iOS 14 및 macOS 11에서 DNS 확인자 선택 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

개요

Umbrella 사용자에게 미치는 영향

- CSC(Cisco Security Connector)
- macOS RC(Umbrella Roaming Client)
- macOS AnyConnect 클라이언트(AC)
- VA(Virtual Appliance) 뒤에 있는 iOS 또는 macOS 디바이스
- 등록된 네트워크 뒤의 iOS 또는 macOS 디바이스

Umbrella 및 암호화된 DNS

iOS 14 및 macOS 11의 세부적인 DNS 변경 사항

- 시스템 전반의 암호화된 리졸버
- 도메인 소유자가 지정하는 암호화된 리졸버
- 앱에서 지정한 암호화된 해결 프로그램

소개

이 문서에서는 암호화된 DNS를 지원하는 iOS 14 및 macOS 11 업데이트의 Umbrella 변경 사항에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CSC(Cisco Security Connector)
- macOS RC(Umbrella Roaming Client)
- macOS AnyConnect 클라이언트(AC)

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.

개요

애플은 2020년 9월 16일 iOS 14 출시를 발표했다. 다른 변경 사항 중에서, iOS 14 및 macOS 11은 암호화된 DNS를 지원하며, 도메인 소유자가 자신이 선택한 DNS 확인자를 지정할 수 있는 기능을 포함합니다. 이러한 변경은 Umbrella가 일부 도메인 이름을 확인하는 기능에 직접적인 영향을 미치므로 해당 도메인에 대한 정책 및 보고가 영향을 받습니다.

iOS 14 및 macOS 11의 변경은 3가지 주요 효과가 있습니다.

1. 사용자는 DHCP 또는 RA에서 설정한 DNS 확인자를 재정의할 수 있는 시스템 차원의 DoH 확인자를 지정할 수 있습니다.

2. 도메인 소유자는 해당 도메인에 대한 쿼리에 대해 DHCP 또는 RA가 설정한 DNS 확인자를 재정의할 수 있는 DoH 확인자를 지정할 수 있습니다.

3. 앱은 앱에서 만든 쿼리에 대해 DHCP 또는 RA가 설정한 DNS 확인자를 재정의할 수 있는 DoH 확인자를 지정할 수 있습니다. Umbrella는 어떤 애플리케이션이 그렇게 하는지 알 수 없습니다.

이러한 업데이트로 Apple은 네트워크 프로비저닝된 리졸버와 동일한 IP에서 실행 중인 암호화된 리졸버를 검색하는 메커니즘을 포함하지 않았습니다. 즉, Umbrella 리졸버에 쿼리를 전달하는 네트워크는 doh.umbrella.com에서 Umbrella의 DoH 서비스로 업그레이드할 수 없습니다.

2020년 10월 1일자로 Umbrella는 도메인 소유자가 지정한 DoH 확인자를 검색하지 못하게 하므로 해당 도메인이 Umbrella 보호를 우회할 수 없습니다. Umbrella 클라이언트가 디바이스에 설치되어 있지 않으면 Umbrella에서 #1 및 #3 영향을 방지할 수 없습니다. 그러한 영향에 대한 보호가 필요한 고객은 이 문서에 설명된 대로 알려진 DoH 제공자의 IP를 차단하는 것을 고려할 수 있습니다.

iOS 14 및 macOS 11의 변경 사항에 대한 자세한 내용은 이 문서를 계속 읽어 보십시오.

Umbrella 사용자에게 미치는 영향

CSC(Cisco Security Connector)

CSC를 사용하는 iOS 장치는 iOS의 레졸버 검색 메커니즘보다 우선 순위가 높은 Apple의 DNS 프록시 메커니즘을 사용하므로 이 변경의 영향을 받을 수 없습니다.

macOS RC(Umbrella Roaming Client)

macOS RC는 현재 로컬 호스트에서 DNS 프록시를 실행하므로 RC를 사용하는 macOS 디바이스는 이 변경의 영향을 받을 수 있습니다. macOS는 이를 암호화되지 않은 확인자로 간주합니다. RC는 DNSCrypt를 사용하여 Umbrella 리졸버와 통신합니다.

Umbrella는 Apple DNS 프록시 공급자를 사용하여 DNS를 제어하는 AnyConnect Roaming Security Module(아래 AC 참조)에서 DoH 검색에 대해 적용할 수 있도록 지원합니다. 이 지원은 현재 RC에 포함되지 않을 예정입니다. Umbrella 패키지는 AC에 대해 라이센스가 부여됩니다. 기사를 보세요.

macOS AnyConnect 클라이언트(AC)

AC를 사용하는 macOS 디바이스는 현재 macOS의 레졸버 검색 메커니즘보다 우선 순위가 높은 Apple의 DNS 프록시 메커니즘을 사용하므로 이 변경의 영향을 받을 수 없습니다.

VA(Virtual Appliance) 뒤에 있는 iOS 또는 macOS 디바이스

CSC, RC 또는 AC가 설치되지 않은 iOS 또는 macOS는 이 변경의 영향을 받을 수 있습니다. 따라서 VA 뒤에 있는 이러한 디바이스는 가상 어플라이언스를 우회하여 구성된 DoH 서버에 직접 쿼리를 전송할 수 있습니다.

등록된 네트워크 뒤의 iOS 또는 macOS 디바이스

CSC, RC 또는 AC가 설치되지 않은 iOS 또는 macOS는 이 변경의 영향을 받지 않습니다. 따라서 등록된 네트워크 뒤에 있는 이러한 디바이스는 로컬 확인자 또는 Umbrella를 우회하여 구성된 DoH 서버에 직접 쿼리를 보낼 수 있습니다.

Umbrella 및 암호화된 DNS

Umbrella는 암호화된 DNS의 사용 및 암호화된 DNS의 사용을 진전시키기 위한 이니셔티브를 완벽하게 지원합니다. Umbrella 리졸버는 2011년부터 DNS 트래픽을 암호화하는 수단으로 DNSCrypt를 지원했으며, 모든 Umbrella 클라이언트 소프트웨어는 DNSCrypt 사용을 지원하고 기본 컨피그레이션에서 이를 사용합니다. 또한 2020년 2월부터 HTTPS(DoH)를 통한 DNS를 지원했습니다.

Umbrella는 또한 캐시의 모든 레코드에 대한 데이터 무결성을 보장하기 위해 업스트림 당국에 전송된 쿼리에 대한 DNSSEC 검증을 수행합니다.

iOS 14 및 macOS 11의 세부적인 DNS 변경 사항

iOS 14와 macOS 11은 DNS 확인자를 선택하는 새로운 메커니즘을 도입했습니다. 특정 세부 사항을 요구하는 고객은 Apple에 문의할 수 있지만, Cisco는 이 메커니즘에 대해 다음과 같은 우선 순위를 두고 DNS 확인자를 선택할 수 있다는 점을 잘 알고 있습니다.

1. 네트워크에서 제공하는 DNS 확인자를 이용한 종속 포털 테스트 영역의 해결

2. VPN 또는 DNS 프록시 구성(예: iOS용 Cisco Security Connector) 및 기업 정책(예: MDM 또는 OTA)에 의해 설정된 DNS 확인자. DNS 정책 설정에 대한 자세한 내용은 MDM 공급업체에 문의하십시오.

3. 장치 소유자가 직접 구성한 시스템 전체의 암호화된 리졸버

4. 도메인소유자가 지정한 암호화된 리졸버

5. 앱에서 지정하는 암호화 레졸버

6. 암호화되지 않은 리졸버(DHCP 또는 RA를 통해 지정된 리졸버와 유사)

특히 3, 4, 5는 확인자 선택에 대한 중요한 변경 사항으로 간주되며, 이는 Umbrella 관리자가 네트워크에서 Umbrella 확인자의 사용을 완전히 시행하는 기능에 직접적인 영향을 미칠 수 있습니다.

시스템 전반의 암호화된 리졸버

사용자는 DNS 공급자에서 구성 프로필 앱을 설치할 수 있으며, 이를 통해 시스템 전반의 암호화된 확인자를 구성할 수 있습니다. 이 확인자는 DHCP 또는 RA를 통해 네트워크에서 지정한 DNS 확인자와 상관없이 모든 쿼리에 사용할 수 있습니다.

현재, 관리되지 않는 디바이스에 이러한 리졸버를 사용하지 못하도록 하는 유일한 방법은 방화벽에서 알려진 DoH 공급자의 IP를 차단하는 것입니다. 이렇게 하면 iOS 디바이스의 사용자에게 경고가 표시될 수 있으며, 디바이스는 암호화되지 않은 DNS로 폴백할 수 없으므로 DNS 호스트 이름을 확인할 수 없습니다.

도메인 소유자가 지정하는 암호화된 리졸버

DNS 영역의 소유자는 영역을 확인하는 데 사용할 특정 확인자를 지정할 수 있습니다. iOS 14 및 macOS 11에서는 DoH 리졸버만 지정할 수 있습니다. 이 지정은 전용 DNS 레코드 유형(유형 65, 이름이 "HTTPS")을 사용하여 이루어지며 DNSSEC 또는 잘 알려진 URI에 의해 검증됩니다.

이러한 지정으로 인해 쿼리가 Umbrella를 우회하게 되므로 Umbrella 확인자는 HTTPS DNS 레코드 유형에 대한 쿼리에 대해 REFUSED 응답을 반환하며, 이는 그러한 지정이 검색되지 않음을 의미합니다.

앱에서 지정한 암호화된 해결 프로그램

높은 우선 순위 메커니즘에서 다른 암호화된 확인자가 검색되지 않는 경우 앱 생성자는 대체 암호화된 확인자를 지정할 수 있습니다. 이 확인자는 DHCP 또는 RA에서 설정한 암호화되지 않은 확인자를 사용하는 경우에만 사용할 수 있습니다.

현재, 관리되지 않는 디바이스에 이러한 리졸버를 사용하지 못하도록 하는 유일한 방법은 방화벽에서 알려진 DoH 공급자의 IP를 차단하는 것입니다. 이러한 시나리오에서 iOS가 암호화되지 않은 DNS로 폴백될 수 있는지 여부는 아직 알려지지 않았습니다.

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.