Cisco Umbrella

FEATURE BRIEF

The Cisco Umbrella intelligent proxy.

Sometimes securing your organization can feel like a lose-lose for everyone. Take web proxies, for example. They frustrate end users with slower speeds. And for security admins, you're only getting coverage for web ports 80 and 443 and maintaining a proxy can be a pain. With Cisco Umbrella's intelligent proxy, we're able to take the best of a proxy – visibility and control – and discard all the bad.

Umbrella is a cloud security platform that provides the first line of defense against threats on the internet. We use the Domain Name System (DNS) as the main mechanism to get traffic to our platform for analysis. Since DNS is a fundamental component of how the internet works and is used by all devices, that makes it an effective and comprehensive way to ensure you see all internet requests – and can stop threats over all ports and protocols.

While DNS is the first point of inspection, we also have a cloud-based web proxy for deeper inspection. But we set out to reimagine how a proxy should work.

First, let's look at how this was done in the past. A traditional web gateway will proxy all web connections – safe, malicious, and risky – negatively impacting your network performance and availability. And, deployments are often complex, requiring always-on VPNs, PAC files and GRE/IPsec tunnels. Umbrella's intelligent proxy only routes requests to risky domains, or sites containing both known safe and known malicious content, for deeper inspection. And it requires no additional deployment beyond pointing your DNS to Umbrella!

Destinations

Original destinations or blocked page

Security controls

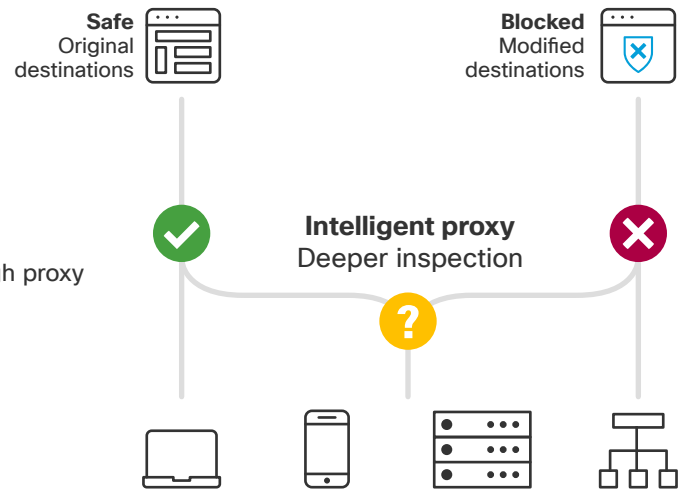
DNS and IP enforcement

Risky domain inspection through proxy

SSL/TLS decryption available

Internet traffic

On-and off-network



With the use of a smarter proxy, we avoid the need to proxy requests to domains that are already known to be safe or bad. Most phishing, malware, ransomware, and other threats are hosted on domains that are classified as malicious. Simple – we block those threats at the DNS layer, with no need to proxy. A domain that poses no threat – say a content-carrying domain for Netflix or YouTube? Umbrella will allow it, and again, no proxy required. Beautiful. Yet some domains are a little trickier - like domains associated with a web server or site that have the possibility of hosting malware. These can include sites that allow users to upload and share content such as Reddit or Pastebin – making them difficult to police. Obviously, if you allow all traffic to these risky domains, users might access malicious content, resulting in an infection or data leak. But if you block traffic, you can expect false positives, an increase in support inquiries, and thus, more headaches. By only proxying risky domains, the Umbrella intelligent proxy delivers more granular visibility and control.

Key Benefits

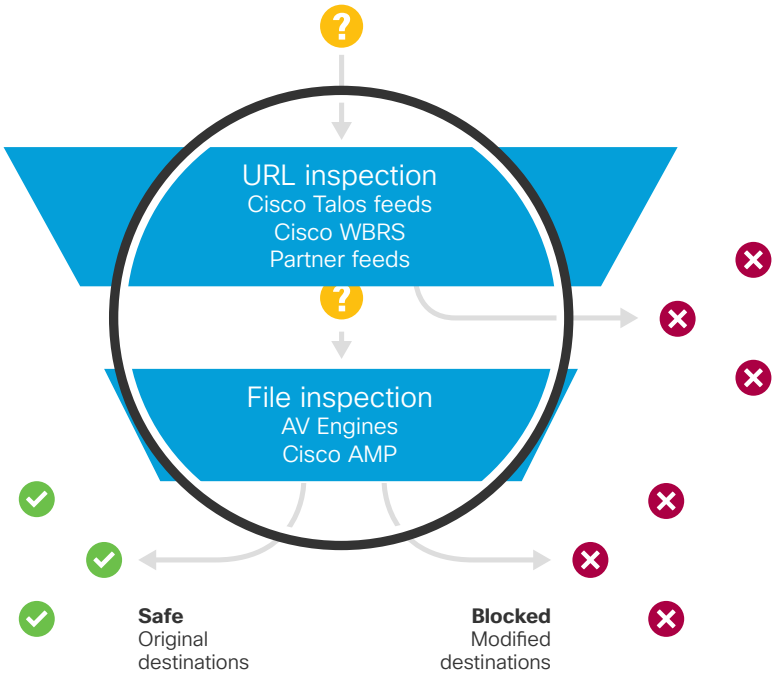
- Granular protection at the URL and file level
- Simpler configuration and management compared to traditional proxies
- Better performance for end users compared to traditional proxies
- Does not require any additional software or hardware
- Custom URL blocking
- All proxy activity is logged and available for viewing by the security team

What makes our proxy different?

The Umbrella intelligent proxy is built using a container-based microservices architecture. The proxy itself, and the services we integrate into the proxy, run and auto-scale independently from one another. For example, if our proxy notices a lot of files coming through for antivirus (AV) scanning, then it will automatically scale and provide more capacity for that function. This results in more effective performance for the Umbrella intelligent proxy.

Localized web content, such as a Google search, can experience issues when sent through a cloud-based proxy. This means a user in San Diego may be shown results in Spanish. By default, our proxy doesn't intercept this traffic. This means that your users receive accurate, localized content and services without the burden of creating a proxy exception.

How it works



In the case of a proxy disposition, we'll see the URL request and file hash at the HTTP/S layer.

The combination of Talos, Cisco web reputation systems, and partner feeds enforces millions of malicious URLs.

It then checks the file hash against a combination of partner AV engines and Cisco Advanced Malware Protection (AMP) – allowing you to benefit from 1.6 million global sensors that see 1.5 million incoming malware samples per day.

What does our proxy inspect?

Our proxy inspects URLs (e.g. https://umbrella.cisco.com/products/features) and over 150 different file types including Office documents, .PDFs, .ZIP files, and, executables that enter and exit the network by web ports 80 and 443 (HTTP/S traffic). To inspect URLs or files over HTTPS, the TLS/SSL traffic must be decrypted. Depending on your environment and needs, TLS/SSL decryption can be turned on or off using policies.