Skyhigh Security

Skyhigh Secure Web Gateway (SWG)

Reverse proxy and ICAP deployment options

Skyhigh Secure Web Gateway: Reverse Proxy

A secure web gateway configured in reverse proxy mode applies malware detection rules to content being uploaded to, rather than downloaded from, a website. Internet Content Adaptation Protocol (ICAP) enables administrators to off-load malware scanning to a dedicated server to improve security and overall performance.

The web has become an essential, yet dangerous place for businesses to operate. Skyhigh Secure Web Gateway security software is designed to protect enterprises against web-borne malware attacks. Skyhigh Secure Web Gateway can be configured to protect against malware downloads from external sites, or it can be configured to protect an internal website against malicious uploads from an external user. In either mode, it allows customers to ensure secure access to vital web-based systems.

The Web Security Problem

The web, while essential, is also a dangerous place for businesses to operate. With the surge in webbased attacks, it's critical for businesses to protect themselves against data breaches caused by external infected websites attempting to download malware onto internal systems. At the same time, organizations need to provide users with the ability to upload content to an internal website. For example, they may want to provide contractors with access to a work order site or customers to a support forum.

A secure web gateway solution can be used to protect an organization in either scenario, using either a forward or reverse proxy configuration, depending on the business problem the company is trying to solve.

Skyhigh Secure Web Gateway Protective Features

Skyhigh Secure Web Gateway uses multiple, layered techniques to scan web traffic to identify and block malware-infected payloads or enforce acceptable usage policy. Malware may be hidden in a wide variety of formats, such as Adobe PDF or Flash files, Java/JavaScript code, or media files.

It leverages Global Threat Intelligence (GTI) service to block websites with a high-risk reputation. The Gateway Anti-Malware (GAM engine scans for previously unknown (zero-day) malware that may be lurking in a web page.

Secure sockets layer (SSL) scanning ensures that encrypted traffic is examined, reducing the threat of hidden malware sneaking in.

Reverse Proxy/ICAP Benefits

- Enhances network security by isolating internal sites from direct contact by external users
- Protects internal websites against malware infection by contaminated content
- Other security measures, such as data loss prevention (DLP) scanning or strong authentication, can be applied in reverse proxy mode
- Provides administrators with multiple deployment options, giving them the flexibility to choose the most appropriate configuration

Administrators can enforce DLP rules to verify that sensitive or regulated content is not being transmitted, and multifactor authentication can verify a user's identity before allowing them access to a sensitive system.

Web Gateway Proxy Modes

Forward proxy

In a forward proxy configuration, Skyhigh Secure Web Gateway intercepts internal user requests to visit a website, which is typically external. The downloaded content from the site is analyzed to verify that it is free of malware before being delivered to the user.

Reverse proxy

Many organizations also have internal websites, which they make available to internal (employees) or external users (contractors, partners, clients, and others) who need to upload content to the site. These sites need to be protected against attempts to upload infected content. For this use case, administrators deploy Skyhigh Secure Web Gateway in reverse proxy mode to scan and analyze content before allowing it to be uploaded to the target site.

In Figure 1 below, an internet user attempts to upload content to a website. A load balancer sends the content to a Skyhigh Secure Web Gateway cluster, which examines it.

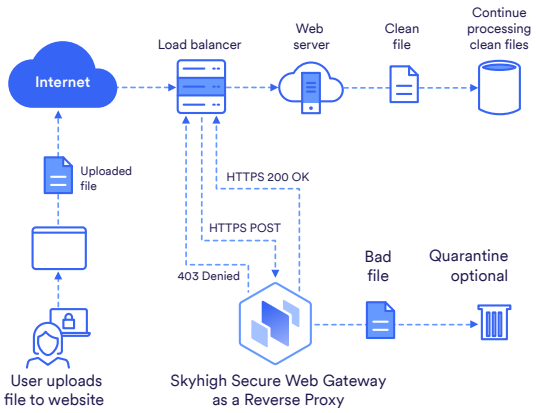

Figure 1. Typical reverse proxy configuration.

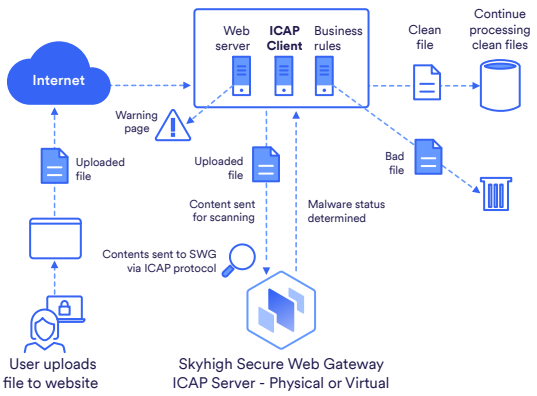

Figure 2. Typical ICAP configuration.

If the content fails examination, Skyhigh Secure Web Gateway returns a 403 “Denied” response to the user. If the content passes inspection, the load balancer forwards it to the web server for further processing.

Internet Content Adaptation Protocol

(ICAP) ICAP provides a standard lightweight mechanism for a web server (the ICAP client) to send content to an ICAP server for some further, specialized action. Skyhigh Secure Web Gateway, acting as an ICAP server, can perform a full range of malware analysis and scanning. Files infected with malware can be prevented from contaminating the web server, while files free of malware can be processed.

In the example shown in Figure 2, the user attempts to upload the file directly to the web server (ICAP client), which transmits the file to the Skyhigh Secure Web Gateway cluster (ICAP server). If the file passes inspection, Skyhigh Secure Web Gateway notifies the web server to continue processing it. If the file fails, then the ICAP client takes the appropriate corrective action, based on the business logic of the ICAP application.

Deployment Considerations

- The major differences between a reverse proxy and an ICAP server configuration are as follows:
- In reverse proxy mode, Skyhigh Secure Web Gateway intercepts the content before it reaches the web server, processes it, and then either blocks or forwards it, depending on the results of the analysis. If the content is blocked, it never reaches the web server.
- In an ICAP configuration, the web server receives the content and forwards it to Skyhigh Secure Web Gateway for further analysis before processing it. The web server gains the benefit of having the ICAP server perform more in-depth analysis, freeing up resources on the web server.
- Reverse proxy mode doesn’t require any additional software development, but block responses returned to the user must be taken into account, and block pages can be designed to conform to the style of the site.
- ICAP mode requires that an ICAP client be written and installed within the data flow of the application.

Learn More

skyhighsecurity.com/swg

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

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2023.
September 2023. DS-EN-000017-01