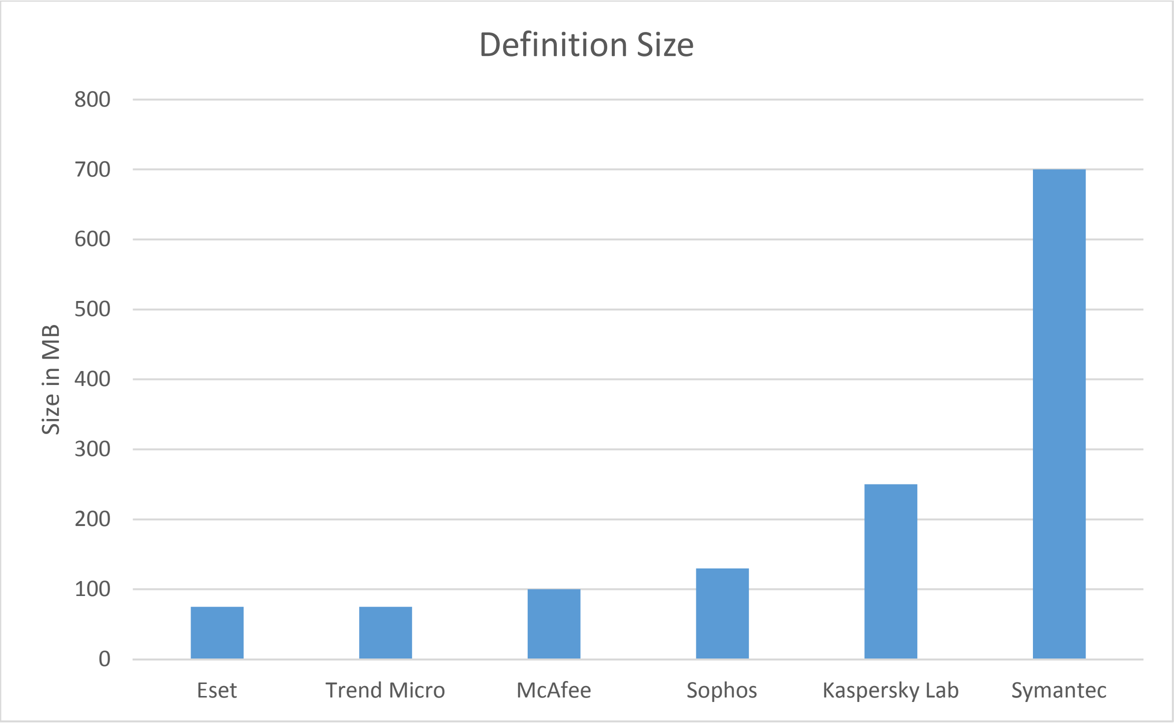
The goal of this test is to compare the size of the virus definitions on the client side. Finding exact values for the virus definitions (and only the virus definitions) is a challenging task and only the vendors themselves can provide exact information. The measurement was taken after Test One, therefore all definitions were up to date.

In this test we examine the client-side installation of each product and look out for virus definition files, selecting them as precisely as possible. As we do not know any details of the exact implementation of each product, we concede the possible existence of noise in our investigation.

Results

All values are in MB (rounded).

Product	Size of client-side virus definitions
ESET	75 MB
Trend Micro	75 MB
McAfee	100 MB
Sophos	130 MB
Kaspersky Lab	250 MB
Symantec	700 MB



Test Four: Machine Load during Update

Methodology

In this test we compare the machine load during updates on the client side. This analysis includes a comparison of CPU loads and RAM usage. For analysis we use the Microsoft Performance Toolkit, included in the Windows Assessment and Deployment Toolkit (ADK), as well as the Windows internal tool Perfmon.exe.

We were not able to trigger updates manually for each and every product in a standardized way. Therefore we decided to use a more generic method to trigger an update. We disconnect the client for 72 hours from the network. This will lead to outdated databases, which will be updated as soon as the network is available. Furthermore we assume that these results are more realistic in a typical configuration, as the definitions are updated in the background without any graphical representation (which consumes hardware resources as well).

The measurement of the machine resources starts before the network connection is available, and ends after two hours. The results are then analysed manually and cropped to include only the actual update process.

Results

The results include the runtime of the update. This is manually determined by measuring the time from the point where the machine load exceeds the idle load to the point where the machine load falls back to the idle load. The results include the average CPU load during the update, and the average additional memory usage during the update in comparison to the memory consumption during idle before the update started.

It is up to the reader to interpret these results. We notice two different approaches of the vendors. One approach is to complete the update in the shortest possible time, such as in the case of ESET. This results in high average CPU loads during a short time period. The other approach is to keep the CPU load low, such as in the case of Symantec. This results in a longer overall update time.

Name	Time [sec]	CPU, average [%]	Additional memory usage, average [MB]
ESET	19	46	64
Kaspersky Lab	58	50	46
McAfee	98	15	9
Sophos	118	13	13
Symantec	353	17	88
Trend Micro	18	8	7

Copyright and Disclaimer

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 a 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 (October 2016)