DNS 쿼리 및 도메인 이름 확인의 동작 검사

목차

소개

이 문서에서는 Cisco OS®가 Cisco AnyConnect 및 스플릿/전체 터널링을 통해 DNS 쿼리 및 도메인 이름 확인에 미치는 영향을 처리하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

스플릿 DNS 대 표준 DNS

스플릿-포함 터널링을 사용하는 경우 DNS(Domain Name System)에 대해 다음 세 가지 옵션이 있습니다.

1. 스플릿 DNS - 도메인 이름과 일치하는 DNS 쿼리는 Cisco ASA(Adaptive Security Appliance)에서 구성됩니다. 터널을 통해 (예를 들어 ASA에 정의된 DNS 서버로) 이동하는 반면 다른 서버는 이동하지 않습니다.

2. Tunnel-all-DNS - ASA에 의해 정의된 DNS 서버에 대한 DNS 트래픽만 허용됩니다. 이 설정은 그룹 정책에 구성됩니다.

3. 표준 DNS - 모든 DNS 쿼리는 ASA에 의해 정의된 DNS 서버를 통해 이동합니다. 부정적인 응답의 경우 DNS 쿼리는 물리적 어댑터에 구성된 DNS 서버로 이동할 수도 있습니다.

참고: split-tunnel-all-dns 명령은 ASA 버전 8.2(5)에서 처음 구현되었습니다. 이 버전 이전에는 스플릿 DNS 또는 표준 DNS만 수행할 수 있었습니다.

모든 경우 터널을 통해 이동하도록 정의된 DNS 쿼리는 ASA에 의해 정의된 DNS 서버로 이동합니다. ASA에서 정의한 DNS 서버가 없는 경우 터널에 대한 DNS 설정이 비어 있습니다. 스플릿 DNS가 정의되지 않은 경우 모든 DNS 쿼리는 ASA에 의해 정의된 DNS 서버로 전송됩니다. 그러나 이 문서에서 설명하는 동작은 운영 체제에 따라 다를 수 있습니다.

참고: 클라이언트에서 이름 확인을 테스트할 때는 NSLookup을 사용하지 마십시오. 대신 브라우저에 의존하거나 ping 명령을 사용합니다. 이는 NSLookup이 OS DNS 확인자에 의존하지 않기 때문입니다. AnyConnect는 특정 인터페이스를 통해 DNS 요청을 강제로 요청하지 않지만 스플릿 DNS 컨피그레이션에 따라 허용하거나 거부합니다. DNS 확인자가 요청을 위해 허용되는 DNS 서버를 시도하도록 강제하려면 도메인 이름 확인을 위해 네이티브 DNS 확인자에 의존하는 애플리케이션(NSLookup, Dig 및 DNS 확인을 직접 처리하는 유사 애플리케이션을 제외한 모든 애플리케이션)에서만 스플릿 DNS 테스트를 수행하는 것이 중요합니다.

True 대 Best Effort 스플릿 DNS

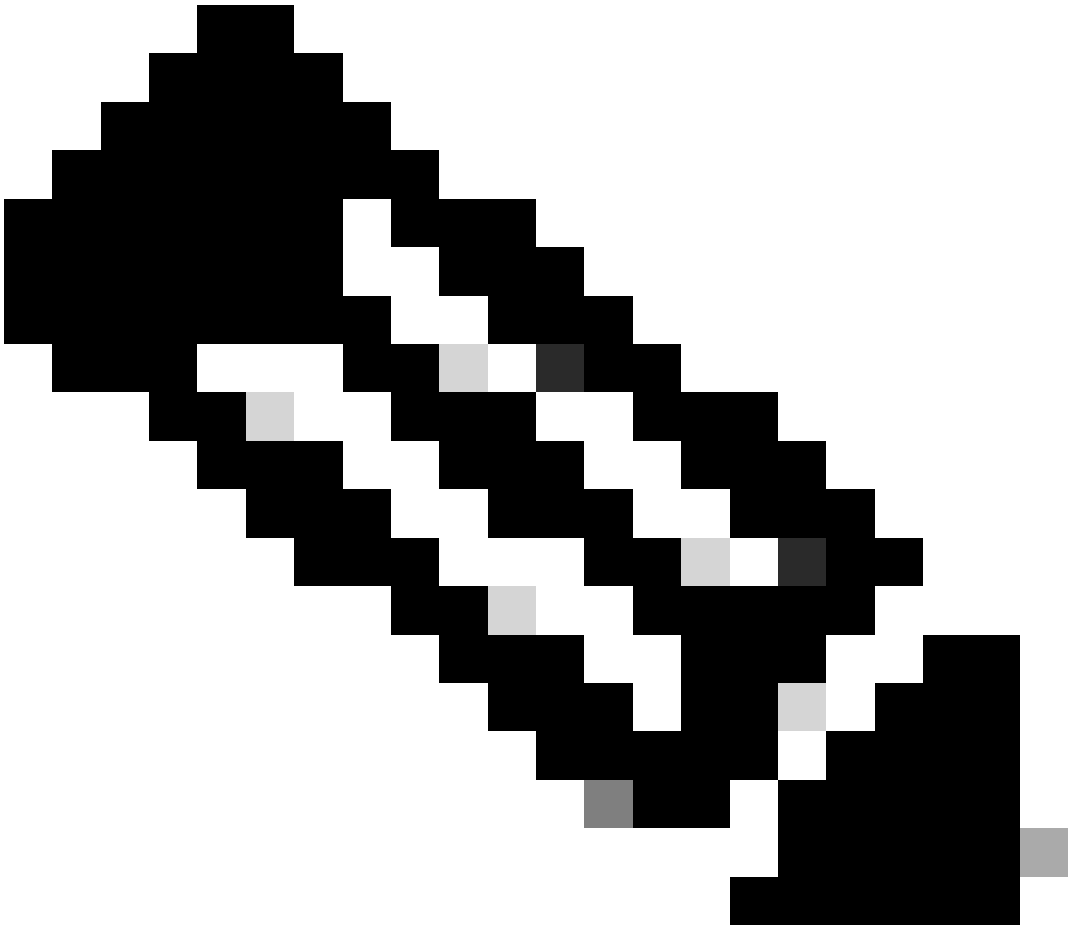
AnyConnect 릴리스 2.4는 진정한 스플릿 DNS가 아니며 레거시 IPsec 클라이언트에서 찾을 수 있는 스플릿 DNS 폴백(Best Effort Split DNS)을 지원합니다. 요청이 스플릿 DNS 도메인과 일치하는 경우 AnyConnect는 요청이 ASA로 터널링되도록 허용합니다. 서버가 호스트 이름을 확인할 수 없는 경우 DNS 확인자는 계속되며 물리적 인터페이스에 매핑된 DNS 서버에 동일한 쿼리를 보냅니다

.

반면, 요청이 스플릿 DNS 도메인과 일치하지 않는 경우 AnyConnect는 ASA로 터널링하지 않습니다. 대신 DNS 확인자가 폴백하여 물리적 인터페이스에 매핑된 DNS 서버로 쿼리를 전송하도록 DNS 응답을 구축합니다. 따라서 이 기능을 스플릿 DNS라고 하지 않고 스플릿 터널링을 위한 DNS 폴백이라고 합니다. AnyConnect는 대상 스플릿 DNS 도메인이 터널링되는 요청만 확인할 뿐 아니라 호스트 이름 확인을 위해 클라이언트 OS DNS 확인자 동작을 사용합니다.

이로 인해 프라이빗 도메인 이름이 유출될 수 있으므로 보안 문제가 발생합니다. 예를 들어, VPN DNS 이름 서버가 DNS 쿼리를 확인할 수 없는 경우 네이티브 DNS 클라이언트는 전용 도메인 이름에 대한 쿼리를 공용 DNS 서버로 전송할 수 있습니다.

버전 3.0(4235)부터 현재 Microsoft Windows에서만 해결된 Cisco 버그 ID CSCtn14578을 참조하십시오. 이 솔루션은 진정한 스플릿 DNS를 구현하며, VPN DNS 서버와 매칭하고 허용되는 구성된 도메인 이름을 엄격하게 쿼리합니다. 다른 모든 쿼리는 물리적 어댑터에 구성된 것과 같은 다른 DNS 서버에만 허용됩니다.



참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

Tunnel-all 및 Tunnel-all DNS

스플릿 터널링이 비활성화되면(Tunnel-all 컨피그레이션) 터널을 통해 DNS 트래픽이 엄격하게 허용됩니다. Tunnel-all DNS 컨피그레이션(그룹 정책에 구성됨)은 일부 스플릿 터널링 유형과 함께 터널을 통해 모든 DNS 조회를 전송하며, DNS 트래픽은 터널을 통해 엄격하게 허용됩니다.

이는 Microsoft Windows에서 한 가지 주의 사항이 있는 여러 플랫폼에서 일관적입니다. Tunnel-all 또는 Tunnel-all DNS가 구성된 경우 AnyConnect는 DNS 트래픽을 보안 게이트웨이에 구성된 DNS 서버로 엄격하게 허용합니다(VPN 어댑터에 적용됨). 이는 앞서 언급한 진정한 스플릿 DNS 솔루션과 함께 구현된 보안 개선 기능입니다.

특정 시나리오에서 문제가 되는 경우(예: DNS 업데이트/등록 요청은 비 VPN DNS 서버로 전송해야 함) 다음 단계를 완료하십시오.

1. 현재 컨피그레이션이 Tunnel-all인 경우 스플릿 제외 터널링을 활성화합니다. 단일 호스트, 스플릿 제외 네트워크(예: 링크-로컬 주소)를 사용할 수 있습니다.

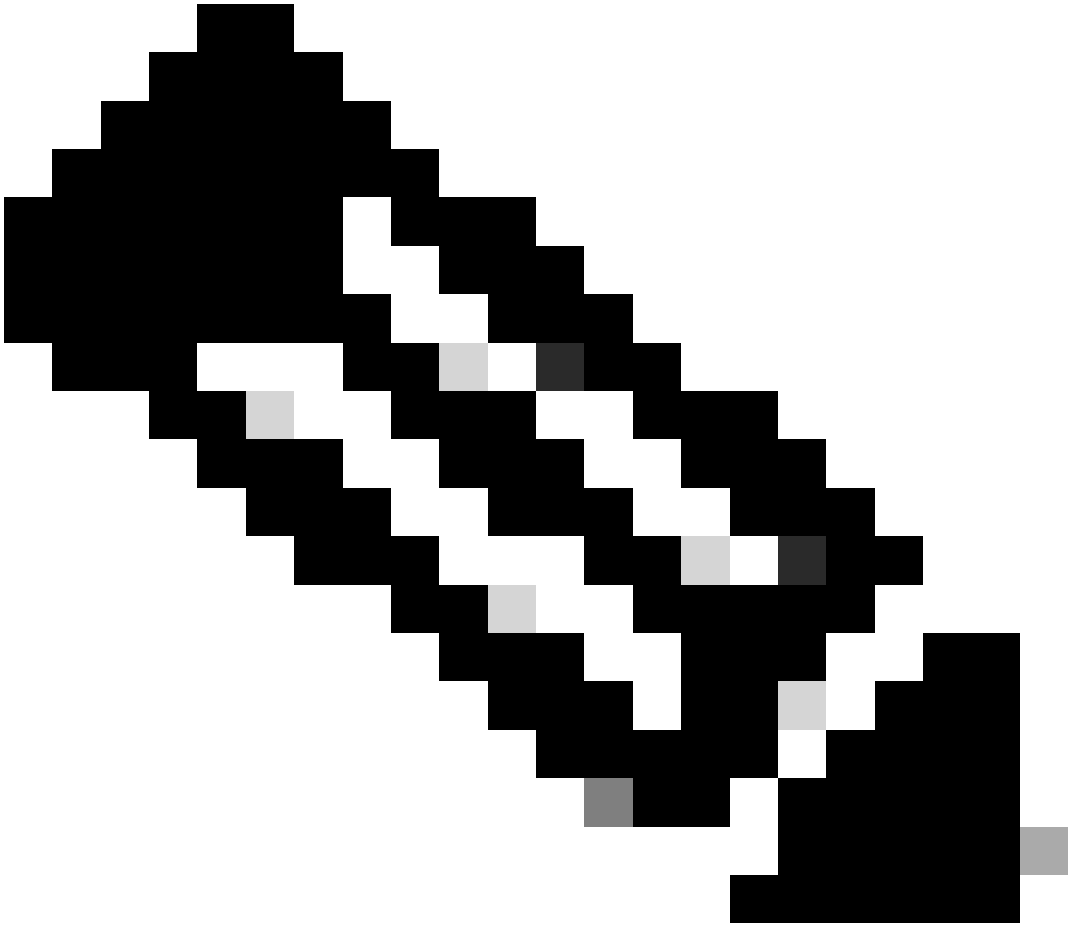
2. Tunnel-all DNS가 그룹 정책에 구성되지 않았는지 확인합니다.

AnyConnect 버전 3.0(4235)에서 해결된 DNS 성능 문제

이 Microsoft Windows 문제는 주로 다음과 같은 상황에서 널리 발생합니다.

- 홈 라우터 설정으로 DNS 및 DHCP 서버에 동일한 IP 주소가 할당됩니다(AnyConnect는 DHCP 서버에 필요한 경로를 생성합니다).
- 많은 수의 DNS 도메인이 그룹 정책에 있습니다.
- Tunnel-all 컨피그레이션이 사용됩니다.
- 이름 확인은 정규화되지 않은 호스트 이름으로 수행되며, 이는 확인자가 쿼리된 호스트 이름과 관련된 DNS 접미사를 시도할 때까지 사용 가능한 모든 DNS 서버에서 여러 DNS 접미사를 시도해야 함을 의미합니다. 이 문제는 AnyConnect가 차단하는 물리적 어댑터를 통해 DNS 쿼리를 보내려고 시도하는 네이티브 DNS 클라이언트(Tunnel-all 컨피그레이션을 감안함) 때문입니다. 이로 인해 이름 확인 지연이 상당히 지연될 수 있으며, 특히 헤드엔드에서 많은 DNS 접미사를 푸시하는 경우 더욱 그러합니다. DNS 클라이언트는 긍정적인 응답을 받을 때까지 모든 쿼리 및 사용 가능한 DNS 서버를 거쳐야 합니다.

이 문제는 AnyConnect 버전 3.0(4235)에서 해결되었습니다. 자세한 내용은 앞서 언급한 진정한 스플릿 DNS 솔루션 소개와 함께 Cisco 버그 ID CSCtq02141 및 Cisco 버그 ID CSCtn14578을 참조하십시오.



참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

업그레이드를 구현할 수 없는 경우 가능한 해결 방법은 다음과 같습니다.

- IP 주소에 대해 스플릿 제외 터널링을 활성화하여 로컬 DNS 요청이 물리적 어댑터를 통해 이동하도록 허용합니다. 어떤 디바이스도 VPN을 통해 IP 주소 중 하나로 트래픽을 전송할 가능성이 없으므로 linklocal 서브넷 169.254.0.0/16의 주소를 사용할 수 있습니다. split-exclude tunneling d를 활성화한 후, 클라이언트 프로파일 또는 클라이언트 자체에서 로컬 LAN 액세스를 활성화하고 Tunnel-all dDNS를 비활성화합니다.

  ASA에서 다음 컨피그레이션을 변경합니다.

```
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
```

클라이언트 프로필에서 다음 행을 추가해야 합니다.

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

또한 AnyConnect 클라이언트 GUI에서 클라이언트 단위로 이를 활성화할 수 있습니다. AnyConnect 기본 설정 메뉴로 이동하여 Enable local LAN access(로컬 LAN 액세스 사용) 확인란을 선택합니다.

- 이름 확인에 대해 정규화되지 않은 호스트 이름 대신 FQDN(정규화된 도메인 이름)을 사용합니다.
- 물리적 인터페이스의 DNS 서버에 대해 다른 IP 주소를 사용합니다.

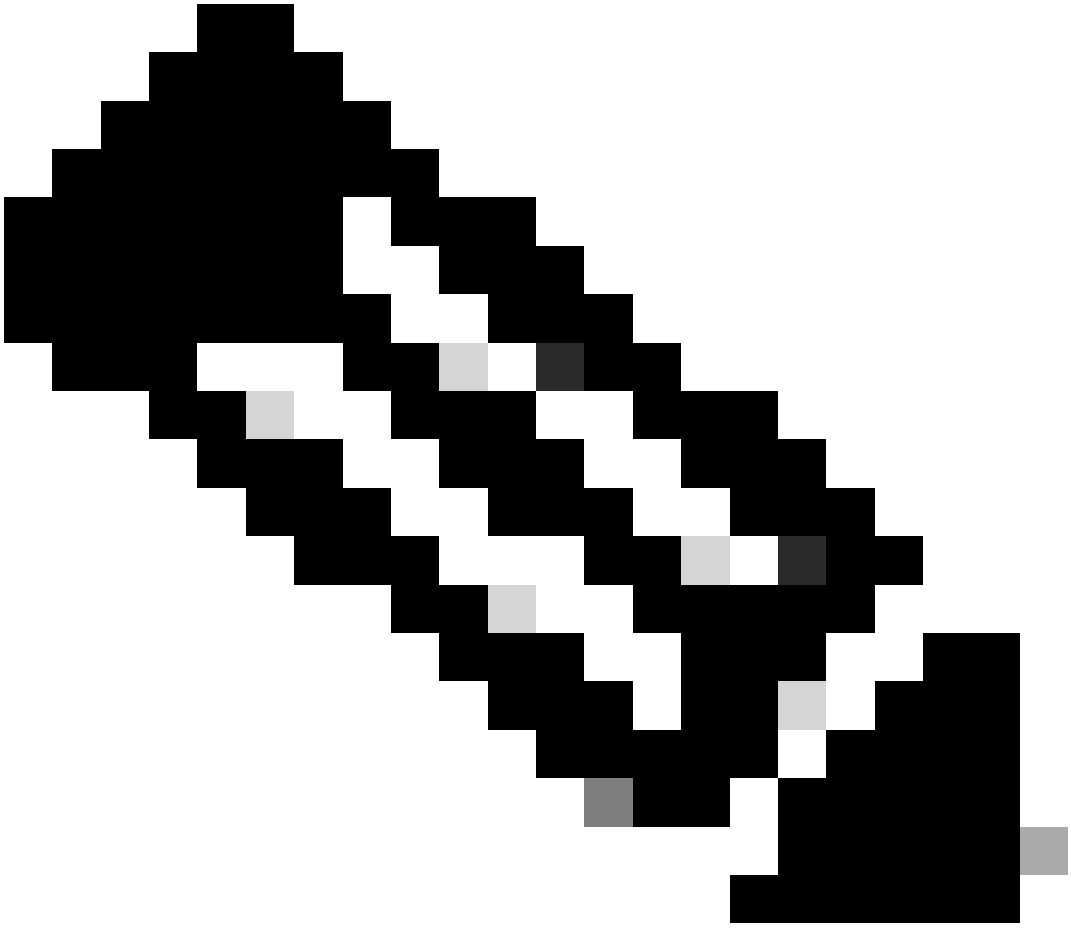
다른 Cisco OS에서 스플릿 터널링을 사용하는 DNS

AnyConnect에 대해 스플릿 터널링과 함께 사용할 경우(스플릿 DNS 없음) Cisco OS마다 다른 방법으로 DNS 검색을 처리합니다. 이 섹션에서는 이러한 차이점에 대해 설명합니다.

Microsoft Windows

Microsoft Windows 시스템에서 DNS 설정은 인터페이스별로 설정됩니다. 스플릿 터널링을 사용하는 경우 VPN 터널 어댑터에서 장애가 발생한 후 DNS 쿼리는 물리적 어댑터 DNS 서버로 폴백될 수 있습니다. 스플릿 DNS 없이 스플릿 터널링을 정의하는 경우 내부 및 외부 DNS 확인이 모두 작동하는데, 이는 외부 DNS 서버로 폴백되기 때문입니다.

Cisco 버그 ID CSCuf07885를 수정한 후 릴리스 4.2의 Windows용 AnyConnect에서 이를 처리하는 DNS 메커니즘에서 동작이 변경되었습니다.



참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

Windows 7 이상

Tunnel-all 컨피그레이션(및 tunnel-all DNS가 활성화된 스플릿 터널링)

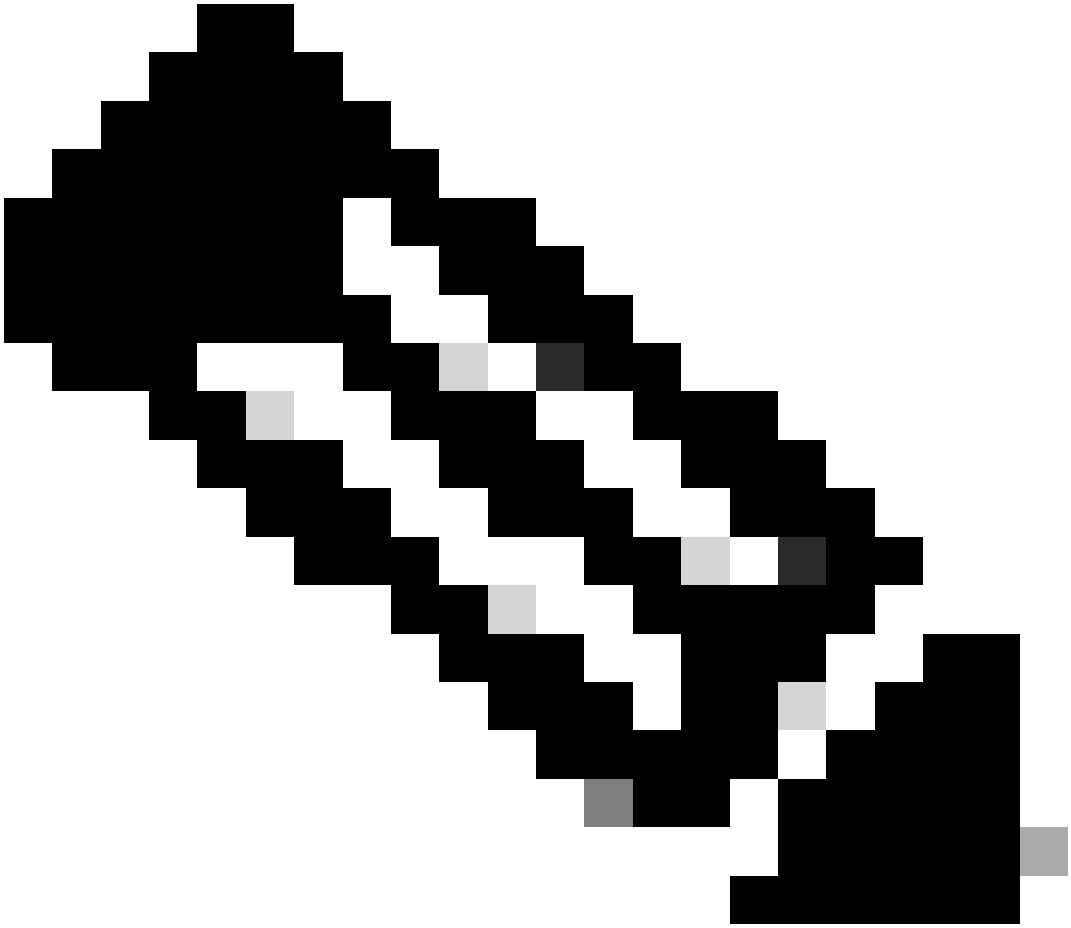
AnyConnect 4.2 이전:

그룹 정책(터널 DNS 서버)에 구성된 DNS 서버에 대한 DNS 요청만 허용됩니다. AnyConnect 드라이버는 "no such name(해당 이름 없음)" 응답으로 다른 모든 요청에 응답합니다. 따라서 DNS 확인은 터널 DNS 서버에서만 수행할 수 있습니다.

AnyConnect 4.2 +

VPN 어댑터에서 시작되어 터널을 통해 전송되는 모든 DNS 서버에 대한 DNS 요청은 허용됩니다. 다른 모든 요청은 해당 이름으로 응답되지 않으며 DNS 확인은 VPN 터널을 통해서만 수행할 수 있습니다.

Cisco 버그 ID CSCuf07885 수정 이전에 AC는 대상 DNS 서버를 제한했지만, 이 버그에 대한 수정으로 이제 어떤 네트워크 어댑터가 DNS 요청을 시작할 수 있는지 제한합니다.



참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

Split-include 컨피그레이션(tunnel-all DNS는 비활성화되고 split-DNS는 없음)

AnyConnect 드라이버는 네이티브 DNS 확인자를 방해하지 않습니다. 따라서 DNS 확인은 VPN 연결 시 AnyConnect가 항상 기본 어댑터인 네트워크 어댑터 순서에 따라 수행됩니다. 또한 DNS 쿼리는 먼저 터널을 통해 전송되며, 확인되지 않으면 확인자는 공용 인터페이스를 통해 확인하려고 시도합니다. split-include access-list에는 터널 DNS 서버를 지원하는 서브넷이 포함됩니다. AnyConnect 4.2로 시작하려면 터널 DNS 서버에 대한 호스트 경로가 AnyConnect 클라이언트에 의

해 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 스플릿-포함 액세스 목록에 터널 DNS 서버 서브넷을 더 이상 명시적으로 추가할 필요가 없습니다.

Split-exclude 컨피그레이션(tunnel-all DNS는 비활성화되고 split-DNS는 없음)

AnyConnect 드라이버는 네이티브 DNS 확인자를 방해하지 않습니다. 따라서 DNS 확인은 VPN 연결 시 AnyConnect가 항상 기본 어댑터인 네트워크 어댑터 순서에 따라 수행됩니다. 또한 DNS 쿼리는 먼저 터널을 통해 전송되며, 확인되지 않으면 확인자는 공용 인터페이스를 통해 확인하려고 시도합니다. 스플릿 제외 액세스 목록은 터널 DNS 서버를 다루는 서브넷을 포함하지 않아야 합니다. AnyConnect 4.2로 시작하려면 터널 DNS 서버에 대한 호스트 경로가 AnyConnect 클라이언트에 의해 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 스플릿-제외 액세스 목록의 잘못된 컨피그레이션을 방지합니다.

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

AnyConnect 4.2 이전

스플릿 DNS 도메인과 일치하는 DNS 요청은 DNS 서버를 터널링할 수 있지만 다른 DNS 서버에는 허용되지 않습니다. 이러한 내부 DNS 쿼리가 터널 밖으로 유출되는 것을 방지하기 위해 AnyConnect 드라이버는 쿼리가 다른 DNS 서버로 전송되는 경우 "해당 이름 없음"으로 응답합니다. 따라서 스플릿 DNS 도메인은 터널 DNS 서버를 통해서만 확인할 수 있습니다.

스플릿 DNS 도메인과 일치하지 않는 DNS 요청은 다른 DNS 서버에 허용되지만 DNS 서버를 터널링할 수 없습니다. 이 경우에도 스플릿 DNS 이외의 도메인에 대한 쿼리가 터널을 통해 시도되면 AnyConnect 드라이버가 "해당 이름 없음"으로 응답합니다. 따라서 스플릿 DNS 도메인이 아닌 도메인은 터널 외부의 공용 DNS 서버를 통해서만 확인할 수 있습니다.

AnyConnect 4.2 +

스플릿 DNS 도메인과 일치하는 DNS 요청은 VPN 어댑터에서 시작되는 한 모든 DNS 서버에 허용됩니다. 쿼리가 공용 인터페이스에서 시작된 경우 AnyConnect 드라이버는 "no such name(해당 이름 없음)"으로 응답하여 이름 확인을 위해 레졸버가 항상 터널을 사용하도록 합니다. 따라서 스플릿 DNS 도메인은 터널을 통해서만 확인할 수 있습니다.

스플릿 DNS 도메인과 일치하지 않는 DNS 요청은 물리적 어댑터에서 시작되는 모든 DNS 서버에 허용됩니다. 쿼리가 VPN 어댑터에서 시작된 경우 AnyConnect는 "no such name(해당 이름 없음)"으로 응답하여 확인자가 항상 공용 인터페이스를 통해 이름 확인을 시도하도록 합니다. 따라서 스플릿 DNS 도메인이 아닌 도메인은 공용 인터페이스를 통해서만 확인할 수 있습니다.

맥 OSx

Macintosh 시스템에서는 DNS 설정이 전역입니다. 스플릿 터널링을 사용하지만 스플릿 DNS를 사용하지 않는 경우 DNS 쿼리가 터널 외부의 DNS 서버에 도달할 수 없습니다. 외부적으로는 해결하

지 않고 내부적으로만 해결할 수 있습니다.

이는 Cisco 버그 ID CSCtf20226 및 Cisco 버그 ID CSCtz86314에 설명되어 있습니다. 두 경우 모두 이 해결 방법으로 문제를 해결해야 합니다.

- 그룹 정책에서 외부 DNS 서버 IP 주소를 지정하고 내부 DNS 쿼리에 FQDN을 사용합니다.
- 외부 이름을 터널을 통해 확인할 수 있는 경우 Advanced(고급) > Split Tunneling(스플릿 터널링)으로 이동하고 그룹 정책에 구성된 DNS 이름을 제거하여 스플릿 DNS를 비활성화합니다. 이를 위해서는 내부 DNS 쿼리에 FQDN을 사용해야 합니다.

스플릿 DNS 케이스는 AnyConnect 버전 3.1에서 해결됩니다. 그러나 다음 조건 중 하나가 충족되는지 확인해야 합니다.

- 스플릿 DNS는 두 IP 프로토콜 모두에 대해 활성화되어야 하며, 이를 위해서는 Cisco ASA 버전 9.0 이상이 필요합니다.
- 하나의 IP 프로토콜에 대해 스플릿 DNS를 활성화해야 합니다. Cisco ASA Version 9.0 이상을 실행하는 경우 다른 IP 프로토콜에 대해 클라이언트 우회 프로토콜을 사용합니다. 예를 들어, 주소 풀이 없고 그룹 정책에서 클라이언트 우회 프로토콜이 활성화되어 있는지 확인합니다. 또는 버전 9.0 이전의 ASA 버전을 실행하는 경우 다른 IP 프로토콜에 대해 구성된 주소 풀이 없는지 확인합니다. 이는 다른 IP 프로토콜이 IPv6임을 의미합니다.

참고: AnyConnect는 Macintosh OS X에서 resolv.conf 파일을 변경하지 않고 OS X 관련 DNS 설정을 변경합니다. Macintosh OS X는 호환성을 위해 resolv.conf 파일을 최신 상태로 유지합니다. Macintosh OS X에서 DNS 설정을 보려면 scutil —dns 명령을 사용합니다.

Tunnel-all 컨피그레이션(및 tunnel-all DNS가 활성화된 스플릿 터널링)

AnyConnect가 연결되면 터널 DNS 서버만 시스템 DNS 컨피그레이션에서 관리되므로 DNS 요청은 터널 DNS 서버로만 보낼 수 있습니다.

Split-include 컨피그레이션(tunnel-all DNS는 비활성화되고 split-DNS는 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다. 터널 DNS 서버는 공용 DNS 서버보다 우선하는 기본 설정 확인자로 구성되므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송됩니다. DNS 설정은 Mac OS X에서 전역이므로 DNS 쿼리에서 Cisco 버그 ID CSCtf20226에 설명된 대로 터널 외부의 공용 DNS 서버를 사용할 수 없습니다. AnyConnect 4.2로 시작하려면 터널 DNS 서버에 대한 호스트 경로가 AnyConnect 클라이언트에 의해 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 스플릿-포함 액세스 목록에 터널 DNS 서버 서브넷을 더 이상 명시적으로 추가할 필요가 없습니다.

Split-exclude 컨피그레이션(tunnel-all DNS는 비활성화되고 split-DNS는 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다. 터널 DNS 서버는 기본 설정 리졸버로 구성되며 공용 DNS 서버보다 우선하므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송됩니다. DNS 설정은 Mac OS X에서 전역이므로 DNS 쿼리에서 Cisco 버그 ID CSCtf20226에 설명된 대로 터널 외부의 공용 DNS 서버를 사용할 수 없습니다. AnyConnect 4.2로 시작하려면 터널 DNS 서버에 대한 호스트 경로가 AnyConnect 클라이언트에 의해 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 스플릿-포함 액세스 목록에 터널 DNS 서버 서브넷을 더 이상 명시적으로 추가할 필요가 없습니다.

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

스플릿 DNS가 두 IP 프로토콜(IPv4 및 IPv6) 모두에 대해 활성화되었거나 한 프로토콜에 대해서만 활성화되었으며 다른 프로토콜에 대해 구성된 주소 풀이 없는 경우:
Windows와 유사한 진정한 스플릿 DNS가 적용됩니다. 진정한 스플릿 DNS는 스플릿 DNS 도메인과 일치하는 요청이 터널을 통해서만 확인되고 터널 외부의 DNS 서버로 유출되지 않음을 의미합니다.

스플릿 DNS가 하나의 프로토콜에 대해서만 활성화되고 클라이언트 주소가 다른 프로토콜에 대해 할당된 경우, 스플릿 터널링에 대한 DNS 대안만 적용됩니다. 즉, AC는 터널을 통해 스플릿 DNS 도메인과 일치하는 DNS 요청만 허용하지만(다른 요청은 공용 DNS 서버로 강제로 장애 조치하기 위해 "거부됨" 응답을 사용하여 AC에서 응답함), 일반 어댑터에서 전송되지 않은 스플릿 DNS 도메인과 일치하는 요청은 공용 어댑터를 통해 시행할 수 없습니다.

Linux

Tunnel-all 컨피그레이션(및 tunnel-all DNS가 활성화된 스플릿 터널링)

AnyConnect가 연결되면 터널 DNS 서버만 시스템 DNS 컨피그레이션에서 관리되므로 DNS 요청은 터널 DNS 서버로만 보낼 수 있습니다.

Split-include 컨피그레이션(tunnel-all DNS는 비활성화되고 split-DNS는 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다. 터널 DNS 서버는 공용 DNS 서버보다 우선하는 기본 설정 확인자로 구성되므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송됩니다.

Split-exclude 컨피그레이션(tunnel-all DNS는 비활성화되고 split-DNS는 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다. 터널 DNS 서버는 공용 DNS 서버보다 우선하는 기본 설정 확인자로 구성되므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송됩니다.

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

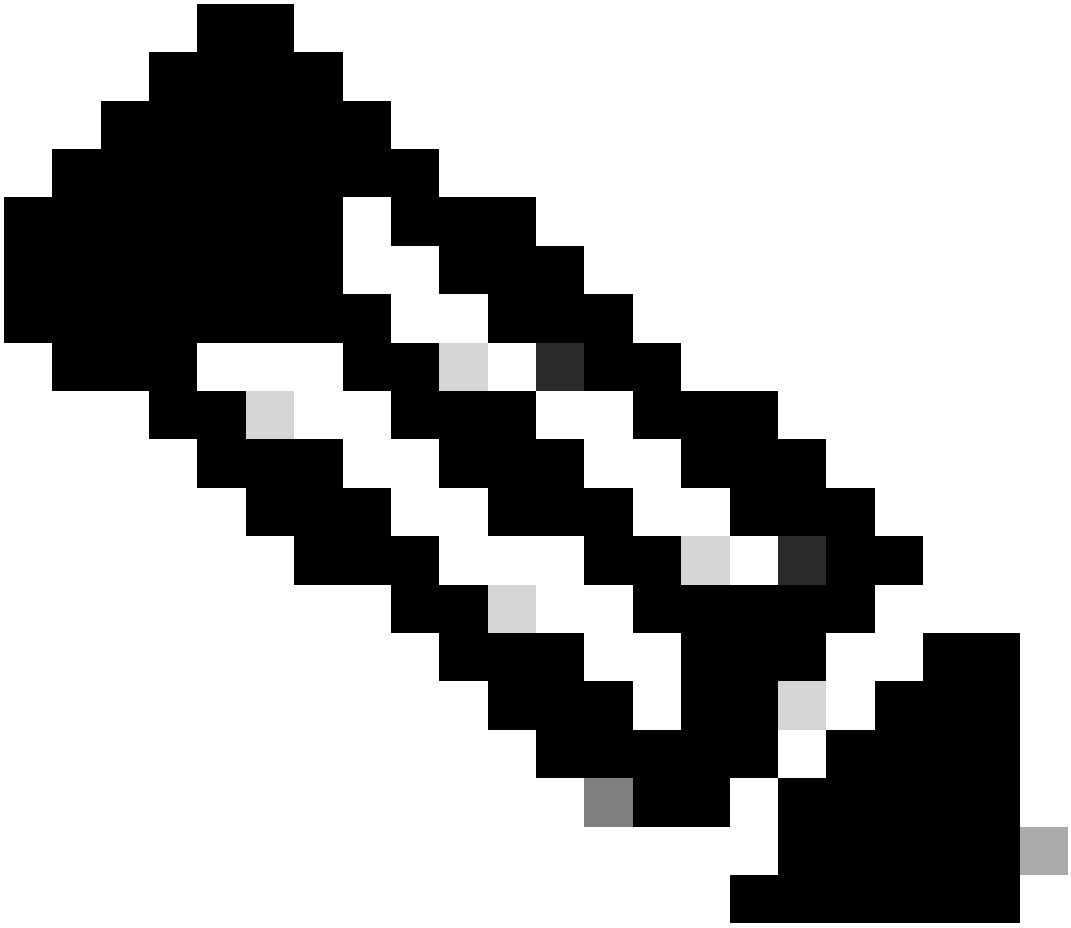
split-DNS가 활성화된 경우 split-tunneling에 대한 DNS 대안만 적용됩니다. 즉, AC는 터널을 통해 스플릿 DNS 도메인과 일치하는 DNS 요청만 허용하지만(다른 요청은 공용 DNS 서버로 강제로 장애 조치하기 위해 "거부됨" 응답과 함께 AC에서 응답함), 공개 어댑터를 통해 암호화되지 않은 스플릿 DNS 도메인과 일치하는 요청은 강제할 수 없습니다.

아이폰

아이폰은 매킨토시 시스템과 완전히 반대이고 마이크로소프트 윈도우와 비슷하지 않다. 스플릿 터널링이 정의되었지만 스플릿 DNS가 정의되지 않은 경우 DNS 쿼리는 정의된 전역 DNS 서버를 통해 종료됩니다. 예를 들어, 내부 확인에는 스플릿 DNS 도메인 항목이 필수입니다. 이 동작은 Cisco 버그 ID CSCtq09624에 문서화되어 있으며 Apple iOS AnyConnect 클라이언트의 버전 2.5.4038에서 수정됩니다.

참고: iPhone DNS 쿼리는 .local 도메인을 무시합니다. 이는 Cisco 버그 ID CSCts89292에 설명되어 있습니다. Apple 엔지니어는 이 문제가 OS의 기능 때문임을 확인합니다. 이는 설계된 행동이며 애플은 이에 대한 변화가 없다고 확인했다.

관련 버그 정보



참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

- Cisco 버그 ID CSCsv34395 - DHCP 서버에 대한 FQDN을 해당 프록시에 대한 AnyConnect 지원 추가
- Cisco 버그 ID CSCtn14578 - AnyConnect는 진정한 스플릿 DNS를 지원하며 폴백이 아님
- Cisco 버그 ID CSCtq02141 - ISP DNS가 공용 IP와 동일한 서브넷에 있는 경우 AnyConnect DNS 문제
- Cisco 버그 ID CSCtf20226 - Mac에 대한 스플릿 터널 동작을 사용하는 AnyConnect DNS를 Windows와 동일하게 만듭니다.
- Cisco 버그 ID CSCtz86314 - Mac: 스플릿 DNS를 사용하는 터널을 통해 DNS 쿼리가 잘못 전송되지 않습니다.
- Cisco 버그 ID CSCtq09624 - AnyConnect iPhone DNS(스플릿 터널링 동작 포함)를 Windows와 동일하게 설정

- Cisco 버그 ID CSCts89292 - iPhone DNS 쿼리의 AC는 .local 도메인을 무시합니다.

관련 정보

- Cisco IOS® 방화벽
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.