Cisco Umbrella

WHITE PAPER

The Rise of the Secure Internet Gateway

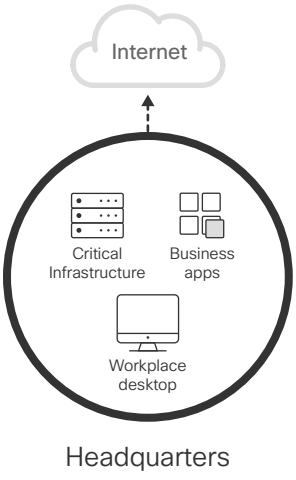
How the world works today: Users have left the building, apps are in the cloud, and security is left behind.

Ed is working from a plane, Emily just uploaded that strategy deck to Box, and you're not exactly sure where Phil is, but you know he's working based on the number of emails you've received from him. Today, this is how the world works. Before, everything was contained within your network perimeter – all of your critical infrastructure, servers, applications, data, and people. (Ah, remember the days of desktop computers?) Branch offices used to backhaul all traffic to corporate, so you could easily extend the scope of your network perimeter. Naturally, your approach to security was different, because the way people worked was different.

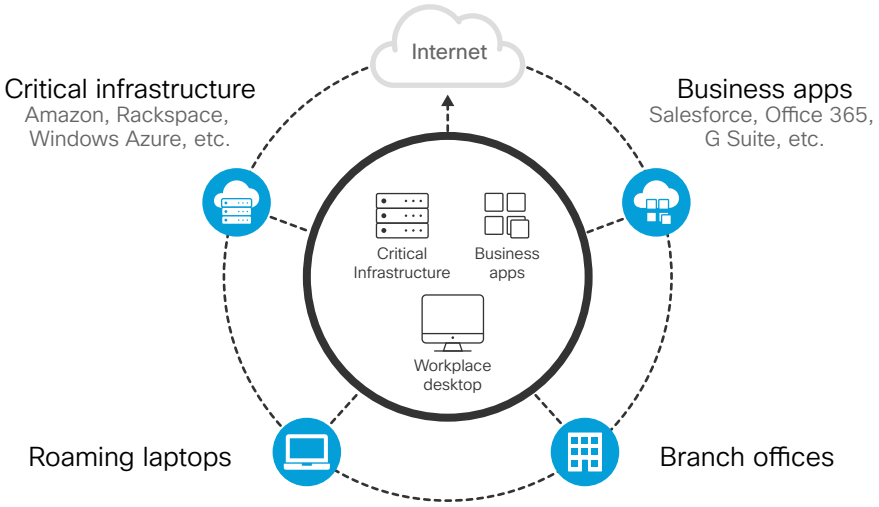
Security used to be more about building a taller wall around your perimeter and checking off boxes for compliance and HR acceptable use policies, instead of defending the business against data breaches and advanced attacks. Most security products were built as closed systems that couldn't integrate together or share intelligence.

82 percent of corporate laptop users admitted to sometimes bypassing their organizations' VPNs.[1]

How IT was built:



IT today:



The IT landscape has evolved. Critical infrastructure, applications, and data are moving to the cloud, leveraging either public or private cloud infrastructure. Salesforce.com, Box, G Suite, Office 365, and other software-as-a-service (SaaS) apps, whether sanctioned by IT or not, are commonplace in companies of all sizes and industries – even the most highly regulated ones. Not only does this raise questions about how to protect where sensitive data is going and how it's being used, but it also changes how employees get their work done.

Your users, especially when working outside of the office, no longer need to always connect to the corporate network to get work done. They often connect directly to SaaS apps. And, let's face it, employees also don't turn on the VPN if they're using their work laptop for personal use – which means they're left with very little security protection.

Plus, many organizations are now using direct internet connections at branch offices, which means employees and guest users don't get the protection of your traditional security stack. Not only are more offices connecting directly to the internet – it's estimated that 70% of branch offices already have some direct internet access[2] – but attackers recognize these weak points in their targets and have started exploiting them more.

To solve these new challenges, security controls must also shift to the cloud. This paper describes how security must evolve to protect users anywhere they access the internet, why traditional secure web gateway (SWG) solutions cannot address these gaps, and why a new kind of internet gateway represents an entirely new way of thinking about securing your users.

Looking back: Secure Web Gateways were originally built to control, not secure users and data.

SWGs are often used as one way to protect users against threats online. But, is that what they were really built to do? Think back a couple of decades to a time when bandwidth was expensive and there was a concern about employee productivity online. To offset these challenges, web proxy technology was born. Web gateways were designed to control web traffic as a way to manage bandwidth consumption, and they controlled access to inappropriate sites to help you manage productivity. Sure, it required a lot of maintenance and exceptions to work around some problematic web apps and sites, but it seemed worth it back then.

Later, companies became increasingly concerned about users going to malicious sites and their sensitive data leaking on the web. In response to these liability and breach risks, SWG vendors strengthened content filtering and added data loss prevention capabilities to better analyze all web traffic and better control its movement. Since they are typically built on a proxy architecture, SWGs are able to analyze web content and determine if a site presents a security risk.

Use case priorities have flipped

Today, the priorities for security teams have flipped. Threat protection is now the highest priority because the financial impact of data theft and loss greatly outweighs any productivity or bandwidth loss. And while employees are still unproductive at times, technology is often not the right solution. After all, how do you prevent someone from playing games on their personal phone? And you probably don't care what they surf or how much they stream when off the network, just as long as they don't get infected or phished, right? When you consider how IT has changed, SWGs were not architected to provide the capabilities needed to address the security risks of today.

While web proxy functionality is necessary to inspect HTTP/S traffic, SWG solutions are often complex to deploy, appliance-based, and closed, siloed platforms that mainly protect users when they are on the corporate network or connected via VPN. Although most now offer a cloud or hybrid delivery model, it increases the complexity for administrators. And shifting the same SWG technology into the cloud won't magically resolve all its maintenance burdens. Plus, it still only gives insight into web-based threats over ports 80 and 443 – leaving you blind to command and control (C2) callbacks that use other ports and protocols to exfiltrate or encrypt data.[3]

The rules of the game aren't working any more – it's time to change the game. We need to reimagine how security can be delivered so it better protects users for the way they work today – and the way they will work in the future. That is the key driver behind a new kind of cloud security platform called the secure internet gateway.

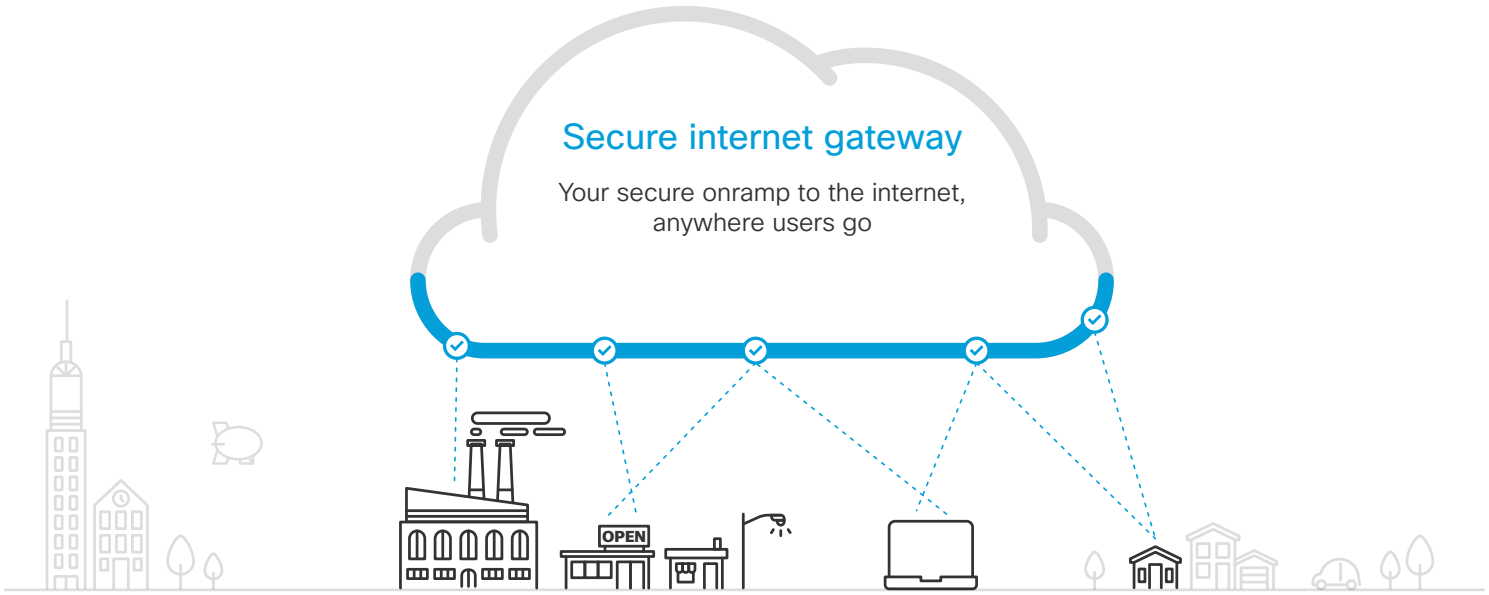
15% of malware C2 callbacks use ports other than 80/433 to communicate with attacker infrastructure to exfiltrate or encrypt data.[3]

Looking forward: Security must move to the cloud to fully protect data, apps, and users – wherever they go.

A secure internet gateway (SIG) provides safe access to the internet anywhere users go, even when they are off the VPN. Think of it as your secure onramp to the internet. Before you connect to any destination, a SIG provides the first line of defense and inspection. Regardless of where users are located or what they're trying to connect to, traffic goes through the internet gateway first. Once traffic gets to the SIG platform, there are different types of inspection and policy enforcement that can happen. Here are the capabilities that define a SIG today:

- Visibility and enforcement on and off the corporate network, even when users are off the VPN and without backhauling all traffic to the corporate network
- Protection against threats over all ports and protocols
- Proxy-based inspection of web traffic and file inspection with AV engines and behavioral sandboxing
- Live threat intelligence derived from global internet activity analyzed in real-time, with updates enforced everywhere within minutes
- Open platform with a bidirectional API to integrate with your existing security stack (including security appliances, intelligence platforms/ feeds, CASB, etc.) and to extend protection everywhere
- Discovery and control of SaaS applications

As more security controls move to the cloud, a SIG provides a platform that future capabilities can be built upon. Let's take a deep dive into each of these capabilities.

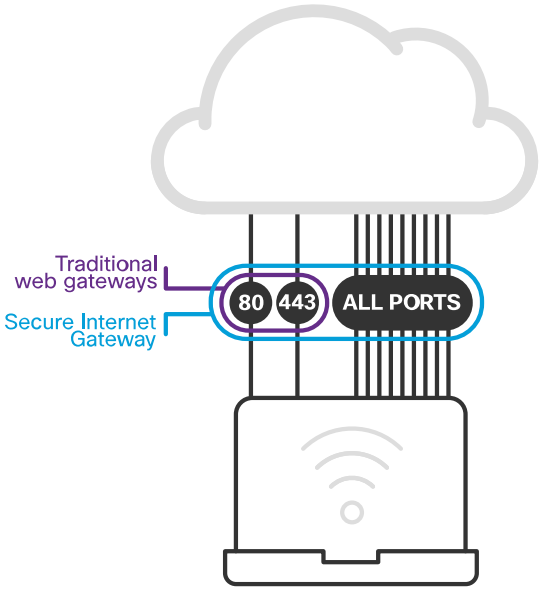


Visibility and enforcement on and off the corporate network, for all ports and protocols

One of the core tenants of a SIG is visibility into all internet activity, anywhere users are located. If you can't see it, then you neither protect it, nor learn from it. A SIG must provide a comprehensive, yet simple way to get all traffic to the cloud platform for analysis. And it should be done without requiring complex deployments. Many IT teams don't even realize how complex setting up always-on VPNs, full GRE or IPSec tunnels, and custom PAC files have been all these years — until they realize that there's a different, far simpler way: leveraging the Domain Name System (DNS).

In fact, 91% of malware uses DNS to carry out campaigns.[4]

DNS is a foundational component of how the internet works — when you click a link or type a URL, a DNS request initiates the process of connecting to the internet. Similar to how you look in your address book for your colleagues' phone numbers, DNS was first developed to map domain names to IP addresses. DNS is used by every device — including laptops, servers, mobile phones, and Internet of Things (IoT) devices — as the first step in nearly every internet connection. DNS is also used by malware. In fact, 91% of all command and control callbacks use DNS.[4] The one exception is when a device autonomously connects directly to an IP address instead, and a SIG should be able to cover those scenarios too. By using DNS, you can stop threats over all ports and protocols — not just web ports 80 and 443 like a SWG.

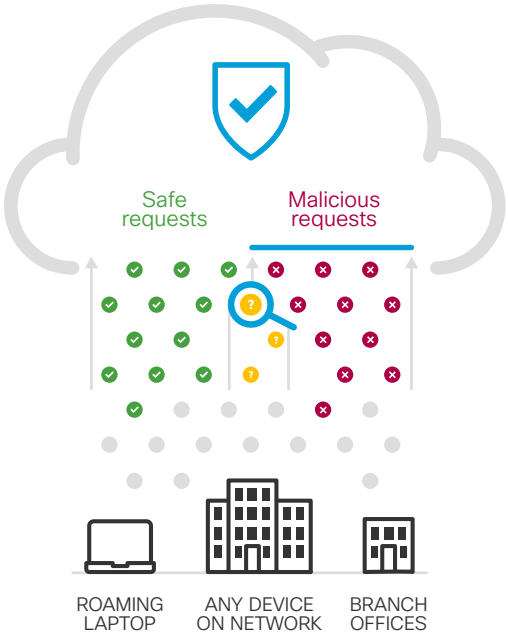


The DNS request becomes the very first point at which a SIG can enforce security, by determining whether the domain or IP is legitimate or malicious. Some domains may require additional inspection, which is why a SIG must also include a way to more deeply inspect web traffic.

Proxy-based inspection of web traffic

An internet gateway needs a cloud-delivered proxy to be able to inspect web traffic, especially when the domain has a risky reputation or includes both legitimate and malicious content. But the proxy should be reimagined from the way it was originally developed for the web gateway.

First, a proxy should not just be bolted onto the network or within the cloud like a cheap aftermarket accessory. Instead, the proxy technology should be built into the cloud in a way that's seamless from a management and user experience perspective. Even though SWG vendors will claim their proxy is "transparent" to end users, it's misleading because many sites and apps break when sent through a proxy — Office 365 for instance. Plus, there are many geo-localized content problems — your branch office in Mexico cannot get Google Search results in Spanish because the traffic is proxied through a data center located in Texas.



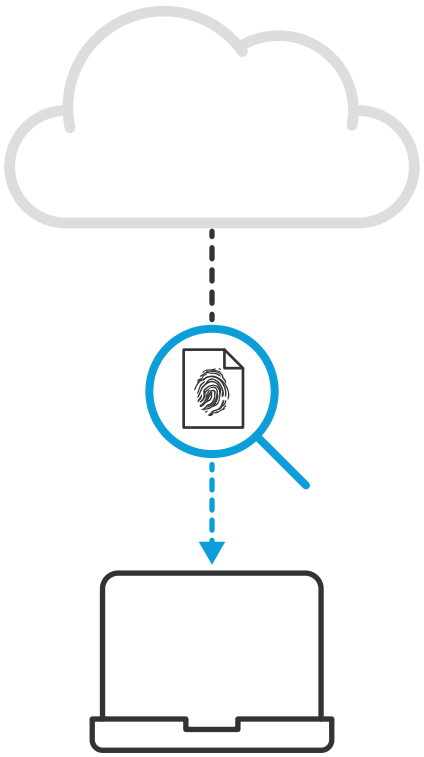
Not all web traffic should be forced to be inspected through a proxy — that adds unnecessary complexity and latency for end users. For instance, why proxy a safe content carrying domain for Netflix? And why proxy domains that are already known to be malicious, when they can be blocked earlier at the DNS layer? Instead, a proxy can intelligently inspect domains that are risky. For instance, sites such as Reddit.com which allow users to upload and share content, which makes them difficult to police.

The proxy should also be built using the latest technology, such as a microservices architecture. By taking a multitenant, container-based approach, any service provided on the proxy is completely detached from any other service, which enables automatic scaling in the event that one service requires more processing power. By automatically providing more capacity for that function, it results in more effective performance for the proxy.

File inspection with AV engines and behavioral sandboxing

The proxy should also offer the ability to inspect files with antivirus (AV) engines and behavioral sandboxing. When analyzing files, an internet gateway must be able to check the file hash against multiple AV engines and other advanced malware protection solutions. And, what's most important are the sources of the file intelligence. The bigger the database of known files that you can check against and the broader the sources of the files, the better.

For example, imagine if the database of file hashes that you were checking against included analysis of files from the following sources:



- Files attached to 35% of worldwide email traffic (after all, email is the number one attack vector, so it's vital to have the broadest view possible)
- Samples from more than 150 million+ endpoints
- Samples from 1.6 million global network sensors

And for files that are unknown, behavioral sandboxing technologies should be integrated in order to detonate the file offline for static and dynamic analysis. That way, even if a file is downloaded initially, your security team can learn within minutes if the file is actually malicious and take immediate action to remediate. Again, the strength of the sandboxing technology also comes from the number of samples it analyzes (i.e. tens of millions of samples per month) and the overall intelligence it correlates that analysis against.

Another important capability is retrospective analysis of files. Let's say at the time of analysis, a file is determined to be safe, but a short time later it's actually determined to be malicious. A SIG should have the ability to retrospectively flag that activity for your security team so you can take action.

Live threat intelligence

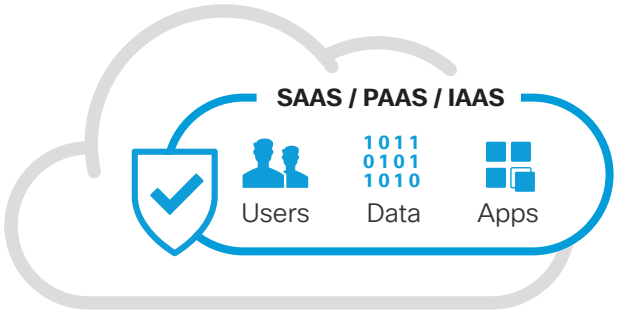
One of the most important aspects of any security solution is the threat intelligence behind it. The difference between a SIG and any other security product is the fact that it was born on the internet – giving it unique insight into internet activity patterns from users and the ability to actually uncover where attackers are staging infrastructure on the internet for future attacks. Because it's delivered from the cloud, a SIG has the horsepower to process billions upon billions of requests globally and uncover threats in real time.

Not only does a SIG provide enforcement based on this intelligence, but it should also provide a way for security teams to access this rich source of intelligence and be able to enrich events in other security systems (SIEM, threat intelligence platform, etc.), too. A SIG should not be a black box of intelligence, but rather a platform that exposes intelligence details that can be used across other systems in your environment.

Open platform

Security products shouldn't be built as closed platforms that create silos for your security team to manage. A secure internet gateway should be built as an open platform that integrates and shares intelligence with other systems. One of the biggest benefits of a SIG is the ability to protect users anywhere they go. By providing a bidirectional API, a SIG has the ability to integrate with security appliances that you have on-prem and extend protection beyond the perimeter. This means that you can amplify the investments that you've made defending your perimeter and extend the protection, and ultimately the value of those products. A SIG provides an added layer of protection that integrates seamlessly with the security investments you've made in the past, while providing an earlier line of defense against threats on the internet.

Discovery and control of SaaS applications



As applications and data move to the cloud, many organizations are looking to Cloud Access Security Brokers (CASB) to protect data usage in the cloud. A SIG should work together with a CASB to provide a more comprehensive view. For example, while a CASB solution helps control data usage for sanctioned apps using native APIs, a SIG logs or blocks access to unsanctioned SaaS apps using DNS, IP, and HTTP/S layer inspection. By working together, SIG and CASB solutions will give your organization the most complete view of sanctioned and unsanctioned app usage.

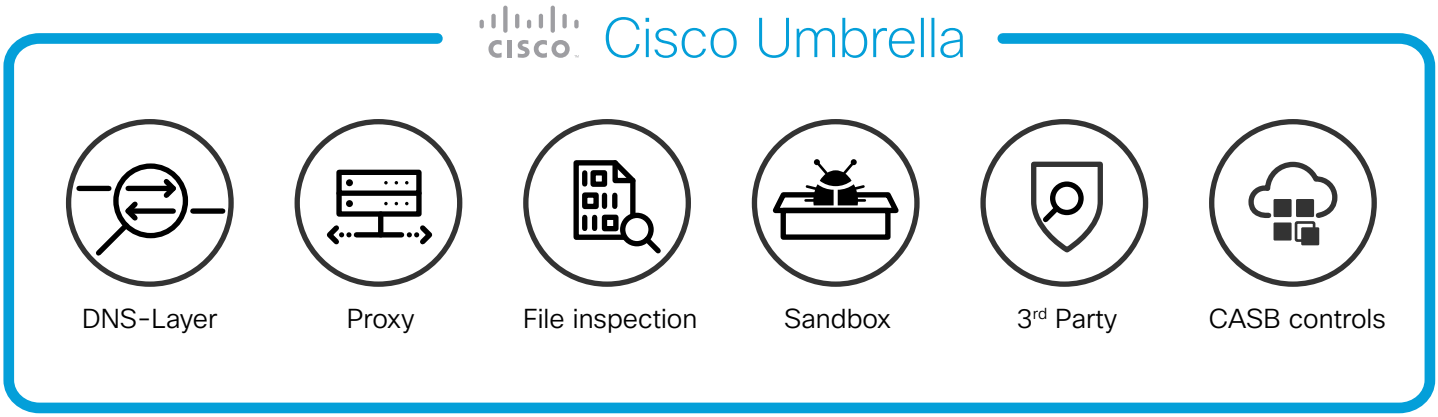
Additional considerations

As you explore secure internet gateway solutions, here are some additional considerations to think about:

- **Ease of deployment**: A SIG must be simple to deploy and you should be able to start protecting users enterprise-wide within minutes. When DNS is used as the main mechanism to send traffic to the cloud platform for analysis, deployment can be as easy as changing a configuration on your DNS or DHCP server to point traffic to the SIG. Out-of-the-box integrations with routers, wireless LAN controllers, or other network devices can also make deployment a breeze. And, for off-network support, integration with a VPN client (so no additional agents are required) or an optional lightweight agent to redirect DNS should be available.
- **Ongoing management:** As a cloud-delivered platform, a SIG should not require any hardware and should offer automatic updates for any software components. Ongoing operational management should be minimal.
- **Non-intrusive to end users:** A SIG is all about securing access to the internet, but it's imperative that it doesn't add any additional latency for end users. In fact, a SIG could actually improve connection speeds.
- **Fast and reliable cloud infrastructure:** A SIG should be built into the foundation of the internet on a cloud infrastructure that is 100% reliable for the most effective service and protection.
- **Future capabilities:** This is just the beginning of the secure internet gateway market. There are many more capabilities that can and should be built into this cloud platform. It's important to understand your vendor's future vision and plans.

Cisco's secure internet gateway – Cisco Umbrella

For more than 20 years, Cisco has provided best-in-class network security and endpoint offers, including next generation firewalls, next generation intrusion prevention systems, VPN clients, email security, and advanced malware protection. Cisco recognized the need to shift security controls to the cloud and acquired OpenDNS to serve as the foundation of its cloud security platform. Now, Cisco has introduced the industry's first secure internet gateway in the cloud, Cisco Umbrella. For more details on our technology, visit umbrella.cisco.com.



[1] http://cs.co/IDG-survey
[2] http://cs.co/Forrester-BranchOffices
[3] http://cs.co/lancope-c2-stat
[4] http://cs.co/dns-c2-stat

Cisco Umbrella