Skyhigh Security

WHITE PAPER

DNS Security vs. Secure Web Gateways

Table of Contents

In today's reality of maniacally heavy cloud usage both for personal and business purposes, the familiar topic of web security has become more paramount yet insidiously complicated. Diverse network architecture, roaming users, a plethora of client platforms, BYOD, the death of the traditional network perimeter, and countless more technical considerations are poised to haunt the dreams of security professionals who dare take on the challenge of securing their organization's web traffic. Domain Name System (DNS) security has arisen as an alternative to the complexity of a full-blown Secure Web Gateway (SWG) solution, promising simplicity and speedy deployments. Essentially, DNS security plugs into domain name resolution to prevent access to risky domains. This allows organizations to streamline web security by treating domains as "neighborhoods" and preventing access to riskier domains and steering users toward more "well-lit" areas. While this approach greatly simplifies the web security problem, it comes with some limitations. Let's take a close look at what makes DNS security such an enticing proposition and analyze whether it's truly the silver bullet many organizations crave.

DNS Security is enticing, but is it enough?

The benefits of DNS security are clear from the outset. Probably most alluring is the lack of need for any network rearchitecting. This is, generally speaking, just a replacement for, or addition to, your DNS infrastructure. The network team's involvement can be minimal. The nature of the technology also enables the protection to extend outside the organization's network effortlessly securing the ever-growing number of offsite users. As an added bonus, DNS security goes beyond the capabilities of SWG by providing coverage for all ports and protocols. But wait, there's more! The policy? Simple! Block high risk domains, block the usual naughty web categories, and you're done! What's not to love here?!

So, what's the cost for all this goodness? In a word, visibility. When you relegate your web security to looking at DNS requests, you lose important context and acuity. A DNS security solution knows simply that a domain was resolved by a client. The traffic sent to the domain after DNS resolution is utterly unknown and lost. Your DNS security solution will not answer questions like, "How much traffic was sent to or received from this domain? Using what protocols? On what ports? What files were transmitted, and were they malicious? Was any sensitive data uploaded to personal cloud accounts?" These unanswered questions represent not only lacking visibility and context but also glaring security gaps.

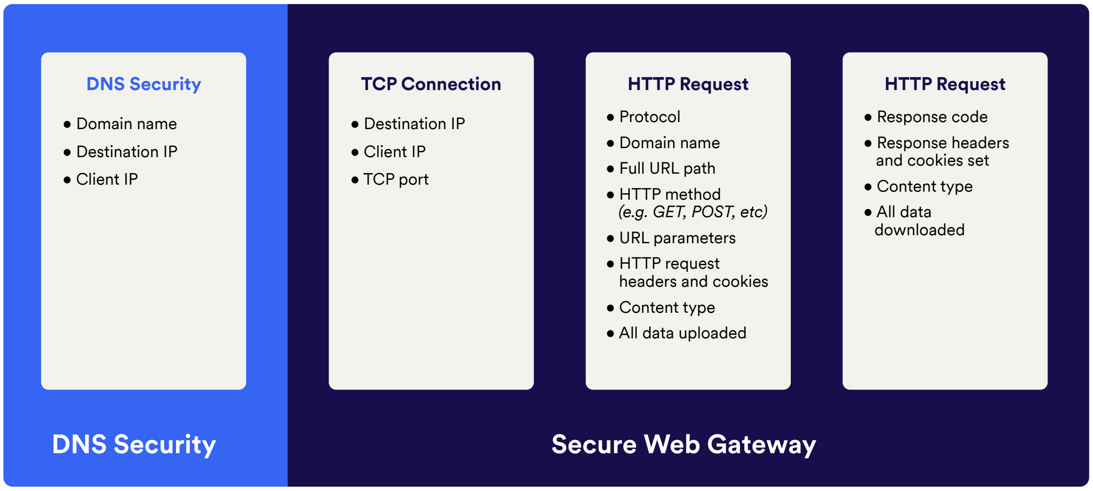
Zoom in one step further and assume a worst-case scenario. What if your organization were being targeted with web-based threats? How hard would it be to circumvent your DNS security entirely? One option would be to get malicious content onto a "known good" domain. This could be as trivial as a shared link to a file on a personal Dropbox or OneDrive account. Better yet, an attacker could simply avoid using domain names. Using a URL with an IP address in a phishing email is probably just as likely to hoodwink a gullible user as a link using a hostname. Even if the attacker needed to use IPs dynamically, there are other ways to get an IP to a victim machine such as posting to a social media account, dropping it in an S3 bucket or countless other options. You simply can't afford to assume DNS queries will be a part of every attack on your environment.

In addition to visibility, control is also sacrificed at the altar of simplicity and fast deployment. When your control point is limited to a DNS request, your response options are limited as well. Often, you're left with the option to allow or block, and this decision has to be made with no more context than a domain name. This results in either an overly-lenient, risky policy or a draconian alternative that will tarnish the internal perception of the security team. There's no option to implement a more sensible policy such as "Facebook is allowed, but you can't chat" or "personal Dropbox accounts are okay, but we're scanning uploads for sensitive data."

What added value can SWG bring?

With this new perspective we take another look at SWG and find that it brings a lot to the table. It's a highly mature technology purpose-built to decipher and scrutinize the one protocol that probably accounts for more than 90% of traffic generated by your endpoints – HTTP/S. Visibility and context abound! Domain names are now full URLs. You can now scrutinize the content of every single request including both traffic sent and received by endpoints.

This increased visibility translates directly into improved security. SWG solutions can not only ensure that users are visiting appropriate and trusted domains but can perform malware analysis on all content downloaded including that link to a file from a personal Dropbox account. When content is uploaded, it can be scanned for sensitive data to ensure no regulations are broken or intellectual property lost. One more recent addition to the SWG toolkit includes the ability to enforce tenant restrictions. Tenant restrictions are a critical way to ensure data protection by enforcing that users not only use sanctioned services but also use a sanctioned tenant, or instance, within those services. Coupled with CASB controls, enforcing tenant restrictions allows data to safely migrate "out the door" through the web security solution and remain within the organization's control. Because API-based CASB controls can only be applied to tenants owned by the organization, ensuring users don't use other "shadow" tenants is critical to this process.



DNS Security

- Domain name
- Destination IP
- Client IP

TCP Connection

- Destination IP
- Client IP
- TCP port

HTTP Request

- Protocol
- Domain name
- Full URL path
- HTTP method *(e.g. GET, POST, etc)*
- URL parameters
- HTTP request headers and cookies
- Content type
- All data uploaded

HTTP Request

- Response code
- Response headers and cookies set
- Content type
- All data downloaded

DNS Security

Secure Web Gateway

Deep inspection of all web traffic also empowers organizations to apply more tactical responses to certain user behaviors. For example, activity controls are a common capability that allow security teams to permit domains related to some cloud applications but prevent certain activities within those applications. Users want access to their personal Dropbox or Evernote accounts, but security teams are concerned about data security. Using activity controls, you can permit these applications but prevent uploads. Another example is user coaching. Perhaps an allowed domain was recently compromised. Rather than react by blocking the domain, the organization can decide to notify the user to change their credentials immediately. Another fairly recent advancement allows content with unknown or only slightly suspicious risk to be viewed through an isolated browser. Remote Browser Isolation (RBI) can be employed to allow access to content not known to be safe while still insulating endpoints from risk. The requested content is loaded in a temporary browser isolated in the web security vendor's datacenter, and the user is allowed to view and interact with that remote browser without loading any of the site's content locally. This allows access to the content while preventing any malware risk on the endpoint.

WHAT ABOUT SKYHIGH SWG?

Now, let's look at some of the ways in which Skyhigh SWG helps you take your web security a step further. Get deeper visibility, control, and build more powerful policies with the intelligent web security that is built for the cloud.

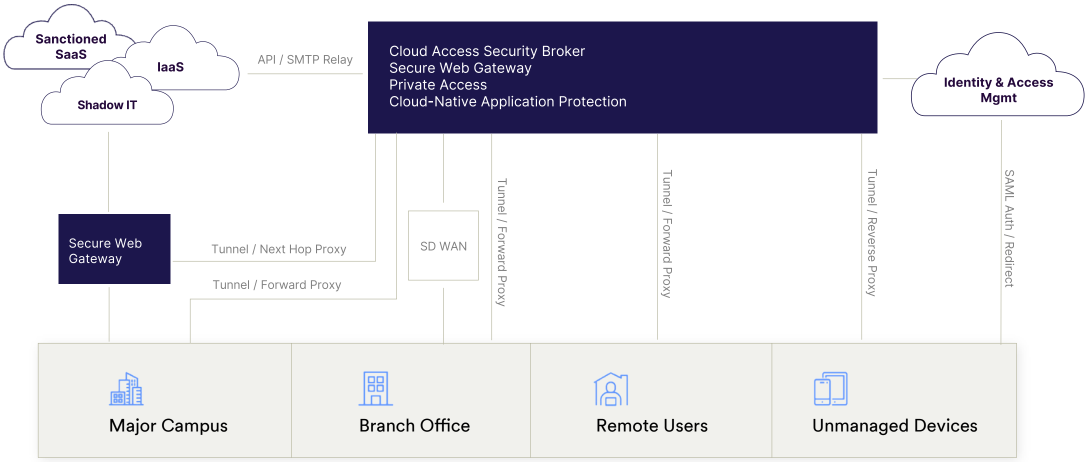
- Apply tenant restrictions to differentiate between personal and enterprise accounts for sanctioned services
- Support activity control for all the cloud applications in our cloud registry (40,000+)
- Native DLP scanning that prevents sensitive data from being sent to an application
- Deeper visibility and reporting into information such as what applications were accessed, how many requests were made, how much data was uploaded and downloaded
- Greater control over what types of files can be downloaded and uploaded from and to specific sites
- Built-in Gateway Anti-Malware (GAM) provides real-time malware capabilities for zero-day attacks
- Inline RBI for Risky Web is included, requiring no additional solution for this additional level of protection

Learn more about Skyhigh SWG.

Is SWG just too difficult to deploy?

While organizations have much more to consider when deploying SWG solutions than DNS security, the market has come a long way toward simplifying the approach of this technology. The days of racking and stacking servers in datacenters across the world are behind us as SWG vendors do the legwork for you. SWG solutions are delivered using cloud-native infrastructures offering a global footprint with performance and reliability rivaling what even the largest organizations would likely achieve. No more do network and security teams have to find ways to backhaul traffic from smaller sites to a central place for filtering as site-to-site VPN capabilities allow the direct use of the SWG vendor's infrastructure. Remote users, likewise, no longer have to rely on VPN for their protection as they have intelligent agents to ensure their traffic is protected using on-premise or cloud assets where appropriate.

SSE architecture

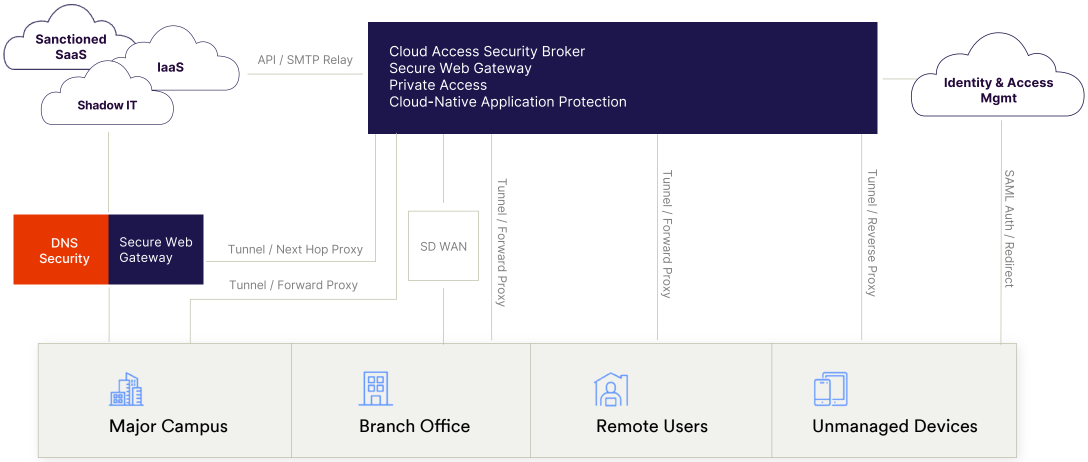


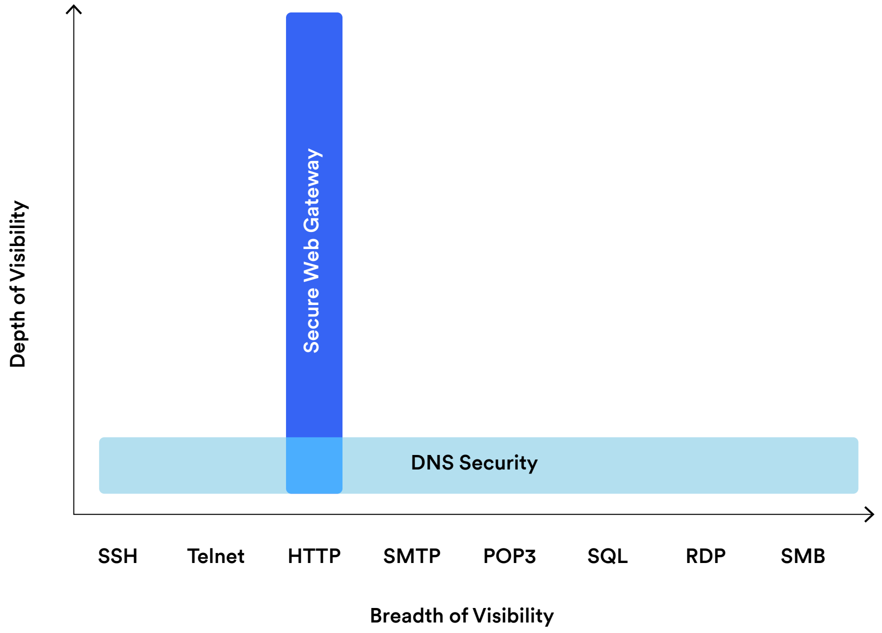
SWG technology has dramatically simplified web security policy in addition to infrastructure. Gone are the days of defining lists of URLs or IP ranges that need to be outright allowed or blocked. Web policy has been up-leveled to think at the cloud application level rather than the domain, and at the activity level rather than the URL. Out-of-the-box policies exist allowing security teams to achieve all of the common desired outcomes in minutes without having to choose between settling for rudimentary control or boil the ocean with byzantine configurations.

A best of both worlds approach

You may be thinking, “If only I could have the best of both worlds.” In a very real sense, you can. Despite many people’s perception, SWG and DNS security technologies are not competing but complementary solutions. If you consider the two offerings strictly from a visibility point of view you’ll find the overlap is fairly minimal. DNS security can be described as a mile wide and an inch deep. The breadth of visibility is clear as all ports and protocols are covered, but there is little depth as you’re working solely with a domain name. SWG, on the other hand, is a mile deep and an inch wide. Generally, a small set of critical protocols are supported, but inspection goes to the deepest levels of web traffic. Each solution’s strength overlaps the weakness of the other. Imagine yourself as a CISO of a mid-sized organization just starting to tackle the problem of security. If you’re starting from scratch, you might start with DNS security as a “quick win” and then advance to a SWG solution to achieve true web security.

General DNS and SSE architecture





To bring it all home, DNS security alone does not constitute true web security. There are simply too many gaps in visibility rendering security and reporting insufficient. There is no malware scanning of content downloaded or data security for content uploaded. Almost no context exists to answer questions about what actually happened between this domain and your endpoints. SWG technology, on the other hand, has advanced throughout the decades to achieve the security goals of the world's largest organizations despite the complexity of a cloud-first world. Deep inspection of all web traffic employs powerful anti-malware and data security technologies to ensure that information and endpoint assets are protected against a variety of threats. Reporting visibility offers rich detail and context into all interaction with cloud-based applications. And, despite the urge to compare the two and choose the superior solution, they pair nicely to offer a best of both worlds approach to secure any organization from the threats of today.

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

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