Zscaler Cloud Web Gateway Test

A test commissioned by Zscaler, Inc. and performed by AV-TEST GmbH. Date of the report: April15th, 2016

Executive Summary

In March 2016, AV-TEST performed a review of the Zscaler Cloud Web Gateway solution for the Enterprise to determine the malware detection and blocking capabilities. Zscaler commissioned AV-TEST to run this independent test.

In order to ensure a fair review, the sponsor has not supplied any samples or had any influence or any prior knowledge regarding the samples being tested. The following test scenarios are standard tests that AV-TEST does on a regular basis for network-based antimalware solutions. The solution provides two ways to stop malware at the network level today. These are static (signature-based) detection options that protect against known vulnerabilities and malware as well as heuristic and dynamic detection options that cover both known and unknown vulnerabilities and malware. The performed tests cover both approaches:

1. **Real World Test:** Testing of the effectiveness of dynamic URL filtering capabilities and protection against malware by accessing real URLs that host malicious downloads,
2. **Sandbox Test:** Detection of relevant current malicious Win32 portable executable (PE) files, also referred as “Prevalent Malware”, which are not older than 4-8 weeks at the start of the review.
3. **False Positive Test:** False detection or classification of clean URLs.
4. **Social Engineering Test:** Detection of current phishing URLs.

Breaking out the data by test shows that Zscaler performed well in nearly all tests. The protection score was on a very high level. On the other hand there were only 2 misclassifications in the test of 1886 benign websites.

	Real-World Testing (URLs)	Sandbox Test (Files)	Social Engineering (Phishing)
Total Samples	6,049	11,567	1,142
Detected Samples	5,892	11,557	1,142
Detection Rate	97.40%	99.91%	100%

Figure1: Summary of the test results for Malware blocking

	Website False Positives
Total Samples	1886
Detected Samples	2
False Positive Rate	0.11%

Figure2: Summary of the test results for False Positives

In total Zscaler detected 99.11% of all malicious threats and had a very low false positive rate in case of benign websites.

Overview

With the increasing volume of malware, targeted attacks and advanced persistent threats spreading through the Internet these days, the danger of getting infected is higher than ever before. In the year 2000, AV-TEST received more than 170,000 new unique samples, and in 2015, the number of new samples grew to over 140,000,000. The growth of these numbers is displayed in Figure 3.

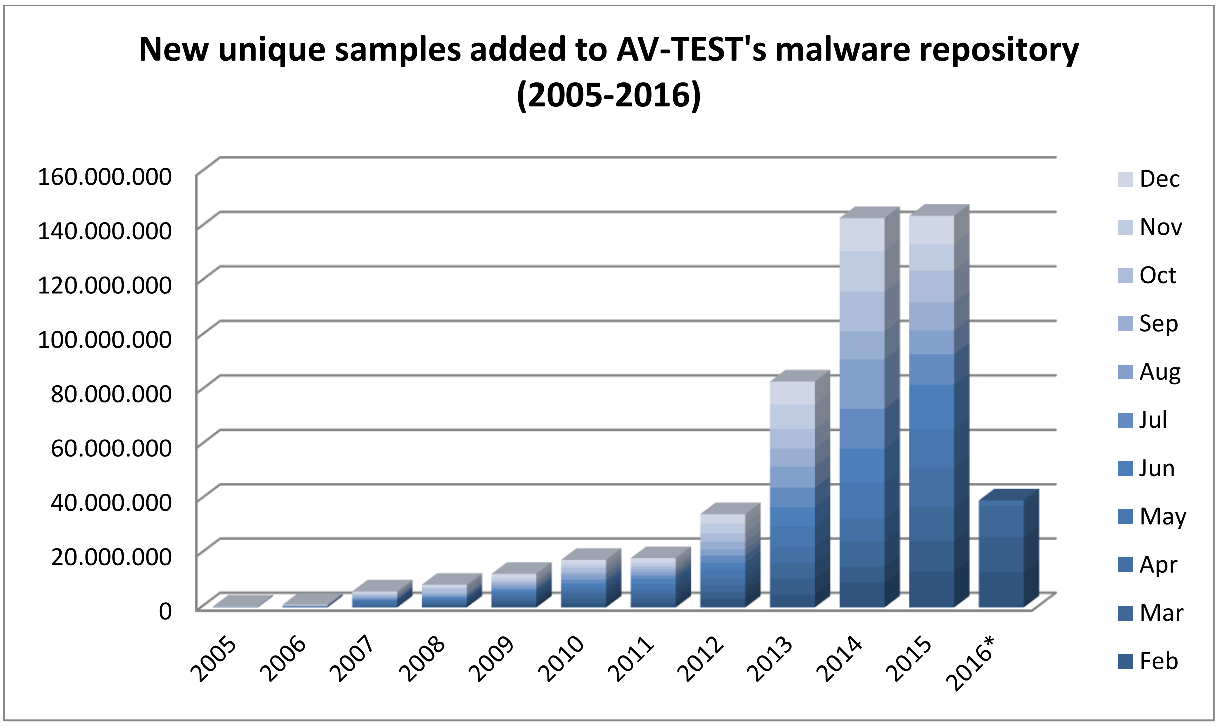


Figure 3: New malware samples per year

To protect the enterprise network against the enormous number of threats a multilayered security setup is recommended. The layers at a minimum should include the enterprise firewall, a web- and content-filter for every kind of traffic, which is the topic of this document, and an endpoint protection product as the last barrier for the malware.

A clever combination of those layers makes it hard for the attacking site to infiltrate the enterprise network.

Product Tested

The product Zscaler Web Security was tested. It is a cloud based web content filter with advanced threat protection, forensics and real-time analytics.

Methodology and Scoring

Platform

The test environment was set up according to figure 4. The client and webserver were physical machines. The Gateway was installed in line between the client and webserver. The webserver hosted the samples for the PE malware detection test. For the Real World test, the Client downloaded files from the sample URLs and notified the Zscaler Gateway after each URL. The Gateway allow or blocked the URL traffic.

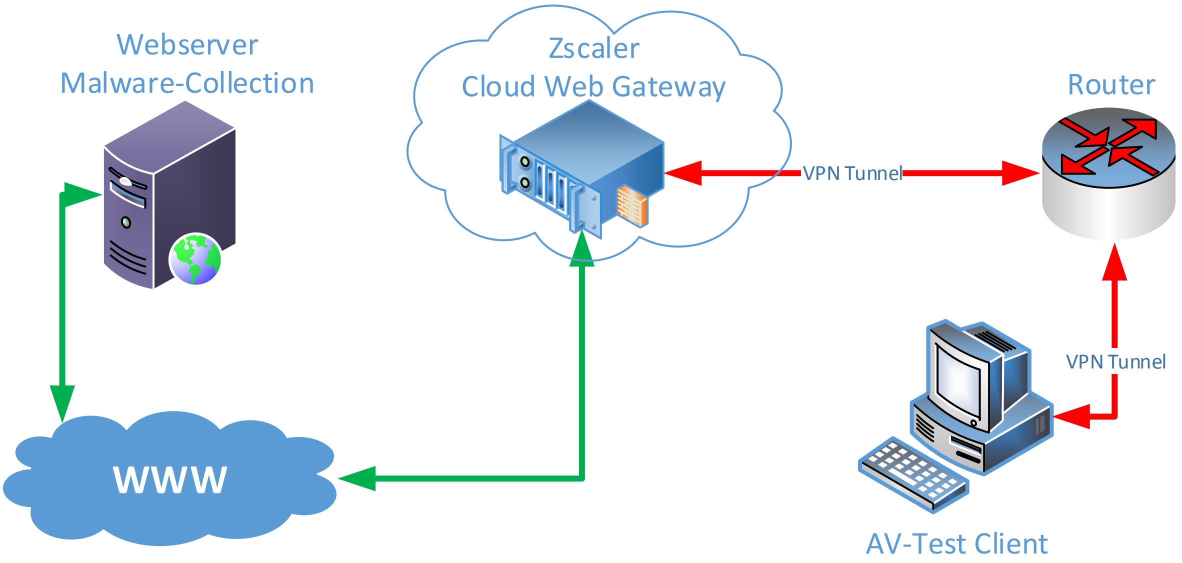


Figure 4: Test platform overview

Testing methodology

AV-TEST received preconfigured appliances from Zscaler and was supported by a Zscaler engineer to setup the appliances.

1. **Internet Access**. The appliances had access to the Internet at all times in order to use any in-the-cloud queries.
2. **Product Configuration**. The product was run with the configuration supplied by Zscaler. The appliance was able to perform automatic signature updates all the time.
3. **Testing**. All files, except for the malicious URLs, were downloaded via http from the webserver to the client system using a Java client. For the URL testing, an additional client with direct internet access has been used to download the reference samples from the Internet.
4. **Analysis**. The downloaded files were compared with the original files (reference files at URL testing) by MD5 hash. For verifying the results, the appliance report files were analyzed.

The static set of files consisted of 11,567 malicious PE files (Prevalent Malware).The dynamic tests were performed using 6,049 working malicious URLs.

Test Results

Test #1: Real World protection rate

Real World threats are typically identified through the Web Gateways ability to open up content for inspection coupled with whatever proactive scanning abilities and cloud intelligence a vendor may provide. A block can be based on URL filtering or Web Reputation services, by signatures or heuristic scanning of the provided content, and other inspection and filtering technologies. In this case 5892 of the 6049 malicious URLs were blocked. With this results Zscaler Web Gateway has a good protection rate of 97.40%.

Test #2: Sandbox detection rate

The total number of malicious samples tested was 11,567. This includes the following number of samples: 770 Backdoors, 558 Bots, 477 Trojan Downloader, 532 Trojan Dropper, 7,993 Trojan Generic, 179 Trojan Password Stealer, 733 Viruses, 211 Worms, 114 Rogue Software as well as 3,059 potentially unwanted applications (PUA).

This test focuses on the generic malware detection and blocking capabilities, especially on the signature-based detection as well as generic and heuristic technologies.

Type of Malware	Number of Samples	Detected Samples	%
Total Malware	11567	11557	99.91%
Backdoors	770	770	100.00%
Bots	558	558	100.00%
Trojan Downloader	477	477	100.00%
Trojan Dropper	532	532	100.00%
Trojan Generic	7993	7984	99.89%
Trojan PasswordStealer	179	178	99.44%
Virus	733	733	100.00%
Worms	211	211	100.00%
Rogue Software	114	114	100.00%

Figure 5: Sandbox detection results of malware

Type of Malware	Number of Samples	Detected Samples	%
Total PUA	3059	3044	99.51%

Figure 6: Sandbox detection results of PUA

It was expected that Zscaler Web Gateway will detect almost all samples, which it achieved with a detections rate of 99.91% only missing 10 files, which is very good.

Test #3: False Positives of popular Websites

The best detection rate is worthless if it involves a high false positive rate. Zscaler achieved a false positive rate of 0.11%. In this part of the test was tested clean popular websites. We also checked whether Zscaler miscategorized certain URLs. Only 2 out of 1886 URLs were not correctly assessed, which is a very good result.

Test #4: Social Engineering

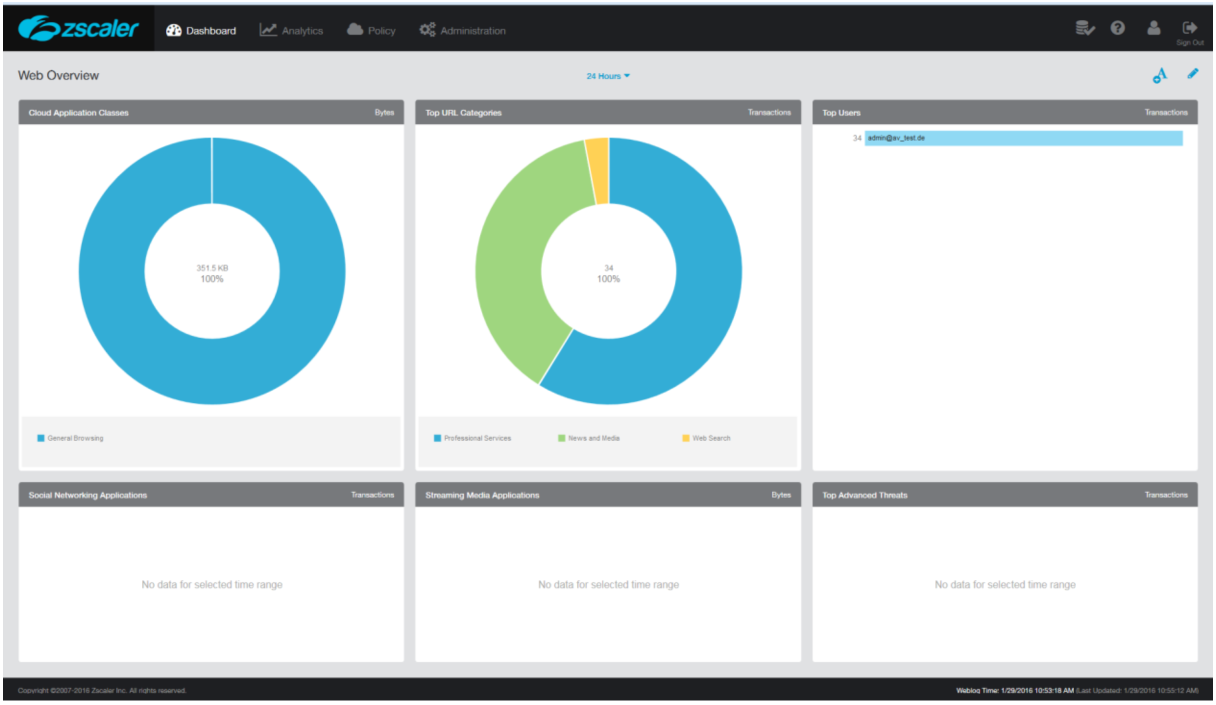
The phishing social engineering URL is very similar to the real one and you might not notice this on the first view. Phishing, also known as "brand spoofing", is an elaborate form of data theft, targeting possible clients. Zscaler achieved a detection rate of 100%. All 1,142 phishing URLs were detected, including forged websites of various companies, social platforms, banks, online banking services, government agencies and others.

Conclusion

With the given configuration, Zscaler scored very well in all reviewed categories. In the blocking of malicious content Zscaler achieved a near perfect result. False Positive testing didn't reveal any problems either. Only 2 benign websites were misclassified, which is a very good result taking into account the 1886 test cases.

The result of the test underlines the reliability of the Zscaler solution for corporate networks.

Appendix



No data for selected time range

No data for selected time range

No data for selected time range

Copyright ©2007-2016 Zscaler Inc. All rights reserved.

Weblog Time: 1/29/2016 10:53:18 AM (Last Updated: 1/29/2016 10:55:12 AM)

Figure 7: Dashboard of Zscaler Web Gateway