회사 네트워크에 Umbrella Roaming 클라이언트 구성

목차

소개

이 문서에서는 회사 네트워크에 있는 Umbrella 로밍 클라이언트의 구성에 대해 설명합니다.

개요

Umbrella 로밍 클라이언트는 원격 사용자를 보호하는 훌륭한 도구이지만 회사 네트워크의 사용자를 보호하여 또 다른 보안 계층을 추가할 수도 있습니다. 비즈니스 요구 사항에 따라 일부 관리자는 기업 네트워크에서 Umbrella 로밍 클라이언트를 지속적으로 보호하기를 원하는 반면, 다른 관리자는 다른 Umbrella 정책을 위해 Umbrella 로밍 클라이언트를 '해제'하기를 선호합니다.

Umbrella는 네트워크에 들어갈 때 Umbrella 로밍 클라이언트가 작동하는 방식에 대한 유연성을 제공합니다. 이 문서에서는 이와 같은 다양한 접근 방식을 간략하게 설명합니다.

목표

Q). 회사 네트워크에서 Umbrella 로밍 클라이언트를 비활성화해야 하는 이유는 무엇입니까?

일반적으로 내부 및 외부 DNS 작업을 위해 Umbrella 로밍 클라이언트를 비활성화할 필요가 없습니다. Umbrella 로밍 클라이언트는 도메인 관리 기능을 사용하여 내부 DNS 트래픽을 일반 DNS 서버로 전달합니다. 이렇게 하면 Umbrella 로밍 클라이언트가 네트워크의 엔드포인트에서 실행되는 동안 보호 및 연결을 모두 유지할 수 있습니다.

그러나 로밍 클라이언트 보호를 사용하지 않도록 설정하는 것을 고려해야 하는 이유가 있을 수 있습니다.

- 네트워크에서 나가는 로밍 사용자에게 다른 '네트워크 내' 및 '네트워크 외' 정책을 제공합니다

.

- 회사 네트워크에서 내부 DNS 서버를 사용하면 캐싱 및 발신 DNS 트래픽 감소의 측면에서 몇 가지 이점이 있습니다.
- Umbrella 로밍 클라이언트는 Umbrella에 대한 연결을 확인하기 위해 프로브 메시지를 주기적으로 전송합니다. 클라이언트 수가 매우 많은 경우 이 추가 트래픽이 원치 않을 수 있습니다.

Q) 회사 네트워크에서 Umbrella 로밍 클라이언트를 계속 활성화하려는 이유는 무엇입니까?

반면 로밍 클라이언트를 항상 활성화해야 하는 몇 가지 좋은 이유가 있습니다.

- Umbrella 로밍 클라이언트 컴퓨터가 항상 동일한 정책을 사용하는지 확인합니다.
- 세분화된 보고를 위해 항상 보고서에서 Umbrella 로밍 클라이언트의 호스트 이름을 식별 가능(네트워크 ID 대신)합니다.
- 로밍 클라이언트는 향상된 개인 정보를 위해 '암호화된 DNS' 트래픽을 사용합니다
- Secure Web Gateway 사용자(AnyConnect 사용)의 경우 SWG 웹 필터링을 제공하려면 클라이언트가 활성화된 상태를 유지해야 합니다.

작동 모드

항상 켜짐

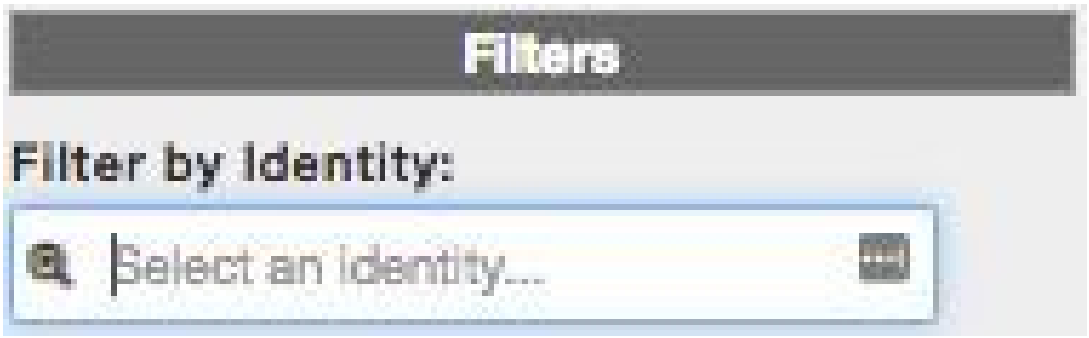
Umbrella 로밍 클라이언트는 회사 네트워크에서 사용하더라도 계속 켜져 있을 수 있습니다. 이 모드에서는 Umbrella 로밍 클라이언트 ID를 사용하여 정책이 구성되며 이 ID가 보고서에 나타납니다
.

정책	Umbrella 로밍 클라이언트 ID는 항상 사용됩니다.
보고	Umbrella 로밍 클라이언트 ID는 시스템별로 세분화된 보고서에 항상 나타납니다
DNS 트래픽	• Umbrella 로밍 클라이언트는 회사 네트워크에서도 Umbrella에 DNS 쿼리를 직접 계속 보냅니다. • Umbrella로 전송된 쿼리는 암호화되어 추가 보안을 제공합니다. • '내부 도메인'에 대한 쿼리는 일반 DNS 서버로 라우팅되고 Umbrella로 전송되지 않습니다.
프로브 메시지	Umbrella 로밍 클라이언트는 Umbrella의 가용성을 확인하기 위해 프로브 메시지를 계속 전송합니다.

'Always ON' 모드 구성 방법:

1. Identities(ID) > Roaming Computers(로밍 컴퓨터)로 이동합니다.
2. (로밍 클라이언트 설정) 아이콘을 클릭합니다.
3. Umbrella Protected Network(Umbrella 보호 네트워크)에 있는 동안 Disable DNS redirection(DNS 리디렉션 비활성화)의 선택을 취소하고 Save(저장)를 클릭합니다.
4. Umbrella 로밍 클라이언트에 대해 별도의 정책을 생성하고 가장 높은 우선순위(목록의 맨 위)인지 확인합니다. Umbrella 로밍 클라이언트 정책은 네트워크 ID를 기반으로 하는 정책보다 우선 순위가 높아야 합니다.

일반 네트워크 정책 사용
Umbrella 로밍 클라이언트가 활성화되어 있고 Umbrella와 직접 계속 통신하지만 네트워크 ID는 정책 및 보고 목적으로 모두 사용됩니다. 이 모드는 네트워크 정책을 Umbrella 로밍 클라이언트 정책보다 우선 순위가 높은 곳에 배치하면 활성화됩니다.

정책	네트워크 정책은 보호된 네트워크에 있을 때 사용됩니다. 이렇게 하면 서로 다른 온/오프 네트워크 정책을 사용할 수 있습니다.
보고	• 보고는 기본 ID로 네트워크 ID와 연결됩니다. • 보고에서는 Umbrella 로밍 클라이언트 호스트 이름을 통해 검색하여 해당 클라이언트에 대한 결과만 필터링할 수 있습니다. 
DNS 트래픽	• Umbrella 로밍 클라이언트는 회사 네트워크에서도 Umbrella에 DNS 쿼리를 직접 계속 보냅니다. • Umbrella로 전송된 쿼리는 암호화되어 추가 보안을 제공합니다. • '내부 도메인'에 대한 쿼리는 일반 DNS 서버로 라우팅되고 Umbrella로 전송되지 않습니다.

프로브 메시지	Umbrella 로밍 클라이언트는 Umbrella의 가용성을 확인하기 위해 프로브 메시지를 계속 전송합니다.

'일반 네트워크 정책 사용'방법

1. Identities(ID) > Roaming Computers(로밍 컴퓨터)로 이동합니다.
2. (로밍 클라이언트 설정) 아이콘을 클릭합니다.
3. Umbrella Protected Network(Umbrella 보호 네트워크)에 있는 동안 Disable DNS redirection(DNS 리디렉션 비활성화)의 선택을 취소하고 Save(저장)를 클릭합니다.
4. 네트워크에 대한 별도의 정책을 생성합니다. 네트워크에 대한 정책이 로밍 클라이언트를 기반으로 하는 정책보다 우선 순위가 높은지 확인합니다.

Disable behind Protected Networks(소규모 네트워크에 적합)
Umbrella 로밍 클라이언트가 보호된 네트워크에 있음을 감지하면 '백 오프'할 수 있습니다. 이는 네트워크 ID가 정책 및 보고 목적으로 모두 사용됨을 의미합니다.

이 모드는 Umbrella 로밍 클라이언트가 실제로 자체 비활성화되고 DNS 트래픽을 방해하지 않는다는 점을 제외하면 '일반 네트워크 정책 사용' 모드와 동작이 유사합니다.

정책	네트워크 정책은 보호된 네트워크에 있을 때 사용됩니다. 이렇게 하면 서로 다른 온/오프 네트워크 정책을 사용할 수 있습니다.
보고	보호된 네트워크에서는 시스템별로 보고를 세분화할 수 없습니다. 보고는 네트워크 ID에만 연결됩니다.
DNS 트래픽	보호된 네트워크에서 Umbrella 로밍 클라이언트는 DNS 쿼리를 방해하지 않으며 일반 내부 DNS 서버로 이동합니다.
프로브 메시지	Umbrella 로밍 클라이언트는 보호 네트워크에 있음을 확인하기 위해 프로브 메시지를 계속 전송합니다.

보호된 네트워크에서 Disable을 구성하는 방법:

1. Identities(ID) > Roaming Computers(로밍 컴퓨터)로 이동합니다.
2. (로밍 클라이언트 설정) 아이콘을 클릭합니다.

3. Disable DNS redirection while on an Umbrella Protected Network(Umbrella 보호 네트워크에 있는 동안 DNS 리디렉션 비활성화)를 선택하고 Save(저장)를 클릭합니다.
4. Policies > Policies List로 이동합니다.
5. 네트워크에 대한 별도의 정책을 생성합니다. 네트워크에 대한 정책이 Umbrella 로밍 클라이언트를 기반으로 하는 정책보다 우선 순위가 높은지 확인합니다.
6. 로컬 DNS 서버는 Umbrella 확인기로 전달되어야 하며 Umbrella 대시보드에 올바르게 등록되어 있어야 합니다.
7. 이 기능이 작동하려면 클라이언트 워크스테이션에서 사용하는 이그레스 IP가 내부 DNS 서버에서 사용하는 이그레스 IP와 동일한 네트워크 ID에 등록되어야 합니다. 자세한 내용은 이 문서를 참조하십시오.

신뢰할 수 있는 네트워크 도메인 뒤에 비활성화(대규모 네트워크에 적합)

이제 고객이 구성한 '신뢰할 수 있는 네트워크 도메인'을 선택할 수 있습니다. 클라이언트는 이 DNS 도메인(A 레코드)을 확인하려고 시도하고 도메인이 성공적으로 확인될 경우 보호를 사용하지 않도록 설정합니다. 이는 클라이언트가 회사 네트워크에 있을 때만 확인되는 내부 전용 DNS 레코드입니다.

정책	신뢰할 수 있는 도메인이 탐지될 때마다 클라이언트는 백오프하며, 반드시 Umbrella 정책 또는 필터링을 수신할 필요는 없습니다. 다른 Umbrella 기능(예: 회사 네트워크에 정책이 계속 적용되도록 합니다.
보고	신뢰할 수 있는 도메인이 탐지될 때마다 클라이언트는 백오프하며, 반드시 Umbrella 정책 또는 필터링을 수신할 필요는 없습니다. 네트워크가 다른 Umbrella 기능(예: 네트워크 보호) 그런 다음 네트워크 ID 아래의 보고서에 트래픽이 나타납니다.
DNS 트래픽	신뢰할 수 있는 네트워크에서 Umbrella 로밍 클라이언트는 DNS 쿼리를 방해하지 않으며 일반 내부 DNS 서버로 이동합니다.
프로브 메시지	Umbrella 로밍 클라이언트는 이 상태에서 대부분의 DNS '프로브' 테스트를 비활성화하므로 로밍 클라이언트에서 생성되는 트래픽의 양이 크게 줄어듭니다.

트러스트된 네트워크 도메인을 구성하는 방법:

1. 내부 DNS 서버에 DNS A 레코드를 만듭니다(예: magic.mydomain.tld).
    1. 레코드는 "하위 도메인"(최소 3개의 DNS 레이블)이어야 합니다.
    2. 레코드가 내부 RFC-1918 주소로 확인되어야 합니다.
    3. 레코드가 공개적으로 존재하지 않도록 주의하십시오.

2. Identities(ID) > Roaming Computers(로밍 컴퓨터)로 이동합니다.
3. (로밍 클라이언트 설정) 아이콘을 클릭합니다.
4. Trusted Network Domain(신뢰할 수 있는 네트워크 도메인) 옵션을 선택하고 도메인 이름을 입력합니다(예: magic.mydomain.tld). 저장을 클릭합니다.

Umbrella Virtual Appliance에서 Umbrella 로밍 클라이언트 사용

Umbrella 'Insights' 제품(Platform and Insights 패키지)의 일부로 네트워크 내 DNS 전달자 역할을 하는 Virtual Appliance(VA)를 제공합니다. 이 VA는 네트워크에서 DNS 요청의 소스에 대한 가시성을 확보하는 데 중요한 요소이며 Active Directory 통합에도 필요합니다.

기본적으로 Umbrella 로밍 클라이언트는 VA가 DNS 전달에 사용되고 있음을 탐지하는 경우 자신을 비활성화합니다. VA가 DNS 서버로 할당된 경우(DHCP 또는 고정 설정 사용) Umbrella 로밍 클라이언트가 이를 감지하고 자체 기능을 비활성화합니다.

VA 백오프

정책	VA 백오프가 활성화된 경우 VA ID를 사용하여 선택한 정책을 결정합니다. 정책은 다음 ID를 기반으로 생성할 수 있습니다. • AD 사용자(AD 통합이 활성화된 경우에만) • AD 컴퓨터(AD 통합이 활성화된 경우에만) • 내부 네트워크 • Umbrella 사이트 이름 정책 우선 순위에 대한 자세한 내용을 보려면 여기를 클릭하십시오.
보고	VA Backoff가 활성화된 경우 Umbrella 로밍 클라이언트는 VA 뒤에 있으면 비활성화되고 보고서에 표시되지 않습니다. 보고는 다음 중 하나로 기록됩니다. • AD 사용자(AD 통합이 활성화된 경우에만) • AD 컴퓨터(AD 통합이 활성화된 경우에만) • 내부 네트워크 • Umbrella 사이트 이름 또한 내부 클라이언트 IP 주소는 요청마다 기록됩니다. 
DNS 트래픽	• Umbrella 로밍 클라이언트는 DNS 쿼리를 방해하지 않으며 가상 어플라이언스로 이동합니다. • VA는 외부 DNS 쿼리를 Umbrella(암호화)로 전달합니다.

	• VA는 내부 DNS 쿼리를 적절하게 라우팅하고 구성된 내부 DNS 서버로 전달합니다.
프로브 메시지	Umbrella 로밍 클라이언트는 프로브 메시지를 Umbrella로 전송하지만 전송 속도는 더 낮습니다.

VA 백오프를 구성하는 방법:

1. 이 기능은 기본적으로 활성화되어 있지만 상태를 확인할 수 있으며 선택적으로 비활성화할 수도 있습니다
2. Identities(ID) > Roaming Computers(로밍 컴퓨터)로 이동합니다.
3. (로밍 클라이언트 설정) 아이콘을 클릭합니다.
4. VA 백오프 옵션 선택

Cisco Umbrella AnyConnect 로밍 보안 모듈

Cisco AnyConnect용 Umbrella 모듈은 위에서 설명한 것과 동일한 모든 작동 모드를 지원합니다. 두 가지 추가 AnyConnect 관련 모드도 사용할 수 있습니다. Identities(ID) > Roaming Computers(로밍 컴퓨터) 페이지의 Umbrella Dashboard(Umbrella 대시보드)에서 이 두 모드를 모두 활성화할 수 있지만 AnyConnect VPN 프로파일 내에 추가 컨피그레이션이 필요합니다.

- AnyConnect Trusted Network Detection을 존중합니다.
  이 기능은 Cisco AnyConnect가 Trusted Network에 있다고 판단할 때 Umbrella Security 모듈을 비활성화합니다. 이는 AnyConnect의 Trusted Network Detection 기능을 통해 네트워크를 식별합니다. 신뢰할 수 있는 도메인, DNS 서버 및 URL을 사용하여 회사 네트워크를 식별할 수 있습니다. 자세한 내용은 AnyConnect 설명서를 참조하십시오.
- 전체 터널 VPN 세션이 활성 상태일 때 로밍 클라이언트 비활성화
  이 기능을 활성화하면 AnyConnect가 전체 터널(또는 모든 DNS 터널) VPN에 연결될 때 Umbrella 모듈이 비활성화됩니다.

비활성화된 경우 로밍 클라이언트는 DNS 트래픽을 필터링하지 않으므로, 네트워크 보호 기능과 같은 다른 보안에서 네트워크를 보호하도록 하는 것이 중요합니다.

추가 정보

회사 네트워크에서 로밍 클라이언트를 비활성화하고 싶지만 더 많은 제어가 필요하거나 다른 옵션에 대해 논의하려면 Cisco Umbrella 지원에 문의하십시오.

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.