

# Easy VPN-Client und -Server auf derselben Schnittstelle

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Änderungen des Cisco IOS-Verhaltens](#)

[Lösung](#)

## Einführung

Dieses Dokument beschreibt ein Problem, das auftritt, wenn der Cisco Easy VPN-Client und der Cisco Easy VPN-Server auf derselben Schnittstelle verwendet werden, auf der Cisco IOS<sup>®</sup> Version 15.2(1)T oder höher ausgeführt wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Easy VPN-Konfigurationen verfügen.

**Tipp:** Konfigurationsdetails finden Sie im [Easy VPN-Konfigurationshandbuch, Cisco IOS Release 15M&T](#).

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS-Versionen 15.2(1)T und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Die Cisco IOS-Versionen 15.2(1)T und frühere Versionen unterstützen diese Funktionen, die in späteren Versionen nicht mehr unterstützt werden:

- **Easy VPN Remote and Server on the same Interface** - Diese Funktion ermöglicht die

Unterstützung des Easy VPN Remote- und Easy VPN-Servers auf derselben Schnittstelle, sodass sowohl ein Tunnel zu einem anderen Easy VPN-Server eingerichtet als auch der Easy VPN-Client auf derselben Schnittstelle gleichzeitig beendet werden kann. Eine typische Anwendung ist ein geografisch verteilter Standort, für den Easy VPN Remote zur Verbindung mit einem Easy VPN-Software-Server des Unternehmens und zur Terminierung der Benutzer der lokalen Software-Clients verwendet wird.

- **Easy VPN Remote und Site-to-Site auf derselben Schnittstelle** - Diese Funktion ermöglicht die Unterstützung von Easy VPN Remote und Site-to-Site (Crypto Map) auf derselben Schnittstelle. So kann sowohl ein Tunnel zu einem anderen Easy VPN-Server eingerichtet werden als auch ein weiterer Site-to-Site-Zugriff auf derselben Schnittstelle gleichzeitig eingerichtet werden. Eine typische Anwendung besteht aus einem VPN-Service-Provider eines Drittanbieters, der einen Remote-Router über den Site-to-Site-Tunnel verwaltet und den Easy VPN Remote verwendet, um den Remote-Standort mit einem Easy VPN-Server des Unternehmens zu verbinden.

**Tip:** Weitere Informationen finden Sie im Abschnitt [Easy VPN Remote and Server](#) im **Easy VPN Configuration Guide, Cisco IOS Release 15M&T**.

## Problem

Wenn Sie eine Crypto Map auf eine Schnittstelle anwenden, die bereits für IOS Easy VPN konfiguriert ist, wird der Befehl `crypto map` nicht auf diese Schnittstelle angewendet.

## Änderungen des Cisco IOS-Verhaltens

In Cisco IOS-Versionen 15.2(1)T und höher ist dies keine unterstützte Konfiguration, da für jede Schnittstelle keine mehrere Security Association Databases (SADB) hinzugefügt werden.

**Hinweis:** Dieses Problem wird in der Cisco Bug-ID [CSCtx47112](#) nachverfolgt - *Crypto Map kann nicht auf dieselbe Schnittstelle angewendet werden, die für ezvpn konfiguriert wurde.*

## Lösung

Um dieses Problem zu beheben, trennen Sie die Konfigurationen für die Crypto Map vom Legacy-Easy VPN, und verschieben Sie eine dieser Konfigurationen in eine VTI-basierte (Virtual Tunnel Interface-basierte) Konfiguration:

- Ändern Sie die Site-to-Site-Crypto-Map in Generic Routing Encapsulation (GRE)/IPSec mit Tunnelschutz oder Secure VTI (SVTI).
- Ändern Sie Easy VPN in FlexVPN.