Examine the Behavior of DNS Queries and Domain Name Resolution

Contents

- Introduction
- Prerequisites
  - Requirements
  - Components Used
- Split Versus Standard DNS
  - Testing DNS — Important
- True Versus Best Effort Split DNS
- Tunnel-all and Tunnel-all DNS
  - Tunnel-all-DNS and Cisco Secure Client Umbrella Module
- DNS Performance Issue Resolved in AnyConnect Version 3.0 (4235)
  - Workarounds (If an Upgrade is not Possible)
- DNS with Split Tunneling on Different Client Operating Systems
  - Microsoft Windows (Windows 10 and Windows 11)
    - Tunnel-all Configuration (and Split Tunneling with Tunnel-all-DNS Enabled)
    - Split-include Configuration (Tunnel-all-DNS Disabled, No Split-DNS)
    - Split-exclude Configuration (Tunnel-all-DNS Disabled, no Split-DNS)
    - Split-DNS (Tunnel-all-DNS Disabled, Split-include Configured)
    - Split-DNS with Split-exclude Tunneling (Secure Client 5.x)
    - Encrypted DNS (DoH/DoT) on Windows
  - macOS
    - Tunnel-all Configuration (and Split Tunneling with Tunnel-all-DNS Enabled)
    - Split-include / Split-exclude (Tunnel-all-DNS Disabled, no Split-DNS)
    - Split-DNS (Tunnel-all-DNS Disabled, Split-include Configured)
  - Linux
    - Tunnel-all Configuration (and Split Tunneling with Tunnel-all-DNS Enabled)
    - Split-include / Split-exclude (Tunnel-all-DNS Disabled, No Split-DNS)
    - Split-DNS (Tunnel-all-DNS Disabled, Split-include Configured)
    - Linux VMs and Containers
  - Apple iOS (iPhone and iPad)
- Dynamic Split Tunneling and DNS (Secure Client 4.5+)
- Historical Client Versions (Reference)
- Related Bug Information
- Related Information
- Revision History
- Document Applies to

Introduction

This document describes how client operating systems handle DNS queries and the effects on domain name resolution using Cisco IOS® Secure Client.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions. Lab examples use Secure Firewall ASA/FTD group policies and Cisco Secure Client on Windows, macOS, Linux, and Apple iOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Split Versus Standard DNS

This document explains how client operating systems handle DNS queries and the effects on domain name resolution when using Cisco Secure Client (formerly Cisco AnyConnect) with split or full tunneling. VPN headends discussed include Cisco Secure Firewall ASA and FTD (formerly ASA); group-policy settings such as **split-dns**, **dns-server**, and **split-tunnel-all-dns** apply to both, unless otherwise noted.

If a section explicitly references older client releases, the behavior described for Secure Client 4.2 and later (including current Secure Client 5.x releases) applies. Cisco AnyConnect 4.x reached end-of-life; migrate to Cisco Secure Client for supported DNS and tunneling features.

DNS resolution behavior depends on three factors:

- VPN DNS Policy: Configured on the headend (split DNS, tunnel-all-DNS, or standard DNS)
- Split-tunneling Mode: Tunnel-all, split-include, or split-exclude
- Client Operating System: DNS resolver architecture (per-interface vs global)

When you run the **split-include** tunneling command, these are the three DNS options available in the group policy:

Mode	Description
Split DNS	DNS queries that match domain names configured on the headend (**split-dns**) are sent through the tunnel to the VPN DNS servers (`dns-server`). All other queries use the client OS resolver and physical adapter DNS servers.
Tunnel-all-DNS	Only DNS traffic to the DNS servers defined by the headend is allowed. Configured with **split-tunnel-all-dns enable** in the group policy.
Standard DNS	All DNS queries are first sent to the VPN DNS servers defined by the headend. On a negative (NXDOMAIN or no answer) response, the resolver can also try DNS servers on the physical adapter.



Note: The **split-tunnel-all-dns** command was first implemented in ASA version 8.2(5). Before that version, only split DNS or standard DNS was available. In all cases, DNS queries that are defined to move through the tunnel, pass to any DNS server defined by the headend. If no DNS servers are defined on the headend, the DNS settings for the tunnel are blank.

If split DNS are **not** defined, all DNS queries are sent to the DNS servers defined by the headend (subject to OS-specific behavior described later in this document.) However, the behaviors described in this document can differ based on the operating system (OS).

Testing DNS — Important



Note: Avoid using **NSLookup** or **dig** when testing the name resolution on the client. Instead, use a web browser or run the **ping** command. NSLookup and dig do not use the OS DNS resolver stub the same way most applications do. Secure Client does not force every DNS request through a specific interface; it allows or rejects requests based on split DNS and tunnel-all-DNS policy.

To observe correct failover behavior, test only with applications that rely on the native OS DNS resolver (browsers, ping, and most business apps.) Tools that perform their own DNS resolution (NSLookup, dig, and some custom apps) can show misleading failures even when the client works correctly.

True Versus Best Effort Split DNS

AnyConnect Release 2.4 introduced split DNS fallback (best-effort split DNS), which is not a true split DNS

and was also found in the legacy IPsec client.

Best-effort (fallback) behavior:

- If the request matches a split DNS domain, Secure Client allows the request to be tunneled to the headend.
- If the VPN DNS server cannot resolve the host name, the OS DNS resolver continues and can send the same query to a DNS server on the physical interface.
- If the request does not match any split DNS domain, Secure Client does not tunnel it. It can synthesize a response so, the resolver falls back to the physical interface DNS servers.

This is why the legacy feature is called DNS fallback for split tunneling, which is not a true split DNS. Secure Client ensures only matching split-DNS-domain queries enter the tunnel, but still relies on the OS resolver behavior for final resolution.

Security concern: A private domain name can leak to a public DNS server when the VPN DNS server returns NXDOMAIN or fails to resolve; and the resolver retries on the physical adapter.

True split DNS: Cisco bug ID CSCtn14578

Resolved on Microsoft Windows in AnyConnect 3.0(4235) and retained in Secure Client 4.2+):

- Queries for configured split-DNS domains are allowed only via the VPN path (tunnel DNS servers/VPN adapter, depending on platform and version.)
- All other queries are allowed only via non-VPN DNS servers (physical adapter.)



Note: Only registered Cisco users have access to internal Cisco bug tools and detailed bug information.

Tunnel-all and Tunnel-all DNS

When split tunneling is disabled (**tunnel-all** configuration), DNS traffic is allowed strictly via the tunnel.

The **tunnel-all-DNS** configuration (**split-tunnel-all-dns enable** in the group policy) sends all DNS lookups through the tunnel while some form of split tunneling is also configured, and DNS traffic is allowed strictly via the tunnel interface.

This is consistent across platforms with one caveat on Microsoft Windows, when the **tunnel-all** or **tunnel-all-DNS** is configured, Secure Client allows DNS traffic strictly to the DNS servers configured on the secure gateway (applied to the VPN adapter). This security enhancement was implemented with true split DNS. If this is problematic (for example, DNS update/registration must reach non-VPN DNS servers), complete these steps:

1. If the current configuration is tunnel-all, enable **split-exclude** tunneling. Any single-host split-exclude network is acceptable, such as a link-local address.
2. Ensure **tunnel-all-DNS** is not enabled in the group policy (**split-tunnel-all-dns disable**.)

Tunnel-all-DNS and Cisco Secure Client Umbrella Module

When **split tunneling** and **tunnel-all-DNS** are both enabled, DNS is intercepted at the kernel level and blocked if it does not egress the correct VPN interface. The Secure Client Umbrella module (formerly AnyConnect Roaming Security) can be affected on networks where encrypted DNS is unavailable. This is because the module can attempt standard DNS via the LAN interface while tunnel-all-DNS requires DNS via the VPN.

By default, the Umbrella module uses encrypted DNS (UDP port 443), which is generally not blocked by tunnel-all-DNS. The issue mainly appears when encryption is unavailable and plain DNS is used.

Recommendation: Add the Cisco Umbrella resolver addresses to the split-include list if you use tunnel-all-DNS with the Umbrella module. Or refer to the Enable Tunnel All DNS for Secure Client with Umbrella Module document (Document ID: 224809.)

DNS Performance Issue Resolved in AnyConnect Version 3.0 (4235)

This Microsoft Windows issue is most prevalent under these conditions:

- Home router setup where DNS and DHCP servers share the same IP address (Secure Client creates a necessary route to the DHCP server.)
- A large number of DNS suffixes/domains in the group policy.
- A **tunnel-all** configuration.
- Name resolution uses an unqualified host name so, the resolver tries multiple DNS suffixes across all available DNS servers.
- The native DNS client attempts to send DNS queries via the physical adapter, which the Secure Client blocks under **tunnel-all**.

This can cause significant name-resolution delays, especially when the headend pushes many DNS suffixes. The resolver must walk through suffixes and servers until it receives a positive response.

This problem is resolved in AnyConnect 3.0(4235) and later Secure Client releases. Refer to Cisco bug ID CSCtq02141 and Cisco bug ID CSCtn14578 for details.

Note: Only registered Cisco users have access to internal Cisco bug tools.

Workarounds (If an Upgrade is not Possible)

Enable split-exclude tunneling for an IP address so, local DNS can use the physical adapter. An address from link-local subnet 169.254.0.0/16 is commonly used as traffic to those addresses is unlikely to traverse the VPN.

After you enable split-exclude tunneling, enable local LAN access on the client profile or client, and disable **tunnel-all-DNS**. This is an ASA/FTD configuration example:

```
access-list acl_linklocal_169.254.1.1 standard permit host 169.254.1.1
group-policy gp_access-14 attributes
split-tunnel-policy excludespecified
split-tunnel-network-list value acl_linklocal_169.254.1.1
split-tunnel-all-dns disable
exit
```

Client profile XML:

```
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
```

You can also enable this in the Secure Client GUI: **Preferences → Enable Allow local (LAN) Access when using VPN**

1. Use fully qualified domain names (FQDNs) instead of unqualified host names.
2. Use a different IP address for the DNS server on the physical interface (separate from DHCP on the same subnet.)

DNS with Split Tunneling on Different Client Operating Systems

Different client operating systems handle DNS differently with split tunneling (without split DNS) for Secure Client; this section describes those differences.

Microsoft Windows (Windows 10 and Windows 11)

On Windows, DNS settings are per network interface. With split tunneling, DNS queries can fall back to physical-adapter DNS servers after they fail on the VPN tunnel adapter. If split tunneling is used without split DNS, both internal and external resolution can work as the resolver can fall back to external DNS servers. There was a significant change in Secure Client for Windows in release 4.2 after the fix for Cisco bug ID CSCuf07885. This behavior is unchanged in Secure Client 5.x.



Note: Only registered Cisco users have access to internal Cisco bug tools.

Tunnel-all Configuration (and Split Tunneling with Tunnel-all-DNS Enabled)

Pre–Secure Client 4.2 (AnyConnect 4.1 and earlier):

- Only DNS requests to DNS servers configured under the group policy (tunnel DNS servers) are allowed.
- The Secure Client driver responds to all other requests with no such name.
- DNS resolution can only use tunnel DNS servers.

Secure Client 4.2 and later:

- DNS requests to any DNS servers are allowed if they originate from the VPN adapter and are sent across the tunnel.
- All other requests receive no such name; resolution via the VPN tunnel only.
- Prior to Cisco bug ID CSCuf07885, Secure Client restricted target DNS servers. After this fix, it restricts which network adapters can initiate DNS requests.

Split-include Configuration (Tunnel-all-DNS Disabled, No Split-DNS)

The Secure Client driver does not interfere with the native DNS resolver. Resolution adheres to the network adapter order; Secure Client is the preferred adapter when the VPN is connected.

A DNS query is first sent via the tunnel; if unresolved, the resolver can try the public interface. The split-include access list must include the subnet covering tunnel DNS server(s) on releases before 4.2. Starting with Secure Client 4.2, the host routes for tunnel DNS server(s) are automatically added as split-include networks (secure routes), so the split-include ACL no longer requires explicit tunnel DNS server subnets.

Split-exclude Configuration (Tunnel-all-DNS Disabled, no Split-DNS)

The same resolver behavior as the split-includes, tunnel first, then the public interface fallback. The split-exclude access list must not include the subnet covering tunnel DNS server(s). Starting with Secure Client 4.2, the automatic host routes for tunnel DNS servers prevent common split-exclude misconfiguration.

Split-DNS (Tunnel-all-DNS Disabled, Split-include Configured)

Split-DNS on Windows requires **split-include** tunneling (**split-tunnel-policy tunnelspecified**.) It does not support split-exclude-only tunnel policies for split-DNS configuration.

Pre–Secure Client 4.2:

- Split-DNS Domain Queries: Allowed to tunnel DNS servers only; no such name if sent to other servers.
- Non-split-DNS Domain Queries: Allowed to other DNS servers only; no such name if attempted via tunnel.

Secure Client 4.2 and later (true split DNS on Windows):

- Split-DNS Domain Queries: Allowed to any DNS server only if they originate from the VPN adapter. Queries from the public interface receive no such name to force tunnel use.
- Non-split-DNS Domain Queries: Allowed to any DNS server only if they originate from the physical adapter. Queries from the VPN adapter receive no such name to force public-interface resolution.

Split-DNS with Split-exclude Tunneling (Secure Client 5.x)

Secure Client 5.x admin documentation adds split DNS for split-exclude configurations. Refer to the Secure Client 5.x Administrator Guide — Configure Split DNS for Split Exclude Tunneling for headend and policy requirements. OS-level enforcement rules still apply once split DNS is active.

Encrypted DNS (DoH/DoT) on Windows

Applications or OS features that use DNS over HTTPS (DoH) or DNS over TLS (DoT) can bypass the Windows stub resolver path that Secure Client filters. If split DNS appears to fail for specific apps but works in a browser, verify whether those apps use encrypted or custom DNS. Standard split-DNS testing ought to use the OS resolver (browser, ping), not NSLookup/dig.

---

macOS

On macOS, DNS settings are global (not per-interface). If split tunneling is used without split DNS, DNS queries often cannot reach DNS servers outside the tunnel as expected, you can resolve internal names only, not external names through the public path. This is documented in Cisco bug ID CSCtf20226 and Cisco bug ID CSCtz86314.

Workarounds:

- Specify an external DNS server IP under the group policy and use FQDNs for internal queries.
- If external names are resolvable through the tunnel, disable split DNS in **Advanced > Split Tunneling** by removing DNS names from the group policy, and use FQDNs for internal queries.

Split DNS on macOS is supported from AnyConnect 3.1 onward, subject to these conditions:

- Split DNS enabled for both IP protocols (requires ASA 9.0+/equivalent FTD), or;
- Split DNS enabled for one IP protocol and **Client Bypass Protocol** enabled for the other with no address pool for the bypassed protocol (or no IPv6 pool on ASA versions before 9.0).



Note: Secure Client does not primarily manage name resolution through **/etc/resolv.conf** on macOS; it configures OS-level DNS settings. macOS can keep **resolv.conf** updated for compatibility. Run **scutil --dns** to view effective DNS configuration.

Tunnel-all Configuration (and Split Tunneling with Tunnel-all-DNS Enabled)

When Secure Client is connected, only tunnel DNS servers remain in system DNS configuration; requests only proceed to tunnel DNS server(s).

Split-include / Split-exclude (Tunnel-all-DNS Disabled, no Split-DNS)

Secure Client does not interfere with the native resolver. Tunnel DNS servers are preferred over public resolvers, so the first query attempt goes over the tunnel. Because DNS is global on macOS, queries do not always reliably use public DNS outside the tunnel (Cisco bug ID: CSCtf20226).

Starting with Secure Client **4.2**, host routes for tunnel DNS servers are added automatically as secure routes.

Split-DNS (Tunnel-all-DNS Disabled, Split-include Configured)

True split DNS (similar to Windows) applies when:

- Split-DNS is enabled for both IPv4 and IPv6, or;
- Split-DNS is enabled for one protocol and no client address pool exists for the other protocol.

True split DNS means matching split-DNS domains resolve only via the tunnel and are not leaked to external resolvers.

If split-DNS is enabled for only one protocol and a client address is assigned for the other protocol, only DNS fallback for split tunneling is enforced: Secure Client allows matching queries via the tunnel (other queries can be refused to force failover), but cannot fully prevent leakage of split-DNS-domain queries sent in the clear via the public adapter.

Platform support (Secure Client admin guide): Full split DNS is supported on Windows and macOS. Linux has limited support (see Linux section).

Linux

Tunnel-all Configuration (and Split Tunneling with Tunnel-all-DNS Enabled)

When Secure Client is connected, only tunnel DNS servers are maintained in system DNS configuration.

Split-include / Split-exclude (Tunnel-all-DNS Disabled, No Split-DNS)

Secure Client does not interfere with the native resolver. Tunnel DNS servers are preferred; the initial resolution attempt goes over the tunnel.

Split-DNS (Tunnel-all-DNS Disabled, Split-include Configured)

If split-DNS is enabled, only DNS fallback for split tunneling is enforced on Linux:

- Secure Client allows split-DNS-domain queries via the tunnel.
- Other queries can receive refusal to encourage failover to public DNS.
- Secure Client cannot fully enforce split-DNS-domain queries, as they are never sent in the clear via the public adapter.

The Secure Client admin guide notes limited split DNS on Linux: only tunneled DNS requests are fully subject to split DNS policy; some queries outside the tunnel cannot comply with split DNS policy.

Linux VMs and Containers

Secure Client supports a **tunnel-from-any-source** custom attribute, so packets with any source address can be routed in split-include or split-exclude mode inside VM instances or Docker containers. Refer to the Secure Client 5.x Administrator Guide for configuration details.

Apple iOS (iPhone and iPad)

iOS behavior differs from macOS and is not identical to Windows. If split tunneling is configured without split DNS, DNS queries typically use the global DNS server defined for the device—not the same fallback pattern as Windows.

Practical impact: Split DNS domain entries are often required for reliable internal name resolution when using split tunneling without split DNS.

Historical fix: Cisco bug ID CSCtq09624 - (AnyConnect for iOS 2.5.4038 and later.) Current Secure Client for iOS obeys the same general requirement; configure split DNS for internal domains when using split-include/split and exclude without relying on Windows-style fallback.

Note: iOS DNS queries ignore .local domains (Cisco bug ID CSCts89292.)

Apple treats this as designed behavior; do not expect **.local** resolution through standard split DNS on iOS. On iOS, Secure Client split-DNS behavior also differs from other platforms when split tunneling is combined with certain split-DNS list configurations. Refer to the Secure Client Administrator Guide section Split DNS Resolution Behavior with Split Tunnel for iOS-specific policy combinations (**split-dns none**, **default-domain**, and so on.)

Dynamic Split Tunneling and DNS (Secure Client 4.5+)

Dynamic split tunneling resolves FQDNs at connect time or on demand, and adjusts routing and filters for traffic to specified domains. This is included in or excluded from the tunnel without static IP lists.

Feature	Description
Dynamic split exclude	Domains (**example.com**) are excluded from the tunnel at runtime when applications resolve those names.
Dynamic split include	Domains are dynamically included in the tunnel.
Enhanced dynamic split	Combined include/exclude domain lists with precedence rules (such as excluding **example.com**, but including **mail.example.com**).

Dynamic split tunneling uses DNS resolution to drive routing changes. It is configured via Secure Client custom attributes on the headend (for example **dynamic-split-exclude-domains**, **dynamic-split-include-domains**.)

Dynamic split tunneling applies to **tunnel-all** and **split-exclude** (dynamic exclude) or **split-include** (dynamic include) policies. It does not replace split DNS policy, however, it complements it: split DNS controls which queries are tunneled; dynamic split tunneling controls which IP traffic is tunneled based on resolved names. Refer to the configuration details: Configure Dynamic Split Tunneling and the Secure Client 5.x Administrator Guide.

Split exclude failover (Secure Client 5.x): Optional custom attribute **SplitExcludeFailoverEnabled** routes traffic through the VPN when the public path has no connectivity to split-exclude targets. See the administrator guide for custom attribute setup.

Historical Client Versions (Reference)

The next table applies only to legacy deployments still running obsolete clients:

Version	Relevance
AnyConnect 2.4	Introduced best-effort split DNS fallback
AnyConnect 2.5 (iOS)	Cisco bug ID: CSCtq09624 iOS DNS alignment
AnyConnect 3.0(4235)	True split DNS on Windows; DNS performance fixes
AnyConnect 3.1 (macOS)	Split DNS support with IPv4/IPv6 conditions

Version	Relevance
AnyConnect 4.2	Cisco bug ID: CSCuf07885 adapter-based enforcement; automatic tunnel DNS host routes

Deploy Secure Client 5.x on all supported platforms for current fixes and features.

Related Bug Information

Note: Only registered Cisco users have access to internal Cisco bug tools.

- Cisco bug ID: CSCtn14578 - True split DNS (not fallback) - Windows, 3.0(4235)+
- Cisco bug ID: CSCtq02141 - DNS delay when ISP DNS is on the same subnet as the public IP
- Cisco bug ID: CSCuf07885 - Windows DNS: restrict by adapter, not target server - 4.2+
- Cisco bug ID: CSCtf20226 - macOS split tunnel DNS unlike Windows
- Cisco bug ID: CSCtz86314 - macOS split DNS queries not sent via tunnel
- Cisco bug ID: CSCtq09624 - iOS split tunnel DNS behavior
- Cisco bug ID: CSCts89292 - iOS ignores **.local** DNS domains
- Cisco bug ID: CSCsv34395 - FQDN proxy to DHCP server support

Related Information

- Examine the Behavior of DNS Queries and Domain Name Resolution (Cisco.com) — Document ID 116016
- Cisco Secure Client 5.x Administrator Guide — Configure VPN Access/Split DNS
- Configure ASA/AnyConnect Dynamic Split Tunneling — Document ID 215383
- Enable Tunnel All DNS for Secure Client with Umbrella Module — Document ID 224809
- Interop between AnyConnect and the OpenDNS Roaming Client — Document ID 200395
- Cisco Technical Support & Downloads

Revision History

Revision	Date	Comments
4.0	28-Jul-2026	Full substantive update: Secure Client branding, platform refresh, dynamic split tunneling, Umbrella/tunnel-all-DNS, typo and config fixes, corrected related links

Revision	Date	Comments
3.0	23-May-2024	Recertification (Cisco.com)
1.0	12-Jun-2014	Initial release

Document Applies to

- Cisco Secure Client (including AnyConnect) — Windows, macOS, Linux, iOS
- Cisco Secure Firewall ASA and FTD Remote Access VPN Group Policies