Skyhigh Security

Skyhigh Cloud Firewall

BUSINESS BENEFITS

- Improved security: Safeguard users accessing the internet and cloud-based resources and applications from malware, phishing attacks, and other types of attacks. Remote workers enjoy a higher level of security and lower latency. Security teams can easily monitor, log, and investigate network traffic in real time from a single console.
- Lower costs: Compared to on-premises firewall appliances, Skyhigh Cloud Firewall eliminates the need for purchasing and maintaining a physical firewall infrastructure, which can be expensive and time-consuming.
- Flexibility: Empower your geographically dispersed or mobile workforce to work from anywhere with a secure connection to authorized internet access.
- Scalability: Skyhigh Cloud Firewall helps you stay agile and respond quickly to changing business demands, whether driven by an expanding workforce or increased cloud and internet traffic.

Policy-Based Access Control for Your Extended Workforce

Transforming your firewall protection

With enterprise applications moving out of the data center and into the cloud and users connecting from anywhere, traditional on-premises firewalls are no longer viable. They're just not built to handle the high demand and throughput requirements for cloud services in today's hybrid work environment. Backhauling outbound traffic to firewall appliances adds management complexity, degrades the user experience, creates security gaps, and increases cost.

It's time for a more effective, reliable, and efficient way to inspect internet and cloud traffic. Skyhigh Cloud Firewall supports your users and protects your vital data with high-performance, comprehensive network security by inspecting all outbound traffic – regardless of location.

Why on-premises firewalls fall short in a hybrid environment

Now that users are accessing the internet and cloud services from any device and any location, the need for protection is more pressing than ever before. An estimated 70% of enterprise workloads will be in the cloud this year, up from 40% in 2020.[1] Organizations need comprehensive cloud-delivered network security to ensure that all users get consistent protection without sacrificing productivity. And they want security solutions that are easy to implement and can scale quickly as their needs change.

If your legacy network is still an important part of your infrastructure, re-architecting your network to accommodate the cloud infrastructure can be time-consuming and challenging. Physical firewall appliances are costly, complex to maintain, difficult to scale, and often slow down productivity for your remote workforce. Adding firewall capabilities in new regions puts a heavy burden on your teams, as it requires shipping and installing on-premises equipment in each new location. Additionally, with sensitive data moving to the cloud and with broad user access to it, protecting data becomes more challenging.

While some enterprises have deployed cloud secure web gateway (SWG) controls, which are critical and required for web protection, they're not enough. You still need to ensure that all traffic from remote users is controlled—and that includes both web and IP-based traffic.

1. Gartner Predicts the Future of Cloud and Edge Infrastructure, Published Feb 11, 2021.

KEY USE CASES

- Minimize latency and delivery a high-performance, seamless user experience: Moving to a cloud-based firewall removes roadblocks for keeping up with an increasingly remote workforce, provides faster access to the internet and cloud, promotes productivity.
- Complete control over outbound network traffic: Scan outbound traffic across all IP protocols and ports. Create consistent security policies to block access to risky and/or malicious cloud assets. Gain visibility and log outbound user access requests and sessions to cloud services.

A more secure, low-latency alternative to protecting remote workers

What's the alternative to expensive and cumbersome on-premises firewalls? Skyhigh Cloud Firewall, which converges with the comprehensive security offered by the Skyhigh Cloud Platform. It's a cost-effective and secure way to for users connecting from anywhere to access the resources they need—without the latency and bandwidth issues that come with backhauling traffic to on-premises firewalls. Skyhigh Cloud Firewall monitors outbound traffic across all IP protocols and ports and applies consistent block or allow policies to connect your users securely to sensitive data, cloud applications, and workloads—from anywhere and without compromising performance.

Outbound traffic monitoring that covers every angle

Skyhigh Cloud Firewall applies multiple controls to any traffic leaving your organization, regardless of where it originates. It detects and filters traffic across all IP-based protocols (TCP, UDP, ICMP, and more) and ports and applies the same consistent policies.

You can configure policies that are consistent with Skyhigh Cloud Platform policies based on IP, host, domain, port, user, group, process name, and other parameters.

Combining the power of cloud firewall with SWG

Skyhigh Cloud Firewall goes beyond basic firewall block and allow policies by seamlessly integrating with SWG to provide an additional layer of security for web traffic. When Skyhigh Cloud Firewall detects HTTP and HTTPS traffic on non-standard ports, it routes that traffic to Skyhigh SWG. Only the traffic that needs deep content inspection is sent to Skyhigh SWG, while the rest takes a faster path for better throughput. Skyhigh Cloud Firewall even uses the same client as Skyhigh SWG, making it easy to deploy and manage.

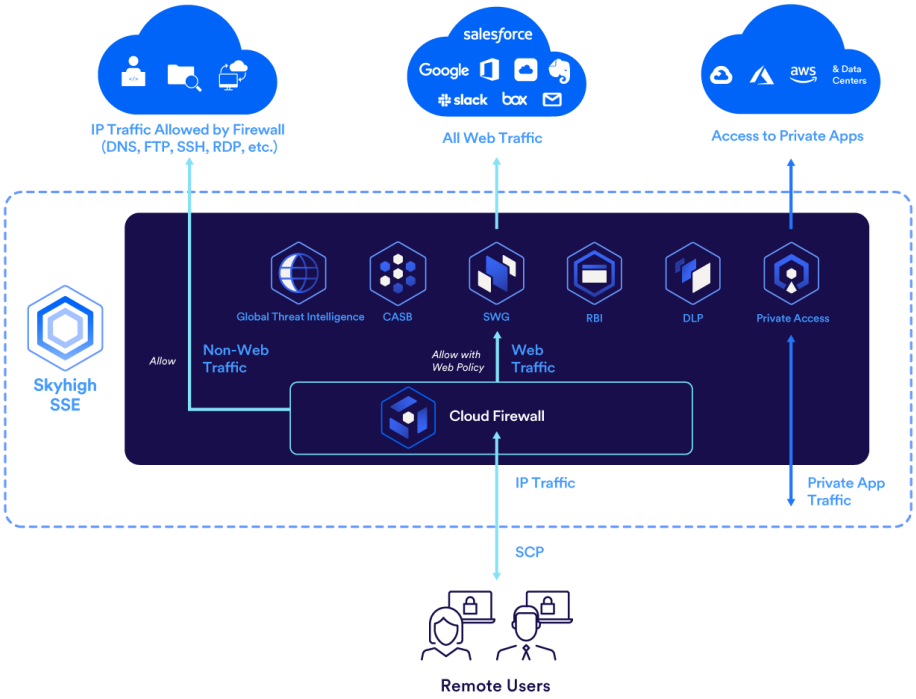

Figure 1. Skyhigh Cloud Firewall diagram

KEY USE CASES

- Stop backhauling traffic to on-premises appliances: There's no need to send traffic back through the data center or anywhere on-premises firewalls are located for network security. Instead, connect to a hyperscale, cloud-delivered service edge that monitors traffic for unauthorized access from anywhere in the world.
- Reduce risk in your hybrid environment, including branch offices and remote workers: This innovative cloud-delivered firewall provides fast, secure access to cloud and internet resources and workloads from anywhere in the world. It performs rules-based network traffic monitoring to prevent non authorized outbound traffic. Cloud firewall allows access, blocks access, silently drops access, or allow access with web policy. When access is allowed with the web policy, the power of SWG is combined with the cloud firewall to send the web traffic for deep content inspection.

Richer options for building firewall policies

Most cloud firewalls have certain limitations when it comes to policy creation. With Skyhigh Cloud Firewall, you can build policies based on process name. The unique advantage of defining policies based on process name is that it enables you to detect and control process-based traffic from applications like Zoom or Microsoft Teams. This gives you greater control over traffic that comes from potentially vulnerable software components in the network, and ultimately, more control on your organization's security posture. Until the vulnerability is mitigated, you can deny outbound access to vulnerable processes.

Since the policy interface is similar to most standard firewalls, Skyhigh Cloud Firewall can handle any traffic use case. Routing actions include allow, block, drop, or elevate to Skyhigh SWG. This shortens your learning curve and makes policy administration and enforcement easy.

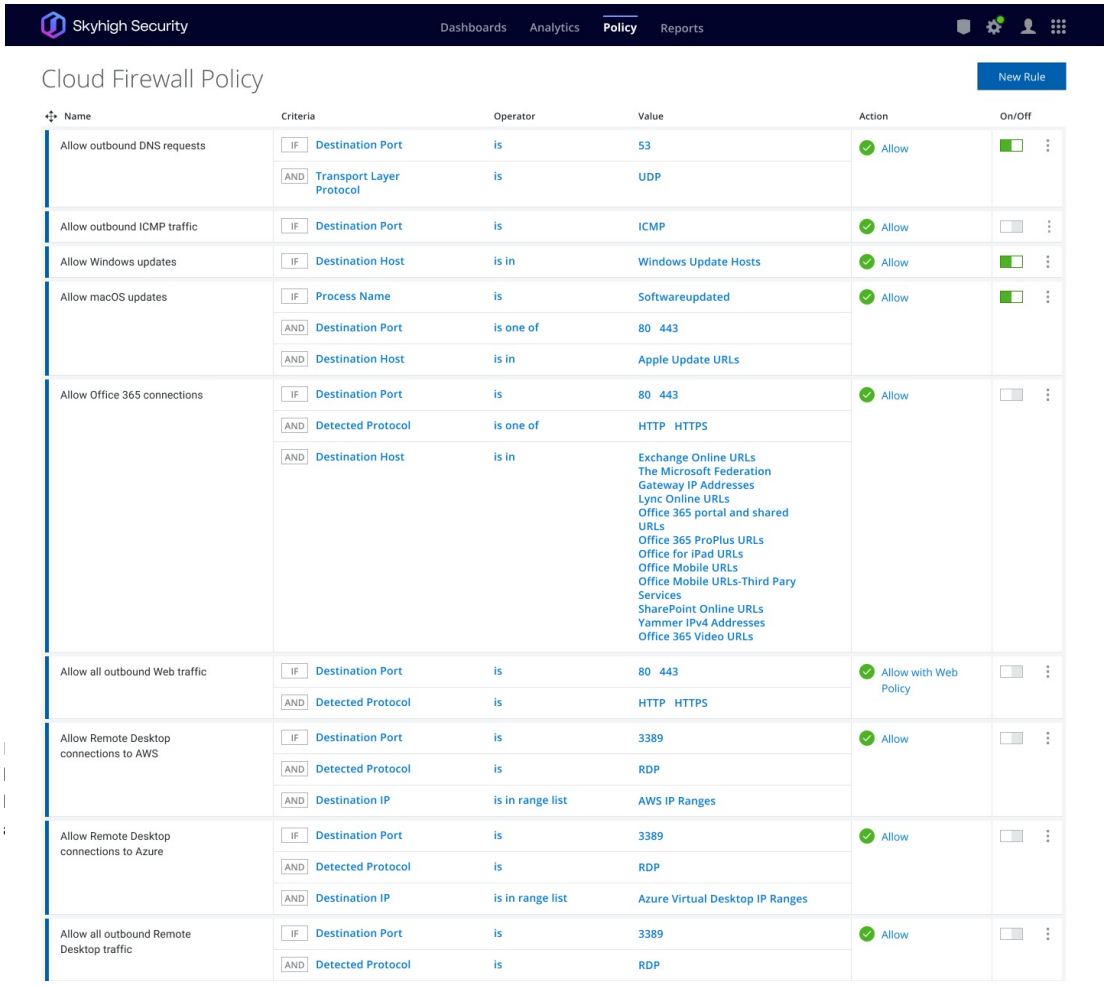

Figure 2. Skyhigh Cloud Firewall policy dashboard.

The Industry-Leading, Data-First Skyhigh Security Service Edge Solution

Skyhigh Cloud Firewall is part of the unified Skyhigh Security Service Edge solution that integrates multiple innovative security technologies – all managed from the same central console, the Skyhigh Cloud Platform. 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 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.

Product Highlights

Feature	Benefit
Policy enforcement over all IP traffic	
Detects and filters all IP-based protocols (TCP, UDP, ICMP, and more) and ports. Uses the same client as Skyhigh SWG.	No need to deploy another client. All user traffic is managed with a single, unified cloud-based management console.
Network visibility	
Provides a view into network analytics, along with a summary of the firewall traffic data.	Traffic visibility from Layer 4 to Layer 7 facilitates risk management, troubleshooting, and compliance.
Seamless integration of Skyhigh Cloud Firewall and Skyhigh SWG	
All IP traffic can be configured to go to the firewall. Specific web traffic that needs additional inspection can be routed to Skyhigh SWG, which either sends it to internet directly or blocks it.	More comprehensive traffic inspection, resulting in greater control over your organization's security posture.
Policy creation based on multiple attributes	
These include all traffic, processes, user, group location, client IP, destination IP, port, detected protocol, host, URL, domain, and others.	Flexible ways to build policies and manage traffic based on your business needs.
Location independence	
Automatic detection and forwarding of IP traffic, regardless of where it originates.	Seamless firewall security no matter where the user works.
Options for routing traffic	
Send all IP traffic or selected traffic to Skyhigh Cloud Firewall.	Offers flexibility in IP-level traffic inspection.

Feature	Benefit
Local breakouts for high-bandwidth traffic	
Bypass certain types of traffic (for example, from conferencing applications, like Zoom and others) and send it directly to the destination while maintaining visibility by logging the traffic on the agent.	Better performance for business-critical applications.
Split traffic steering	
Forward certain traffic via Skyhigh Cloud Firewall and certain domains to the local proxy.	Flexibility for hybrid enterprise deployments through effective integration with corporate IT infrastructure to handle specific traffic, thereby improving security and performance.
Protocol detection	
Detects web traffic on non-standard protocols and routes it to Skyhigh SWG for analysis. While users can escape web traffic inspection by sending HTTP/HTTPS traffic on non-web ports, Skyhigh Cloud Firewall detects HTTP/HTTPS on such traffic, inspect it, and apply necessary firewall policies.	Receive better visibility to and control over web traffic, and ensure traffic is secure This feature is directly available on the firewall policy creation, increasing ease of use.
Prevents HTTP traffic masked through IP ports	
Uses standard ports for other protocols like HTTPS or DNS.	Prevent C&C (command and control) communications by attackers, which can lead to network compromise and data exfiltration.
Policy interface is similar to most standard firewalls	
Can handle any traffic use case; traffic routing actions, including allow, block, drop, or elevate to Skyhigh SWG.	Makes administration easier, with multiple routing options and a minimal learning curve.
Ease of management	
Integrated with the Skyhigh Cloud Platform, with event login capabilities, management, and reporting consolidated into one pane of glass, along with centralized policies for data protection.	Simplifies administration, saves time, and reduces complexity.
Cloud deployment	
Skyhigh Cloud Firewall provides consistent access policies and protection against malicious network traffic, while handling the high-throughput demand for access to cloud applications and services.	Forward-looking, flexible, model that delivers the agility and scalability that only a cloud firewall can offer, without the high costs and management complexities.

For More Information

Step up your network security while providing your workforce with faster access to the cloud and internet resources they need to be productive with Skyhigh Cloud Firewall.

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

March 2023