AV-TEST Evaluates Secure Web Gateway and DNS-Layer Security Efficacy

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

Report Date: October 28th, 2020

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Contents

01

Executive Summary

In September and October 2020, AV-TEST performed a lab test of comparable security offerings from Akamai, Cisco, Infoblox, Netskope, Palo Alto Networks, and Zscaler.

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

The lab test assessed each secure web gateway vendor's ability to protect roaming and remote workers. Given that the global pandemic has accelerated the move of edge security controls to a cloud-delivered model, each of the vendors' offerings was configured with the protection of their roaming agents. A separate test for DNS-layer protection was also performed.

In order to ensure a fair review, the sponsor did not supply any samples (such as malicious or clean samples, URLs or associated metadata) and did not influence or have any prior knowledge of the samples tested or the testing methodology. 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 portable executables (PEs) 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 3,572 malicious samples were tested. All links and malicious samples tested were verified by AV-TEST as recent and active.

In addition, AV-TEST evaluated false positive ratings for each vendor. AV-TEST assessed downloads for well-known applications from HTTP and HTTPS websites. An additional false positive test was performed against known clean popular websites from Alexa's top list. A total of 2,165 clean websites and downloads were used.

In the first part of the study, secure 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 and inspects all files and the full URLs, enabling more granular inspection and control.

For secure web gateway testing, the products achieved the following blocking and false positive rates (ordered by best detection rate):

Product Number of test cases	Package	Detection rate 3,572	False positive rate 2,165
Cisco Umbrella	SIG Essentials	96.39%	0.65%
Zscaler Internet Access	Transformation	89.67%	0.69%
Palo Alto Networks Prisma Access	Prisma Access for Mobile Users	73.15%	1.29%
Netskope Secure Web Gateway	Cloud Inline Protection	61.90%	4.53%
Akamai Enterprise Threat Protector	Advanced Threat	58.43%	1.89%

In the second 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 a selective cloud proxy redirects specific requests for deeper inspection of their web content and full URLs to improve security efficacy. This process is accomplished transparently through the DNS response. The increased security efficacy with the selective proxy does not add latency to known safe domains or increase the rate of false positives. The Cisco Umbrella DNS Security and Akamai Enterprise Threat Protector offerings include a selective proxy. Umbrella's selective proxy inspects risky domains to ensure malicious content is blocked. Akamai's selective proxy supports proxying risky domains as well as file sharing applications.

For the DNS-layer protection testing, the products achieved the following blocking and false positive rates (ordered by best detection rate):

Product Number of test cases	Package	Detection rate 3,572	False positive rate 2,165
Cisco Umbrella	DNS Security Advantage	70.69%	0.28%
Akamai Enterprise Threat Protector	Intelligence	53.58%	1.34%
Infoblox BloxOne	Advanced	36.28%	11.78%

In both test scenarios, Cisco Umbrella outperformed the other vendor's detection rates. Umbrella also had the lowest false positive rate. The full details of the testing can be found in the detailed sections of the report below.

02

Overview

More than 130 million malware samples are discovered by AV-TEST every year; that's about 350,000 malware attacks per day or around 4 new samples every second.

While most 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. Phishing is a great example of an attack that impacts all operating systems and relies on fooling the end user into thinking the site is legitimate so the attacker can steal sensitive information.

In order to compare some of the different offerings available on the market, Cisco commissioned a test of Umbrella's secure web gateway solution with full proxy as well as comparable solutions from other vendors. In addition, Umbrella's DNS-layer protection 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.

- **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, web gateway configurations can be complex, requiring PAC files and static routes. As part of Umbrella's DNS-layer protection, only risky domain requests are redirected to a selective cloud proxy for deeper inspection of their web content. This redirection is done 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 secure web gateway and DNS-layer protection can be leveraged across all client and server operating systems, giving enterprises the ability to protect all their assets against a pervasive and expanding attack landscape.

03

Methodology: Test Cases

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

No vendor had access to sample URLs before the testing, nor did any included vendor provide such data for the testing. All samples were previously verified by AV-TEST to actually be malicious. 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 (for Windows, EXE files)
- URLs with other malicious destinations (non-PE files, usually HTML or PHP websites, including links to scripts such as JavaScript or VBS)
- Links to phishing websites

A total of 3,572 samples were used. This included 850 malicious links to PE files, 1,756 links to other files with other malicious content (non-PE), and 966 samples with phishing websites.

For false positive testing, AV-TEST used the following types of known clean files and websites from HTTP and HTTPS sources:

- URLs pointing to clean file downloads (mainly PE for Windows, EXE files)
- URLs with other non-malicious destinations (non-PE files, usually HTML or PHP websites, including links to scripts such as JavaScript or VBS)

All samples used for the false positive testing were carefully selected and validated. In an exhaustive review by AV-TEST, the samples did not show any signs of malicious behavior and were considered clean. A total of 2,165 clean websites and downloads were used (715 downloads and 1,450 websites).

All URLs were accessed on virtualized Windows systems running Windows 10 Professional (version 1909), with all patches installed. For all vendors participating in the full web proxy testing, platform specific endpoint agent software was used to protect the test machine, simulating a remote worker. Given that remote agents were used, only features supported by the roaming agents were included in the testing. DNS testing was configured via network settings to simulate on-network protection.

All download attempts were triggered using Python scripts to access the URLs for the test. Testing included checking if access to the URL was successful or if it was blocked by the product. All samples were processed at the same time for any given URL. The tests were performed in September and October, 2020 by AV-TEST.

04

Configuration for Test #1: Secure Web Gateway Test

For the first part of the test, the protection offered by cloud-based secure web gateways was evaulated.

The following products and associated packages were tested:

- Cisco Umbrella – SIG Essentials
- Akamai Enterprise Threat Protector – Advanced Threat
- Netskope Secure Web Gateway – Cloud Inline Protection
- Palo Alto Networks Prisma Access – Prisma Access for Mobile Users
- Zscaler Internet Access – Transformation

All services were configured to provide the highest level of protection, utilizing all security-related features available at the time. Retroactive sandboxing was not enabled, even if supported. Testing focused on zero day threat protection and each sample URL was only processed once. For service configuration, any setting not specifically mentioned was disabled.

Cisco Umbrella Configuration

The Cisco Umbrella SIG Essentials package with full-proxy secure web gateway was used in this test. Since this package includes DNS-layer protection, this functionality was also enabled. The DNS policy for full-proxy testing included the following security categories: malware, newly seen domains, command and control callbacks, phishing attacks, potentially harmful domains, DNS tunneling VPN, and cryptomining. Umbrella's DNS selective proxy and content filtering were disabled.

For Umbrella's web policy, HTTPS was inspection enabled for all content categories with the Cisco Umbrella issued certificate authority. All possible security settings were enabled (malware, command and control callbacks, and phishing attacks). File inspection was also enabled. The following features were disabled: destination lists, content categories, application blocks, file type controls, tenant controls. The test endpoint was running Cisco AnyConnect version 4.9.01095.

Palo Alto Networks (PAN) Prisma Access Configuration

Palo Alto Networks' Prisma Access for mobile user was configured and managed via the Prisma Access App (cloud managed). The policy consisted of a number of defaults and included best practice rules, as well as some custom ones. The out-of-the-box rule: drop-outbound-malicious-ip was enabled to drop traffic to the PAN-defined destination address list of panw-known-ip-list. HTTPS decryption was enabled for all destinations using SSL forward proxy and the best-practice-ssl-decryption profile. HTTP/S and new apps had the same group of security profiles enabled. These security profile groups consisted of the antivirus profile which was set to the out-of-the-box best-practice profile. Anti-spyware used the out-of-the-box best-practice-strict profile. Vulnerability protection used the out-of-the-box best-practice-strict profile. URL filtering used a custom list that blocked site access and user credentials submission on the following content categories: command and control, cryptocurrency, grayware, malware, and phishing. File blocking and Wildfire analysis were disabled. Being cloud managed, all signatures are automatically updated by Palo Alto Networks. The GlobalProtect client version 5.1.5 was used in the testing.

Zscaler Internet Access (ZIA)

Zscaler's ZIA product was used in this test with malware, advanced threat, browser control and SSL inspection enabled per the Zscaler recommended policy. Blocked content categories at proxy and DNS-layer included other security and spyware/adware. Proxy content categories were enforced across all supported protocols and request types. Sandboxing was enabled for all supported file types with allow and scan new files. Subsequent downloads were set to block. File type, cloud app & bandwidth controls were all disabled. The test client was configured with the Zscaler client connector version 2.1.2.112.

Netskope Secure Web Gateway (SWG) Configuration

Netskope SWG was setup and configured to steer all web traffic to the platform for protection. SSL Decryption was enabled, and all secure web traffic was decrypted. No category exceptions were configured. Real-time policies were configured for malware file blocking and content security categories. The content categories blocked include: security risk, ad fraud, attacks, botnets, command and control servers, compromised/malicious sites, cryptocurrency mining, DGA, malware call-home, malware distribution point, phishing/fraud, spam sites, spyware and questionable software. The file block policy was applied to all cloud apps with the threat protection malware profile of default malware scan. The file block policy was applied to the download and upload activities. Access method was set to client and the user type was user. The actions for events of low, medium, and high were set to block. The Netskope client version used was 79.0.0.509.

Akamai Enterprise Threat Protector (ETP) Configuration

Akamai ETP was setup and configured with the ETP client and full proxy. Akamai's full proxy follows a similar configuration and enforcement as their DNS Selective proxy, with the exception of the proxy default action set to classify. The threat policy for both known and suspected malware, phishing, command and control, and DNS exfiltration all were set to block. The proxy was enabled with logging level one with HTTPS inspection enabled and the Akamai issued root certificate authority. Proxy options for the default action, risky domains & file sharing were all set to classify. The setting for invalid certificate responses was set to bypass. All other options were disabled. The ETP endpoint client version 3.1.1 was used during the testing.

05

Test Results #1: Secure Web Gateway Test

For the first part of the testing focusing on the full proxies, the following results were obtained.

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

For this protection test, a higher number of blocked samples and a low false positive rate indicate better results.

Vendor Number of test cases	Blocking rate (total) 3,572	PE URLs 850	Non-PE URLs 1,756	Phishing URLs 966
Cisco Umbrella	3,443	796	1,741	906
Zscaler Internet Access	3,203	742	1,638	823
Palo Alto Networks Prisma Access	2,613	713	1,016	884
Netskope Secure Web Gateway	2,211	698	975	538
Akamai Enterprise Threat Protector	2,087	522	849	716

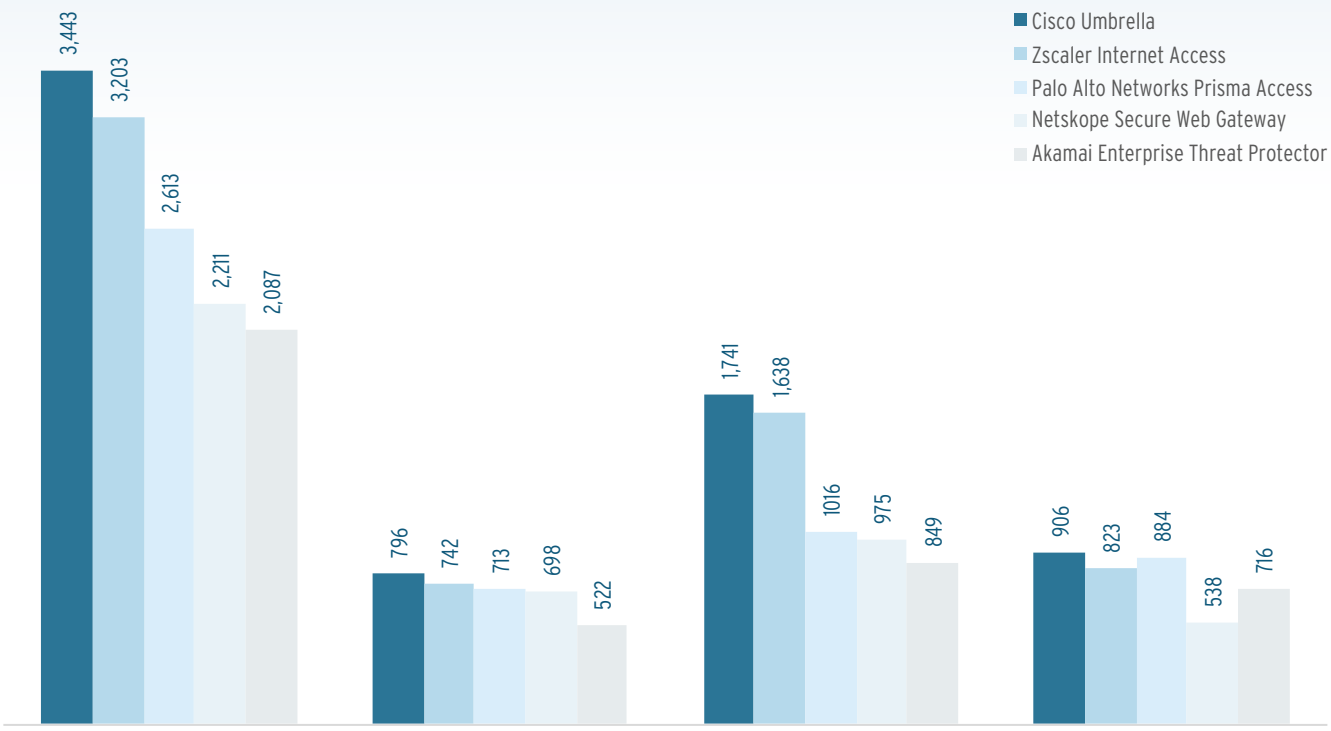
Vendor Number of test cases	False positives (total) 2,165	Downloads 715	Websites 1,450
Cisco Umbrella	14	14	0
Zscaler Internet Access	15	12	3
Palo Alto Networks Prisma Access	28	25	3
Netskope Secure Web Gateway	98	34	64
Akamai Enterprise Threat Protector	41	28	13

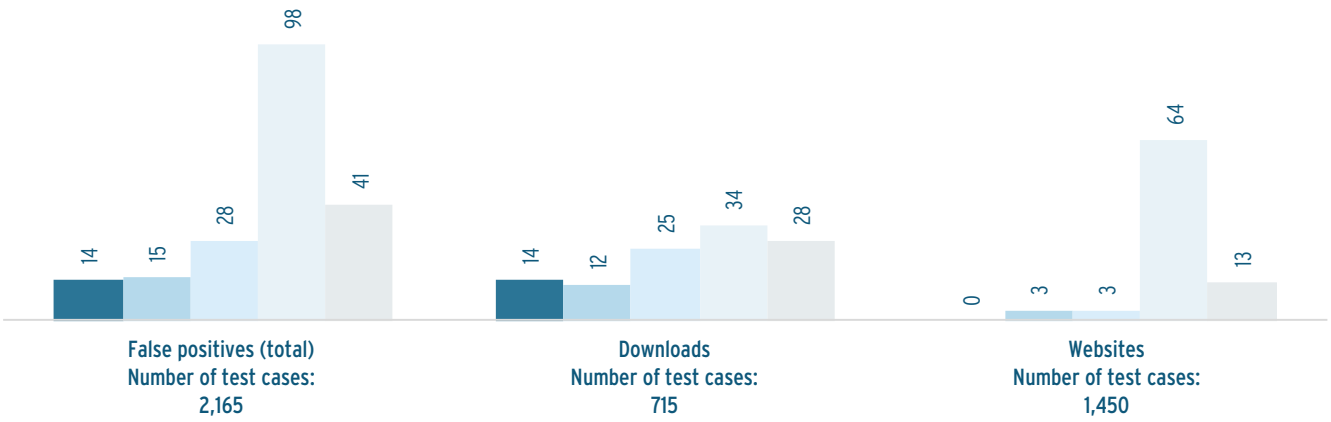
The protection rate for all tested solutions can be found in the following table.

Vendor Number of test cases	Blocking rate (total) 3,572	PE URLs 850	Non-PE URLs 1,756	Phishing URLs 966
Cisco Umbrella	**96.39%**	93.65%	99.15%	93.79%
Zscaler Internet Access	**89.67%**	87.29%	93.28%	85.20%
Palo Alto Networks Prisma Access	**73.15%**	83.88%	57.86%	91.51%
Netskope Secure Web Gateway	**61.90%**	82.12%	55.52%	55.69%
Akamai Enterprise Threat Protector	**58.43%**	61.41%	48.35%	74.12%

Vendor Number of test cases	False positives (total) 2,165	Downloads 715	Websites 1,450
Cisco Umbrella	**0.65%**	1.96%	0.00%
Zscaler Internet Access	**0.69%**	1.68%	0.21%
Palo Alto Networks Prisma Access	**1.29%**	3.50%	0.21%
Netskope Secure Web Gateway	**4.53%**	4.76%	4.41%
Akamai Enterprise Threat Protector	**1.89%**	3.92%	0.90%

Cisco Umbrella successfully blocked more than 95% of all malicious and phishing content with the lowest false positive rate of all tested services. The solution from Zscaler reached almost 90%. The solution offered by Palo Alto Networks was not able to reach the 75% checkmark. Netskope as well as Akamai only detected around 60% of the malicious and phishing content and showed a higher false positive rate at the same time. Akamai's efficacy with their full proxy secure web gateway performed worst in the test, only detecting slightly more than 58% of the malicious samples.


Cisco Umbrella
Zscaler Internet Access
Palo Alto Networks Prisma Access
Netskope Secure Web Gateway
Akamai Enterprise Threat Protector
3,443
3,203
2,613
2,211
2,087
796
742
713
698
522
1,741
1,638
1016
975
849
906
823
884
538
716
Blocking rate (total)
Number of test cases:
3,572
PE URLs
Number of test cases:
850
Non-PE URLs
Number of test cases:
1,756
Phishing URLs
Number of test cases:
966


14
15
28
98
41
14
12
25
34
28
0
3
3
64
13
False positives (total)
Number of test cases:
2,165
Downloads
Number of test cases:
715
Websites
Number of test cases:
1,450

06

Configuration for Test #2: DNS-Layer Protection Test

For the second part of the test, only the DNS-layer protection was reviewed.

The following services and associated packages were tested:

- Cisco Umbrella – DNS Security Advantage with selective proxy
- Akamai Enterprise Threat Protector (ETP) – Intelligence with selective proxy
- Infoblox BloxOne Threat Defense - Advanced

For the DNS-layer protection tests, all products were configured to provide the highest level of DNS protection, utilizing all DNS security-related features and feeds available at the time, as well as the selective proxy where available. For policy configuration, any setting not specifically mentioned was disabled.

Umbrella DNS-layer protection was configured with the following security settings enabled: malware, newly seen domains, command and control callbacks, phishing attacks, potentially harmful domains, DNS tunneling VPN, and cryptomining. The selective proxy was enabled along with SSL decryption and file analysis. No content categories were blocked.

Akamai DNS-layer protection includes a selective proxy with HTTPS support, which was enabled with proxy logging level one. Risky domains & file sharing was set to classify and invalid certificate response set to bypass. All known threats were set to block with alerts enabled and suspected threats set to monitor with alerts enabled.

Infoblox DNS-layer protection was configured with geolocation disabled. Infoblox BloxOne Threat Defense does not have a selective proxy and, therefore, HTTPS decryption is also not an option. All 32 feeds and threat insights were set to block. Blocked content categories included: malicious sites, phishing, PUPs, spam URLs, and spyware/adware/keyloggers.

07

Test Results #2: DNS-Layer Protection Test

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

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

For this DNS-layer protection test, a higher number of blocked samples and a low false positive rate indicate better results.

Vendor Number of test cases	Blocking rate (total) 3,572	PE URLs 850	Non-PE URLs 1,756	Phishing URLs 966
Cisco Umbrella	2,525	686	972	867
Akamai ETP	1,914	462	740	712
Infoblox BloxOne Threat Defense	1,296	318	410	568

Vendor Number of test cases	False positives (total) 2,165	Downloads 715	Websites 1,450
Cisco Umbrella	6	6	0
Akamai ETP	29	22	7
Infoblox BloxOne Threat Defense	255	56	199

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

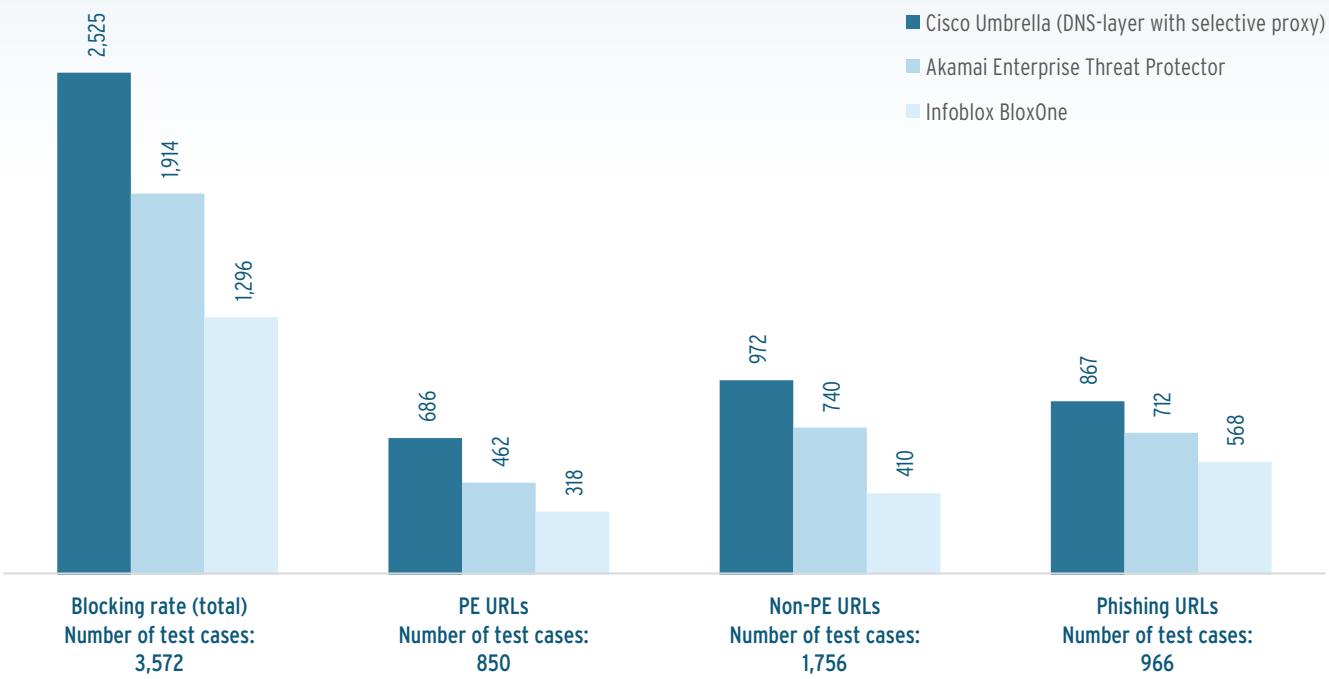
Vendor Number of test cases	Blocking rate (total) 3,572	PE URLs 850	Non-PE URLs 1,756	Phishing URLs 966
Cisco Umbrella	**70.69%**	80.71%	55.35%	89.75%
Akamai ETP	**53.58%**	54.35%	42.14%	73.71%
Infoblox BloxOne Threat Defense	**36.28%**	37.41%	23.35%	58.80%

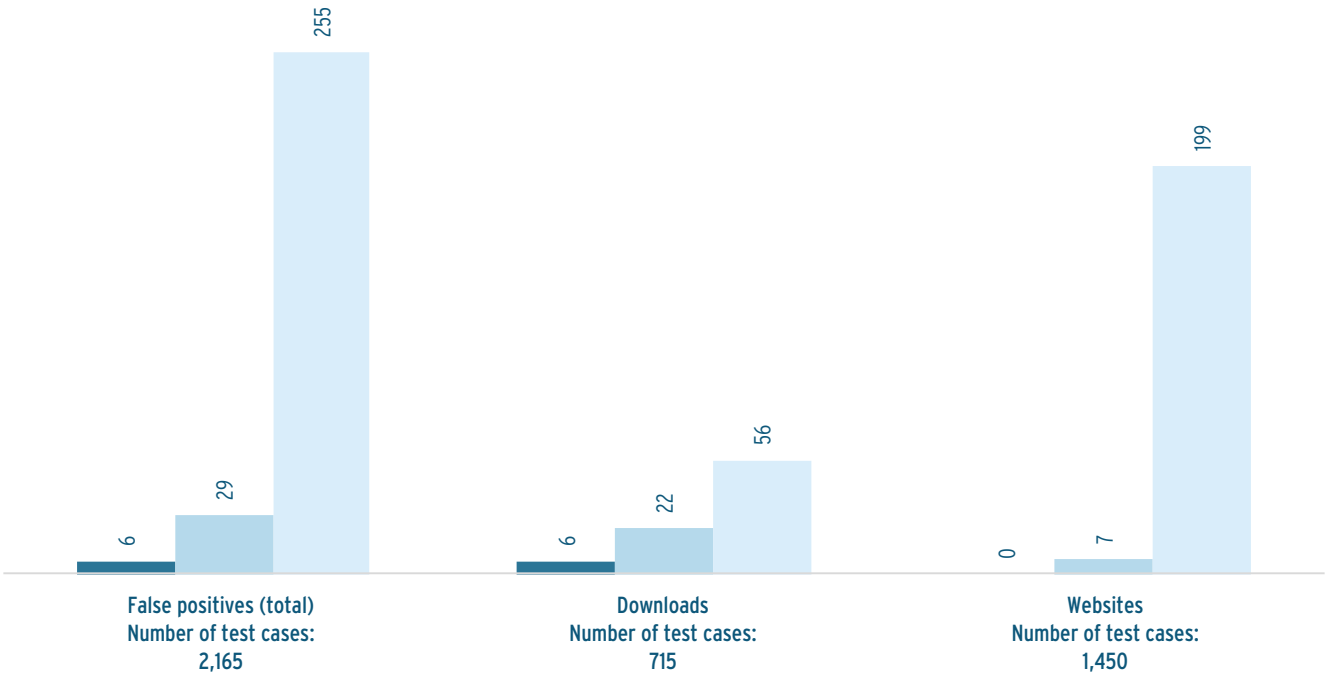
Vendor Number of test cases	False positives (total) 2,165	Downloads 715	Websites 1,450
Cisco Umbrella	**0.28%**	0.84%	0.00%
Akamai ETP	**1.34%**	3.08%	0.48%
Infoblox BloxOne Threat Defense	**11.78%**	7.83%	13.72%

When comparing between the secure web gateway and DNS test cases, in general the blocking rates from the secure web gateway test are higher than the DNS-layer protection test.

Cisco Umbrella DNS Security Advantage performed the best in all test scenarios, blocking 70.69% of all malicious content. Akamai blocked only 53.58% of the URLs used in the DNS-layer protection testing, compared to their block rate of 58.43% in the secure web gateway test. Infoblox was only able to block just 36.28% of the test cases.

A note about the Infoblox results: the threat feed "EECN_IP" was set to block during the testing. This feed includes country blocks which are described as "these countries are often found in cyber-attacks seeking intellectual property or other sensitive or classified data and stealing credit card or financial information." This feed contributed towards the block rates in the malware and phishing testing, but it also led to a majority of the false positives measured.


Cisco Umbrella (DNS-layer with selective proxy)
Akamai Enterprise Threat Protector
Infoblox BloxOne
2,525
1,914
1,296
686
462
318
972
740
410
867
712
568
Blocking rate (total)
Number of test cases:
3,572
PE URLs
Number of test cases:
850
Non-PE URLs
Number of test cases:
1,756
Phishing URLs
Number of test cases:
966


6
29
255
6
22
56
0
7
199
False positives (total)
Number of test cases:
2,165
Downloads
Number of test cases:
715
Websites
Number of test cases:
1,450

08

Conclusion

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

In the secure web gateway test, Cisco Umbrella SIG-Essentials (with secure web gateway and DNS-layer security), performed best in the test and demonstrated a higher detection and lower false positive rate than all other tested solutions.

In the DNS-layer protection test, Cisco Umbrella DNS Security Advantage (with selective proxy) also clearly outperformed the other vendors in case of malware and phishing protection as well as in false positive avoidance.

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, and when combined with DNS-layer security, this is further enhanced.

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