

L2TP Over IPsec zwischen Windows 8 PC und ASA mithilfe eines vorinstallierten Schlüssels konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Einschränkungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Vollständige Tunnel-Konfiguration](#)

[ASA-Konfiguration mit Adaptive Security Device Manager \(ASDM\)](#)

[ASA-Konfiguration über CLI](#)

[Windows 8 - Client-Konfiguration für L2TP/IPsec](#)

[Split-Tunnel-Konfiguration](#)

[Konfiguration auf ASA](#)

[Konfiguration auf L2TP/IPsec-Client](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie das Layer 2 Tunneling Protocol (L2TP) über IPsec mithilfe eines vorinstallierten Schlüssels zwischen der Cisco Adaptive Security Appliance (ASA) und dem nativen Windows 8-Client konfiguriert wird.

L2TP over Internet Protocol Security (IPsec) ermöglicht die Bereitstellung und Verwaltung einer L2TP Virtual Private Network (VPN)-Lösung zusammen mit dem IPsec-VPN und den Firewall-Services in einer einzigen Plattform.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- IP-Verbindungen vom Client-Computer zur ASA Versuchen Sie, die Verbindung zu testen,

indem Sie die IP-Adresse der ASA vom Client-Endgerät und umgekehrt pingen.

- Stellen Sie sicher, dass das UDP-Port 500 und 4500 sowie das ESP-Protokoll (Encapsulating Security Payload) an keiner Stelle entlang des Verbindungspfad blockiert wird.

Einschränkungen

- L2TP über IPsec unterstützt nur IKEv1. IKEv2 wird nicht unterstützt.
- L2TP mit IPsec auf der ASA ermöglicht die Zusammenarbeit des LNS mit nativen VPN-Clients, die in Betriebssystemen wie Windows, MAC OS X, Android und Cisco IOS integriert sind. Nur L2TP mit IPsec wird unterstützt, natives L2TP selbst wird auf ASA nicht unterstützt.
- Die vom Windows-Client unterstützte Mindestlebensdauer der IPsec-Sicherheitszuordnung beträgt 300 Sekunden. Wenn die Lebensdauer auf der ASA auf weniger als 300 Sekunden festgelegt ist, wird sie vom Windows-Client ignoriert und durch eine Lebensdauer von 300 Sekunden ersetzt.
- Die ASA unterstützt nur das Point-to-Point Protocol (PPP) Authentication Password Authentication Protocol (PAP) und das Microsoft Challenge-Handshake Authentication Protocol (CHAP), Versionen 1 und 2, in der lokalen Datenbank. Extensible Authentication Protocol (EAP) und CHAP werden von Proxy-Authentifizierungsservern durchgeführt. Wenn ein Remote-Benutzer zu einer Tunnelgruppe gehört, die mit den Befehlen **Authentication eap-Proxy** oder **Authentication Chap** konfiguriert ist und die ASA für die Verwendung der lokalen Datenbank konfiguriert ist, kann dieser Benutzer keine Verbindung herstellen.

Unterstützte PPP-Authentifizierungstypen

L2TP über IPsec-Verbindungen auf der ASA unterstützen nur die in Tabelle aufgeführten PPP-Authentifizierungstypen

<i>AAA-Serverunterstützung und PPP-Authentifizierungstypen</i>	
AAA-Servertyp	Unterstützte PPP-Authentifizierungstypen
LOKAL	PAP, MSCHAPv1, MSCHAPv2
RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TACACS+	PAP, CHAP, MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

Merkmale des PPP-Authentifizierungstyps

Schlüsselwort	Authentifizierungstyp	Merkmale
Klotz	CHAP	Als Antwort auf die Server-Herausforderung gibt der Client verschlüsselten [Herausforderung plus Kennwort] mit einem eindeutigen Text-Benutzernamen zurück. Dieses Protokoll ist sicherer als der PAP, verschlüsselt jedoch keine Daten.
eap-proxy	EAP	Aktiviert EAP, das der Sicherheits-Appliance die Proxy-Funktion für den PPP-Authentifizierungsprozess auf einem externen RADIUS-Authentifizierungsserver zuweist.
ms-chap-v1	Microsoft CHAP, Version 1	Ähnlich wie CHAP, aber sicherer, da der Server nur verschlüsselte Passwörter speichert und vergleicht, anstatt Klartext-Passwörter.
ms-chap-v2	Microsoft CHAP, Version 2	CHAP. Dieses Protokoll generiert auch einen Schlüssel für die Datenverschlüsselung durch MPPE.
Pay	PAP	Übergibt während der Authentifizierung Klartext-Benutzername und

Kennwort und ist nicht sicher.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA der Serie 5515, auf der die Softwareversion 9.4(1) ausgeführt wird
- L2TP/IPSec-Client (Windows 8)

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.

Zugehörige Produkte

Diese Konfiguration kann auch mit Cisco Security Appliance der Serie ASA 5500 8.3(1) oder höher verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions \(Technische Tipps zu Konventionen von Cisco\)](#).

Hintergrundinformationen

Layer 2 Tunneling Protocol (L2TP) ist ein VPN-Tunneling-Protokoll, das es Remote-Clients ermöglicht, das öffentliche IP-Netzwerk für die sichere Kommunikation mit privaten Unternehmensnetzwerkservern zu verwenden. L2TP verwendet PPP over UDP (Port 1701), um die Daten zu tunneln.

Das L2TP-Protokoll basiert auf dem Client/Server-Modell. Die Funktion ist unterteilt in den L2TP-Netzwerkserver (LNS) und den L2TP-Zugriffs-Konzentrator (LAC). Das LNS wird in der Regel auf einem Netzwerk-Gateway wie in diesem Fall der ASA ausgeführt, während die LAC ein DFÜ-Netzwerkzugriffsserver (NAS) oder ein Endgerät mit einem gebündelten L2TP-Client wie Microsoft Windows, Apple iPhone oder Android sein kann.

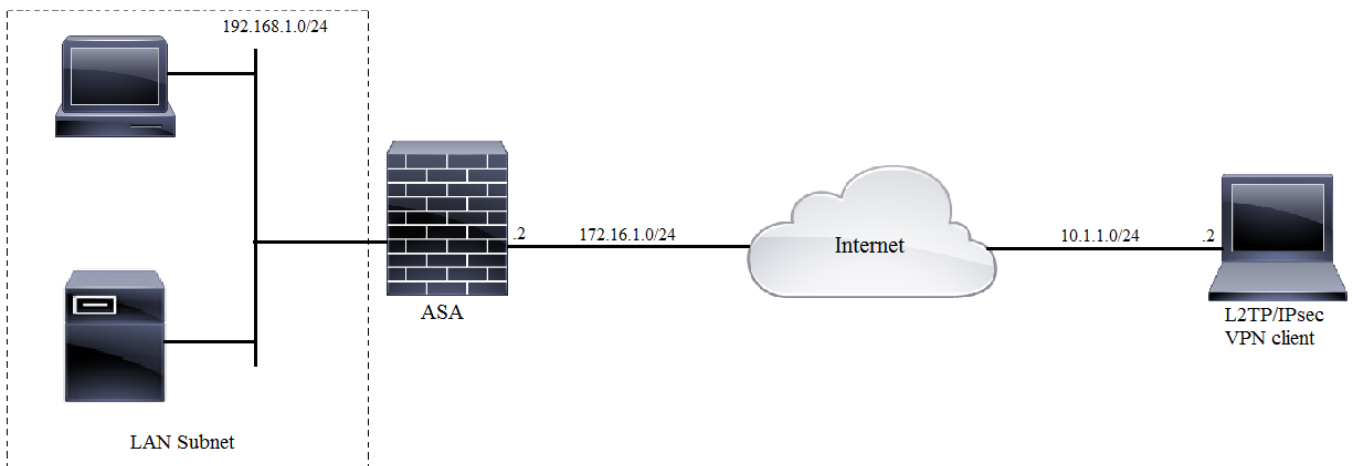
Konfigurieren

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Netzwerkdiagramm

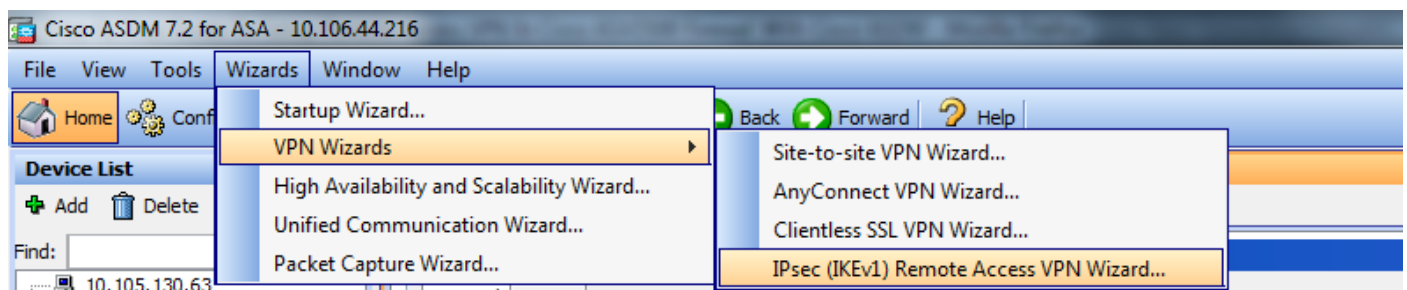


Vollständige Tunnel-Konfiguration

ASA-Konfiguration mit Adaptive Security Device Manager (ASDM)

Gehen Sie wie folgt vor:

Schritt 1: Melden Sie sich beim ASDM an, und navigieren Sie zu **Wizards > VPN Wizards > Ipsec (IKEv1) Remote Access VPN Wizard**.




Schritt 2: Ein Setup-Fenster für Remote Access VPN wird angezeigt. Wählen Sie aus der Dropdown-Liste die Schnittstelle aus, auf der der VPN-Tunnel terminiert werden soll. In diesem Beispiel ist eine externe Schnittstelle mit dem WAN verbunden, sodass VPN-Tunnel an dieser Schnittstelle terminiert werden. Behalten Sie das Kontrollkästchen **Eingehende IPsec-Sitzungen aktivieren, um Schnittstellenzugriffslisten zu umgehen. Gruppenrichtlinien und Zugriffsberechtigungslisten pro Benutzer gelten weiterhin für den überprüften Datenverkehr**, sodass die neue Zugriffsliste nicht auf der externen Schnittstelle konfiguriert werden muss, damit die Clients auf interne Ressourcen zugreifen können. Klicken Sie auf **Weiter**.

VPN Wizard

VPN Wizard

IPsec IKEv1 Remote Access Wizard (Step 1 of ...)

Use this wizard to configure new new IPsec (IKEV1) remote access VPN tunnels. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.

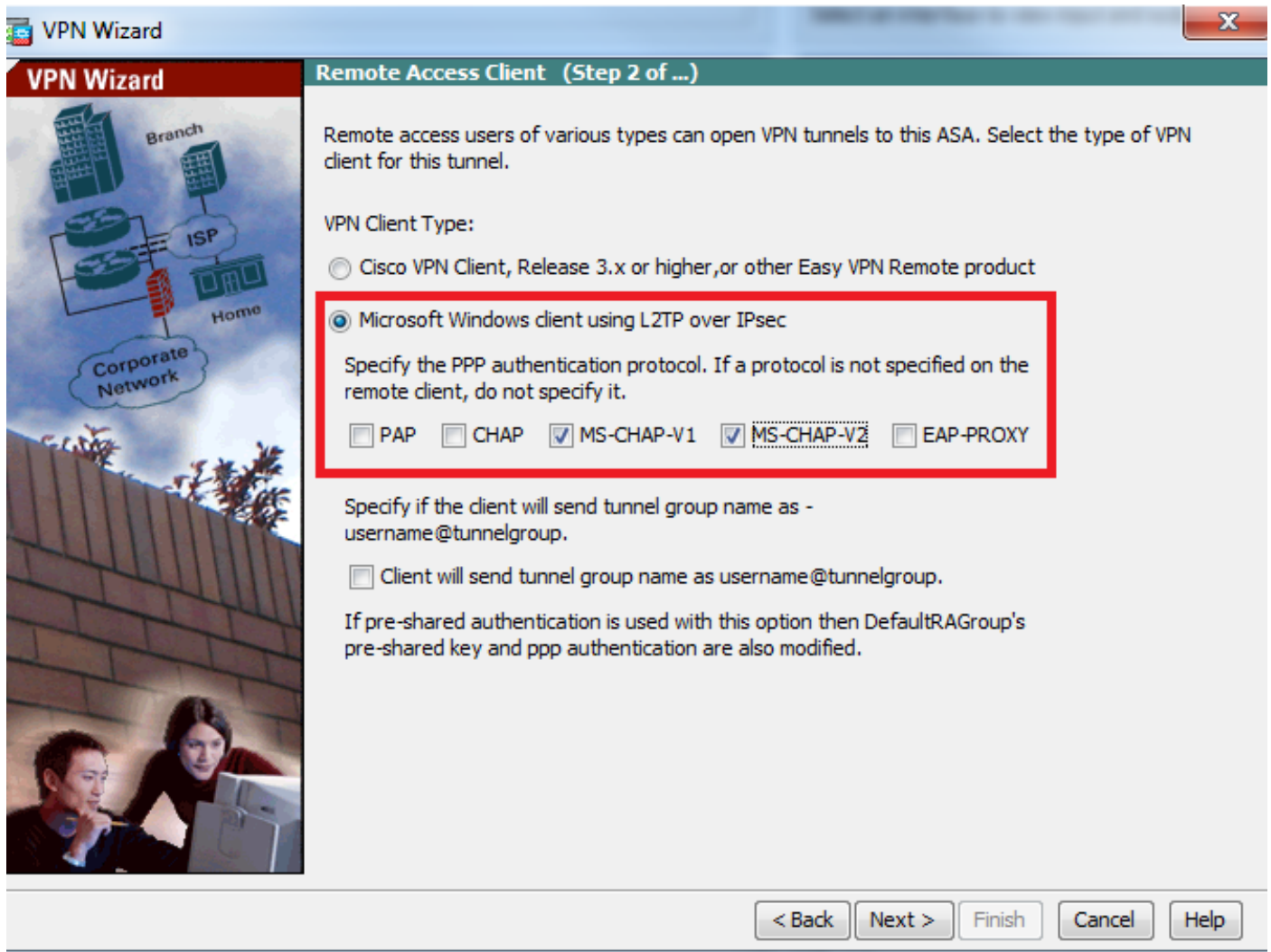


VPN Tunnel Interface:

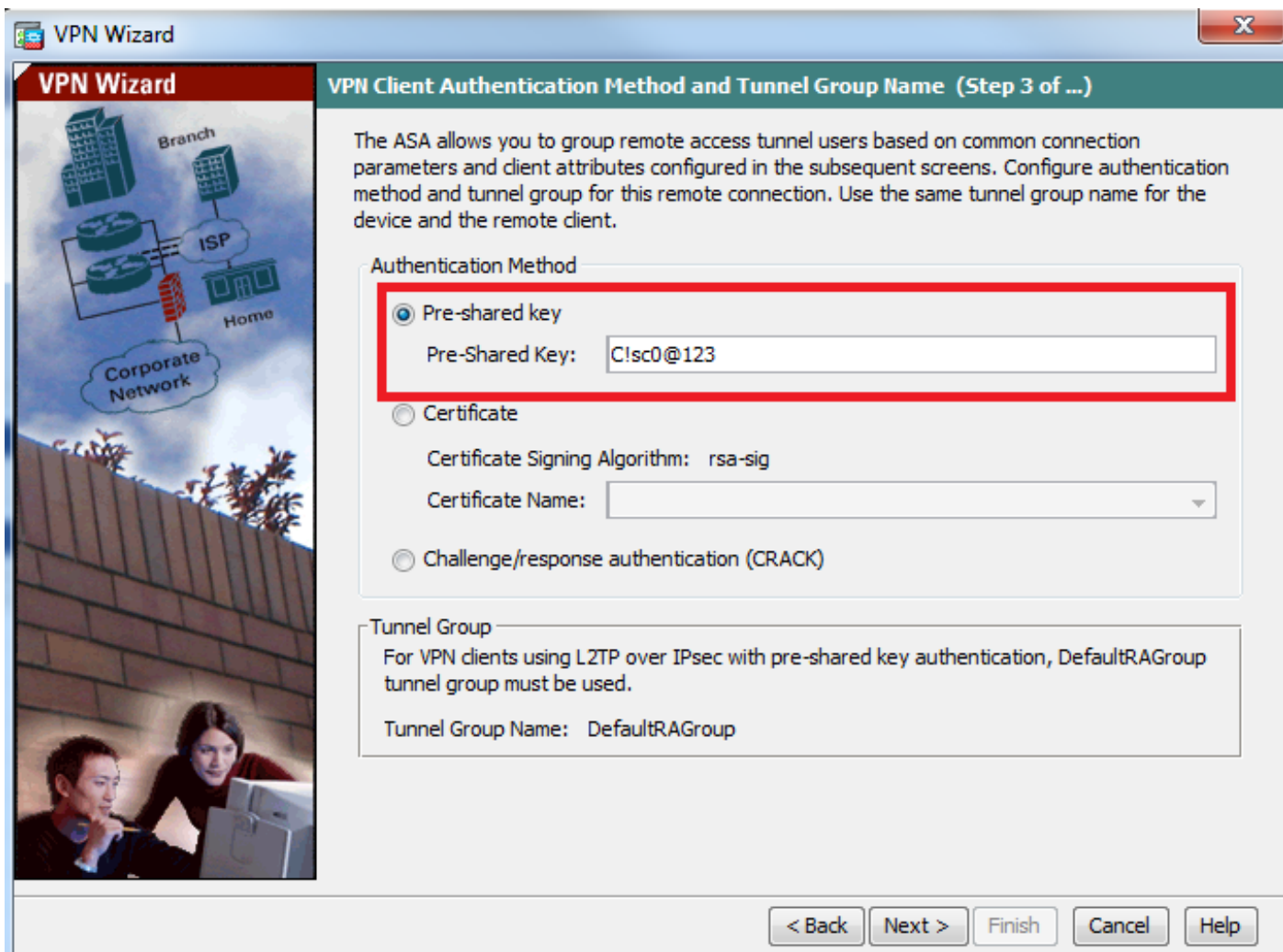
Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

< Back Next > Finish Cancel Help

Schritt 3: Wählen Sie, wie in diesem Bild gezeigt, den Client-Typ als **Microsoft Windows-Client** aus, der **L2TP über IPsec** und **MS-CHAP-V1** und **MS-CHAP-V2** als PPP-Authentifizierungsprotokoll **verwendet**, da PAP nicht sicher ist und andere Authentifizierungstypen nicht von LOCAL als Authentifizierungsserver und Klicken auf unterstützt werden.

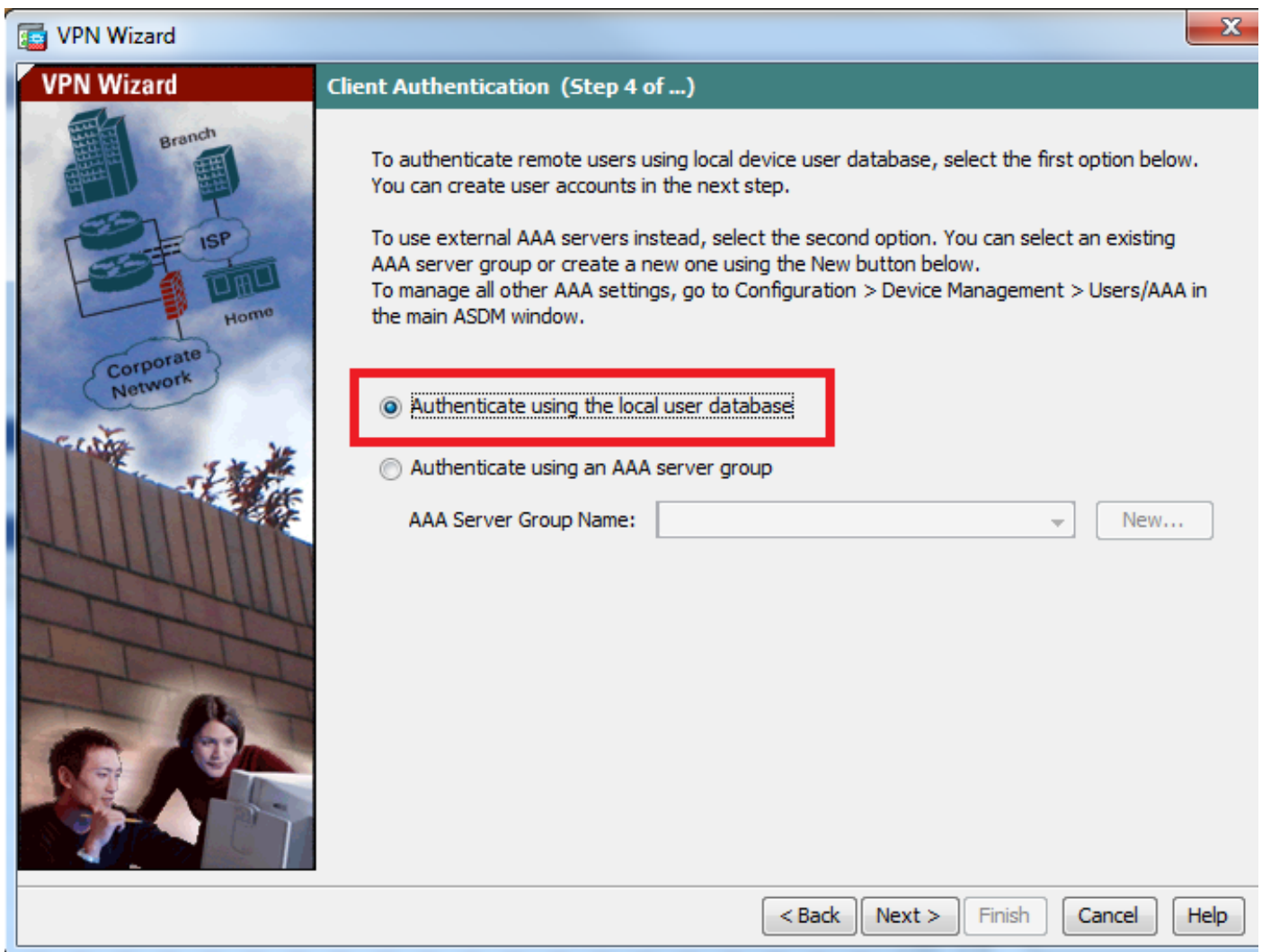


Schritt 4: Wählen Sie die Authentifizierungsmethode als **Pre-shared-key aus**, geben Sie den Pre-shared-Key ein, der auch auf der Client-Seite gleich sein muss, und klicken Sie auf **Next**, wie in diesem Bild gezeigt.

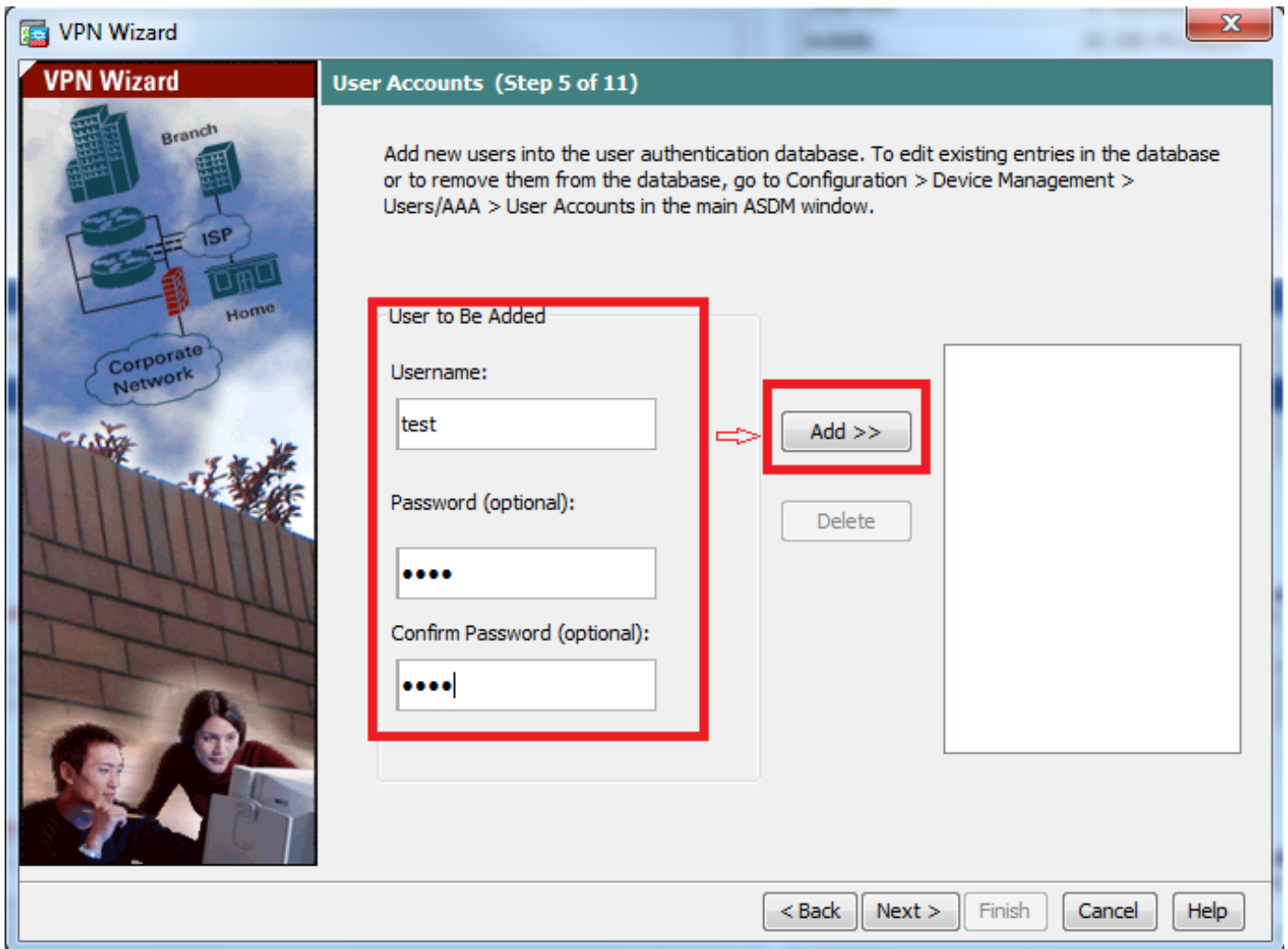


Schritt 5: Geben Sie eine Methode zum Authentifizieren von Benutzern an, die L2TP über IPsec-Verbindungen versuchen. Es können entweder ein externer AAA-Authentifizierungsserver oder eine eigene lokale Datenbank verwendet werden. Wählen Sie **Authentifizierung mithilfe der lokalen Benutzerdatenbank aus**, wenn Sie die Clients anhand der lokalen Datenbank von ASA authentifizieren möchten, und klicken Sie auf **Weiter**.

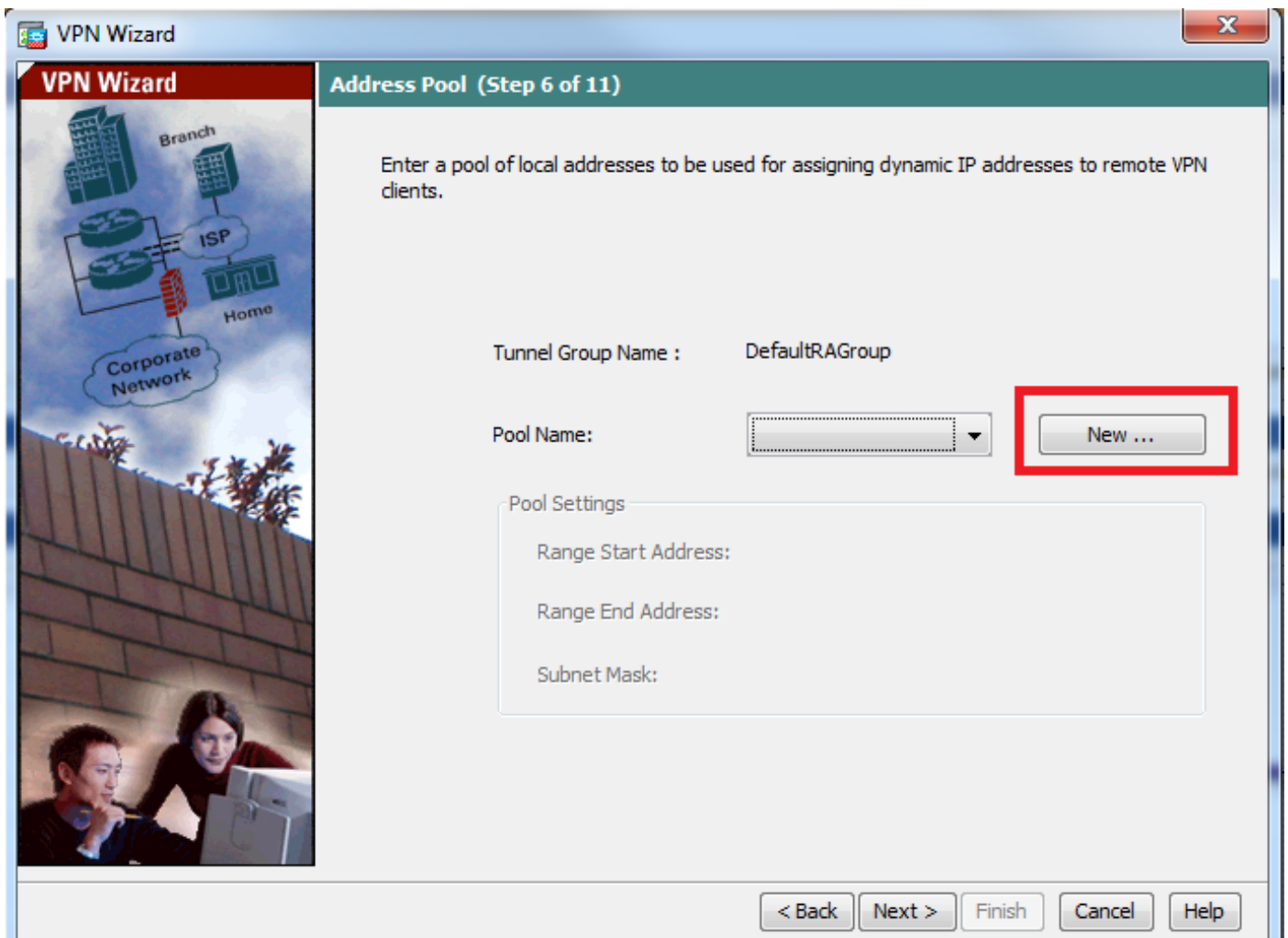
Hinweis: Weitere Informationen finden Sie unter [Konfigurieren der RADIUS-Authentifizierung für VPN-Benutzer](#), um die Benutzer mithilfe des externen AAA-Servers zu authentifizieren.



Schritt 6: Um der lokalen Datenbank neue Benutzer zur Benutzerauthentifizierung hinzuzufügen, geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie dann auf **ADD (Hinzufügen)**, oder es können vorhandene Benutzerkonten in der Datenbank verwendet werden, wie in diesem Bild gezeigt. Klicken Sie auf **Weiter**.

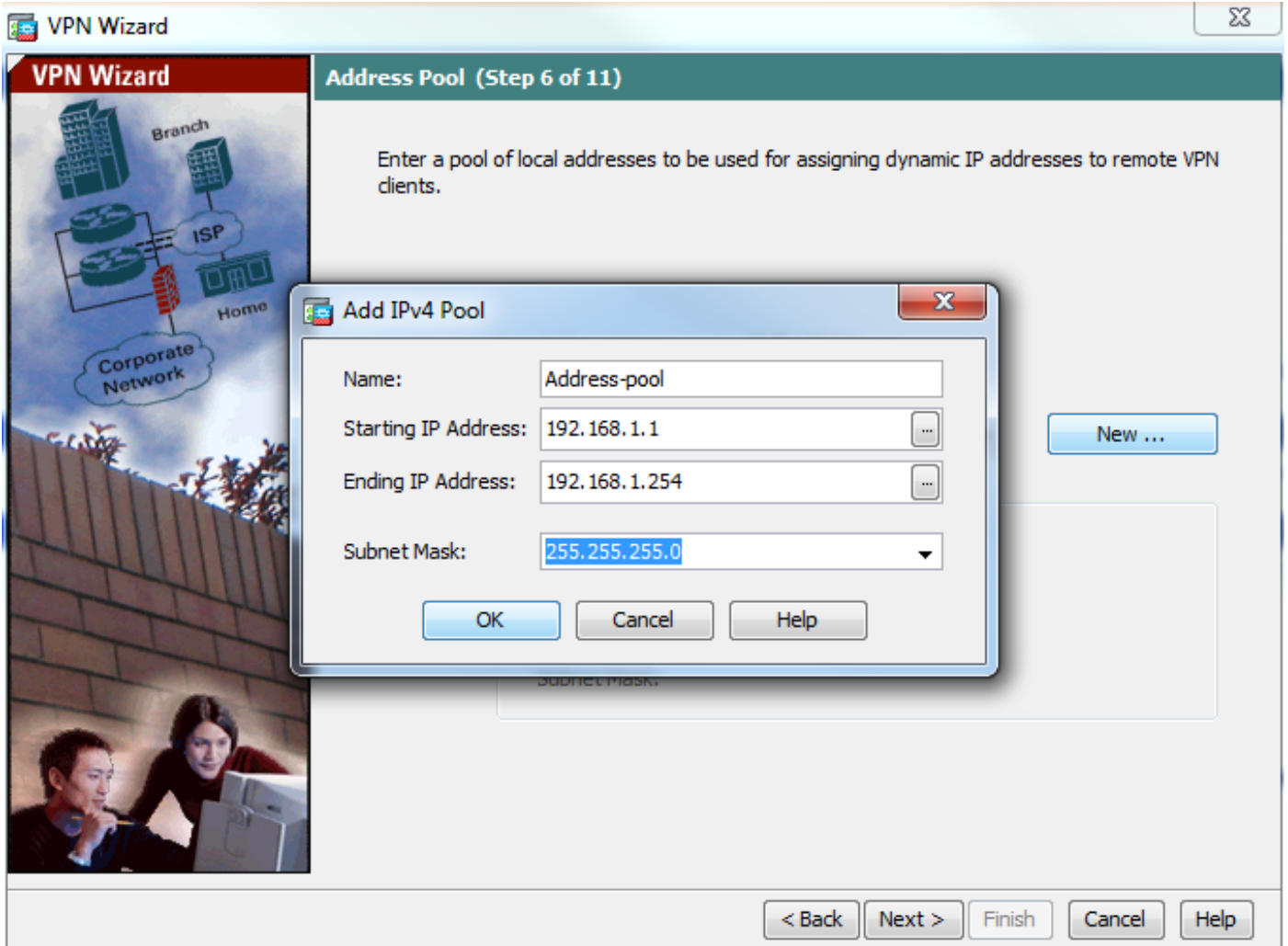


Schritt 7: Wählen Sie aus der Dropdown-Liste den Adresspool aus, der für die Zuweisung von IP-Adressen an die Clients verwendet werden soll. Um einen neuen Adresspool zu erstellen, klicken Sie auf **Neu**, wie in diesem Bild gezeigt.

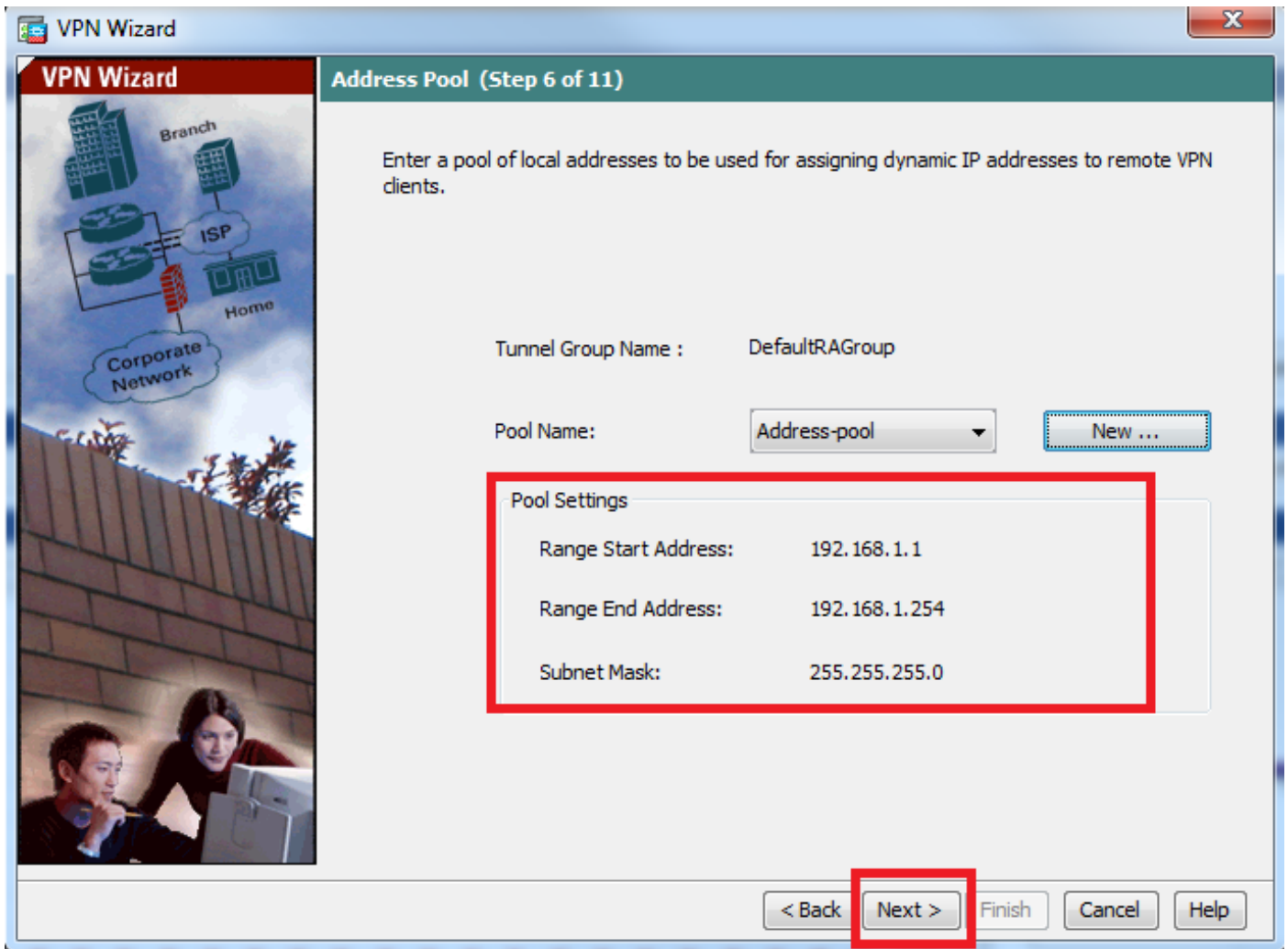


Schritt 8: Das Dialogfeld **IPv4-Pool hinzufügen** wird angezeigt.

1. Geben Sie den Namen des neuen IP-Adresspools ein.
2. Geben Sie die Start- und End-IP-Adressen ein.
3. Geben Sie die Subnetzmaske ein, und klicken Sie auf **OK**.



Schritt 9: Überprüfen Sie die Pool-Einstellungen, und klicken Sie auf **Weiter**.



Schritt 10: Konfigurieren Sie die Attribute, die an die Clients gesendet werden sollen, oder lassen Sie sie leer, und klicken Sie auf **Weiter**.

VPN Wizard

VPN Wizard

Attributes Pushed to Client (Optional) (Step 7 of 11)

Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.

Tunnel Group: DefaultRAGroup

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

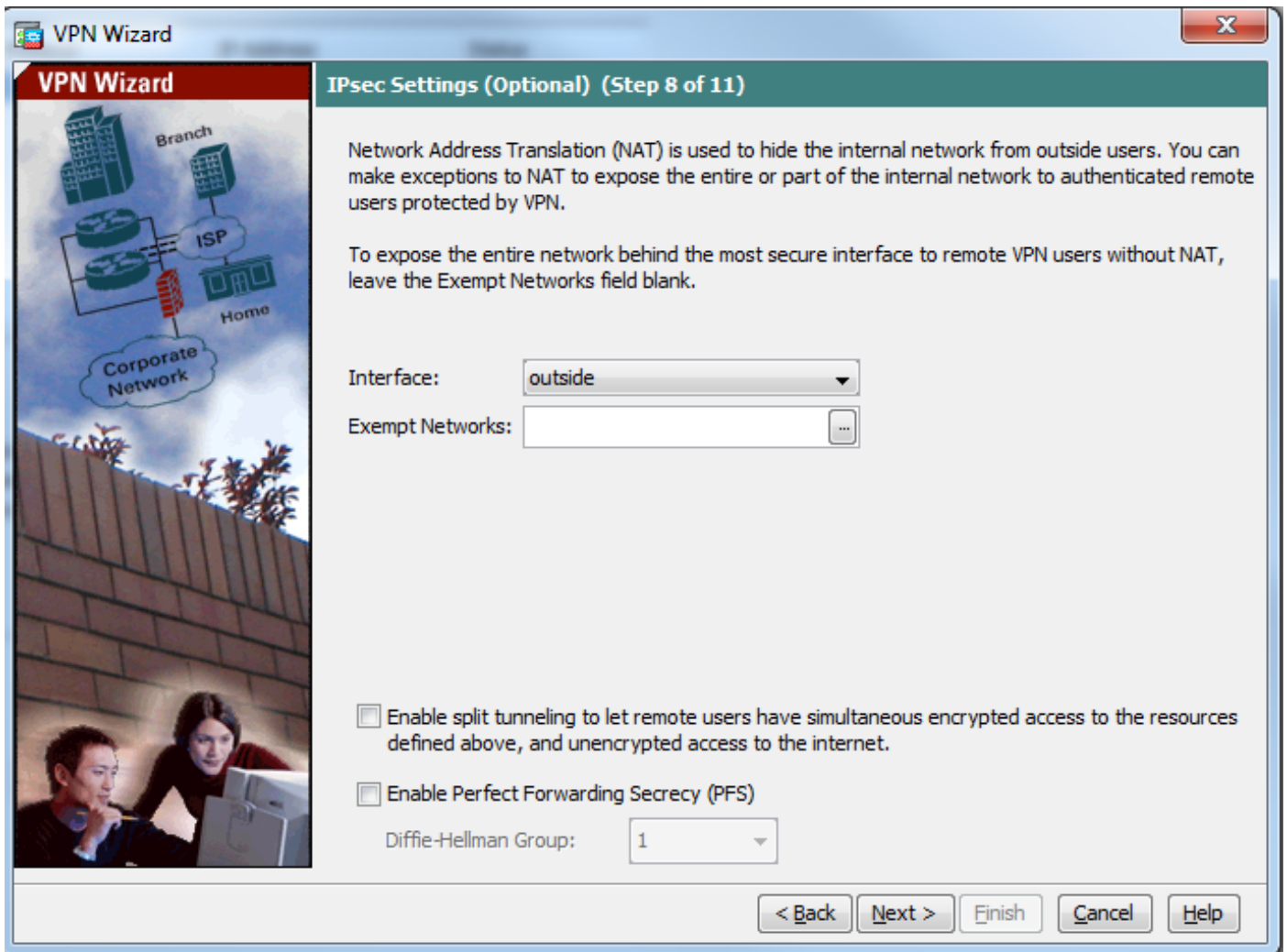
Secondary WINS Server:

Default Domain Name:

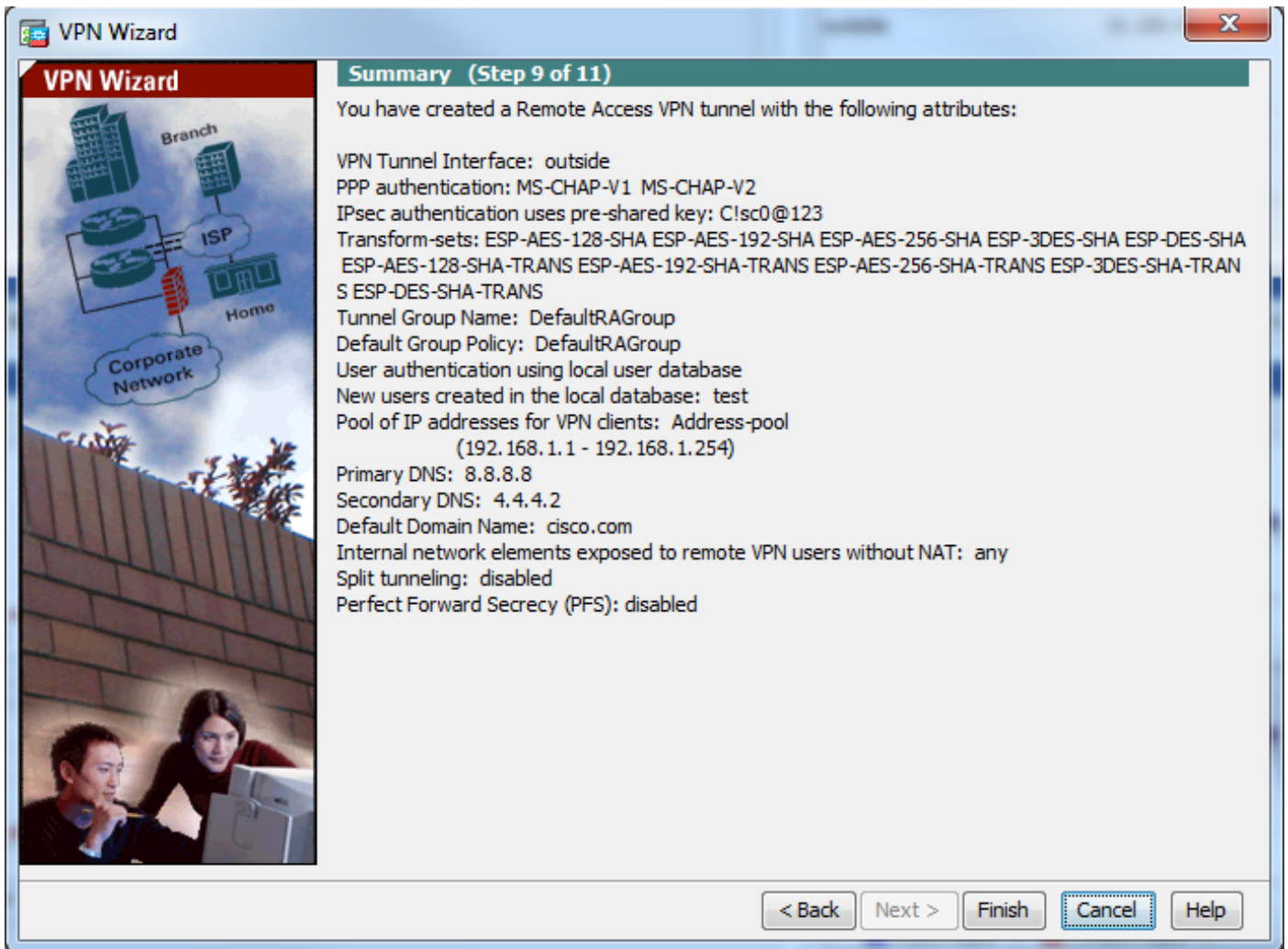
< Back Next > Finish Cancel Help

The image shows a screenshot of the 'VPN Wizard' software interface. On the left, there is a network diagram with labels: 'Branch', 'ISP', 'Home', and 'Corporate Network'. The main area is titled 'Attributes Pushed to Client (Optional) (Step 7 of 11)'. It contains a text box explaining that attributes are pushed to the VPN client. Below this are several configuration fields: 'Tunnel Group' (set to 'DefaultRAGroup'), 'Primary DNS Server' (8.8.8.8), 'Secondary DNS Server' (4.4.4.2), 'Primary WINS Server' (empty), 'Secondary WINS Server' (empty), and 'Default Domain Name' (cisco.com). At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Schritt 11: Stellen Sie sicher, dass das Kontrollkästchen **Enable Perfect Forwarding Secrecy (PFS)** deaktiviert ist, da einige Clientplattformen diese Funktion nicht unterstützen. **Aktivieren Sie das Split-Tunneling**, damit **Remote-Benutzer gleichzeitig verschlüsselten Zugriff auf die oben definierten Ressourcen haben und der unverschlüsselte Zugriff auf die Internet-Box nicht aktiviert** ist. Dies bedeutet, dass das vollständige Tunneling aktiviert ist, bei dem der gesamte Datenverkehr (einschließlich des Internetdatenverkehrs) vom Client-System über den VPN-Tunnel an die ASA gesendet wird. Klicken Sie auf **Weiter**.



Schritt 12: Überprüfen Sie die zusammengefassten Informationen, und klicken Sie dann auf **Fertig stellen**.



ASA-Konfiguration über CLI

Schritt 1: Konfigurieren der Richtlinienparameter für IKE Phase 1

Diese Richtlinie dient dem Schutz des Kontrolldatenverkehrs zwischen Peers (d. h. zum Schutz von Pre-Shared Key und Phase-2-Verhandlungen).

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

Schritt 2: Konfigurieren des Umwandlungssatzes

Sie enthält IKE Phase 2-Richtlinienparameter, die zum Schutz des Datenverkehrs verwendet werden. Da der Windows L2TP/IPsec-Client den IPsec-Transportmodus verwendet, legen Sie den Modus auf transport fest. Der Standardwert ist "Tunnel-Modus".

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

Schritt 3: Konfigurieren Sie die dynamische Zuordnung.

Wenn Windows-Clients dynamische IP-Adressen für ISP oder lokalen DHCP-Server (z. B.

Modem) erhalten, ist ASA über die Peer-IP-Adresse nicht informiert, und dies stellt ein Problem bei der Konfiguration eines statischen Peers auf dem ASA-Ende dar. Daher muss eine dynamische Verschlüsselungskonfiguration angefordert werden, bei der nicht unbedingt alle Parameter definiert sind und die fehlenden Parameter später dynamisch erfasst werden, als Ergebnis der IPsec-Aushandlung vom Client.

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA
```

Schritt 4: Binden Sie eine dynamische Zuordnung an eine statische Crypto Map, und wenden Sie die Crypto Map an, und aktivieren Sie IKEv1 auf der externen Schnittstelle.

Dynamische Kryptozuordnung kann nicht auf eine Schnittstelle angewendet werden und bindet sie daher an statische Crypto Map. Dynamische Kryptografiesätze sollten die Kryptozuordnungen mit der niedrigsten Priorität im Crypto Map-Satz sein (d. h. sie sollten über die höchsten Sequenznummern verfügen), sodass die ASA zuerst andere Crypto Maps auswertet. Sie untersucht die dynamische Crypto Map nur, wenn die anderen (statischen) Zuordnungseinträge nicht übereinstimmen.

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

Schritt 5: IP-Adresspool erstellen

Erstellen Sie einen Adresspool, aus dem den Remote-VPN-Clients dynamisch IP-Adressen zugewiesen werden. Ignorieren Sie diesen Schritt, um vorhandenen Pool auf ASA zu verwenden.

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

Schritt 6: Gruppenrichtlinie konfigurieren

Identifizieren Sie die Gruppenrichtlinie als intern, d. h., die Attribute werden aus der lokalen Datenbank gezogen.

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

Hinweis: L2TP-/IPsec-Verbindungen können entweder mit einer Standard-Gruppenrichtlinie (DfltGrpPolicy) oder einer benutzerdefinierten Gruppenrichtlinie konfiguriert werden. In beiden Fällen muss die Gruppenrichtlinie so konfiguriert werden, dass sie das L2TP/IPsec-Tunneling-Protokoll verwendet. Konfigurieren Sie l2tp-ipsec für das VPN-Protokollattribut in der Standardgruppenrichtlinie, die von der benutzerdefinierten Gruppenrichtlinie geerbt wird, wenn das VPN-Protokoll-Attribut nicht konfiguriert ist.

Konfigurieren Sie die Attribute wie das VPN-Tunnelprotokoll (in unserem Fall l2tp-ipsec), den Domännennamen, die DNS- und WINS-Server-IP-Adresse und neue Benutzerkonten.

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

Konfigurieren Sie neben der Verwendung von AAA Benutzernamen und Kennwörter auf dem Gerät. Wenn der Benutzer ein L2TP-Client ist, der Microsoft CHAP-Version 1 oder 2 verwendet und die ASA für die Authentifizierung über die lokale Datenbank konfiguriert ist, muss das

mschap-Schlüsselwort enthalten sein. Beispiel: username <username> password <password> mschap.

```
ciscoasa(config-group-policy)# username test password test mschap
```

Schritt 7: Tunnelgruppe konfigurieren

Erstellen Sie eine Tunnelgruppe mit dem Befehl **tunnel-group**, und geben Sie den Namen des lokalen Adresspools an, mit dem die IP-Adresse dem Client zugewiesen wird. Wenn die Authentifizierungsmethode ein Pre-Shared-Key ist, muss der Tunnelgruppenname DefaultRAGroup sein, da auf dem Client keine Option zum Angeben der Tunnelgruppe vorhanden ist. Daher wird sie nur in die Standard-Tunnelgruppe aufgenommen. Binden Sie die Gruppenrichtlinie mithilfe des Befehls **default-group-policy** an tunnel group.

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

Hinweis: Das Standard-Verbindungsprofil (Tunnelgruppe) DefaultRAGroup muss konfiguriert werden, wenn eine vorinstallierte Schlüsselauthentifizierung durchgeführt wird. Wenn eine zertifikatbasierte Authentifizierung durchgeführt wird, kann ein benutzerdefiniertes Verbindungsprofil basierend auf Zertifikatbezeichnern ausgewählt werden.

Verwenden Sie den Befehl **tunnel-group ipsec-attribute**, um in den Konfigurationsmodus ipsec-attribute zu wechseln, um den vorinstallierten Schlüssel festzulegen.

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

Konfigurieren Sie das PPP-Authentifizierungsprotokoll mithilfe des Befehls **Authentifizierungstyp** im Tunnelgruppen-ppp-Attributmodus. Deaktivieren Sie CHAP, das standardmäßig aktiviert ist, da es nicht unterstützt wird, wenn AAA-Server als lokale Datenbank konfiguriert ist.

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

Schritt 8: Konfigurieren der NAT-Ausnahme

Konfigurieren Sie die NAT-Ausnahme so, dass die Clients auf interne Ressourcen zugreifen können, die mit internen Schnittstellen verbunden sind (in diesem Beispiel sind interne Ressourcen mit internen Schnittstellen verbunden).

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-
Pool no-proxy-arp route-lookup
```

Vollständige Beispielkonfiguration

```
crypto ikev1 policy 10
```

```

authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit

crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside

ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
default-group-policy L2TP-VPN
exit

tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

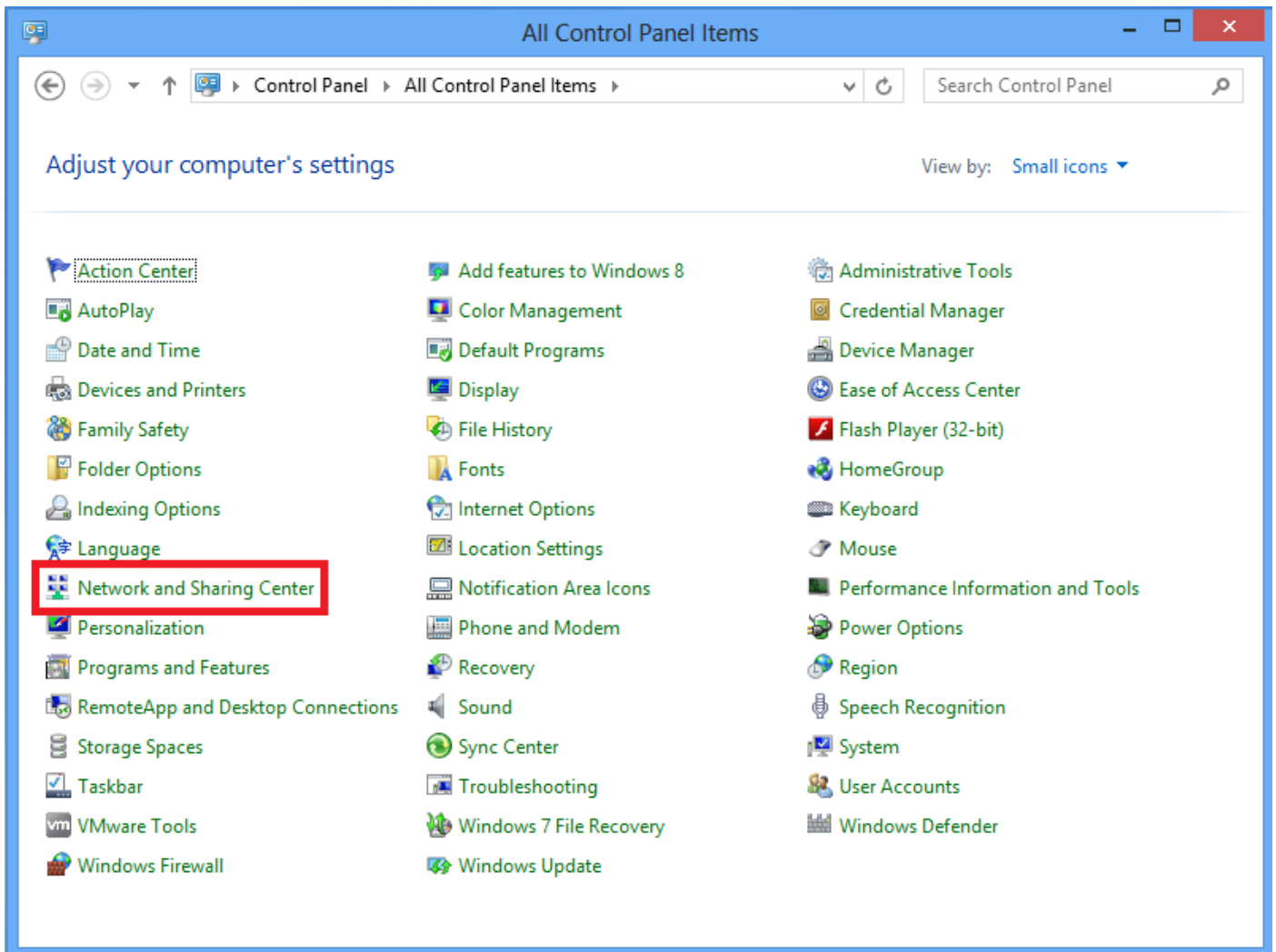
tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
exit

object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup

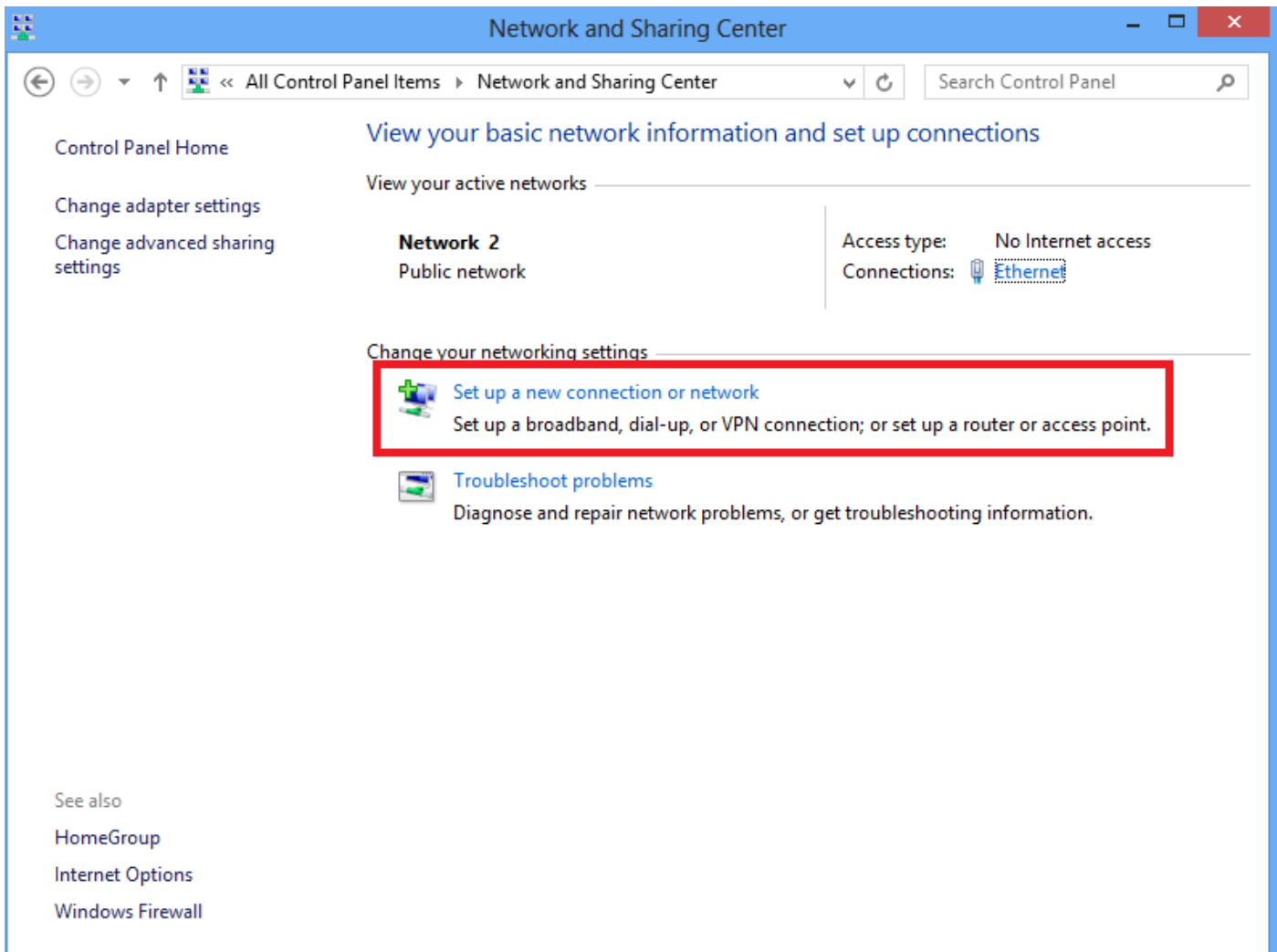
```

Windows 8 - Client-Konfiguration für L2TP/IPsec

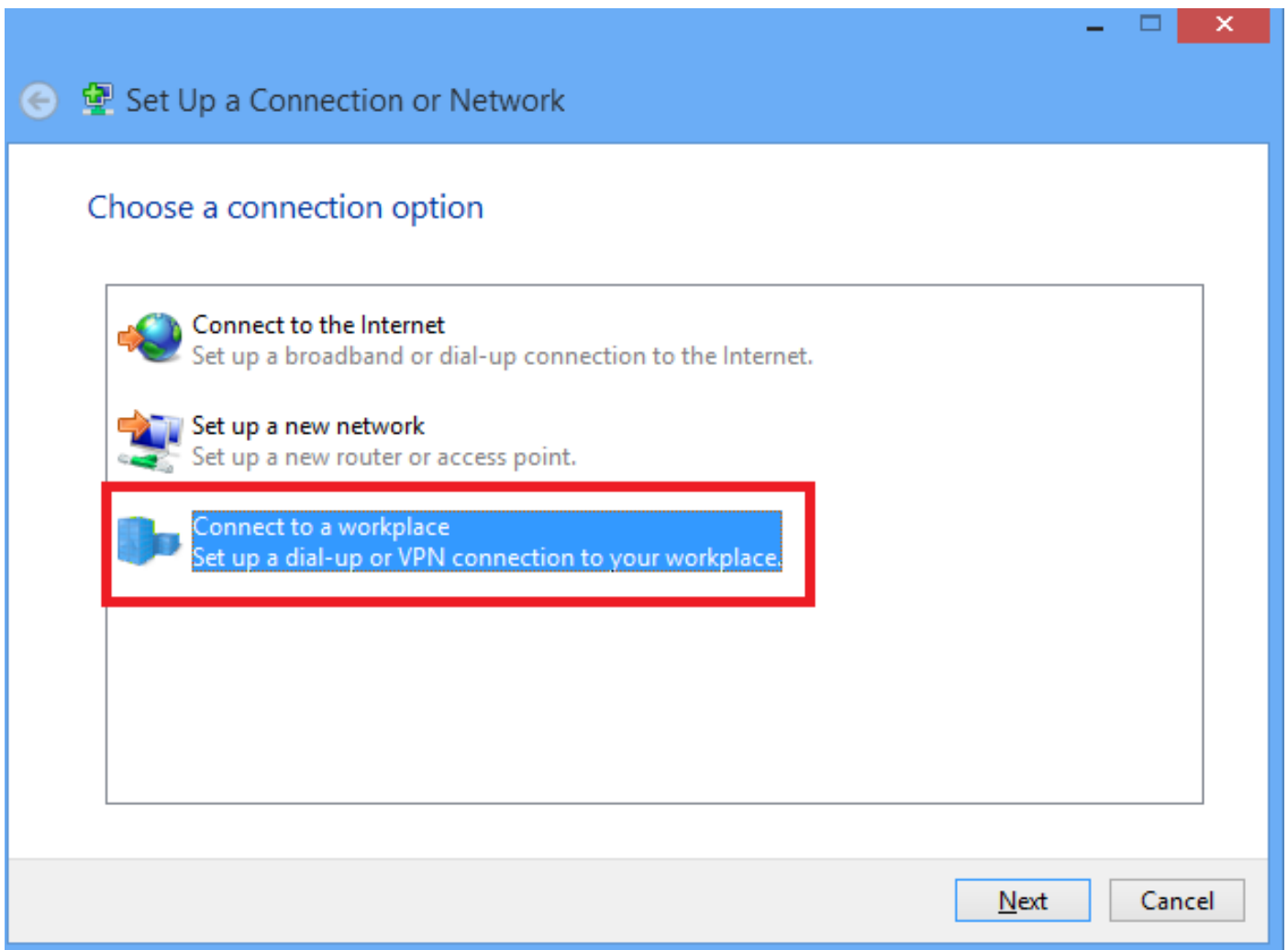
1. Öffnen Sie die Systemsteuerung, und wählen Sie Netzwerk- und Freigabecenter aus.



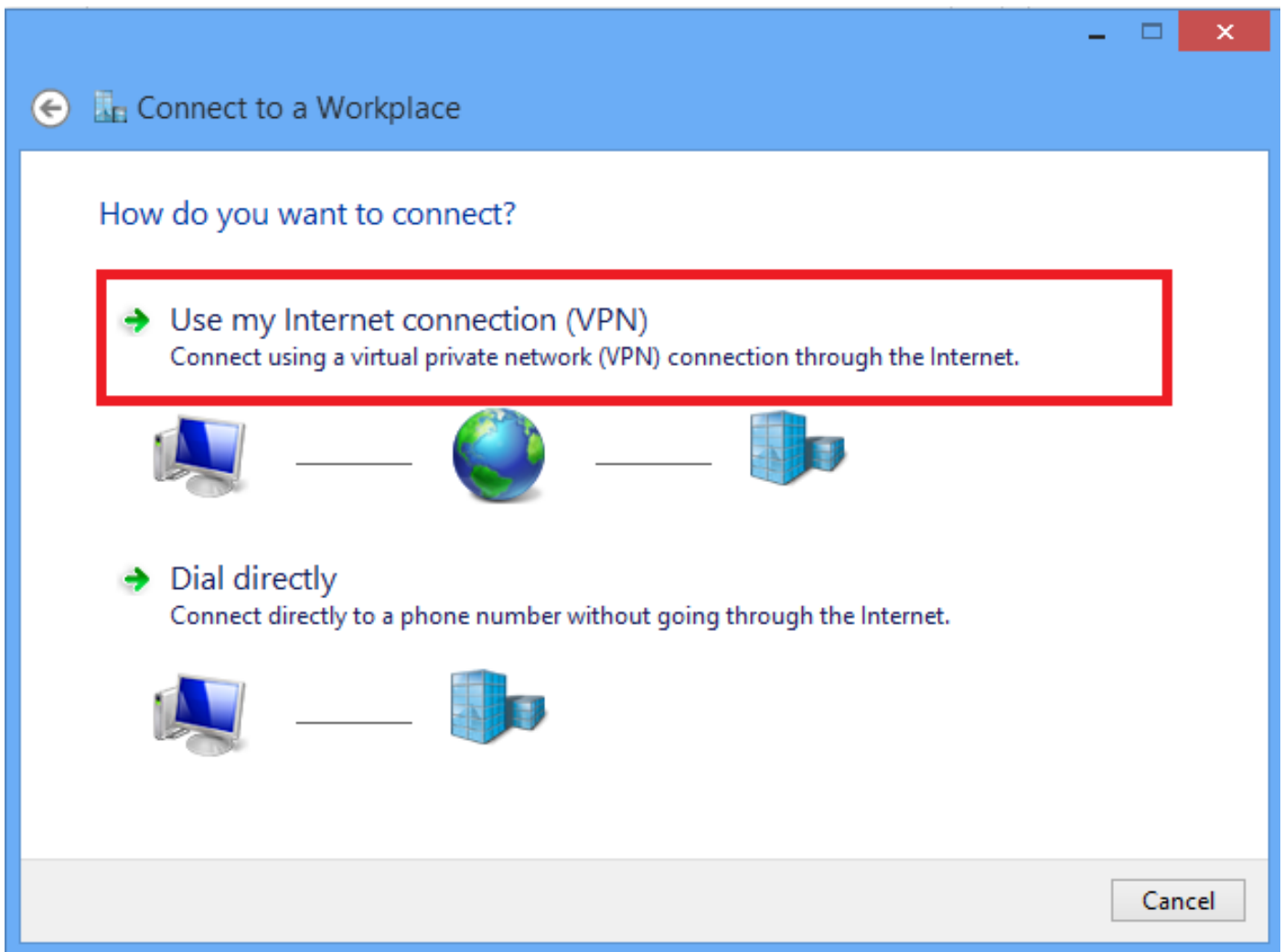
2. Wählen Sie **Neue Verbindung** oder **Netzwerkoption einrichten** aus.



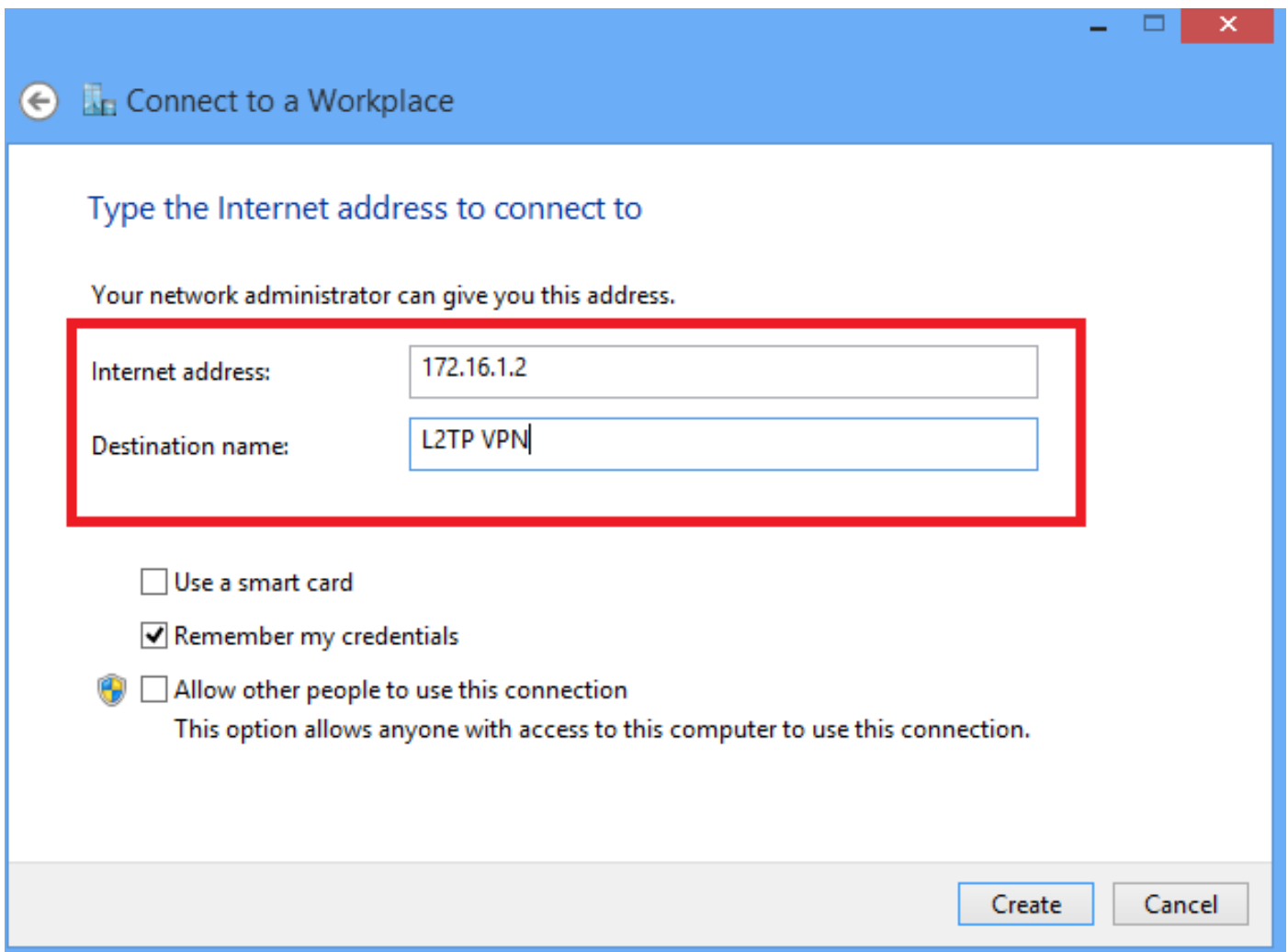
3. Wählen Sie die Option **Verbindung mit einem Arbeitsplatz herstellen aus**, und klicken Sie auf **Weiter**.



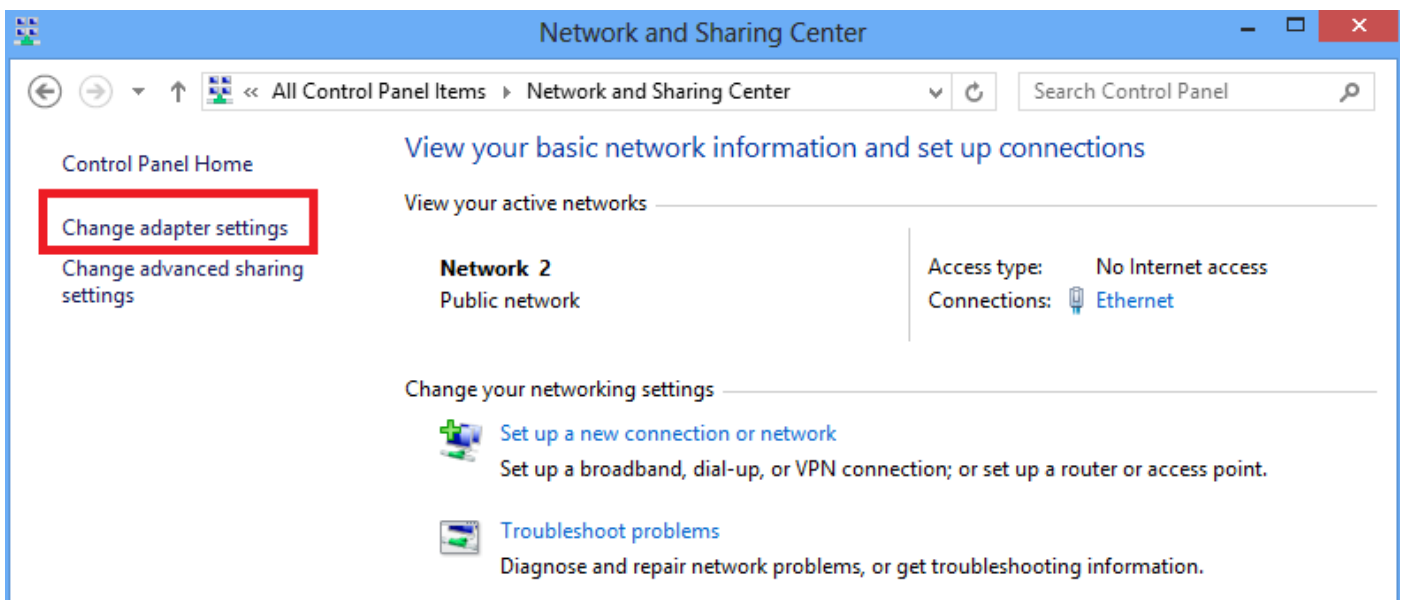
4. Klicken Sie auf Option **Meine Internetverbindung (VPN) verwenden**.



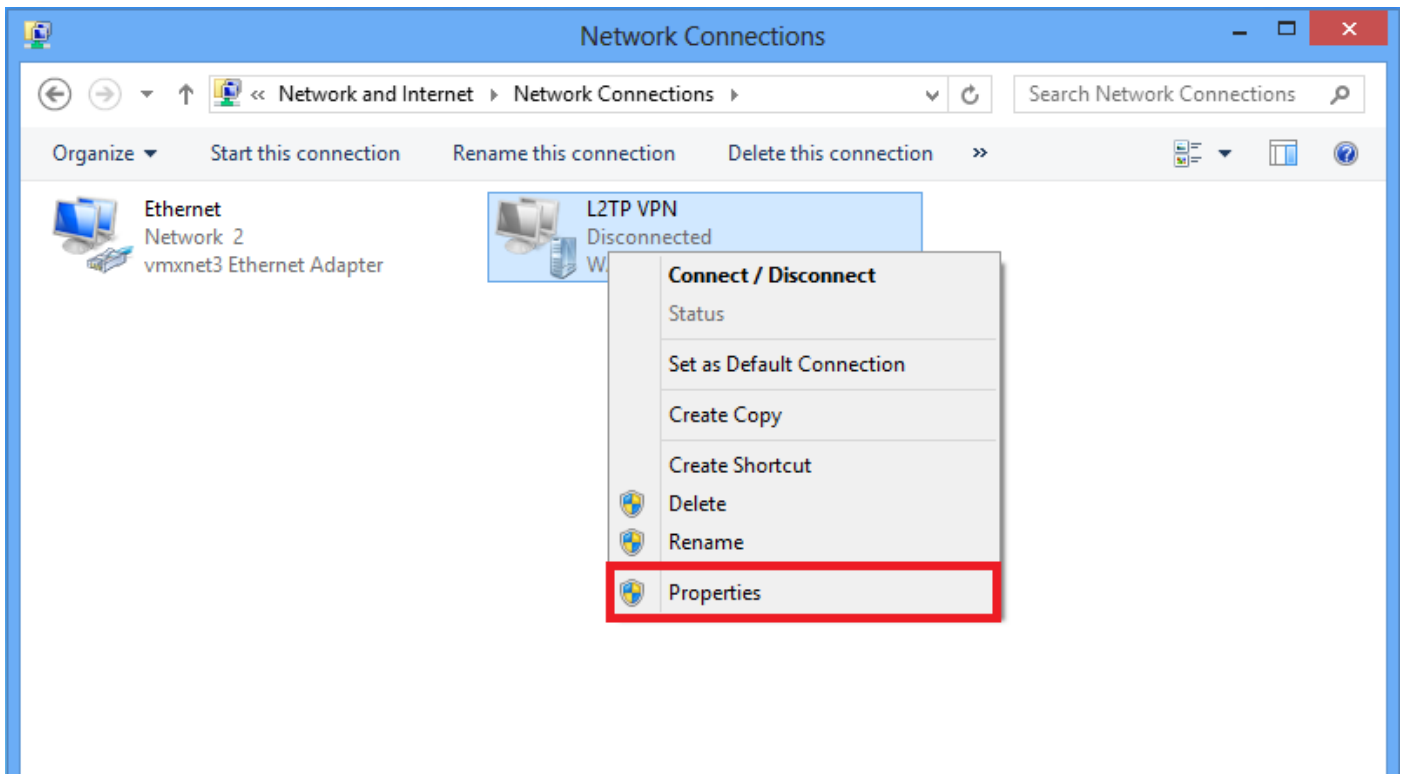
5. Geben Sie die IP-Adresse der WAN-Schnittstelle oder des FQDN sowie einen beliebigen lokal bedeutsamen Namen für den VPN-Adapter ein, und klicken Sie auf **Erstellen**.



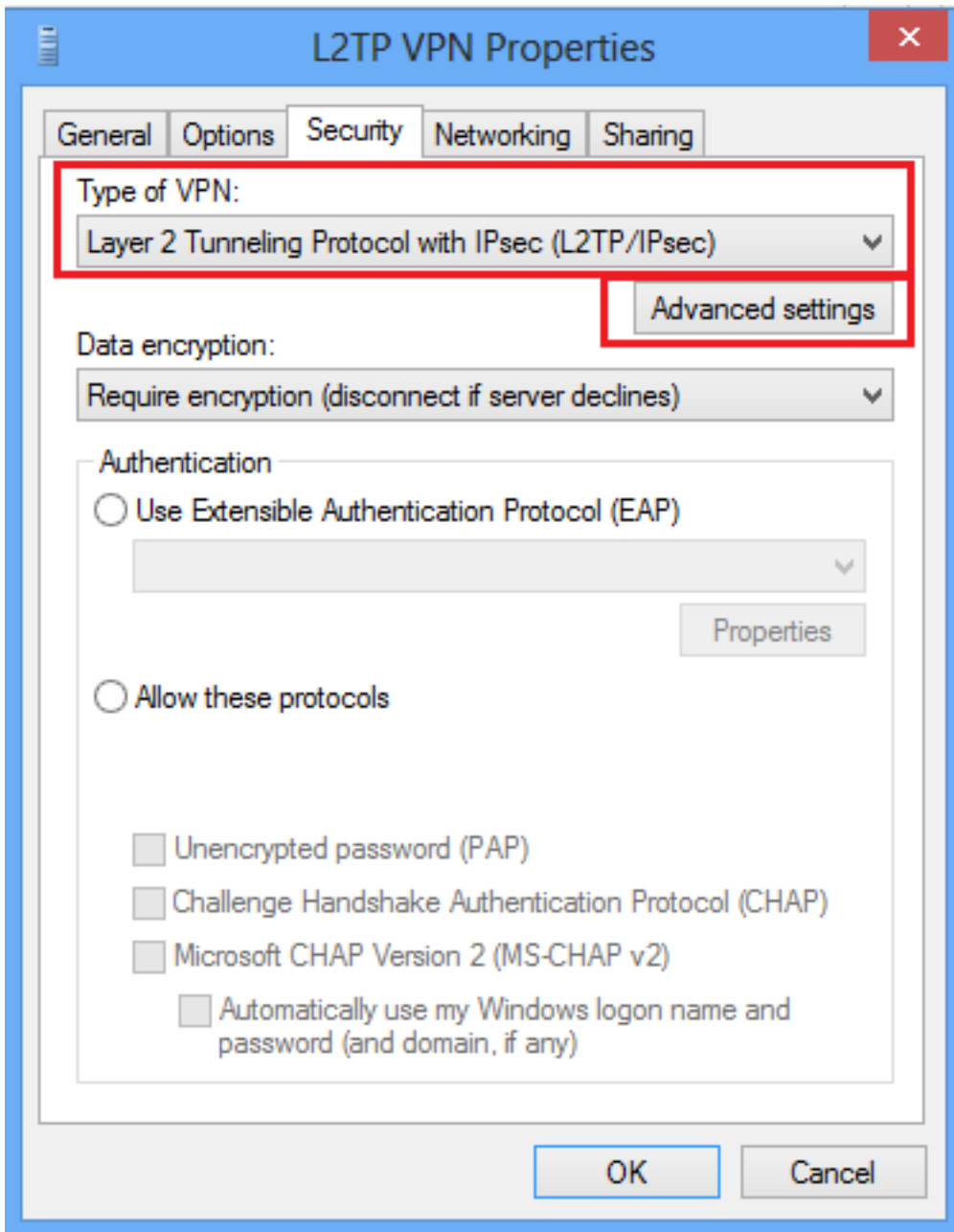
6. Wählen Sie im Netzwerk- und Freigabecenter im linken Fensterbereich die Option **Adaptoreinstellungen ändern** aus.



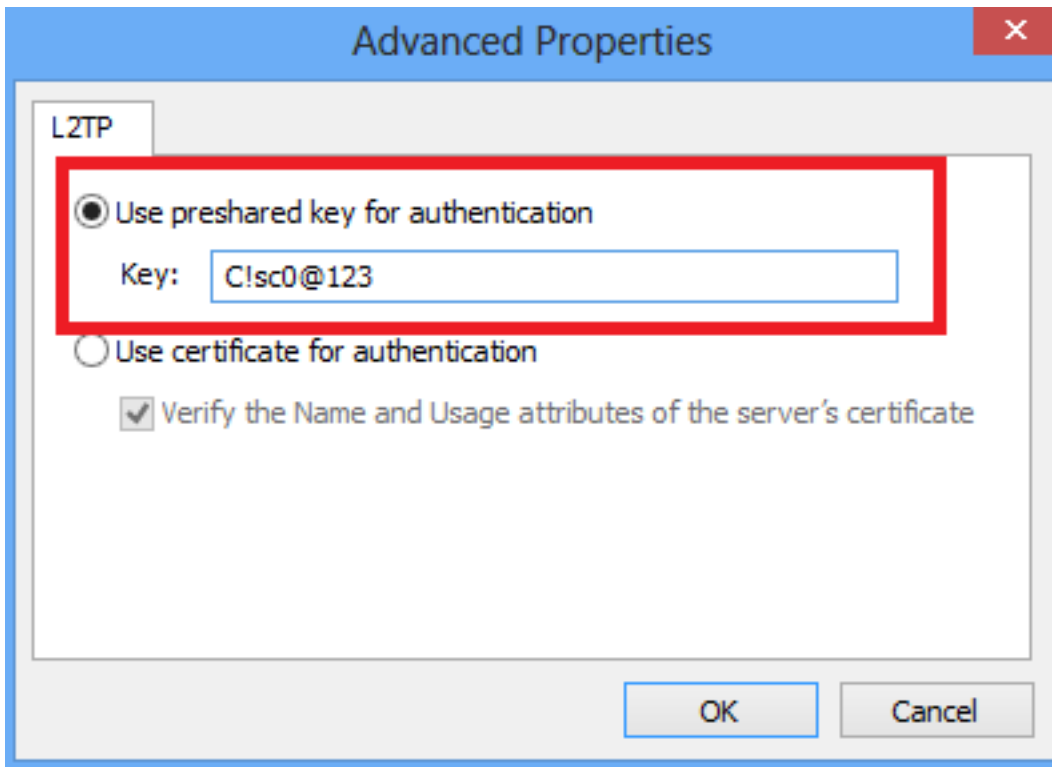
7. Klicken Sie mit der rechten Maustaste auf den kürzlich erstellten Adapter für L2TP VPN, und wählen Sie **Eigenschaften** aus.



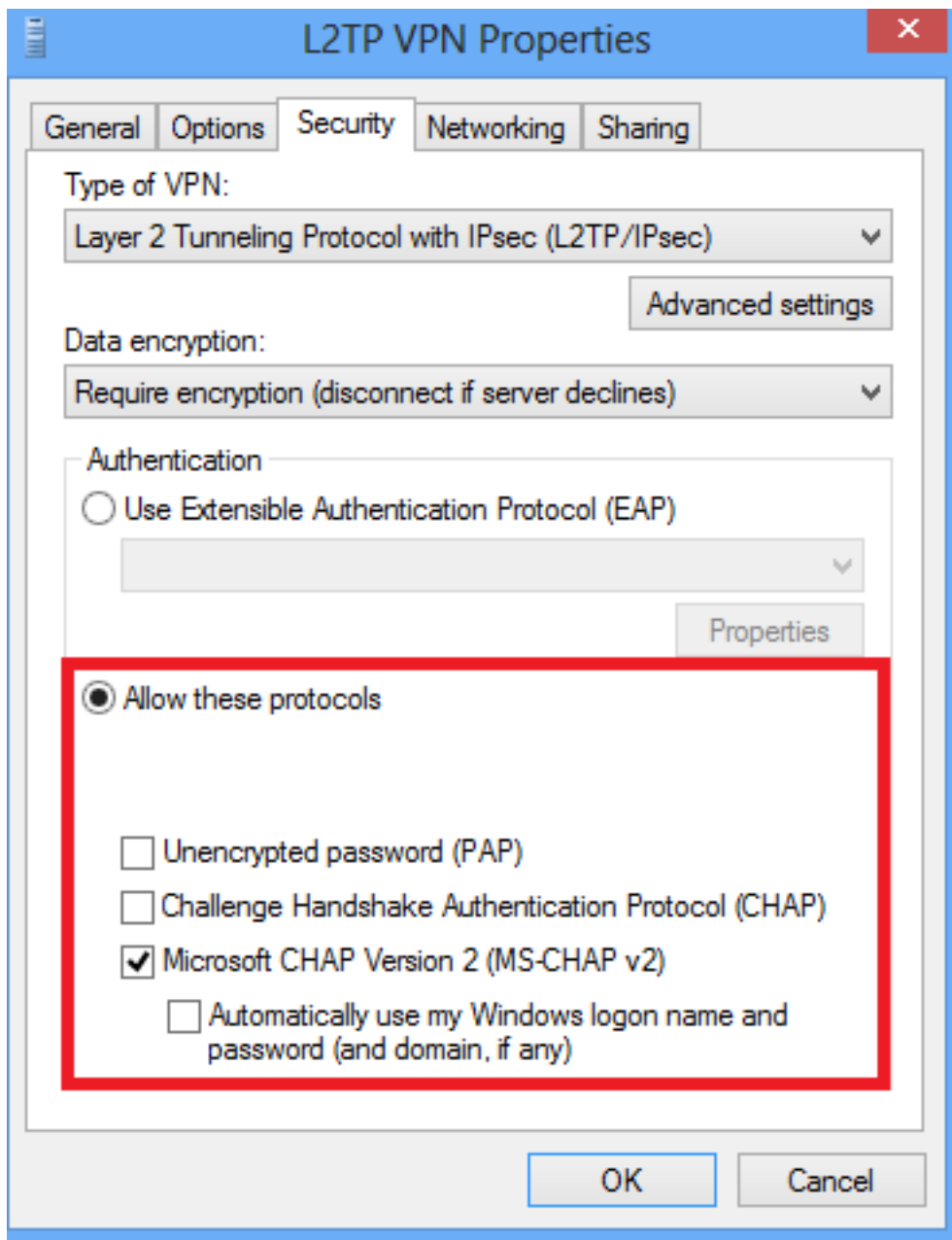
8. Navigieren Sie zur Registerkarte **Sicherheit**, wählen Sie den VPN-Typ als **Layer-2-Tunneling-Protokoll mit IPsec (L2TP/IPsec)** aus, und klicken Sie dann auf **Erweiterte Einstellungen**.



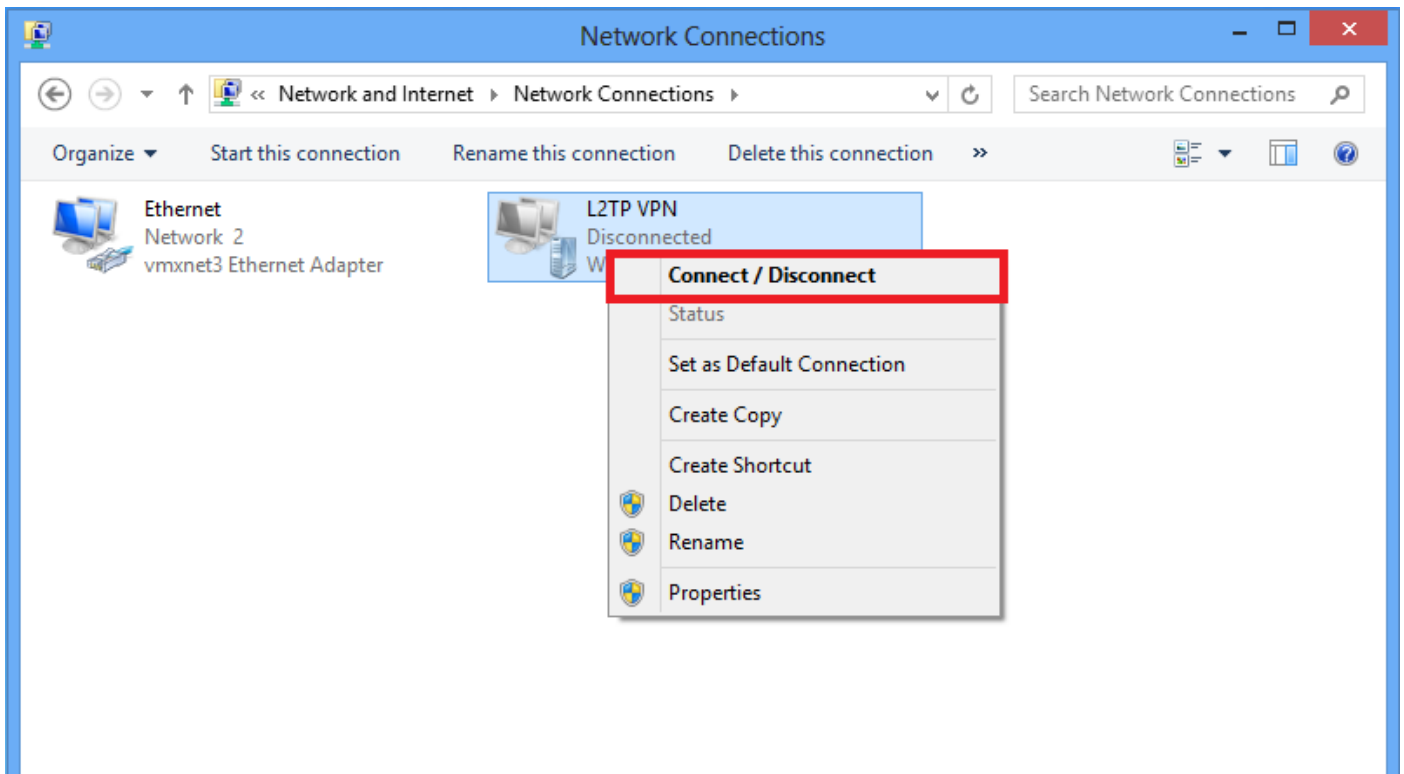
9. Geben Sie den vorinstallierten Schlüssel ein, der in der Tunnelgruppe **DefaultRAGroup** identisch ist, und klicken Sie auf **OK**. In diesem Beispiel wird **C!sc0@123** als vorinstallierter Schlüssel verwendet.



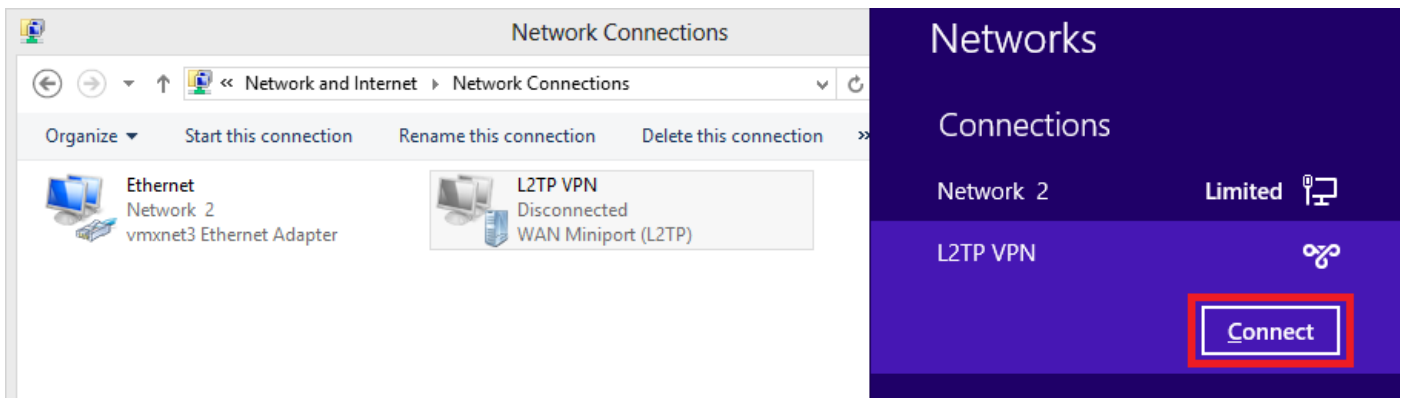
10. Wählen Sie die Authentifizierungsmethode als Diese Protokolle zulassen aus, und stellen Sie sicher, dass nur das Kontrollkästchen "**Microsoft CHAP Version 2 (MS-CHAP v2)**" aktiviert ist, und klicken Sie auf **OK**.



11. Klicken Sie unter Netzwerkverbindungen mit der rechten Maustaste auf den L2TP VPN-Adapter, und wählen Sie **Verbinden/Trennen aus**.



12. Das Symbol "Netzwerke" wird angezeigt, und Sie klicken auf "Connect on L2TP VPN connection" (**Verbinden** mit L2TP-VPN-Verbindung).



13. Geben Sie die Benutzeranmeldeinformationen ein, und klicken Sie auf **OK**.

← Networks

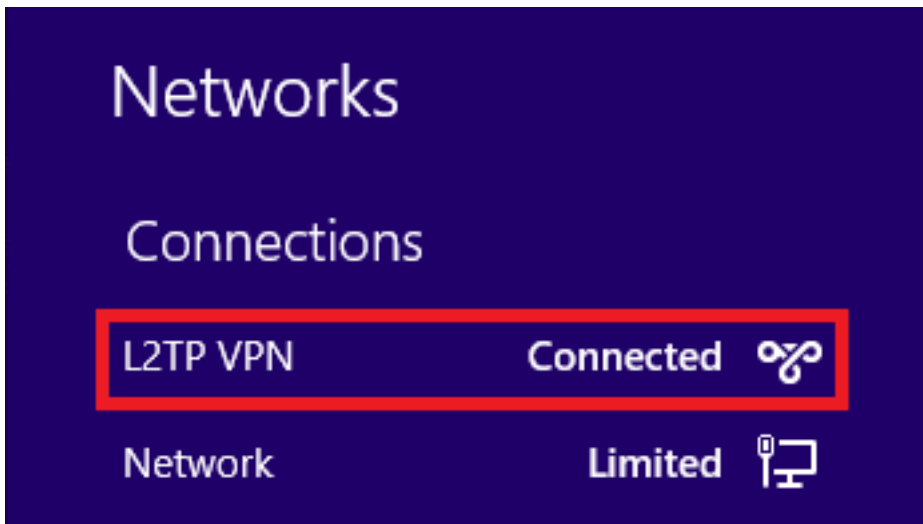
Connecting to 172.16.1.2

Network Authentication



Domain:

Wenn die erforderlichen Parameter an beiden Enden übereinstimmen, wird eine L2TP/IPsec-Verbindung hergestellt.



Split-Tunnel-Konfiguration

Split-Tunneling ist eine Funktion, mit der Sie den Datenverkehr für die zu verschlüsselnden Subnetze oder Hosts definieren können. Dazu gehört die Konfiguration einer Zugriffssteuerungsliste (ACL), die dieser Funktion zugeordnet ist. Der Datenverkehr für die in dieser ACL definierten Subnetze oder Hosts wird vom Client-End über den Tunnel verschlüsselt, und die Routen für diese Subnetze werden in der PC-Routing-Tabelle installiert. ASA fängt DHCPINFORM-Nachrichten von einem Client ab und antwortet mit der Subnetzmaske, dem Domännennamen und klassischen statischen Routen.

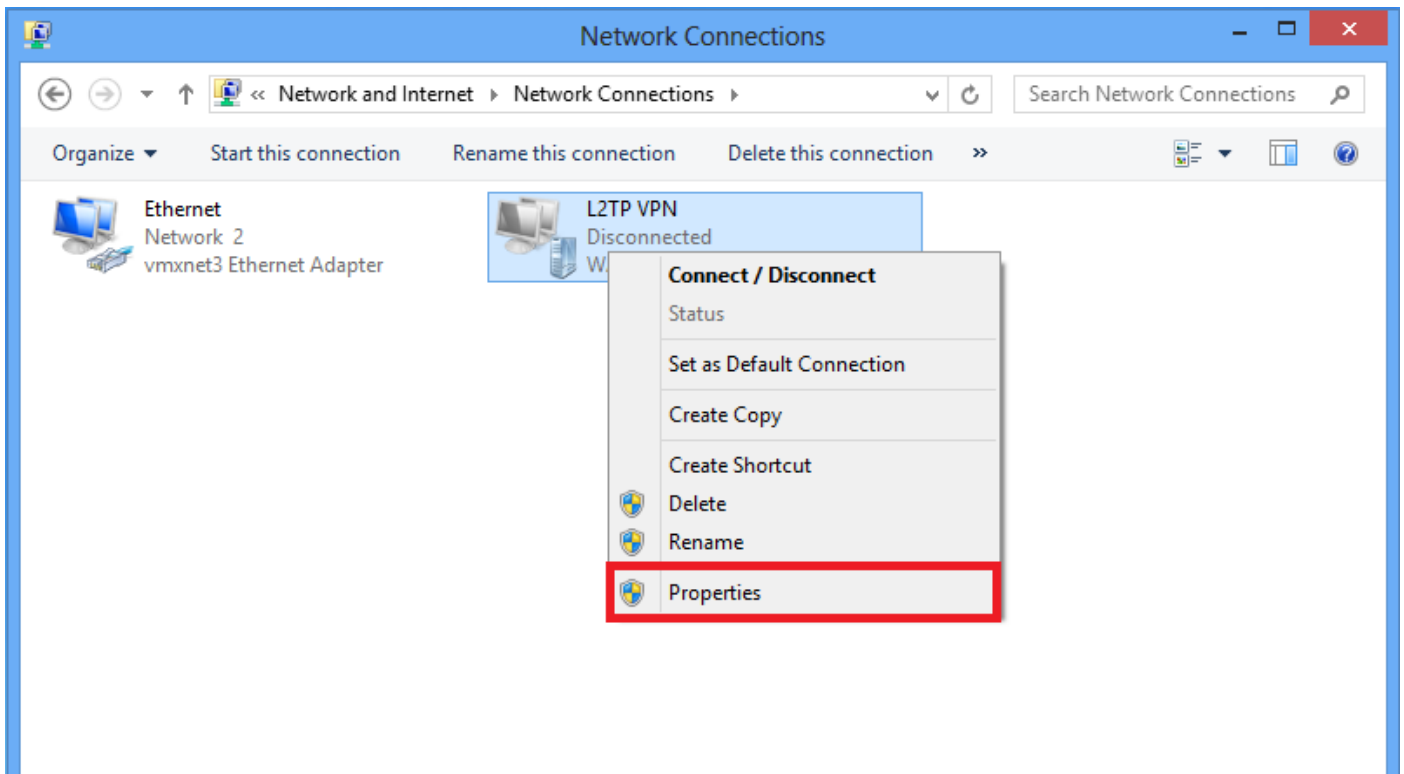
Konfiguration auf ASA

```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0
```

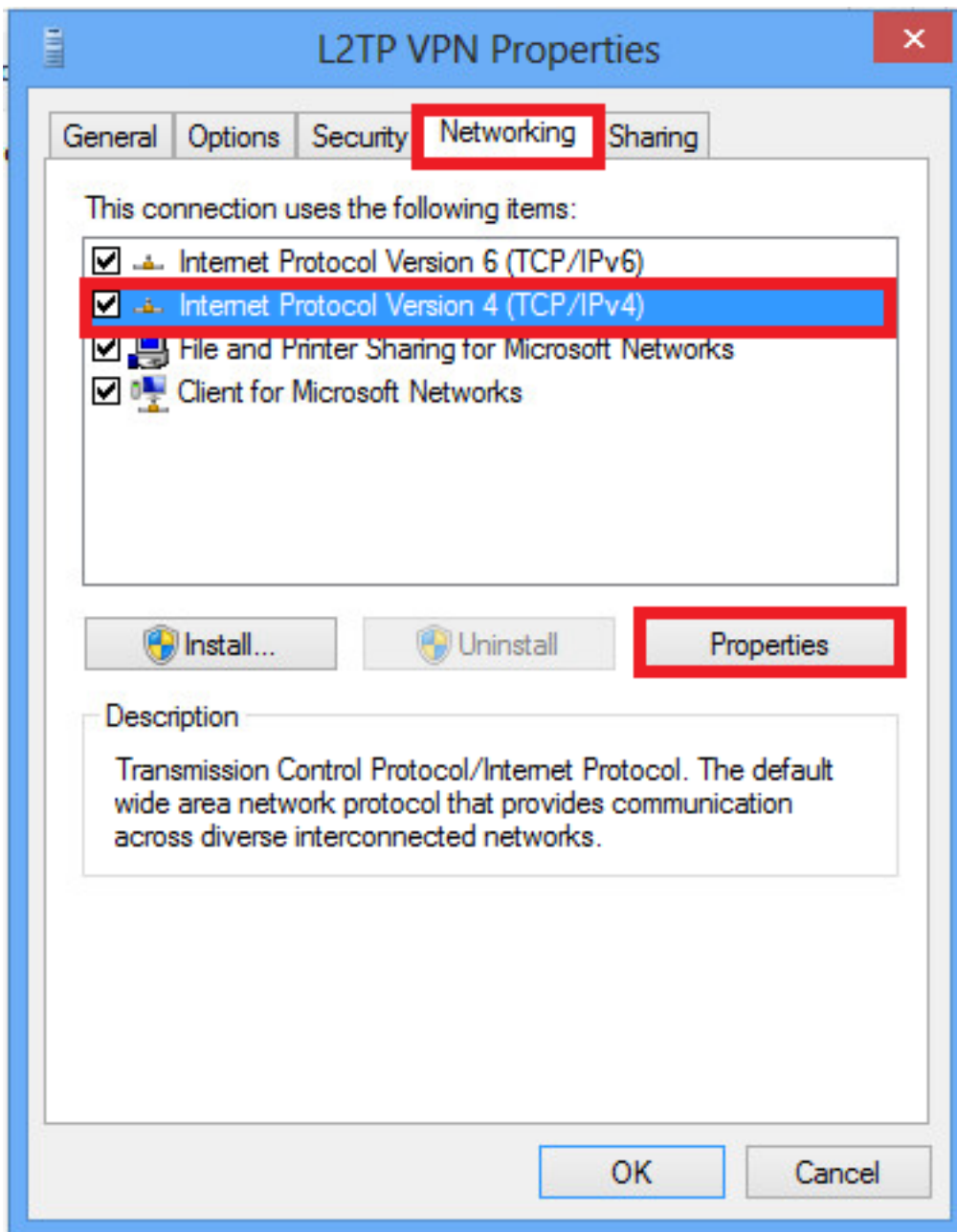
```
ciscoasa(config)# group-policy DefaultRAGroup attributes  
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified  
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT  
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

Konfiguration auf L2TP/IPsec-Client

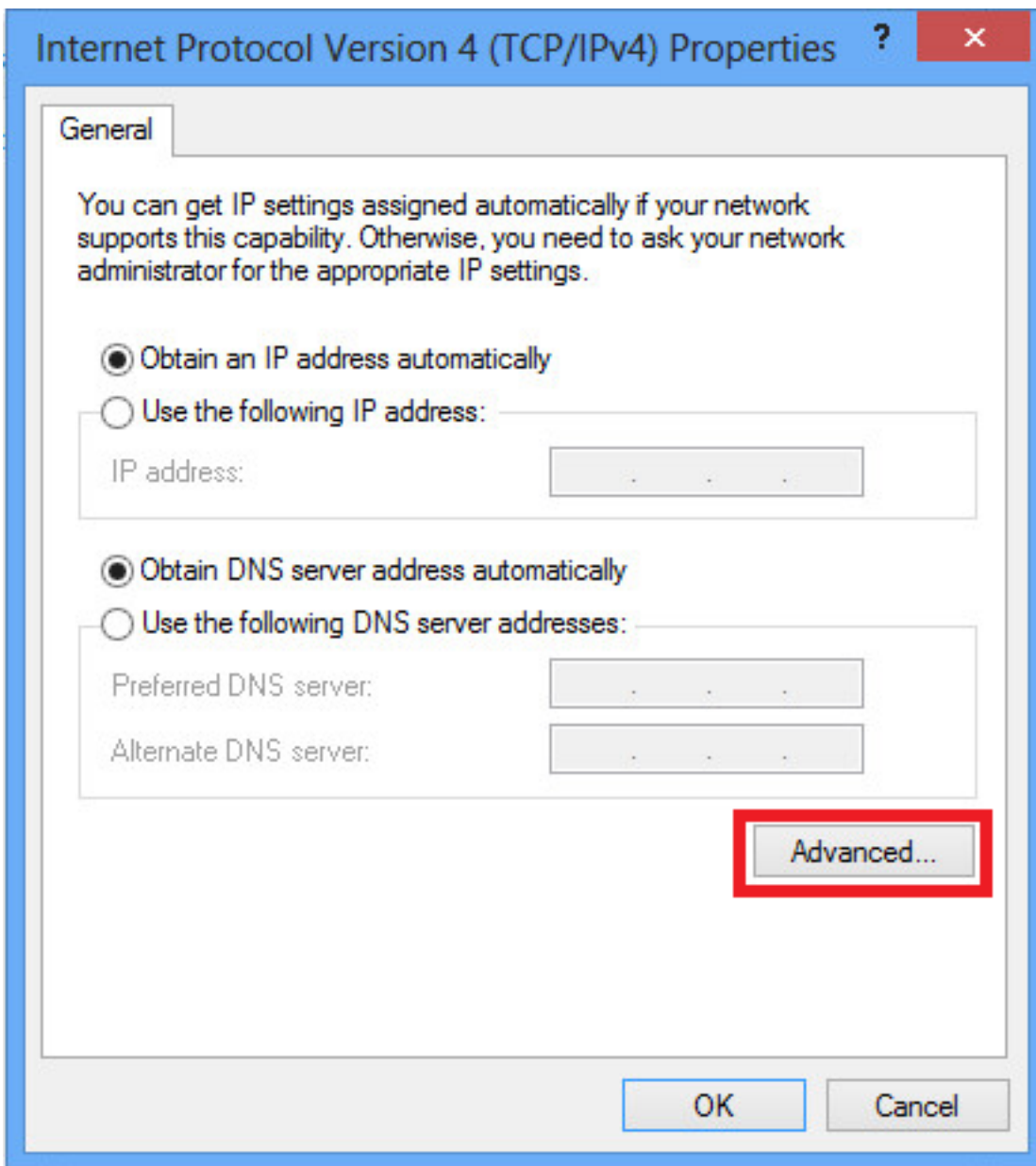
1. Klicken Sie mit der rechten Maustaste auf den L2TP VPN-Adapter, und wählen Sie **Eigenschaften aus**.



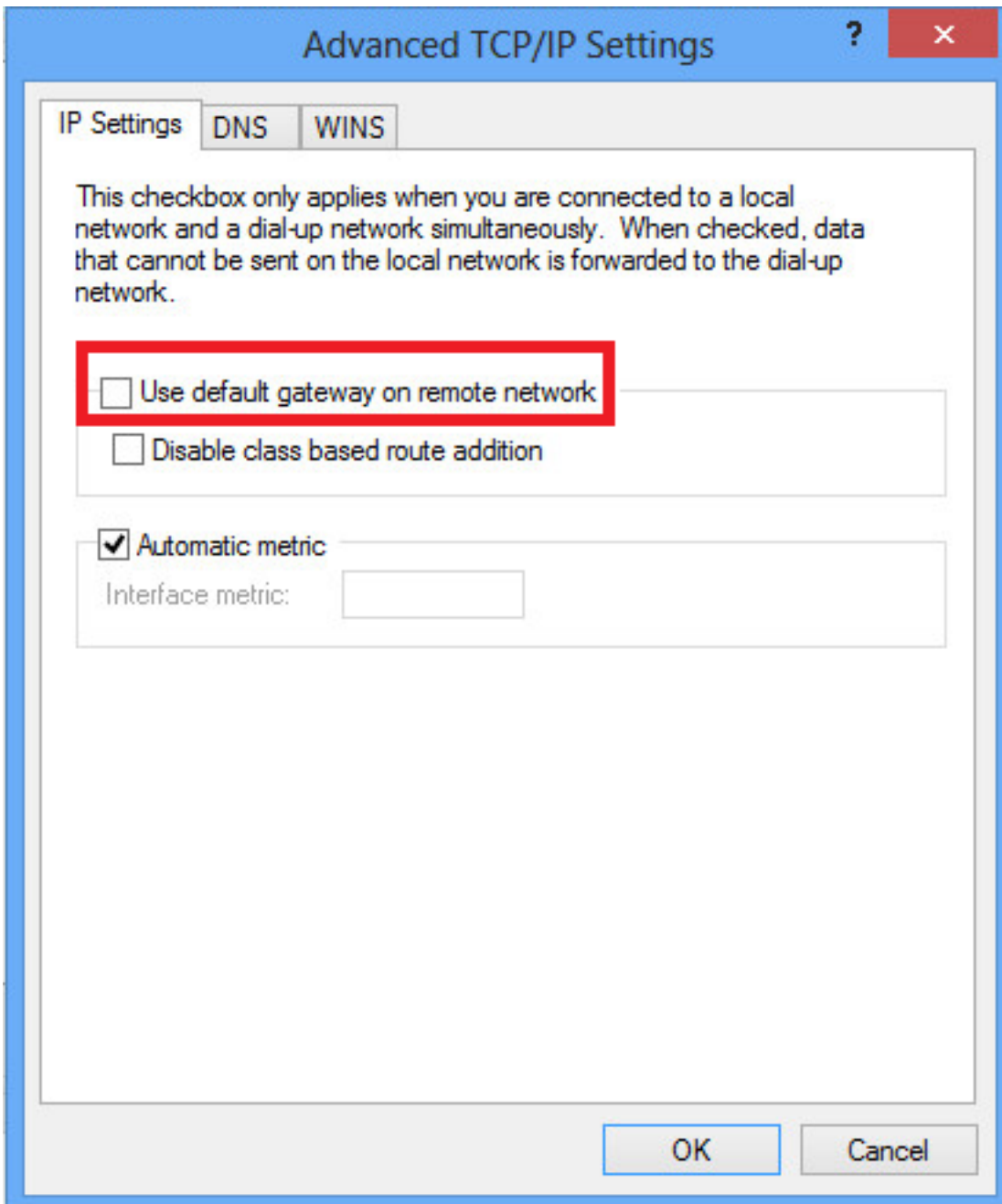
2. Navigieren Sie zur Registerkarte Networking, wählen Sie Internetprotokoll Version 4 (TCP/IPv4) aus, und klicken Sie dann auf **Eigenschaften**.



3. Klicken Sie auf **Erweiterte** Option.



4. Deaktivieren Sie die Option **Standard-Gateway für Remote-Netzwerk verwenden**, und klicken Sie auf **OK**.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Hinweis: Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

- `show crypto ikev1 sa` - Zeigt alle aktuellen IKE-SAs in einem Peer an.

```
ciscoasa# show crypto ikev1 sa
```

```
IKEv1 SAs:
```

```
Active SA: 1
```

```
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
```

Total IKE SA: 1

1 IKE Peer:

10.1.1.2

Type : user Role : responder
Rekey : no

State : MM_ACTIVE

- **show crypto ipsec sa** - Zeigt alle aktuellen IPsec-SAs in einem Peer an.

```
ciscoasa# show crypto ipsec sa  
interface: outside  
Crypto map tag:
```

outside_dyn_map

, seq num: 10, local addr: 172.16.1.2

local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

17/1701

)
remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

17/1701

)

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

dynamic allocated peer ip(ipv6): 0.0.0.0

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

```
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
path mtu 1500, ipsec overhead 58(36), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: E8AF927A
current inbound spi : 71F346AB
```

```
inbound esp sas:
spi: 0x71F346AB (1911768747)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Transport, IKEv1, }
  slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (237303/3541)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000003
```

```
outbound esp sas:
spi: 0xE8AF927A (3903820410)
  transform: esp-3des esp-sha-hmac no compression
  in use settings = {RA, Transport, IKEv1, }
  slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (kB/sec): (237303/3541)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

- show vpn-sessiondb detail ra-ikev1-ipsec filterprotokoll l2tpOverIPsec - Zeigt detaillierte Informationen über L2TP über IPsec-Verbindungen.

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIPsec
```

Session Type: IKEv1 IPsec Detailed

Username : test

Index : 1

Assigned IP : 192.168.1.1 Public IP : 10.1.1.2

```
Protocol : IKEv1 IPsec L2TPOverIPsec
License : Other VPN
Encryption : IKEv1: (1)3DES IPsec: (1)3DES L2TPOverIPsec: (1)none
Hashing : IKEv1: (1)SHA1 IPsec: (1)SHA1 L2TPOverIPsec: (1)none
Bytes Tx : 1574                      Bytes Rx : 12752
Pkts Tx : 29                        Pkts Rx : 118
Pkts Tx Drop : 0                    Pkts Rx Drop : 0
```

Group Policy : L2TP-VPN Tunnel Group : DefaultRAGroup

Login Time : 23:32:48 UTC Sat May 16 2015

Duration : 0h:04m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2577000010005557d3a0
Security Grp : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1

IKEv1:

Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Main Auth Mode : preSharedKeys
Encryption : 3DES Hashing : SHA1
Rekey Int (T): 28800 Seconds Rekey Left(T): 28555 Seconds
D/H Group : 2
Filter Name :

IPsec:

Tunnel ID : 1.2
Local Addr : 172.16.1.2/255.255.255.255/17/1701
Remote Addr : 10.1.1.2/255.255.255.255/17/1701
Encryption : 3DES Hashing : SHA1
Encapsulation: Transport
Rekey Int (T): 3600 Seconds Rekey Left(T): 3576 Seconds
Rekey Int (D): 250000 K-Bytes Rekey Left(D): 250000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 1574 Bytes Rx : 12752
Pkts Tx : 29 Pkts Rx : 118

L2TPOverIPsec:

Tunnel ID : 1.3

Username : test

Assigned IP : 192.168.1.1

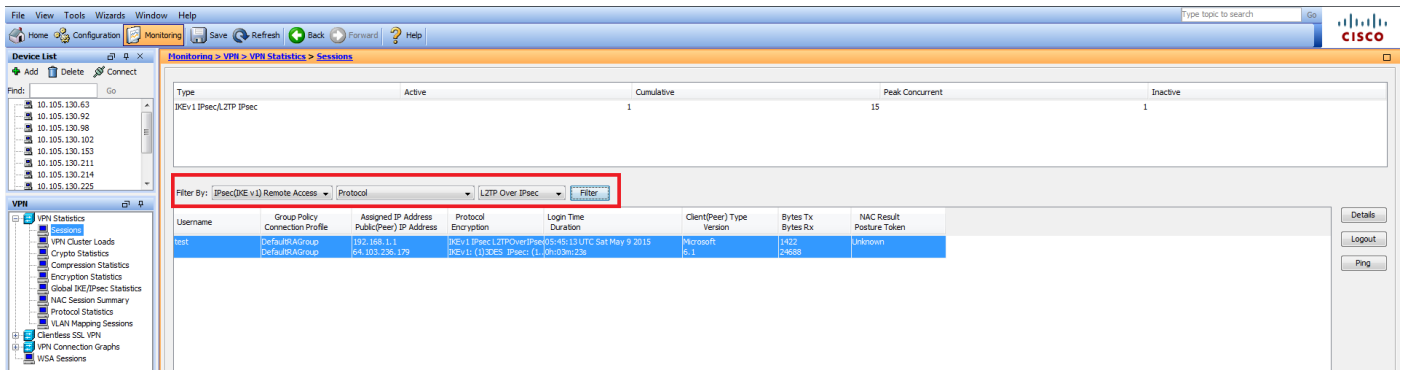
Public IP : 10.1.1.2

Encryption : none Hashing : none

Auth Mode : msCHAPV2

Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Microsoft
Client OS Ver: 6.2
Bytes Tx : 475 Bytes Rx : 9093
Pkts Tx : 18 Pkts Rx : 105

Auf ASDM sind unter **Monitoring > VPN > VPN Statistics > Sessions** die allgemeinen Informationen zur VPN-Sitzung zu sehen. L2TP über IPsec-Sitzungen können durch **IPsec (IKEv1) Remote Access > Protocol > L2TP Over IPsec** gefiltert werden.



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Hinweis: Weitere Informationen [zu Debug-Befehlen](#) vor der Verwendung von **Debug-**Befehlen finden Sie unter [Wichtige Informationen](#).

Vorsicht: Auf der ASA können Sie verschiedene Debug-Ebenen festlegen. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debugebene ändern, kann sich die Ausführlichkeit der Debuggen erhöhen. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor!

Verwenden Sie die folgenden **Debugbefehle mit Vorsicht**, um Probleme mit dem VPN-Tunnel zu beheben.

- **debug crypto ikev1** - Zeigt Debuginformationen über IKE an
- **debug crypto ipsec** - Zeigt Debuginformationen über IPsec an

Hier ist die Debug-Ausgabe für eine erfolgreiche L2TP über IPsec-Verbindung:

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
```

May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,

Connection landed on tunnel_group DefaultRAGroup

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304

May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPsec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

IPsec SA Proposal # 2, Transform # 1 acceptable

Matches global IPsec SA entry # 10

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!

IPSEC: New embryonic SA created @ 0x00007ffffe13ab260,

SCB: 0xE1C00540,

Direction: inbound

SPI : 0x7AD72E0D

Session ID: 0x00001000

VPIF num : 0x00000002

Tunnel type: ra

Protocol : esp

Lifetime : 240 seconds

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine:

SPI = 0x7ad72e0d

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constructing quick mode

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPsec SA payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPsec nonce payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload

May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd QM pkt: msg id = 00000001

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160

May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + NONE (0) total length : 52

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;

```
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x00007ffffelc75c00,
  SCB: 0xE13ABD20,
  Direction: outbound
  SPI      : 0x8C14FD70
  Session ID: 0x00001000
  VPIF num : 0x00000002
  Tunnel type: ra
  Protocol  : esp
  Lifetime  : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x8C14FD70
IPSEC: Creating outbound VPN context, SPI 0x8C14FD70
  Flags: 0x00000205
  SA    : 0x00007ffffelc75c00
  SPI   : 0x8C14FD70
  MTU   : 1500 bytes
  VCID  : 0x00000000
  Peer  : 0x00000000
  SCB   : 0x0AC609F9
  Channel: 0x00007ffffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
  VPN handle: 0x000000000000028d4
IPSEC: New outbound encrypt rule, SPI 0x8C14FD70
  Src addr: 172.16.1.2
  Src mask: 255.255.255.255
  Dst addr: 10.1.1.2
  Dst mask: 255.255.255.255
```

Src ports

Upper: 1701

Lower: 1701

Op : equal

Dst ports

Upper: 1701

Lower: 1701

Op : equal

Protocol: 17

```
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
Src addr: 172.16.1.2
Src mask: 255.255.255.255
Dst addr: 10.1.1.2
Dst mask: 255.255.255.255
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0x8C14FD70
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User () Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007ffffel13ab260,
SCB: 0xE1C00540,
Direction: inbound
SPI       : 0x7AD72E0D
Session ID: 0x00001000
VPIF num  : 0x00000002
Tunnel type: ra
Protocol   : esp
Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
Flags: 0x00000206
SA    : 0x00007ffffel13ab260
SPI   : 0x7AD72E0D
MTU   : 0 bytes
VCID  : 0x00000000
Peer  : 0x000028D4
SCB   : 0x0AC5BD5B
Channel: 0x00007ffffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
VPN handle: 0x00000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
Flags: 0x00000205
SA    : 0x00007ffffelc75c00
SPI   : 0x8C14FD70
MTU   : 1500 bytes
VCID  : 0x00000000
```

Peer : 0x00004174
SCB : 0x0AC609F9
Channel: 0x00007ffffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
VPN handle: 0x00000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
Rule ID: 0x00007ffffelc76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
Src addr: 10.1.1.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.2
Dst mask: 255.255.255.255
Src ports
Upper: 1701
Lower: 1701
Op : equal
Dst ports
Upper: 1701
Lower: 1701
Op : equal
Protocol: 17
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
Rule ID: 0x00007ffffel3aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
Src addr: 10.1.1.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.2
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x7AD72E0D
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
Rule ID: 0x00007ffffelc77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
Src addr: 10.1.1.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.2
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x7AD72E0D
Use SPI: true

IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D

Rule ID: 0x00007ffffe13abb80

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received KEY_UPDATE, spi 0x7ad72e0d

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer: 3420 seconds.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 2 COMPLETED

(msgid=00000001)

May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask <0xFFFFFFFF> port <1701>

May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1

In dieser Tabelle sind einige der häufig auftretenden VPN-bezogenen Fehler auf Windows-Clients aufgeführt.

Fehlercode	Mögliche Lösung
691	Stellen Sie sicher, dass Benutzername und Kennwort korrekt eingegeben wurden.
789.835	Stellen Sie sicher, dass der auf dem Client-Computer konfigurierte Pre-Shared Key mit dem der ASA identisch ist.
600	1. Stellen Sie sicher, dass der VPN-Typ auf "Layer 2 Tunneling Protocol (L2TP)" eingestellt ist. 2. Stellen Sie sicher, dass der vorinstallierte Schlüssel korrekt konfiguriert wurde.
809	Stellen Sie sicher, dass der UDP-Port 500 und 4500 (falls sich der Client oder Server hinter ein NAT-Gerät befindet) und der ESP-Datenverkehr nicht blockiert wurde.

Zugehörige Informationen

- [Cisco Adaptive Security Appliances der Serie ASA 5500](#)
- [Häufigste L2L- und IPsec-VPN-Lösungen zur Fehlerbehebung für Remote-Zugriff](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)