

Enforce Umbrella DNS and Prevent Bypass with Firewall Rules

Contents

[Introduction](#)

[Prerequisites](#)

[Enforcing Umbrella DNS—Most Common Method](#)

[Firewall Rule Example](#)

[Enforcement Against DNS over HTTPS \(DoH\)](#)

[Recommended Configuration](#)

[Details and Background](#)

[Enforcement Against DNS over TLS \(DoT\)](#)

[Enforcement Example](#)

[Firewall Support Disclaimer](#)

Introduction

This document describes how to prevent DNS bypass and enforce Umbrella DNS protections using firewall rules and network policies.

Prerequisites

- Network firewall
- Firewall access privileges
- Knowledge of firewall configuration

Enforcing Umbrella DNS—Most Common Method

Most routers and firewalls allow you to enforce all DNS traffic over port 53, requiring all network devices to use the DNS settings defined on the router, which must point to Umbrella DNS servers.

The preferred approach is to forward all DNS requests from non-Umbrella IP addresses to the Umbrella DNS IPs listed below. This method forwards DNS requests transparently and prevents manual DNS configuration from simply failing.

Alternatively, create a firewall rule to allow DNS (TCP/UDP) only to Umbrella DNS servers and block all other DNS traffic to any other IP addresses.

Firewall Rule Example

1. Add this rule to the edge firewall:

- **Allow**TCP/UDP inbound and outbound to 208.67.222.222 or 208.67.220.220 on **port 53**.
- **Block**TCP/UDP inbound and outbound to **all IP addresses** on **port 53**.

The allow rule for Umbrella DNS takes priority over the block rule. DNS requests to Umbrella are allowed, while all other DNS requests are blocked.

Depending on your firewall configuration interface, configure a separate rule for each protocol or a single rule covering both TCP and UDP. Apply the rule on the network edge device. You can also apply a similar rule to software firewalls on workstations, such as the built-in firewall in Windows or macOS.

If you are using the roaming client and Active Directory Group Policy, refer to the documentation on locking down the Enterprise Roaming Client using Group Policy.

Enforcement Against DNS over HTTPS (DoH)

Recommended Configuration

1. In Umbrella, enable the **Proxy / Anonymizer** and **DoH / DoT** [content categories](#).
2. Block the IP addresses of known DoH providers on your firewall.

Details and Background

Umbrella supports the `use-application-dns.net` domain, [as defined by Mozilla](#), to prevent Firefox from enabling DoH by default. For information on Firefox and DoH, see the related documentation.

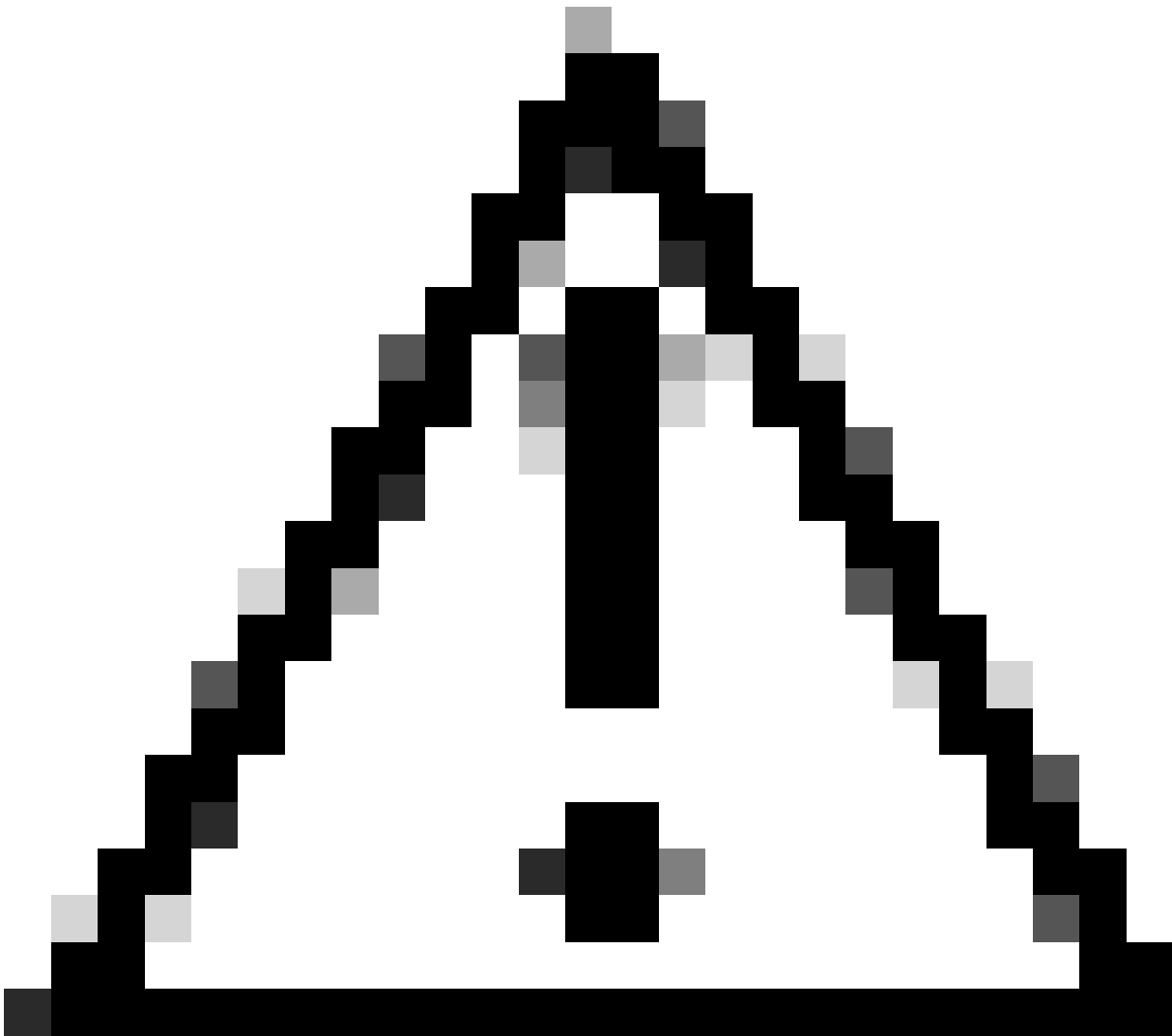
Even after blocking alternate DNS providers, DNS can still be bypassed with DoH. A local DNS resolver translates DNS requests into HTTPS and sends them to an endpoint using JSON or POST/GET. This traffic typically avoids DNS inspection.

Because DoH can be used to bypass Umbrella, Umbrella includes known DoH servers in the **Proxy / Anonymizer** content category. This mechanism has some limitations:

- It cannot block brand new DoH providers that are not yet known.
- It cannot block DoH used directly via IP address.

To address new DoH providers, monitor for updates and block **Newly Seen Domains** for improved coverage.

For DoH via IP address, scenarios are limited. Firefox with CloudFlare is a prominent example.



Caution: Do not add Mozilla Kill Switch domains to the block list. Blocking these domains results in an A-record for block pages, and Firefox treats this as valid and automatically upgrade its DoH usage.

Enforcement Against DNS over TLS (DoT)

Even after blocking alternate DNS providers and DoH, DNS can be bypassed over TLS, which uses [RFC7858](#) over port 853. For example, [CloudFlare](#) is a DoT provider.

Enforcement Example

- Block the IP addresses `1.1.1.1` and `1.0.0.1` on **port 853** (CloudFlare).

Firewall Support Disclaimer

This document assists network administrators in enforcing Umbrella DNS. Cisco Umbrella Support does not provide assistance with individual firewall or router configurations, as each device has a unique configuration interface. Consult your router or firewall documentation or contact the device manufacturer to

confirm whether these configurations are possible.