Zscaler DNS Security and Control

Reference Architecture — Zscaler for Users

Contents

About Zscaler Reference Architectures Guides

The Zscaler™ Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who Is This Guide For?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A Note for Federal Cloud Customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler account team on feature availability and configuration requirements.

Conventions Used in This Guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding Out More

You can find our guides on the **Zscaler website** (**https://www.zscaler.com/resources/reference-architectures**).

You can join our user and partner community and get answers to your questions in the **Zenith Community** (**https://community.zscaler.com**).

Terms and Acronyms Used in This Guide

Acronym	Definition
C2	Command & Control
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DoH	DNS over HTTPS
DoT	DNS over TLS
ECS	EDNS Client Subnet
EDNS	Extension Mechanisms for DNS
FQDN	Fully Qualified Domain Name
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
GRE	Generic Routing Encapsulation
NAT	Network Address Translation
NRD	Newly Revived Domain
NROD	Newly Registered and Observed Domains
SSL	Secure Socket Layer (superseded by TLS)
TCP	Transport Control Protocol
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
URL	Universal Resource Locator
ZDX	Zscaler Digital Experience
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access
ZTE	Zero Trust Exchange
ZTR	Zscaler Trusted Resolver

Icons Used in This Guide

The following icons are used in the diagrams contained in this guide.

Zscaler Zero Trust Exchange


ZIA or ZPA Service Edge

Zscaler ZTR

Zscaler DNS Gateway

DNS

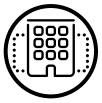

Zscaler Dedicated Load Balancer


Zscaler Policy


Laptop with Zscaler Client Connector Installed


Zscaler Client Connector on Phone


Generic Cloud Application or Workload


Headquarters Location

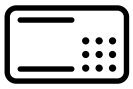

Legacy Firewall

User


User Laptop


Hacker Laptop


Infected Laptop


IoT Device


Zscaler Client Connector on IoT Device


Router


Internet


Data Tunnel

Introduction

The domain name system (DNS) is a core internet technology that works in the background of almost every request you make. DNS works to turn names for websites and applications into internet protocol (IP) addresses. Designed in the early years of the internet, DNS allows users to remember human-friendly names instead of a series of numbers and delineators. DNS is an open system of hierarchical naming and resolution that relies on distributed servers around the world.

The DNS system is used almost universally by user devices, network servers, IoT devices, cloud workloads, and SaaS applications to request the IP address for a fully qualified domain name (FQDN). An FQDN contains the host, domain, and top-level domain (TLD) for any internet resource. Using the website *www.safemarch.com* as an example:

.com	The top-level domain
safemarch	The apex domain for the organization
www	The target host

A device or service makes a DNS request in an attempt to resolve a resource's IP address, such as *www.safemarch.com*. This request is made to the configured DNS server for the device or service. Through a system of requests and redirects, that name is translated into an IP address, or the device is told the name cannot be resolved. This resolution functionality exists across all DNS servers including the Zscaler Trusted Resolver (ZTR) service.

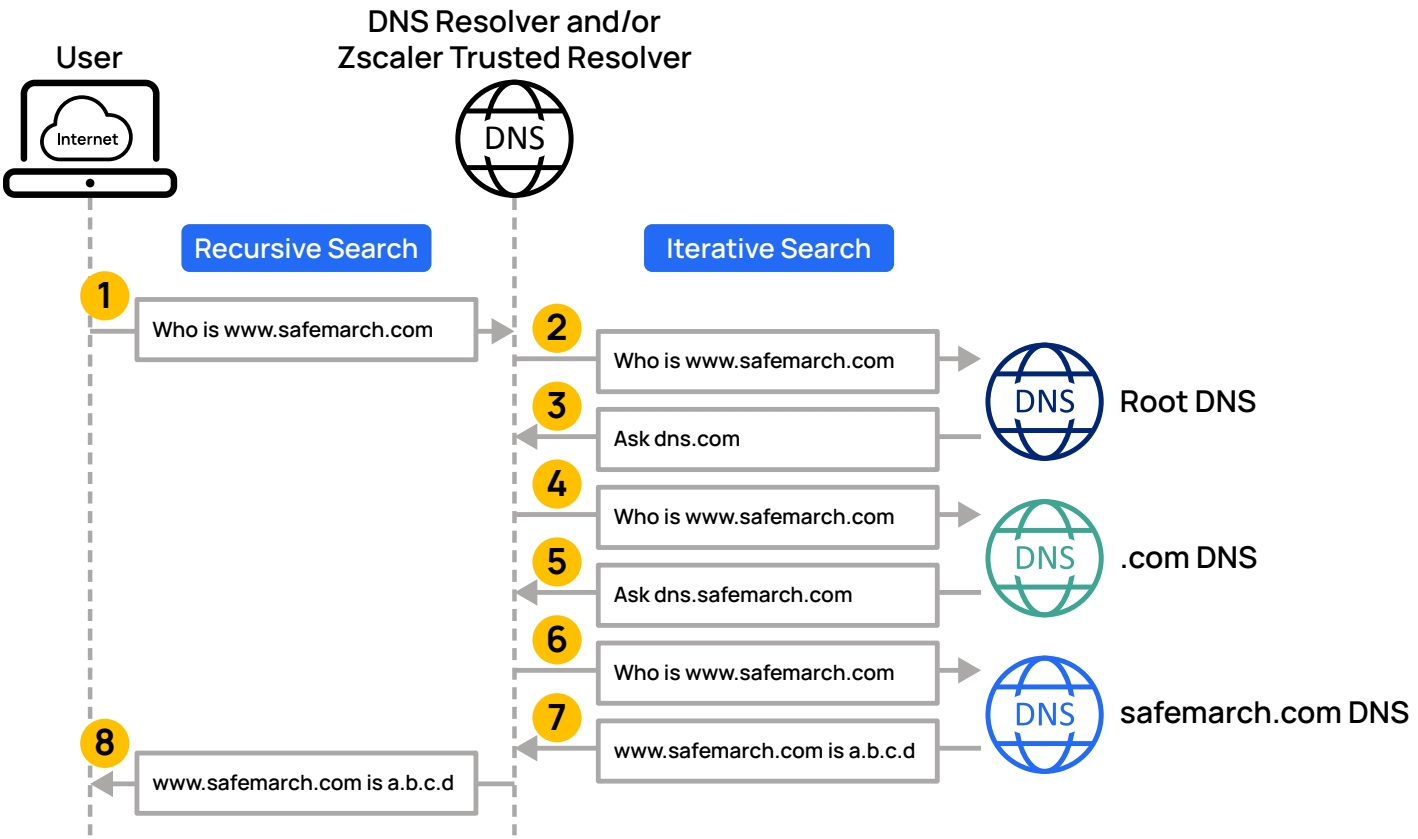


Figure 1. A user's request for an internet resource triggers a series of name lookups by servers until the resource's IP address is found

1. A device, workload, or application makes a request for *www.safemarch.com* from its configured local DNS resolver. This happens automatically when a browser or other network application needs to connect to a remote application or service.
2. The resolver first checks its cache to see if it has recently resolved that FQDN for another user. If the cache has a match, the resolver returns that information, saving a full lookup. The ZTR service caches any response for the time to live (TTL) value specified in the response. If the address is not in the DNS cache, the request is sent to one of 13 root name servers. ZTR also leverages DNS security (DNSSEC) where it authenticates responses to domain name lookups. Typically, the response is to contact another server.
3. In this case, the root DNS redirects to the server responsible for the top-level domain (TLD) .com in our example.
4. The resolver sends the same request to the .com DNS server.
5. The name server for .com won't have the address either, as that's specific to the domain owner. However, the .com DNS server knows who the DNS is for the domain safemarch.com and redirects the resolver to the authoritative server.
6. The resolver sends the same request to the safemarch.com DNS server, which is the authoritative server from the domain.
7. The authoritative server returns the IP address for *www.safemarch.com* to the resolver.
8. The resolver forwards the response to the user device. The ZTR service then stores the result in its cache for the length of the response until the TTL expires.

DNS name resolution is critical to the workings of the modern internet. With remote and hybrid work, you want to ensure your users are accessing appropriate and legitimate resources on the internet. You also want to make sure DNS is not making your network or application look bad by slowing down access. Slow DNS resolution and application access takes one of two forms: long resolution times by the DNS service, or using a DNS service that is too far away from the user.

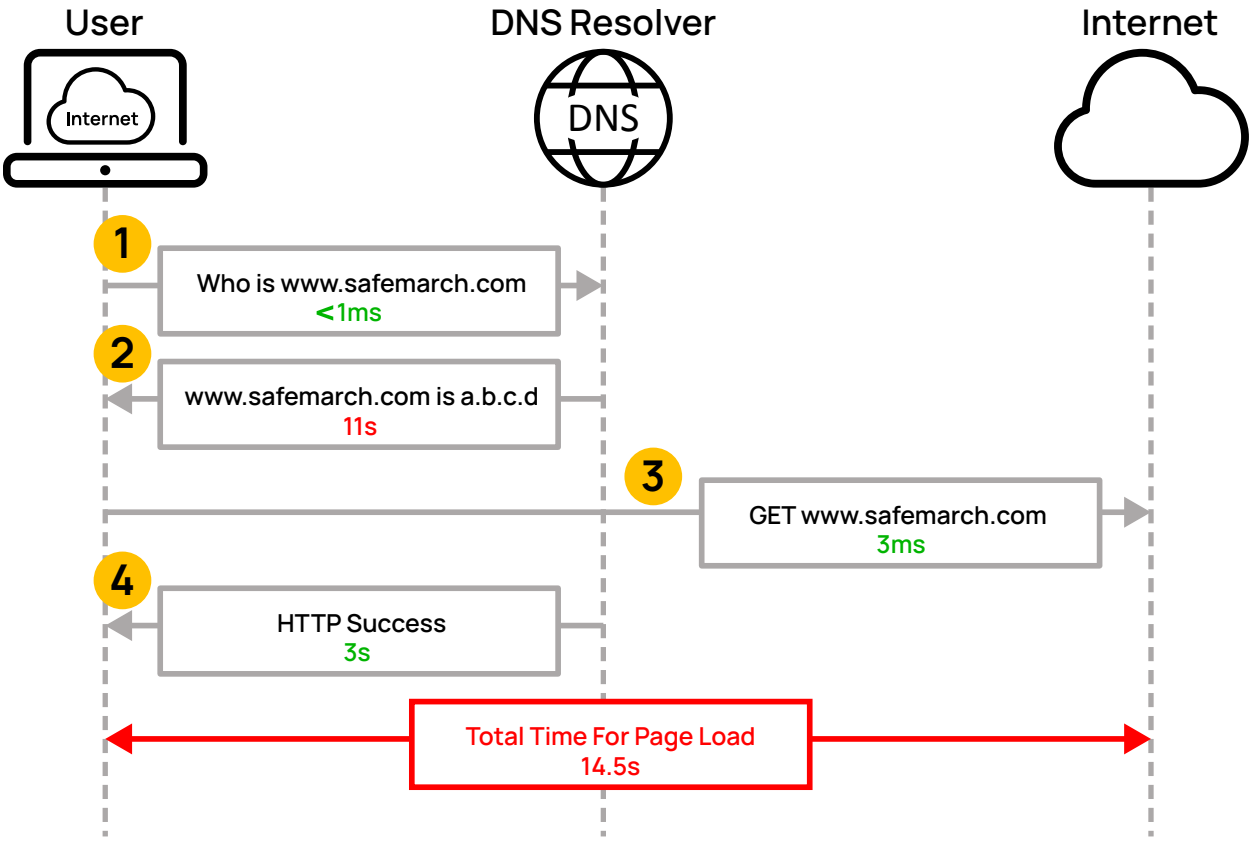


Figure 2. Slow DNS response leads to a perception of slow applications and internet connections

1. The device requests resolution of a domain name.
2. The DNS server responds to the request but takes an amount of time that is noticeable to the user. This could be due to a high volume of traffic or an issue with the server.
3. The device with its delayed response finally makes its request to the internet resource it requested.
4. The page is returned. Even though the web resource is performing well, the overall transaction was slow for the user.

Because of its role and placement in accessing resources on the internet, DNS is also a critical link in your user's perception of your internet and application performance. Slow DNS services make applications and website appear to perform poorly. The page itself might load quickly, but the time it takes to locate the page's address leads to a delay in loading time overall. Fast DNS response is critical to easing user frustration and increasing access to the internet.

The second issue involving fast resolution is ensuring that your users are connecting to a geographically local DNS service. When you send a request to a DNS server, that server resolves the IP address based on the resources closest to the server. If the server is on the other side of the world, it also refers you to applications that are local to the server. This can lead to extreme application latency and application issues such as incorrect language selection.

For example, users in Tokyo, NYC, and Seattle all have their DNS service configured for a server in Seattle. While the Seattle user experiences fast and appropriate resolution, the users in Tokyo and NYC don't have the same experience. The NYC user experiences long resolution and load times from the Seattle servers, while the user in Tokyo experiences both of those effects and an incorrect language selection for their request. It's critical that your users have access to fast, consistent, and geographically close DNS services.

Zscaler solves the issue of fast, local DNS resolution through the ZTR DNS service. Zscaler has over 150 data centers around the world that host the ZTR service for consistent, fast, and geographically local DNS resolution.

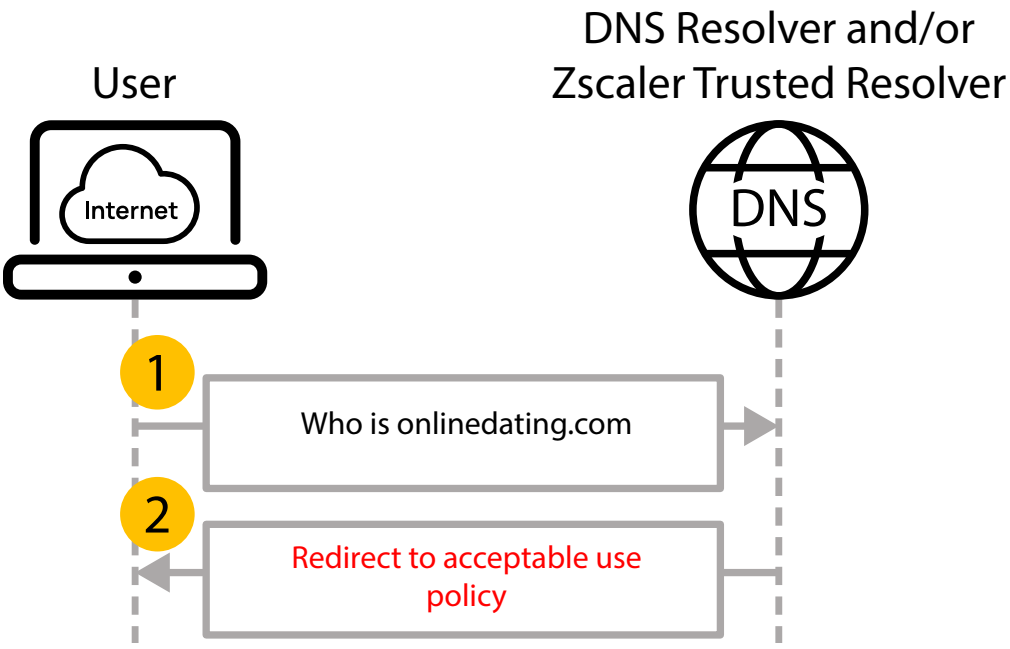


Figure 3. Stopping a request at the DNS layer is the fastest way to end a transaction

In many organizations, the DNS server also acts as a first-layer content filter. This can include filtering out categories of material to enforcing the use of safe search when searching the internet. When a user discovers that DNS is limiting their ability to find and access content, they might try to reach a less restrictive DNS server.

DNS is more than just a way for us to have easy-to-remember names for resources. It's also a list of websites you've visited and resources you've accessed. What a user is asking for on the internet has also become a concern due to monitoring and manipulation by nation states and malicious actors. In response to these threats, major browsers and public DNS services have implemented DNS over HTTPS (DoH) to prevent tracking of user DNS requests.

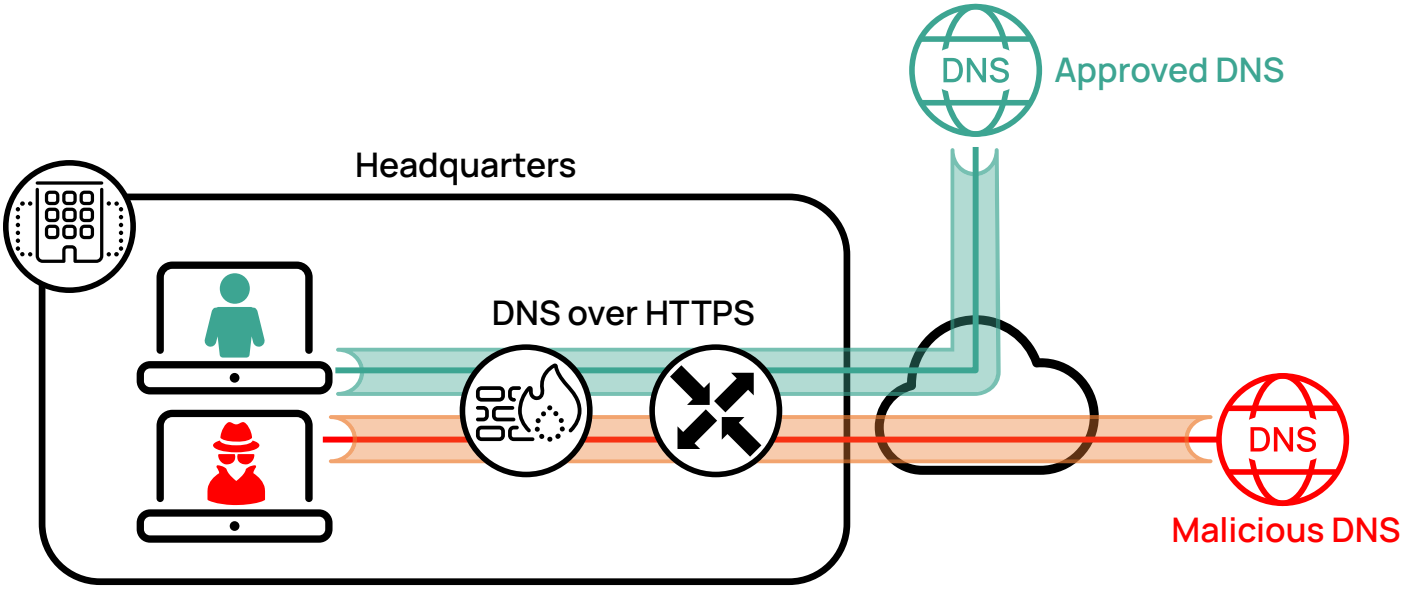


Figure 4. DNS over HTTPS places DNS protocol messages inside a TLS/SSL tunnel that provides confidentiality and integrity through TLS encryption, but also allows malicious actors to hide their activities

DoH operates by wrapping a DNS request inside of an HTTPS stream. HTTPS streams are encrypted with transport layer security (TLS). By securely encrypting the DNS request, inspection and interference are reduced or eliminated. Direct DoH requests can also be made by browsers and other applications, bypassing the system's configured DNS.

While this legitimate use is a benefit to privacy advocates, it's created a new way to bypass security controls for malicious users or infected machines. DoH gives users the ability to resolve otherwise banned URLs, exfiltrate data from the organization, and act as a command and control (C2) channel for botnets.

To ensure you are inspecting and applying policy to all your DNS traffic, you must enable TLS/SSL inspection. With Zscaler, you can decrypt, inspect, and apply policy to all your traffic in nearly real time. Zscaler maintains a list of well-known malicious DNS resolvers that can be blocked automatically. Traffic to resolvers that hasn't been seen before is inspected, and DNS policy is applied in the same way as traffic to known DNS resolvers. By inspecting tunneled traffic, the Zscaler firewall can enforce your DNS policy and block malicious traffic masquerading as a DNS request.

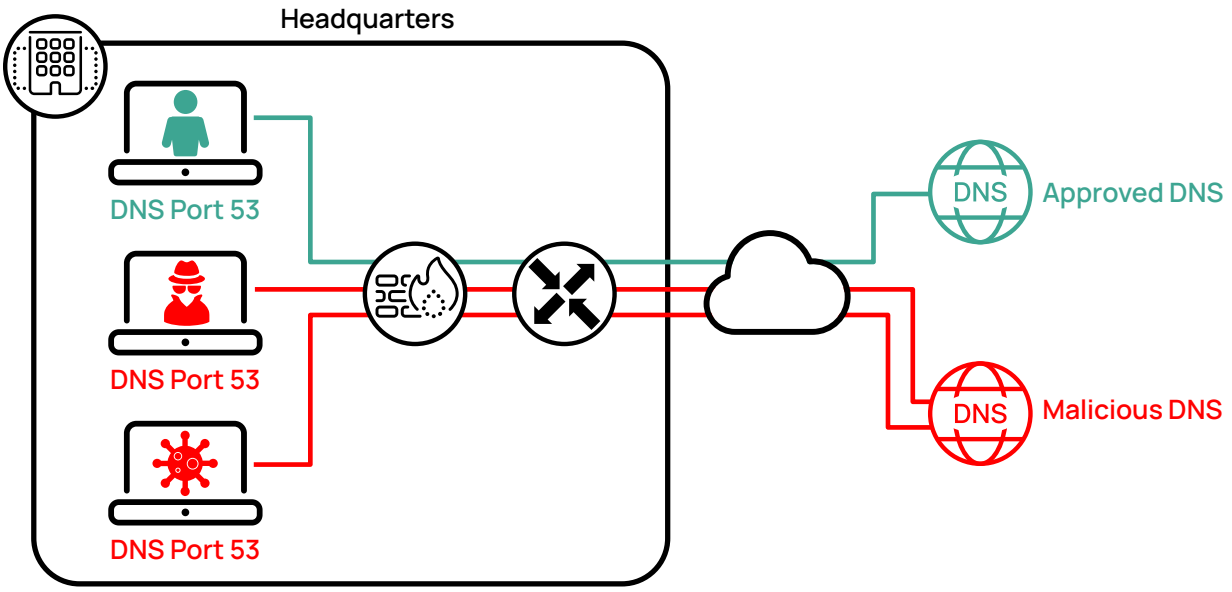


Figure 5. Legacy firewalls are often configured to allow access to offsite DNS servers

As a core internet technology, DNS is often allowed through legacy firewalls if the payload conforms to what is expected of a DNS request or response. This has led different threat actors leveraging DNS to bypass filters and leak content. Your users might attempt to tunnel through DNS ports to avoid policy controls and inspection. DNS tunnels leverage various forms of text attributes and record types supported by the DNS protocol to slowly leak information from the organization. Using these same message types, DoH tunnels are leveraged by C2 servers to communicate with compromised devices inside your organization.

Zscaler DNS Security and Control services offer mechanisms to take control of your DNS architecture and response. By proxying the DNS request, you can enforce your organization's DNS policies in the Zscaler Zero Trust Exchange (ZTE). When the DNS request reaches the ZTE, the request is open and inspected. No DNS requests can bypass inspection unless you authorize it, as you can restrict your users to only using DNS servers you specify. You can even leverage Zscaler as your DNS resolver directly without the need to specify other infrastructure.

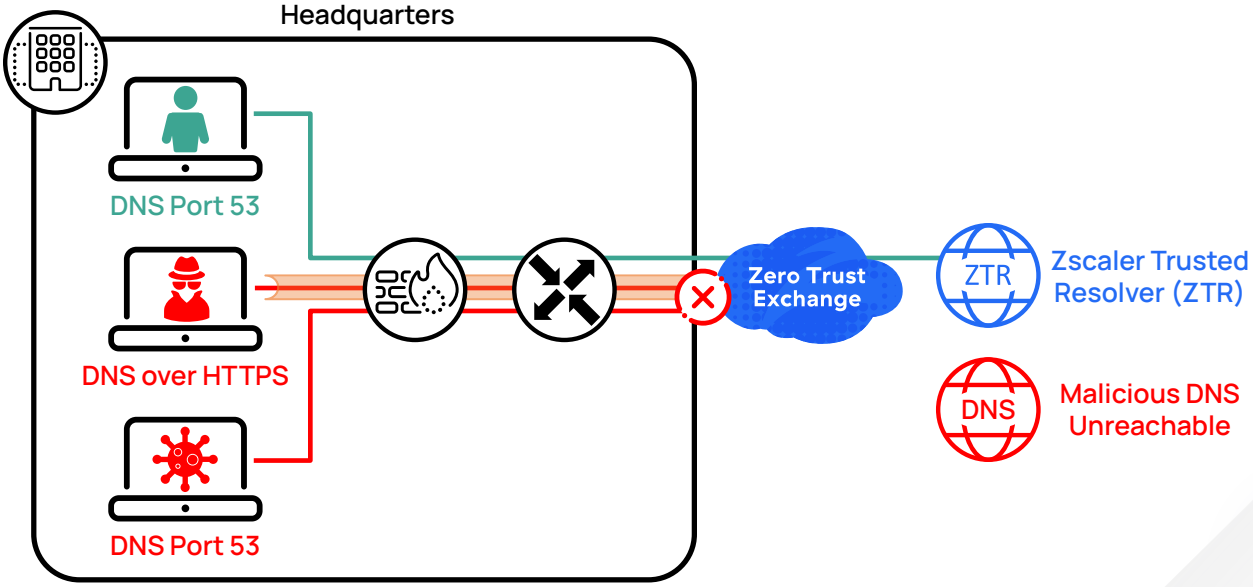


Figure 6. Zscaler's ZTE provides DNS resolution and the Zscaler firewall provides the ability to block DNS requests and tunnels to unapproved sources, redirecting DNS requests to authorized resolvers when possible

You can choose how you respond to requests as well, either by allowing, denying, or modifying a request. You can simply drop any requests for content or resources you don't believe are appropriate for your users and allow the rest to pass through. You also have the option to modify DNS responses to point at the resource of your choosing, such as a page explaining your content policy. Many organizations reroute users' search requests to the "safe search" version of a search engine, such as requests for *www.bing.com* being redirected to *strict.bing.com*.

Zscaler provides the capability to examine and modify DNS requests sent using multiple protocols, including transport control protocol (TCP), user datagram protocol (UDP) streams, and DNS over HTTPS (DoH). Zscaler's proxy architecture and full TLS/SSL inspection allows for the inspection and modification of DoH streams as well. This allows you to enforce policies no matter the protocol in use by an application.

ZTR does not support DOH tunnel termination.

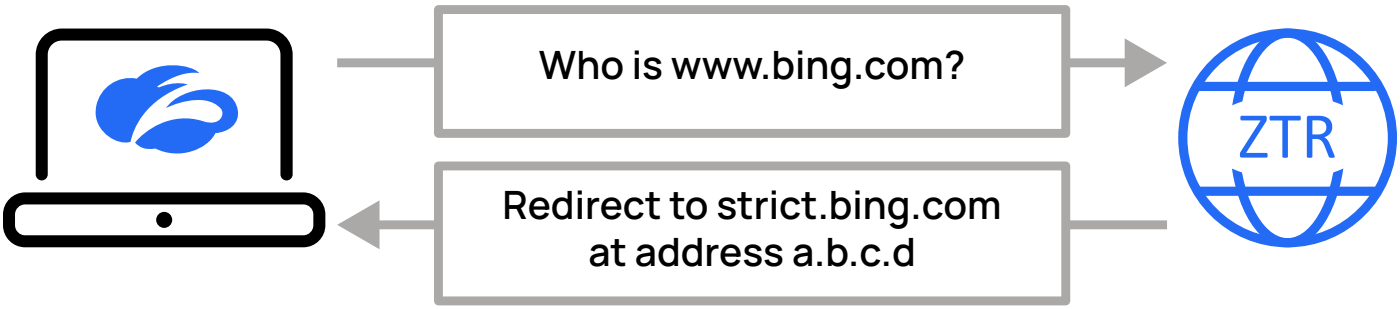


Figure 7. You can modify DNS responses to point to alternative resources

DNS modification can be used to enforce search policy, such as redirecting requests for a search engine to the more restrictive versions. In the previous example, a user tries to access the Bing search engine. The organization's policy is to use the strict search version of Bing, and the response is modified to redirect the user to *strict.bing.com*. This is done by configuring the IP address of the response and creating an appropriate DNS A-record response for the client.

In some instances, you might want to reroute traffic for a traveling user to a specific resource or deny access all together. This might be due to geopolitical concerns or increased local network security threats. By modifying the request for resources, you can direct users to a known good instance. You can also redirect them to a page explaining why the resource is currently unavailable to them.

With Zscaler, DNS policy is applied both to the outbound request and inbound response. The request and response are both examined against all your policy rules. Unlike other firewall requests, if a match is made, processing of additional rules stops and the appropriate action is taken for the request. This action could be to allow, modify, or block either the request or the response. For example, the request might be valid and allowed to pass through, but something in the response might trigger an action such as dropping the response.

Finally, you can inspect and act on DNS tunneling by your users or devices. You might want to prevent data exfiltration or ensure that content inspection bypass attempts fail. This, coupled with reporting, is another way to look for malicious actors leveraging internet of things (IoT) devices for nefarious purposes.

Zscaler DNS Control allows you to define a granular mix of conditions that must match before action is taken. By matching specific conditions, your policy can be tailored to your specific use cases.

Key Benefits

- Monitor and apply policies to all DNS requests and responses, irrespective of the protocol and the encryption used. This includes UDP, TCP, and DNS over HTTPS (DoH).
- Define granular DNS filtering rules using several DNS conditions, such as users, groups, departments, client locations, categorization of domains and IP addresses, DNS record types, the location of countries for resolved IP addresses, etc.
- Enforce condition-based actions on DNS traffic, such as allowing or blocking traffic, redirecting requests to specific DNS servers, redirecting users by overwriting DNS responses, etc.
- Detect and prevent DNS-based attacks and data exfiltration through DoH tunnels.
- Enhance your security posture by using Zscaler Trusted DNS Resolver for domain resolution.

New to Zscaler DNS Control?

If this is your first time reading about the Zscaler DNS Control functionality, the following resources can help get you up to speed quickly on the features and capabilities of the Zscaler platform.

- View a video introduction to the Zscaler DNS Control and learn more at **About DNS Control** (**https://help.zscaler.com/zia/about-dns-control**).
- Read the **Zscaler Firewall data sheet** (**https://www.zscaler.jp/sites/default/files/resources/en/data-sheets/zscaler-firewall.pdf**).
- Learn more about Zscaler's Zscaler Firewall technical features at **Understanding Firewall Capabilities** (**https://help.zscaler.com/zia/understanding-firewall-capabilities**).

Choosing a DNS Resolver Architecture

For most organizations, running a local DNS resolver on site was normal when traffic was mostly heading to the data center. Today we have users who are no longer on the organization's network. VPN connections lead to slow load times and incorrect resolutions for remote workers. Applications have also left the organization for SaaS and public cloud alternatives. Your DNS resolver faces the same pressure to be accessible and responsive to users, SaaS applications, and cloud workloads. Your DNS resolver also needs to be highly responsive to requests. Slow DNS requests that must travel halfway around the globe can lead to user frustration and complaints.

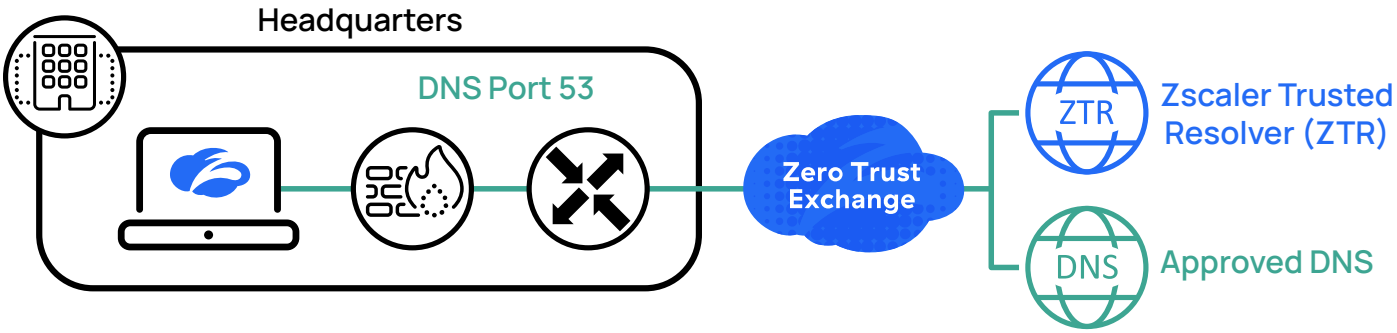


Figure 8. Zscaler Trusted Resolver provides a consistent and scalable DNS solution, or you can use your own external DNS resolver

Zscaler's DNS proxy architecture means that no matter where a DNS request is going or over what protocol, inspection and control are still available to you. Users cannot avoid inspection by simply hiding in another protocol, choosing a different server, or being outside the office with a disabled VPN. You have two options when leveraging the DNS proxy:

1. **Resolver Option –** Zscaler recommends leveraging the ZTR service as your DNS resolver. ZTR instances exist in each of Zscaler's 150+ data centers around the world. The ZTR service is included as part of your subscription to Zscaler.
2. **Transit Option –** In this model, you rely on a cloud-based DNS service. All requests are still proxied by a ZIA Service Edge for policy enforcement.

You can choose to have Zscaler be the primary DNS resolver via the ZTR service, or continue to leverage an external resolver. The ZIA service directs your requests to the DNS resolver service of your choice. The ZTR exists with all Zscaler data centers and can quickly respond to your users with consistent responses. You can also forward specific domains to the resolver of your choice, such as for local DNS servers referencing local resources.

Resolver Option: Zscaler Trusted Resolver

The ZIA service includes the ability to identify recursive queries and direct them to the ZTR service. This service is co-located in Zscaler data centers with the ZIA Public Service Edges and ZPA Public Service Edges. This results in both faster DNS response and results appropriate to the geographic region the user is connecting from. Together these translate into a better experience, as the user gets to the domain resolution faster by pointing to an instance that is closer to where they are geographically located—all while guaranteeing the use of a trusted DNS resolver regardless of device configuration.

If you plan to send iterative DNS queries, you need to configure a bypass option in the firewall rules. See Enabling Iterative DNS Lookups for Local DNS Servers in this guide.

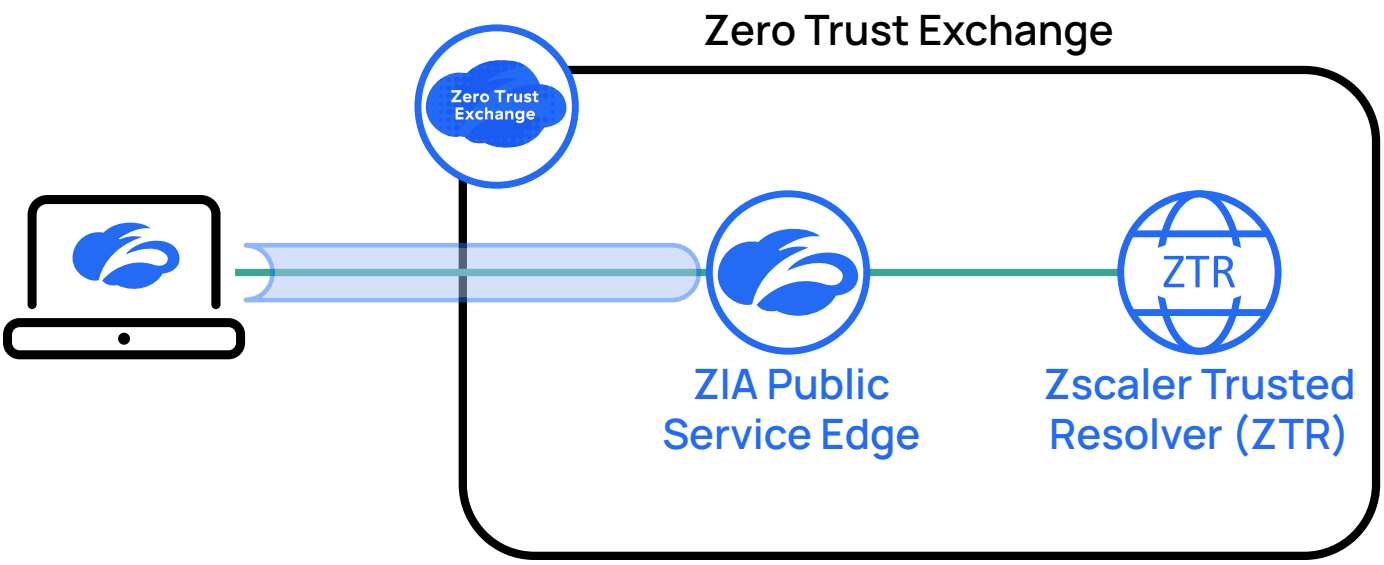


Figure 9. When a DNS request is received at a Zscaler Service Edge, it is inspected and redirected to the ZTR

When you leverage ZTR, your device DNS queries are intercepted when they reach the ZIA Public Service Edge and are resolved by the ZTR service. The traffic is routed to ZTR by leveraging a destination NAT rule in the firewall policy that captures and redirects all DNS requests to the ZTR service. Because the ZTR service exists at every Zscaler data center, your DNS requests are handled locally to the user with consistent policy.

The destination NAT policy rule for ZTR is preconfigured for you and enabled by default. If you are not planning to use ZTR, you need to disable this rule for any users and devices. To learn more about configuring the DNS NAT rule, see **About NAT Control** (**https://help.zscaler.com/zia/about-nat-control**).

Defining ZTR as an Explicit DNS Resolver

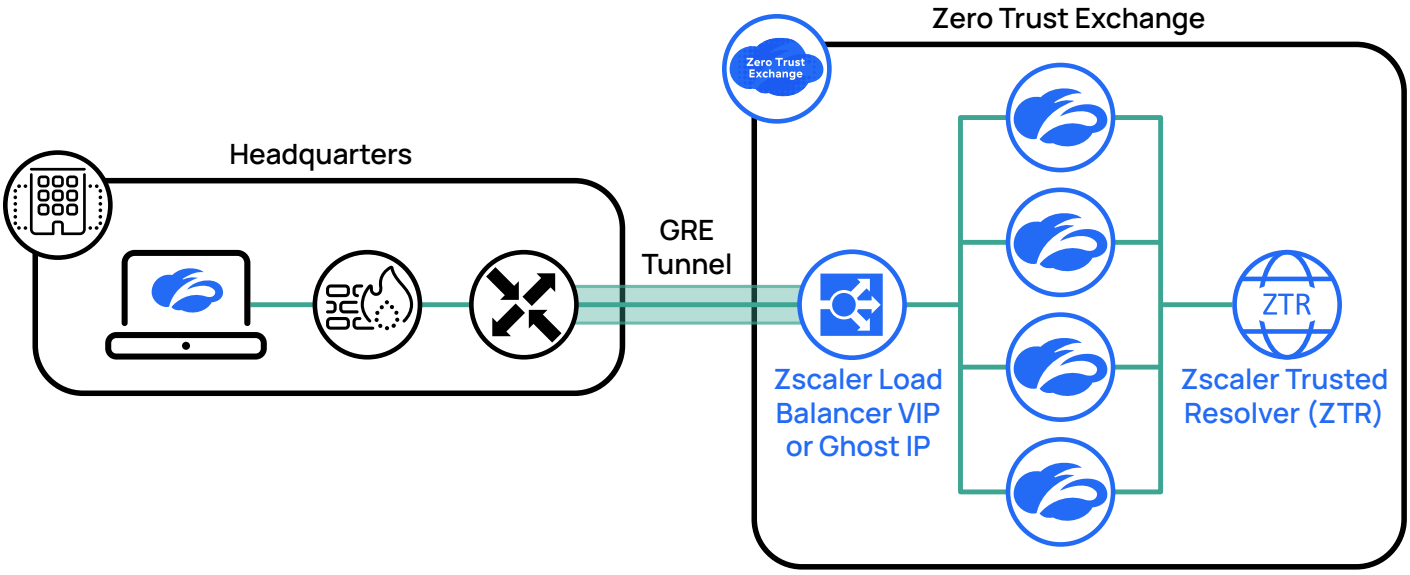


Figure 10. Using a virtual or ghost IP address lets you specify an explicit DNS request for your devices, with an IP address that is shared across multiple devices for high availability

If your organization has a policy requiring that an explicit DNS resolver be configured that matches the one used, Zscaler provides a scalable solution and a set of IP addresses for this purpose. Using one of our global or ghost IP addresses, any request to UDP or TCP port 53 to one of these ghost addresses is resolved by the ZTR service. By using these addresses, you ensure the fastest response without having to worry about an outage of a specific server.

Ghost IP addresses are only available for use over existing tunnels. These tunnel types include GRE, IPSec, and Z-Tunnel 2.0.

The ghost IP addresses require that a request come from a known location configured in ZIA. The DNS request can be forwarded over Z-Tunnel 2.0, GRE, or IPSec, or directly from an established location to the data center's ghost IP address. This model is most appropriate for locations with existing infrastructure.

In some organizations, the network is architected in a manner that prevents a DNS request from using an existing GRE or IPSec connection to Zscaler, and Zscaler Client Connector is also not an option. In this case, you first need to configure your organization's location in ZIA. This new location in ZIA is defined by the source IP address of the DNS requests. For example, if a DNS forwarder is sending DNS requests outside of a Zscaler tunnel ("tunnel-less"), then a new location would be created using the public source IP address seen by ZIA of the DNS forwarder for that location. Any DNS request from a known location is sent to ZTR for resolution, and all other DNS requests are dropped.

- To learn more about configuring locations in ZIA, see **About Locations** (**https://help.zscaler.com/zia/about-locations**).
- You can view a list of Zscaler IP addresses for your cloud at **Zscaler Config** (**https://config.zscaler.com/zscaler.net/cenr**).

Transit Option: DNS Proxy to a Remote DNS Server

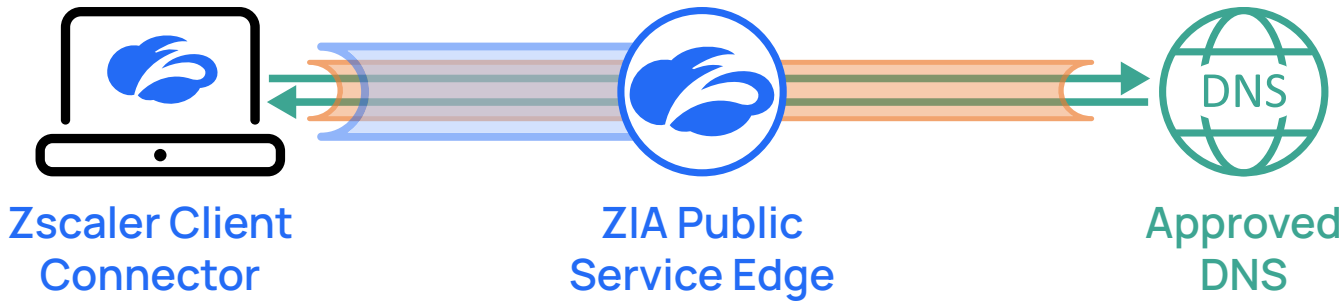


Figure 11. DNS is tunneled to a ZIA Public Service Edge that inspects DNS requests in both directions, including DoH streams via TLS/SSL inspection

In the transit option, Zscaler acts as a DNS proxy. The ZIA Public Service Edge opens and inspects the DNS request. If the request meets your organization's policy, the request is forwarded on to the public DNS resolver. The request is forwarded with the ZIA Service Edge IP address listed as the source, shielding your organization's IP addresses from inspection. The return response is also open and inspected. This allows you to modify or deny the request later in the process if the response is found to be objectionable.

Forwarding DNS Traffic to ZIA

Protecting your organization from online threats starts by forwarding all your DNS requests to Zscaler for DNS inspection and resolution. DNS requests and responses are both inspected against your defined policy. There are primary ways that Zscaler receives DNS requests: from Zscaler Client Connector users over Z-Tunnel 2.0, over GRE or IPSec tunnels from fixed sites, and directly from internal DNS resolvers or forwarders.

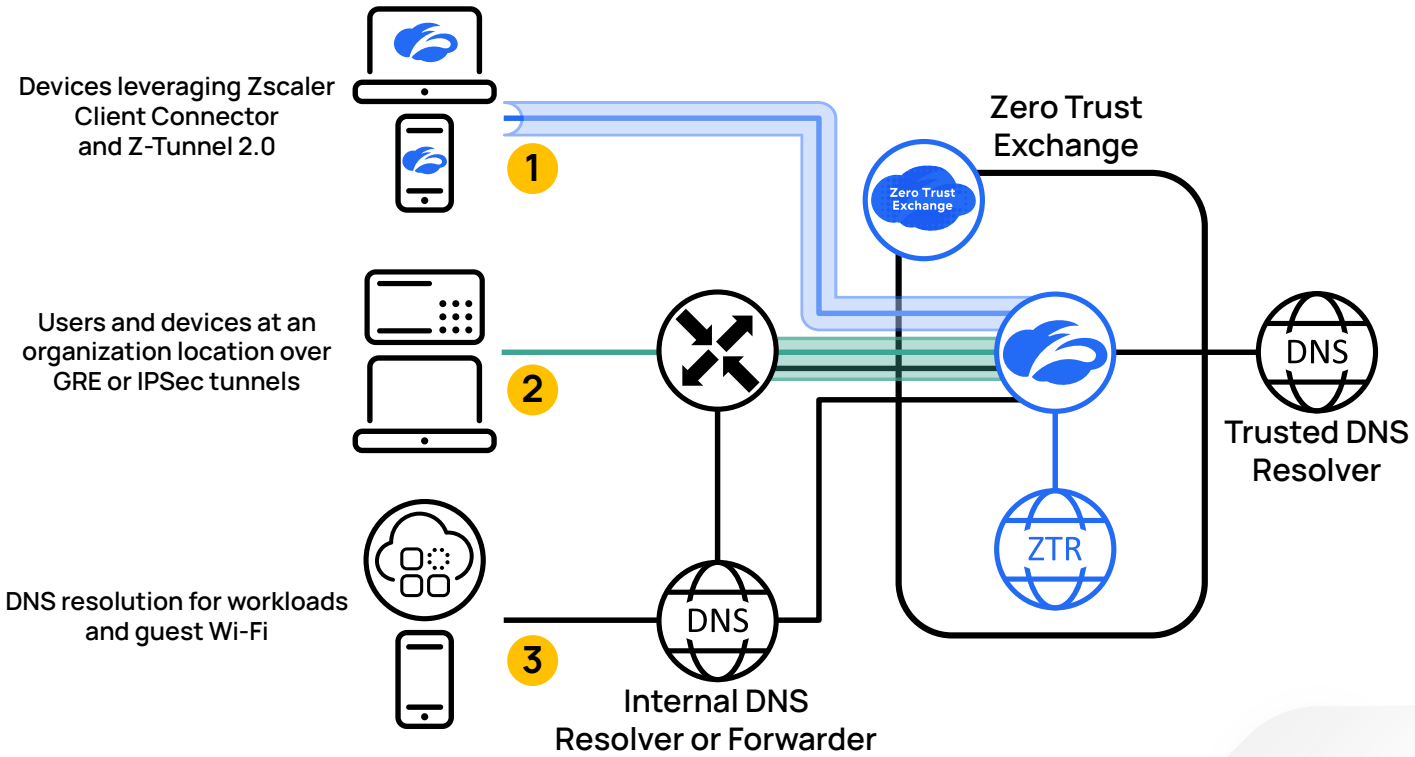


Figure 12. Forwarding your traffic to Zscaler ensures all DNS traffic is inspected and policy is enforced

1. **Devices leveraging Zscaler Client Connector and Z-Tunnel 2.0:** The Zscaler Client Connector agent is included with your Zscaler subscription. This lightweight agent connects your devices automatically to ZIA, ZPA, and ZDX services. Zscaler Client Connector is perfect for remote and mobile users and can be used at campus locations to enable pervasive Zero Trust access.
2. **Users and devices at an organization location over GRE or IPSec:** GRE and IPSec tunnels are established typically from routers or firewalls at your organization's location. With a tunnel established, all your internet-bound traffic can be forwarded directly to Zscaler.
3. **DNS resolution for workloads and guest Wi-Fi:** In some situations, a workload or guest user needs resolution to ZTR without the ability to authenticate. These requests can be forwarded across an existing GRE or IPSec tunnel from a known location, or sent directly from a known location to the nearest Zscaler data center. A new location in ZIA is defined by the source IP address of the DNS requests.

It is common for organizations to leverage multiple types of forwarding to ZIA. Not every device or situation allows for the use of Zscaler Client Connector, and not every router supports GRE or IPSec. For more information on understanding your forwarding options, see Traffic Forwarding in Zscaler Internet Access (https://www.zscaler.com/resources/reference-architectures/traffic-forwarding-zia.pdf).

DNS Filtering Rules and Condition-Based Actions

Building and enforcing DNS controls are handled by the Zscaler firewall policy engine. No matter which method you use for resolution, DNS controls can be applied to inspect and enforce policy. Depending on your needs, you can match all DNS traffic and enforce the same policy. In other organizations, you might want to have more granular control for different users or device types.

As an example, an organization might have their internet of things (IoT) devices configured to use an on-site DNS server. You would then configure your policy to reject any outbound DNS requests from an IoT device and redirect them to the local server. This prevents any attempts to leverage DNS to control a compromised IoT device while also handling device misconfigurations gracefully. Coupled with alerting, you can rapidly remediate any infected or misconfigured devices.

Matching DNS policy requests can be done for one or more values including users, groups, departments, defined locations, categorization of domains, destination or resolved IP addresses, DNS application types, and time intervals. When you've matched a DNS request, you can then specify an action.

The firewall's traditional allow and block actions are supported, but Zscaler also gives you the ability to modify the stream in real time. You can take actions to redirect DNS requests to servers of your choosing instead of what the request specified. You can also modify the response, changing the DNS response to point at a different resource for instance.

The Zscaler firewall acts on the first match and stops processing all other rules. Ensure that your rules are ordered correctly to avoid taking an incorrect action on a request.

To learn more about creating a DNS Control rule, see **Configuring the DNS Control Policy** (**https://help.zscaler.com/zia/configuring-dns-control-policy**).

Forwarding DNS Requests to ZTR or an External DNS Server

As mentioned previously, the default behavior of the ZIA service is to redirect DNS queries to the trusted Zscaler DNS resolver. A rule highlighting this setting is added to the NAT Control Policy tab indicating this redirection.

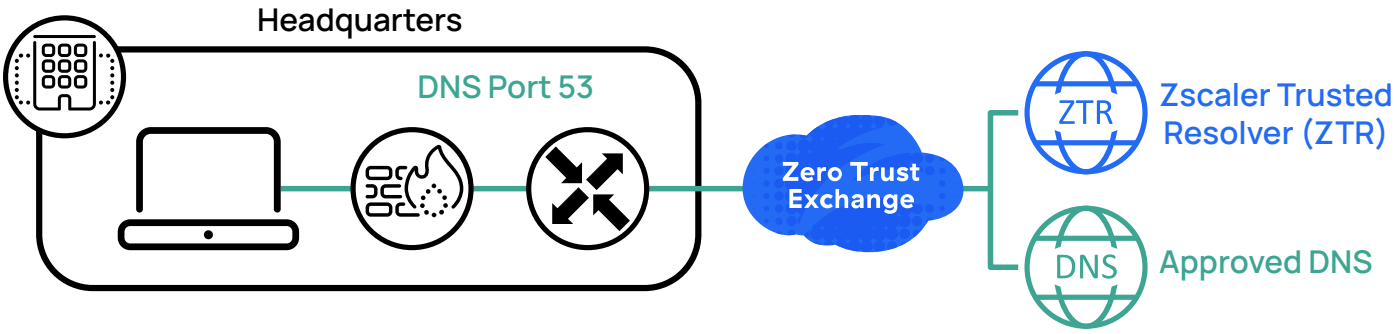


Figure 13. DNS requests are directed to the Zscaler ZTR service or an external DNS server of your choosing for name resolution

The ZTR rule is enabled by default.

If you plan to use a resolver on the internet, such as in a public cloud, you need to create a rule allowing DNS requests to that external resource. In this case, Zscaler will NAT the DNS request sent to the external sever instead of the ZTR. You also need to disable the rule for ZTR.

The inputs for the rule are the fully qualified domain name (FQDN) of the DNS service you are forwarding to, and the port number. To learn more about configuring NAT rules, see **About NAT Control** (**https://help.zscaler.com/zia/about-nat-control**).

Zscaler DNS Gateway Service

The Zscaler DNS Gateway service provides DNS high availability and protocol translation services for DNS requests.

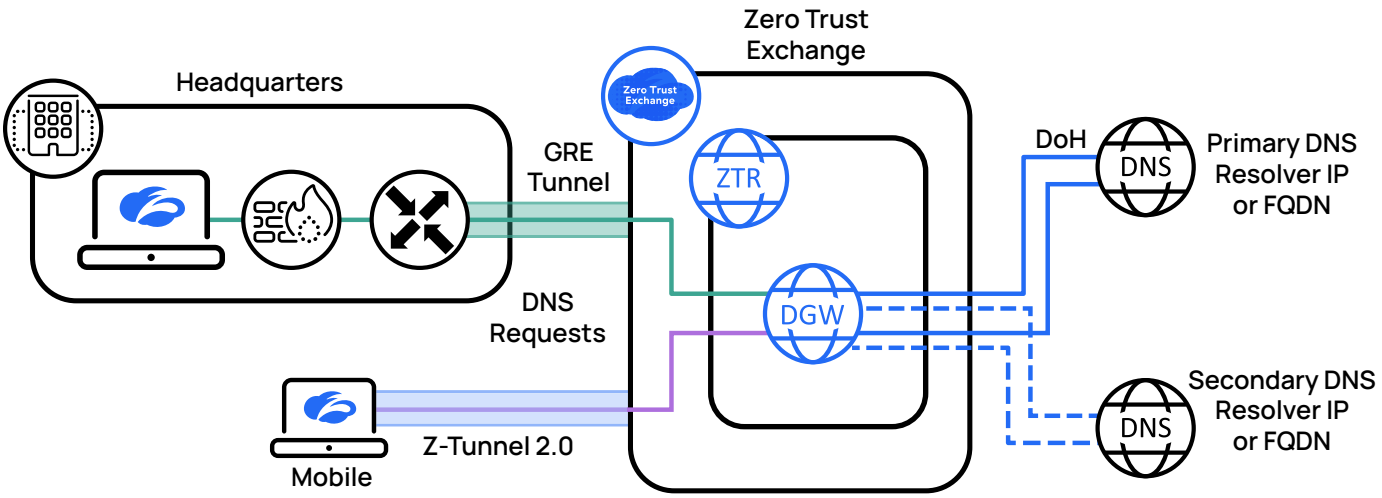


Figure 14. The Zscaler DNS Gateway service provides high availability and protocol translation

High availability allows you to configure a primary and backup destination address for your DNS service provider. The Zscaler service monitors the DNS service help, failing over to the secondary address automatically if the service degrades. Zscaler checks the health of your DNS service by monitoring for failures including:

- The service FQDN failing to resolve.
- When using DNS over HTTPS (DoH), the service monitors to see if the service responds with a DNS response.
- The DNS service responds with a server failure response (SERVFAIL).
- Responses time out.

Protocol translation occurs when your DNS request needs to be sent to your DNS provider using a protocol that is different than the one that was received. This could be switching to TCP or encrypting a connection for DoH. The following table highlights which protocol translations are available:

Protocol Translation	UDP to Server	TCP to Server	DoH to Server
UDP from Client	Supported	Not supported	Supported
TCP from Client	Not supported	Supported	Supported
DoH from Client	Supported	Supported	Supported

Table 1. DNS protocol translation matrix supported by the Zscaler DNS Gateway service

The DNS Gateway is invoked as part of the regular DNS Control policy when you select actions such as “Redirect as DNS over HTTPS” that implicitly call the DNS Gateway that you subsequently select.

The Zscaler DNS Gateway service, protocol translation, and high availability services are included as a part of the Advanced Firewall subscription.

To learn more about high availability and the DNS protocol translation service, see **About DNS Gateways** (**https://help.zscaler.com/zia/about-dns-gateways**).

EDNS Client Subnet Injection

Zscaler supports extension mechanisms for DNS (EDNS) client subnet (ECS) injection to obtain DNS responses from geolocated DNS resolvers. This extension mechanism allows you to pass the IP address or subnet information for the client along with the DNS request. This ensures that the correct DNS response is relayed to the user based on their location.

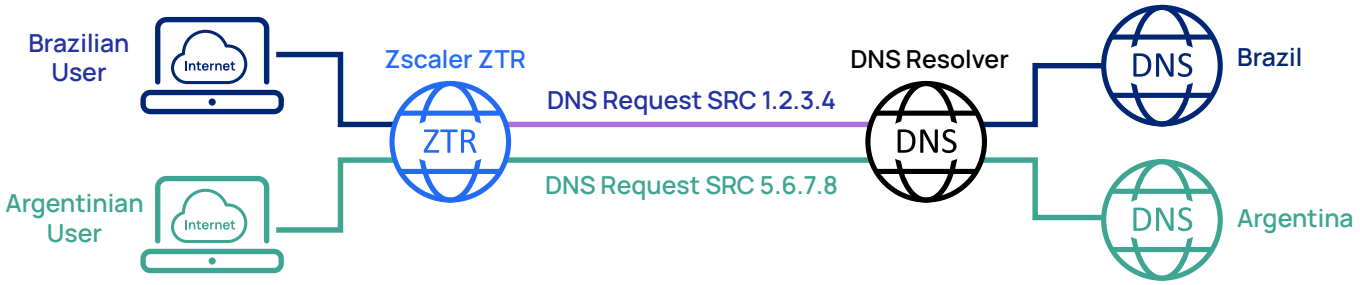


Figure 15. ECS injection includes source information in the DNS request, helping the resolver select the right responder

You should consider ECS injection when you have users who need to be directed to local resources when the nearest Zscaler data center is not local to the user. In many locations, the Zscaler data center might be in a location that results in users receiving the wrong instance of an application, such as being in the wrong language or not in compliance with local regulations.

When ECS is enabled, Zscaler implements one of two options. If the client request already contains an ECS prefix, Zscaler can preserve that information when forwarding the request. Otherwise, you can configure a public IP address or subnet prefix from your existing IP address space. The subnet range supported is /20 to /24 (single station). By including the ECS field, your DNS provider can provide an appropriate response.

ZTR does not support ECS. When ECS injection is enabled, you must configure destination NAT (DNAT) to send DNS requests to a public resolver that supports ECS resolution.

To learn more, see **About EDNS Client Subnet (ECS) Injection** (**https://help.zscaler.com/zia/about-edns-client-subnet-ecs-injection**).

Enabling Iterative DNS Lookups for Local DNS Servers

A recursive DNS lookup happens between an endpoint and its configured DNS server. The endpoint asks for an address, and the DNS server provides one or a response that no address could be found. An iterative request is what a DNS server does in the back end for any address that it doesn't know about.

When a request is received from a client, the DNS server begins making a series of requests. Iterative DNS requests start at the root server's DNS server, and through a series of referrals, the server works its way to the authoritative DNS server for that domain. The DNS server returns the result to the requester.

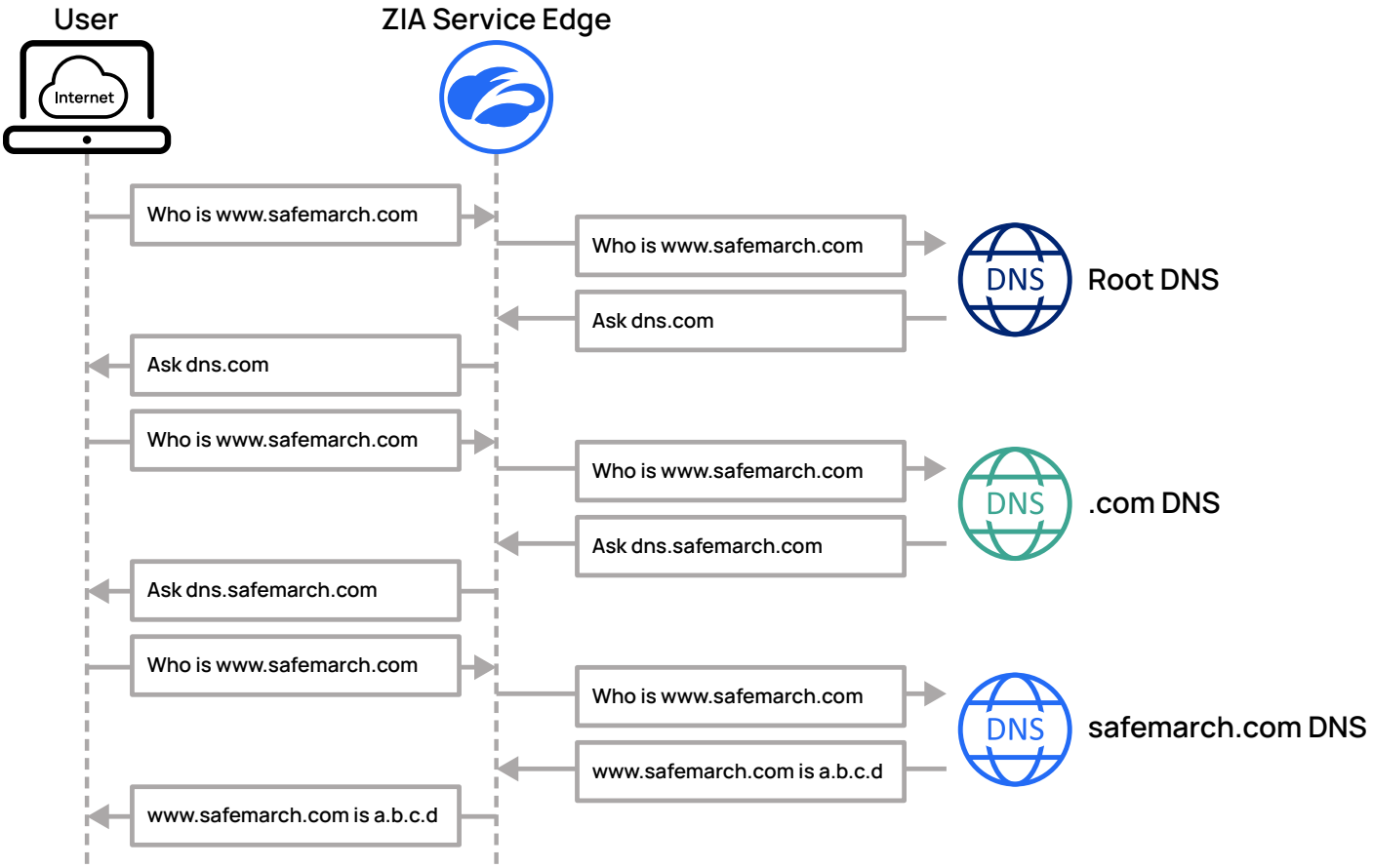


Figure 16. A recursive DNS request and an iterative DNS request

ZIA supports customers using both iterative and recursive DNS query types, though each is quite different. Iterative queries require specific additional configuration to transit the ZIA service, or the request will fail. By default, iterative queries are not supported by the Zscaler DNS service as it expects to receive requests from end user devices.

When an iterative query arrives, the service assumes it is a misconfiguration and the request is dropped. A policy is therefore needed to transit DNS queries through the Zscaler service to an external DNS provider that supports responses to iterative DNS queries. Because ZTR cannot resolve iterative requests, destination NAT rules cannot be applied to iterative requests and should be excluded from the rule.

In the iterative scenario, the client device sends the DNS query to the intended recipient. A destination NAT rule is needed to identify the matching conditions (the source IP address of the DNS server making the iterative query, for example) and direct this traffic to transit the ZIA service. If this is not done, then the query is directed to the Zscaler DNS resolver and ultimately dropped.

The destination NAT needs at least one of either a destination IP address or destination port to complete the transit. If the original source can be trusted to use the sanctioned destination, then simply specify the destination port again (port 53). If you want to force DNS requests to a specific service, you would also specify its IP address or FQDN.

Rule Order	Rule Name	Criteria	Action
1	DNS_DNAT	NETWORK SERVICES – DNS	NAT Port 53

Table 2. DNS destination NAT policy to forward all DNS requests

The previous example is of a destination NAT rule used to transit DNS traffic and is the current best practice for supporting iterative DNS queries. This rule as defined transits all DNS traffic regardless of whether it is iterative or recursive. Add the IP address sources of the iterative DNS servers as a criterion in the rule if the goal is to transit only the iterative requests while allowing the recursive requests to be directed to Zscaler's trusted DNS resolver.

It's important to note that the rule does not need to specify an IP address or FQDN of the DNS service. The only thing required is that the destination NAT policy be set to port 53. The request is then forwarded normally by the Zscaler service to the DNS service in the request.

- To learn more about recursive and iterative DNS Control, see **About DNS Control – DNS Server Traffic** (**https://help.zscaler.com/zia/about-dns-control#dns_server_traffic**).
- To learn more about configuring NAT rules for iterative and recursive requests, see **About NAT Control** (**https://help.zscaler.com/zia/about-nat-control**).

Blocking DNS Tunnels

The concept of DNS tunneling leveraging DNS over HTTPS (DoH) was developed as a method to prevent interception, modification, and recording of DNS requests. In the wake of actions by criminal threat actors and nation states, DNS-encoded channels can pass through many organizations' firewalls. Additionally, these tunnels don't carry arbitrary data, but instead leverage legitimate DNS record formats such as TXT, AAAA (IPv6 address record), and MX (mail exchange) records to pass information in small chunks. DNS tunneling can be leveraged by malicious actors both inside and outside of the organization.

Zscaler does not support DNS over TLS (DoT) tunnels. Zscaler recommends explicitly blocking destination port 853 to prevent the operation of DoT tunnels. By blocking these tunnels, the device or application is forced to fall back to DoH, TCP, or UDP connections that Zscaler can inspect and enforce policy on.

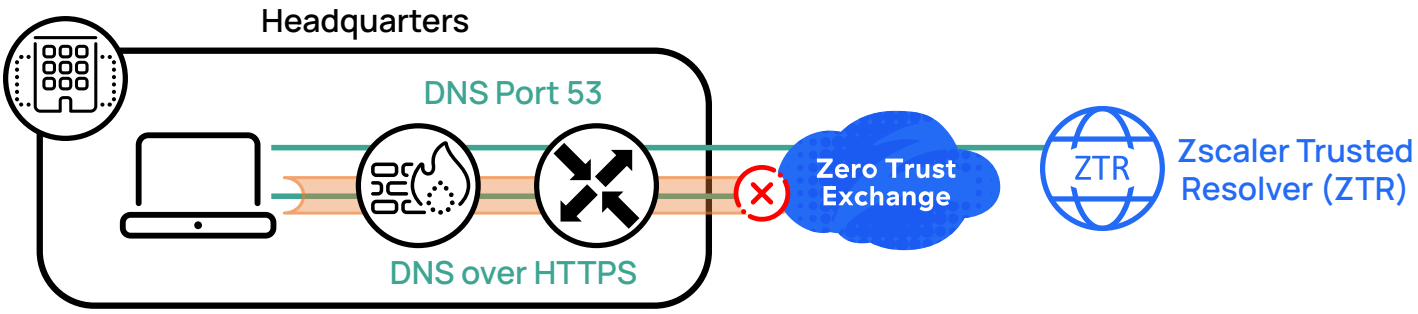


Figure 17. DNS tunnels are used as vectors for malicious actors

DNS tunnels open the organization to risk in the following ways:

1. **Bypass the organization's defined DNS protections:** For technically sophisticated users, they might realize that the organization's DNS is not only logged but might not return the results they want due to policy. Using DoH, the user can attempt to tunnel to an outside DNS server, such as one run by a browser developer.
2. **Pass Command and Control messages to compromised systems:** Command and Control (C2) messages are used to communicate with compromised systems. Devices participating in a botnet for instance receive C2 messages telling them the information about their next target for attack.
3. **Exfiltrate data from the organization:** Data can also be sent back to remote servers from clients, allowing a compromised device to send out data from the organization. This is done using small text-based messages hidden in what look like legitimate DNS responses.

Zscaler mitigates these risks by allowing you to inspect and block DoH tunnels. Zscaler can detect both well-known and previously unseen application tunnels. New tunnels are identified via machine learning comparison with other well-known tunnels, leveraging what Zscaler sees across the Zscaler cloud.

Zscaler recommends blocking all DNS tunnels if possible. Zscaler provides a default DoH tunnel policy that blocks all tunnels, but you must enable that control for your organization. If you plan to leverage a third-party DNS server and DoH, you can allow that tunnel specifically. If you cannot block all tunnels, consider blocking the categories Blocked DNS Tunnels and Unknown DNS Tunnels. Blocked tunnels are services known or suspected to be malicious tunnel services.

DNS Control Rules

After blocking DNS tunneling, there are other recommended policies that you might consider when deploying DNS Control. Zscaler considers running these policies as a best practice, but they should be compared with your policy and operating requirements. The following set of rules come predefined in your tenant instance and in some instances can be modified to suit your needs.

- **Unknown DNS Traffic:** The Unknown DNS Traffic rule is preconfigured to take action on suspected malformed traffic, non-standard DNS traffic, or even non-DNS traffic attempting to conceal itself as DNS traffic (not otherwise identified as another application). Zscaler recommends blocking the traffic matching this rule.
- **Default Firewall DNS Rule:** The Default Firewall DNS Rule is preconfigured to manage all DNS traffic that is not specifically defined and actioned in the higher-ranked, user-defined rules. Zscaler recommends blocking the traffic matching the rule, but only if the permitted DNS traffic is defined in a higher-ranked rule.
- **Fallback ZPA Resolver for Locations:** The Fallback ZPA Resolver for Locations rule is predefined to redirect source IP anchored traffic from location users to the preconfigured IP pools during control plane maintenance. This rule is disabled by default and cannot be deleted. It is only enabled during control plane maintenance to ensure the resiliency of the Source IP Anchoring feature.
- **Fallback ZPA Resolver for Road Warrior:** The Fallback ZPA Resolver for Road Warrior rule is predefined to redirect source IP anchored traffic of remote users to the preconfigured IP pools during control plane maintenance. This rule is disabled by default and cannot be deleted. It is only enabled during control plane maintenance to ensure the resiliency of the Source IP Anchoring feature.
- **Critical Risk DNS Categories:** The predefined rule, Critical Risk DNS Categories, blocks DNS traffic with the highest security risks in DNS request and response categories that are encountered by every organization. This block rule is implemented by all organizations, unless they are exceptional and have very permissive circumstances. It blocks traffic that matches known or suspected critical security threats in DNS requests and responses, such as malicious IP addresses and FQDNs, Domain Generation Algorithm (DGA) domains, and other advanced security threats. This rule is enabled by default and is created with a higher rule order.
- **Critical Risk DNS Tunnels:** The predefined rule, Critical Risk DNS Tunnels, blocks DNS tunnels with the highest security risks (e.g., commonly blocked DNS tunnels) that are encountered by every organization. This block rule is implemented by all organizations, unless they are exceptional and have very permissive circumstances. This rule is enabled by default and is created with a higher rule order.
- **High-Risk DNS Categories:** The predefined rule, High-Risk DNS Categories, blocks DNS traffic with high security risks to an organization's network. It blocks DNS traffic that matches newly registered and observed domains, newly revived domains, and other similar security threats in DNS requests and responses. This rule warrants careful consideration by an organization, and Zscaler strongly recommends implementing this block rule. This rule is enabled by default and is created with a higher rule order.
- **High-Risk DNS Tunnels:** The predefined rule, High-Risk DNS Tunnels, blocks DNS tunnels with high security risks (e.g., unknown DNS tunnels) to an organization's network. This rule warrants careful consideration by an organization, and Zscaler strongly recommends implementing this block rule. This rule is enabled by default and is created with a higher rule order.
- **Risky DNS Categories:** The predefined rule, Risky DNS Categories, is a recommended rule to block common DNS security threats to an organization's network. It blocks traffic that matches risky categories in DNS requests and responses, including content representing abuse or exploitative behavior, adult material, militancy/hate and extremism, violence, malicious content, etc. Blocking these categories is recommended, but the rule implementation might vary depending on your organization's requirements and corporate policies. The Risky DNS Categories rule is not enabled by default. Admins of sufficient rank can enable, fully customize, or delete this rule.
- **Risky DNS Tunnels:** The predefined rule, Risky DNS Tunnels, is a recommended rule to block DNS tunnels that are common security threats to an organization's network. Blocking these tunnels is recommended, but the rule implementation might vary depending on your organization's requirements and corporate policies. The Risky DNS Tunnels rule is not enabled by default. Admins of sufficient rank can enable, fully customize, or delete this rule.

Deploying Zscaler DNS Control in Your Organization

Because DNS plays such a central role to accessing internet resources, modifying your organization's deployment should be done in a controlled and tested manner. Taking the time to plan and test your deployment with small groups of technical users will give you the greatest chance of success.

For more information on deploying and operating Zscaler DNS Control, including a downloadable deployment checklist for these steps, see the DNS Control Deployment and Operations Guide (https://help.zscaler.com/zscaler-deployments-operations/dns-control-deployment-and-operations-guide).

Identifying and Bypassing External DNS Servers for Internal Name Resolution

DNS resolution can be handled either by having clients send traffic directly to Zscaler, or to a local DNS server first, which then forwards requests on to Zscaler for non-local name resolution. If you choose to leverage local name resolution, you need to identify the DNS subnets and/or domains associated with your DNS services. You can also use this information to configure the Zscaler firewall to forward the server's iterative requests to a third-party resolver.

Migrating from an Existing DNS Provider

For many organizations moving to Zscaler, ZTR means moving away from an existing DNS security provider that is currently configured on your devices.

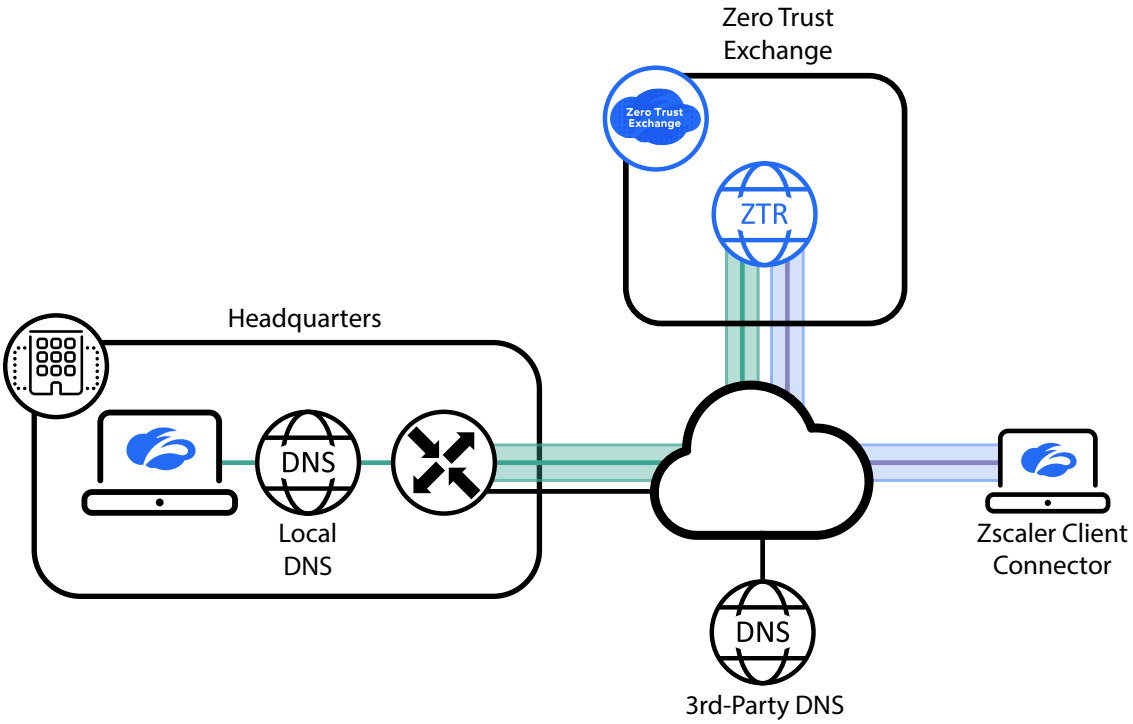


Figure 18. Migration from an existing DNS provider to ZTR can be achieved by either redirecting your local DNS server and pointing it to the ZTR service (left), or installing Zscaler Client Connector on your devices (right)

In this case, there are two common approaches to moving DNS resolution to ZTR:

1. **Point your DNS resolvers from the existing solution to ZTR:** In this model, you update your DNS entries so that your internal DNS resolver points at the Zscaler DNS VIP address. In this model, devices migrate to ZTR via configuration changes and DHCP settings. For each location, you need to define a location with the public source IP address of the DNS requests and activate firewalls at those locations. For redundancy purposes, you should configure two Zscaler VIP IP addresses from two different Zscaler data centers. A list of IP addresses is available at Zscaler Config (https://config.zscaler.com). The receiving data center can also be used to determine policy for users. See Differentiating DNS Policy for Users at a Common Location for more information.

2. **Install Zscaler Client Connector on your local devices and forward non-private DNS to ZTR:** In this case, you install the Zscaler Client Connector agent on your devices. You exclude domains that you don't want forwarded, such as .local or .test, and forward all other requests to Zscaler. Zscaler Client Connector intercepts the DNS requests and forwards them as appropriate to ZTR.

You must create a location defined by the public source IP address from which ZIA will receive DNS requests. You must also ensure that the location has the firewall enabled for the location.

When using Zscaler Client Connector to forward DNS requests to ZTR, you must use Z-Tunnel 2.0 on the Zscaler Client Connector client. DNS forwarding is not available on Z-Tunnel 1.0.

Differentiating DNS Policy for Users at a Common Location

When determining which policy to apply to users from a given location, you might want to provide different policies based on the device or user type. Each Zscaler data center has a VIP IP address that can be used as a DNS server address for your devices. The receiving VIP that receives the DNS request can be used as a variable when selecting policy.

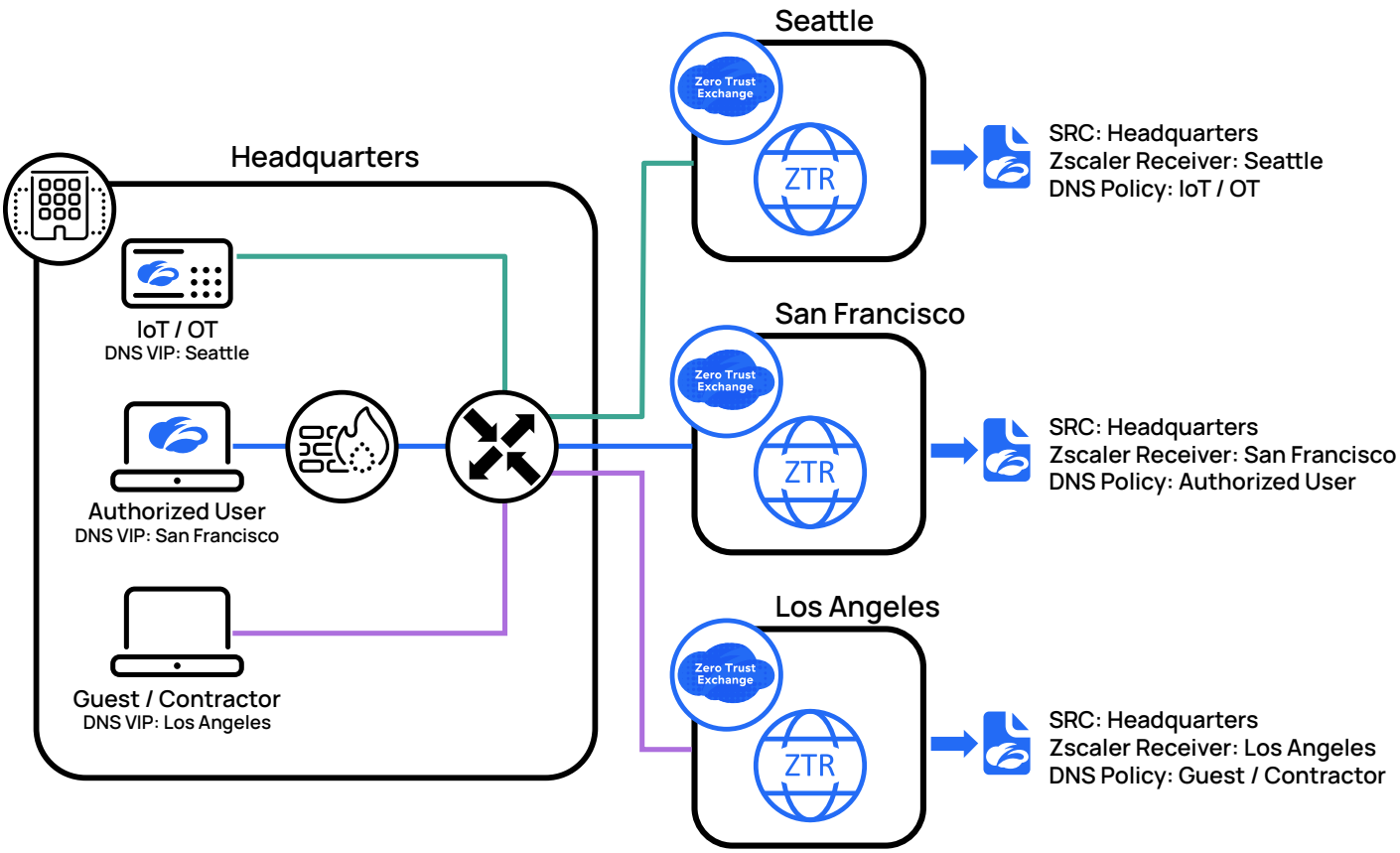


Figure 19. Your authorized users, guests, contractors, and IoT/OT can each receive a different DNS policy from the same location

As an example, you might want to provide different DNS access to authorized users, guests, contractors, or IoT/OT technology on your network. In this case, you would assign devices to send their DNS traffic to a VIP at a selected Zscaler data center by including that data center in your DHCP response. When Zscaler receives the request, it combines the location the request originated from with the receiving VIP to select the appropriate policy.

Forwarding All DNS Traffic to Zscaler

For DNS Control to be completely effective, all DNS traffic (legitimate or otherwise) must be sent to Zscaler. At locations where GRE or IPSec are in use as tunneling mechanisms, this can be handled by simply forwarding the request to Zscaler. For mobile clients, Zscaler recommends the use of Zscaler Client Connector and Z-Tunnel 2.0. For more information on forwarding decisions, see **Traffic Forwarding in Zscaler Internet Access** (**https://www.zscaler.com/resources/reference-architectures/traffic-forwarding-zia.pdf**).

Modifying the Firewall Policy to Allow DNS

The Zscaler firewall policy needs to be modified to allow DNS traffic to be allowed through the firewall. This allows the DNS Control module to act on the DNS request. Blocking DoH and DoT streams should also be configured here.

Defining DNS Application Groups (optional)

DNS application groups allow you to create groups of DNS servers that can be used as policy objects when configuring DNS Control. While this step is optional, server groups often allow for easier modification of resources without having to modify individual policy rules. For more information on configuring DNS application groups, see **About DNS Application Groups** (**https://help.zscaler.com/zia/about-dns-application-groups**).

Configuring DNS Control Policies

When you begin configuring DNS Control policies, you should start off by building policy to handle your majority use cases. In most instances, this will be your user base, setting policy around DNS use. After that policy is in place, you can identify cases that need special handling for DNS, and from there it is possible to build more granular policy for those users or devices. See **DNS Control Rules** for a list of recommended policy configurations.

Enabling Firewall and DNS Control in a Controlled Rollout

Before rolling out a change to your DNS structure across your organization, Zscaler recommends taking a phased approach by testing with a subset of users. Ideally this would be a subset of IT users or other technical users in your organization. This change should be done in real time for these users with the support of the team managing the Zscaler DNS Control configuration.

When making changes to your DNS infrastructure, make sure any changes won't affect your ability to reach the Zscaler Admin Portal or your local DHCP servers. Additionally, it's recommended to provide manual backup instructions to restore access until changes can be reverted to restore access.

After you have successfully tested your pilot group, you can begin rolling out the DNS changes to the rest of your organization. As you roll out your changes, you might become aware of local differences that necessitate location or group-based policy changes. These could be a location, user population, or device category that needs differentiated DNS controls. Using the granular policy match available in the Zscaler firewall, you can create a policy that matches your differentiated use case.

Ensure that your users in these locations are aware of the upcoming changes and how to contact support around any slowness or resource location issues.

Summary

Taking proactive control of users' DNS interactions gives you the ability to enforce policy at the very beginning of a transaction. This security is applied across any application needing to resolve a name to an IP address, not just web traffic. Zscaler DNS Control gives you the ability to monitor and control DNS activity within your organization, enforcing policy on which servers the user can access, controlling or modifying the response, and preventing DNS tunneling exploits. These controls expand your defense-in-depth capabilities and help ensure secure transactions, while local resolution speeds up applications and internet access for your users.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.