W

Secure Web Gateway: How SWG Filtering, TLS Inspection, and Policy Work

Learn how a secure web gateway applies URL, file, identity, and data policy, how traffic reaches it, what TLS inspection changes, and how to deploy one safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What does SWG stand for?
02 How traffic reaches an SWG
03 Common capabilities
04 SWG versus DNS filtering, proxy, and firewall
05 TLS inspection
06 Common deployment failures
07 Deployment checklist
08 SWG and SASE

A **secure web gateway (SWG)** applies security and acceptable-use policy to users' web traffic. It can evaluate URLs, domains, files, browser requests, user identity, and data movement before allowing, blocking, isolating, or recording an action. SWGs can be physical appliances, virtual proxies, cloud services, endpoint agents, or part of a SASE platform.

01 What does SWG stand for?

SWG stands for **Secure Web Gateway**. A proxy is one mechanism an SWG may use to receive and relay traffic, while the SWG category adds security controls such as malware scanning, URL classification, data-loss policy, identity context, and reporting. A basic proxy is therefore not automatically a secure web gateway.

02 How traffic reaches an SWG

- **Explicit proxy:** browsers and applications are configured to send requests to the gateway.
- **Network forwarding:** routing, tunnels, or firewall policy directs traffic through an on-premises or cloud enforcement point.
- **Endpoint agent:** managed software steers web traffic, including when a device is away from the office.
- **Browser integration:** an enterprise browser or extension applies selected policy and isolation.

The design must cover remote users, IPv6, cloud workloads, mobile devices, and applications that do not obey ordinary browser proxy settings.

03 Common capabilities

- URL and category filtering.
- Malware scanning, file-type controls, and sandboxing.

- Phishing and newly observed domain detection.
- Identity-aware access and acceptable-use policy.
- Data loss prevention and controls for uploads or form submissions.
- Remote browser isolation for high-risk destinations.
- Logging and integration with SIEM, SOAR, EDR, and incident workflows.

04 SWG versus DNS filtering, proxy, and firewall

Control	Typical visibility
DNS filtering	Domain-resolution requests and responses.
Proxy server	Relays traffic; security inspection depends on its configured purpose and features.
Network firewall	Connections, addresses, ports, state, and sometimes application identity.
Secure web gateway	Web requests, URLs, users, files, and selected content or data policy.

05 TLS inspection

Most web traffic is encrypted. To inspect content, an SWG may terminate the user's TLS connection and create a second encrypted connection to the destination using an organization-managed certificate. This can expose malware and prohibited data, but it also gives the gateway access to sensitive content.

TLS inspection requires protected certificate keys, clear privacy policy, narrow exclusions for sensitive categories where appropriate, certificate lifecycle management, and testing for pinned or mutually authenticated applications. A broken inspection configuration can weaken validation or interrupt business systems.

06 Common deployment failures

- Remote devices bypass policy outside the office.
- Applications use direct connections, another proxy, QUIC, or unsupported protocols.
- Broad TLS inspection captures more sensitive data than necessary.
- Category blocks lack an exception and review process.
- Gateway outages or latency become organization-wide web failures.
- Logs identify users and destinations without appropriate access controls and retention.

07 Deployment checklist

1. Map required traffic, identities, devices, locations, and bypass cases.
2. Start with monitor mode or a pilot group and measure latency and false positives.
3. Define fail-open or fail-closed behavior according to application risk.
4. Protect administration, certificates, policy changes, and service accounts.
5. Create a narrow exception workflow with owner and expiration.
6. Test uploads, downloads, IPv6, remote users, VPNs, browsers, APIs, and business-critical pinned applications.
7. Measure threat blocks, coverage, user impact, unreviewed exceptions, and time to correct false positives.

08 SWG and SASE

Secure web gateway is commonly one component of Secure Access Service Edge (SASE), alongside capabilities such as zero-trust network access, cloud access security broker functions, firewall as a service, and software-defined connectivity. Buying a bundled platform does not eliminate the need to define identity, routing, privacy, response, and resilience requirements.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com