AnyConnect 종속 포털 탐지 및 교정

목차

소개

이 문서에서는 Cisco AnyConnect Mobility Client 종속 포털 탐지 기능 및 기능이 올바르게 작동하기 위한 요구 사항에 대해 설명합니다.호텔, 레스토랑, 공항 및 기타 공공 장소의 많은 무선 핫스팟은 사용자 인터넷 액세스를 차단하기 위해 종속 포털을 사용합니다.HTTP 요청을 자체 웹 사이트로 리디렉션합니다. 이 웹 사이트에서는 사용자가 자격 증명을 입력하거나 핫스팟 호스트의 약관을 승인해야 합니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco AnyConnect Secure Mobility Client에 대한 지식을 보유하고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- AnyConnect 버전 3.1.04072
- Cisco ASA(Adaptive Security Appliance) 버전 9.1.2

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

공항, 커피숍, 호텔 등 Wi-Fi 및 유선 액세스를 제공하는 많은 시설에서는 사용자가 액세스 권한을 얻기 전에 요금을 지불하도록 요구하고, 허용되는 사용 정책을 준수하도록 동의하거나, 또는 둘 다 마찬가지입니다.이러한 기능은 사용자가 브라우저를 열고 액세스 조건을 수락할 때까지 애플리케이션이 연결되지 않도록 종속 포털이라는 기술을 사용합니다.

종속 포털 교정 요구 사항

종속 포털 탐지 및 교정을 모두 지원하려면 다음 라이센스 중 하나가 필요합니다.

- AnyConnect Premium(SSL(Secure Sockets Layer) VPN Edition)
- Cisco AnyConnect Secure Mobility

AnyConnect Essentials 또는 AnyConnect Premium 라이센스와 함께 종속 포털 탐지 및 교정을 지원하기 위해 Cisco AnyConnect Secure Mobility 라이센스를 사용할 수 있습니다.

> **참고**: 종속 포털 탐지 및 교정은 사용 중인 AnyConnect 릴리스에서 지원하는 Microsoft Windows 및 Macintosh OS X 운영 체제에서 지원됩니다.

종속 포털 핫스팟 탐지

AnyConnect는 GUI**에서 연결할** 수 없는 경우 **VPN 서버** 메시지에 **연결할 수 없음**(원인**과** 상관없이)을 표시합니다.VPN 서버는 보안 게이트웨이를 지정합니다.Always-on이 활성화되고 종속 포털이 없는 경우 클라이언트는 VPN에 연결을 계속 시도하고 그에 따라 상태 메시지를 업데이트합니다.

Always-on VPN이 활성화된 경우 연결 실패 정책이 닫히고 종속 포털 보안은 비활성화되며 AnyConnect가 종속 포털의 존재를 탐지하면 AnyConnect GUI는 연결당 한 번, 다시 연결당 한 번 이 메시지를 표시합니다.

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

AnyConnect가 종속 포털의 존재를 탐지하고 AnyConnect 컨피그레이션이 이전에 설명한 것과 다른 경우 AnyConnect GUI는 연결당 한 번, 다시 연결당 한 번 이 메시지를 표시합니다.

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

> **주의:**종속 포털 감지는 기본적으로 활성화되어 있으며 구성할 수 없습니다. 종속 포털 감지 중에 AnyConnect는 브라우저 구성 설정을 수정하지 않습니다.

종속 포털 핫스팟 교정

종속 포털 교정은 네트워크 액세스를 얻기 위해 종속 포털 핫스팟의 요구 사항을 충족하는 프로세스입니다.

AnyConnect는 종속 포털을 치료하지 않습니다.엔드 유저가 교정을 수행하는 데 의존합니다.

종속 포털 교정을 수행하기 위해 최종 사용자는 핫스팟 공급자의 요구 사항을 충족합니다.이러한 요구 사항에는 네트워크에 액세스하는 데 드는 비용 지불, 사용 제한 정책에 대한 서명, 둘 다 또는

공급자가 정의한 기타 요구 사항이 포함될 수 있습니다.

AnyConnect Always-On이 활성화되고 Connect 실패 정책이 Closed로 설정된 경우 종속 포털 교정이 AnyConnect VPN 클라이언트 프로파일에서 명시적으로 허용되어야 합니다.Always-on이 활성화되고 Connect Failure(연결 실패) 정책이 Open(열기)으로 설정된 경우 사용자가 네트워크 액세스에서 제한되지 않으므로 AnyConnect VPN 클라이언트 프로파일에서 종속 포털 교정을 명시적으로 허용하지 않아도 됩니다.

False Captive Portal 탐지

이러한 상황에서 AnyConnect는 종속 포털에 있다고 잘못 판단할 수 있습니다.

- AnyConnect가 잘못된 서버 이름(CN)이 포함된 인증서를 사용하여 ASA에 연결을 시도하면 AnyConnect 클라이언트는 종속 포털 환경에 있는 것으로 간주합니다.

  이 문제를 방지하려면 ASA 인증서가 올바르게 구성되었는지 확인하십시오.인증서의 CN 값은 VPN 클라이언트 프로파일의 ASA 서버 이름과 일치해야 합니다.

- ASA에 대한 HTTPS 액세스를 차단하여 ASA에 연결하려는 클라이언트의 시도에 응답하는 ASA 전에 네트워크에 다른 디바이스가 있으면 AnyConnect 클라이언트는 종속 포털 환경에 있는 것으로 간주합니다.사용자가 내부 네트워크에 있고 ASA에 연결하기 위해 방화벽을 통해 연결할 때 이러한 상황이 발생할 수 있습니다.

  회사 내에서 ASA에 대한 액세스를 제한해야 하는 경우 ASA 주소에 대한 HTTP 및 HTTPS 트래픽이 HTTP 상태를 반환하지 않도록 방화벽을 구성합니다.ASA로 전송된 HTTP/HTTPS 요청이 예기치 않은 응답을 반환하지 않도록 하려면 ASA에 대한 HTTP/HTTPS 액세스를 허용하거나 완전히 차단해야 합니다(블랙홀이라고도 함).

AnyConnect 동작

이 섹션에서는 AnyConnect의 작동 방식을 설명합니다.

1. AnyConnect는 XML 프로필에 정의된 FQDN(Fully Qualified Domain Name)에 HTTPS 프로브를 시도합니다.

2. 인증서 오류(신뢰할 수 없음/잘못된 FQDN)가 있는 경우 AnyConnect는 XML 프로파일에 정의된 FQDN에 대한 HTTP 프로브를 시도합니다.HTTP 302 이외의 응답이 있는 경우 종속 포털 뒤에 있는 것으로 간주합니다.

종속 포털이 IKEV2로 잘못 탐지됨

포트 443에서 ASDM(Adaptive Security Device Manager) 포털을 실행하는 SSL 인증이 비활성화된 ASA에 대한 IKEv2(Internet Key Exchange Version 2) 연결을 시도하면 종속 포털 탐지에 대해 수행된 HTTPS 프로브는 ASDM 포털(**/admin/public/index.html**)으로 리디렉션됩니다. 클라이언트가 이를 예상하지 않으므로 종속 포털 리디렉션처럼 보이며 종속 포털 리미디에이션이 필요한 것처럼 보이기 때문에 연결 시도를 차단합니다.

해결 방법

이 문제가 발생하는 경우 다음과 같은 몇 가지 해결 방법이 있습니다.

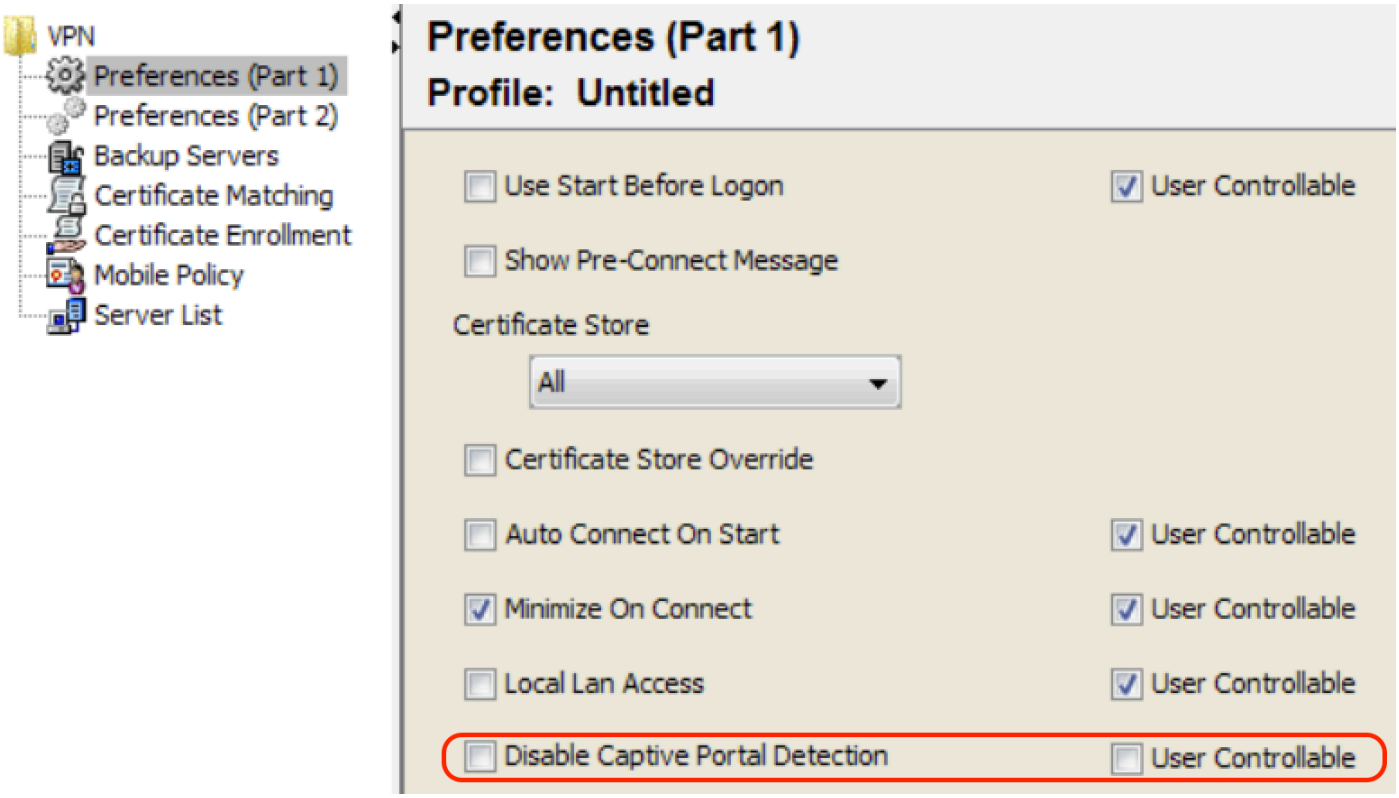
- ASA가 인터페이스에서 HTTP 연결을 수신하지 않도록 해당 인터페이스에서 HTTP 명령을 제거합니다.
- 인터페이스에서 SSL 신뢰 지점을 제거합니다.
- IKEV2 클라이언트 서비스를 활성화합니다.
- 인터페이스에서 WebVPN을 활성화합니다.

이 문제는 버전 3.1(3103)에서 Cisco 버그 ID CSCud17825로 해결되었습니다.

> **주의:**Cisco IOS® 라우터에 대해서도 동일한 문제가 있습니다.Cisco IOS에서 IP **http 서버**가 활성화되어 있는 경우, 동일한 상자가 PKI 서버와 사용되는 경우 AnyConnect는 종속 포털을 잘못 탐지합니다.해결 방법은 인증을 요청하는 대신 AnyConnect HTTP 요청에 대한 응답을 중지하기 위해 **ip http access-class**를 사용하는 것입니다.

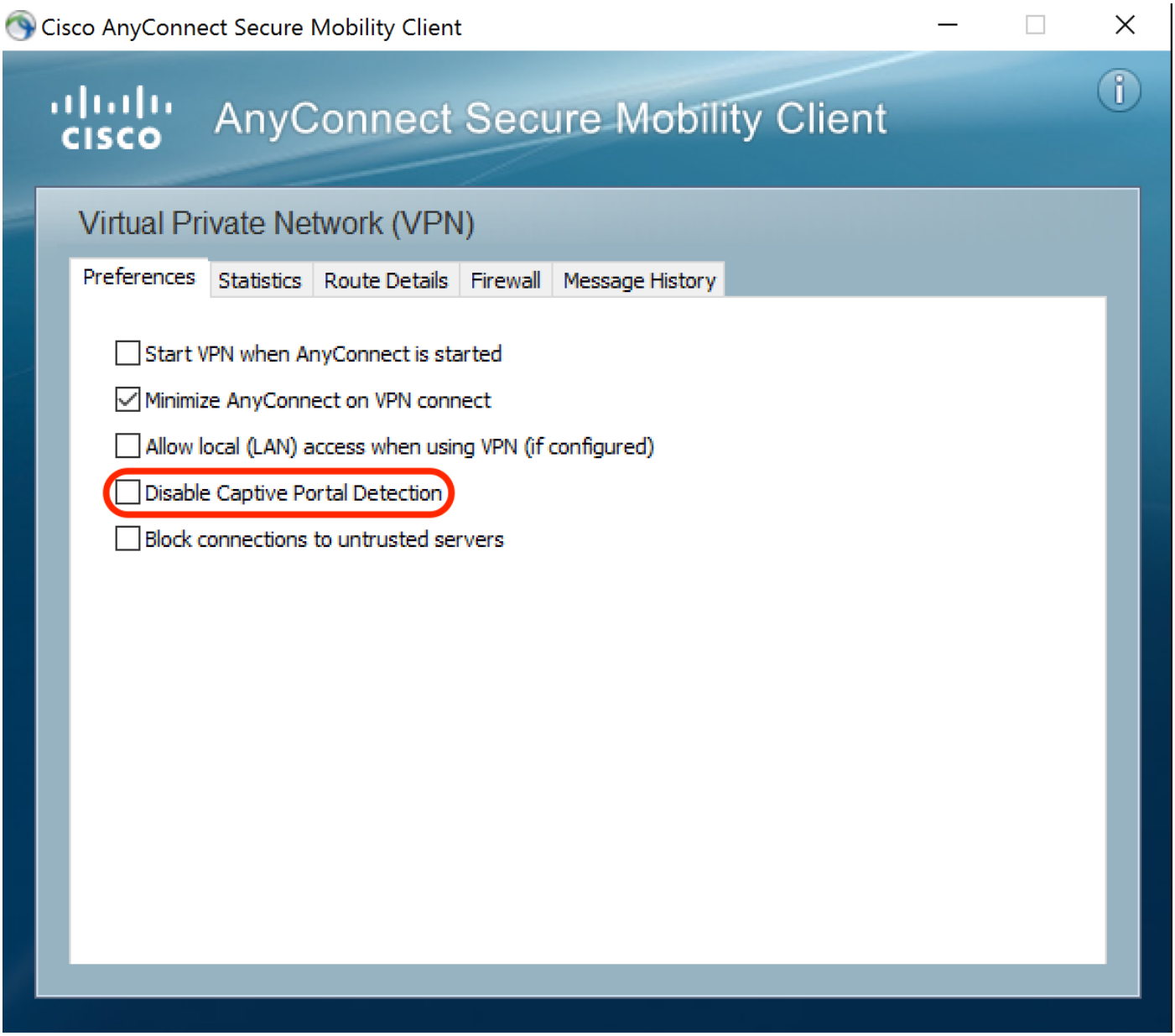
종속 포털 기능 비활성화

AnyConnect 클라이언트 버전 4.2.00096 이상에서 종속 포털 기능을 비활성화할 수 있습니다(Cisco 버그 ID CSCud97386 참조). 관리자는 옵션을 사용자가 구성 가능 또는 사용 안 함으로 설정할지 여부를 결정할 수 있습니다.이 옵션은 프로파일 편집기의 기본 설정(1부) 섹션에서 사용할 수 있습니다.관리자는 이 프로파일 편집기 스냅샷에 표시된 대로 **Disable Captive Portal Detection** 또는 **User Controllable**을 선택할 수 있습니다.



사용자 제어 가능 을 선택하면 AnyConnect Secure Mobility Client UI의 기본 설정 탭에 다음과 같이

확인란이 나타납니다.


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Start VPN when AnyConnect is started
Minimize AnyConnect on VPN connect
Allow local (LAN) access when using VPN (if configured)
Disable Captive Portal Detection
Block connections to untrusted servers