Independent Tests of
Anti-Virus Software

Secure Access Service Edge

Palo Alto Networks SASE Comparative Report

TEST PERIOD: SEPTEMBER 2021 – FEBRUARY 2022

LAST REVISION: 14TH APRIL 2022

COMMISSIONED BY: PALO ALTO NETWORKS

WWW.AV-COMPARATIVES.ORG

Content

Introduction

This comparative test was commissioned by Palo Alto Networks to evaluate the security efficacy of leading secure access service edge (SASE) solutions designed to address the needs of today's hybrid workforces. Palo Alto Networks chose the products to test, the configuration to use in their product, and the test scenarios to be covered in this comparative test. For the two competitor products in the test, the respective vendors' publicly recommended best practices were used to configure the products. Different settings could have led to different results in the test.

In today's global economy, many companies have employees distributed across multiple locations, such as headquarters and branch offices. Due to the Covid-19 pandemic, remote working from home has also increased greatly in recent times. Wherever they are, a company's staff will need to access IT services, applications and data that are also spread out over a number of physical locations. These could be within the company LAN, in a datacentre (private cloud), or public cloud. Hence, the solutions need to allow users in multiple locations to securely access permitted content distributed over further physical locations, which provides a challenge for IT departments.

In the past, multiple products might have been needed to control access from distributed users to data in distributed locations, resulting in a complicated management system with no real overview of all access policies and security measures. *Secure access service edge* (SASE) solutions aim to simplify this situation by allowing IT administrators to manage all the necessary security measures and access permissions from a single cloud-based management interface / architecture.

SASE solutions can provide enterprises with secure, optimal and automated access to applications and workloads in the cloud, by extending software-defined networking and security to the doorstep of major IaaS and SaaS providers. Regardless of the location of users and applications, SASE provides unified secure access from a single management platform.

While SASE used to be a matter of sacrificing speed for control, improved technology now offers businesses both speed and control. Secure Access Service Edge (SASE) merges network traffic and security priorities, ubiquitous threat and data protection, and ultra-fast, direct network-to-cloud connectivity.

A SASE solution should be able to enforce uniform and ubiquitous security for a user from any location to any application, regardless of port/protocol being used, detecting and preventing malicious activity bidirectionally given insider threats and/or users inadvertently connecting from a previously infected host. Hence, the overall threat protection capabilities, and the completeness of attack surface protection (multiple attack vectors) for both remote and branch user-based scenarios are important. This also includes benign and malicious traffic classification, time to prevent, time-to-identify, and time-to-detect threats and reporting and visibility.

Tested SASE Solutions

The following up-to-date products were validated for an extended period of six months (September 2021 till February 2022):

- Cisco Umbrella

- Palo Alto Networks Prisma Access Enterprise
- Zscaler Internet Access

SASE Test Setup & Deployment

The SASE solutions were configured based upon best practices provided by Palo Alto Networks for their own product, as well as each respective vendors' publicly available best practices for their products. The SASE configurations included multiple security and compliance applications-URL filtering, anti-virus, advanced threat protection, sandboxing, firewall, data loss prevention, cloud application security, traffic bandwidth management, and much more in a single, seamless system. Prevention and protection capabilities (ability to block) were activated. Product updates were permitted. All test scenarios were executed in their entirety where applicable.

SASE Test Overview

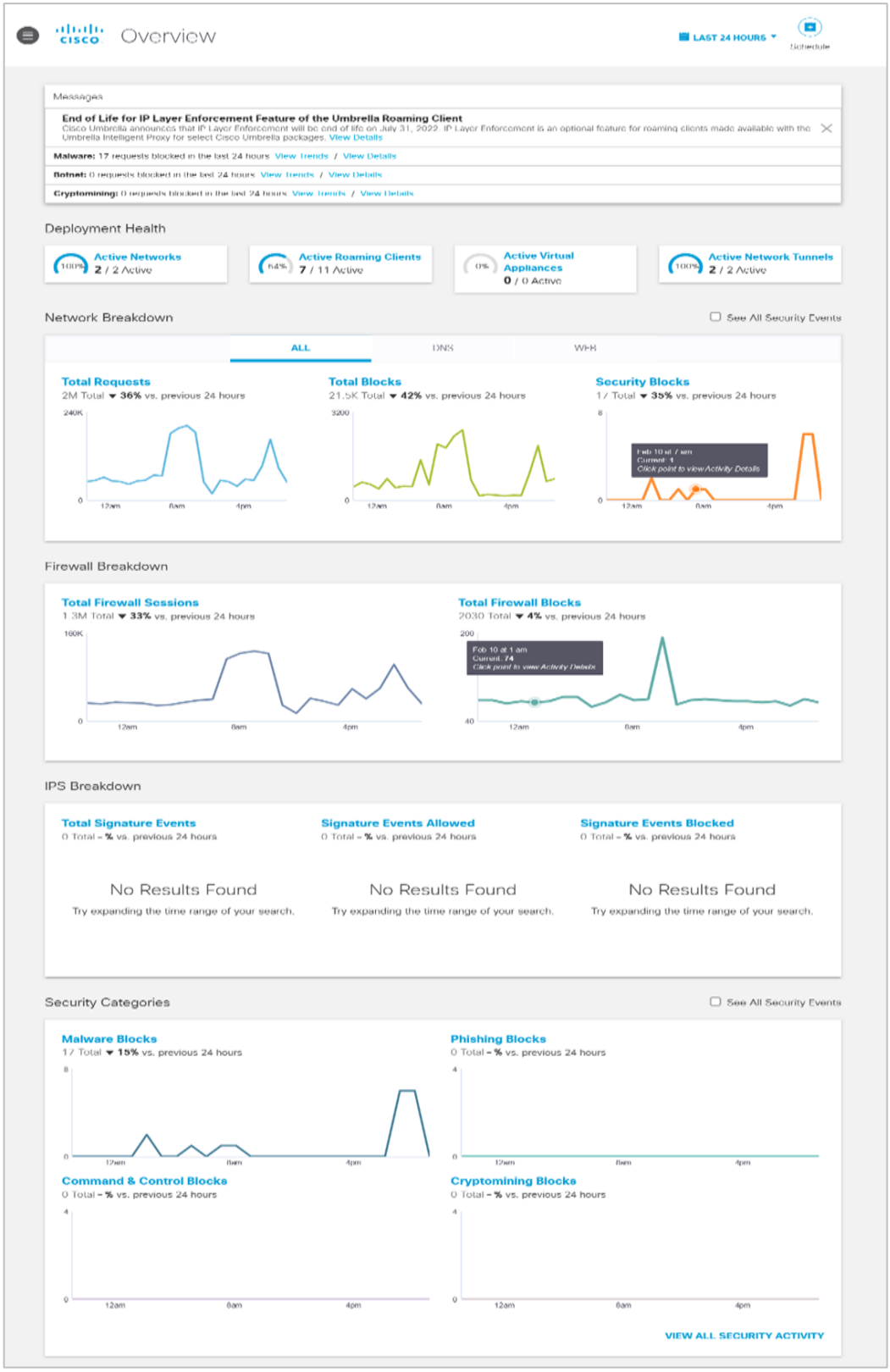
The overall test procedure included 8 different sub-tests, each covering a major aspect of the respective product's capabilities in a specific real-world scenario. The Web URL Filtering Protection, DNS Security and Malware Protection sub-tests were broken down into further individual categories, as shown below:

1. Web URL Filtering Protection (CnC Block Rate, Malware Block Rate, Phishing Block Rate, Average Benign URL Categorization)
2. DNS Security (DNS Tunnelling Prevention, DGA Protection Rate)
3. Malware Protection (Sandbox Analysis Time, Protection Against Modified Malware, Malware Protection via Email Protocol, Artifact Extraction, File Transfer)
4. Public SaaS Application Security
5. Private SaaS Application Security
6. Vulnerability Protection
7. Evasion Protection
8. Credential-Theft Prevention

Detailed test results for each product are provided later in this report. The settings that were applied to each respective product may be found in the Appendix of this report under the section "Product Settings".

Product Thumbnails

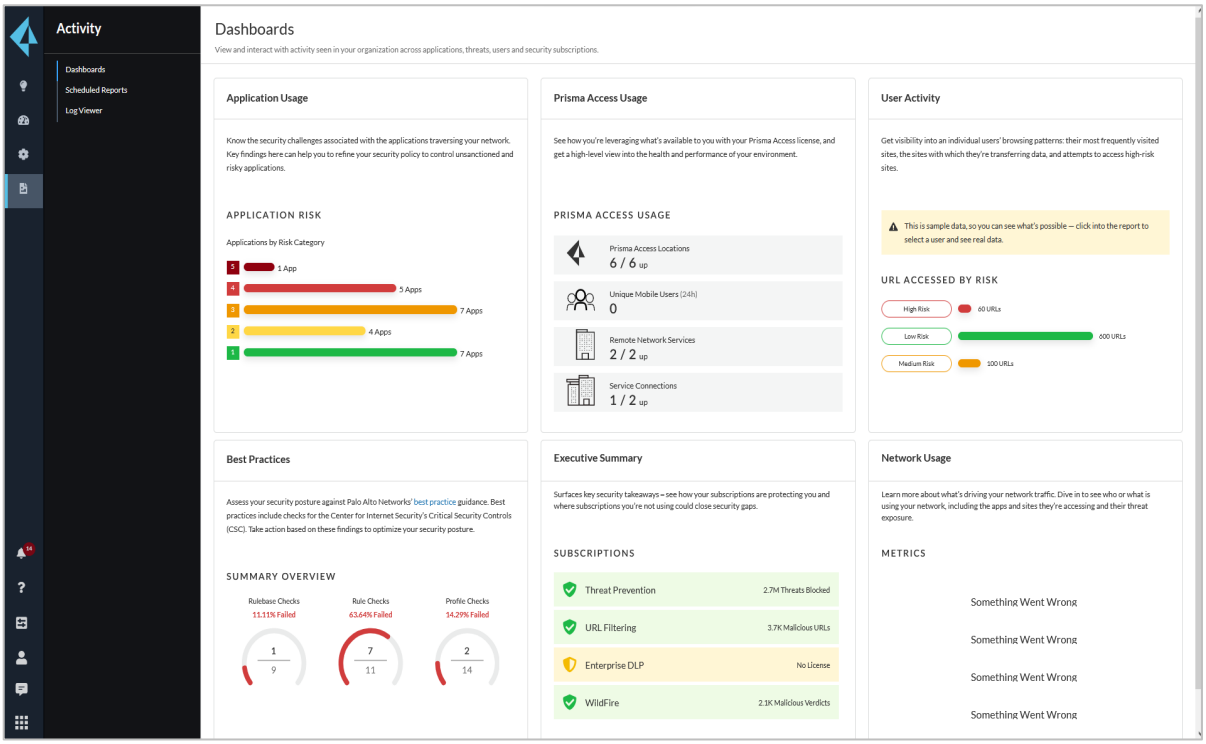
Cisco Umbrella



Cisco Umbrella

Cisco's SASE solution achieved excellent results in the following sections: DNS Tunnelling Prevention and Protection Against Unknown Malware; Protection Against Modified Malware.

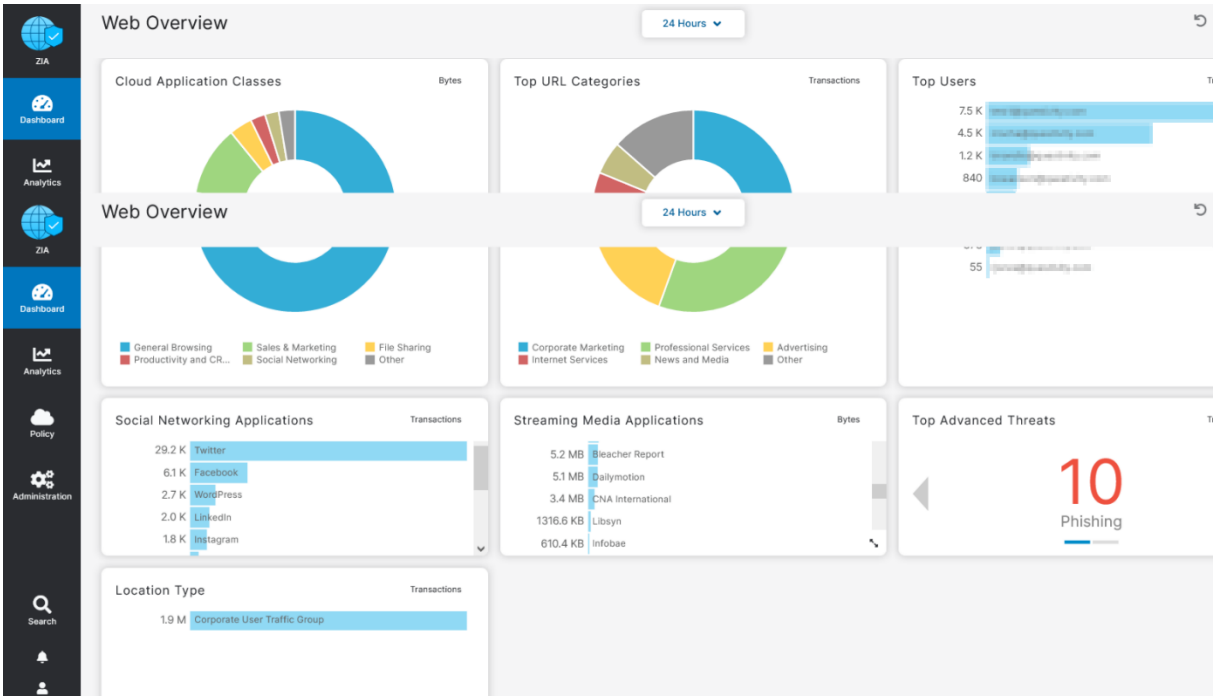
Palo Alto Networks Prisma Access Enterprise



Palo Alto Networks Prisma Access Enterprise

The Palo Alto Networks SASE solution achieved excellent results in most of the tested sections, such as: CnC URL Block Rate; Malware URL Block Rate; Phishing URL Block Rate; Average Benign URL Categorization; DNS Tunnelling Prevention; DGA Protection Rate; Protection Against Modified Malware; Malware Protection via Email Protocol; File Transfer; Public SaaS Application Security; Private SaaS Application Security; Vulnerability Protection; Evasion Protection; Credential-Theft Prevention. In the Malware Protection via Email Protocol section, Palo Alto Networks covered IMAP as well as SMTP. In the Artifact Extraction section, Palo Alto Networks supported the PPT format in addition to the PDF format.

Zscaler Internet Access



Zscaler Internet Access

Zscaler achieved excellent results in the Average Benign URL Categorization section.

AV-Comparatives' SASE Comparative Analysis

The summary of key results below shows how the three tested products fared during our validation across eight different categories.

SASE Security Categories	Cisco	Palo Alto Networks	Zscaler
1. Web URL Filtering Protection			
CnC Block Rate	37%	**91%**	63%
Malware Block Rate	37%	**84%**	66%
Phishing Block Rate	23%	**78%**	35%
Average Benign URL Categorization	81%	**98%**	97%
2. DNS Security			
DNS Tunnelling Prevention and Logging	100%	**100%**	75%
DGA Protection Rate	64%	**100%**	76%
3. Malware Protection			
Sandbox Feature to Protect Against Unknown Malware	N/A	**Yes**	Yes
Protection Against Modified Malware	85%	**100%**	16%
Malware Protection via Email Protocol	SMTP	**IMAP/SMTP**	-
Artifact Extraction	PDF	**PDF/PPT**	PDF
File Transfer	N/A	**Yes**	N/A
SaaS Application Security			
4. Public SaaS Application Security	Yes	**Yes**	Yes
5. Private SaaS Application Security	N/A	**Yes**	-
6. Vulnerability Protection	71%	**100%**	29%
7. Evasion Protection	50%	**100%**	100%
8. Credential-Theft Prevention	N/A	**Yes**	N/A

Conclusion

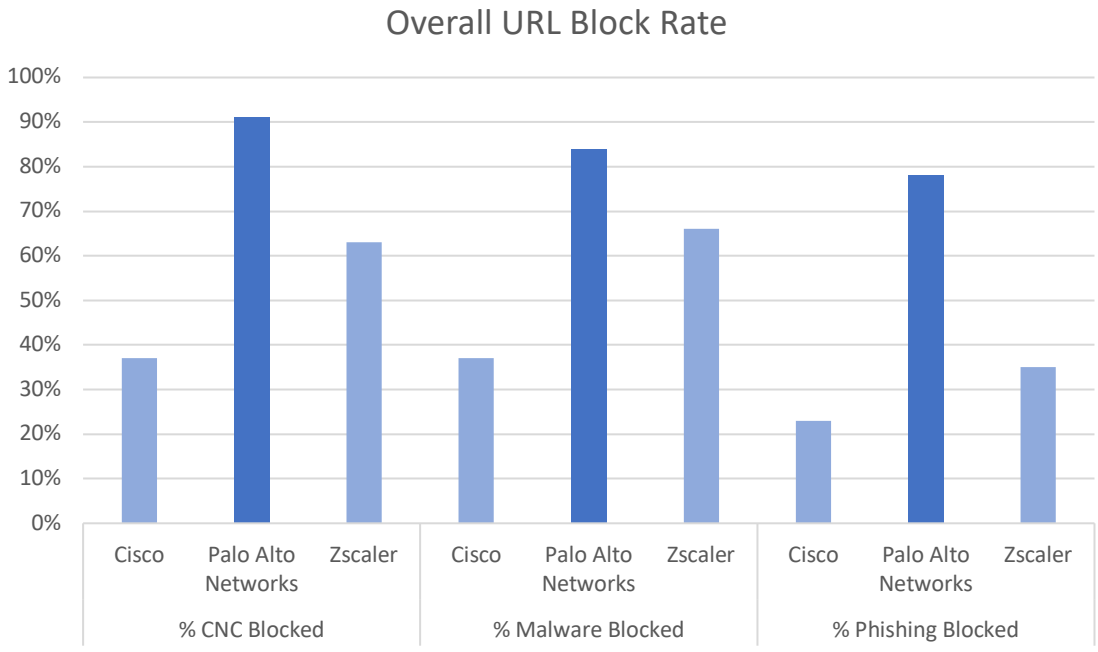
This comparative test of SASE products, commissioned by Palo Alto Networks, considered a range of protective functionality to secure hybrid workforces, including URL filtering, DNS security, malware protection, vulnerability protection, and credential-theft prevention. In most of these test categories, Palo Alto Networks achieved best or joint-best scores. In the URL Filtering Protection Tests, it achieved the highest protection rates in all three categories. Palo Alto Networks was also the only product tested to include credential-theft prevention, and to provide malware protection for the IMAP email protocol.

Individual sub-tests

The following sections contain detailed results for the individual sub-tests.

1. Web URL Filtering

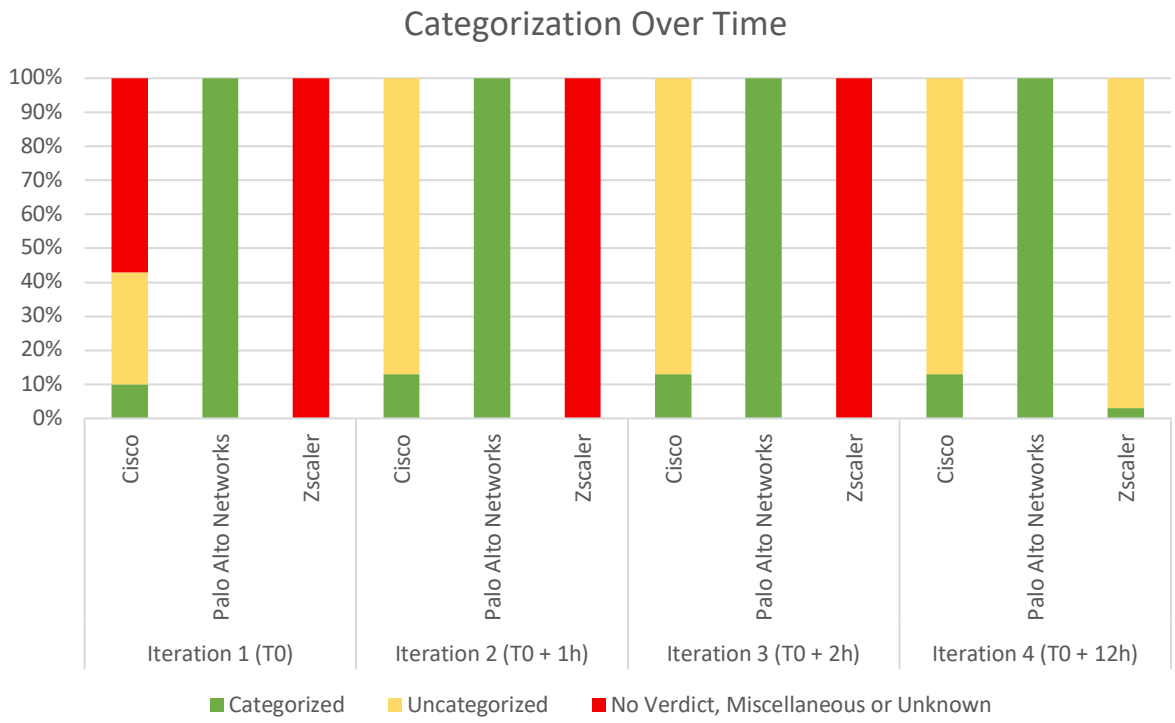
Enterprises are responsible for the network traffic they allow and hence need to enforce control on employee browsing behaviour. Effective SASE solutions should correctly identify content and block material that is deemed inappropriate based on the organization's policy. The SASE solutions used in today's enterprise environment should be able to differentiate URL categories, and also have the ability to enforce on-demand control on these categories. While blocking malicious URLs is paramount for organizational threat defence, letting the end-user browse to benign, permitted URL categories is equally important.



Overall URL block rate

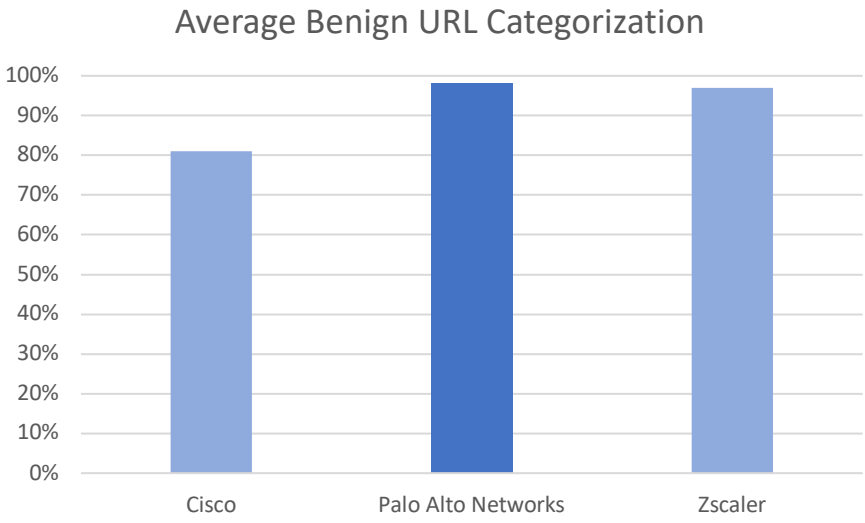
AV-Comparatives tested a combined total of more than 1,700 URLs for malicious command and control (CnC), malware, and phishing protection. It is noteworthy here to reiterate that all features required per best practices were enabled for all vendors throughout testing. Web filtering is often a combination of DNS and URL filtering. DNS protection features remained enabled during testing to reflect real-world scenarios and best practices. As a result, in this test, some URLs may have been blocked at the DNS level. The table above reflects the effective URL block rates for each vendor within each test category.

The table above shows that Palo Alto Networks provided higher levels of protection against malicious URLs than its competitors. This was true for all individual categories, namely CnC, malware, and phishing.



New URL/Domain Categorization over time

The graph above showcases categorization over time for 30 newly created URLs. Categorization testing started within one day of their creation. The first scan of the newly created URLs represents T0. Subsequent iterations occurred at T0 plus 1 hour, 2 hours, and 12 hours, respectively. Palo Alto Networks categorized all domains/URLs during the first iteration. Cisco categorization and alert capabilities during the first test iteration reached about 45%, while Zscaler was at 0%. Both Cisco and Zscaler gradually improved their respective domain/URL categorizations in the subsequent three iterations.



Average Benign URL Categorization Percentage (%)

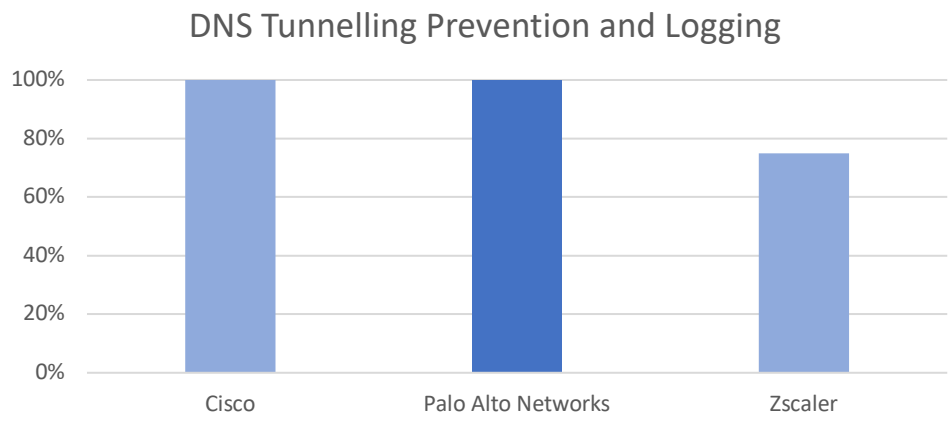
The graph above demonstrates the total average benign URL categorization, using 429 test cases. Zscaler's benign URL categorization for both the branch and remote user(s) was excellent at an average

of 97% in the seven categories that were evaluated. Cisco's categorization came in at a total average of 81%. Palo Alto Networks fared the best, with a 98% success rate.

2. DNS Security

DNS Tunnelling Prevention

Threat actors regularly use DNS protocols to exfiltrate data, spread malware, or for command and control activities. Organizations rarely monitor DNS traffic flowing in and out of their IT infrastructure. SASE solutions should be able to provide protection against DNS tunnelling and detect the use of domain generation algorithms (DGAs). The chart below captures the results from testing four different DNS tunnelling methods using publicly available tools. This functionality test was performed using standard ports.

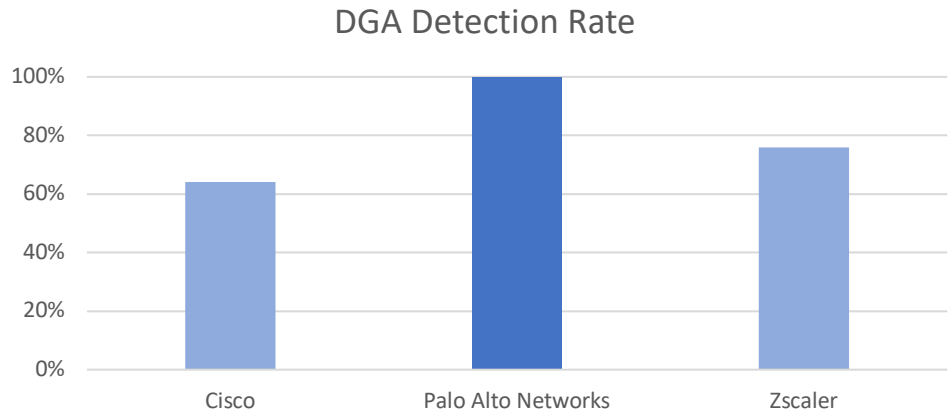


DNS Tunnelling Prevention and Logging

Two products were successful at preventing 4 out of 4 DNS tunnelling tests.

DGA Security

Domain generation algorithms (DGAs) have been widely used by malware authors for command-and-control activities for quite some time. This is because this is one of the more effective methods for evading reputation-based defences. We chose relevant malware families that were proliferating in the wild during the testing window, and generated five DGAs, with five samples each, based on those families. The results below show the detection and block rates of the SASE solutions.



DGA Protection Rate

As shown in the chart above, Palo Alto Networks provided effective coverage in terms of identifying the malicious DGA domain, categorizing it correctly, and then actively blocking it. Cisco's solution was

64% successful at blocking any of the DGA techniques tested. Zscaler offered a 76% detection and blocking rate.

3. Malware Protection

Unknown Malware

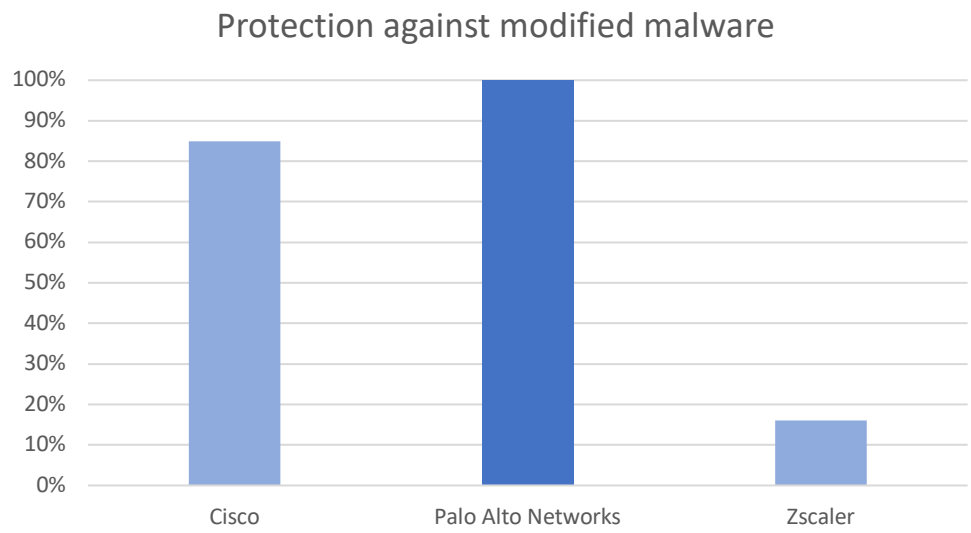
The ability to block unknown malware is a key feature for SASE solutions. This ensures that users are protected from unknown attacks that other technologies could not protect against. Sandboxing is one of the main technologies that SASE solutions utilize to combat such threats. In addition to providing the information on such attacks, the ability to derive protection from this information defines a critical component of SASE solutions. Both Palo Alto Networks and Zscaler have a sandboxing feature to sandbox unknown threats.

	Cisco	Palo Alto Networks	Zscaler
Sandbox Feature to Protect Against Unknown Malware	-	✓	✓

Sandboxing feature

Modified Malware

Threat actors will mutate the baseline threats, threats that have been previously seen, using different mechanisms to defeat signature, heuristics or behavioural protection. AV-Comparatives used different file modification mechanisms in an attempt to evade the protection provided by the SASE solutions.



Modified-Malware Protection

Cisco and Palo Alto Networks demonstrated resilient capabilities against such attacks.

Malware Protection via Email Protocol

SASE solutions should be able to support common email protocols. SASE products should also provide the ability to extract relevant information from emailed threats in the form of URLs, packing techniques or command-line parameters. Palo Alto Networks provided protection both for IMAP and SMTP mail protocols, whereas Cisco only demonstrated effectiveness on SMTP protocol. Zscaler failed to demonstrate the ability to provide protection on IMAP or SMTP protocols. The table below provides an overview of email protocol protection results:

Vendor	IMAP Protection	SMTP Protection
Cisco	-	✓
Palo Alto Networks	✓	✓
Zscaler	-	-

Malware Protection via Email Protocol

The next table demonstrates the ability of the vendors to extract relevant threat information from two popular file types:

Vendor	Artifact Extraction for PDF	Artifact Extraction for PPT
Cisco	✓	-
Palo Alto Networks	✓	✓
Zscaler	✓	-

Relevant Threat Intelligence Extraction Capabilities

File Transfer

SASE Solutions should protect against the transfer of malicious files bidirectionally. The SMB is one of such protocols that has been repeatedly used by threat actors. Palo Alto Networks demonstrated protection against malware delivered over SMB, whereas Cisco and Zscaler did not.

Vendor	SMB File Transfer Protection
Cisco	-
Palo Alto Networks	✓
Zscaler	-

File Transfer Protection through SMB Protocol

4. Public Cloud SaaS Application Access and Security

A comprehensive zero trust SASE solution should provide deep content inspection on traffic in both directions, regardless of the ports or protocols used while accessing public SaaS applications in the cloud and irrespective of the location of the users. SASE solutions should be able to enforce granular control on users accessing such applications.

Public SaaS Application	Cisco	Palo Alto Networks	Zscaler
Consistently distinguish Google Drive Business from Consumer Version	-	-	-
Consistently distinguish OneDrive Business from Consumer Version	-	✓	✓

SaaS Application Control

While evaluating the ability of the SASE solutions to identify specific application types in the cloud and to then provide controlled access, it was determined that none of the SASE vendors tested had the ability to consistently distinguish between business and consumer versions of the Google Drive application. This capability doesn't explicitly translate into a prevention capability issue. Cisco was the only vendor that lacked the ability to distinguish consumer and business versions of OneDrive (see table above).

Security Efficacy – Upload			
Public SaaS Application	**Cisco**	**Palo Alto Networks**	**Zscaler**
Box	-	✓	✓
DropBox	-	✓	✓
Google Drive	-	✓	-
OneDrive	-	✓	✓

Malicious transfers from User to Public SaaS Applications

Palo Alto Networks was able to consistently demonstrate a high detection and blocking rate when users tried transferring malicious samples (file format and others) to publicly hosted SaaS applications. Cisco did not have the capability to detect any of these transfers to the cloud and was oblivious to all of them. Zscaler also demonstrated a high detection and block rate when it came to Dropbox and OneDrive, but had zero visibility into Google-Drive-based transfers (see table above).

Security Efficacy – Download			
Public SaaS Application	**Cisco**	**Palo Alto Networks**	**Zscaler**
Box	✓	✓	✓
DropBox	✓	✓	✓
Google Drive	-	✓	-
OneDrive	✓	✓	✓

Malicious transfers to the User from the Public SaaS Applications

Palo Alto Networks was able to consistently demonstrate a high detection and blocking rate when there were malicious transfers made from public SaaS applications to users. Cisco was also able to demonstrate a high detection and block rate when it came to Box and DropBox. However, Cisco had minimal or lacked visibility completely with Google Drive and OneDrive. Zscaler had a decent consistent coverage when it came to Box, DropBox and OneDrive, but was completely oblivious to transfers originating from Google Drive. The table above shows which vendors were able to demonstrate security for the public SaaS applications tested.

5. Private/Internal SaaS Application Access and Security

Inspection Scenario	Cisco	Palo Alto Networks	Zscaler
Inside Threat Scenario	N/A	✓	-
Remote User Exploitation	N/A	✓	-
Bi-Directional Malware Protection (Standard Ports)	N/A	✓	-
Bi-Directional Malware Protection (Non-Standard Ports)	N/A	✓	-

Palo Alto Networks Private/Internal SaaS Content Inspection

Note: At the time of testing, Cisco did not have the required features to evaluate and hence receives a “not applicable score”. Zscaler did have the feature and functionality configured but was unable to provide any protection in any of the scenarios shown in the table above.

Palo Alto Network showcased protection by blocking exploitation of a vulnerable remote user from a malicious staged application and protection by blocking exploitation of vulnerable staged applications from remote users (insider threat scenario). Only Palo Alto Networks demonstrated bi-directional malware protection to and from a remote user in both standard and non-standard ports.

	Cisco	Palo Alto Networks	Zscaler
Application Control per user	N/A	✓	✓

Application Control per user

Note: At the time of testing, Cisco did not have the required features to evaluate, and hence received a “not applicable” score. Both Palo Alto Networks and Zscaler were able to enforce different granular access policies to an application for each user (see table above).

6. Vulnerability Protection

Despite the shift outside the perimeter, network architectures are still designed such that everything must pass through a network perimeter and then back out. Users, regardless of where they are, must still channel back to the corporate network. This demands that the SASE solutions can provide protection for both client and server-side vulnerabilities that exist with high or critical Common Vulnerability Scoring System (CVSS) scores. Seven vulnerabilities with a CVSS score of over 7.5 were used as test cases.

Vulnerability Protection	Cisco	Palo Alto Networks	Zscaler
Protection Rate Against Recent Vulnerabilities	100%	100%	50%
Remote User Protection Rate	100%	100%	50%
Remote Application Protection Rate	33%	100%	0%
Total Vulnerability Protection Rate	**71%**	**100%**	**29%**

Vulnerability protection

Palo Alto Networks and Cisco were able to identify, detect and protect against the two recent vulnerabilities. Zscaler was only able to protect against one of the recent vulnerabilities at the time of testing.

Both Palo Alto Networks and Cisco were able to successfully protect their remote users from getting compromised when they attempted to access or work on applications that were compromised or were malicious in nature and hosted on the public internet. Zscaler's protection rate for this scenario on the other hand was only 50% as demonstrated in the table above (Remote User Protection Rate).

Palo Alto Networks consistently displayed protection across both remote users and branch users throughout all three tested scenarios and use cases for the exploitation of vulnerable applications on the public internet. The table above (Remote Application Protection Rate) showcases how Palo Alto Networks was once again 100% successful in securing a vulnerable application from exploitation. This is the important use case where a rogue user or a compromised remote user’s system tries to exploit a remote application or services hosted on the public Internet. Cisco’s protection rate for this scenario fell to 33% and Zscaler’s to 0%.

This indicates that while both Cisco and Zscaler were able to offer some protection to remote users against malicious applications, they were not able to protect publicly facing applications from compromised users or insider threats based upon the above-stated scenarios.

7. Evasion Protection

Evasions give the attacker the ability to add an extra layer on top of the malware/exploits via transport or also as content modification to get past security controls. Evasions also give the attacker the ability to repurpose existing attacks to slip past security controls. In this section we examine the tested products' ability to handle evasions in six commonly used categories of attack.

Evasion techniques	Cisco	Palo Alto Networks	Zscaler
Combined Evasion	50%	100%	100%
Evasion Driveby Baseline	50%	100%	100%
HTML Evasion	50%	100%	100%
HTTP Evasion	50%	100%	100%
Script Obfuscation	50%	100%	100%
TCP/IP Evasion	50%	100%	100%

Evasion protection scores (sum of results for both standard and non-standard ports)

For each evasion technique, two test cases were used, one with standard ports, and one with non-standard ports. All three products were able to protect against evasion techniques when standard ports were used. However, Cisco lacked protection in all six of the tested categories of evasions when a non-standard port was used by the attacker.

8. Credential-Theft Prevention

It is imperative that users' corporate credentials and information, should be prevented from being submitted into non-legitimate sites or compromised through similar means that result in data leakage. SASE solutions need the ability to identify and detect phishing attacks and then detect and prevent a subsequent submission of usernames or corporate credentials. The table below reports the results of the testing of multiple credential phishing threats. For this functionality check, two test cases were used.

Credential Theft - Validation Type	Cisco	Palo Alto Networks	Zscaler
Identify and detect phishing attacks in the context of credential-based phishing	N/A	✓	N/A
Detect and block username submission for phishing related sites	N/A	✓	N/A
Detect and block corporate credentials submission	N/A	✓	N/A

Credential-Theft Prevention

Cisco and Zscaler did not support "Credential-theft prevention" at the time of testing.

Appendix

Product Settings

Please find below the different product settings, configurations and functionality that were enabled while evaluating theses SASE solutions for this test. Palo Alto Networks chose the configuration to use in Prisma Access based on their best practices. For the other two products in the test, the respective vendors' publicly recommended best practices were used to configure the products. It is possible that results might have differed if different settings had been used for these two products.

Palo Alto Networks:
URL Filtering: high-risk, adult, command-and-control, copyright-infringement, dynamic-dns, extremism, gambling, grayware, hacking, insufficient-content, malware, newly-registered-domain, parked, peer-to-peer, phishing, proxy-avoidance-and-anonymizers, questionable, unknown, and weapons.
DNS Security: Command and Control Domains, Dynamic DNS Hosted Domains, Grayware Domains, Malware Domains, Newly Registered Domains, Parked Domains, Phishing Domains, and Proxy Avoidance and Anonymizers.
Malware Protection: Enabled.
IPS Protection: Enabled for vulnerability protection evaluation.

Cisco:
URL Filtering: Command & Control Callbacks, and Phishing Attack.
DNS Security: Malware, Newly Seen Domains, Command and Control Callbacks, Phishing Attacks, Dynamic DNS, Potentially Harmful Domains, DNS Tunneling VPN, and Cryptomining.
Malware Protection: Enabled.
IPS Protection: Enabled for vulnerability protection evaluation.

Zscaler:
URL Filtering: Anonymizers, Browser Exploits, Command & Control Servers, Command & Control Traffic, Cookie Stealing, Cryptomining, File Format Vulnerabilities, IRC Tunneling, Known Adware & Spyware Sites, Known Phishing Sites, Malicious Content & Sites, Potentially Malicious Requests, Spyware Callback, SSH Tunneling, Suspected Phishing Sites, Vulnerable ActiveX Controls, Web Spam, Viruses, Unwanted Applications, Trojans, Worms, Ransomware, Adware, and Spyware.
DNS Security: Phishing, Malicious Content, Newly Registered Domains, and DNS Over HTTPS Services.
Malware Protection: Enabled.
IPS Protection: Enabled for vulnerability protection evaluation.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(April 2022)