Untersuchen des Verhaltens von DNS-Abfragen und der Domänennamenauflösung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Cisco OS® DNS-Abfragen verarbeitet und welche Auswirkungen Cisco AnyConnect und Split- oder Full-Tunneling auf die Auflösung von Domänennamen haben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Split versus Standard-DNS

Wenn Sie Split-Include-Tunneling verwenden, stehen Ihnen die folgenden drei Optionen für das Domain Name System (DNS) zur Verfügung:

1. Split DNS: Die DNS-Abfragen, die den Domänennamen entsprechen, werden auf der Cisco Adaptive Security Appliance (ASA) konfiguriert. Sie durchlaufen den Tunnel (z. B. zu den DNS-Servern, die auf der ASA definiert sind), andere dagegen nicht.

2. Tunnel-all-DNS - Nur DNS-Datenverkehr zu den DNS-Servern, die von der ASA definiert werden, ist zulässig. Diese Einstellung wird in der Gruppenrichtlinie konfiguriert.

3. Standard-DNS - Alle DNS-Abfragen durchlaufen die DNS-Server, die von der ASA definiert werden. Bei einer negativen Antwort können die DNS-Abfragen auch an die DNS-Server geleitet werden, die auf dem physischen Adapter konfiguriert sind.

Hinweis: Der Befehl split-tunnel-all-dns wurde zuerst in ASA Version 8.2(5) implementiert. Vor dieser Version konnten Sie nur Split-DNS oder Standard-DNS.

In allen Fällen werden die DNS-Abfragen, die so definiert sind, dass sie sich durch den Tunnel bewegen, an alle DNS-Server gesendet, die von der ASA definiert werden. Wenn von der ASA keine DNS-Server definiert wurden, sind die DNS-Einstellungen für den Tunnel leer. Wenn Sie keinen Split-DNS definiert haben, werden alle DNS-Abfragen an die DNS-Server gesendet, die von der ASA definiert werden. Die in diesem Dokument beschriebenen Verhaltensweisen können je nach Betriebssystem jedoch unterschiedlich sein.

Hinweis: Vermeiden Sie die Verwendung von NSLookup, wenn Sie die Namensauflösung auf dem Client testen. Verwenden Sie stattdessen einen Browser, oder verwenden Sie den Befehl ping. Dies liegt daran, dass NSLookup nicht auf den DNS-Resolver des Betriebssystems angewiesen ist. AnyConnect erzwingt die DNS-Anforderung nicht über eine bestimmte Schnittstelle, lässt sie jedoch zu oder lehnt sie in Abhängigkeit von der geteilten DNS-Konfiguration ab. Um den DNS-Resolver zu zwingen, einen akzeptablen DNS-Server für eine Anforderung zu testen, ist es wichtig, dass Split-DNS-Tests nur mit Anwendungen

---

durchgeführt werden, die für die Auflösung von Domänennamen auf dem nativen DNS-Resolver basieren (alle Anwendungen mit Ausnahme von NSLookup, Dig und ähnlichen Anwendungen, die die DNS-Auflösung beispielsweise selbst verarbeiten).

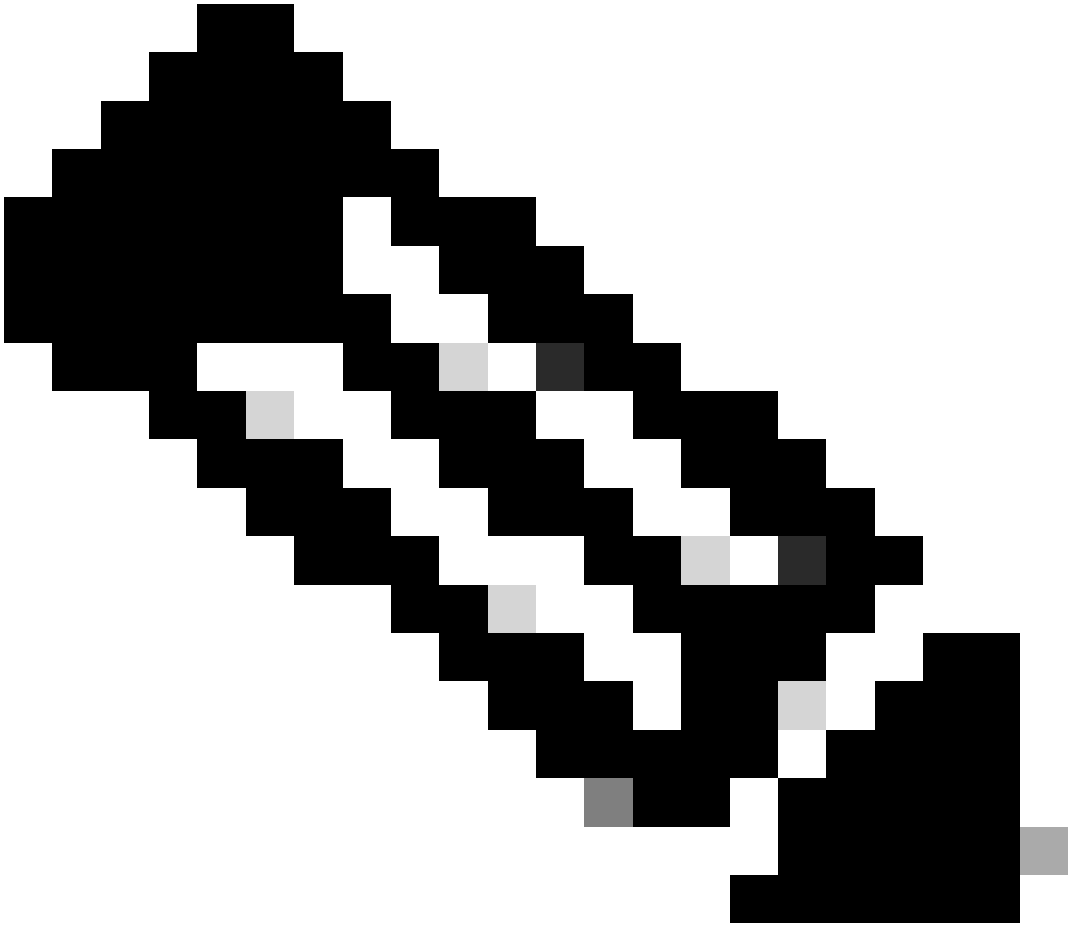
True versus Best Effort Split DNS

AnyConnect Release 2.4 unterstützt Split DNS Fallback (Best Effort Split DNS), das nicht der echte Split DNS ist und im Legacy-IPsec-Client zu finden ist. Wenn die Anforderung mit einer geteilten DNS-Domäne übereinstimmt, ermöglicht AnyConnect das Tunneling der Anforderung in die ASA. Wenn der Server den Hostnamen nicht auflösen kann, wird der DNS-Resolver fortgesetzt und sendet dieselbe Abfrage an den DNS-Server, der der physischen Schnittstelle zugeordnet ist.

Wenn die Anforderung jedoch mit keiner der geteilten DNS-Domänen übereinstimmt, tunnelt AnyConnect sie nicht in die ASA. Stattdessen wird eine DNS-Antwort erstellt, sodass der DNS-Resolver zurückfällt und die Abfrage an den DNS-Server sendet, der der physischen Schnittstelle zugeordnet ist. Aus diesem Grund wird diese Funktion nicht als Split-DNS, sondern als DNS-Fallback für Split-Tunneling bezeichnet. AnyConnect stellt nicht nur sicher, dass nur Anforderungen, die geteilte DNS-Zieldomänen betreffen, eingetunnelt werden, sondern setzt auch das DNS-Auflösungsverhalten des Client-Betriebssystems für die Auflösung von Hostnamen voraus.

Dies wirft Sicherheitsbedenken auf, da möglicherweise ein privater Domain-Namen-Leak vorliegt. Beispielsweise kann der native DNS-Client eine Abfrage für einen privaten Domänennamen an einen öffentlichen DNS-Server senden, wenn der VPN-DNS-Namensserver die DNS-Abfrage nicht auflösen konnte.

Weitere Informationen finden Sie unter der Cisco Bug-ID CSCtn14578, die derzeit nur unter Microsoft Windows behoben wurde, ab Version 3.0(4235). Die Lösung implementiert True-Split-DNS und fragt nur die konfigurierten Domänennamen ab, die mit den VPN-DNS-Servern übereinstimmen und für diese zulässig sind. Alle anderen Abfragen sind nur für andere DNS-Server zulässig, z. B. für die physischen Adapter konfigurierte Abfragen.



Hinweis: Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Informationen von Cisco.

Tunnel-all und Tunnel-all DNS

Wenn Split-Tunneling deaktiviert ist (die Tunnel-all-Konfiguration), wird DNS-Datenverkehr ausschließlich über den Tunnel zugelassen. Die Tunnel-all DNS-Konfiguration (konfiguriert in der Gruppenrichtlinie) sendet alle DNS-Lookups durch den Tunnel, zusammen mit einer Art von Split-Tunneling, und der DNS-Verkehr wird ausschließlich über den Tunnel zugelassen.

Dies ist plattformübergreifend konsistent, wobei unter Microsoft Windows nur ein einziger Vorbehalt gilt: Wenn ein Tunnel-all- oder Tunnel-all-DNS konfiguriert ist, lässt AnyConnect den DNS-Datenverkehr ausschließlich zu den DNS-Servern, die auf dem sicheren Gateway konfiguriert sind (auf den VPN-Adapter angewendet). Dies ist eine Sicherheitserweiterung, die zusammen mit der zuvor erwähnten echten Split-DNS-Lösung implementiert wurde.

Wenn sich dies in bestimmten Szenarien als problematisch erweist (z. B. müssen DNS-Update-

/Registrierungsanforderungen an Nicht-VPN-DNS-Server gesendet werden), führen Sie die folgenden Schritte aus:

1. Wenn die aktuelle Konfiguration Tunnel-all lautet, aktivieren Sie Split-Exclude Tunneling. Jedes Netzwerk mit einem Host und Split-Exclusion ist zulässig, z. B. eine Link-Local-Adresse.

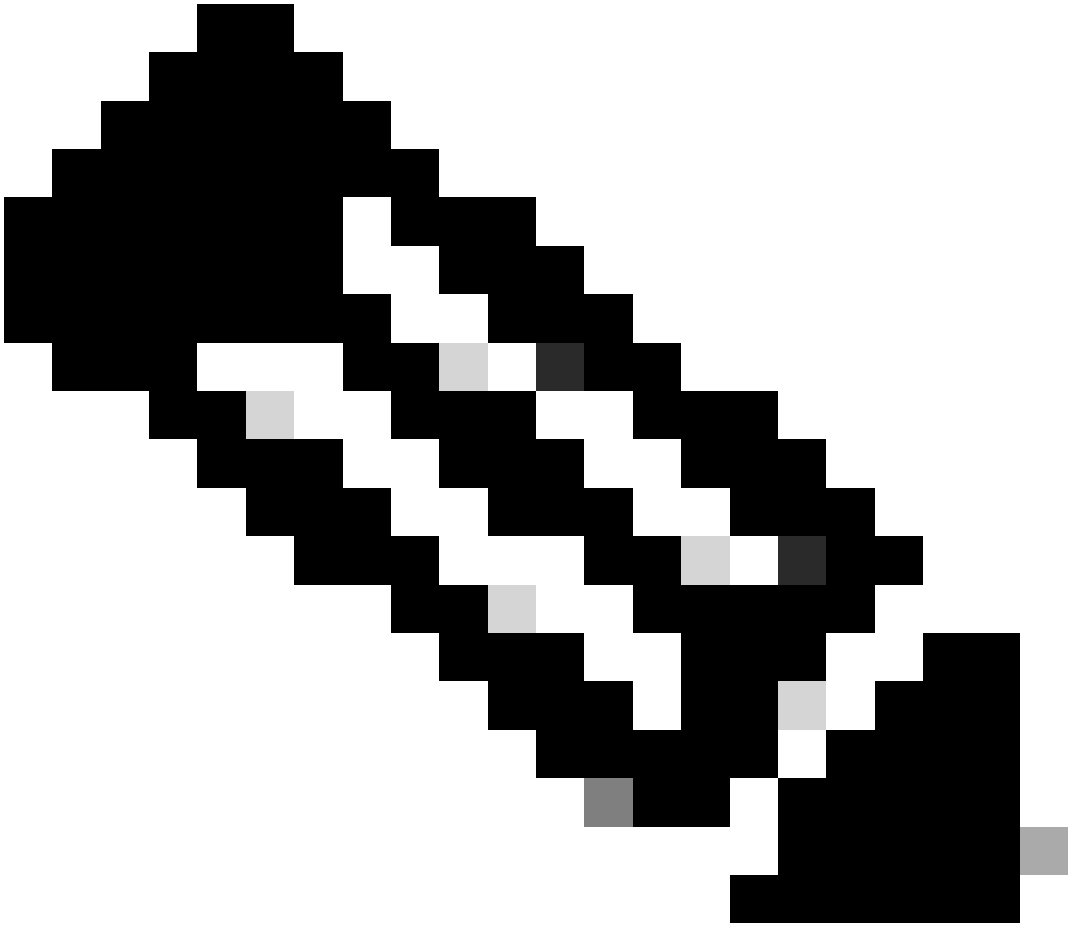
2. Stellen Sie sicher, dass Tunnel-all DNS nicht in der Gruppenrichtlinie konfiguriert ist.

DNS-Leistungsproblem in AnyConnect Version 3.0 behoben (4235)

Dieses Microsoft Windows-Problem tritt vor allem unter den folgenden Bedingungen auf:

- Beim Home-Router-Setup erhalten die DNS- und DHCP-Server dieselbe IP-Adresse (AnyConnect erstellt eine erforderliche Route zum DHCP-Server).
- Die Gruppenrichtlinie enthält eine große Anzahl von DNS-Domänen.
- Es wird eine Tunnel-all-Konfiguration verwendet.
- Die Namensauflösung erfolgt über einen nicht qualifizierten Hostnamen. Dies bedeutet, dass der Resolver eine Reihe von DNS-Suffixen auf allen verfügbaren DNS-Servern ausprobieren muss, bis der für den abgefragten Hostnamen relevante versucht wird. Dieses Problem ist auf den nativen DNS-Client zurückzuführen, der versucht, DNS-Abfragen über den physischen Adapter zu senden, der von AnyConnect blockiert wird (bei der Tunnel-all-Konfiguration). Dies führt zu einer Verzögerung bei der Namensauflösung, die erheblich sein kann, insbesondere wenn eine große Anzahl von DNS-Suffixen vom Headend weitergeleitet wird. Der DNS-Client muss alle Abfragen und verfügbaren DNS-Server durchlaufen, bis er eine positive Antwort erhält.

Dieses Problem wurde in AnyConnect Version 3.0(4235) behoben. Weitere Informationen finden Sie unter den Cisco Bug-IDs CSCtq02141 und Cisco Bug-ID CSCtn14578 sowie in der Einführung in die zuvor erwähnte echte Split-DNS-Lösung.



Hinweis: Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Informationen von Cisco.

Wenn ein Upgrade nicht implementiert werden kann, sind folgende Problemumgehungen möglich:

- Aktivieren Sie Split-Exclude-Tunneling für eine IP-Adresse, sodass die lokalen DNS-Anfragen durch den physischen Adapter fließen können. Sie können eine Adresse aus dem linklocal-Subnetz 169.254.0.0/16 verwenden, da es unwahrscheinlich ist, dass ein Gerät Datenverkehr über das VPN an eine dieser IP-Adressen sendet. Nachdem Sie den Split-Exclude-Tunnel aktiviert haben, aktivieren Sie im Clientprofil oder auf dem Client selbst den lokalen LAN-Zugriff, und deaktivieren Sie Tunnel-all dDNS.

  Nehmen Sie auf der ASA die folgenden Konfigurationsänderungen vor:

```
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
```

Im Clientprofil müssen Sie folgende Zeile hinzufügen:

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

Sie können dies auch auf Client-Basis in der AnyConnect-Client-GUI aktivieren. Navigieren Sie zum Menü AnyConnect Preference (AnyConnect-Voreinstellungen), und aktivieren Sie das Kontrollkästchen Enable local LAN access (Lokalen LAN-Zugriff aktivieren).

- Verwenden Sie für die Namensauflösungen vollqualifizierte Domänennamen (Fully Qualified Domain Names, FQDNs) anstelle der unqualifizierten Hostnamen.
- Verwenden Sie eine andere IP-Adresse für den DNS-Server auf der physischen Schnittstelle.

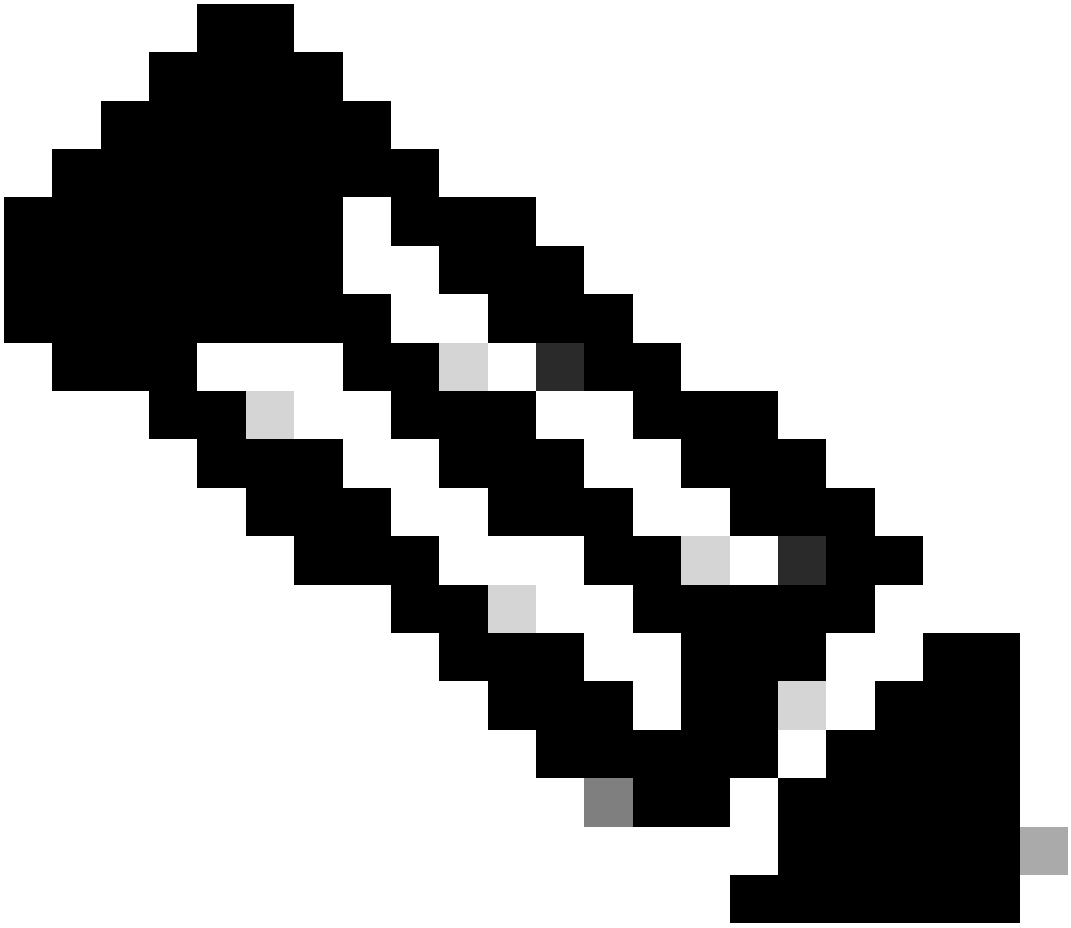
DNS mit Split Tunneling auf den verschiedenen Cisco Betriebssystemen

Die verschiedenen Cisco Betriebssysteme verarbeiten DNS-Suchen auf unterschiedliche Weise, wenn sie mit Split-Tunneling (ohne Split-DNS) für AnyConnect verwendet werden. In diesem Abschnitt werden diese Unterschiede beschrieben.

Microsoft Windows

Auf Microsoft Windows-Systemen sind die DNS-Einstellungen schnittstellenabhängig. Wenn Split-Tunneling verwendet wird, können DNS-Abfragen auf die DNS-Server des physischen Adapters zurückgreifen, nachdem sie auf dem VPN-Tunneladapter fehlschlagen. Wenn Split-Tunneling ohne Split-DNS definiert ist, funktioniert die interne und externe DNS-Auflösung, da sie auf die externen DNS-Server zurückfällt.

Es gab eine Verhaltensänderung im DNS-Mechanismus, der dies auf AnyConnect für Windows behandelt, in Version 4.2 nach der Behebung des Fehlers für die Cisco Bug-ID CSCuf07885.



Hinweis: Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Informationen von Cisco.

Windows 7 oder höher

Konfiguration "Tunnel-all" (und Split-Tunneling mit aktiviertem "tunnel-all DNS")

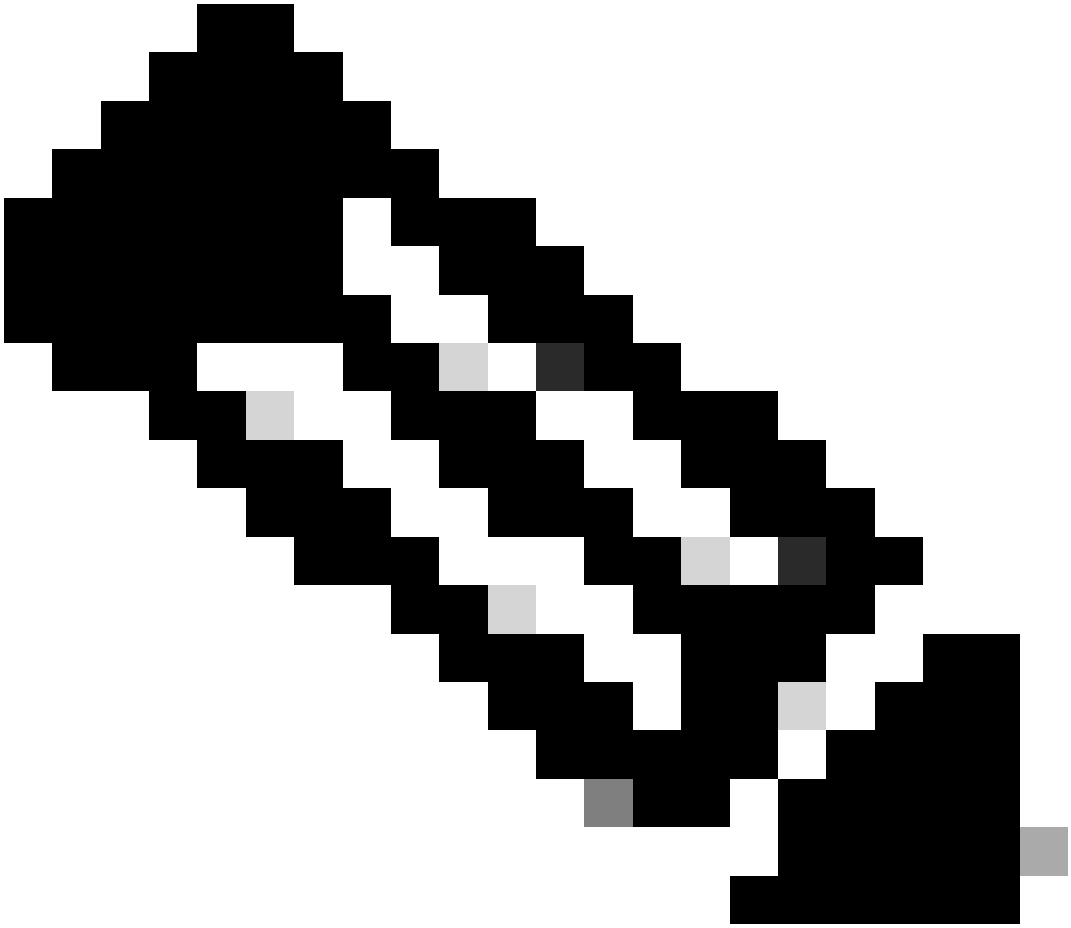
Vor AnyConnect 4.2:

Es sind nur DNS-Anfragen an DNS-Server zulässig, die unter der Gruppenrichtlinie (Tunnel-DNS-Server) konfiguriert wurden. Der AnyConnect-Treiber antwortet auf alle anderen Anfragen mit der Antwort "Kein solcher Name". Daher kann die DNS-Auflösung nur mit den Tunnel-DNS-Servern durchgeführt werden.

AnyConnect 4.2 und

DNS-Anfragen an beliebige DNS-Server sind zulässig, sofern sie vom VPN-Adapter stammen und über den Tunnel gesendet werden. Alle anderen Anfragen werden mit keinem solchen Namen beantwortet, und die DNS-Auflösung kann nur über den VPN-Tunnel durchgeführt werden.

Vor der Cisco Bug-ID CSCuf0785 Fix hat AC die Ziel-DNS-Server eingeschränkt. Mit der Behebung dieses Fehlers wird nun jedoch eingeschränkt, welche Netzwerkadapter DNS-Anfragen initiieren können.



> Hinweis: Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Informationen von Cisco.

Split-include-Konfiguration (tunnel-all DNS deaktiviert und kein split-DNS)

Der AnyConnect-Treiber beeinträchtigt den nativen DNS-Resolver nicht. Aus diesem Grund wird

die DNS-Auflösung in der Reihenfolge der Netzwerkadapter vorgenommen, bei denen AnyConnect bei VPN-Verbindungen immer der bevorzugte Adapter ist. Darüber hinaus wird zunächst eine DNS-Abfrage über den Tunnel gesendet, und wenn sie nicht aufgelöst wird, versucht der Resolver, sie über eine öffentliche Schnittstelle aufzulösen. Die split-include-Zugriffsliste enthält das Subnetz, das den/die Tunnel-DNS-Server abdeckt. Um mit AnyConnect 4.2 zu beginnen, werden vom AnyConnect-Client automatisch Host-Routen für den/die Tunnel-DNS-Server als Split-Include-Netzwerke (sichere Routen) hinzugefügt. Daher erfordert die Split-Include-Zugriffsliste keine explizite Hinzufügung des Tunnel-DNS-Server-Subnetzes mehr.

Split-exclude-Konfiguration (tunnel-all DNS disabled und no split-DNS)

Der AnyConnect-Treiber beeinträchtigt den nativen DNS-Resolver nicht. Aus diesem Grund wird die DNS-Auflösung in der Reihenfolge der Netzwerkadapter vorgenommen, bei denen AnyConnect bei VPN-Verbindungen immer der bevorzugte Adapter ist. Darüber hinaus wird zunächst eine DNS-Abfrage über den Tunnel gesendet, und wenn sie nicht aufgelöst wird, versucht der Resolver, sie über eine öffentliche Schnittstelle aufzulösen. Die Split-Exclude-Zugriffsliste darf nicht das Subnetz enthalten, das die Tunnel-DNS-Server abdeckt. Um mit AnyConnect 4.2 zu beginnen, werden vom AnyConnect-Client automatisch Host-Routen für den/die Tunnel-DNS-Server als Split-Include-Netzwerke (sichere Routen) hinzugefügt und verhindern so die Fehlkonfiguration in der Split-Exclude-Zugriffsliste.

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

Vor AnyConnect 4.2

DNS-Anfragen, die mit den Split-DNS-Domänen übereinstimmen, dürfen DNS-Server tunneln, aber nicht mit anderen DNS-Servern. Um zu verhindern, dass solche internen DNS-Abfragen den Tunnel verlassen, antwortet der AnyConnect-Treiber mit "no such name" (Kein solcher Name), wenn die Abfrage an andere DNS-Server gesendet wird. Daher können die split-dns-Domänen nur über Tunnel-DNS-Server aufgelöst werden.

DNS-Anfragen, die nicht mit den Split-DNS-Domänen übereinstimmen, sind für andere DNS-Server zulässig, jedoch nicht für das Tunneling von DNS-Servern. Selbst in diesem Fall antwortet der AnyConnect-Treiber mit "no such name" (Kein solcher Name), wenn über Tunnel eine Abfrage nach Nicht-Split-DNS-Domänen versucht wird. Daher können die Nicht-Split-DNS-Domänen nur über öffentliche DNS-Server außerhalb des Tunnels aufgelöst werden.

AnyConnect 4.2 und

DNS-Anfragen, die mit den Split-DNS-Domänen übereinstimmen, sind auf allen DNS-Servern zulässig, sofern sie vom VPN-Adapter stammen. Wenn die Abfrage von der öffentlichen Schnittstelle generiert wird, antwortet der AnyConnect-Treiber mit einem "no such name" (Kein solcher Name), um den Resolver zu zwingen, den Tunnel immer für die Namensauflösung zu

verwenden. Daher können die split-dns-Domänen nur über einen Tunnel aufgelöst werden.

DNS-Anfragen, die nicht mit den Split-DNS-Domänen übereinstimmen, sind auf allen DNS-Servern zulässig, solange sie vom physischen Adapter stammen. Wenn die Abfrage vom VPN-Adapter generiert wird, antwortet AnyConnect mit "no such name" (Kein solcher Name), um den Resolver zu zwingen, immer die Namensauflösung über die öffentliche Schnittstelle zu versuchen. Daher können die Nicht-Split-DNS-Domänen nur über eine öffentliche Schnittstelle aufgelöst werden.

Mac OSx

Auf Macintosh-Systemen sind die DNS-Einstellungen global. Wenn Split-Tunneling verwendet wird, Split-DNS jedoch nicht verwendet wird, ist es für die DNS-Abfragen nicht möglich, DNS-Server außerhalb des Tunnels zu erreichen. Sie können nur intern lösen, nicht extern.

Dies ist dokumentiert in Cisco Bug-ID CSCtf2026 und Cisco Bug-ID CSCtz86314. In beiden Fällen muss das Problem durch diese Problemumgehung behoben werden:

- Geben Sie unter der Gruppenrichtlinie eine externe IP-Adresse für den DNS-Server an, und verwenden Sie einen FQDN für die internen DNS-Abfragen.

- Wenn die externen Namen im Tunnel auflösbar sind, navigieren Sie zu Advanced > Split Tunneling, und deaktivieren Sie Split DNS, indem Sie die in der Gruppenrichtlinie konfigurierten DNS-Namen entfernen. Dies erfordert die Verwendung eines FQDN für die internen DNS-Abfragen.

Das Problem mit dem geteilten DNS wurde in AnyConnect Version 3.1 behoben. Sie müssen jedoch sicherstellen, dass eine der folgenden Bedingungen erfüllt ist:

- Split DNS muss für beide IP-Protokolle aktiviert sein. Hierfür ist Cisco ASA Version 9.0 oder höher erforderlich.

- Split DNS muss für ein IP-Protokoll aktiviert sein. Wenn Sie Cisco ASA Version 9.0 oder höher ausführen, verwenden Sie das Client-Umgehungsprotokoll für das andere IP-Protokoll. Stellen Sie beispielsweise sicher, dass es keinen Adresspool gibt und dass Client Bypass Protocol in der Gruppenrichtlinie aktiviert ist. Wenn Sie eine ASA-Version vor Version 9.0 ausführen, stellen Sie alternativ sicher, dass kein Adresspool für das andere IP-Protokoll konfiguriert ist. Dies impliziert, dass das andere IP-Protokoll IPv6 ist.

Hinweis: AnyConnect ändert nicht die Datei resolv.conf unter Macintosh OS X, sondern die OS X-spezifischen DNS-Einstellungen. Macintosh OS X hält die Datei resolv.conf aus Kompatibilitätsgründen auf dem neuesten Stand. Verwenden Sie den Befehl scutil —dns, um die DNS-Einstellungen unter Macintosh OS X anzuzeigen.

Konfiguration "Tunnel-all" (und Split-Tunneling mit aktiviertem "tunnel-all DNS")

Wenn AnyConnect verbunden ist, werden nur Tunnel-DNS-Server in der DNS-Konfiguration des Systems verwaltet, und DNS-Anfragen können daher nur an die Tunnel-DNS-Server gesendet werden.

Split-include-Konfiguration (tunnel-all DNS deaktiviert und kein split-DNS)

AnyConnect beeinträchtigt den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, die Vorrang vor öffentlichen DNS-Servern haben. Auf diese Weise wird sichergestellt, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird. Da die DNS-Einstellungen unter Mac OS X global sind, können für DNS-Abfragen keine öffentlichen DNS-Server außerhalb des Tunnels verwendet werden, wie in Cisco Bug-ID CSCtf2026 dokumentiert. Um mit AnyConnect 4.2 zu beginnen, werden vom AnyConnect-Client automatisch Host-Routen für den/die Tunnel-DNS-Server als Split-Include-Netzwerke (sichere Routen) hinzugefügt. Daher erfordert die Split-Include-Zugriffsliste keine explizite Hinzufügung des Tunnel-DNS-Server-Subnetzes mehr.

Split-exclude-Konfiguration (tunnel-all DNS disabled und no split-DNS)

AnyConnect beeinträchtigt den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, sie haben Vorrang vor öffentlichen DNS-Servern, sodass sichergestellt ist, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird. Da die DNS-Einstellungen unter Mac OS X global sind, können für DNS-Abfragen keine öffentlichen DNS-Server außerhalb des Tunnels verwendet werden, wie in Cisco Bug-ID CSCtf2026 dokumentiert. Um mit AnyConnect 4.2 zu beginnen, werden vom AnyConnect-Client automatisch Host-Routen für den/die Tunnel-DNS-Server als Split-Include-Netzwerke (sichere Routen) hinzugefügt. Daher erfordert die Split-Include-Zugriffsliste keine explizite Hinzufügung des Tunnel-DNS-Server-Subnetzes mehr.

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

Wenn Split-DNS für beide IP-Protokolle (IPv4 und IPv6) aktiviert ist oder nur für ein Protokoll aktiviert ist und für das andere Protokoll kein Adresspool konfiguriert ist:
True-Split-DNS wird ähnlich wie Windows erzwungen. Echte Split-DNS bedeutet, dass Anfragen, die mit den Split-DNS-Domänen übereinstimmen, nur über den Tunnel aufgelöst werden. Sie werden nicht an DNS-Server außerhalb des Tunnels weitergeleitet.

Wenn Split-DNS nur für ein Protokoll aktiviert ist und eine Client-Adresse für das andere Protokoll zugewiesen ist, wird nur der DNS-Fallback für Split-Tunneling erzwungen. Das bedeutet, dass AC nur DNS-Anfragen zulässt, die über Tunnel mit den Split-DNS-Domänen übereinstimmen (andere Anfragen werden von AC mit "abgelehnter" Antwort beantwortet, um Failover auf öffentliche DNS-Server zu erzwingen), jedoch die Anfragen, die mit den Split-DNS-Domänen übereinstimmen, die nicht unverschlüsselt über einen öffentlichen Adapter gesendet werden, nicht erzwingen kann.

Linux

Konfiguration "Tunnel-all" (und Split-Tunneling mit aktiviertem "tunnel-all DNS")

Wenn AnyConnect verbunden ist, werden nur Tunnel-DNS-Server in der DNS-Konfiguration des Systems verwaltet, und DNS-Anfragen können daher nur an die Tunnel-DNS-Server gesendet werden.

Split-include-Konfiguration (tunnel-all DNS deaktiviert und kein split-DNS)

AnyConnect beeinträchtigt den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, die Vorrang vor öffentlichen DNS-Servern haben. Auf diese Weise wird sichergestellt, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird.

Split-exclude-Konfiguration (tunnel-all DNS disabled und no split-DNS)

AnyConnect beeinträchtigt den nativen DNS-Resolver nicht. Die Tunnel-DNS-Server werden als bevorzugte Resolver konfiguriert, die Vorrang vor öffentlichen DNS-Servern haben. Auf diese Weise wird sichergestellt, dass die erste DNS-Anforderung für eine Namensauflösung über den Tunnel gesendet wird.

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

Wenn Split-DNS aktiviert ist, wird nur der DNS-Fallback für Split-Tunneling erzwungen. Dies bedeutet, dass AC nur DNS-Anfragen zulässt, die mit den Split-DNS-Domänen über Tunnel übereinstimmen (andere Anfragen werden von AC mit "abgelehnter" Antwort beantwortet, um Failover auf öffentliche DNS-Server zu erzwingen), jedoch nicht die Anfragen durchsetzen kann, die mit den Split-DNS-Domänen übereinstimmen, die nicht unverschlüsselt über den öffentlichen Adapter gesendet werden.

iPhone

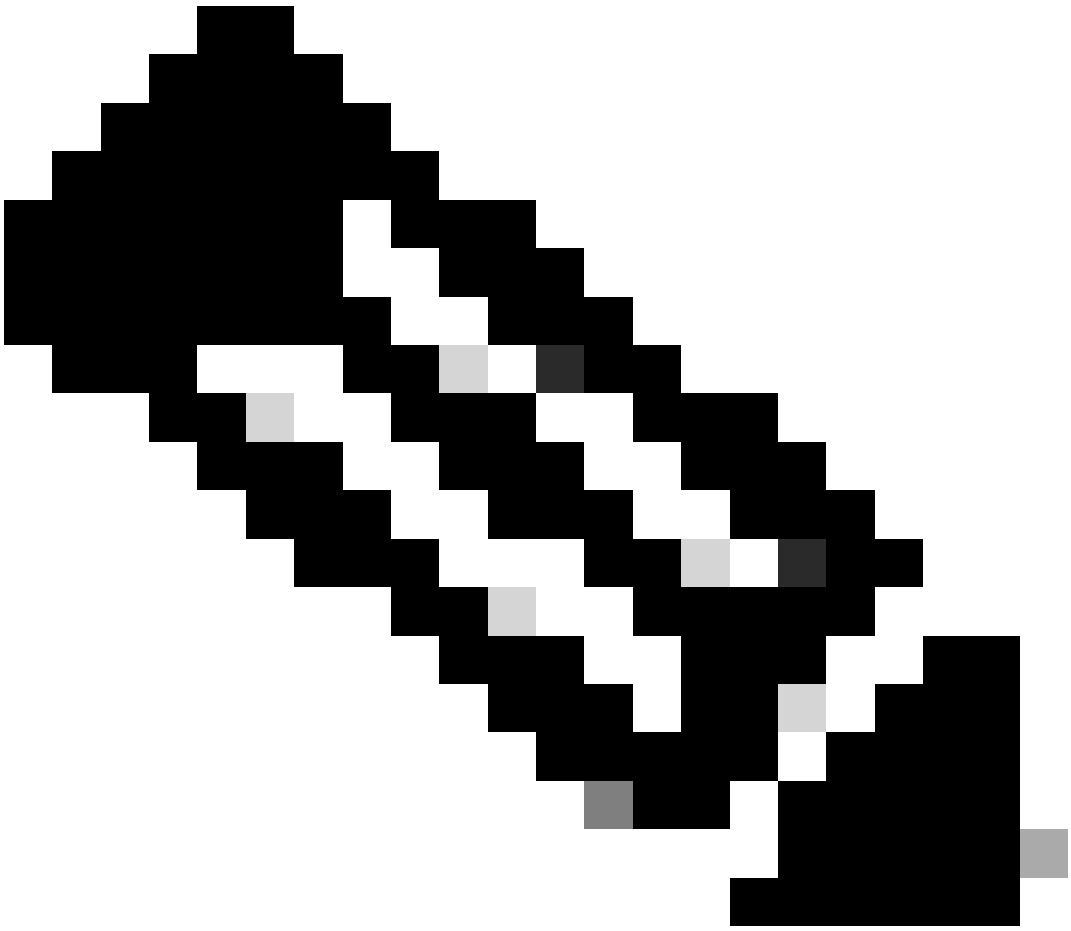
Das iPhone ist das komplette Gegenteil des Macintosh-Systems und ist nicht ähnlich wie Microsoft Windows. Wenn Split-Tunneling definiert ist, Split-DNS jedoch nicht definiert ist, werden DNS-Abfragen über den globalen DNS-Server beendet, der definiert ist. So sind z. B. getrennte DNS-Domäneneinträge für die interne Auflösung erforderlich. Dieses Verhalten ist in der Cisco Bug-ID CSCtq09624 dokumentiert und in Version 2.5.4038 für den Apple iOS AnyConnect-Client behoben.

Hinweis: Beachten Sie, dass die iPhone DNS-Abfragen .local-Domänen ignorieren. Dies ist

---

in der Cisco Bug-ID CSCts89292 dokumentiert. Die Apple-Techniker bestätigen, dass das Problem durch die Funktionalität des Betriebssystems verursacht wird. Dies ist das geplante Verhalten, und Apple bestätigt, dass es keine Änderung gibt.

Zugehörige Fehlerinformationen



Hinweis: Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Informationen von Cisco.

- Cisco Bug-ID CSCsv34395 - Add Support in AnyConnect for that proxies the FQDN to DHCP server
- Cisco Bug-ID CSCtn14578 - AnyConnect unterstützt True Split DNS, nicht Fallback
- Cisco Bug-ID CSCtq02141 - AnyConnect-DNS-Problem, wenn sich ISP DNS im gleichen Subnetz wie Public IP befindet

- Cisco Bug-ID CSCtf20226 - Ermöglicht AnyConnect DNS mit Split-Tunnel-Verhalten für Mac wie Windows
- Cisco Bug-ID CSCtz86314 - Mac: DNS-Abfragen fälschlicherweise nicht über den Tunnel mit Split-DNS gesendet
- Cisco Bug-ID CSCtq09624 - Ermöglicht das AnyConnect iPhone DNS mit getrenntem Tunneling und Windows
- Cisco Bug-ID CSCts89292 - AC für iPhone DNS-Abfragen ignorieren .local-Domänen

Zugehörige Informationen

- Cisco IOS®-Firewall
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.