Use Case-Driven Web Security Evaluator Guide

The Netskope platform was designed to address a variety of web security use cases encompassing granular policy controls, web filtering, threat protection, and data protection spanning managed and unmanaged apps, cloud services, plus web traffic. This document covers seven of the most common use cases, the functional requirements to deliver each use case, deployment configurations needed, and how to test Netskope or any web security product's ability to cover each use case.

netskope

01

Provide monitoring and visibility of user behavior on the web, plus for apps including activity and risk ratings

For an average organization, approximately 85% of web traffic is now related to the 1,295 apps and cloud services they use[1]. Web security solutions need to provide monitoring and visibility of user behavior on the web as expected, however, they must also provide the same for apps and cloud services inclusive of activity. Given more than 95% of apps and cloud services are outside the administration control of IT, risk ratings for tens of thousands of apps are also required.

[1] Netskope Cloud Security Report, July 2019

Netskope provides monitoring and visibility for thousands of managed and unmanaged apps, plus web traffic to profile user activity and behavior including inspecting TLS encrypted traffic. Netskope Cloud Confidence IndexTM (CCI) risk ratings for over 36,000 apps and cloud services are based on CSA attributes for seven profiles including security, risk, privacy, compliance, vulnerabilities, financial, and legal/audit. Netskope also supports any user, device, or location and deploys in line with forward or reverse proxy modes, supports direct-to-internet IPsec and GRE tunnels for remote offices, and a lightweight steering client for mobile users.

01

Functional Requirements

- Profile user activity and behavior on the web by categorizing websites and profiling apps and cloud services with risk ratings
- Decode app and cloud service traffic to profile user, app, instance, data, and activity to understand the content and context of user behavior

Deployment Requirements

- Deploy cloud-based web security inline for all office locations and remote users without backhauling web traffic or using VPNs, enabling direct-to-internet for any user, device, or location
- Provide performance and scale to inspect encrypted TLS web traffic

TIP:

Exercise the strength of a web security by uploading sensitive test information via an unmanaged file sharing app to determine if this visibility and monitoring is provided.

How to Test with Cloud Security Products

- Deploy the cloud-based web security solution inline for a selected office via IPsec or GRE tunnels, or a set of remote users with a steering client
- Enable encrypted TLS traffic inspection making exceptions for personal finance and healthcare categories
- Allow 24-48 hours of web activity to complete
- View risk ratings for all apps and cloud services accessed during the 24-48 hours
- Select and profile users with personal instances of apps versus company instances
- Select specific users and view all web activity and behavior in summary site and event pages
- Drill down into users who posted sensitive test information via an unmanaged app
- Verify visibility and monitoring of user, app, instance, data, and activity

02

Protect against malware and provide multi-layer advanced threat detection

Increasingly web threats abuse cloud apps and social media to both opportunistically and target victims. Cloud storage also plays an important role to deliver payloads where it often by-passes legacy defenses not inspecting TLS encrypted traffic for managed and unmanaged apps. Just because your company uses Google Drive, Box, or Dropbox cloud data storage does not imply all instances should be allowed. Your web security solution needs to determine company instances and what activities are permitted, and the same for personal instances of users for managed and unmanaged apps and cloud services.

Also, scripts and macros more frequently within Office files may start a web threat kill chain as the use of portable executables (PEs) decreases in comparison. So, while sandboxing PEs is advised, pre-execution script and macro analysis with heuristics becomes an important part of a multi-layer defense alongside machine learning anomaly detection.

02

Functional Requirements

- Provide real-time threat protection for all web traffic, apps, and cloud services for offices and remote users with managed devices with no by-passing of apps or cloud services
- Provide real-time threat protection for users on personal devices accessing managed apps
- Leverage third-party threat intelligence feeds as part of the inspection, plus custom IOC hashes and URLs

Deployment Requirements

- Deploy cloud-based web security inline via forward or reverse proxy for desired office locations and remote users, and funnel all traffic including O365 and other managed apps
- Provide performance and scale to inspect encrypted TLS web traffic making exceptions for personal finance and healthcare categories

TIP:

Test the web security solutions custom coaching page capabilities with websites and apps.

How to Test with Cloud Security Products

- Enable and configure the cloud-based web security threat protection capabilities
- Attempt to visit a known malware infected website and verify the solution blocks the user
- Attempt to sync a malware test file from a shared folder to a local Box or OneDrive sync client and verify the product blocks the sync activity
- Post an HTML file to an unmanaged app such as WeTransfer, then configure the web security solution to block uploads, shares, and downloads for this specific app and re-test to verify the HTML file is blocked, this is a known phishing technique that by-passes some email security solutions
- Search for a specific file name or hash within the solution query tool, it should be able to provide the past 90 days of activity for web traffic, apps and cloud services
- Enter a custom IOC hash or malicious URL as new threat intelligence to the solution

03

Provide direct-to-internet coverage for remote offices and mobile users

Driven by digital transformation, company networks are changing from hub-and-spoke architecture where remote offices backhaul data over costly, dedicated links to having direct-to-internet access. The same holds true for remote users migrating from the poor experience of VPNs to direct app, cloud service, and data access from any device and location, plus using zero-trust network access to private apps and resources. The network location of users becomes less important as policy controls focus on content and context in a cloud-first environment.

Netskope also recognizes the standard web is inefficient for business transactions requiring low latency and high capacity. Netskope NewEdge data centers optimize routes and local access to less than 20ms for users. The speed of NewEdge architecture also enables multiple defenses with no trade-off between security and performance. Netskope is building the largest secure and performant security cloud service available, where every NewEdge data center further optimizes speed and capacity.

03

Functional Requirement

- Provide IPsec or GRE tunnels for remote offices for direct-to-internet access
- Provide a lightweight steering client (i.e. 4MB) for remote user managed devices
- By-pass traffic based on location, category, or domain

Deployment Requirements

- Steer thousands of apps and cloud services for inspection and policy controls
- Integrate with SSO/IAM solutions for transparent authentication into managed apps
- Provide zero-trust network access (ZTNA) to private apps and resources

How to Test with Cloud Security Products

- Enable and configure the cloud-based web security solution for remote offices and mobile users
- Use a known unmanaged cloud storage / file sharing app from a remote office or mobile user
- Verify visibility of the unmanaged app use for the user, data, and activity, plus optional policy controls
- Configure a policy to by-pass personal finance websites, then access a personal finance website and verify it was not inspected by the web security solution
- Test remote access to the cloud security service and measure RTT from multiple regions if your organization has global operations
- Test zero-trust network access to private apps and resources in the cloud or to a private data center

TIP:

Test the cloud-based web security solution round-trip time (RTT) for multiple regions and locations.

04

Provide web filtering and coaching users on acceptable use including apps

Web filtering is a known security control with URL categories, custom categories, and dynamic web page ratings for new sites, pages, or content. This is an area where supervised machine learning has taken over for human raters to cover 99.9% of the active web. However, 85% of web traffic is now related to apps and cloud services where less than 5% have IT administration rights. The elephant in the room for web security is unmanaged apps, often more than 1,200 for an organization, exposing data by accident or intentionally, plus opening a path for malware or advanced threats.

Netskope provides web filtering with 100+ categories for over 200 languages, plus dynamic web page ratings for 70 categories. Custom categories can be defined with support from a site look-up tool and a reclassification service. Over 40 threat intelligence feeds also include malicious URLs, plus defining custom URLs from internal threat intelligence. Granular policy controls for web traffic, apps, and cloud services include coaching pages for acceptable use, including blocking the use of high-risk apps and providing safer alternatives in alerts.

04

Functional Requirements

- Provide URL filtering by category and custom categories for web traffic
- Provide visibility and monitoring of apps, plus app risk profile ratings
- Provide alerts with coaching for users on acceptable use and preferred low risk apps

Deployment Requirements

- Cloud performance and scale to inspect TLS encrypted web traffic
- Inline visibility of web traffic, apps, and cloud services via forward proxy

TIP:

Validate the web security solution synthesizes and distills web activity to user site and page visits with the ability to drill down into fine grain details.

How to Test with Cloud Security Products

- Enable and configure the cloud-based web security solution for a remote office or mobile users
- Upload known sensitive information to a managed app personal instance to validate coaching alerts to users about this type of data in their personal instance versus a company instance
- Set an app risk score policy of 60 or higher and then access an unmanaged app with a risk rating below this policy level, validate the coaching alert with suggested lower risk profile apps to utilize
- Configure URL filtering to block gambling sites with a coaching alert on acceptable use, test by accessing a known gambling site to verify it is blocked, then put the gambling site into a custom category to allow and re-test and validate access is allowed
- Profile a user's behavior by site and page visits, plus apps at a summary level, then validate the ability to drill down into fine grain details about the user, device, app, instance, risk level, category, data, and activity

05

Provide data protection across websites, apps, and cloud services

While digital transformation is driving a shift for secure web gateways (SWGs) from appliances to cloud for many reasons, the same impact is shifting data loss prevention (DLP) from an on-premises product suite to an integrated feature in cloud-based cloud access security brokers (CASBs). As apps and data move to the cloud, it only makes sense security defenses should move to the cloud. Protecting data and data privacy are leading cloud adoption concerns, and for good reason with the ease of use to post, share, and download data. The challenge for web security goes beyond managed apps and into web-based blogs, discussion forums, social media, and thousands of unmanaged apps easily adopted by business units and users.

Netskope recognizes that more than 95% of apps and cloud services are not managed by IT administration. However, data flows like water in the cloud and data protection for any user, device, or location is required no matter the app, managed or unmanaged, or the website. Having CASB critical capabilities in a cloud SWG solution also means advanced DLP critical capabilities so both content and context apply to granular policy controls.

05

Functional Requirements

- Provide standard and advanced DLP critical capabilities with granular policy controls and actions
- Provide dozens of ready to use DLP compliance and regulation templates
- Provide alerts on sensitive data being exposed externally or publicly

Deployment Requirements

- Cloud performance and scale to inspect TLS encrypted web traffic
- Inline visibility of web traffic, apps, and cloud services via forward proxy

TIP:

Exercise the DLP strength of a cloud-based web security solution by using fingerprinting to detect sensitive data within a form. Test in a file upload and download between company and personal instances of an unmanaged file sharing app.

How to Test with Cloud Security Products

- Enable and configure the cloud-based web security solution DLP capabilities to recognize sensitive test data
- Upload the sensitive test data into an unmanaged app to validate DLP alerting, plus the solution's alert dashboard, how it facilitates the investigation, and workflow to remediate
- Upload the sensitive test data into both a company and personal instance of a managed app with policy controls to coach and block the personal instance upload while allowing the company instance
- Copy multiple files from a managed app company instance into an unmanaged app personal instance for the same user, the web security solution should automatically alert on possible data exfiltration without setting any policies

06

Provide advanced web analytics and metadata for security analyst investigations

In a perfect world all malicious and bad things are prevented, and we live within a safe perimeter. The reality is quite the opposite as perimeters fade, identities and access are compromised, insider threats are real, mistakes and misconfigurations happen, and attacks land and expand quietly doing their reconnaissance. Good prevention comes from great detection and that requires rich metadata for security analysts. Logs, events, and alerts are helpful, however, as an industry we have learned the value of context and content with metadata, plus it drives machine-learning and new advances in our security defenses. The other key challenge is reducing the number of solution silos, consoles, chair pivots, and manual effort to link all the parts and pieces for an investigation.

Netskope provides 90 days of rich metadata (longer by contract) defined by the granular policy controls of Cloud XD that decodes the language of apps, cloud services, and personalized websites. Netskope also synthesizes and distills web activity to user site and page visits with the ability to drill down into fine grain details. Security analysts can quickly view user activity for apps, cloud services and web activity avoiding the complexity of high-volume web proxy logs of legacy solutions.

06

Functional Requirements

- Provide access to 90 days or more of rich metadata for apps, cloud services and web activity
- Provide user site and event page summary information with the ability to drill down into details
- Provide security analysts ad hoc query capabilities for investigations and threat hunting

Deployment Requirements

- Ability to export metadata to third party solutions including EDR, SIEM, SOAR and UEBA
- Ability to bi-directionally share new threat intelligence with EDR and SIEM solutions

TIP:

Validate the web security solution has a published data dictionary of metadata for security analysts and data science teams working on internal machine-learning projects.

How to Test with Cloud Security Products

- Enable and configure the cloud-based web security solution to monitor all web traffic for 24-48 hours
- View user site and event page summary information to profile activities for the 24-48 hours
- Drill down into granular details for a specific user including apps, cloud services and web activity
- Make an ad-hoc query for all unmanaged apps for the file sharing app category with upload activity
- Make an ad-hoc query to show all apps with a risk score below 50 during the 24-48 hours
- Configure the web security solution to bi-directionally share threat intelligence with an EDR solution

07

Compare an existing appliance SWG deployment with Cloud SWG capabilities

Almost three out of four SWG deployments are appliance based today, however, the cloud headwinds are strong and within a few years there will be more cloud SWG deployments than appliances. Part of the migration challenge is mapping and comparing functionality, plus understanding how defenses consolidate and change focus in a cloud-first environment.

Traditional SWG features such as anti-malware, URL filtering, allow or deny app controls, authentication, and reporting are shifting to cloud SWG features including CASB, DLP, advanced threat defenses, cloud services, and hybrid functionality. The net summary is a better understanding of content and context for inline policy controls across apps, cloud services, and web traffic with improved threat and data protection.

Netskope has provided inline proxy capability since 2012 and protects some of the largest inline deployments for Office365, Box and Slack. While a traditional CASB is API out of band focused for a handful of managed apps, the larger web security challenge is thousands of apps and cloud services knowing they are 85% of web traffic today.

07

Functional Requirements

- Visibility, monitoring and granular policy controls for apps, cloud services, and web traffic
- Provide advanced threat defenses and data protection for apps, cloud services, and web traffic
- Single console and policy for consolidated SWG, CASB, and DLP critical capabilities

Deployment Requirements

- Performance to inspect TLS encrypted traffic without a degradation in service
- Direct-to-internet access for remote offices (IPsec and GRE tunnels) and mobile users (steering client)

TIP:

Validate the round-trip-time (RTT) for your existing web security solution for main offices, remote offices, and mobile workers to apps and websites. Compare to cloud-based SWG solutions and educate your team on access (or edge) architecture

How to Test with Cloud Security Products

- Compare visibility, monitoring, and policy controls for apps, cloud services, and web traffic
- Compare threat and data protection capabilities, threat intelligence sharing, and exporting metadata
- How many appliances and consoles are required for matching functionality of SWG, CASB, and DLP capabilities
- Validate the percentage of your web traffic that is TLS encrypted and how much is inspected
- Validate the percentage of your web traffic related to apps and cloud services
- Compare your worst remote user experience (RTT) today to a cloud SWG solution

Test Results

Given guidance on how to test a web security vendor's ability to cover each use case, here is where you can tally your test results. Use a scoring system of 0-5 with 5 being the highest and most comprehensive coverage of the use case. Giving a vendor a 0 would obviously reflect the vendor's inability to cover the use case. Some vendors may cover some of the requirements, but come up short, resulting in a lower score.

It is also worth documenting how many separate products and administrator consoles your current web security vendor requires to cover all use cases. This could impact your ability to deploy, manage, and operationalize the vendor's products.

USE CASE	VENDOR A Score (0-5): Product(s) required:	VENDOR B Score (0-5): Product(s) required:
Provide monitoring and visibility of user behavior on the web, plus for apps including activity and risk ratings	S: P:	S: P:
Protect against malware and provide multi-layer advanced threat detection	S: P:	S: P:
Provide direct-to-internet coverage for remote offices and mobile users	S: P:	S: P:
Provide web filtering and coaching users on acceptable use including apps	S: P:	S: P:
Provide data protection across websites, apps, and cloud services	S: P:	S: P:
Provide advanced web analytics and metadata for security analyst investigations	S: P:	S: P:
Compare an existing appliance SWG deployment with Cloud SWG capabilities	S: P:	S: P:
Number of use cases comprehensively covered by meeting all functional requirements		
Number of products and administrator consoles required to deploy and manage		

About Netskope

The network perimeter is dissolving. A new perimeter is needed that can protect data and users everywhere, without introducing friction to the business. The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey. Reimagine your perimeter with Netskope.

netskope.com