Skyhigh Security

Navigating the Limitations of a Shared Cloud Infrastructure

DEDICATED IP ADDRESS USE CASES

- IP restrictions for authentication or cloud service logins: In environments where sensitive data is being handled, access to services is typically restricted based on the source IP address. This can be used for authentication purposes, or to ensure that only users that are authorized can access critical services
- Abide to local governance and jurisdiction laws: It is now common in today's globalized regulatory landscape for countries to enforce data laws and infrastructure compliance. Organizations may fall under these jurisdictions, needing to source traffic through specific locations and ensure that their data be processed and stored within their borders.
- Reputation management: Monitoring and managing IP reputation is crucial for an organization, as it directly impacts ability to conduct regular business, email deliverability, and other digital interactions. Organizations must ensure that their business activities are not impacted by being blacklisted due to a "noisy neighbor" from a shared IP address

As organizations transition from on-premises to cloud environments in today's interconnected digital landscape, the use of a shared cloud infrastructure can introduce significant challenges and risks. Modern day organizations must have an understanding of the risks associated with a shared cloud infrastructure and prioritize risk mitigation. If so, they can effectively manage these concerns by implementing appropriate technologies, and by enabling enhanced control and monitoring capabilities.

Challenges of shared IP addresses

One of the challenges faced by organizations migrating from on-premises to cloud is the loss of control over outbound traffic. Before, organizations with an on-premises security solution were accustomed to using unique IP addresses for ingress and egress traffic. But after migrating to a cloud security solution, organizations find themselves challenged with using a pool of IP addresses shared by other organizations with the same cloud security vendor. This imposes limitations on how much control an organization has over security measures, and can impact compliance with industry or government regulations that require specific IP-based controls.

This leads organizations into the next challenge, regulatory compliance. Many industries, such as financial services and healthcare, are subject to strict regulations with limitations on where data is stored and requirements on where traffic can originate. Shared IP addresses do not guarantee adherence to these regulations, potentially exposing organizations to risks, monetary penalties, and legal trouble.

A final challenge faced by organizations with shared IP addresses is IP reputation management. The risk of reputational damage caused by the actions of others, such as "noisy neighbors", is high for organizations with shared IP environments. This can happen in the form of blacklisting by email servers, impacting online service access, and affecting general business operations.

How to maintain control, compliance, and IP reputation

When faced with these challenges in maintaining control, compliance, and IP reputation over outbound internet traffic in cloud environments, what can an organization migrating from on-premises to the cloud do? Skyhigh Security addresses these concerns by offering two options to use dedicated IP addresses, exclusively used by an organization; Dedicated Egress IP Service and Source IP Anchoring.

BUSINESS BENEFITS

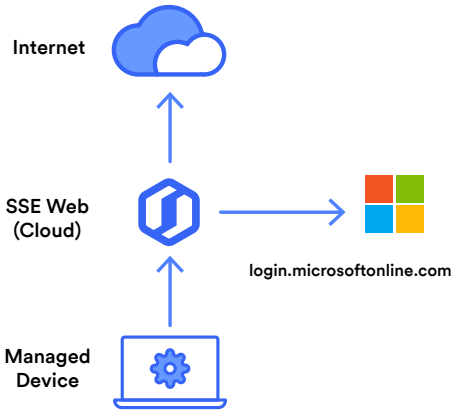
Dedicated Egress IP Service:

- Enhanced Control: Purchase additional IP addresses and choose the Point of Presence (PoP) for traffic routing
- Traffic Monitoring: Route traffic through a specific IP address, allowing to monitor traffic more closely
- Selective Traffic Routing: Redirect selective traffic through the dedicated IP address
- Improved Reputation Management: Avoid issues such as “noisy neighbor” scenarios and protect against IP reputation damage

Dedicated Egress IP Service

The Dedicated Egress IP Service allows organizations to use a dedicated IP address, exclusively used by them, to egress from Skyhigh Secure Web Gateway (SWG) to the Internet. This addresses the challenge of shared IP addresses in cloud environments, allowing organizations to:

- Selectively route traffic through Peering Points of Presence (PoPs) using IP addresses purchased from Skyhigh Security
- Comply with local governance and jurisdiction laws by sourcing traffic from designated countries
- Manage and monitor IP reputation effectively, avoiding issues like IP reputational damage



Skyhigh SWG for Cloud offers Dedicated Egress IP Service. This feature allows an organization to use a dedicated IP address exclusively assigned for egress from cloud SWG to the Internet. An organization can utilize this IP for either selected traffic or all traffic, depending on their requirements. As part of this feature, organizations will have the flexibility to choose the country through which they want to route traffic.

BUSINESS BENEFITS

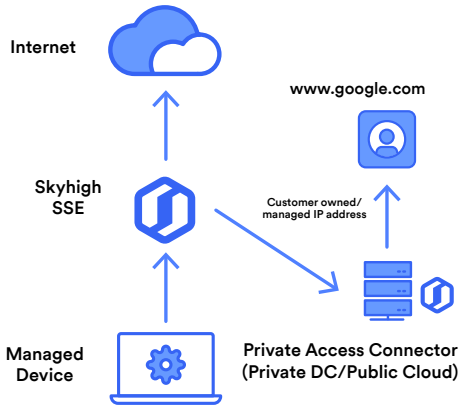
Source IP Anchoring:

- Utilization of Customer-Owned IP Addresses: an organization can leverage its existing IP addresses or blocks within the service framework
- Flexible Deployment: connectors can be installed in both public and private data centers, ensuring compatibility and scalability
- Cost Savings: no additional costs associated with this feature for organizations with Skyhigh Private Access
- Complete Management Control: an organization maintains full control over the solution, managing and configuring their IP anchoring setup according to their specific requirements

Source IP Anchoring

Skyhigh Private Access leverages Source IP Anchoring, empowering organizations to safeguard internet traffic and SaaS applications. This feature enables control over the endpoints, which are used to access external third-party resources with source IP restrictions. Key capabilities include:

- Route private and public traffic through the Skyhigh Secure App Connector to ensure it exits through a fixed egress IP, maintaining control and compliance
- Use of the organization's own IP address space (BYOIP) to control and manage the solution entirely
- No additional bandwidth costs for public and private application traffic, included as part of Skyhigh Private Access



With Source IP Anchoring, organizations can enable access to private and public applications using public IP addresses by defining them as Skyhigh Private Access applications. By doing so, all requests are routed through the Secure App Connector, ensuring traffic exits from the organization's network and egresses with the public IPs, allowing full control and monitoring.

Enhanced Traffic Routing Control with Skyhigh Security

In summary, Dedicated Egress IP Service and Source IP Anchoring address important challenges faced by organizations in maintaining traffic control, remaining compliant, and managing their IP reputation.

With Skyhigh SWG, Dedicated Egress IP Service offers businesses much-needed control over their outbound traffic. By using these IPs, companies can avoid the pitfalls of shared IPs, such as the loss of control over outbound traffic, lack of regulatory compliance, and the risk of IP reputational damage. With this solution, organizations can selectively route their traffic through our Peering Points of Presence (PoPs) using IP addresses purchased from Skyhigh Security.

With Skyhigh Private Access, Source IP Anchoring allows organizations to leverage their existing IP addresses efficiently. Simplifying access management across different data centers—both public and private—without adding extra costs beyond the initial setup. This ensures that organizations can operate securely and in line with regulatory standards.

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

Skyhigh SWG and Skyhigh Private Access are part of the unified Skyhigh Security Service Edge (Skyhigh SSE) 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.

For More Information

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

July 2024. DS-EN-000033-01 DS-EN-000033-01