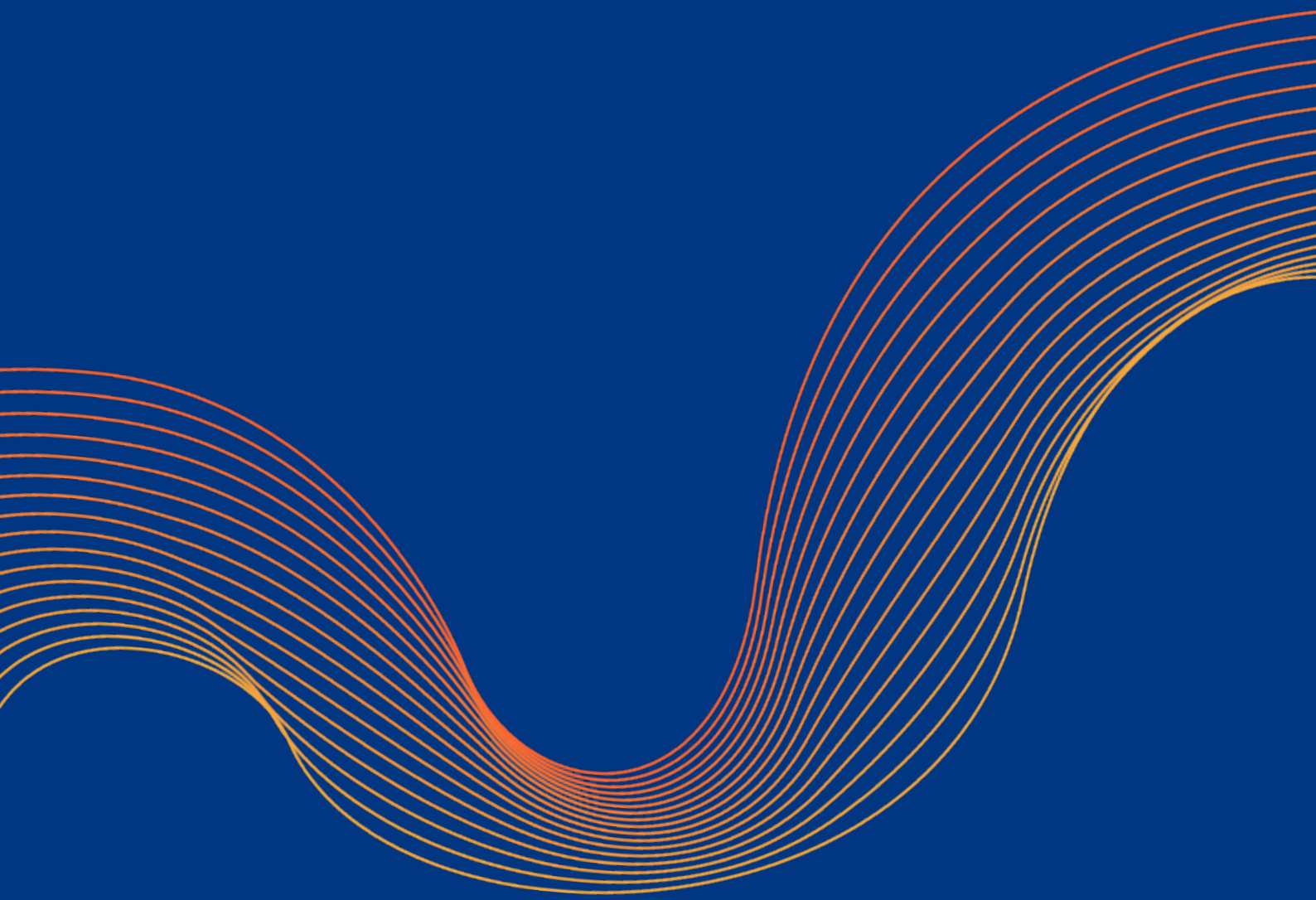
WHITE PAPER

CLOUDFLARE®

Cloudflare One Design Guide



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

INDEX

About this Guide 3

Secure Access for Web Applications 4

- Legacy Design - First Glance 5
- Legacy Design - Security Flaws 6
- Legacy Design - Required Security Add-ons 7
- Cloudflare One Design 8
- Diagram Comparison 9
- Table Comparison 10

DNS Filtering 11

- Legacy Design - First Glance 12
- Legacy Design - Operational Flaws 13
- Legacy Design - Required Network Modifications 14
- Cloudflare One Design 15
- Diagram Comparison 16
- Table Comparison 17

About this Guide

This design guide describes how organizations can simplify and strengthen their network and security architecture with Cloudflare One, our SASE platform. Cloudflare One combines network connectivity services with Zero Trust security services— all delivered on our global network. Unifying these networking and security services under one consistent, cloud-based architecture addresses many of the challenges of traditional, perimeter-based, on-premise deployments.

Each section of this design guide walks through a common technical use case — first, how that problem is typically solved with a legacy approach, and then, how Cloudflare One solves the same problem with greater efficiency and heightened security.

This guide covers the following use cases:

- Secure access for private and public web applications
- DNS filtering for on-prem and remote employees

These initial use cases were prioritized based on their popularity among customers, but they by no means represent the full scope of Cloudflare One's capabilities. We will continue to expand this guide with additional use cases, including secure access to private networks, advanced threat/data protection, and more.

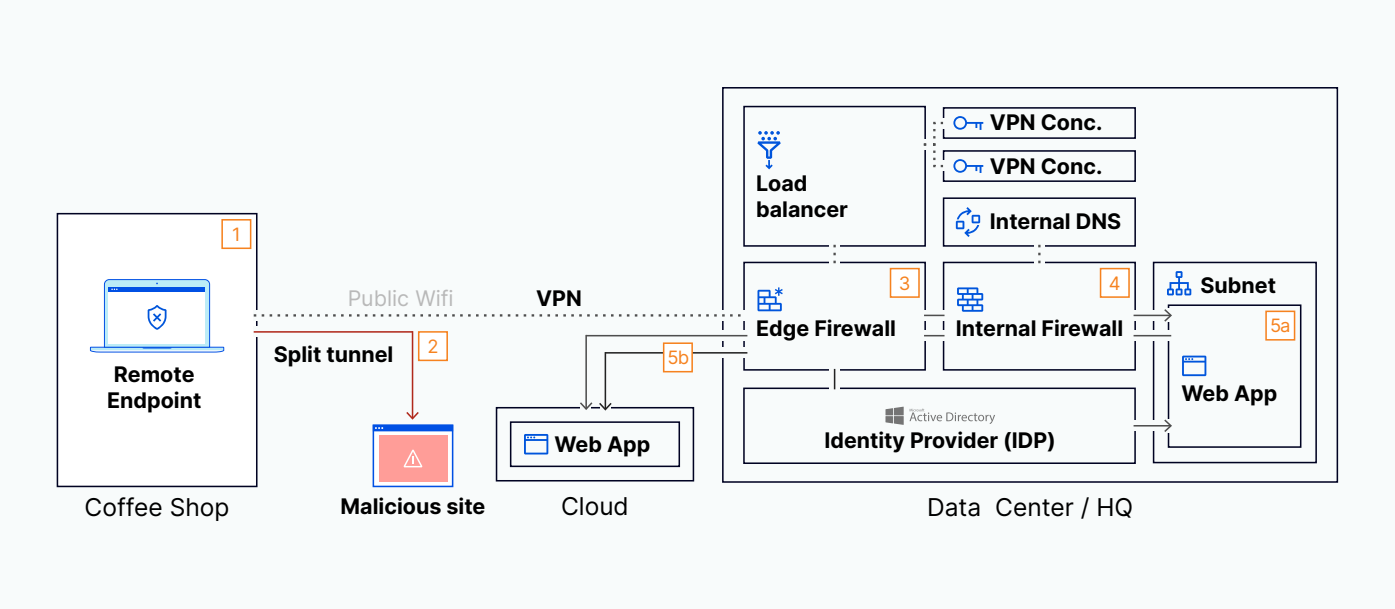
This design guide is intended for technically-minded practitioners to provide illustrative examples of how Cloudflare One, as a SASE platform, can be implemented to holistically transform and modernize an organization's network and security architecture.

Secure Access for Web Applications

Legacy Design - First Glance

This graphic represents a traditional method of providing remote access to web applications. Here, a remote employee accesses corporate resources, specifically both a private (self-hosted) and public (cloud-based) web application. We have included a few of the most common security measures any reasonable organization would have in place, including an edge firewall, an internal firewall for segmentation, and a VPN.

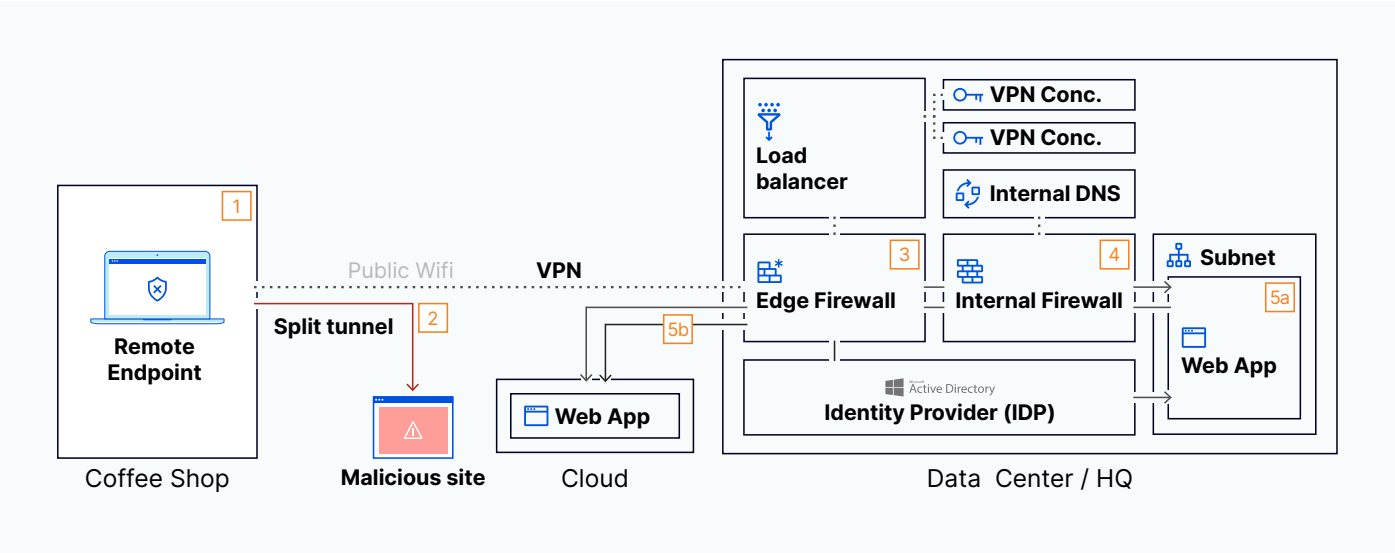
From left to right, this scenario illustrates the life of a session as a user logs in from a public location— a scenario that subsequent design graphics will build upon. **Note**: This graphic only depicts the devices, appliances, and traffic flows involved in this specific network transaction and does not represent a comprehensive snapshot of all technologies that would be present in a legacy network architecture.



	Network/Security Action
1	A remote device connects to corporate resources via public Wifi
2	The remote device reaches corporate edge via VPN client, but split tunnels other traffic
3	VPN terminates at Edge Firewall or VPN Concentrator behind firewall
4	Firewall policy grants remote user access to subnet with private web application
5	User accesses web app via private IP/URL [5a] or Public URL [5b] after authenticating to IDP

Legacy Design - Security Flaws

This graphic adds another column to the table below highlighting security flaws issues that are associated with each specific step in this scenario and that leave an organization vulnerable.

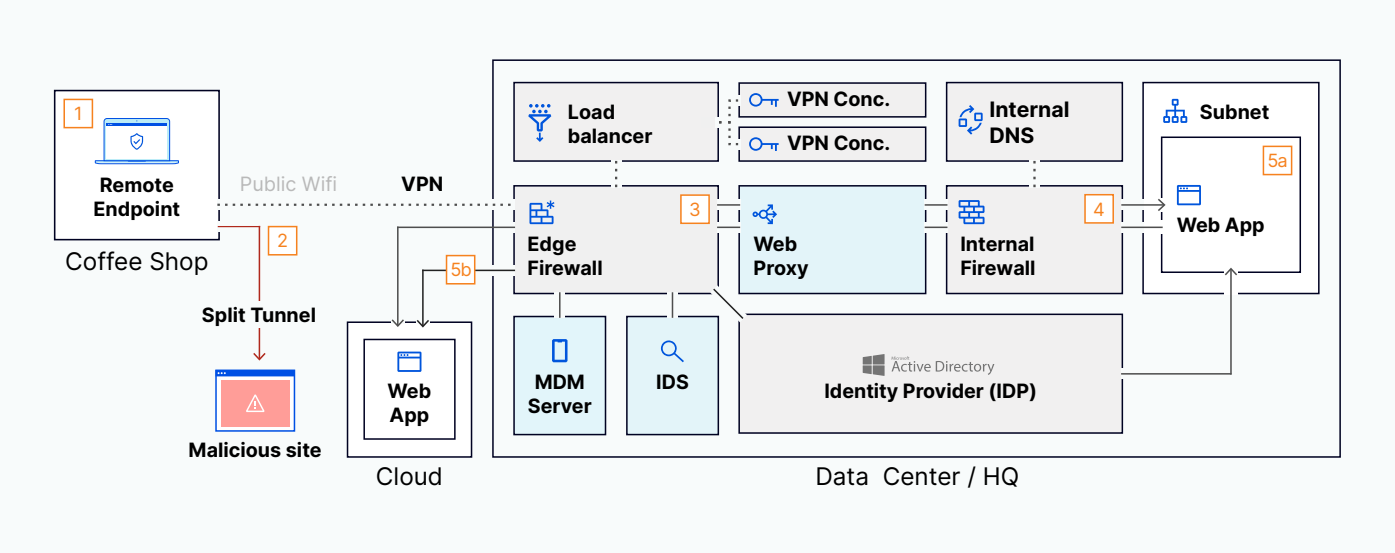


	Network/Security Action	Relevant Legacy Solution	Legacy Design Flaw
1	A remote device connects to corporate resources via public Wifi	Corporate VPN Client	An unsecured device on public wi-fi is a target for bad actors
2	The remote endpoint reaches corporate edge via VPN client, but split tunnels other traffic	Corporate VPN Client	VPN-specific security will not protect split-tunneled traffic
3	VPN terminates at Edge Firewall or VPN Concentrator behind firewall	Load balancer Edge Firewall VPN Concentrator	Inbound FW/VPN Rules may expose ports/ protocols to the internet, expanding potential attack surface
4	Firewall policy grants remote user access to subnet with private web application	Internal Firewall	The user has access to resources outside their job function
5	User accesses web app via private IP/URL **[5a]** or Public URL **[5b]** after authenticating to IDP	Active Directory Internal DNS (Private)	If the endpoint is compromised, company app/network is at risk

Legacy Design - Required Security Add-ons

To address the design flaws highlighted in the previous page, the organization now needs to modify their existing network architecture.This graphic adds another column to the table below, detailing typical solutions to protect users and resources.

Layering each security add-on adds complexity and ongoing management costs across likely multiple vendors to the legacy environment.

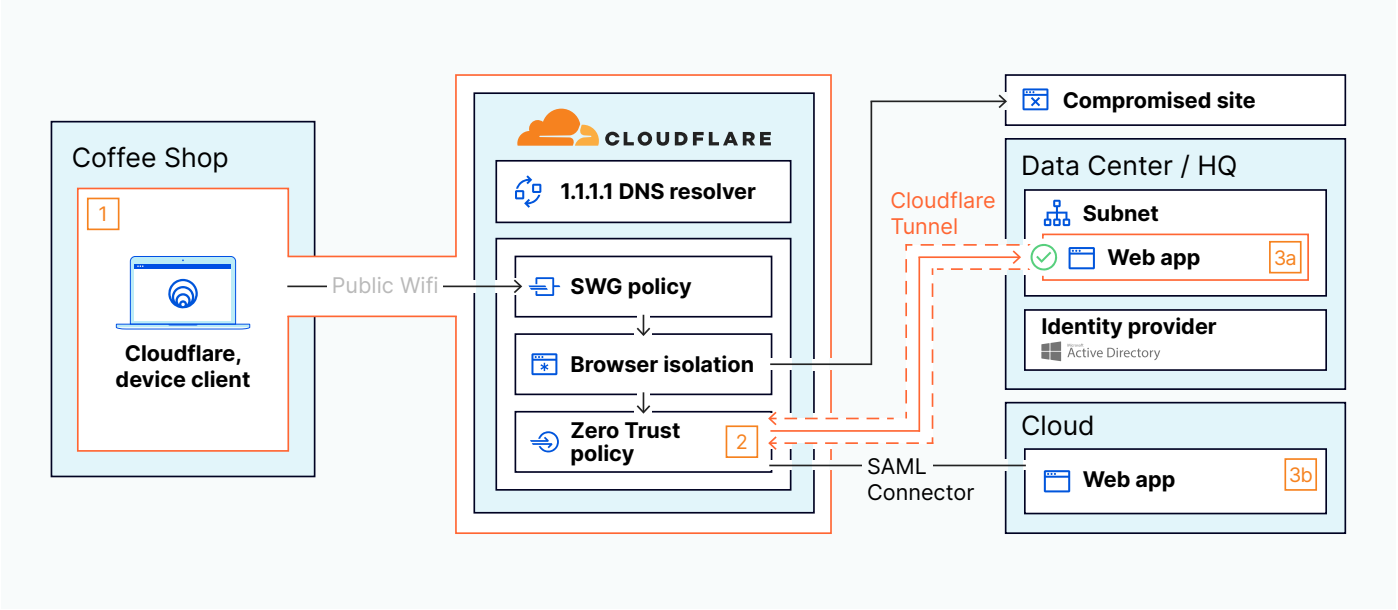


	Network/Security Action	Relevant Legacy Solution	Legacy Design Flaw	Required Security Add-on
1	A remote device connects to corporate resources via public Wifi	Corporate VPN Client	An unsecured device on public wi-fi is a target for bad actors	Endpoint Protection Platform (EPP)
2	The remote device reaches corporate edge via VPN client, but split tunnels other traffic	Corporate VPN Client	VPN-specific security will not protect split-tunneled traffic	Disable Split Tunnel
3	VPN terminates at Edge Firewall or VPN Concentrator behind firewall	Load balancer Edge Firewall VPN Concentrator	Inbound FW/VPN Rules may expose ports/protocols to the internet, expanding potential attack surface	Intrusion Detection System (IDS)
4	Firewall policy grants remote user access to subnet with private web application	Internal Firewall	The user has access to resources outside their job function	Web Proxy
5	User accesses web app via private IP/URL [5a] or Public URL [5b] after authenticating to IDP	Active Directory Internal DNS (Private)	If the endpoint is compromised, company app/network is at risk	Mobile Device Mgmt (MDM) Server

Cloudflare One Design

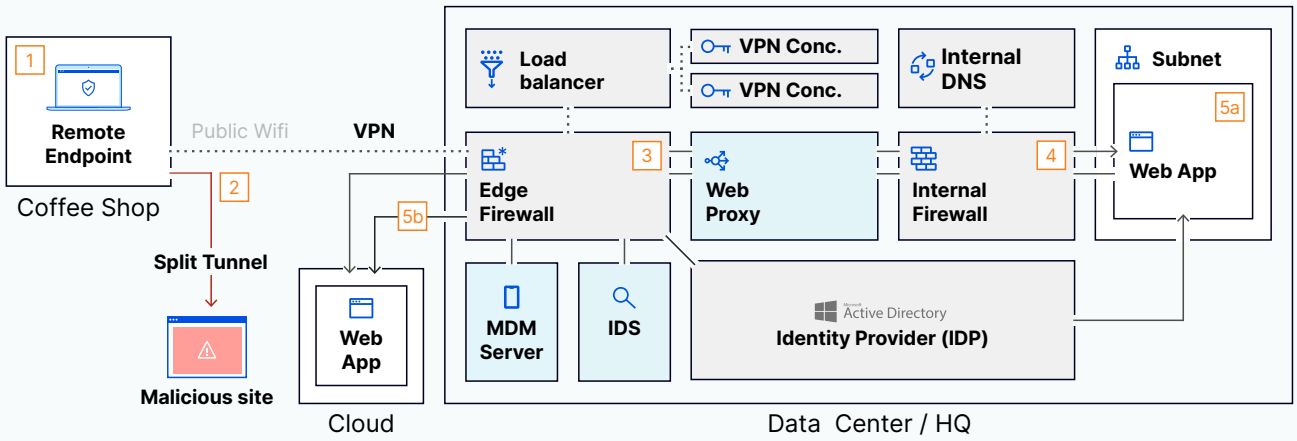
This below graphic highlights how an organization can adopt a simpler, more efficient approach to secure application access by implementing Cloudflare One.

Here, much of the legacy network architecture shown beforehand is offloaded to Cloudflare, and many of the existing design flaws are corrected without the need for additional solutions. With Cloudflare One, the traffic between the remote user and the organization's resources runs along Cloudflare's global network with single-pass inspection. All services shown below run in all of Cloudflare's data centers, located in 250+ cities in over 100 countries.

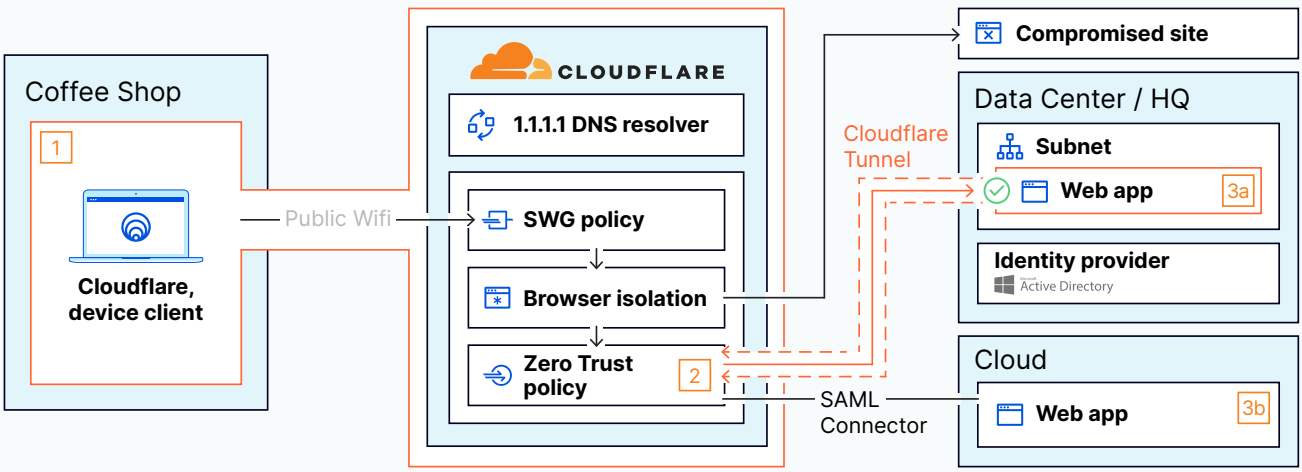


	Network/Security Action	Relevant Cloudflare One Element	Design Flaw Correction
1	A remote device connects to corporate resources and the internet via Cloudflare	Cloudflare Device Client Secure Web Gateway policy Browser Isolation	Local Secure Web Gateway client lets Cloudflare One filter DNS/HTTP/Network traffic to user's device via gateway policy Browser Isolation absorbs/isolates impact of successful malware attacks from websites
2	User undergoes IDP and device posture checks in Cloudflare	Zero Trust policy	Zero Trust policy performs device posture check before permitting access, mitigating risk of compromised devices Zero Trust policy authenticates user to the resource instead of the underlying network, preventing lateral movement
3	Access [Private | Public] web app directly via [Cloudflare Tunnel | SAML Connector]	Cloudflare Tunnel 1.1.1.1 DNS resolver	Cloudflare Tunnel securely brokers a connection to the web application and eliminates the use of explicit FW rules

Legacy Design - Required Security Add-ons



Cloudflare One Design



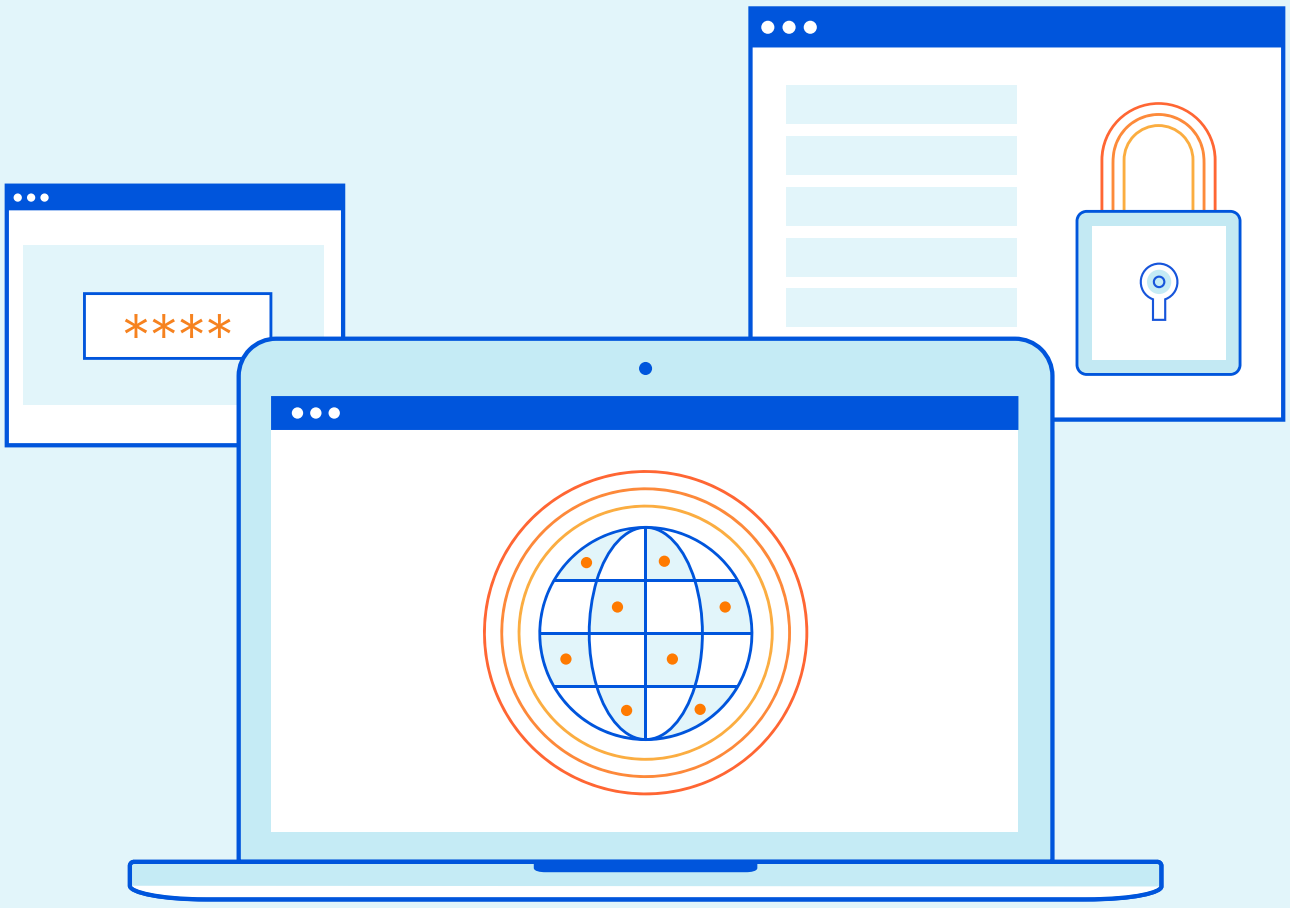
Legacy Design - Required Security Add-ons

	Network/Security Action	Relevant Legacy Solution	Legacy Design Flaw	Required Security Add-on
1	An remote device connects to corporate resources via public Wifi	Corporate VPN Client	An unsecured device on public wi-fi is a target for bad actors	Endpoint Protection Platform (EPP)
2	The remote device reaches corporate edge via VPN client, but split tunnels other traffic	Corporate VPN Client	VPN-specific security will not protect split-tunneled traffic	Disable Split Tunnel
3	VPN terminates at Edge Firewall or VPN Concentrator behind firewall	Load balancer Edge Firewall VPN Concentrator	Inbound FW/VPN Rules may expose ports/protocols to the internet, expanding potential attack surface	Intrusion Detection System (IDS)
4	Firewall policy grants remote user access to subnet with private web application	Internal Firewall	The user has access to resources outside their job function	Web Proxy
5	User accesses web app via private IP/URL **[5a]** or Public URL **[5b]** after authenticating to IDP	Active Directory Internal DNS (Private)	If the endpoint is compromised, company app/network is at risk	Mobile Device Mgmt (MDM) Server

Cloudflare One Design

	Network/Security Action	Relevant Cloudflare One Element	Design Flaw Correction
1	A remote device connects to corporate resources and the internet via Cloudflare	**Cloudflare Device Client** **Secure Web Gateway policy** **Browser Isolation**	Local Secure Web Gateway client lets Cloudflare One filter DNS/HTTP/Network traffic to user's device via gateway policy Browser Isolation absorbs/isolates impact of successful malware attacks from websites
2	User undergoes IDP and device posture checks in Cloudflare	**Zero Trust policy**	Zero Trust policy performs device posture check before permitting access, mitigating risk of compromised devices Zero Trust policy authenticates user to the resource instead of the underlying network, preventing lateral movement
3	Access [Private | Public] web app directly via [Cloudflare Tunnel | SAML Connector]	**Cloudflare Tunnel** **1.1.1.1 DNS resolver**	Cloudflare Tunnel securely brokers a connection to the web application and eliminates the use of explicit FW rules

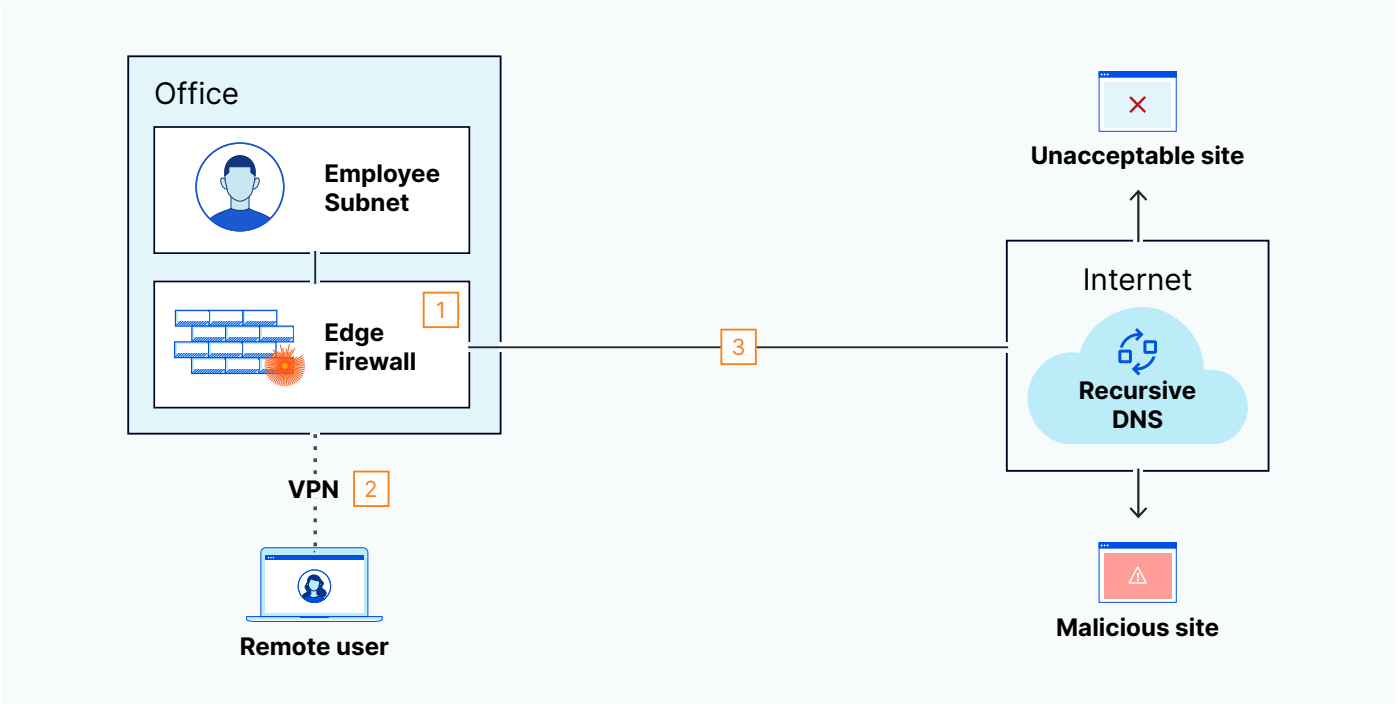
DNS Filtering



Legacy Design - First Glance

This graphic represents how organizations implement DNS filtering for onsite and remote employees in a legacy environment. Typically, DNS filtering for organizations is accomplished via built-in features of on-prem solutions like a firewall. Remote users send requests through this firewall by first backhauling traffic through a full-tunnel VPN. TTo resolve websites, the organization sends its DNS queries to a recursive DNS (like Google's 8.8.8.8).

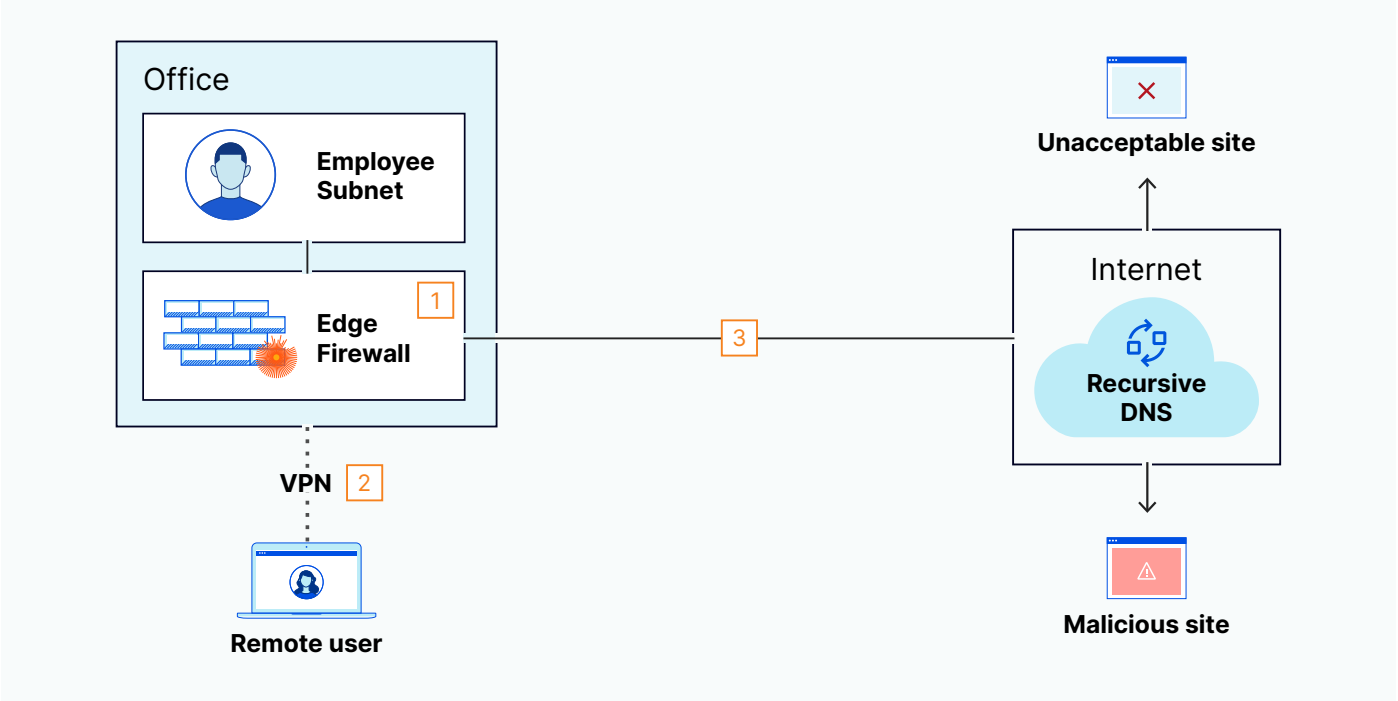
Note: Just as with other sections in this guide, this legacy environment does not represent every technology inside an office, but only the ones involved in this specific use case.



	DNS-Related Event
1	An onsite user has their DNS requests content filtered for security by the built-in feature on the Edge Firewall
2	A remote user has their DNS requests filtered after connecting to the organization's full tunnel VPN
3	Outbound DNS requests are transmitted in the clear.

Legacy Design - Operational Flaws

This next graphic adds a column to the table below articulating the challenges associated with this traditional design. The most pressing challenge is that relying on local hardware to perform DNS filtering at-scale will eventually bottleneck performance for all users,especially when that hardware is responsible for other critical services as well (such as terminating the remote-user VPN). In addition, sending DNS queries without encryption (which occurs by default) creates a new attack vector with unknown risk.

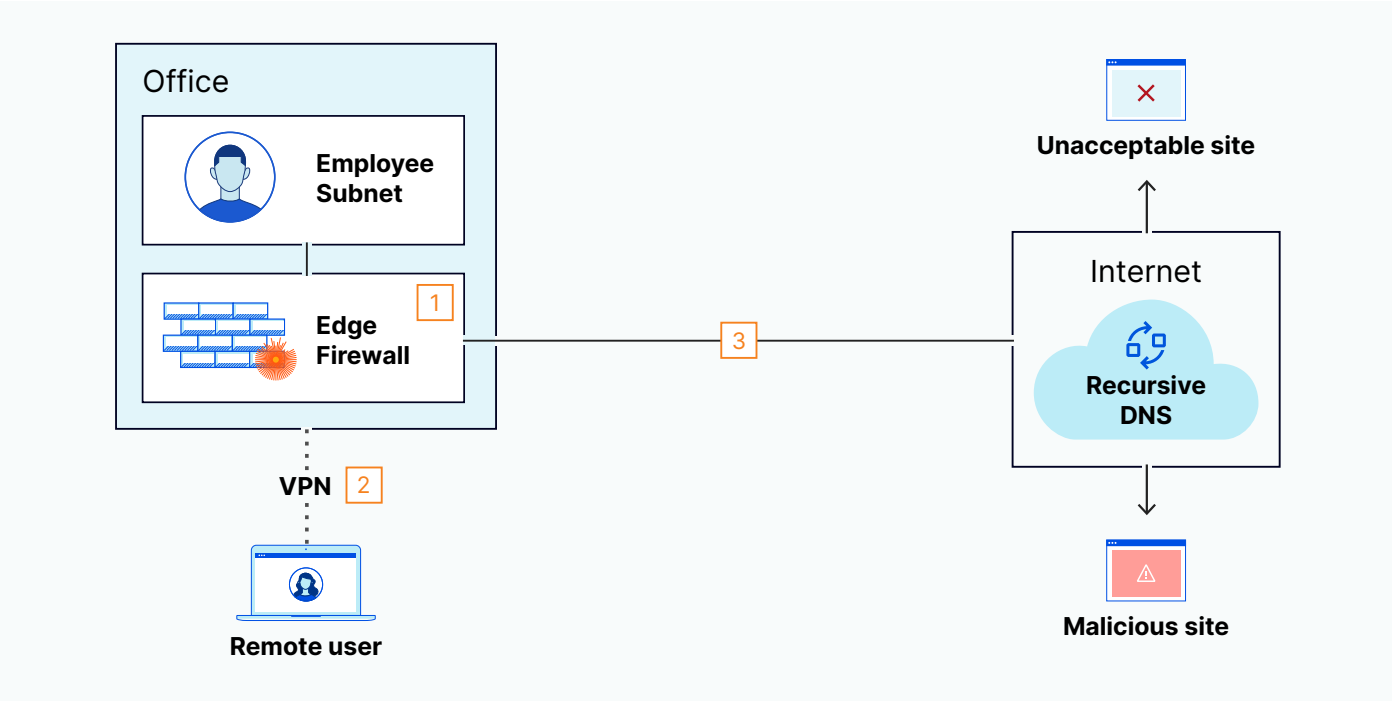


	DNS-Related Event	Relevant Elements	Design Flaw
1	An onsite user has their DNS requests content filtered for security by the built-in feature on the Edge Firewall	Edge Firewall	Relying on the Edge FW for too many essential operations can degrade performance across the organization
2	A remote user has their DNS requests filtered after connecting to the organization's full tunnel VPN	VPN Concentrator Edge Firewall	A full-tunnel VPN creates a 'double tax' of internet packets, which can create a performance bottleneck for the entire organization tunneled traffic
3	Outbound DNS requests are transmitted in the clear.	UDP53	DNS over UDP port 53 is unencrypted and therefore not private. Anyone who sees that can recon user web behavior

Legacy Design - Required Network Modifications

To address the design flaws highlighted in the previous page, the organization now needs to modify their existing network architecture. This graphic adds another column to the table below, highlighting common solutions with their own drawbacks. Here, buying new hardware to handle more users or increase bandwidth consumption will lead to higher capital and operational expenses over time.

Organizations that attempt to scale this approach themselves often encounter considerable growing pains, and in fact, many organizations avoid DNS filtering entirely because of these operational concerns.



	DNS-Related Event	Relevant Elements	Design Flaw	Non-Cloudfare Solution
1	An onsite user has their DNS requests content filtered for security by the built-in feature on the Edge Firewall	Edge Firewall	Relying on the Edge FW for too many essential operations can degrade performance across the organization	Discrete DNS Filter
2	A remote user has their DNS requests filtered after connecting to the organization's full tunnel VPN	VPN Concentrator Edge Firewall	A full-tunnel VPN creates a 'double tax' of internet packets, which can create a performance bottleneck for the entire organization tunneled traffic	Increase ISP bandwidth Hardware upgrade Enable Split Tunnel*
3	Outbound DNS requests are transmitted in the clear.	UDP53	DNS over UDP port 53 is unencrypted and therefore not private. Anyone who sees that can recon user web behavior	DNS over TLS/HTTPS

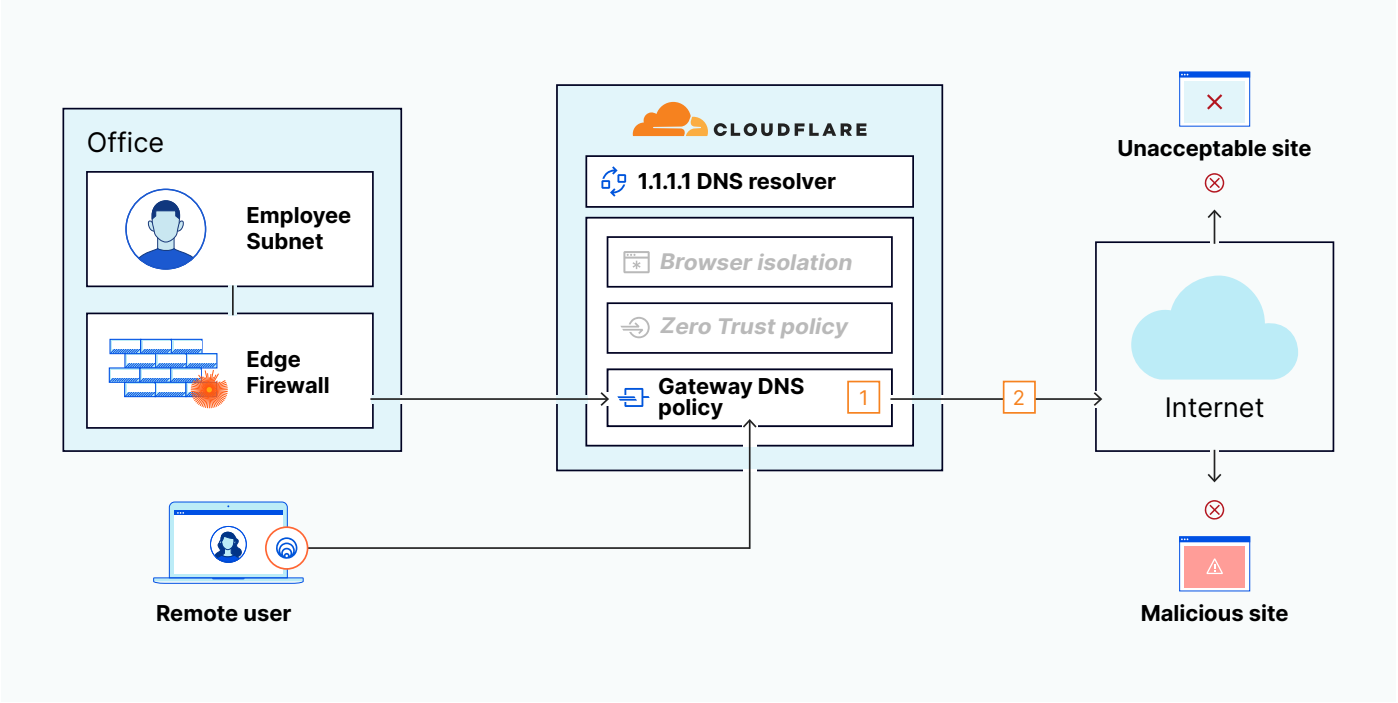
Cloudflare One Design

Organizations that adopt Cloudflare One point their traffic to Cloudflare's global network and can perform DNS filtering for the entire workforce without worrying about the operational limits of their local hardware.

Cloudflare's DNS filtered is easy to deploy for both on-prem and remote users:

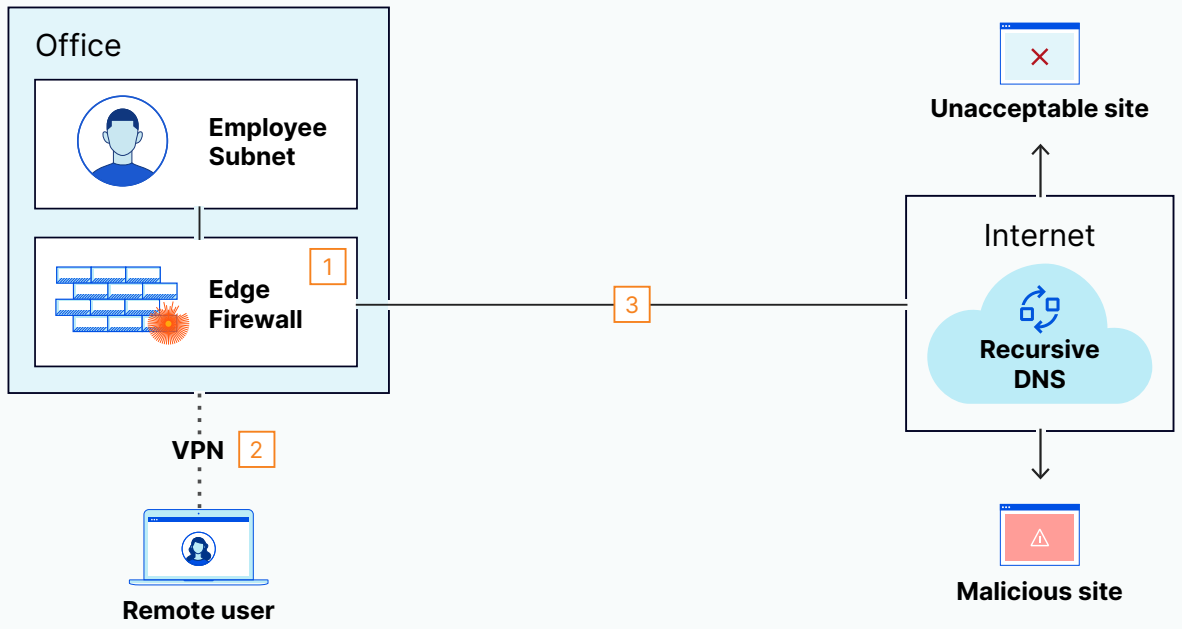
- Traffic from office users is sent to Cloudflare based on the outbound IP from the edge firewall
- Traffic from remote users is sent to Cloudflare from our device client

In addition, Cloudflare's 1.1.1.1 DNS resolver supports DNS over TLS/HTTPs, which resolves the security issue detailed in the legacy environment.

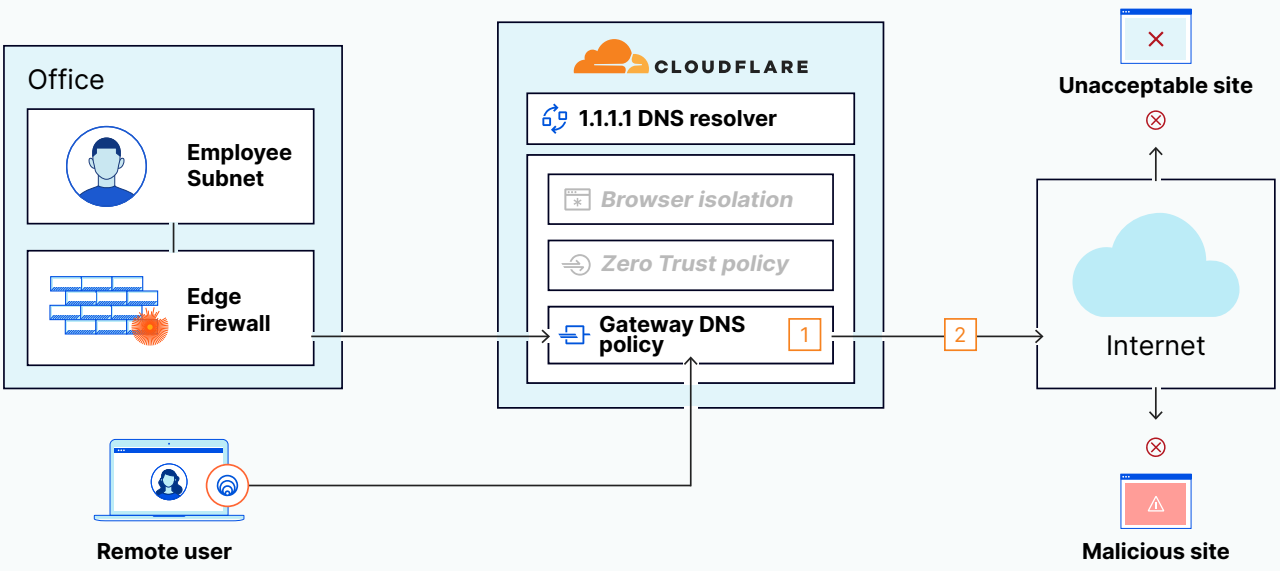


	DNS-Related Event	Relevant Cloudflare One Element	Design Flaw Correction
1	Both onsite and remote users have their DNS requests content filtered by Cloudflare	Secure Web Gateway	Gateway DNS policies offloads DNS filtering from local hardware (or provides it for the first time)
2	The organization's DNS requests are encrypted before being sent out.	1.1.1.1 DNS resolver	Cloudflare's 1.1.1.1 DNS resolver supports DNS over TLS/HTTPs, encrypting DNS requests and hindering hostile reconnaissance

Legacy Design



Cloudfare One Design



Legacy Design

	DNS-Related Event	Relevant Elements	Design Flaw	Non-Cloudfare Solution
1	An onsite user has their DNS requests content filtered for security by the built-in feature on the Edge Firewall	Edge Firewall	Relying on the Edge FW for too many essential operations can degrade performance across the organization	Discrete DNS Filter
2	A remote user has their DNS requests filtered after connecting to the organization's full tunnel VPN	VPN Concentrator Edge Firewall	A full-tunnel VPN creates a 'double tax' of internet packets, which can create a performance bottleneck for the entire organization tunneled traffic	Increase ISP bandwidth Hardware upgrade Enable Split Tunnel*
3	Outbound DNS requests are transmitted in the clear.	UDP53	DNS over UDP port 53 is unencrypted and therefore not private. Anyone who sees that can recon user web behavior	DNS over TLS/HTTPS

Cloudfare One Design

	DNS-Related Event	Relevant Cloudflare One Element	Design Flaw Correction
1	Both onsite and remote users have their DNS requests content filtered by Cloudflare	Secure Web Gateway	Gateway DNS policies offloads DNS filtering from local hardware (or provides it for the first time)
2	The organization's DNS requests are encrypted before being sent out.	1.1.1.1 DNS resolver	Cloudflare's 1.1.1.1 DNS resolver supports DNS over TLS/HTTPs, encrypting DNS requests and hindering hostile reconnaissance