Examine the Behavior of DNS Queries and Domain Name Resolution

Contents

Introduction

This document describes how Cisco OS® handles DNS queries and the effects on domain name resolution with Cisco AnyConnect and split or full tunneling.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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

When you use split-include tunneling, these are the three options you have for the Domain Name System (DNS):

1. **Split DNS** - The DNS queries which matches the domain names, are configured on the Cisco Adaptive Security Appliance (ASA). They move through the tunnel (to the DNS servers that are defined on the ASA, for example) while others do not.

2. **Tunnel-all-DNS** - Only DNS traffic to the DNS servers which are defined by the ASA is allowed. This setting is configured in the group policy.

3. **Standard DNS** - All of the DNS queries move through the DNS servers which are defined by the ASA. In the case of a negative response, the DNS queries can also go to the DNS servers which are configured on the physical adapter.

Note: The **split-tunnel-all-dns** command was first implemented in ASA Version 8.2(5). Before this version, you could only do split DNS or standard DNS.

In all cases, the DNS queries which are defined to move through the tunnel, go to any DNS servers which are defined by ASA. If there are no DNS servers defined by the ASA, then the DNS settings are blank for the tunnel. If you do not have split DNS defined, then all of the DNS queries are sent to the DNS servers which are defined by the ASA. However, the behaviors that are described in this document can be different, based on the Operating System (OS).

Note: Avoid the use of the NSLookup when you test the name resolution on the client. Instead, rely on a browser or use the **ping** command. This is because NSLookup does not rely on the OS DNS resolver. AnyConnect does not force the DNS request via a certain interface but allows it or rejects it dependent on the split DNS configuration. In order to force the DNS resolver to try an acceptable DNS server for a request, it is important that split DNS testing is only performed with applications that rely on the native DNS resolver for domain name resolution (all applications except NSLookup, Dig, and similar applications that handle DNS resolution by themselves, for example).

True Versus Best Effort Split DNS

AnyConnect Release 2.4 supports split DNS Fallback (best effort split DNS), which is not the true split DNS and is found in the legacy IPsec client. If the request matches a split DNS domain, AnyConnect allows the request to be tunneled into the ASA. If the server cannot resolve the host name, the DNS resolver continues and sends the same query to the DNS server that is mapped to the physical interface.

On the other hand, if the request does not match any of the split DNS domains, AnyConnect does not tunnel it into the ASA. Instead, it builds a DNS response so that the DNS resolver falls back and sends the query to the DNS server that is mapped to the physical interface. That is why this feature is not called split DNS, but DNS fallback for split tunneling. Not only does AnyConnect assure that only requests that target split DNS domains are tunneled in, it also relies on the client OS DNS resolver behavior for host name resolution.

This raises security concerns due to a potential private domain name leak. For example, the native DNS client can send a query for a private domain name to a public DNS server specifically when the VPN DNS name server could not resolve the DNS query.

Refer to Cisco bug ID CSCtn14578, currently resolved on Microsoft Windows only, as of Version 3.0(4235). The solution implements true split DNS, it strictly queries the configured domain names that matches and are allowed to the VPN DNS servers. All other queries are only allowed to other DNS servers, such as those configured on the physical adapter(s).

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

Tunnel-all and Tunnel-all DNS

When split tunneling is disabled (the **Tunnel-all** configuration), DNS traffic is allowed strictly via tunnel. The **Tunnel-all DNS** configuration (configured in the group policy) sends all of the DNS lookups through the tunnel, along with some type of split tunneling, and DNS traffic is allowed strictly via tunnel.

This is consistent across platforms with one caveat on Microsoft Windows: when any **Tunnel-all** or **Tunnel-all DNS** is configured, AnyConnect allows DNS traffic strictly to the DNS servers that are configured on the secure gateway (applied to the VPN adapter). This is a security enhancement implemented along with the previously mentioned true split DNS solution.

If this proves problematic in certain scenarios (for example, DNS update/registration requests must be sent to non-VPN DNS servers), then complete these steps:

1. If the current configuration is Tunnel-all, then enable **split-exclude tunneling** . Any single-host, split-exclude network is acceptable for use, such as a link-local address.

2. Ensure that **Tunnel-all DNS** is not configured in the group policy.

DNS Performance Issue Resolved in AnyConnect Version 3.0(4235)

This Microsoft Windows issue is mostly prevalent under these conditions:

- With the home router setup, the DNS and DHCP servers are assigned the same IP address (AnyConnect creates a necessary route to the DHCP server).
- A large number of DNS domains are in the group policy.
- A **Tunnel-all** configuration is used.
- The name resolution is performed by a non-qualified host name, which implies that the resolver must try a number of DNS suffixes on all of the available DNS servers until the one relevant to the queried host name is attempted. This issue is due to the native DNS client that attempts to send DNS queries via the physical adapter, which AnyConnect blocks (given the **Tunnel-all** configuration). This leads to a name resolution delay that can be significant, especially if a large number of DNS suffixes are pushed by the headend. The DNS client must walk through all of the queries and available DNS servers until it receives a positive response.

This problem is resolved in AnyConnect Version 3.0(4235). Refer to Cisco bug IDs CSCtq02141 and Cisco bug ID CSCtn14578, along with the introduction to the previously-mentioned true split DNS solution, for more information.

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

If an upgrade cannot be implemented, then these are the possible workarounds:

- Enable **split-exclude tunneling** for an IP address, which allows the local DNS requests to flow through the physical adapter. You can use an address from the linklocal subnet **169.254.0.0/16** because it is unlikely that any device sends traffic to one of those IP addresses over the VPN. After you enable the **split-exclude tunnelingd**, enable local LAN access on the client profile or on the client itself, and disable **Tunnel-all dDNS**.

  On the ASA, make these configuration changes:

  ```
  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
  ```

On the client profile, you must add this line:

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

You can also enable this on a per-client basis in the AnyConnect client GUI. Navigate to the **AnyConnect Preference** menu, and check the **Enable local LAN access** check-box.

- Use the fully qualified domain names (FQDNs) instead of the unqualified host names for the name resolutions.
- Use a different IP address for the DNS server on the physical interface.

DNS with Split Tunneling on the Different Cisco OS

The different Cisco OS handle DNS searches in different ways when used with split tunneling (without split DNS) for AnyConnect. This section describes those differences.

Microsoft Windows

On Microsoft Windows systems, DNS settings are per-interface. If split tunneling is used, DNS queries can fall back to the physical adaptor DNS servers after they fail on the VPN tunnel adaptor. If split tunneling without split DNS is defined, then both internal and external DNS resolution works because it falls back to the external DNS servers.

There has been a change in behavior in the DNS mechanism that handles this on AnyConnect for Windows, in release 4.2 after the fix for Cisco bug ID CSCuf07885.

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

Windows 7+

Tunnel-all configuration (and split-tunneling with tunnel-all DNS enabled)

Pre AnyConnect 4.2:

Only DNS requests to DNS servers configured under the group-policy (tunnel DNS servers) are allowed. The AnyConnect driver responds to all other requests with a "no such name" response. As a result, DNS resolution can only be performed with the tunnel DNS servers.

AnyConnect 4.2 +

DNS requests to any DNS servers are allowed, as long as they originated from the VPN adapter and are sent across the tunnel. All other requests are responded with **no such name** , and DNS resolution can only be performed via the VPN tunnel.

Prior to Cisco bug ID CSCuf07885 fix, AC restricted the target DNS servers, however with the fix for this bug, it now restricts which network adapters can initiate DNS requests.

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

Split-include configuration (tunnel-all DNS disabled and no split-DNS)

AnyConnect driver does not interfere with the native DNS resolver. Therefore, DNS resolution is performed based on the order of network adapters where AnyConnect is always the preferred adapter when VPN is connected. Moreover, a DNS query is first sent via the tunnel and if it does not get resolved, the resolver attempts to resolve it via public interface. The split-include access-list includes the subnet which covers the Tunnel DNS server(s). To start with AnyConnect 4.2, host routes for the Tunnel DNS server(s) are automatically added as split-include networks (secure routes) by the AnyConnect client, and therefore the split-include access-list no longer requires explicit addition of the tunnel DNS server subnet.

Split-exclude configuration (tunnel-all DNS disabled and no split-DNS)

AnyConnect driver does not interfere with the native DNS resolver. Therefore, DNS resolution is performed based on the order of network adapters where AnyConnect is always the preferred adapter when VPN is connected. Moreover, a DNS query is first sent via the tunnel and if it does not get resolved, the resolver attempts to resolve it via public interface. The split-exclude access-list must not include the subnet that covers the Tunnel DNS server(s). To start with AnyConnect 4.2, host routes for the Tunnel DNS server(s) are automatically added as split-include networks (secure routes) by the AnyConnect client, and therefore prevents the misconfiguration in the split-exclude access-list.

Split-DNS (tunnel-all DNS disabled, split-include configured)

Pre AnyConnect 4.2

DNS requests, which matches with the split-dns domains are allowed to tunnel DNS servers, but are not allowed to other DNS servers. To prevent such internal DNS queries from leaking out the tunnel, the AnyConnect driver responds with "no such name" if the query is sent to other DNS servers. Therefore, the split-dns domains can only be resolved via tunnel DNS servers.

DNS requests, which does not match with the split-dns domains are allowed to other DNS servers, but are not allowed to tunnel DNS servers. Even in this case, the AnyConnect driver responds with "no such name" if a query for non split-dns domains is attempted via tunnel. Therefore, the non split-dns domains can only be resolved via public DNS servers outside the tunnel.

AnyConnect 4.2 +

DNS requests, which matches with the split-dns domains are allowed to any DNS servers, as long as they originate from the VPN adapter. If the query is originated by the public interface, AnyConnect driver responds with a "no such name" to force the resolver to always use the tunnel for name resolution. Therefore, the split-dns domains can only be resolved via tunnel.

DNS requests, which does not match with the split-dns domains are allowed to any DNS servers as long as they originate from the physical adapter. If the query is originated by the VPN adapter, AnyConnect responds with "no such name" to force the resolver to always attempt the name resolution via the public interface. Therefore, the non split-dns domains can only be resolved via public interface.

Mac OSx

On Macintosh systems, the DNS settings are global. If split tunneling is used, but split DNS is not used, it is not possible for the DNS queries to reach DNS servers outside of the tunnel. You can only resolve internally, not externally.

This is documented in Cisco bug ID CSCtf20226 and Cisco bug ID CSCtz86314. In both cases, this workaround must resolve the issue:

- Specify an external DNS server IP address under the group policy and use a FQDN for the internal DNS queries.
- If the external names are resolvable through the tunnel, then navigate to **Advanced > Split Tunneling** and disable split DNS via removal of the DNS names that are configured in the group policy. This requires the use of a FQDN for the internal DNS queries.

The split DNS case is resolved in AnyConnect Version 3.1. However, you must ensure that one of these conditions is met:

- Split DNS must be enabled for both IP protocols, which requires Cisco ASA Version 9.0 or later.
- Split DNS must be enabled for one IP protocol. If you run Cisco ASA Version 9.0 or later, then use client bypass protocol for the other IP protocol. For example, ensure that there is no address pool and that **Client Bypass Protocol** is enabled in the group policy. Alternatively, if you run an ASA version which is earlier than Version 9.0, ensure that there is no address pool configured for the other IP protocol. This implies that the other IP protocol is IPv6.

Note: AnyConnect does not change the **resolv.conf** file on Macintosh OS X, but rather changes OS X-specific DNS settings. Macintosh OS X keeps the **resolv.conf** file current for compatibility reasons. Use the **scutil --dns** command in order to view the DNS settings on Macintosh OS X.

Tunnel-all configuration (and split-tunneling with tunnel-all DNS enabled)

When AnyConnect is connected, only Tunnel DNS servers are maintained in the system DNS configuration, and therefore DNS requests can only be sent to the Tunnel DNS server(s).

Split-include configuration (tunnel-all DNS disabled and no split-DNS)

AnyConnect does not interfere with the native DNS resolver. The tunnel DNS servers are configured as preferred resolvers, which takes precedence over public DNS servers, thus it ensures that the initial DNS request for a name resolution is sent over the tunnel. Since DNS settings are global on Mac OS X, it is not possible for DNS queries to use public DNS servers outside the tunnel as documented in Cisco bug ID CSCtf20226 . To start with AnyConnect 4.2, host routes for the Tunnel DNS server(s) are automatically added as split-include networks (secure routes) by the AnyConnect client, and therefore the split-include access-list no longer requires explicit addition of the tunnel DNS server subnet.

Split-exclude configuration (tunnel-all DNS disabled and no split-DNS)

AnyConnect does not interfere with the native DNS resolver. The tunnel DNS servers are configured as preferred resolvers, they take precedence over public DNS servers, thus this ensures that the initial DNS request for a name resolution is sent over the tunnel. Since DNS settings are global on Mac OS X, it is not possible for DNS queries to use public DNS servers outside the tunnel as documented in Cisco bug ID CSCtf20226 . To start with AnyConnect 4.2, host routes for the Tunnel DNS server(s) are automatically added as split-include networks (secure routes) by the AnyConnect client, and therefore the split-include access-list no longer requires explicit addition of the tunnel DNS server subnet.

Split-DNS (tunnel-all DNS disabled, split-include configured)

If split-DNS is enabled for both IP protocols (IPv4 and IPv6) or it is only enabled for one protocol and there is no address pool configured for the other protocol:
True split-DNS, similar to Windows, is enforced. True split-DNS means that request which matches with the split-DNS domains are only resolved via the tunnel, they are not leaked to DNS servers outside the

tunnel.

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. This means AC only allows DNS request which matches the split-DNS domains via tunnel (other requests are replied by AC with "refused" response to force failover to public DNS servers), but cannot enforce the request which matches with the split-DNS domains that are not sent in the clear, via public adapter.

Linux

Tunnel-all configuration (and split-tunneling with tunnel-all DNS enabled)

When AnyConnect is connected, only Tunnel DNS servers are maintained in the system DNS configuration, and therefore DNS requests can only be sent to the Tunnel DNS server(s).

Split-include configuration (tunnel-all DNS disabled and no split-DNS)

AnyConnect does not interfere with the native DNS resolver. The tunnel DNS servers are configured as preferred resolvers, which takes precedence over public DNS servers, thus it ensures that the initial DNS request for a name resolution is sent over the tunnel.

Split-exclude configuration (tunnel-all DNS disabled and no split-DNS)

AnyConnect does not interfere with the native DNS resolver. The tunnel DNS servers are configured as preferred resolvers, which takes precedence over public DNS servers, thus it ensures that the initial DNS request for a name resolution is sent 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. This means AC only allows DNS request which matches with the split-DNS domains via tunnel (other requests are replied by AC with "refused" response to force failover to public DNS servers), but cannot enforce that request which matches with the split-DNS domains that are not sent in the clear, via the public adapter.

iPhone

The iPhone is the complete opposite of the Macintosh system and is not similar to Microsoft Windows. If split tunneling is defined but split DNS is not defined, then DNS queries exit through the global DNS server that is defined. For example, split DNS domain entries are mandatory for internal resolution. This behavior is documented in Cisco bug ID CSCtq09624 and is fixed in Version 2.5.4038 for the Apple iOS AnyConnect client.

Note: Be aware that the iPhone DNS queries ignore **.local domains**. This is documented in Cisco bug ID CSCts89292. Apple engineers confirm that the issue is caused by the functionality of the OS. This is the designed behavior, and Apple confirms there is no change for it.

Related Bug Informaton

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

- **Cisco bug ID CSCsv34395 - Add support in AnyConnect for that proxies the FQDN to DHCP server**
- **Cisco bug ID CSCtn14578 - AnyConnect to support true split DNS; not fallback**
- **Cisco bug ID CSCtq02141 - AnyConnect DNS issue when ISP DNS is on same subnet as Public IP**
- **Cisco bug ID CSCtf20226 - Make AnyConnect DNS w/ split tunnel behavior for Mac same as windows**
- **Cisco bug ID CSCtz86314 - Mac: DNS queries incorrectly not sent via the tunnel with split DNS**
- **Cisco bug ID CSCtq09624 - Make AnyConnect iPhone DNS w/ split tunneling behavior same as Windows**
- **Cisco bug ID CSCts89292 - AC for iPhone DNS queries ignore .local domains**

Related Information

- **Cisco IOS® Firewall**
- **Cisco Technical Support & Downloads**