

W

Web Security Gateway: How secure web traffic filtering works

What it is A web security gateway, often called a secure web gateway or SWG, is a security service that applies policy to users' web traffic. It can block malicious or prohibited sites, inspect downloads, enforce acceptable-use rules...

PUBLISHER

Gridinsoft Support

UPDATED

Jul 17, 2026

READ TIME

1 min

What it is

A web security gateway, often called a secure web gateway or SWG, is a security service that applies policy to users' web traffic. It can block malicious or prohibited sites, inspect downloads, enforce acceptable-use rules, and reduce data leakage between an organization and the internet.

How it works

Traffic is directed through an on-premises appliance, cloud proxy, endpoint agent, or network tunnel. The gateway evaluates the requested URL, domain reputation, content type, file behavior, user identity, and policy. Some deployments inspect encrypted HTTPS traffic using an organization-managed certificate, which requires careful privacy and certificate management.

Key points

- An SWG complements endpoint, email, identity, and DNS controls; it does not replace them.
- Remote users need an enforced path to the gateway or equivalent endpoint controls outside the office.
- Overly broad TLS inspection can expose sensitive information and break certificate-pinned applications.

Deployment basics

- Define user and data policies before choosing categories or block rules.
- Start in monitor mode, tune business exceptions, and retain clear audit logs.
- Use identity-aware policy and prevent simple bypass through alternate proxies or unmanaged browsers.
- Measure blocked threats, false positives, latency, and coverage for remote devices.

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](https://support.gridinsoft.com)