Skyhigh Security

Skyhigh Security Secure Web Gateway for On-Premises

KEY ADVANTAGES

- Block access to potentially malicious websites and web-based applications and services
- Protect against malware in real time
- Prevent loss of sensitive data through monitoring of inbound and outbound traffic
- Enforce compliance with company, industry, and regulatory policies
- Provide onsite and hybrid workers with secure access to internet resources and SaaS applications
- Accelerate your cloud migration and digital transformation with Skyhigh SSE

Intelligent web security to protect your onsite workforce and data

In the aftermath of the pandemic-driven remote work model, a return-to-the-office trend is gaining ground, typically in form of a flexible hybrid scenario, with some days spent at the office and some remotely. When employees are at the office, you need to protect them against web-based attacks, data exfiltration, and malware threats when they access the internet from the corporate network. Whether you have a hybrid infrastructure or a traditional corporate network, Skyhigh Secure Web Gateway for on-premises (on-premises SWG) adapts to your needs.

On-premises SWG protects your organization from zero-day threats and data exfiltration when users access the internet, cloud applications, and cloud services, while helping you maintain regulatory compliance. Deployed as a physical or virtual appliance, on-premises SWG handles the common HTTP, HTTPS protocols as well as legacy protocols such as SOCKs, FTP, and TCP protocols that need a proxy to communicate with other parts of the network or the internet.

Multi-layered security technologies—URL filtering, antivirus, zero-day anti-malware, SSL scanning, and data loss prevention (DLP)—are unified under a single easy-to-use management console to protect your users and data while ensuring regulatory compliance.

High-performance appliance with high-performance security

Whenever users request web access, on-premises SWG swings into gear, immediately enforcing your internet use policy by providing proactive protection against unknown or emerging threats for inbound and outbound traffic. In addition to blocking users from accessing malicious URLs, on-Premises SWG uses deep secure sockets layer (SSL) traffic inspection to detect and filter malware and unauthorized code and content hidden through encryption.

If you host websites that accept data or document uploads from external sources, inbound protection helps mitigate risks. In reverse-proxy mode, on-premises SWG scans content before it's uploaded, securing both the server and the content.

For outbound traffic, it uses industry-leading DLP technology to scan user-generated content on supported web protocols. It also protects against loss or leakage of confidential, sensitive, or regulated information when accessing all types of internet sites and services—from social media to online productivity tools offered by web-based platforms like Google G Suite, Box, Dropbox, and others.

BUSINESS BENEFITS

Protection against zero-day and unknown threats

- The gateway anti-malware engine keeps threats from reaching your users with multi-layered security.

Advanced protection for sensitive data

- Protect sensitive data by inspecting content in inbound and outbound traffic and use built-in predefined/ custom classifications and dictionaries.

Reduced management complexity

- Ease the burden on security teams with single-console management for policies and incident and increase performance and reliability.

Adaptable model for your hybrid environment

- Move to the cloud with confidence. Keep some appliances for regulatory compliance as you scale to meet the needs of your business and secure a remote workforce.

Gateway anti-malware engine provides comprehensive, up-to-date protection

Skyhigh Secure Web Gateway for on-premises leverages our unique gateway anti-malware engine that uses proactive intent analysis to filter out unknown or zero-day malicious content from web traffic in real time. It accomplishes this by scanning active web content, understanding how it behaves, and predicting its intent. This prevents zero-day malware from infecting endpoints, significantly reducing costly and labor-intensive system cleanup and remediation.

On-premises SWG also delivers web filtering protection through the powerful combination of reputation and category-based filtering. The appliance compares the site a user accesses against a global database of websites, email, and IP addresses based on hundreds of attributes and then assigns a reputation score based on the security risk posed. This helps your administrators apply granular rules about what users are permitted to access. Additionally, on-premises SWG helps your team gain geographic visibility and formulate policy management based on the country where users work and where web traffic originates.

Flexible integrations for a smooth hybrid deployment

For hybrid work environments, Skyhigh SWG for on-premises - the appliance trusted and used by enterprises worldwide - integrates fully with Skyhigh SWG for Cloud. As part of the Skyhigh SSE platform, the two solutions enable you to enforce the same security policy for web access by both on-premises and cloud users in just a single click. With Skyhigh SWG, you can combine the strength of appliances with the power of the cloud.

The hybrid deployment mode for Skyhigh SWG allows you to move to the cloud at your own pace, while keeping necessary on-premises appliances for your business needs. This hybrid model extends the same classifications and security policies for web access for both on-premises and cloud users—managed from a single console. Skyhigh Security is the first vendor to offer this powerful implementation mode.

Our latest on-premises F-Series Appliance provides exceptional performance, increased capacity, and a smaller appliance footprint, with its 2x Xenon Gold CPU and 192 GB of memory. Whether your organization continues to operate on premises or has evolved to a hybrid environment, this appliance provides maximum flexibility and adaptability.

SKYHIGH SWG FOR ON-PREMISES FEATURES

Advanced data protection:

- Inbound and outbound content scanning: Works across all key web protocols, including SSL, to protect sensitive data and intellectual property while ensuring regulatory compliance.
- Pre-built DLP dictionaries: Enables custom dictionaries to be created through keyword matching and/or regular expressions.

Enterprise-grade threat protection:

- Gateway anti-malware engine: Provides protection from zero-day and unknown threats.
- Powerful threat protection controls: Improves security response and mitigation and applies granular access policies based on global threat intelligence and reputation scores.
- Application visibility and control: Blocks access to websites based on categories, reputation, or risk. It applies different policies to personal and corporate tenants, prevents potential infections and data loss, and enforces internet browsing policy. Apply granular controls on uploads and downloads based on corporate policy.
- URL and category filtering: Blocks access to risky and/or malicious content and sites and prevents malware.

The industry-leading data-first Skyhigh Security Service Edge (SSE) Platform

For organizations moving to hybrid SWG or full cloud SWG, having a central console is pivotal. Skyhigh Secure Web Gateway is part of the unified Skyhigh Cloud Platform that integrates multiple innovative security technologies—Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and Remote Browser Isolation (RBI)—all managed from the same central console. The Skyhigh Cloud Platform enables fast, reliable, and safe work-from-anywhere and digital transformation by securing web, cloud, and private applications.

The Skyhigh Cloud Platform addresses the complexity of remote workforce deployments with centralized visibility and incident management, adaptive and tailored access control, end-to-end data protection, and advanced threat protection. By partnering with leading SD-WAN vendors, Skyhigh Security delivers cloud security with a simplified, reliable, and low-latency service that aligns with your roadmap for your SSE journey.

The Skyhigh Cloud Platform provides modern data protection policies for data in motion and data at rest that determine what can be accessed, what can be shared, and how it can be used. It goes beyond zero trust by monitoring user actions to identify risky behavior: sites visited, personal or work devices, employee or contractor, type of data, and many other factors. It ensures sensitive data is accessed, shared, and stored appropriately.

Large enterprises across all sectors—from government agencies to financial institutions—look to Skyhigh Security to protect their data across their hybrid infrastructure. Our customers include nearly half of the Fortune 100 and more than a third of the Fortune 500.

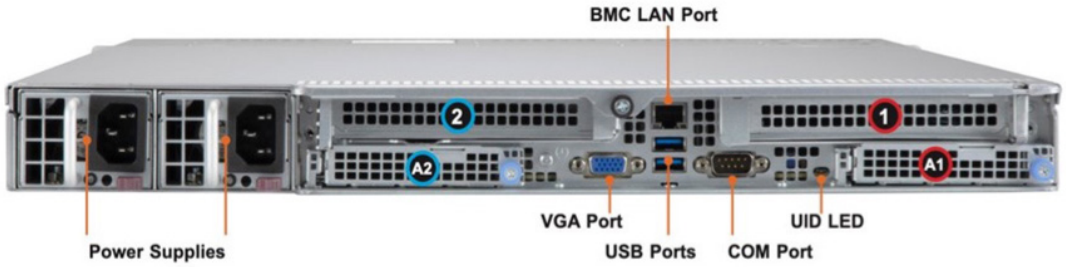
Features	Skyhigh Secure Web Gateway for On-Premises Web filtering solution for your on-premises workforce
Hybrid SWG	Yes
Management Console	On-premises Secure Web Gateway platform
Appliance-based	Yes, physical and virtual options
Supported Protocols	HTTP, HTTPS, FTP, SOCKS, and other TCP traffic
SSL Decryption	Yes
Load Balancing	Yes, bandwidth optimization, load balancing
Access Control	Yes, robust and granular policies
URL and Category Filtering	Yes
Application Visibility and Control	Yes
Real-Time Threat Prevention	Yes, inline on-premises emulation-based sandboxing via the gateway anti-malware engines
Data Protection	DLP policies on web traffic only
Built-in Data Protection	Yes, based on predefined/custom classifications and dictionaries

HYBRID TRANSFORMATION BENEFITS

- Quickly start moving remote users to the cloud.
- Use Skyhigh SSE as your central, cloud-based management, reporting, and policy enforcement platform.
- Extend on-premises policy to the cloud with a single click.
- Update lists in Skyhigh SSE and sync to appliances.
- Configure Skyhigh SSE as the next hop.
- Continue to use appliances for compliance, legacy protocols, and compliance.
- Extend and expand scanning capabilities.

F-Series Appliances Specifications

Features	On-Premises Security Gateway Appliance: WBG-5000-F	On-Premises Security Gateway Appliance: WBG-5500-F
Form Factor	IU	IU
Processor	1x CPU 12C, 2.0 GHZ, 30MB CACHE (XEON SILVER 4410Y)	2x CPU 24C, 2.1 GHZ, 45MB CACHE (XEON GOLD 5418Y)
Memory	64GB	192GB
Network Interface	1 x 4-PORT, 10GBPS, RJ45	1 x 4-PORT, 10GBPS, RJ45
USB Interfaces	Front: 2 x USB 2.0 Back: 2 X USB 3.0	Front: 2 x USB 2.0 Back: 2 X USB 3.0
Serial Interface	1 COM Port(s) (1 rear)	1 COM Port(s) (1 rear)
RAID	RAID 1	RAID 1
SSD	2 x SSD, 2.5”, 960GB, SATA	2 x SSD, 2.5”, 960GB, SATA



For More Information

Protect your users from web-based threats and prevent data exfiltration with Skyhigh Secure Web Gateway for on-premises. Visit us to learn more or contact your sales account manager or partner.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

October 2023. DS-EN-000019-01