netskope

7 Things Your Next-Gen SWG and Firewall Must Do

Table of Contents

Introduction

For many organizations, work looks very different today than it did just a few years ago.

More and more of their key applications – from Office 365 and Google Workspace to Slack and Zoom – are on the internet rather than in their private network. And employees are highly dispersed, in many cases spending more time working outside of the office than in it.

This creates new challenges for IT teams – and leaves legacy tools struggling to keep up.

A traditional secure web gateway (SWG) or firewall solution assumes all traffic, even from virtual private networks (VPNs), will be routed back to the office's data center first. That's not only impractical in the cloud era, but it can also be counterproductive from a security perspective. It causes latency that users won't put up with and creates visibility gaps that infrastructure and operations professionals can't allow.

As a result, increasing numbers of enterprises are embracing next-generation solutions that are cloud native. These solutions offer the essential capabilities to defend against the fast-moving threats we all face today.

But what should an infrastructure and operations practitioner look for in a new SWG or firewall? In the rest of this eBook, we'll outline seven things your next-gen tool must do to effectively modernize your architecture and keep you protected in today's threat landscape.

1. Stop backhauling everything to nowhere.

Legacy hubs don’t work for today’s distributed world.

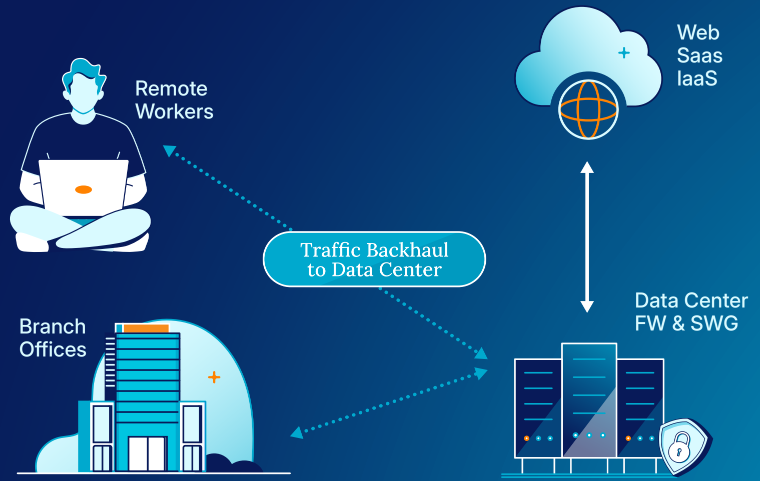
There was a time when organizations had data centers keeping everything on premises, which could then act as the enforcement points for network security. But today’s users and applications are everywhere – remote work is commonplace and the average company uses around 100 different apps* (plus many hundreds more across unmanaged SaaS and shadow IT). The “perimeter” model has become totally outdated.

Not surprisingly, those organizations sticking with the old approach are struggling on multiple fronts. Trying to funnel all user traffic through centralized hubs overwhelms legacy infrastructure, adding latency and complexity. Employees suffer poor remote user experience and have to keep logging into VPNs, with daily impact on their productivity. Security teams get limited visibility of application-layer behavior.

A modern architecture takes a different approach, enforcing security more intelligently, closer to the user and app, where data and risk live. This approach provides a more robust defense, and allows infrastructure professionals to maintain more granular policies. User experience is the first priority for modern architecture, which makes use of network adjacencies and peering to optimize performance to apps, data, and resources.

How we do it

Netskope’s NewEdge infrastructure is a globally distributed cloud platform that brings enforcement close to users without the performance hit of legacy hub and spoke models.



*Okta Businesses at Work 2025, https://www.okta.com/reports/businesses-at-work/

2. Decrypt without breaking everything (or everyone's patience).

Cloud-based SWG/firewall solutions mean there's no excuse to avoid decryption.

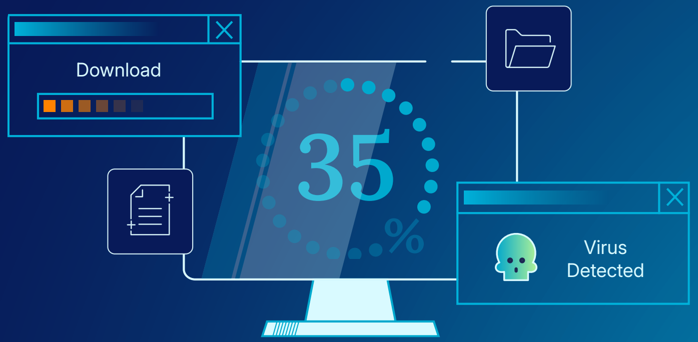
Encrypted SSL/TLS traffic is increasingly prevalent on today's internet. But IT teams regularly need to decrypt it, whether to inspect for threats, protect data, enforce security policies, or comply with regulations.

Legacy on-premises SWGs and firewalls often choke on decryption, lacking the capacity to handle it. Inspecting key apps such as office productivity systems, for example, might involve looking at as much as one-third of total network traffic. Rather than overwhelming their infrastructure, some organizations avoid the decryption of major app suites altogether – with potentially serious consequences for their security posture.

In contrast, modern cloud-based SWG/firewall systems have massive scale, so decryption even of large amounts of traffic is achievable. IT teams can decrypt without disruption, enjoying both performance and security without trade-offs.

How we do it

Netskope performs high-performance TLS decryption inline, with single-pass inspection using intelligent traffic steering to preserve app functionality and reduce unnecessary inspection.



Microsoft OneDrive and SharePoint are the source of **35%** of malware downloads.*

* *Netskope Cloud and Threat Report 2024, https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-2024*

3. Move beyond “allow” and “block” rules.

Make better access decisions based on a fuller understanding of users and live context.

Traditional firewalls have long supported application-based rules. But many of these have been simple “allow” or “block” decisions, based on app name or traffic pattern. Such policies are blunt instruments that lack the flexibility or intelligence demanded by modern security challenges.

An example: Legacy tools might set a threshold that blocks one user from uploading 100 files, but lets another upload 99 – even if the former is part of a daily backup cycle and the latter is a huge anomaly. Or they could stop a user putting source code into a public LLM and allow it into the company’s private LLM.

Modern solutions instead enable rich contextual decision-making. They can enforce policies based on factors like user role, device trust, and behavior anomalies. And they can enable adaptive security controls, such as real-time coaching, step-up authentication, and collecting justifications, to encourage the right behavior and protect key data.

How we do it

Netskope uses deep contextual awareness to enforce adaptive access policies. These capabilities respond to live context rather than static rules.

4. Write a policy once, not in three consoles.

Achieve better consistency with a single data security rule you can leverage everywhere.

Anyone who works in the SOC knows what it's like pivoting their chair from one console to another, as they look at different apps, controls, and data identifiers. This kind of policy sprawl and tool fragmentation might be commonplace today, but it creates an enormous management burden and kills operational efficiency.

The problem is that most tools can't create defined rules that apply uniformly across apps, endpoints, email, web, and so on. Instead, IT teams find that they need separate consoles for their SWG, firewalls, VPNs, and zero trust network access (ZTNA). All of this complexity creates inconsistency, policy drift, increases risk, and causes untold frustration for administrators and users alike.

Modern SWG/firewall solutions instead act as a unified policy engine, enabling you to benefit from operational efficiency and scale. This "define once, apply everywhere" approach is both more consistent and more secure.

How we do it

Netskope's unified policy framework applies consistently across web, cloud, and private app traffic – one policy, everywhere.

> "[In Netskope], I understand what my policy set looks like across multiple features and applications, versus some of our legacy applications where I had four different places to manage a single application and its features."
>
> **VP of Infrastructure, Technology Sector***

*Forrester: Total Economic Impact of Netskope SSE, October 2024

5. Catch the unknown bad stuff before it gets in.

With threats moving faster, real-time detection becomes the new security standard.

Legacy security tools were built for a different era, when operating reactively and spotting threats within four to 48 hours was the norm. (Given industry-wide intelligence sharing, almost all threats should be known a day later anyway.) But that approach is unacceptable today when the business impact of a breach could be so much greater.

Additionally, today's threats – increasingly cloud-delivered and evasive – are much harder to pin down. Post-delivery detection is completely ineffective against such fast-moving dangers. The new battlefront is in real-time AI/ML-based detection of unknown threats, with inline defense at the edge of the network. In this way, malicious traffic can be blocked before it spreads, and policies can be enforced at the point where access happens.

In this landscape, if an organization's SWG isn't inspecting inline and in real time, then it's already behind. Integrated platforms are better suited than point products to the security challenges of modern distributed work, and their AI/ML-based defenses can detect unknown and zero-day threats.

How we do it

Netskope provides inline threat protection with malware, phishing, C2, and data exfiltration detection built into the inspection pipeline, not bolted on.

6. Stay fast. Everywhere. Always.

Avoid performance compromises and enhance protection.

Users are famously impatient in their online behavior. Even the slightest slowdown tends to cause frustration and prompt them to find workarounds that increase security risk. And with today's proliferation of personal apps and devices, temptation is never far away.

Unfortunately, many legacy SWG or firewall solutions are built on a "hub and spoke" design that creates data bottlenecks, delaying the user experience. That's why the smooth performance of corporate networks isn't just "nice to have" garnish: From a security point of view, it's an essential meal component to encourage the right user behavior.

Modern cloud-hosted SWG and firewall solutions provide the fast, reliable network access that people expect today. This should include mechanisms such as global load balancing to dynamically find the fastest data center location, and route control to automatically direct traffic around outages in milliseconds.

How we do it

Netskope's NewEdge Network is purpose-built for security at speed, with <30ms latency globally, full redundancy, and scalability.

> "Netskope SSE permitted faster connection speeds across vast regions compared with legacy network solutions, courtesy of Netskope's widely distributed NewEdge PoPs and robust fiber network." *

*Forrester: Total Economic Impact of Netskope SSE, October 2024

7. Provide actionable logs.

Greater visibility improves operations and incident response.

When issues arise or data activity needs to be inspected by infrastructure and security teams, their logs have to provide the appropriate level of visibility. Logs must be rich, near real-time, and usable for both troubleshooting and investigation.

Too often, however, teams are left flying blind with logs that don't provide key information, such as file names. That makes it impossible to work out, for instance, what documents a senior employee might have moved to personal cloud storage on his or her way out of the company.

With modern inline cloud access security broker (CASB) solutions, it's possible to see file names as well as additional details. With the right architecture underpinning the platform, modern solutions can go even further and provide traffic packet captures and session keys for decrypting. This ensures security teams can benefit from actionable telemetry, not just dump files or static reports.

How we do it

Netskope offers deep observability and session-level logging, with integrations into SIEM, SOAR, and observability stacks that infrastructure and operations teams already rely on.

TC
In
01
02
03
04
05
06
Number 7
C

Conclusion

The shift to remote working and the adoption of cloud, SaaS, and AI applications have transformed modern enterprises. User expectations have changed, while the attack surface has grown.

Infrastructure and operations (I&O) professionals need tools that are built for this reality, and that give them the ability to better understand and respond to the risks to their IT environment. With improved visibility, faster detection, more adaptive policies, and better performance, I&O teams can ensure users get secure, seamless access, wherever they work.

Book a meeting here for a personalized session with a Netskope expert. Discover how to modernize proxies, firewalls, and VPNs to improve operational efficiency and reduce complexity in your organization.

So when looking for a new solution, remember that your next-gen SWG and firewall must allow you to:

- Stop backhauling everything to nowhere.
- Decrypt without breaking everything (or everyone’s patience).
- Move beyond “allow” and “block” rules.
- Write a policy once, not in three consoles.
- Catch the unknown bad stuff before it gets in.
- Stay fast. Everywhere. Always.
- Provide actionable logs.

About Netskope

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.

Interested in learning more?

Request a demo

netskope