DNS-Layer Protection & Secure Web Gateway Security Efficacy Test

A test commissioned by Cisco Inc. and performed by AV-TEST GmbH

Date of the report: February 18th, 2020

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Contents

01

Executive Summary

In November and December 2019, AV-TEST performed a review of Cisco cloud security solutions alongside comparable offerings from Akamai, Infoblox, Palo Alto Networks, Symantec and Zscaler.

The test was commissioned by Cisco and performed by AV-TEST to determine the malware protection and phishing block capabilities of all vendors.

In order to ensure a fair review, the sponsor did not supply any samples (such as URLs or metadata) and did not influence or have any prior knowledge of the samples being tested. All products were configured to provide the highest level of protection, utilizing all security-related features available at the time. The test focused on the detection rate of links pointing directly to PE malware (e.g. EXE files), links pointing to other forms of malicious files (e.g. HTML, JavaScript) as well as phishing URLs. A total of 3,668 samples were tested.

In the first part of this study, DNS-layer protection was tested. DNS-layer protection uses the internet's infrastructure to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established as part of recursive DNS resolution. DNS-layer protection stops malware earlier and prevents callbacks to attackers if infected machines connect to your network.

DNS-layer protection with selective cloud proxy redirects only risky domain requests for deeper inspection of their web content, and does so transparently through the DNS response.

For the DNS-layer protection testing, the products achieved the following blocking rates:

Vendor	Detection rate Number of test cases 3,668
Cisco Umbrella (DNS-layer with selective proxy)	72.6%
Cisco Umbrella (DNS-layer)	51.8%
Infoblox BloxOne	35.3%
Akamai Enterprise Threat Protector	26.5%
Palo Alto Networks Next-Generation Firewall	13.7%

In the second part of the study, the web gateway solutions were tested. A secure web gateway is based on a full web proxy that sees and inspects all web connections. Unlike DNS-layer protection which only analyzes domain names and IP addresses, a web proxy sees all files and the full URLs enabling more granular inspection and control.

For secure web gateway testing, the products achieved the following blocking rates:

Vendor	Detection rate Number of test cases 3,668
Cisco Umbrella Secure Web Gateway	90.5%
Symantec Web Security Service	84.7%
Zscaler Internet Access	83.7%
Palo Alto Networks Prisma Access	72.4%

In both test scenarios, the Cisco Umbrella detection rate outperformed the other vendor's offerings. The full details of the testing can be found in the report below.

02

Overview

More than 4.4 new malware samples are identified by AV-TEST every second. That's more than 350,000 malware attacks per day, and while the majority of malware targets Windows platforms, securing protection across all operating systems is good practice. Attaining protection against the growing number of threats is essential for all enterprises.

In order to compare the different offerings available on the market, Cisco commissioned a test of Umbrella's DNS-layer protection offerings as well as comparable solutions from other providers. In addition, Umbrella's secure web gateway solution with full proxy was reviewed, and the effectiveness against other solutions was measured. The following definitions are used:

- DNS-layer protection: DNS-layer protection uses the internet's infrastructure to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established as part of recursive DNS resolution. DNS-layer protection is an effective way to stop malware earlier and prevent callbacks to attackers if infected machines connect to your network.

- DNS-layer protection with selective proxy: Traditional web gateways proxy all web connections – safe, malicious, and risky – sometimes negatively impacting network performance and availability. In some cases, their configuration can be complex, requiring PAC files and static routes. As part of the DNS-layer protection, a selective cloud proxy redirects only risky domain requests for deeper inspection of their web content, and does so transparently through the DNS response.

- Secure web gateway: A secure web gateway is based on a full web proxy that sees and inspects all web connections. Unlike DNS-layer protection which only analyzes domain names and IP addresses, a web proxy sees all files and the full URLs enabling more granular inspection and control.

Both DNS-layer protection and secure web gateway connections are prevalent across all client and server operating systems, giving enterprises the ability to protect all of their assets against a pervasive and expanding attack landscape.

03

Methodology: Test Cases

All of the data used for testing, including all samples, URLs and meta data, was exclusively sourced by AV-TEST.

No vendor had access to this data before the testing, nor did any included vendor provide such data for the testing. All samples were previously verified to be either malicious websites or phishing links. AV-TEST uses static and dynamic analysis of samples to ensure that the domains are actively hosting malicious content at the time of the testing and exhibit their malicious behavior.

Both performed tests were split into three categories, covering the different types of attacks:

- URLs pointing to malicious PE files (portable executables for Windows, EXE files)
- URLs with other malicious destinations (non-PE files, usually HTML or PHP websites, including links to scripts like JavaScript or VBS)
- Links to phishing websites

A total of 3,668 test cases were used. This includes 1,632 malicious links to PE files, 1,100 links to other files with other malicious content (non-PE), as well as 936 samples with phishing websites.

All of the URLs were accessed on virtualized Windows systems running the latest edition of Windows 10 Professional (version 1909), with all patches installed. The system was protected by the client software from the vendors (when applicable), or the network settings were adjusted accordingly, to ensure that the system is protected with the security solution from the vendor under testing.

All download attempts were triggered using Python scripts to access the URLs for the test. It was checked if the access to the URL was successfully blocked or the download of malicious content was possible. All product tests were performed at exactly the same time for any given URL. The tests were performed in November and December 2019 by AV-TEST.

04

Configuration for Test #1

DNS-Layer Protection Test

For the first part of the test, only the DNS-layer protection was reviewed. The following services were tested:

- Cisco Umbrella with only DNS-layer protection enabled
- Cisco Umbrella with DNS-layer protection and selective proxy
- Akamai Enterprise Threat Protector with DNS-layer protection and selective proxy
- Infoblox BloxOne (previously ActiveTrust Cloud) with DNS-layer protection
- Palo Alto Networks Next-Generation Firewall with DNS Security service enabled

In case of the DNS-layer protection test, the products were configured to provide the highest level of DNS protection, utilizing all DNS security-related features available at the time.

For both tests with Umbrella DNS-layer protection, all security settings were enabled. For Umbrella's DNS-layer protection with selective proxy the selective proxy was enabled with HTTPS inspection.

The Akamai DNS Security solution includes a selective proxy which was enabled with logging level 1, and risky domains and file sharing set to classify. All security settings were enabled to block malicious content.

The Infoblox solution does not have a selective proxy. Geolocation was enabled. For threat protection all feeds and threat insights were enabled and set to block.

Palo Alto Networks' DNS Security service was enabled on a Next-Generation Firewall. The testing determined if DNS queries sent through the firewall were blocked by this service (the service does not provide security as part of recursive DNS). To focus on Palo Alto Network's DNS security intelligence, no other security subscriptions were enabled on the Next-Generation Firewall, unless required to facilitate the DNS service's maximum functionality. The DNS proxy policy was set up with the latest signatures and both Palo Alto Networks content DNS signatures and DNS security signatures were set to sinkhole. No DNS policy exceptions were enabled.

05

Test Results #1

DNS-Layer Protection Test

In the case of the DNS-layer protection test, the following results were obtained.

The table shows the number of test cases (for every category and the total number) and the number of blocked samples for all solutions under test.

For this DNS-layer protection test, a higher number of blocked samples indicates better results.

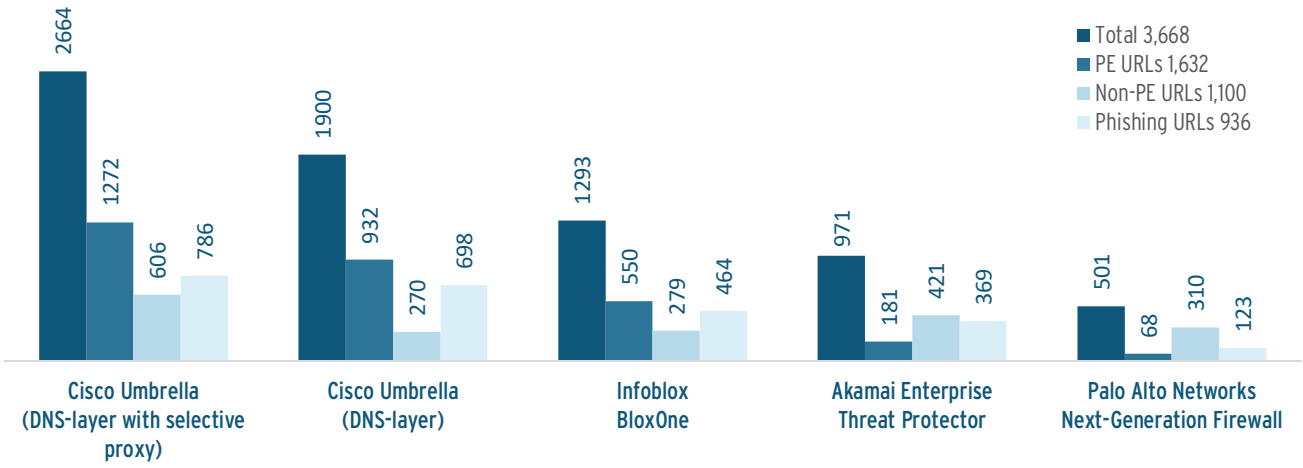
Vendor Number of test cases	Total 3,668	PE URLs 1,632	Non-PE URLs 1,100	Phishing URLs 936
Cisco Umbrella (DNS-layer with selective proxy)	2,664	1,272	606	786
Cisco Umbrella (DNS-layer)	1,900	932	270	698
Infoblox BloxOne	1,293	550	279	464
Akamai Enterprise Threat Protector	971	181	421	369
Palo Alto Networks Next-Generation Firewall	501	68	310	123

The protection rate for all tested solutions can be found in the following table.

Vendor Number of test cases	Total 3,668	PE URLs 1,632	Non-PE URLs 1,100	Phishing URLs 936
Cisco Umbrella (DNS-layer with selective proxy)	72.6%	77.9%	55.1%	84.0%
Cisco Umbrella (DNS-layer)	51.8%	57.1%	24.5%	74.6%
Infoblox BloxOne	35.3%	33.7%	25.4%	49.6%
Akamai Enterprise Threat Protector	26.5%	11.1%	38.3%	39.4%
Palo Alto Networks Next-Generation Firewall	13.7%	4.2%	28.2%	13.1%

Cisco Umbrella DNS-layer protection with selective proxy performed best in all test scenarios, blocking 72.6% of all malicious content. Even without the selective proxy enabled, Cisco Umbrella DNS-layer security was still able to block more than 50% of the malware and phishing websites. Infoblox was only able to block just over 35% of the test cases. Akamai blocked only around 26% of the URLs used in the testing. The DNS-layer solution offered by Palo Alto Networks performed worst in most testing scenarios, blocking just over 13% of the test cases.

Test Results #1:
DNS-Layer Protection Test



February 18th, 2020

06

Configuration for Test #2

Secure Web Gateway Test

For the second part of the test, the protection offered by cloud-based secure web gateway and cloud firewall solutions were reviewed. The following products were tested:

- Cisco Umbrella Secure Web Gateway (SWG)
- Palo Alto Networks Prisma Access (previously GlobalProtect Cloud Services)
- Symantec Web Security Service (WSS)
- Zscaler Internet Access (ZIA)

All products were configured to provide the highest level of protection, utilizing all security-related features available at the time.

In the case of Cisco, Umbrella's full-proxy secure web gateway was used in this test, and the DNS-layer protection was not enabled. Umbrella's web policy had all security settings, file inspection and HTTPS inspection enabled.

Palo Alto Networks' Prisma Access product was tested with several subscriptions enabled. Subscriptions enabled include antivirus, anti-spyware, URL filtering, vulnerability protection, Wildfire & file blocking. All subscriptions had the latest signatures and were configured per best practice recommendations.

Symantec's Web Security Service was used in this test with content and malware analysis enabled. The default content and threat protection policy was applied.

Zscaler's ZIA product was used in this test with malware, advanced threat, sandbox, browser control, SSL inspection, all enabled with the Zscaler recommended policy.

07

Test Results #2

Secure Web Gateway Test

For the second part of the testing, focusing on the full proxy of security options, the following results were obtained.

The table shows the number of test cases (for every category and the total number) and the number of blocked samples for all solutions being tested.

For this protection test, a higher number of blocked samples indicates better results.

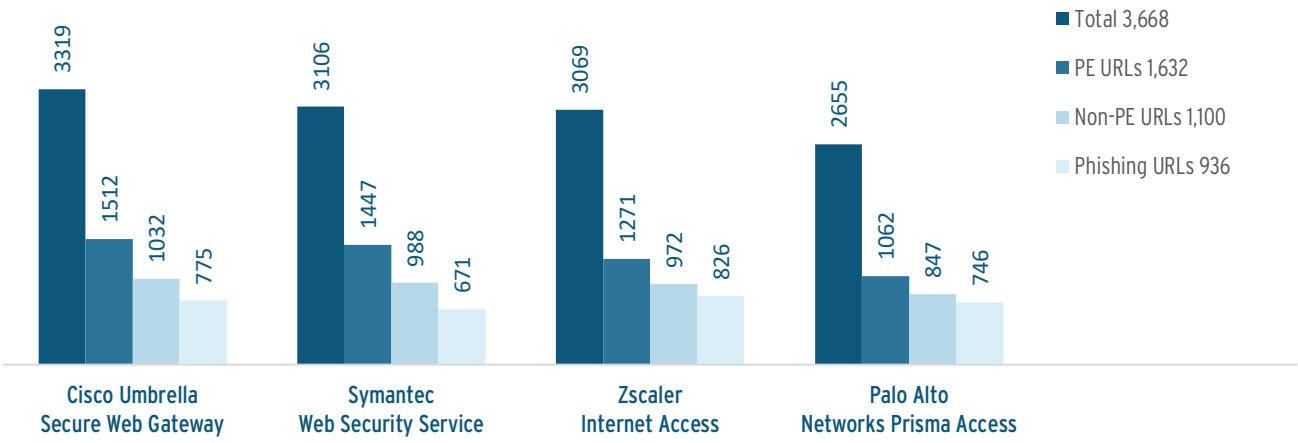
Vendor Number of test cases	Total 3,668	PE URLs 1,632	Non-PE URLs 1,100	Phishing URLs 936
Cisco Umbrella Secure Web Gateway	3,319	1,512	1,032	775
Symantec Web Security Service	3,106	1,447	988	671
Zscaler Internet Access	3,069	1,271	972	826
Palo Alto Networks Prisma Access	2,655	1,062	847	746

The protection rate for all tested solutions can be found in the following table.

Vendor Number of test cases	Total 3,668	PE URLs 1,632	Non-PE URLs 1,100	Phishing URLs 936
Cisco Umbrella Secure Web Gateway	90.5%	92.6%	93.8%	82.8%
Symantec Web Security Service	84.7%	88.7%	89.8%	71.7%
Zscaler Internet Access	83.7%	77.9%	88.4%	88.2%
Palo Alto Networks Prisma Access	72.4%	65.1%	77.0%	79.7%

In the case of the secure web gateway test, all products performed significantly better when compared with the DNS-layer protection test. Cisco Umbrella successfully blocked more than 90% of the malicious and phishing content. The solutions from Symantec and Zscaler performed at a similar level of protection, but at a weaker protection level, both at less than 85%. The solution offered by Palo Alto Networks was able to protect against less than 73% of the threats in the test.

Test Results #2:
Secure Web Gateway Test



February 18th, 2020

08

Conclusion

In both test scenarios, Cisco Umbrella outperformed the other vendor offerings.

In the DNS-layer protection test, Cisco Umbrella outperformed the next competitor by a factor of two.

In the secure web gateway test, the scores of the other vendors were higher, but Cisco Umbrella Secure Web Gateway still performed best.

The test results demonstrate that organizations should adopt a layered approach to security. DNS-layer protection is simple and effective and in use cases where deploying a selective proxy is possible, doing so adds to the overall efficacy. A secure web gateway full proxy solution provides the highest level of protection as seen in the test results.

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

About **AV-TEST**

AV-TEST GmbH is an independent supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software and its use in comprehensive comparative testing of security products.

Due to the timeliness of the testing data, malware can instantly be analyzed and categorized, trends within virus development can be detected early, and IT-security solutions can be tested and certified. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, special interest magazines to publish research data, and end users to make good product choices.

AV-TEST has operated out of Magdeburg (Germany) since 2004 and employs more than 30 team members, professionals with extensive practical experience.

The AV-TEST laboratories include 300 client and server systems, where more than 2,500 terabytes of independently-collected test data, containing both malicious and harmless sample information, are stored and processed.

For more information please visit our website at https://www.av-test.org .

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org