AnyConnect와 OpenDNS 로밍 클라이언트 간의 상호 운용성

목차

소개

이 문서에서는 AnyConnect와 OpenDNS 로밍 클라이언트가 함께 작동하도록 하기 위한 현재 제한 사항 및 사용 가능한 해결 방법에 대해 설명합니다. Cisco 고객은 회사 네트워크와의 안전하고 암호화된 통신을 위해 AnyConnect VPN 클라이언트를 사용합니다.마찬가지로 OpenDNS Roaming 클라이언트는 OpenDNS 공용 서버의 도움을 받아 DNS 서비스를 안전하게 사용할 수 있는 기능을 제공합니다.두 클라이언트 모두 엔드포인트에 다양한 보안 기능을 추가하므로 서로 상호 운용해야 합니다.

사전 요구 사항

AnyConnect 및 OpenDNS 로밍 클라이언트에 대한 작업 지식

AnyConnect VPN에 대한 ASA 또는 IOS/IOS-XE 헤드엔드 컨피그레이션(tunnel-group/group-policy)에 익숙합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA 또는 IOS/IOS-XE 헤드엔드
- AnyConnect VPN 클라이언트 및 OpenDNS 로밍 클라이언트를 실행하는 엔드포인트

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 릴리스 9.4를 실행하는 ASA 헤드엔드
- Windows 7
- AnyConnect 클라이언트 4.2.00096
- OpenDNS 로밍 클라이언트 2.0.154

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

배경 정보

OpenDNS는 향후 Cisco AnyConnect 팀과 함께 AnyConnect 플러그인을 개발하고 있습니다.날짜가 설정되지 않은 상태에서 로밍 클라이언트가 해결 방법 없이 AnyConnect 클라이언트에서 작동할 수 있습니다.이렇게 하면 AnyConnect가 로밍 클라이언트를 위한 전달 메커니즘이 됩니다.

기능

AnyConnect DNS 처리

VPN 헤드엔드는 AnyConnect 클라이언트의 트래픽을 처리하기 위해 여러 가지 방법으로 구성할 수 있습니다.

1. 전체 터널 구성(tunnel-all):이렇게 하면 엔드포인트의 모든 트래픽이 VPN 터널을 통해 암호화되므로 트래픽이 일반 텍스트로 공용 인터페이스 어댑터를 떠나지 않습니다
2. 스플릿 터널 구성:

   a.스플릿-포함 터널링:VPN 헤드엔드에 정의된 특정 서브넷 또는 호스트로만 향하는 트래픽은 터널을 통해 전송되며, 다른 모든 트래픽은 일반 텍스트로 터널 외부로 전송됩니다.

   b.스플릿 제외 터널링:VPN 헤드엔드에 정의된 특정 서브넷 또는 호스트로만 향하는 트래픽은 암호화에서 제외되고 공용 인터페이스를 일반 텍스트로 남겨둡니다. 다른 모든 트래픽은 암호화되며 터널을 통해서만 전송됩니다.

이러한 각 컨피그레이션은 엔드포인트의 운영 체제에 따라 AnyConnect 클라이언트에서 DNS 확인을 처리하는 방법을 결정합니다.CSCuf07885의 수정 후 릴리스 4.2에서 Windows용 AnyConnect의 DNS 처리 메커니즘에서 동작이 변경되었습니다.

Windows 7+

터널 전체 컨피그레이션(tunnel-all DNS가 활성화된 스플릿 터널링)

AnyConnect 4.2 이전:

group-policy(터널 DNS 서버)에 구성된 DNS 서버에 대한 DNS 요청만 허용됩니다.AnyConnect 드라이버는 'no such name' 응답으로 다른 모든 요청에 응답합니다.따라서 터널 DNS 서버를 통해서만 DNS 확인을 수행할 수 있습니다.

AnyConnect 4.2 +

DNS 서버가 VPN 어댑터에서 시작되어 터널을 통해 전송되는 경우 모든 DNS 서버에 대한 DNS 요청이 허용됩니다.다른 모든 요청은 'no such name' 응답으로 응답되며, DNS 확인은 VPN 터널을 통해서만 수행할 수 있습니다.

CSCuf07885 수정 전에 AC는 대상 DNS 서버를 제한하지만 CSCuf07885 수정을 통해 DNS 요청을 시작할 수 있는 네트워크 어댑터가 제한됩니다.

Split-include 컨피그레이션(tunnel-all DNS 비활성화됨 및 split-DNS 없음)

AnyConnect 드라이버는 네이티브 DNS 확인자를 방해하지 않습니다.따라서 DNS 확인은 네트워크 어댑터의 순서에 따라 수행되며, VPN이 연결된 경우 AnyConnect가 항상 기본 어댑터입니다.따라서 DNS 쿼리는 터널을 통해 먼저 전송되며 해결되지 않으면 확인자가 공용 인터페이스를 통해 확인하려고 시도합니다.split-include access-list는 터널 DNS 서버를 포함하는 서브넷을 포함해야 합니다. AnyConnect 4.2부터 터널 DNS 서버의 호스트 경로는 AnyConnect 클라이언트에서 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 split-include access-list에 터널 DNS 서버 서브넷을 명시적으로 추가할 필요가 없습니다.

Split-exclude 컨피그레이션(tunnel-all DNS 비활성화됨 및 split-DNS 없음)

AnyConnect 드라이버는 네이티브 DNS 확인자를 방해하지 않습니다.따라서 DNS 확인은 네트워크 어댑터의 순서에 따라 수행되며, VPN이 연결된 경우 AnyConnect가 항상 기본 어댑터입니다.따라서 DNS 쿼리는 터널을 통해 먼저 전송되며 해결되지 않으면 확인자가 공용 인터페이스를 통해 확인하려고 시도합니다.split-exclude access-list는 터널 DNS 서버를 포함하는 서브넷을 포함하지 않아야 합니다. AnyConnect 4.2부터 Tunnel DNS 서버의 호스트 경로는 AnyConnect 클라이언트에서 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 split-exclude access-list에서 잘못된 컨피그레이션을 방지할 수 있습니다.

Split-DNS(tunnel-all DNS 사용 안 함, split-include 구성)

AnyConnect 4.2 이전

스플릿 DNS 도메인과 일치하는 DNS 요청은 DNS 서버를 터널링할 수 있지만 다른 DNS 서버에는 허용되지 않습니다.이러한 내부 DNS 쿼리가 터널에서 유출되는 것을 방지하기 위해 쿼리가 다른 DNS 서버로 전송된 경우 AnyConnect 드라이버가 'no such name'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 수는 없습니다.이 경우에도 터널을 통해 분할되지 않은 dns 도메인에 대한 쿼리를 시도하면 AnyConnect 드라이버가 'no such name'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'으로 응답하여 확인자가 항상 이름 확인을 위해 터널을 사용하도록 합니다.따라서 스플릿 DNS 도메인은 터널을 통해서만 확인할 수 있습니다.

스플릿 DNS 도메인과 일치하지 않는 DNS 요청은 물리적 어댑터에서 시작되는 한 모든 DNS 서버에 허용됩니다.쿼리가 VPN 어댑터에서 시작된 경우 AnyConnect는 'no such name'으로 응답하여 확인자가 항상 공용 인터페이스를 통해 이름 확인을 시도하도록 합니다.따라서 분할되지 않은 DNS 도메인은 공용 인터페이스를 통해서만 확인할 수 있습니다.

Mac OS X

터널 전체 컨피그레이션(tunnel-all DNS가 활성화된 스플릿 터널링)

AnyConnect가 연결되면 터널 DNS 서버만 시스템 DNS 컨피그레이션에서 유지되므로 DNS 요청은 터널 DNS 서버로만 전송할 수 있습니다.

Split-include 컨피그레이션(tunnel-all DNS 비활성화됨 및 split-DNS 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다.터널 DNS 서버는 공용 DNS 서버보다 우선하므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송되도록 하는 기본 확인 서버로 구성됩니다.DNS 설정은 Mac OS X에서 전역 설정이므로 DNS 쿼리가 CSCtf20226에 설명된 대로 터널 외부의 공용 DNS 서버를 사용할 수 없습니다.AnyConnect 4.2부터 터널 DNS 서버의 호스트 경로는 AnyConnect 클라이언트에서 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 split-include access-list에 터널 DNS 서버 서브넷을 명시적으로 추가할 필요가 없습니다.

Split-exclude 컨피그레이션(tunnel-all DNS 비활성화됨 및 split-DNS 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다.터널 DNS 서버는 공용 DNS 서버보다 우선하므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송되도록 하는 기본 확인 서버로 구성됩니다.DNS 설정은 Mac OS X에서 전역 설정이므로 DNS 쿼리가 CSCtf20226에 설명된 대로 터널 외부의 공용 DNS 서버를 사용할 수 없습니다.AnyConnect 4.2부터 터널 DNS 서버의 호스트 경로는 AnyConnect 클라이언트에서 스플릿-포함 네트워크(보안 경로)로 자동으로 추가되므로 split-

include access-list에 터널 DNS 서버 서브넷을 명시적으로 추가할 필요가 없습니다.

Split-DNS(tunnel-all DNS 사용 안 함, split-include 구성)

스플릿-DNS가 IP 프로토콜(IPv4 및 IPv6)에 대해 활성화되었거나 한 프로토콜에 대해서만 활성화되고 다른 프로토콜에 대해 구성된 주소 풀이 없는 경우:
Windows와 유사한 True split-DNS가 적용됩니다.True split-DNS는 스플릿-DNS 도메인과 일치하는 요청이 터널을 통해서만 확인되며 터널 외부의 DNS 서버로 유출되지 않음을 의미합니다.

스플릿-DNS가 한 프로토콜에 대해서만 활성화되고 다른 프로토콜에 대해 클라이언트 주소가 할당되는 경우 "스플릿 터널링을 위한 DNS 대체(fallback for split-tunneling)"만 적용됩니다.즉, AC는 터널을 통해 스플릿 DNS 도메인과 일치하는 DNS 요청만 허용합니다(다른 요청은 AC에서 "거부" 응답으로 퍼블릭 DNS 서버로 장애 조치를 강제 수행). 그러나 스플릿 DNS 도메인과 일치하는 요청은 공용 어댑터를 통해 암호화되지 않도록 적용할 수는 없습니다.

리눅스

터널 전체 컨피그레이션(tunnel-all DNS가 활성화된 스플릿 터널링)

AnyConnect가 연결되면 터널 DNS 서버만 시스템 DNS 컨피그레이션에서 유지되므로 DNS 요청은 터널 DNS 서버로만 전송할 수 있습니다.

Split-include 컨피그레이션(tunnel-all DNS 비활성화됨 및 split-DNS 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다.터널 DNS 서버는 공용 DNS 서버보다 우선하므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송되도록 하는 기본 확인 서버로 구성됩니다.

Split-exclude 컨피그레이션(tunnel-all DNS 비활성화됨 및 split-DNS 없음)

AnyConnect는 네이티브 DNS 확인자를 방해하지 않습니다.터널 DNS 서버는 공용 DNS 서버보다 우선하므로 이름 확인에 대한 초기 DNS 요청이 터널을 통해 전송되도록 하는 기본 확인 서버로 구성됩니다.

Split-DNS(tunnel-all DNS 사용 안 함, split-include 구성)

split-DNS가 활성화된 경우 "스플릿 터널링을 위한 DNS 대체(fallback for split-tunneling)"만 적용됩니다.즉, AC는 터널을 통해 스플릿 DNS 도메인과 일치하는 DNS 요청만 허용합니다(다른 요청은 AC에서 "거부" 응답으로 퍼블릭 DNS 서버로 장애 조치를 강제 수행). 그러나 스플릿 DNS 도메인과 일치하는 요청은 공용 어댑터를 통해 암호화되지 않도록 적용할 수는 없습니다.

OpenDNS 로밍 클라이언트

로밍 클라이언트는 엔드포인트에서 DNS 서비스를 관리하고 OpenDNS 공용 DNS 서버를 사용하여 DNS 트래픽을 보호하고 암호화하는 소프트웨어의 일부입니다.

클라이언트가 보호 및 암호화된 상태여야 합니다.그러나 클라이언트가 OpenDNS 공용 확인자 서버(208.67.222.222)으로 TLS 세션을 설정할 수 없는 경우 UDP 포트 53에서 208.67.222.222으로 암호화되지 않은 DNS 트래픽을 보내려고 시도합니다. 로밍 클라이언트는 OpenDNS의 공용 확인자 IP 주소 208.67.222.222(208.67.220.220, 208.67.222.220, 208.67.220.222과 같은 몇 가지 다른 내용이 있음)만 사용합니다. 로밍 클라이언트가 설치되면 127.0.0.1(localhost)을 로컬 DNS 서버로 설정하고 현재 인터페이스별 DNS 설정을 재정의합니다.현재 DNS 설정은 Roaming Client 컨피그레이션 폴더 내의 로컬 resolv.conf 파일(Windows에서도)에 저장됩니다.OpenDNS는 AnyConnect 어댑터를 통해 학습된 DNS 서버도 백업합니다.예를 들어, 192.168.92.2이 공용 어댑터의 DNS 서버인 경우 OpenDNS는 다음 위치에 resolv.conf를 생성합니다.

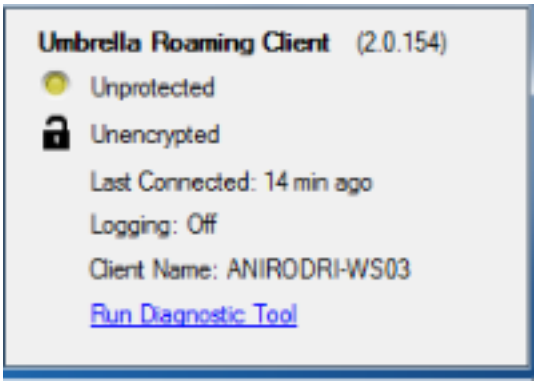
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
이름 서버 192.168.92.2

로밍 클라이언트는 OpenDNS로 설정된 각 패킷을 암호화합니다.그러나 암호화 터널을 시작하거나 208.67.222.222에 사용하지 않습니다. 로밍 클라이언트에는 IP 주소를 차단하기 위해 비 DNS 목적으로 IPSec 연결을 여는 선택적 IP 레이어 적용 기능이 있습니다.이렇게 하면 활성 AnyConnect 연결이 있으면 자동으로 비활성화됩니다.또한 127.0.0.1:53에 바인딩되어 컴퓨터에서 로컬로 생성된 쿼리를 받습니다.엔드포인트가 이름을 확인해야 할 경우 재정의로 인해 로컬 쿼리가 127.0.0.1으로 전달되고, 로밍 클라이언트의 기본 dnscrypt-proxy 프로세스는 암호화된 채널을 통해 OpenDNS 공용 서버로 전달합니다.

DNS가 127.0.0.1:53으로 이동할 수 없는 경우 로밍 클라이언트가 작동하지 않으며 다음 작업이 발생합니다. 클라이언트가 공용 DNS 서버 또는 127.0.0.1:53 바운드 주소에 연결할 수 없는 경우 fail-open 상태로 전환되고 로컬 어댑터의 DNS 설정을 복원합니다.백그라운드에서 프로브는 208.67.222.222으로 계속 전송되며 보안 연결이 다시 설정되면 활성 모드로 전환될 수 있습니다.

제한 사항

두 클라이언트의 고급 기능을 살펴본 결과, 로밍 클라이언트는 로컬 DNS 설정을 변경하고 127.0.0.1:53에 바인딩하여 보안 채널을 통해 쿼리를 전달할 수 있어야 합니다.VPN이 연결된 경우 AnyConnect가 네이티브 DNS 확인자에 간섭하지 않는 유일한 컨피그레이션은 split-include 및 split-exclude(split-tunnel-all DNS가 비활성화된 경우)입니다. 따라서 현재 로밍 클라이언트가 사용 중인 경우 이러한 구성 중 하나를 사용하는 것이 좋습니다.터널-모두 컨피그레이션을 사용하거나 이미지에 표시된 대로 스플릿-터널-전체 DNS를 활성화하면 로밍 클라이언트는 보호되지 않거나 암호화되지 않은 상태로 유지됩니다.



해결 방법

VPN 터널을 사용하여 로밍 클라이언트와 OpenDNS 서버 간의 통신을 보호하려는 경우에는 VPN 헤드엔드에서 더미 분할 제외 액세스 목록을 사용할 수 있습니다.이는 전체 터널 컨피그레이션에 가장 가까운 것입니다.이러한 요구 사항이 없는 경우 access-list에 OpenDNS 공용 서버가 포함되지 않은 경우 split-include를 사용하거나, access-list에 OpenDNS 공용 서버가 포함된 경우 split-exclude를 사용할 수 있습니다.

또한 로밍 클라이언트를 사용할 경우 로컬 DNS 확인이 손실되므로 스플릿 DNS 모드를 사용할 수 없습니다.스플릿-터널-전체 DNS도 비활성화된 상태로 유지해야 합니다.그러나 부분적으로 지원되며 로밍 클라이언트가 장애 조치 후 암호화되도록 허용해야 합니다.

구성

터널 OpenDNS 트래픽

이 예에서는 split-exclude access-list에서 더미 IP 주소를 사용합니다.이 컨피그레이션에서는 208.67.222.222와의 모든 통신이 VPN 터널을 통해 이루어지며, 로밍 클라이언트는 암호화된 상태로 보호된 상태로 작동합니다.

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

VPN 터널에서 OpenDNS 트래픽 제외

이 예에서는 split-exclude access-list의 OpenDNS 확인자 주소를 사용합니다.이 컨피그레이션에서

는 208.67.222.222와의 모든 통신이 VPN 터널 외부에서 수행되며, 로밍 클라이언트는 암호화된 상태로 보호된 상태로 작동합니다.

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

이 예에서는 내부 192.168.1.0/24 서브넷에 대한 스플릿-포함 컨피그레이션을 보여줍니다.이 컨피그레이션에서는 208.67.222.222에 대한 트래픽이 터널을 통해 전송되지 않으므로 로밍 클라이언트가 여전히 암호화된 보호 상태로 작동합니다.

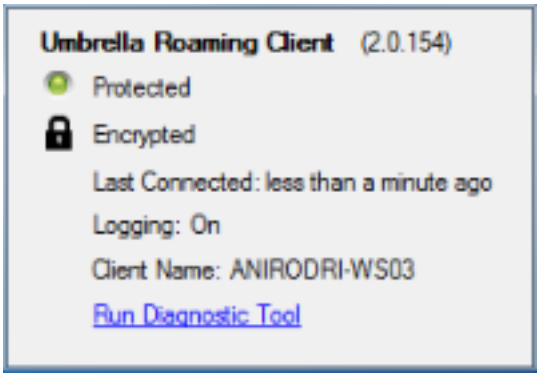
```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Note: Split-tunnel-all-dns must be disabled in all of the scenarios

다음을 확인합니다.

VPN이 연결된 경우 로밍 클라이언트는 다음 이미지에 표시된 대로 보호 및 암호화되어 표시되어야 합니다.


Umbrella Roaming Client (2.0.154)
Protected
Encrypted
Last Connected: less than a minute ago
Logging: On
Client Name: ANIRODRI-WS03
Run Diagnostic Tool