Next Gen SWG Evaluator Guide

Netskope's Next Gen Secure Web Gateway (NG SWG) is designed to address the key cloud and web security use cases encompassing granular policy controls, web filtering, threat protection, and data protection spanning managed and unmanaged apps, cloud services, and web traffic.

This document covers six of the most common use cases, the functional requirements to deliver each use case, deployment configurations needed, and how to test Netskope or any other product's ability to cover each use case.

netskope

01 Monitor and assess risk with cloud app and web usage

02 Granular control of unmanaged cloud apps

03 Provide web filtering and coach users on acceptable use including apps

04 Protect against malware and apply multi-layer advanced threat detection

05 Provide advanced data protection across the cloud and web

06 Provide direct-to-internet coverage for remote offices and remote workers

netskope

01

Monitor and assess risk with cloud app and web usage

For an average organization, approximately 85% of web traffic is now related to the 1,295 apps and cloud services they use. A next gen secure web gateway (SWG) needs to provide monitoring and visibility of activity-level user behavior when accessing websites and cloud apps. Given that more than 95% of cloud apps are outside the administrative control of IT, risk ratings for tens of thousands of apps are also required.

Netskope inspects TLS encrypted traffic to provide visibility and monitoring, profile user activity and understand user behavior for thousands of managed and unmanaged apps, plus web traffic. Netskope Cloud Confidence IndexTM (CCI) risk ratings for over 33,000 cloud apps are based on CSA attributes for seven profiles: security, risk, privacy, compliance, vulnerabilities, financial, and legal/audit. Netskope also supports direct-to-internet IPsec and GRE tunnels for remote offices, and offers a lightweight steering client for mobile users.

01

Functional Requirements

- Profile user activity and behavior on the web by categorizing websites and profiling tens of thousands of cloud apps with risk ratings
- Decode cloud app traffic to profile user, app, instance, data, and activity to understand the content and context of user behavior
- See data movement across cloud apps and alert on this behavior

Deployment Requirements

- Deploy the next gen SWG 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 the next gen SWG product by downloading sensitive data from a managed cloud app and uploading that same data to a cloud app not managed by IT. Verify what level of visibility and monitoring is provided.

How to Test

- Deploy the web security product 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 exfiltrated data
- Verify visibility and monitoring of user, app, instance, data, and activity

02

Granular control of unmanaged cloud apps

Instead of disrupting the business by blocking the potentially thousands of cloud apps not managed by IT, safely enable the cloud by applying granular controls and targeting risky activities. A next gen secure web gateway needs to provide the granular control required to stop the bad and safely enable the good.

Unlike other security products, Netskope's NG SWG was architected from the beginning to provide real-time, granular visibility and control of thousands of cloud apps including the ones led by lines of business and users. This enables you to optionally block the use of high-risk cloud apps, but more importantly, safely enable the majority of apps that the business relies on.

02

Functional Requirements

- Steer all cloud traffic (thousands of cloud services) and decode in real-time dozens of activities such as login, logout, upload, download, share, post, view, edit, etc.
- Differentiate between corporate-managed instances of apps and personal instances and reflect the difference in policy
- Support the selection of app categories as part of policies
- Provide “allow” actions as part of a layered policy

TIP:

When testing instance-awareness, use cloud apps that have a URL that persists across instances of the app. For example, Google Drive, OneDrive for Business, and dozens of other apps will always use drive.google.com making it difficult to determine whether a corporate, partner or personal instance is in use. Apps like Box and Slack change their URL for every account so it is relatively easy to apply policies based on the changed URL.

How to Test

- Select 5-6 cloud apps such as Slack, Dropbox, Evernote, etc. that may be used by lines of business and not managed by IT
- Select at least two cloud apps that are managed by IT and may have personal instances in use. Examples are IT-managed Google Drive and Slack and personal (unmanaged) Google Drive and OneDrive for Business
- Configure the cloud security product for instance-awareness, identifying IT-managed versions of the apps you selected in the previous step
- With the cloud security product configured for real-time visibility and control, upload sensitive data to each of the identified cloud apps and verify that the activities are captured by the product
- Configure policies in the cloud security product to block PII data going to any of the selected apps in previous steps, while allowing PII to go to the versions of the apps managed by IT
- Attempt to upload PII to an unmanaged app and verify the block
- Attempt to upload PII to the app instance managed by IT and verify that the activity is allowed

03

Provide web filtering and coach users on acceptable use including apps

Web filtering is a well-known security control with URL categories, custom categories, and dynamic web page ratings for new sites, pages, or content. With 85% of web traffic being cloud, a next gen SWG needs to also cover acceptable use policies for the potentially thousands of cloud apps in use.

Netskope's NG SWG provides comprehensive web filtering and user coaching for cloud app and website access use cases.

03

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
- Provide a combination policy that incorporates both cloud and web into a single policy

Deployment Requirements

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

04

Protect against malware and apply multi-layer advanced threat detection

Increasingly web threats abuse cloud apps and social media to both opportunistically and directly 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.

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

Netskope's next gen SWG provides multi-layered, advanced threat protection when accessing websites and cloud apps.

04

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
- Leverage third-party threat intelligence feeds as part of the inspection, plus custom Indicators Of Compromise (IOC) hashes and URLs

Deployment Requirements

- Deploy cloud-based web security inline proxy for desired office locations and remote users, and steer all traffic including Office 365 and other managed apps
- Provide performance and scale to inspect encrypted TLS web traffic

TIP:

Test the product's custom coaching page capabilities with websites and apps.

How to Test

- 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

05

Provide advanced data protection across the cloud and web

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. A next gen SWG needs to have advanced cloud Data Loss Prevention (DLP) capabilities with both content and context applied to granular policy controls.

05

Functional Requirements

- Provide dozens of ready to use DLP compliance and regulation templates
- Inspect files in transit to and from the cloud and web, posts to websites, posts to social media, posts to cloud apps like Slack
- Follow data that has been downloaded from one app and uploaded to another
- Bring in context including user, device, location, app, app instance, activity, and content to increase accuracy
- Support for fingerprinting with similarity matching, and exact data matching

TIP:

Use native apps like Slack desktop and sync clients like Box Drive and the OneDrive sync client to try and leak data. Verify that this traffic is also inspected.

Deployment Requirements:

- Cloud performance and scale to inspect TLS encrypted web traffic
- Inline visibility of cloud and web traffic via an inline proxy

How to Test

- Use sample sensitive data that should trigger compliance violations tied to PCI, HIPAA, GDPR, etc.
- Configure a DLP policy to alert when compliance violated data is uploaded to categories of cloud apps and websites
- Upload the data to a variety of cloud apps and choose websites from social media to web forums
- Copy and paste sensitive data in Slack posts
- Verify alerts occur and walk through the incident management process

06

Provide direct-to-internet coverage for remote offices and remote workers

Driven by digital transformation, company networks are changing from a hub-and-spoke architecture, where remote offices backhaul data over costly dedicated links, to having direct-to-internet access. A next gen SWG needs to provide infrastructure and capabilities that deliver fast and secure access to the cloud and web from anywhere.

06

Functional Requirements

- Provide a globally distributed network infrastructure that is optimized for performance and security
- Provide IPsec or GRE tunnels for remote offices for direct-to-internet access
- Provide a lightweight steering client (i.e. 10MB) for managed devices outside the office
- By-pass traffic based on location, category, or domain
- Ability to classify devices based on security posture and reflect this classification in access policies

Deployment Requirements:

- A client deployment that steers all cloud and web traffic from managed devices to the cloud-delivered service

USE CASE	VENDOR A Score (0-5): Product(s) required:	VENDOR B Score (0-5): Product(s) required:
Monitor and assess risk with cloud app and web usage	S: P:	S: P:
Granular control of unmanaged cloud apps	S: P:	S: P:
Provide web filtering and coach users on acceptable use including apps	S: P:	S: P:
Protect against malware and apply multi-layer advanced threat detection	S: P:	S: P:
Provide advanced data protection across the cloud and web	S: P:	S: P:
Provide direct-to-internet coverage for remote offices and remote workers	S: P:	S: P:
Number of use cases comprehensively covered by meeting all functional requirements		

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