ASA/AnyConnectダイナミックスプリットトンネリングの設定

内容

はじめに

このドキュメントでは、ASDMを介したダイナミックスプリット除外トンネリング用にAnyConnectセキュアモビリティクライアントを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASAに関する基本的な知識
- Cisco AnyConnectセキュリティモビリティクライアントに関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

AnyConnectスプリットトンネリングにより、Cisco AnyConnectセキュアモビリティクライアントは、IKEV2またはSecure Sockets Layer(SSL)を介して企業リソースに安全にアクセスできます。

AnyConnectバージョン4.5よりも前では、適応型セキュリティアプライアンス(ASA)で設定されたポリシーに基づいて、スプリットトンネルの動作をトンネル指定、トンネルすべて、または除外の指定とすることができました。

クラウドホスト型のコンピュータリソースが登場すると、ユーザの場所やクラウドホスト型リソースの負荷に基づいて、サービスが異なるIPアドレスに解決される場合があります。

AnyConnectセキュアモビリティクライアントは、IPV4またはIPV6のスタティックサブネット範囲、ホスト、またはプールへのスプリットトンネリングを提供するため、ネットワーク管理者がAnyConnectを設定する際にドメイン/FQDNを除外することが困難になります。

たとえば、ネットワーク管理者がスプリットトンネル設定からCisco.comドメインを除外したいが、Cisco.comのDNSマッピングはクラウドホストであるため変更される。

AnyConnectは、ダイナミックスプリット除外トンネリングを使用して、ホステッドアプリケーションのIPv4/IPv6アドレスを動的に解決し、トンネルの外部で接続が確立されるようにルーティングテーブルとフィルタに必要な変更を加えます。

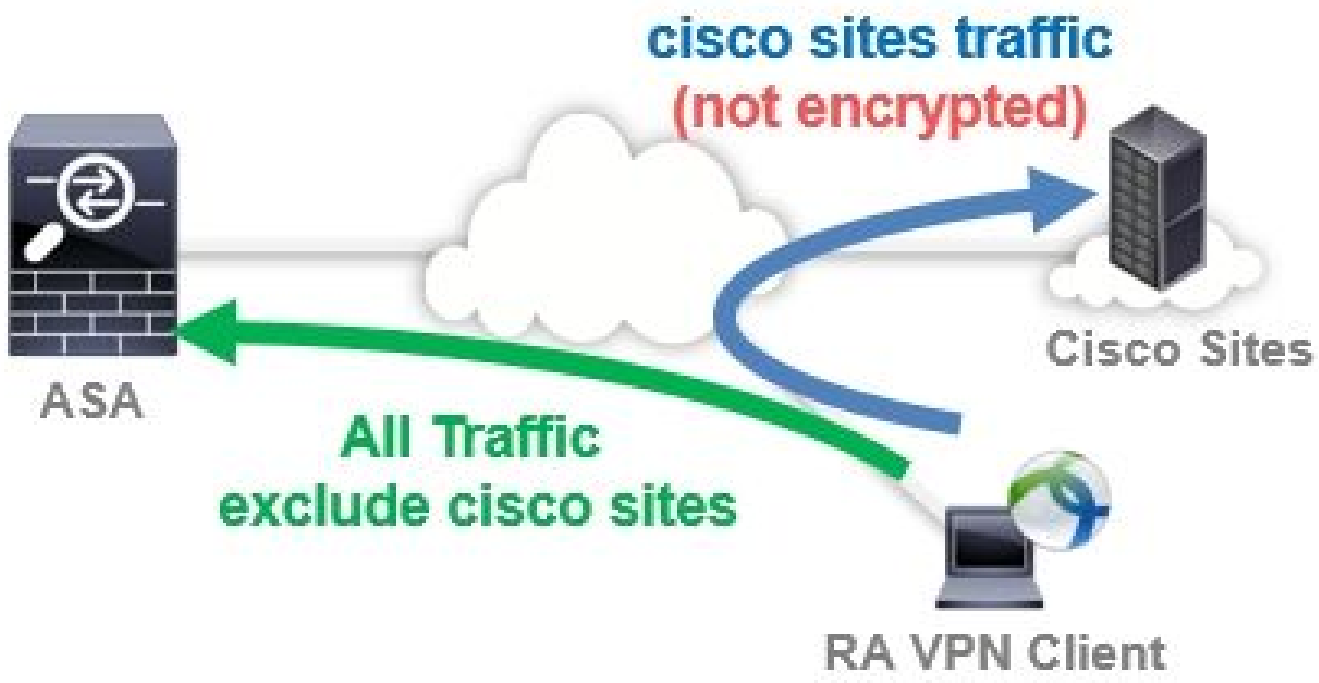
AnyConnect 4.5以降では、ダイナミックスプリットトンネリングを使用できます。この場合、AnyConnectはホステッドアプリケーションのIPv4/IPv6アドレスを動的に解決し、ルーティングテーブルとフィルタに必要な変更を加えて、トンネルの外部で接続を確立できます

コンフィギュレーション

ここでは、ASA で Cisco AnyConnect セキュア モビリティ クライアントを設定する方法について説明します。

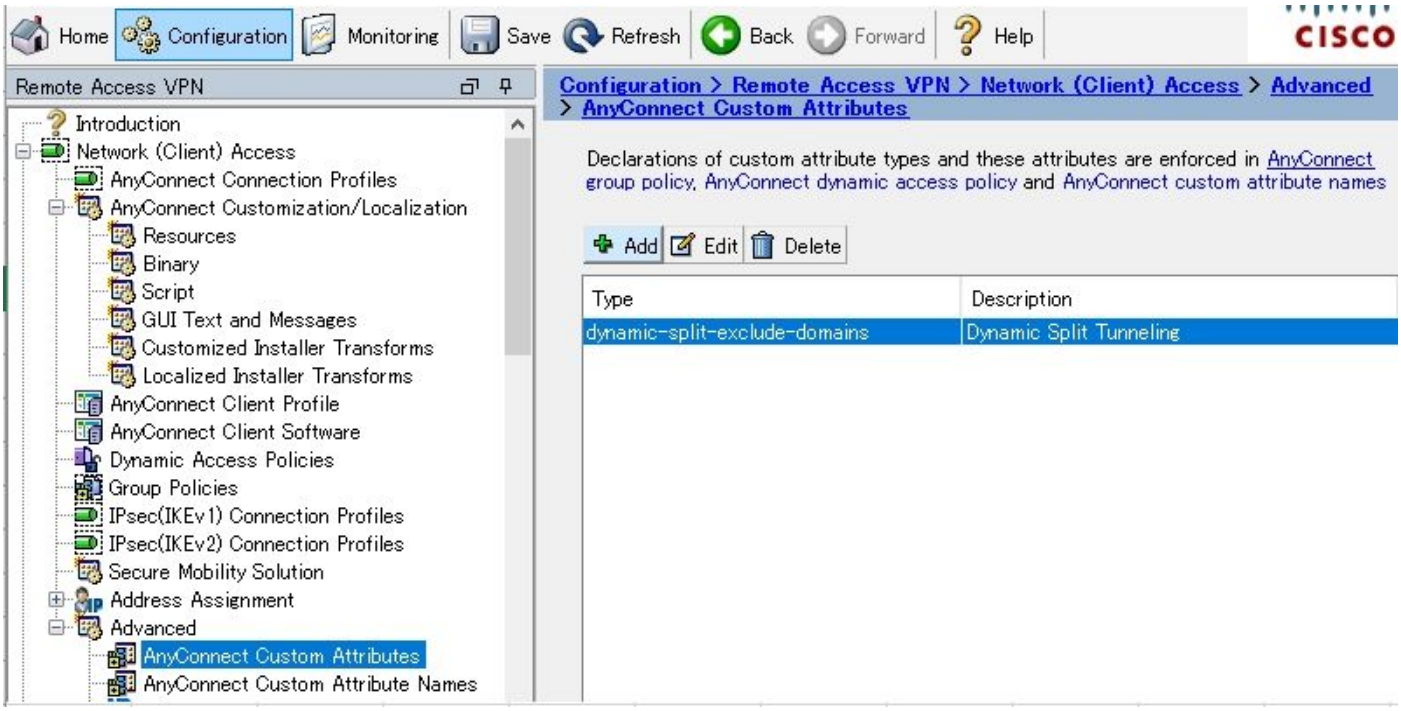
ネットワーク図

次の図に、このドキュメントの例で使用するトポロジを示します。



ステップ 1：AnyConnectカスタム属性の作成

移動先 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes**を参照。クリック **Add** ボタン、および設定 **dynamic-split-exclude-domains** 属性とオプションの説明を次の図に示します。

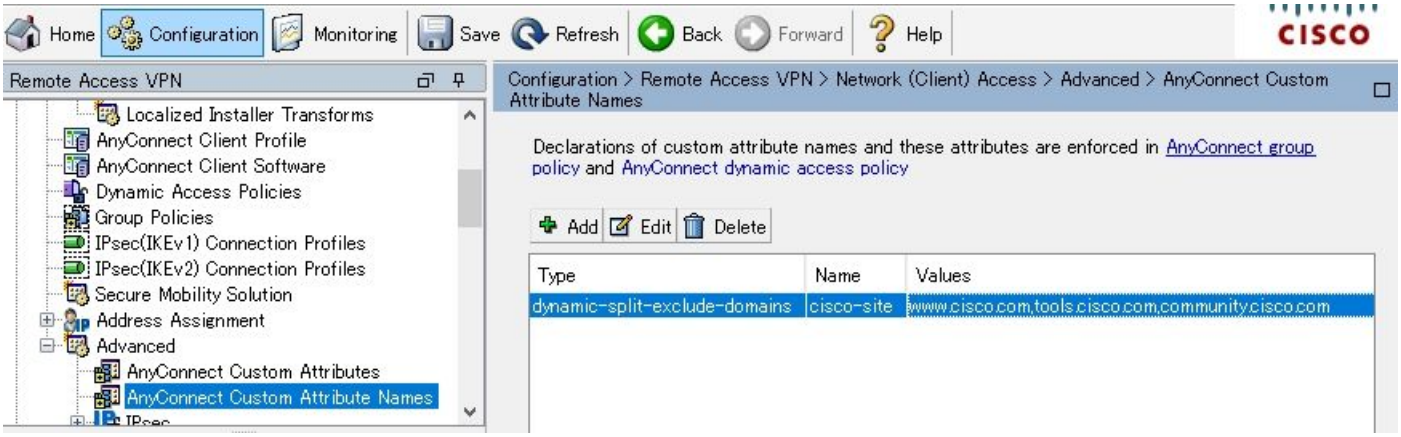


ステップ 2：AnyConnectのカスタム名の作成と値の設定

移動先 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names**を参

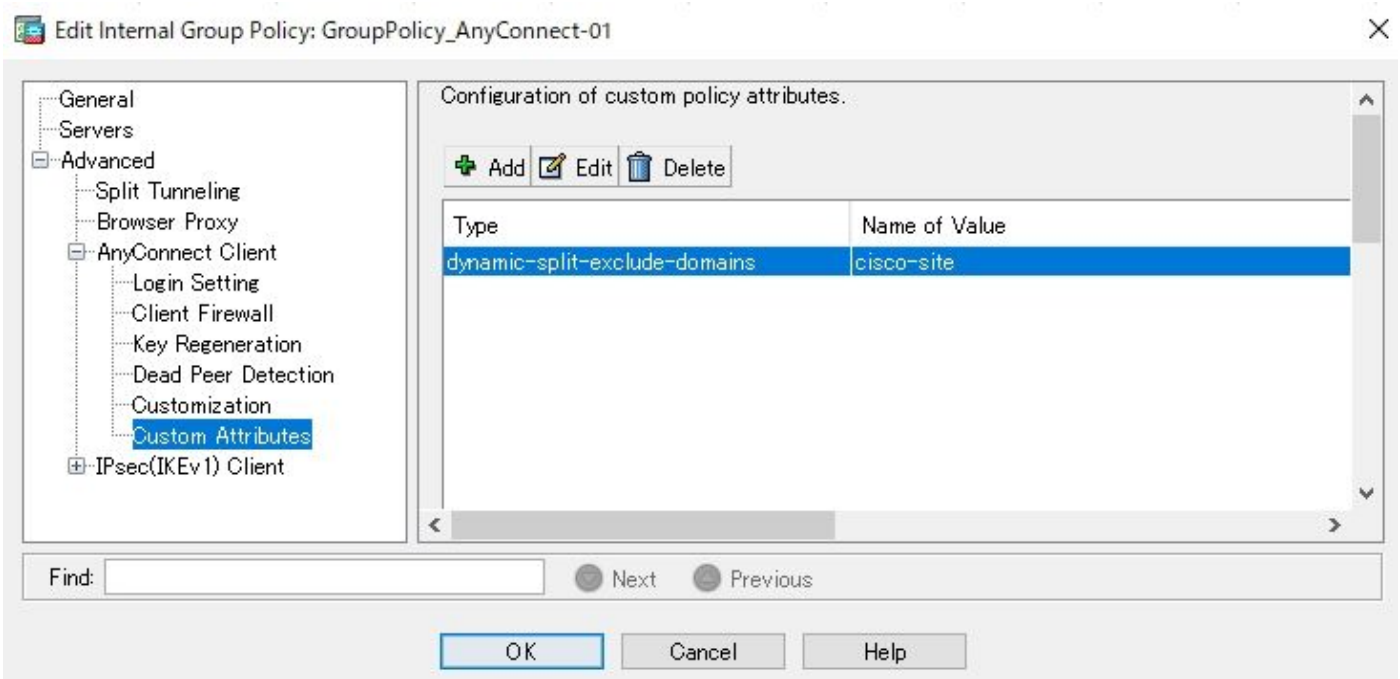
照。クリック **Add** ボタンをクリックし、 **dynamic-split-exclude-domains** 属性は以前にTypeから作成されました。これは任意の名前と値です（図を参照）。

[名前]にスペースを入力しないように注意してください。（例：Possible cisco-site, Inpossible cisco site）。値に複数のドメインまたはFQDNが登録されている場合は、カンマ(,)で区切ります。



ステップ 3：グループポリシーにタイプと名前を追加する

移動先 **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** グループポリシーを選択します。その後、 **Advanced> AnyConnect Client> Custom Attributes** 設定した設定を **Type** と **Name**を参照してください（図を参照）。



CLIの設定例

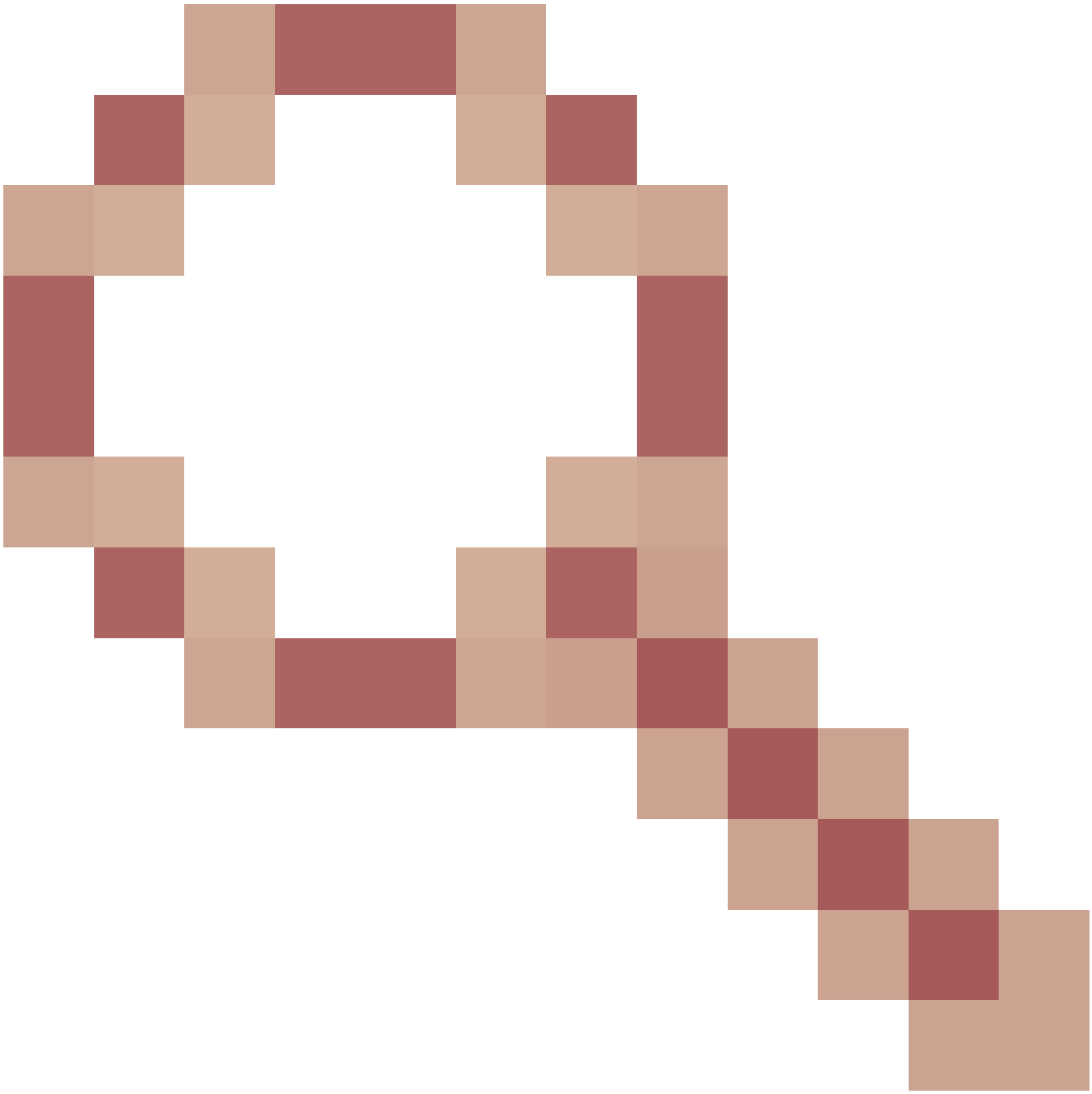
ここでは、参考のために、ダイナミックスプリットトンネリングのCLI設定について説明します。

<#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
```

制限事項

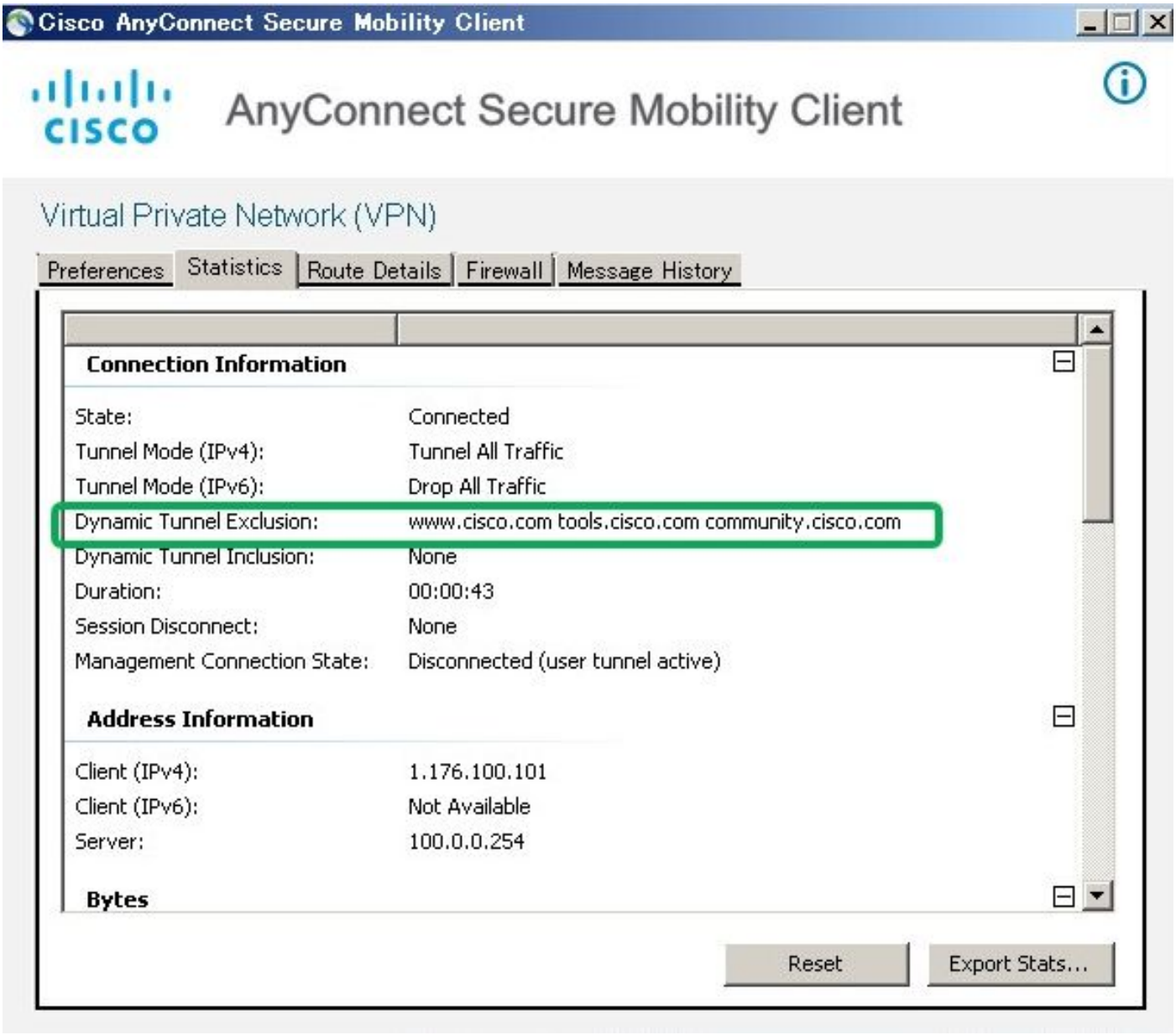
- ダイナミックスプリットトンネリングのカスタム属性を使用するには、ASAバージョン9.0以降が必要です。
- 値フィールドのワイルドカードはサポートされていません。
- ダイナミックスプリットトンネリングは、iOS(Apple)デバイスではサポートされていません(機能拡張要求：Cisco Bug ID CSCvr54798



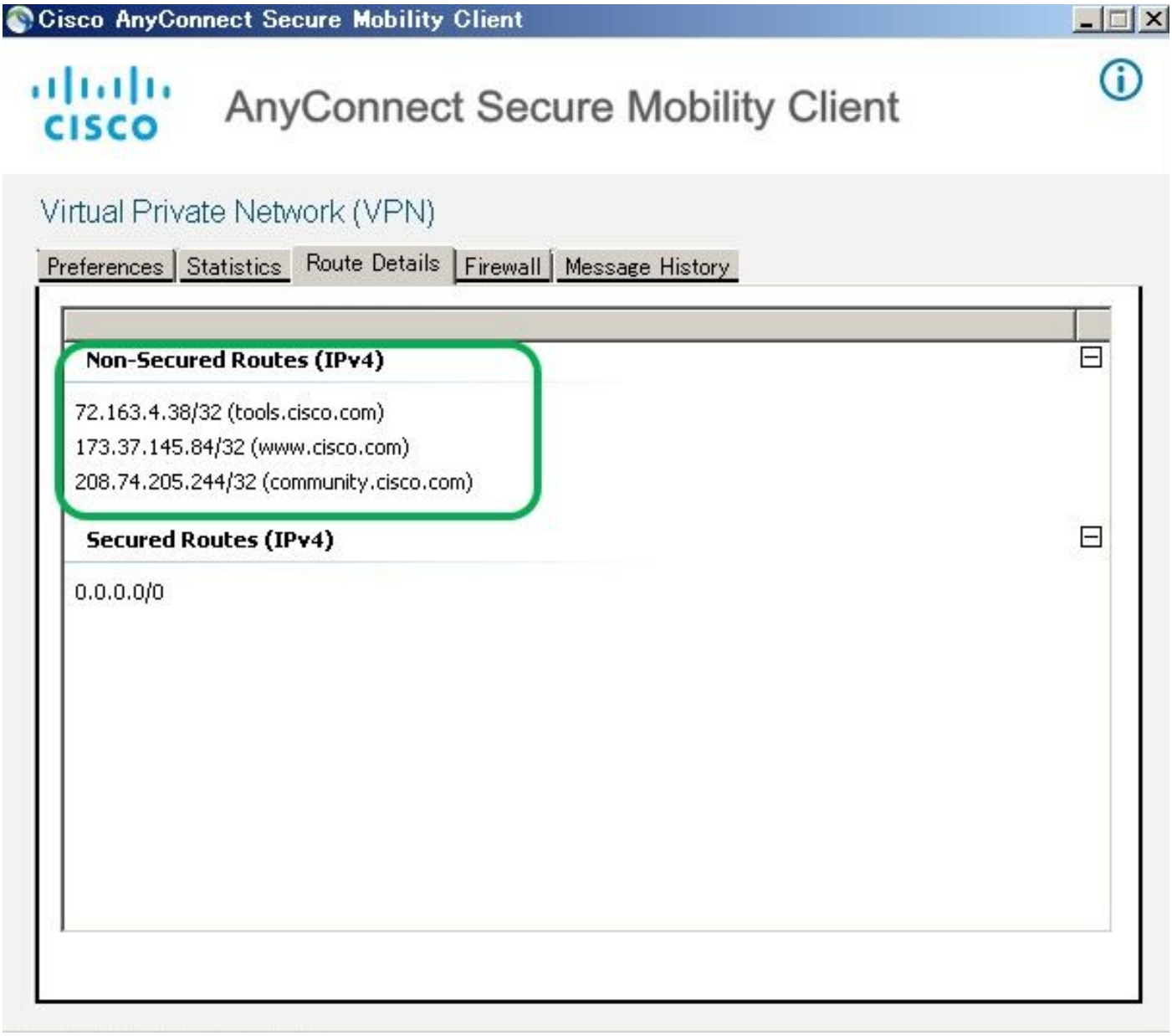
）。

確認

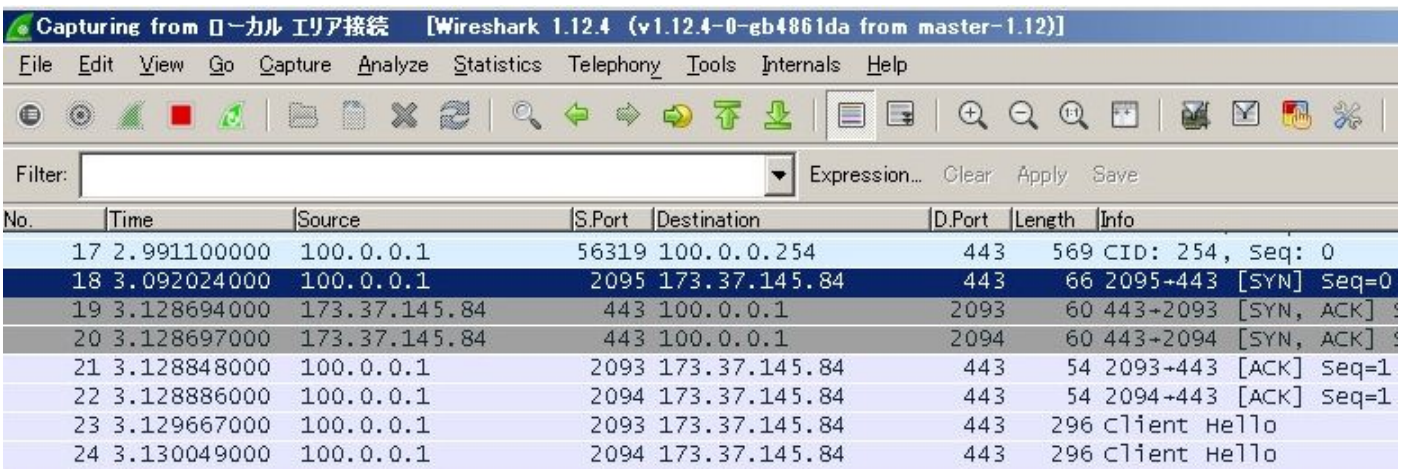
設定を確認するには、 **Dynamic Tunnel Exclusions**, 開始AnyConnectSoftwareをクリックし、 **Advanced Window > Statistics**を参照してください（図を参照）。



また、次の場所に移動することもできます **Advanced Window** > **Route Details** タブをクリックして確認します。**Dynamic Tunnel Exclusions**は、 **Non-Secured Routes**, を参照してください。



この例では、www.cisco.comを**Dynamic Tunnel Exclusion list**AnyConnectクライアントの物理インターフェイスで収集されたWiresharkキャプチャから、www.cisco.com(198.51.100.0)へのトラフィックがDTLSで暗号化されていないことが確認できます。



トラブルシュート

ワイルドカードが値フィールドで使用される場合

ワイルドカードがValuesフィールドで設定されている場合、たとえば、*.cisco.comがValuesフィールドで設定されている場合、AnyConnectセッションはログに示されているように接続解除されます。

```
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
```

注：別の方法として、値でcisco.comドメインを使用して、www.cisco.comやtools.cisco.comなどのFQDNを許可することもできます。

非セキュアルートがRoute Detailsタブに表示されない場合

AnyConnectクライアントは、除外された宛先へのトラフィックを開始すると、自動的に学習し、Route DetailsタブにIPアドレスとFQDNを追加します。

AnyConnectユーザが正しいAnyconnectグループポリシーに割り当てられていることを確認するには、次のコマンドを実行します **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
```

一般的なトラブルシューティング

AnyConnect Diagnostics and Reporting Tool(DART)を使用して、AnyConnectのインストールおよび接続の問題のトラブルシューティングに役立つデータを収集できます。 DART ウィザードは、AnyConnect が稼働するコンピュータで使用します。DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。クライアントマシンで実行するために管理者権限は不要です。

関連情報

- Cisco AnyConnectセキュアモビリティクライアント管理者ガイド、リリース4.7：ダイナミックスプリットトンネリングについて
- ASDMブック3:Cisco ASAシリーズVPN ASDMコンフィギュレーションガイド7.13：ダイナミックスプリットトンネリングの設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。