ASA/AnyConnect Dynamic Split Tunneling konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der AnyConnect Secure Mobility Client für Dynamic Split Exclude Tunneling über ASDM konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der ASA
- Grundkenntnisse des Cisco AnyConnect Security Mobility Client

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- ASA 9.12(3)9
- Adaptive Security Device Manager (ASDM) 7.13(1)
- AnyConnect 4.7.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die

möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

AnyConnect Split-Tunneling ermöglicht dem Cisco AnyConnect Secure Mobility Client den sicheren Zugriff auf Unternehmensressourcen über IKEV2 oder Secure Sockets Layer (SSL).

Vor AnyConnect Version 4.5 konnte das Split-Tunnelverhalten auf Basis der mit der Adaptive Security Appliance (ASA) konfigurierten Richtlinie auf "Tunnel Specified", "Tunnel All" oder "Exclude Specified" gesetzt werden.

Sobald in der Cloud gehostete Computerressourcen verfügbar sind, werden Services je nach Standort des Benutzers oder der Auslastung der in der Cloud gehosteten Ressourcen manchmal zu einer anderen IP-Adresse aufgelöst.

Da der AnyConnect Secure Mobility Client Split-Tunneling zu einem statischen Subnetzbereich, Host oder Pool von IPV4 oder IPV6 bereitstellt, wird es für Netzwerkadministratoren schwierig, Domänen/FQDNs auszuschließen, während sie AnyConnect konfigurieren.

Beispielsweise möchte ein Netzwerkadministrator die Domäne Cisco.com von der Split-Tunnelkonfiguration ausschließen, aber die DNS-Zuordnung für Cisco.com ändert sich, da sie in der Cloud gehostet wird.

Mit Dynamic Split Exclude Tunneling löst AnyConnect dynamisch die IPv4/IPv6-Adresse der gehosteten Anwendung auf und nimmt die erforderlichen Änderungen an der Routing-Tabelle und den Filtern vor, damit die Verbindung außerhalb des Tunnels hergestellt werden kann.

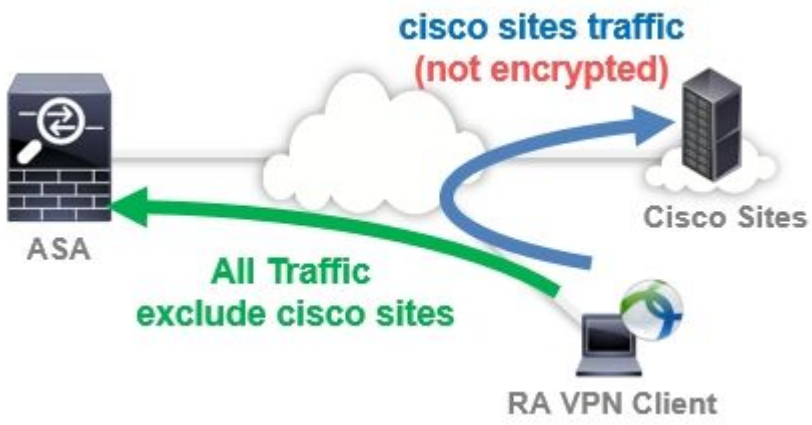
Ab AnyConnect 4.5 kann Dynamic Spit Tunneling verwendet werden, bei dem Anyconnect die IPv4/IPv6-Adresse der gehosteten Anwendung dynamisch auflöst und die erforderlichen Änderungen an der Routing-Tabelle und den Filtern vornimmt, damit die Verbindung außerhalb des Tunnels hergestellt werden kann

Konfiguration

In diesem Abschnitt wird die Konfiguration von Cisco AnyConnect Secure Mobility Client auf der ASA beschrieben.

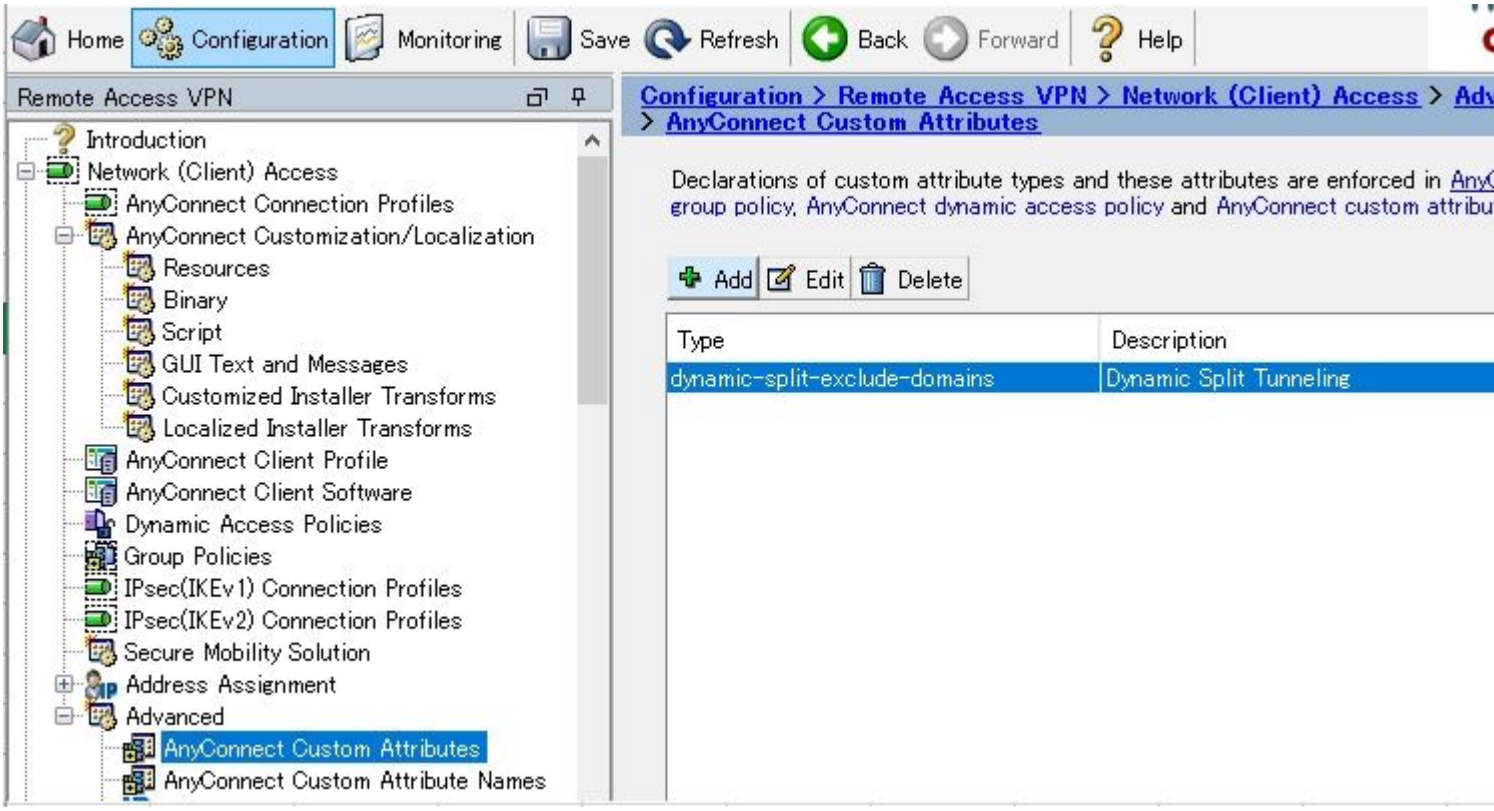
Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für die Beispiele dieses Dokuments verwendet wird.



Schritt 1: Erstellen von benutzerdefinierten AnyConnect-Attributen

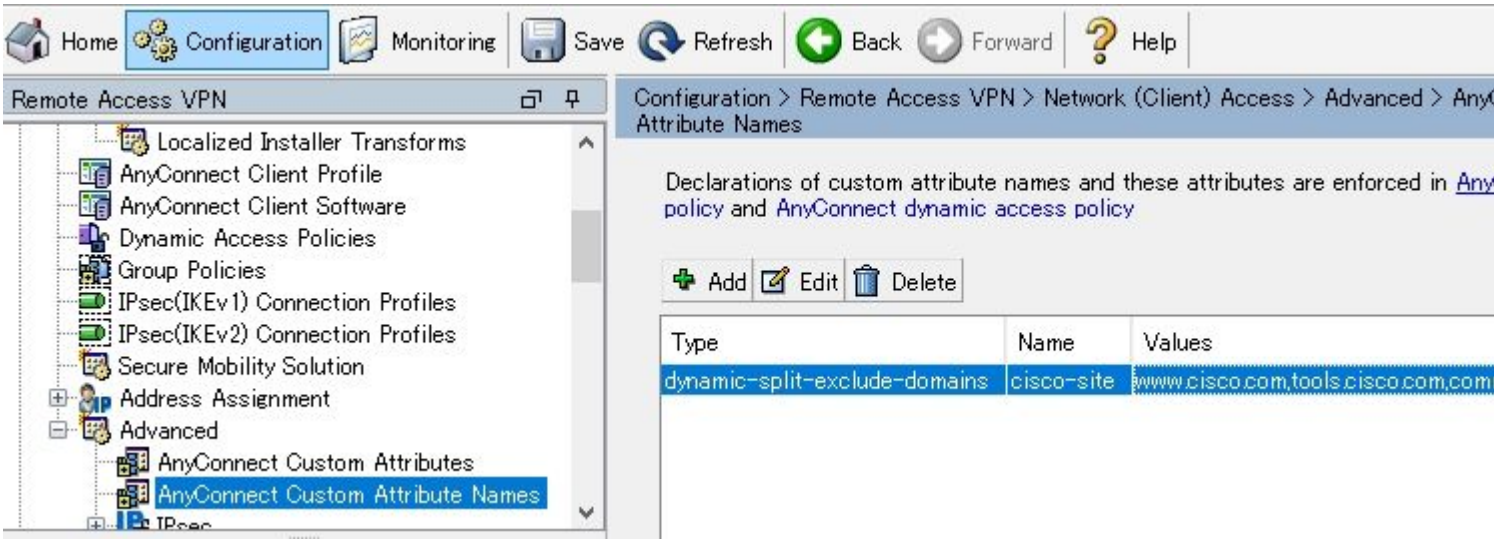
Navigieren Sie zu **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.**Klicken Sie auf **Add** Taste und setzen **dynamic-split-exclude-domains** Attribut und optionale Beschreibung, wie in der Abbildung dargestellt:



Schritt 2: Erstellen eines benutzerdefinierten AnyConnect-Namens und Konfigurieren von Werten

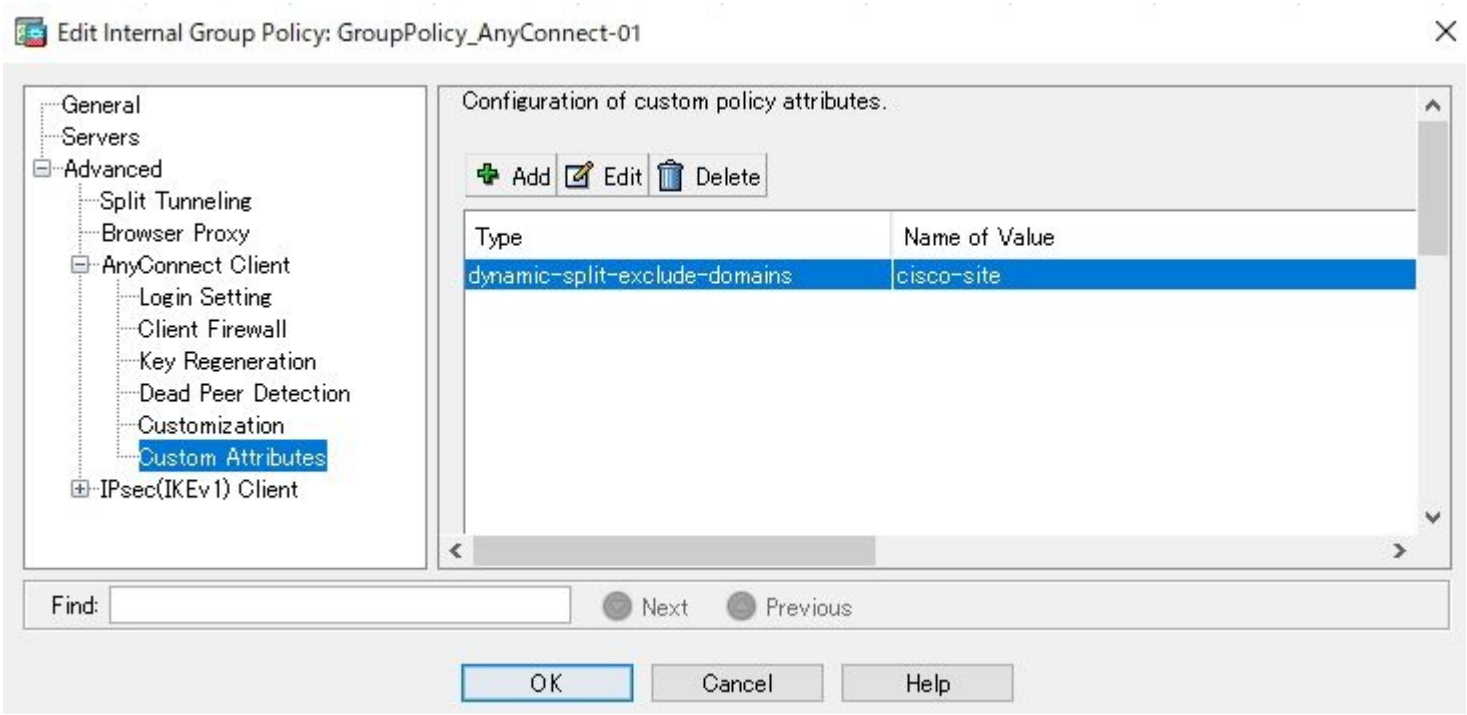
Navigieren Sie zu **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.**Klicken Sie auf **Add** -Taste und stellen Sie **dynamic-split-exclude-domains** -Attribut, das zuvor aus Type, einem beliebigen Namen und Values erstellt wurde, wie im Bild gezeigt:

Achten Sie darauf, dass Sie unter Name kein Leerzeichen eingeben. (Beispiel: Mögliche "cisco-site" Impossible "cisco site") Wenn mehrere Domänen oder FQDNs in Values registriert sind, trennen Sie sie durch ein Komma (,).



Schritt 3: Fügen Sie der Gruppenrichtlinie Typ und Name hinzu.

Navigieren Sie zu **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** und eine Gruppenrichtlinie auswählen. Navigieren Sie anschließend zu **Advanced> AnyConnect Client> Custom Attributes** und die konfigurierten **Type** und **Name,** wie in der Abbildung dargestellt:



CLI-Konfigurationsbeispiel

In diesem Abschnitt wird die CLI-Konfiguration von Dynamic Split Tunneling zu Referenzzwecken beschrieben.

<#root>

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

webvpn

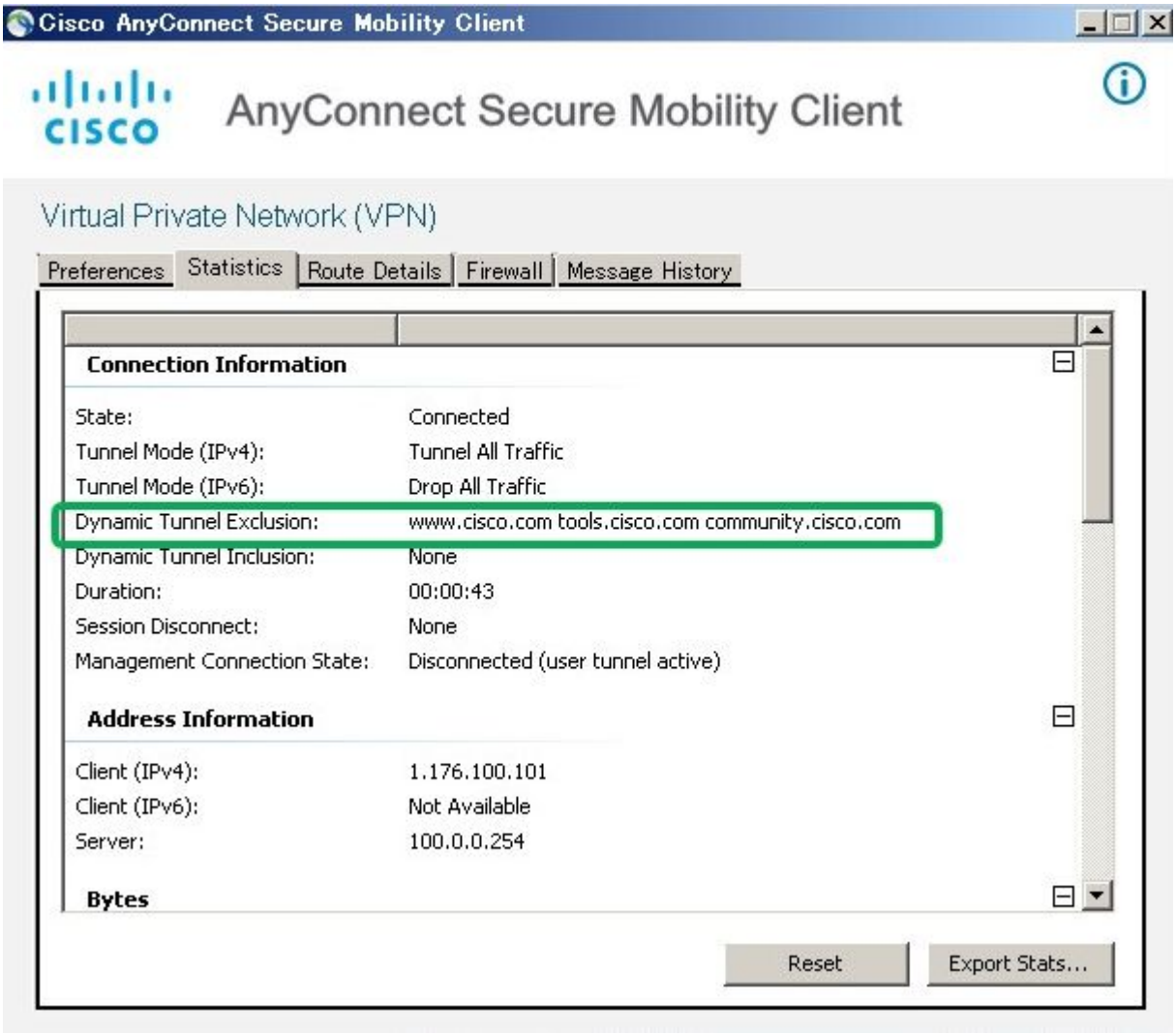
```
 enable outside

 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
```

Einschränkungen

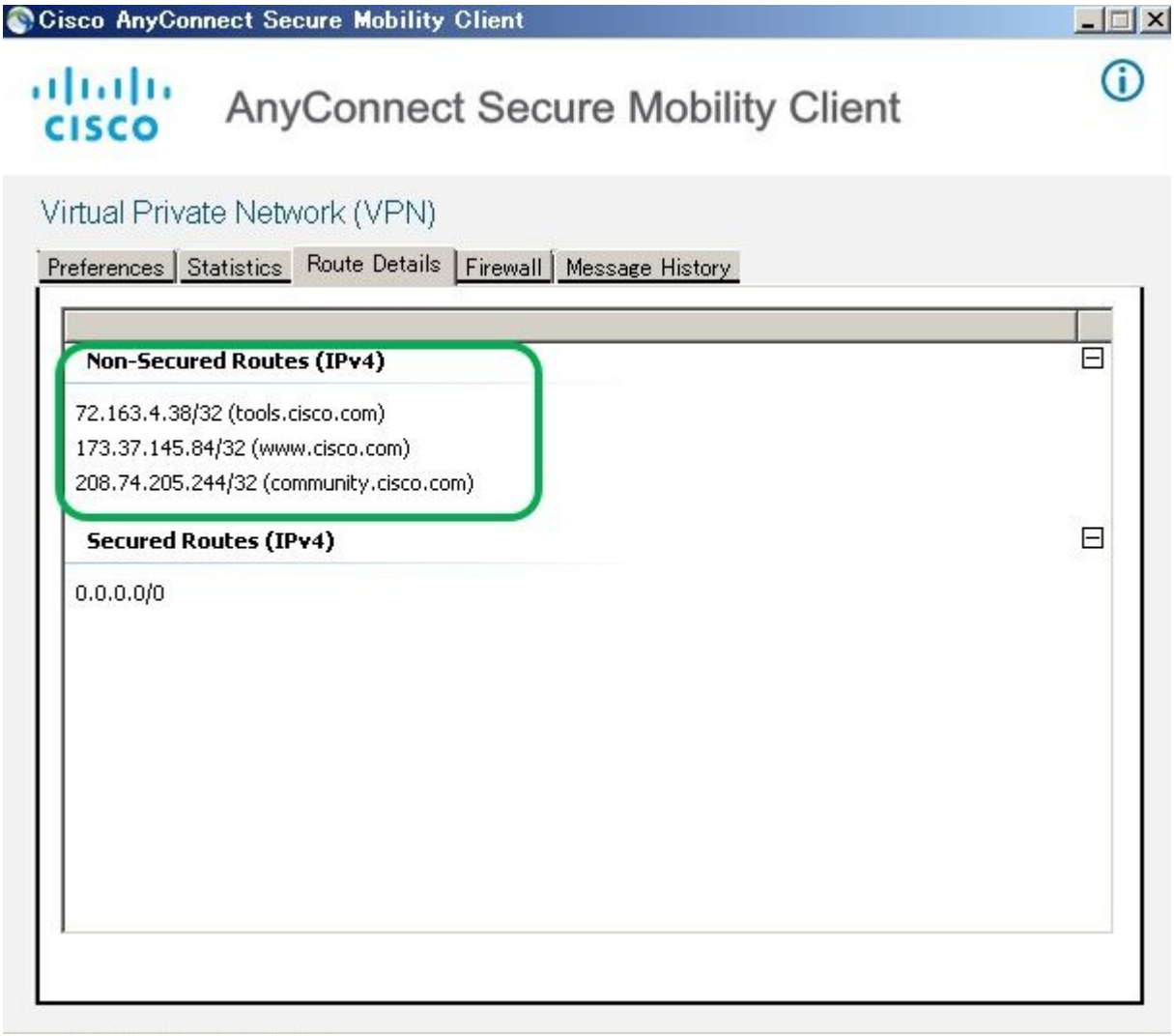
- Für die Verwendung der benutzerdefinierten Attribute von Dynamic Split Tunneling ist die ASA-Version 9.0 oder höher erforderlich.
- Platzhalter im Feld "Werte" wird nicht unterstützt.
- Dynamic Split Tunneling wird auf iOS-Geräten (Apple) nicht unterstützt (Erweiterungsanforderung: "Cisco bug ID CSCvr54798").

Überprüfung

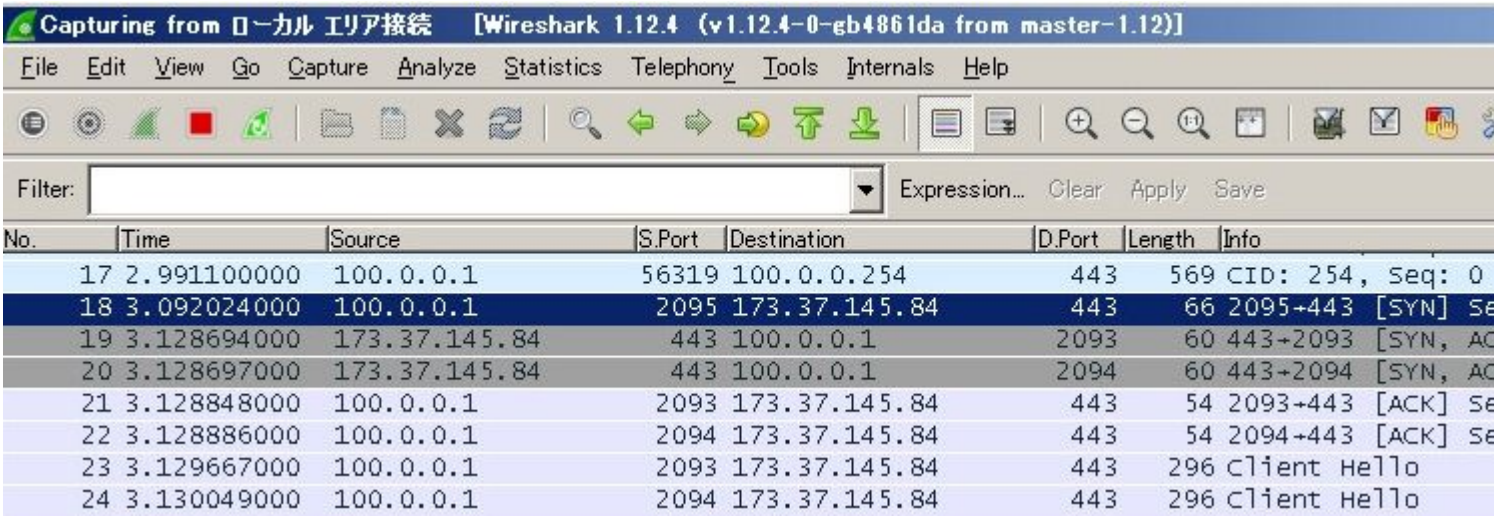
Zur Überprüfung der konfigurierten **Dynamic Tunnel Exclusions,** Starten **AnyConnect** Software auf dem Client, klicken Sie auf **Advanced Window** > **Statistics,** wie in der Abbildung dargestellt:



Sie können auch zu navigieren **Advanced Window** > **Route Details** Karteireiter, den Sie überprüfen können **Dynamic Tunnel Exclusions** sind aufgeführt unter **Non-Secured Routes,** wie im Bild dargestellt.



In diesem Beispiel haben Sie www.cisco.com konfiguriert unter **Dynamic Tunnel Exclusion list** und die Erfassung von Wireshark, die über die physische AnyConnect-Client-Schnittstelle erfolgt, bestätigt, dass der Datenverkehr zu www.cisco.com (198.51.100.0) nicht mit DTLS verschlüsselt wird.



Fehlerbehebung

Falls der Platzhalter im Feld "Werte" verwendet wird

Wenn ein Platzhalter im Feld "Values" (Werte) konfiguriert ist, z. B. "***.cisco.com**" in "Values" (Werte) konfiguriert ist, wird die AnyConnect-Sitzung getrennt, wie in den Protokollen gezeigt:

```
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> Firs
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> Clie
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv4
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (172
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> WebV
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session d
```

> **Hinweis**: Alternativ können Sie die Domäne **cisco.com** unter Values verwenden, um FQDNs wie www.cisco.com und tools.cisco.com zuzulassen.

Falls nicht sichere Routen nicht auf der Registerkarte "Routendetails" angezeigt werden

Der AnyConnect-Client erkennt automatisch die IP-Adresse und den FQDN auf der Registerkarte "Route Details" (Routendetails) und fügt sie hinzu, wenn der Client den Datenverkehr für die ausgeschlossenen Ziele initiiert.

Um sicherzustellen, dass die AnyConnect-Benutzer der richtigen AnyConnect-Gruppenrichtlinie zugewiesen sind, können Sie den Befehl '**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
```

Allgemeine Fehlerbehebung

Sie können das AnyConnect Diagnostics and Reporting Tool (DART) verwenden, um die Daten zu erfassen, die zur Behebung von AnyConnect-Installations- und Verbindungsproblemen nützlich sind. Der DART-Assistent wird auf dem Computer verwendet, auf dem AnyConnect ausgeführt wird. DART stellt die Protokolle, Status und Diagnoseinformationen für die Analyse durch das Cisco Technical Assistance Center (TAC) zusammen. Für die Ausführung von DART auf dem Client-Computer sind keine Administratorrechte erforderlich.

Zugehörige Informationen

- **Cisco AnyConnect Secure Mobility Client - Administratoranleitung, Version 4.7 - Informationen zu Dynamic Split Tunneling**
- **ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.13 - Configure Dynamic Split Tunneling**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.