ASA/AnyConnect 동적 스플릿 터널링 구성

목차

소개

이 문서에서는 ASDM을 통한 동적 스플릿 제외 터널링을 위해 AnyConnect Secure Mobility Client를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA에 대한 기본 지식
- Cisco AnyConnect Security Mobility Client에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- ASA 9.12(3)9
- ASDM(Adaptive Security Device Manager) 7.13(1)

- AnyConnect 4.7.0

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.

배경 정보

AnyConnect 스플릿 터널링을 사용하면 Cisco AnyConnect Secure Mobility Client가 IKEV2 또는 SSL(Secure Sockets Layer)을 통해 기업 리소스에 안전하게 액세스할 수 있습니다.

AnyConnect 버전 4.5 이전에는 ASA(Adaptive Security Appliance)에 구성된 정책에 따라 스플릿 터널 동작이 Tunnel Specified, Tunnel All 또는 Exclude Specified일 수 있습니다.

클라우드 호스팅 컴퓨터 리소스의 등장으로 인해 서비스는 사용자의 위치 또는 클라우드 호스팅 리소스의 로드를 기준으로 다른 IP 주소로 해결하는 경우가 있습니다.

AnyConnect Secure Mobility Client는 고정 서브넷 범위, 호스트 또는 IPV4 또는 IPV6 풀로 스플릿 터널링을 제공하므로 네트워크 관리자가 AnyConnect를 구성하는 동안 도메인/FQDN을 제외하는 것이 어려워집니다.

예를 들어 네트워크 관리자가 스플릿 터널 컨피그레이션에서 Cisco.com 도메인을 제외하려고 하지만 Cisco.com이 클라우드 호스트이므로 에 대한 DNS 매핑이 변경됩니다.

AnyConnect는 Dynamic Split Exclude 터널링을 사용하여 호스트된 애플리케이션의 IPv4/IPv6 주소를 동적으로 확인하고 연결이 터널 외부에서 이루어질 수 있도록 라우팅 테이블 및 필터에서 필요한 변경을 수행합니다.

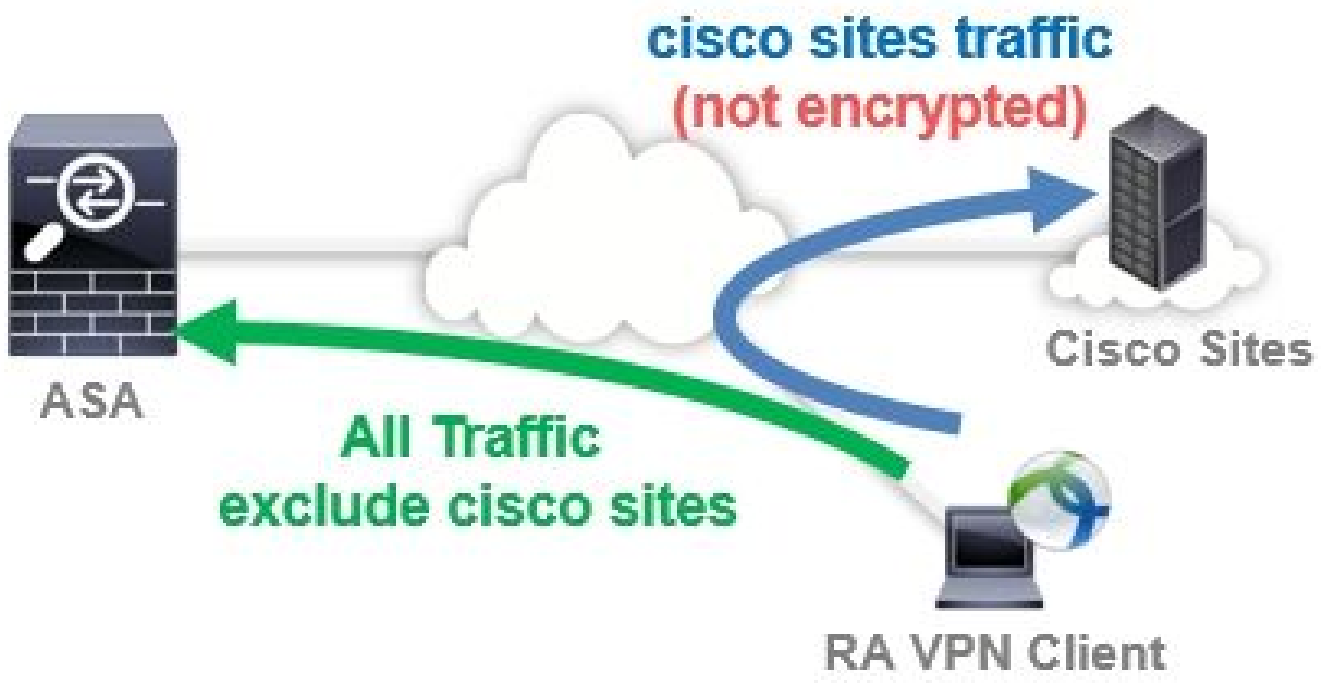
AnyConnect 4.5부터 AnyConnect가 호스트된 애플리케이션의 IPv4/IPv6 주소를 동적으로 확인하고 라우팅 테이블 및 필터에서 필요한 변경을 수행하여 터널 외부에서 연결을 허용하는 동적 스플릿 터널링을 사용할 수 있습니다

설정

이 섹션에서는 ASA에서 Cisco AnyConnect Secure Mobility Client를 구성하는 방법에 대해 설명합니다.

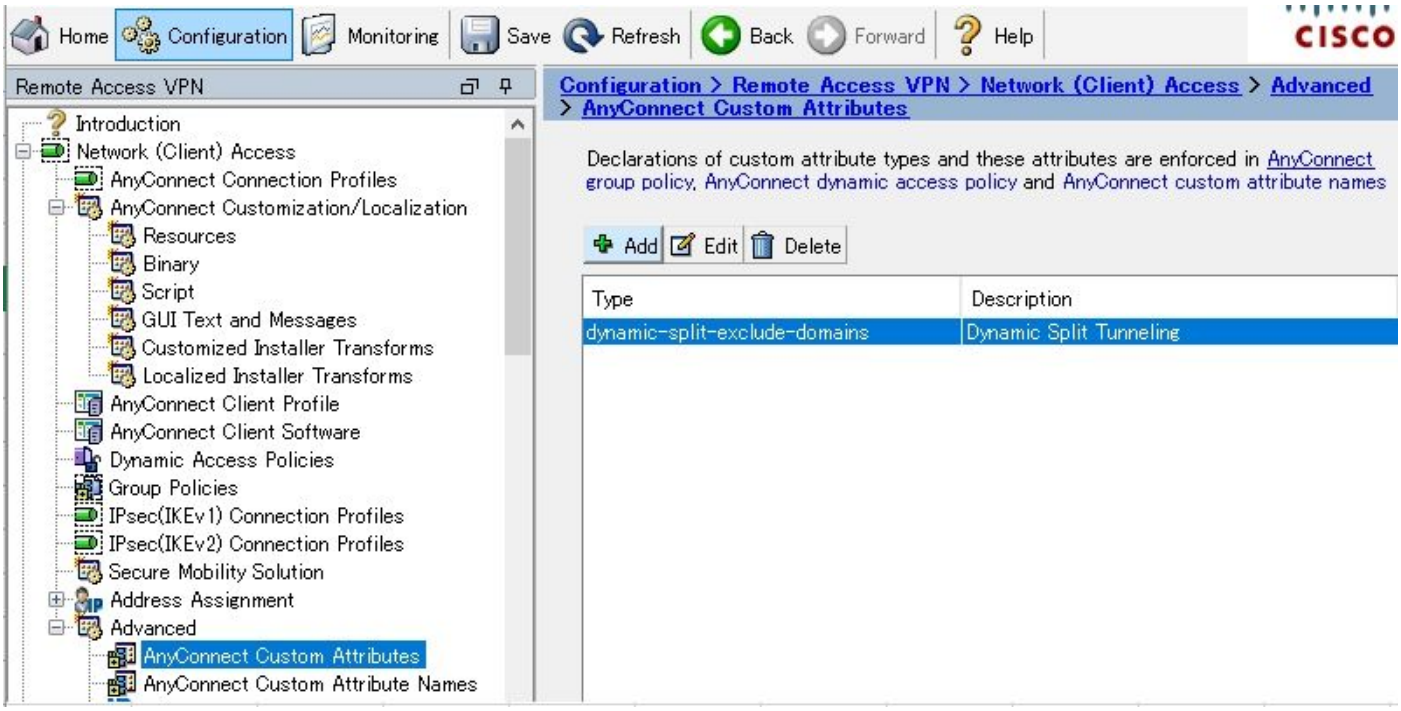
네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용되는 토폴로지를 보여 줍니다.



1단계. AnyConnect 사용자 지정 특성 생성

탐색 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.** 클릭 **Add** 단추 및 설정 **dynamic-split-exclude-domains** 이미지에 표시된 대로 특성 및 설명(선택 사항):

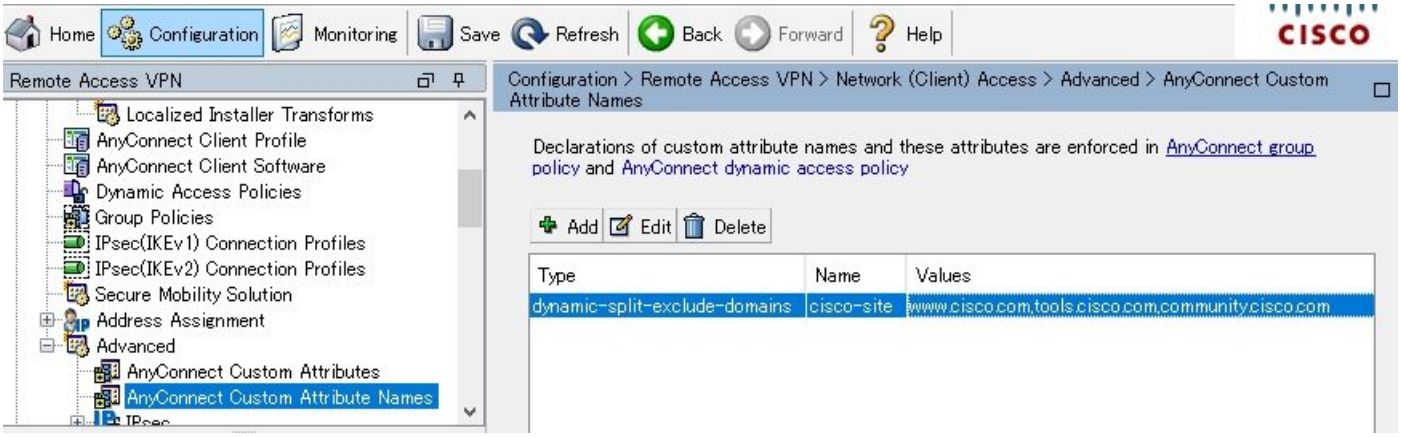


2단계. AnyConnect 사용자 지정 이름 생성 및 값 구성

탐색 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** 클릭 **Add** 단추를 누르고 **dynamic-split-exclude-domains** 이미지에 표시된 대로 Type, 임의의 이름 및 Values에서

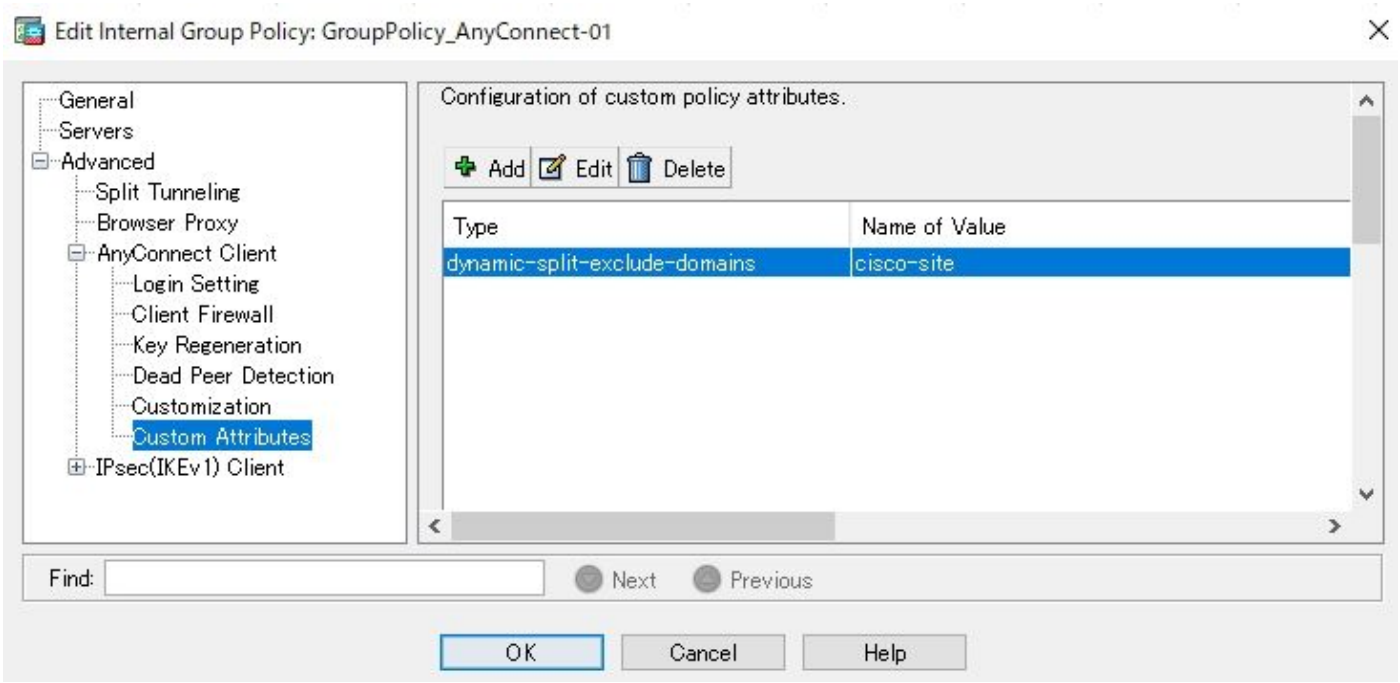
앞서 생성된 특성:

이름에 공백을 입력하지 않도록 주의하십시오. (예: Possible cisco-site, Impossible cisco site) Values의 여러 도메인 또는 FQDN이 등록된 경우 쉼표(,)로 구분하십시오.



3단계. 그룹 정책에 유형 및 이름 추가

탐색 **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** 그룹 정책을 선택합니다. 그런 다음 **Advanced> AnyConnect Client> Custom Attributes** 구성된 **Type** 및 **Name**, 이미지에 표시된 대로



CLI 컨피그레이션 예

이 섹션에서는 참조를 위해 동적 스플릿 터널링의 CLI 컨피그레이션을 제공합니다.

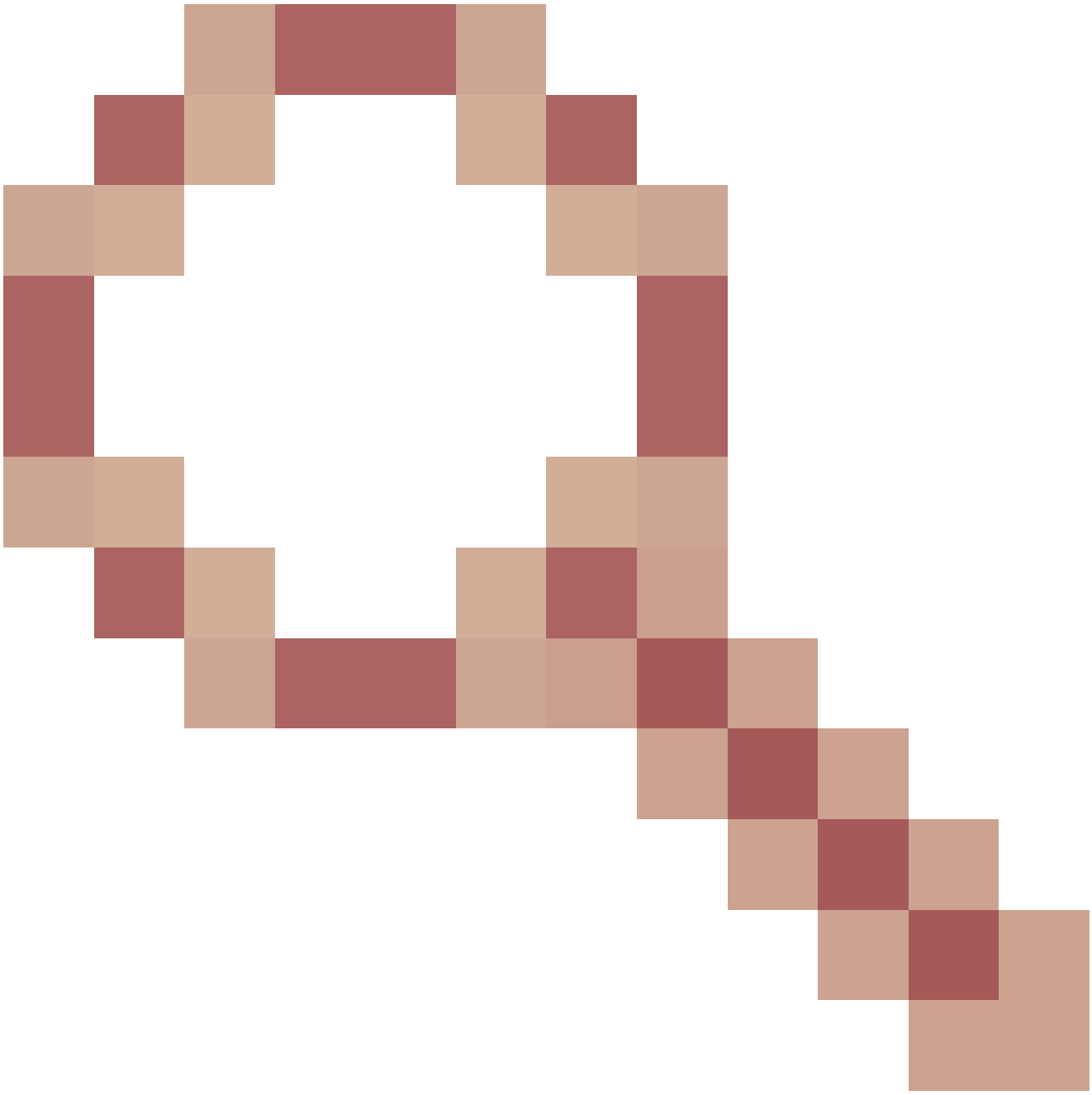
<#root>

```
ASAv10# show run
  --- snip ---
```

```
webvpn

 enable outside

 AnyConnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling


 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 AnyConnect image disk0:/AnyConnect-win-4.7.04056-webdeploy-k9.pkg 1
 AnyConnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable

AnyConnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.


group-policy GroupPolicy_AnyConnect-01 internal

group-policy GroupPolicy_AnyConnect-01 attributes


 wins-server none
 dns-server value 10.0.0.0
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 split-tunnel-network-list value SplitACL
 default-domain value cisco.com

 AnyConnect-custom dynamic-split-exclude-domains value cisco-site
```

제한 사항

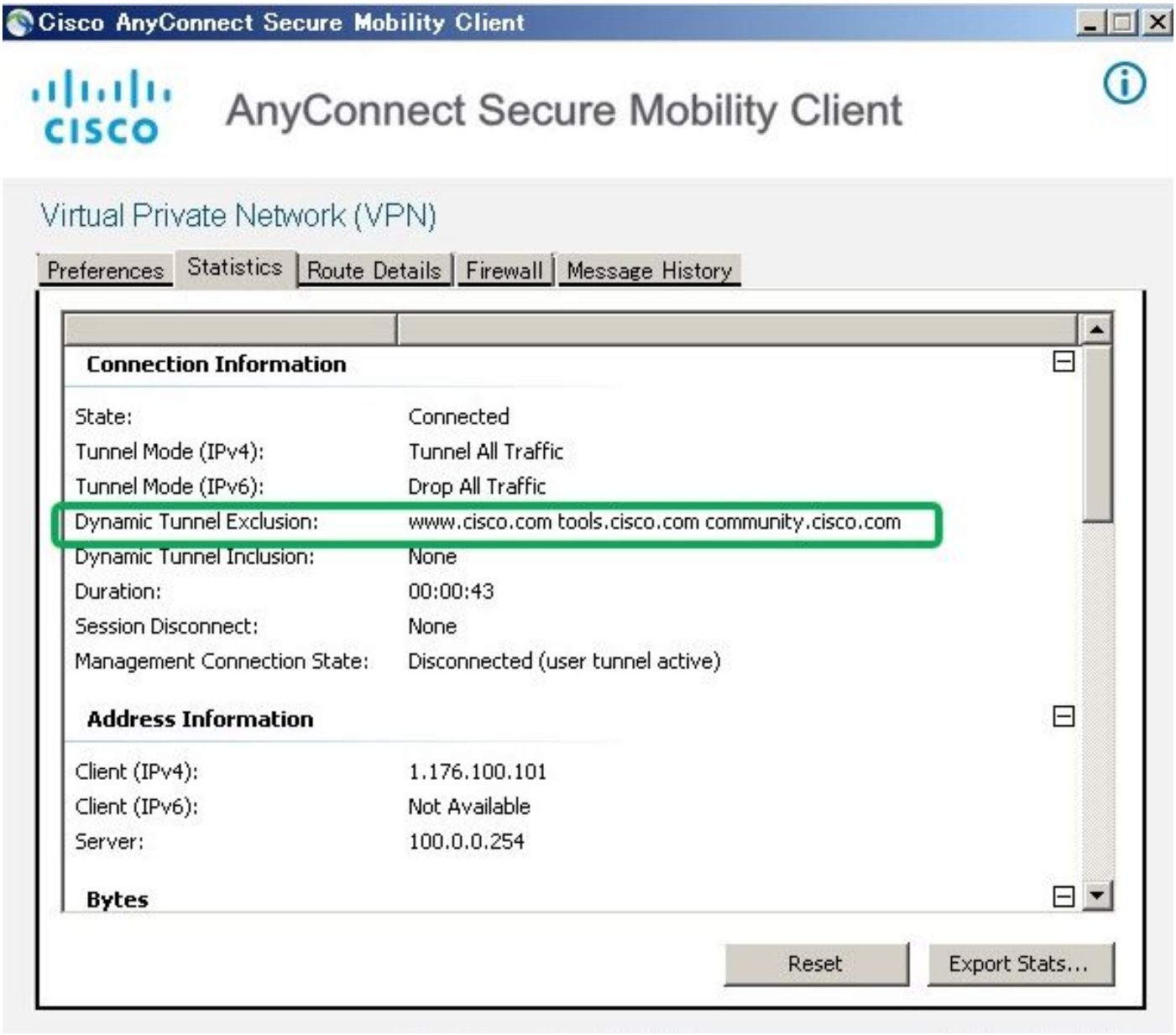
- 동적 스플릿 터널링 사용자 지정 특성을 사용하려면 ASA 버전 9.0 이상이 필요합니다.
- 값 필드의 와일드카드는 지원되지 않습니다.
- iOS(Apple) 디바이스에서는 동적 스플릿 터널링이 지원되지 않습니다(개선 요청: Cisco 버그 ID CSCvr54798



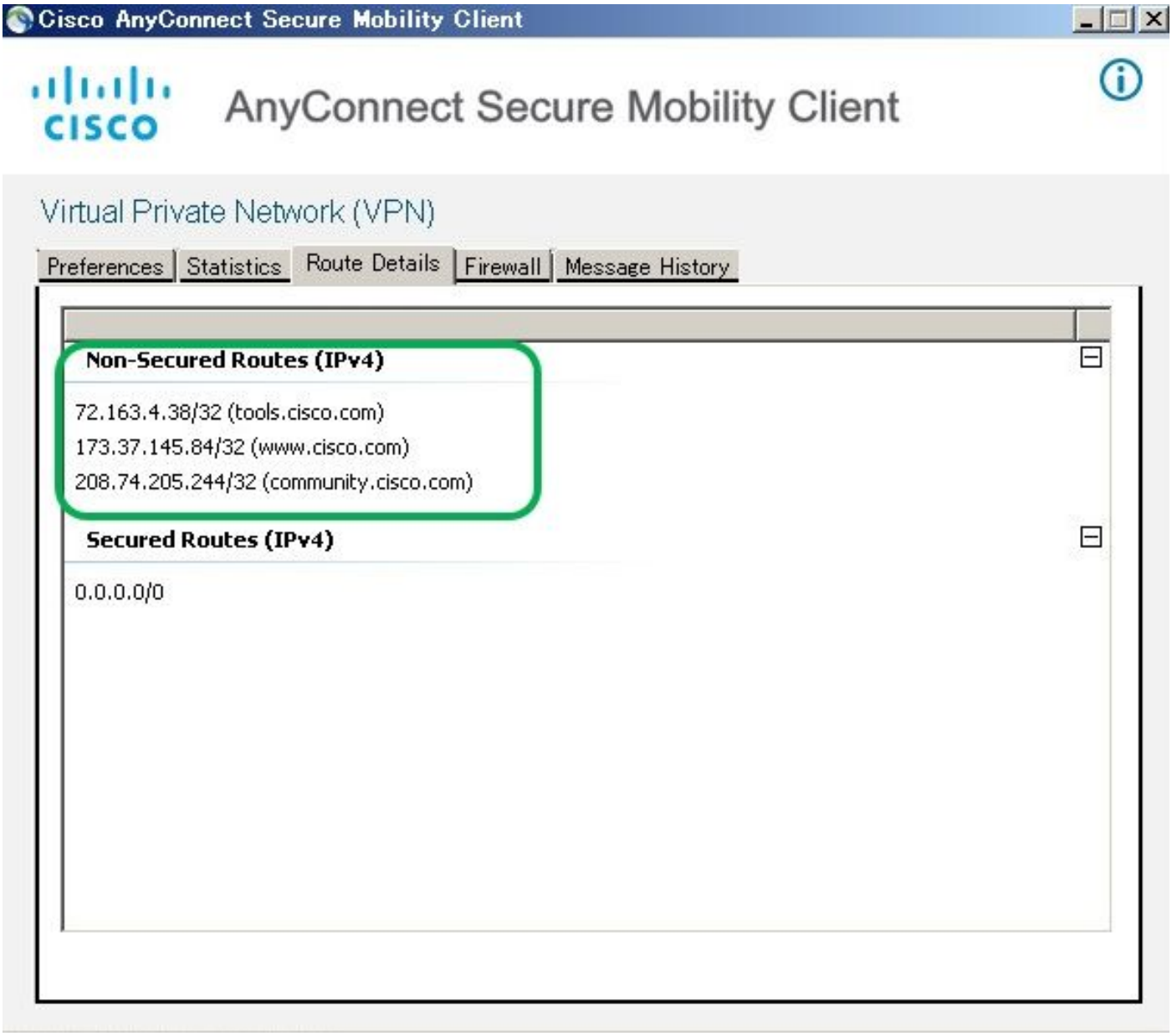
).

다음을 확인합니다.

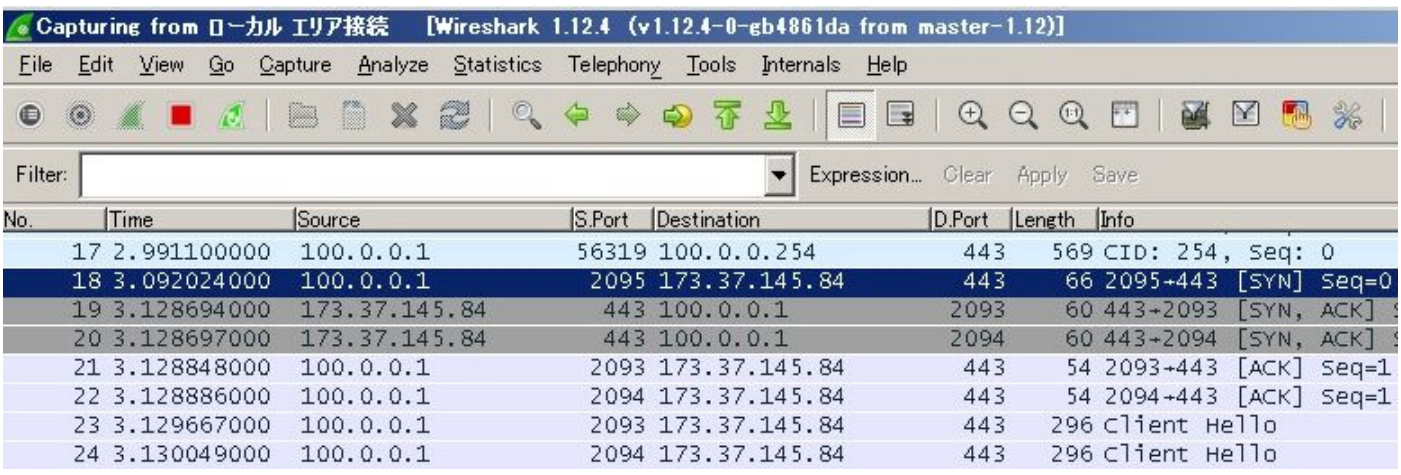
구성된 것을 확인하기 위해 **Dynamic Tunnel Exclusions**, 발사AnyConnect클라이언트의 소프트웨어를 클릭하고 **Advanced Window>Statistics**, 그림과 같이



또한 다음 사이트로 이동할 수 있습니다 **Advanced Window>Route Details** 확인할 수 있는 탭**Dynamic Tunnel Exclusions**아래에 나열되어 있습니다.**Non-Secured Routes**, 그림에 표시된 것과 같습니다.



이 예에서는 아래에 www.cisco.com을 구성했습니다.**Dynamic Tunnel Exclusion list**AnyConnect 클라이언트 물리적 인터페이스에서 수집된 Wireshark 캡처는 www.cisco.com(198.51.100.0)에 대한 트래픽이 DTLS에 의해 암호화되지 않았음을 확인합니다.



문제 해결

와일드카드가 값 필드에 사용되는 경우

값 필드에 와일드카드가 구성되어 있는 경우(예: *.cisco.com이 Values에 구성되어 있는 경우) AnyConnect 세션의 연결이 로그와 같이 끊어집니다.

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Fir
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Cli
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (17
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Web
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session
```

참고: 대안으로 Values(값)의 cisco.com 도메인을 사용하여 www.cisco.com 및 tools.cisco.com과 같은 FQDN을 허용할 수 있습니다.

Route Details(경로 세부사항) 탭에 비보안 경로가 표시되지 않는 경우

AnyConnect 클라이언트는 제외된 목적지에 대한 트래픽을 시작할 때 Route Details(경로 세부사항) 탭에서 IP 주소와 FQDN을 자동으로 인식하고 추가합니다.

AnyConnect 사용자가 올바른 Anyconnect 그룹 정책에 할당되었는지 확인하려면 명령을 실행합니다 **show vpn-sessiondb anyconnect filter name**

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco

Session Type: AnyConnect

Username     : cisco                  Index : 7
Assigned IP  : 172.16.0.0          Public IP : 10.0.0.0
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx     : 7795373                Bytes Rx : 390956
```

Group Policy : GroupPolicy_AnyConnect-01

```
Tunnel Group : AnyConnect-01
Login Time   : 13:20:48 UTC Tue Mar 31 2020
Duration     : 20h:19m:47s
```

```
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN : none
Audt Sess ID : 019600a9000070005e8343b0
Security Grp : none
```

일반 문제 해결

AnyConnect Diagnostics and Reporting Tool(DART)을 사용하여 AnyConnect 설치 및 연결 문제를 해결하는 데 유용한 데이터를 수집할 수 있습니다. DART 마법사는 AnyConnect를 실행하는 컴퓨터에서 사용됩니다. DART는 Cisco TAC(Technical Assistance Center) 분석을 위해 로그, 상태 및 진단 정보를 취합하며 클라이언트 시스템에서 실행하는 데 관리자 권한이 필요하지 않습니다.

관련 정보

- Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 4.7 - 동적 스플릿 터널링 정보
- ASDM Book 3: Cisco ASA Series VPN ASDM 컨피그레이션 가이드, 7.13 - 동적 스플릿 터널링 구성

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.