# AV-TEST Evaluates Secure Web Gateway & DNS-Layer Security Efficacy, DNS Tunneling Protection

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

Report Date: September 26, 2022

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# Contents

# 01

## Executive Summary

Between June-September 2022, AV-TEST performed a lab test of comparable security offerings from Cisco Umbrella, Cloudflare, DNSFilter, Iboss, Infoblox, Netskope, Palo Alto Networks, Skyhigh Security (formerly McAfee), and Zscaler.

The scope of this test focused on secure web gateway and DNS-layer security, including the ability to detect and block DNS tunneling.

The test was commissioned by Cisco and performed by AV-TEST to determine the various vendors' malware and phishing block capabilities, as well as DNS tunneling protection.

In order to ensure a fair review, Cisco as a 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 in the specific test cases, utilizing the security related features available at the time of testing.

The first and second parts of 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 3,682 malicious samples were used for the secure web gateway test. The number of test cases for the DNS-layer security test covered 3,154 objects. All links and malicious samples tested were verified by AV-TEST as recent and active.

In these test cases, AV-TEST also evaluated the 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 2,984 clean websites and downloads were used.

The third part of the test focused on testing the ability of the solutions to protect against malicious data exfiltration sent via DNS tunneling.

## Security Efficacy Results

In the first part of the test, secure web gateway solutions were tested. A secure web gateway is based on a full web proxy that inspects all web connections. Unlike DNS-layer security which only analyzes domain names and IP addresses, a web proxy inspects all aspects of the connection and payload. For secure web gateway testing, the evaluated products listed below achieved the following blocking and false positive rates (ordered by best blocking detection rate):

| Vendor<br>Number of test cases | Package | Detection rate<br>3,682 | False positive rate<br>2,984 |
|---|---|---|---|
| Cisco Umbrella | SIG Advantage | 90.41% | 1.44% |
| Netskope | Secure Web Gateway | 80.12% | 0.57% |
| Zscaler | Internet Access Transformation | 79.60% | 0.44% |
| Palo Alto Networks | Prisma Access for Mobile Users | 79.33% | 3.42% |
| Skyhigh Security | Secure Web Gateway | 63.96% | 0.60% |
| Iboss | Zero Trust Edge | 44.60% | 0.20% |

The second part of this test evaluated DNS-layer security. DNS-layer security uses the internet's infrastructure to block malicious and unwanted domains, and cloud applications before a connection is ever established as part of recursive DNS resolution.

DNS-layer security with a selective cloud proxy redirects specific requests seen as risky 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 provided by the selective proxy does not add latency to known safe domains and can help to decrease the rate of false positives.

As part of the DNS-layer security testing, the evaluated products listed below achieved the following blocking and false positive rates (ordered by best blocking detection rate):

| Vendor<br>Number of test cases | Package | Detection rate<br>3,154 | False positive rate<br>2,984 |
|---|---|---|---|
| Cisco Umbrella | DNS Security Advantage | 65.44% | 0.23% |
| DNSFilter | DNSFilter | 34.84% | 0.10% |
| Infoblox | BloxOne Advanced | 24.10% | 0.03% |

In both the secure web gateway and DNS-layer security test scenarios, Cisco Umbrella outperformed the other vendors' detection rates. For the achieved detection rate, Umbrella also had a reasonable false positive rate. The full details of the testing can be found in the detailed sections of the report below.

## DNS Tunneling Results

In the third and final part of the test, AV-TEST reviewed the protection against DNS tunneling mechanisms. As DNS is usually considered a trustworthy service, it's not blocked or limited in most firewalls. DNS tunneling is a method of sending data over the DNS protocol, whereby the DNS protocol is misused to tunnel malware and other data through client-server communication.

Three different tools (DNSCat2, DNSExfiltrator and Iodine) were used to assess the level of protection for DNS tunneling attacks.
The solutions Cisco Umbrella, Cloudflare, DNSFilter and Infoblox were reviewed.

| Vendor | Package | Protection against: | | |
|---|---|---|---|---|
| | | DNSCat2 | DNSExfiltrator | Iodine |
| Cisco Umbrella | DNS Security Advantage | 50% | 100% | 100% |
| Cloudflare | Secure Web Gateway | 0% | 50% | 100% |
| DNSFilter | DNSFilter | 100% | 0% | 100% |
| Infoblox | BloxOne Advanced | 0% | 0% | 100% |

In the DNS tunneling test scenario, Cisco Umbrella again offered the best protection out of the tested solutions.

# 02

## Overview

More than 120 million malware samples are discovered by AV-TEST every year; that's about 330,000 malware attacks per day or almost 4 new malicious samples every second.

While most malware targets Windows platforms, securing protection across all operating systems, including but not limited to MacOS and Linux, is a 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 evaluate some of the offerings available on the market, Cisco commissioned a test of Umbrella's secure web gateway solution with full web proxy as well as comparable solutions from other vendors. In addition, Umbrella's DNS-layer security was reviewed, and the effectiveness against other solutions was measured. The last part of the test focused on testing the ability of solutions to detect and protect against malicious data exfiltration sent via DNS tunneling.

The following definitions are used:

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

- **DNS-layer security:** DNS-layer security uses the internet's infrastructure to block malicious and unwanted domains, and cloud applications before a connection is ever established as part of recursive DNS resolution. DNS-layer security is an effective way to stop malware at the earliest possible point and to prevent callbacks to attackers. Some DNS-layer security solutions include a selective proxy, where requests to risky domains are redirected to the cloud proxy for deeper inspection of their web content and full URL. This redirection is done transparently through the DNS response, increasing the security efficacy while keeping the deployment method simple.

- **DNS tunneling:** DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53. It sends http(s) and other protocol traffic over DNS. There are various, legitimate reasons to utilize DNS tunneling. For example, DNS tunneling is often used as a login mechanism for hotspot security controls at airports or hotels to access the internet. However, there are also malicious reasons to use DNS Tunneling VPN services. This includes data exfiltration and command & control server callbacks used for various malware attacks, or to bypass local (policy) restrictions.

# 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 be malicious.

AV-TEST used static and dynamic analysis of samples to ensure that the domains were actively hosting malicious content at the time of the testing and were exhibiting malicious behavior.

Both types of analysis performed tests for security efficacy 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

In the secure web gateway test, a total of 3,682 malicious samples were used. This included 957 malicious links to PE files, 1,479 links to other files with other malicious content (non-PE), and 1,246 samples with phishing websites.

The number of test cases for the DNS-layer security test covered 3,154 objects. Here, the test included 686 malicious links to PE files, 1,231 links to other files with other malicious content (non-PE), and 1,237 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 for both parts of the test:

- 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 2,984 clean websites and downloads were used (1,142 downloads and 1,842 websites).

All URLs for security efficacy and false positive testing were accessed on virtualized Windows systems running Windows 10 Professional (version 21H2), 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. Given that remote agents were used, only features supported by the roaming agents were included in the testing. In the case of DNSFilter, the 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 June, July and August 2022 by AV-TEST.

The DNS tunneling protection test was performed in August and September 2022. The tools "DNSCat2", "DNSExfiltrator" and "Iodine" were used for this part of the test. AV-TEST tested if these tools were able to successfully transfer the file to a remote server, or if the product has intercepted or completely blocked the transfer.

# 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 evaluated.

The following products and associated packages were tested:

- Cisco Umbrella – SIG Advantage
- Netskope - Secure Web Gateway
- Zscaler - Internet Access Transformation
- Palo Alto Networks - Prisma Access for Mobile Users
- Skyhigh Security - Secure Web Gateway
- Iboss - Zero Trust Edge

All services were configured to provide the highest level of protection, utilizing all security related features available at the time of testing. The 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 Advantage" package was used in this test. All security categories except for "Dynamic DNS" were blocked. In the DNS policies, the selective proxy and TLS decryption were all enabled. Additionally, DNS content settings were set to block DoH and DoT, Parked Domains, and Peer File Transfer.

The secure web gateway policy was set to block all default security categories: Malware, Command and Control Callbacks, Phishing Attacks, and Potentially Harmful Domains. Additionally, three content categories were blocked in the web policy: DoH and DoT, Parked Domains, and Peer File Transfer. HTTPS decryption was enabled in the web policy, as was file analysis.

The following features were disabled or unused: Cloud Firewall, IPS/IDS, File Type Control, Tenant Controls, Destination Lists, and Application Control. For the secure web gateway test, the AnyConnect Roaming Security Module (version 4.10) was used.

### Netskope Configuration

The "Netskope Secure Web Gateway" package was used in this test. Netskope policies were configured as suggested in the "Best Practice Policies – Inline", "Focus: "Real-time Protection" Policy (Not "API Data Protection" Policy)", document from their website. Decryption was enabled for all traffic.

A real-time policy was created that included all "Security Risk" categories and configured to block using the default template.

A second real-time policy was created to block malware download/upload for all categories and severities. A third real-time policy was created to block DNS over HTTPS. Dynamic categorization was also enabled. All traffic was steered to the cloud solution via the client software version 97.1.3.1032.

## Zscaler Configuration

The "Zscaler Internet Access Transformation" package was used for this test. Two SSL Inspection policies were configured: the first was set to block based on "Other Security" and "Spyware/Adware" categories, and the second to decrypt all traffic. The Advanced Threat Protection, Malware Protection, and Mobile Malware Protection features were configured per the Zscaler UI "Recommended Policy" tooltip, with no exceptions set.

The Sandbox was configured to scan all file types, categories, and protocols, with a block action for subsequent downloads. A URL Filtering rule was created to block the "Other Security" and "Spyware/Adware" categories over all request methods and protocols. All Advanced Filtering Options were enabled except for SafeSearch. The Zscaler client connector version 3.6.1.26 was used in this testing.

## Palo Alto Configuration

The "Palo Alto Networks - Prisma Access for Mobile Users" solution was configured and managed via the Prisma Access App (cloud managed). Traffic was steered via the Global Protect client. The policy consisted of several default settings in place and included best practice rules, as well as some custom ones. The Anti-Spyware policy used the out-of-the-box best-practice profile. An additional profile was applied matching DNS Tunneling signatures.

The DNS Security policy was configured using the best-practice profile as a base with the following modifications: Grayware Domains, Newly Registered Domains, Command and Control domains, Dynamic DNS Hosted Domains, Phishing Domains, Malware Domains and Parked Domains and Proxy Avoidance and Anonymizers set to block. URL Access Management used best practices as a base and blocked all medium-risk and high-risk categories.

Additionally, command-and-control, cryptocurrency, grayware, hacking, malware, newly-registered-domain, parked and phishing were all set to block. Wildfire and Antivirus was also configured with the best-practice profile with no additional modifications or exemptions. The Global Protect client version 5.1.5-20 was used in this test.

## Skyhigh Security Configuration

The "Skyhigh Security - Secure Web Gateway" solution (formerly a McAfee product and still partly branded as such) was used in this test. Traffic was redirected using the McAfee Client Proxy Connector.

The policy was configured with several default settings in place and followed best practices. HTTPS Scanning and HTTPS Decryption were enabled by default. Global Bypass was left disabled by the default. The Category, Reputation & Geo rule was set to block, Uncategorized Traffic set to Allow All and Reputation was set to block High Risk. Category and Domain Coaching was disabled by default. No Archive and Transfer exemptions were made as this was a default setting. Threat Protection and Anti-Malware was applied to all traffic and was enabled with no exceptions configured. The McAfee Client Proxy Connector 4.3.1 (Build 1) was used in this testing.

## Iboss Configuration

Iboss was configured to steer all traffic via the vendor's native client. The policy was configured from default with guidance from Iboss' official Help Docs webpage. All additional settings were not changed from the default settings. The main categories set to block were Illegal Activity, Malicious Sources, P2P, Phishing, Scams, Spam, Suspicious, Hacking, Malware Content, Parked Domains and Web Proxies.

Malware Defense was also set-up with the following settings enabled: Streaming Malware & Reputation Defense (Global), Advanced Malware Analysis Defense, Block Scan on Error, Scan Archives, Scan Email Database Types, Scan Email Messages and Scan Packed Executables.

Additionally, the following High Risk Browsing settings were enabled: High Risk Protection Enabled and Block Unreachable Sites. The Iboss Windows Cloud Connector version 5.4.80.0 was used in this test.

# 05

## Test Results #1: Secure Web Gateway Test

For the first part of the testing focusing on the full proxy SWG solutions, 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 SWG security efficacy test, a higher number of blocked samples and a lower false positive rate indicate better results.

| Vendor<br>Number of test cases | Blocking rate (total)<br>3,682 | PE URLs<br>957 | Non-PE URLs<br>1,479 | Phishing URLs<br>1,246 |
|---|---|---|---|---|
| Cisco Umbrella | 3,329 | 822 | 1,450 | 1,057 |
| Netskope | 2,950 | 825 | 1,397 | 728 |
| Zscaler | 2,931 | 735 | 1,300 | 896 |
| Palo Alto Networks | 2,921 | 862 | 1,091 | 968 |
| Skyhigh Security | 2,355 | 630 | 926 | 799 |
| Iboss | 1,642 | 577 | 474 | 591 |

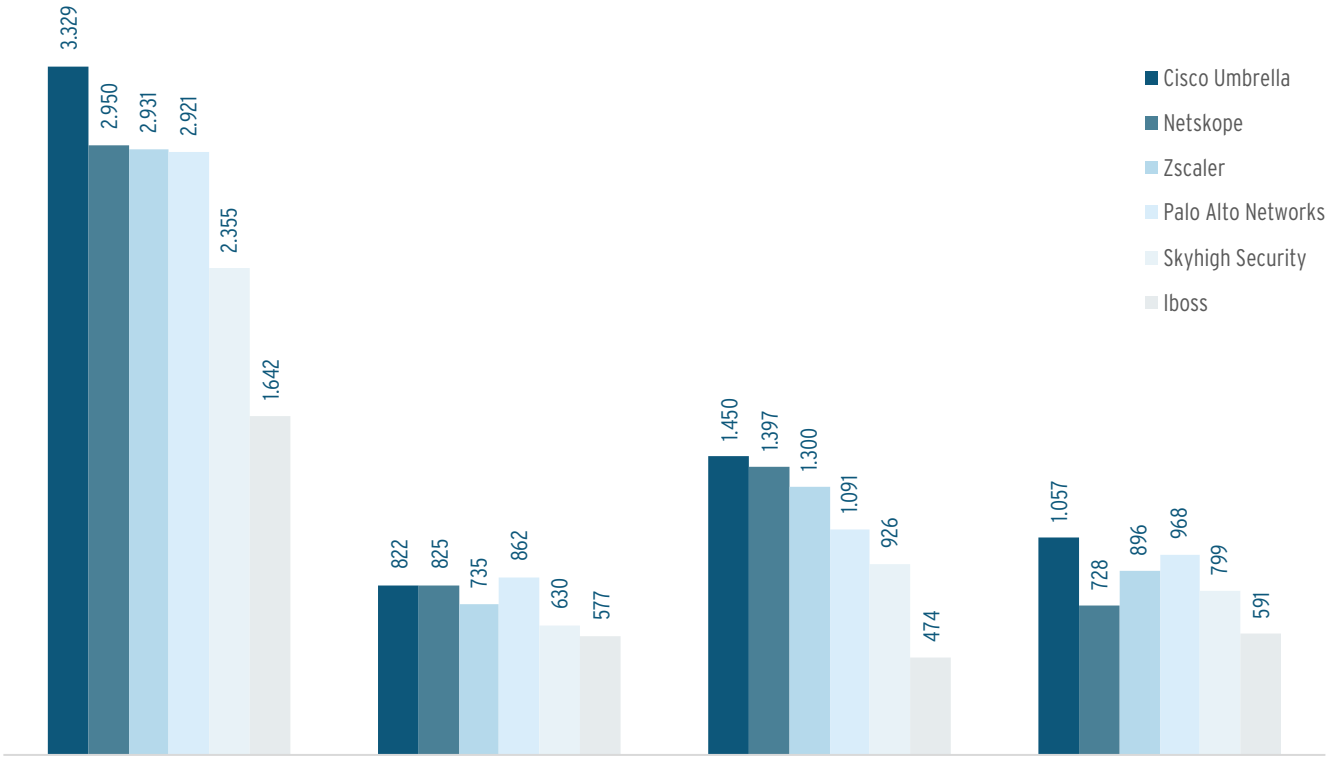
| Vendor<br>Number of test cases | False positives (total)<br>2,984 | Downloads<br>1,142 | Websites<br>1,842 |
|---|---|---|---|
| Cisco Umbrella | 43 | 43 | 0 |
| Netskope | 17 | 17 | 0 |
| Zscaler | 13 | 13 | 0 |
| Palo Alto Networks | 102 | 63 | 39 |
| Skyhigh Security | 18 | 15 | 3 |
| Iboss | 6 | 1 | 5 |

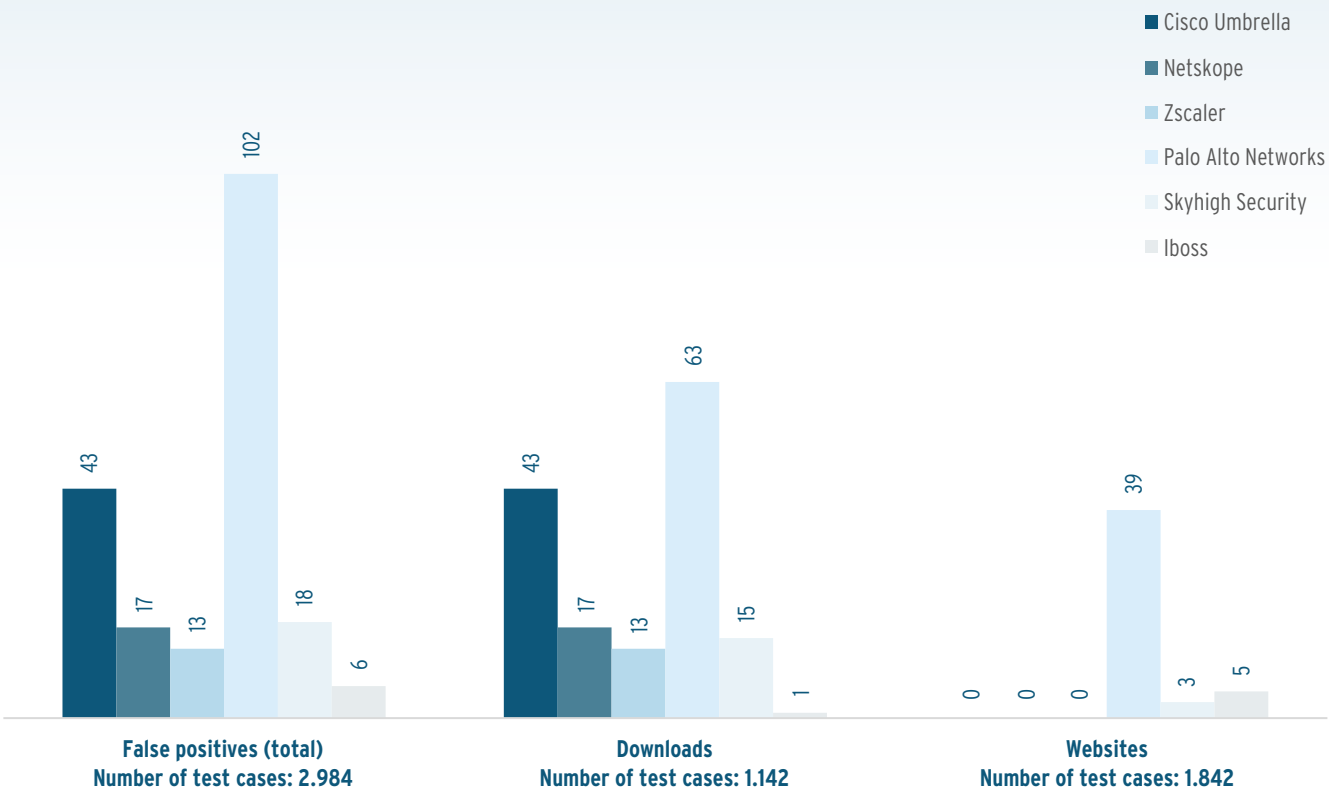
The protection and false positive rates for all tested solutions can be found in the following tables.

| Vendor<br>Number of test cases | Blocking rate (total)<br>3,682 | PE URLs<br>957 | Non-PE URLs<br>1,479 | Phishing URLs<br>1,246 |
|---|---|---|---|---|
| Cisco Umbrella | 90.41% | 85.89% | 98.04% | 84.83% |
| Netskope | 80.12% | 86.21% | 94.46% | 58.43% |
| Zscaler | 79.60% | 76.80% | 87.90% | 71.91% |
| Palo Alto Networks | 79.33% | 90.07% | 73.77% | 77.69% |
| Skyhigh Security | 63.96% | 65.83% | 62.61% | 64.13% |
| Iboss | 44.60% | 60.29% | 32.05% | 47.43% |

| Vendor<br>Number of test cases | False positives (total)<br>2,984 | Downloads<br>1,142 | Websites<br>1,842 |
|---|---|---|---|
| Cisco Umbrella | 1.44% | 3.77% | 0.00% |
| Netskope | 0.57% | 1.49% | 0.00% |
| Zscaler | 0.44% | 1.14% | 0.00% |
| Palo Alto Networks | 3.42% | 5.52% | 2.12% |
| Skyhigh Security | 0.60% | 1.31% | 0.16% |
| Iboss | 0.20% | 0.09% | 0.27% |

The Cisco Umbrella SIG Advantage package successfully blocked more than 90% of all malicious and phishing content, outperforming the second-best solution in this test by more than 10%. The solutions from Netskope, Zscaler and Palo Alto Networks achieved levels around 80%. Neither Skyhigh Security nor Iboss were able to protect against more than two-thirds of the tested samples. All products generated false positives, especially with downloaded content.




Cisco Umbrella
Netskope
Zscaler
Palo Alto Networks
Skyhigh Security
Iboss
43
17
13
102
18
6
43
17
13
63
15
1
0
0
0
39
3
5
False positives (total)
Number of test cases: 2.984
Downloads
Number of test cases: 1.142
Websites
Number of test cases: 1.842

# 06

# Configuration for Test #2: DNS-Layer Security Test

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

The following services and associated packages were tested:

- Cisco Umbrella – DNS Security Advantage
- DNSFilter - DNSFilter
- Infoblox - BloxOne Advanced

For the DNS-layer security 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.

## Cisco Umbrella Configuration

The Cisco Umbrella DNS Security Advantage package was used in this test. The DNS policy included the following security categories: malware, newly seen domains, command and control callbacks, phishing attacks, potentially harmful domains, DNS tunneling VPN, and cryptomining. Additionally, File Inspection was enabled.

## DNSFilter Configuration

For DNSFilter, a single policy was configured based on source network address. All threat categories were set to block. No Acceptable Use Policy (AUP) categories were blocked. SafeSearch was disabled and no applications were blocked.

## Infoblox Configuration

The Infoblox BloxOne Advanced package was used in this test. A custom filter was created to block six risk categories: Browser Exploits, Malicious Downloads, Malicious Sites, Phishing, Spam URLs, and Spyware/Adware/Keyloggers. This filter was attached to a policy along with 29 "Feeds and Threat Insights" lists and all set to block. SafeSearch was disabled and the source queries were identified by IP.

# 07

## Test Results #2: DNS-Layer Security Test

In the case of the DNS-layer security testing, 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 security test, a higher number of blocked samples and a lower false positive rate indicate better results.

| Vendor<br>Number of test cases | Blocking rate (total)<br>3,154 | PE URLs<br>686 | Non-PE URLs<br>1,231 | Phishing URLs<br>1,237 |
|---|---|---|---|---|
| Cisco Umbrella | 2,064 | 477 | 717 | 870 |
| DNSFilter | 1,099 | 195 | 196 | 708 |
| Infoblox | 760 | 124 | 112 | 524 |

| Vendor<br>Number of test cases | False positives (total)<br>2,984 | Downloads<br>1,142 | Websites<br>1,842 |
|---|---|---|---|
| Cisco Umbrella | 7 | 7 | 0 |
| DNSFilter | 3 | 1 | 2 |
| Infoblox | 1 | 0 | 1 |

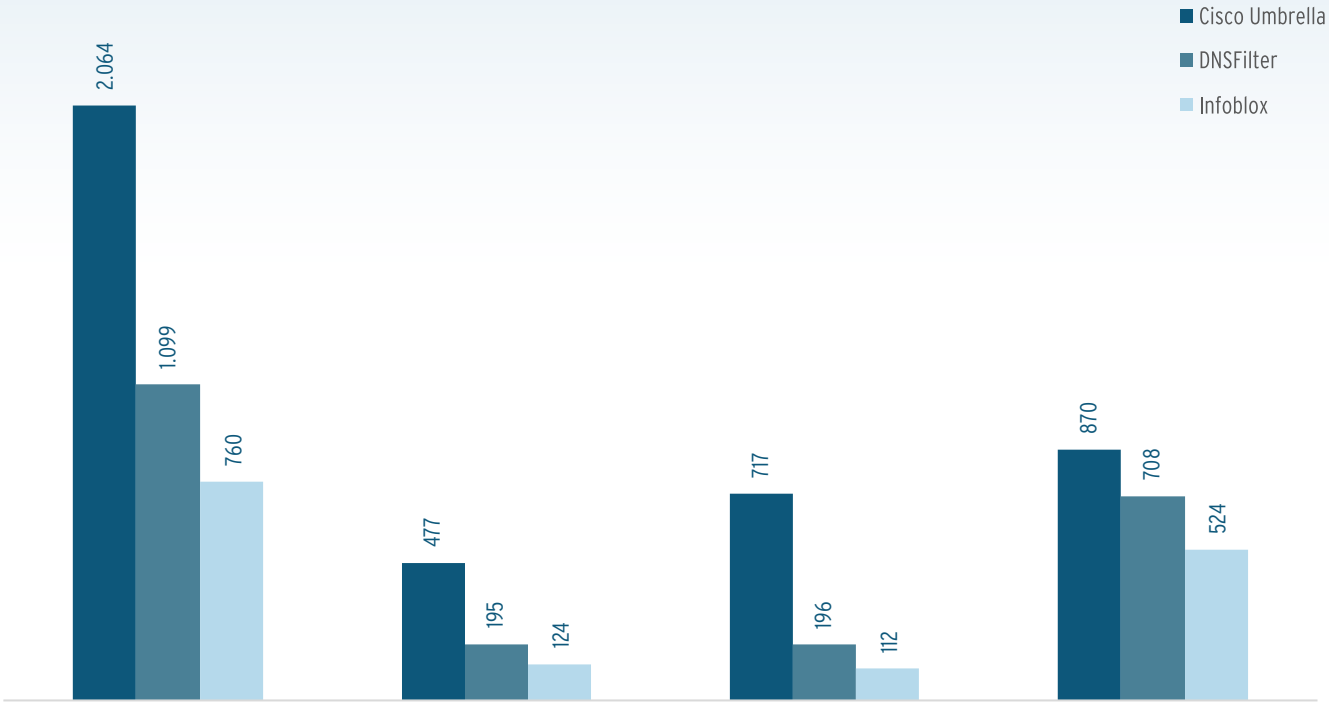
The protection and false positive rates for all tested solutions can be found in the following tables.

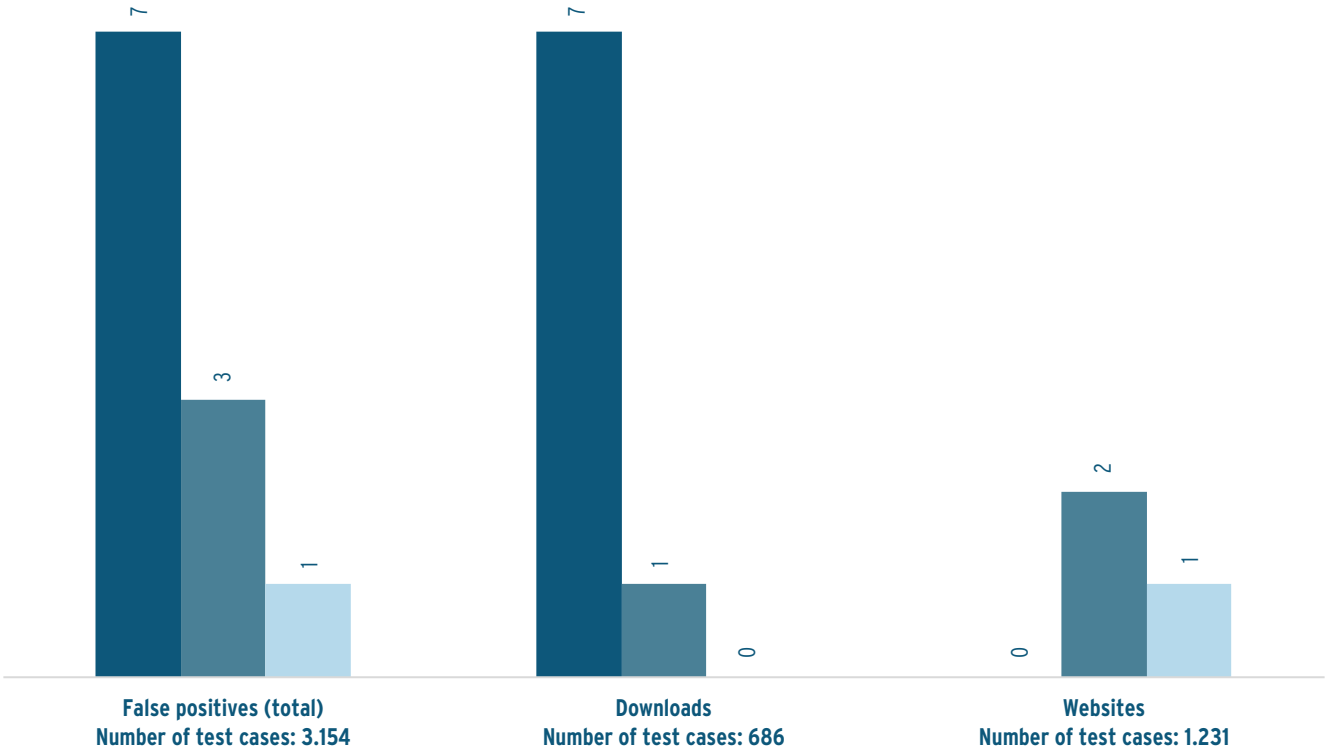
| Vendor<br>Number of test cases | Blocking rate (total)<br>3,154 | PE URLs<br>686 | Non-PE URLs<br>1,231 | Phishing URLs<br>1.237 |
|---|---|---|---|---|
| Cisco Umbrella | **65.44%** | 69.53% | 58.25% | 70.33% |
| DNSFilter | **34.84%** | 28.43% | 15.92% | 57.24% |
| Infoblox | **24.10%** | 18.08% | 9.10% | 42.36% |

| Vendor<br>Number of test cases | False positives (total)<br>2,984 | Downloads<br>1,142 | Websites<br>1,842 |
|---|---|---|---|
| Cisco Umbrella | **0.23%** | 0.61% | 0.00% |
| DNSFilter | **0.10%** | 0.09% | 0.11% |
| Infoblox | **0.03%** | 0.00% | 0.05% |

When comparing 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 test as a layered approach to security provides better protection.

The Cisco Umbrella DNS Security Advantage package performed the best in all test scenarios, blocking more than 65% of all malicious content. DNSFilter blocked around 35% and Infoblox only about 24% of the samples tested in the DNS-layer security testing. The false positive rates were slightly lower when compared with the full proxy testing.


Cisco Umbrella
DNSFilter
Infoblox
2.064
1.099
760
477
195
124
717
196
112
870
708
524
Blocking rate (total)
Number of test cases: 3.154
PE URLs
Number of test cases: 686
Non-PE URLs
Number of test cases: 1.231
Phishing URLs
Number of test cases: 1.237


7
3
1
7
1
0
0
2
1
False positives (total)
Number of test cases: 3.154
Downloads
Number of test cases: 686
Websites
Number of test cases: 1.231

# 08

## Configuration and Test Results for Test #3: DNS Tunneling Protection

In addition to testing secure web gateway and DNS-layer security, AV-TEST also tested the protection against DNS tunneling attempts.

For this test scenario, AV-TEST tested 3 different tools (DNSCat2, DNSExfiltrator and Iodine) for their ability to exploit the DNS protocal as a covert channel to transfer data or files. Solutions from Cisco Umbrella, Cloudflare, DNSFilter and Infoblox were reviewed.

### Cisco Umbrella Configuration

The Cisco Umbrella DNS Security Advantage package was used in this test. The DNS policy included the following security categories: malware, newly seen domains, command and control callbacks, phishing attacks, potentially harmful domains, DNS tunneling VPN, and cryptomining. Additionally File Inspection was enabled. DNS Tunneling VPN was configured for DNS Tunneling protection.

### Cloudflare Configuration

For Cloudflare a single security policy was configured to block with the following parameter selected: "All Security Risks." This includes the following categories: Anonymizer, Brand Embedding, Command and Control & Botnet, Cryptomining, DGA Domains, DNS Tunneling, Malware, Phishing, Private IP Address, Spam and Spyware.

### DNSFilter Configuration

For DNSFilter a single policy was configured based on source network address. The following threat categories were selected to be blocked: Botnet, Cryptomining, Malware, New Domains, Phishing & Deception, Proxy & Filter Avoidance and Translation Sites.

### Infoblox Configuration

The Infoblox BloxOne Advanced package was used in this test. A custom filter was created to block six risk categories: Browser Exploits, Malicious Downloads, Malicious Sites, Phishing, Spam URLs, and Spyware/Adware/Keyloggers. This filter was attached to a policy along with 29 "Feeds and Threat Insights" lists and all set to block. For the DNS Tunneling configuration Threat Insight – Data Exfiltration was also enabled.

The results of the DNS tunneling test are as follows (ordered by best protection rate):

| Product | Package | Offered protection rate against: | | |
|---|---|---|---|---|
| | | DNSCat2 | DNSExfiltrator | Iodine |
| Cisco Umbrella | DNS Security Advantage | 50% | 100% | 100% |
| Cloudflare | Secure Web Gateway | 0% | 50% | 100% |
| DNSFilter | DNSFilter | 100% | 0% | 100% |
| Infoblox | Advanced | 0% | 0% | 100% |

In this test, the results show the percentage of file transfers blocked or allowed per DNS Tunneling tool. 0% indicates traffic was fully bypassed by the solution, 100% means all blocked and 50% indicates that some blocked but not others.

Cisco Umbrella offered the best protection of the tested solutions for this scenario. Other solutions only blocked one-third to two-thirds of these attacks.

# 09

## Conclusion

In all test scenarios, the protection offered by Cisco Umbrella outperformed the other vendors' offerings.

In the secure web gateway test, Cisco Umbrella SIG Advantage (with secure web gateway and DNS-layer security), performed best in the test and demonstrated a high detection and low false positive rate.

In the DNS-layer security test, Cisco Umbrella DNS Security Advantage (with selective proxy) also clearly outperformed the other vendors in case of malware and phishing protection while maintaining a low false positive rate.

Cisco Umbrella also offered strong protection against DNS tunneling attempts.

The test results demonstrate that organizations should adopt a layered approach to security. DNS-layer security is simple and effective and can be enhanced by deploying a selective proxy when possible.
A secure web gateway full proxy solution provides the highest level of protection as seen in the test results, and it provides even stronger protection when combined with DNS-layer security.

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 500 client and server systems, where more than 3,500 terabyte 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