L2TP Over IPsec zwischen Windows 2000/XP PC und PIX/ASA 7.2 mithilfe eines Konfigurationsbeispiels für einen vorinstallierten Schlüssel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie das Layer 2 Tunneling Protocol (L2TP) über IP Security (IPsec) von Microsoft Windows 2000/2003- und XP-Remote-Clients in eine PIX Security Appliance-Geschäftsstelle mithilfe von vorinstallierten Schlüsseln mit Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS Server für die Benutzerauthentifizierung konfiguriert wird. Weitere Informationen finden Sie unter Microsoft - Checkliste: Konfiguration von IAS für Einwahl- und VPN-Zugriff für weitere Informationen zu IAS.

Der Hauptvorteil der Konfiguration von L2TP mit IPsec in einem Remote-Zugriffsszenario besteht darin, dass Remote-Benutzer über ein öffentliches IP-Netzwerk ohne Gateway oder dedizierte Leitung auf ein VPN zugreifen können. Dies ermöglicht Remote-Zugriff von praktisch jedem Ort mit POTS. Ein weiterer Vorteil ist, dass der einzige Client, der einen VPN-Zugriff benötigt, die Verwendung von Windows 2000 mit Microsoft Dial-Up Networking (DUN) ist. Es ist keine zusätzliche Client-Software erforderlich, z. B. die Cisco VPN Client-Software.

In diesem Dokument wird auch beschrieben, wie Sie den Cisco Adaptive Security Device Manager (ASDM) verwenden, um die Sicherheitslösung der Serie PIX 500 für L2TP über IPsec zu konfigurieren.

Hinweis: Layer 2 Tunneling Protocol (L2TP) über IPsec wird von der Cisco Secure PIX Firewall Software 6.x und höher unterstützt.

Informationen zum Konfigurieren von L2TP Over IPsec zwischen PIX 6.x und Windows 2000 finden Sie unter Konfigurieren von L2TP Over IPsec zwischen PIX Firewall und Windows 2000 PC mithilfe von Zertifikaten.

Informationen zum Konfigurieren von L2TP über IPsec von Microsoft Windows 2000- und XP-Remote-Clients zu einem Firmenstandort mithilfe einer verschlüsselten Methode finden Sie unter Konfigurieren von L2TP über IPsec von einem Windows 2000- oder XP-Client zu einem Cisco VPN-Konzentrator der Serie 300 mithilfe vorinstallierter Schlüssel.

Voraussetzungen

Anforderungen

Vor der Einrichtung eines sicheren Tunnels muss eine IP-Verbindung zwischen den Peers bestehen.

Stellen Sie sicher, dass der UDP-Port 1701 an keiner Stelle am Verbindungspfad blockiert wird.

Verwenden Sie auf der Cisco PIX/ASA nur die Standard-Tunnelgruppe und die Standard-Gruppenrichtlinie. Benutzerdefinierte Richtlinien und Gruppen funktionieren nicht.

Hinweis: Die Sicherheits-Appliance richtet keinen L2TP/IPsec-Tunnel mit Windows 2000 ein, wenn entweder Cisco VPN Client 3.x oder Cisco VPN 3000 Client 2.5 installiert ist. Deaktivieren Sie in Windows 2000 den Cisco VPN-Service für Cisco VPN Client 3.x oder den ANetIKE-Service für Cisco VPN 3000 Client 2.5 im Fenster Dienste. Wählen Sie dazu **Start > Programme > Verwaltung > Dienste aus**, starten Sie den IPsec Policy Agent Service im Fenster Dienste neu, und starten Sie den Computer neu.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- PIX Security Appliance 515E mit Softwareversion 7.2(1) oder höher
- Adaptive Security Device Manager 5.2(1) oder höher
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional mit SP2

- Windows 2003 Server mit IAS

Hinweis: Wenn Sie ein Upgrade von PIX 6.3 auf Version 7.x durchführen, stellen Sie sicher, dass Sie SP2 in Windows XP (L2TP-Client) installiert haben.

Hinweis: Die Informationen im Dokument gelten auch für die ASA Security Appliance.

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Verwandte Produkte

Diese Konfiguration kann auch mit Cisco Security Appliances der Serie ASA 5500 7.2(1) oder höher verwendet werden.

Konventionen

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

Hintergrundinformationen

Führen Sie diese Schritte aus, um L2TP über IPsec zu konfigurieren.

1. Konfigurieren Sie den IPsec-Transportmodus, um IPsec mit L2TP zu aktivieren.Der Windows 2000 L2TP/IPsec-Client verwendet den IPsec-Transportmodus - Nur die IP-Nutzlast wird verschlüsselt, und die ursprünglichen IP-Header bleiben intakt. Der Vorteil dieses Modus besteht darin, dass jedem Paket nur wenige Byte hinzugefügt werden und Geräte im öffentlichen Netzwerk die endgültige Quelle und das Ziel des Pakets sehen können. Damit Windows 2000 L2TP/IPsec-Clients eine Verbindung zur Sicherheits-Appliance herstellen können, müssen Sie den IPsec-Transportmodus für eine Transformation konfigurieren (siehe Schritt 2 in der ASDM-Konfiguration). Mit dieser Funktion (Transport) können Sie auf Basis der Informationen im IP-Header eine spezielle Verarbeitung (z. B. QoS) im zwischengeschalteten Netzwerk aktivieren. Der Layer-4-Header ist jedoch verschlüsselt, wodurch die Paketprüfung eingeschränkt wird. Leider ermöglicht die Übertragung des IP-Headers im Klartext, im Transportmodus, einem Angreifer, einige Datenverkehrsanalysen durchzuführen.
2. Konfigurieren Sie L2TP mit einer VPDN-Gruppe (Virtual Private Dial-up Network).

Die Konfiguration von L2TP mit IPsec unterstützt Zertifikate, die die vorinstallierten Schlüssel oder RSA-Signaturmethoden verwenden, sowie die Verwendung dynamischer (im Gegensatz zu statischen) Kryptozuordnungen. Der vorinstallierte Schlüssel dient als Authentifizierung zum Einrichten des L2TP über IPsec-Tunnel.

Konfiguration

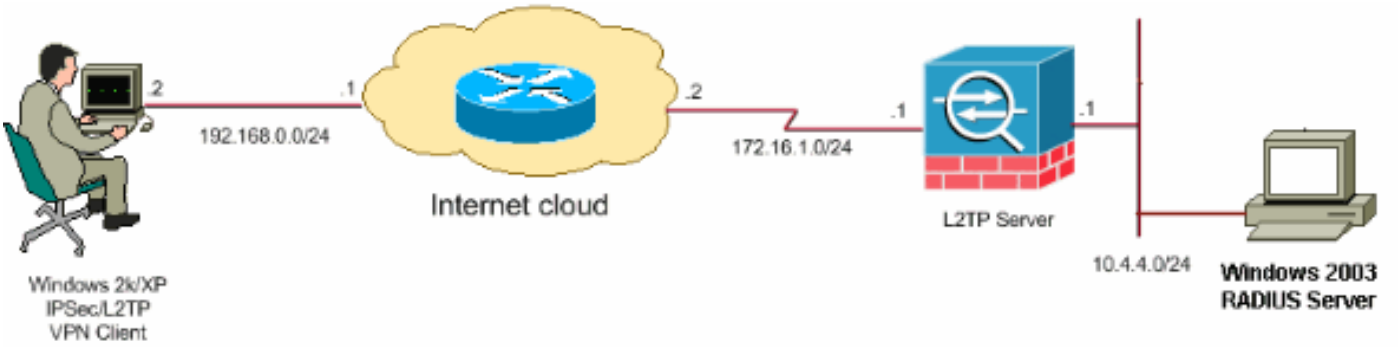
In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

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

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Windows-Client-Konfiguration für L2TP/IPsec
- L2TP-Server in PIX-Konfiguration
- L2TP mithilfe der ASDM-Konfiguration
- Microsoft Windows 2003 Server mit IAS-Konfiguration

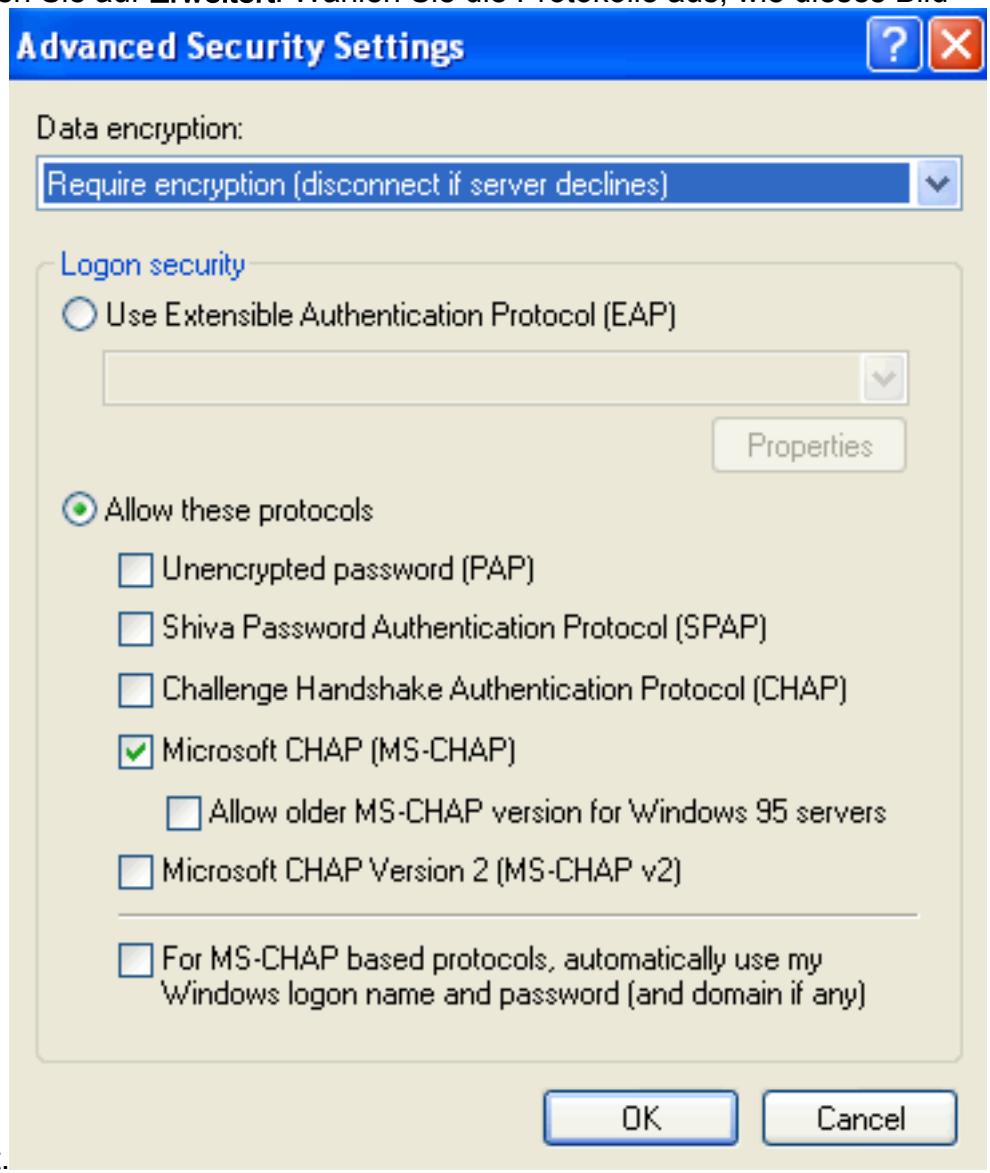
Windows-Client-Konfiguration für L2TP/IPsec

Führen Sie diese Schritte aus, um L2TP über IPsec unter Windows 2000 zu konfigurieren. Überspringen Sie in Windows XP die Schritte 1 und 2 und beginnen Sie von Schritt 3:

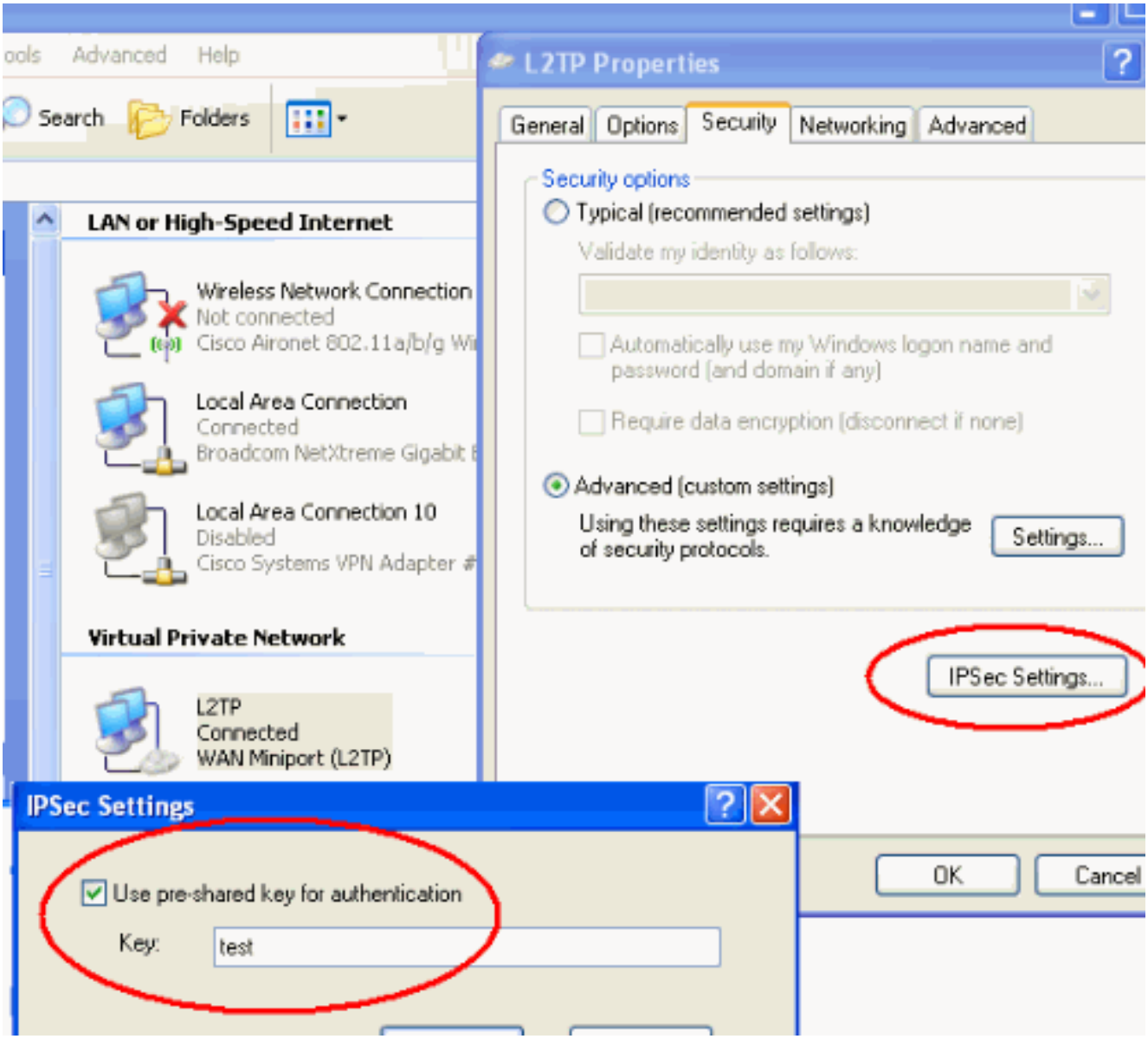
1. Fügen Sie diesen Registrierungswert Ihrem Windows 2000-Computer hinzu:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`
2. Fügen Sie diesem Schlüssel diesen Registrierungswert hinzu:
   ```
   Value Name: ProhibitIpSec
   Data Type: REG_DWORD
   Value: 1
   ```
   Hinweis: In einigen Fällen (Windows XP SP2), die Addition dieses Schlüssels **(Wert: 1)** scheint die Verbindung zu unterbrechen, da es das XP-Feld veranlasst, nur L2TP auszuhandeln und nicht ein L2TP mit IPsec-Verbindung. Es ist obligatorisch, eine IPsec-Richtlinie in Verbindung mit diesem Registrierungsschlüssel hinzuzufügen. Wenn Sie beim Herstellen einer Verbindung den `Fehler 800` erhalten, entfernen Sie den Schlüssel (Wert: 1), um die Verbindung zur Arbeit herzustellen.**Hinweis:** Sie müssen den Windows 2000/2003- oder XP-Computer neu starten, damit die Änderungen wirksam werden. Standardmäßig versucht der Windows-Client, IPsec mit einer Zertifizierungsstelle (Certificate Authority, CA)

zu verwenden. Die Konfiguration dieses Registrierungsschlüssels verhindert, dass dies geschieht. Jetzt können Sie eine IPsec-Richtlinie auf der Windows-Station so konfigurieren, dass sie mit den Parametern übereinstimmt, die Sie auf dem PIX/ASA wünschen. Unter Konfigurieren einer L2TP/IPSec-Verbindung mithilfe der Authentifizierung mit vorinstalliertem Schlüssel (Q240262) finden Sie eine schrittweise Konfiguration der Windows-IPsec-Richtlinie.Weitere Informationen finden Sie unter Konfigurieren eines vorinstallierten Schlüssels für die Verwendung mit Layer-2-Tunneling-Protokollverbindungen in Windows XP (Q281555)\ .

3. Erstellen Sie Ihre Verbindung.
4. Klicken Sie unter Netzwerk- und DFÜ-Verbindungen mit der rechten Maustaste auf die Verbindung, und wählen Sie **Eigenschaften aus**.Öffnen Sie die Registerkarte Sicherheit, und klicken Sie auf **Erweitert**. Wählen Sie die Protokolle aus, wie dieses Bild zeigt.



5. **Hinweis:** Dieser Schritt gilt nur für Windows XP.Klicken Sie auf **IPSec-Einstellungen**, aktivieren Sie **Pre-shared Key für Authentifizierung verwenden** und geben Sie den Pre-Shared Key ein, um den Pre-Shared Key festzulegen.In diesem Beispiel wird der Test als vorinstallierter Schlüssel
verwendet.



L2TP-Server in PIX-Konfiguration

PIX 7.2

```
pixfirewall#show run

PIX Version 7.2(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside and inside interfaces.
interface Ethernet0 nameif outside security-level 0 ip
address 172.16.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0
nat (inside) 0 access-list nonat

pager lines 24
```

```
logging console debugging
mtu outside 1500
mtu inside 1500

!--- Creates a pool of addresses from which IP addresses
are assigned !--- dynamically to the remote VPN Clients.
ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0

no failover
asdm image flash:/asdm-521.bin
no asdm history enable
arp timeout 14400

!--- The global and nat command enable !--- the Port
Address Translation (PAT) using an outside interface IP
!--- address for all outgoing traffic.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0


route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute

!--- Create the AAA server group "vpn" and specify its
protocol as RADIUS. !--- Specify the IAS server as a
member of the "vpn" group and provide its !--- location
and key. aaa-server vpn protocol radius
aaa-server vpn host 10.4.4.2
 key radiuskey

!--- Identifies the group policy as internal. group-
policy DefaultRAGroup internal
!--- Instructs the security appliance to send DNS and !-
-- WINS server IP addresses to the client. group-policy
DefaultRAGroup attributes
 wins-server value 10.4.4.99
 dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec
 default-domain value cisco.com
!--- Configure usernames and passwords on the device !--
- in addition to using AAA. !--- If the user is an L2TP
client that uses Microsoft CHAP version 1 or !---
version 2, and the security appliance is configured !---
to authenticate against the local !--- database, you
must include the mschap keyword. !--- For example,
username



          .


username test password DLaUiAX3178qgoB5c7iVNw== nt-
```

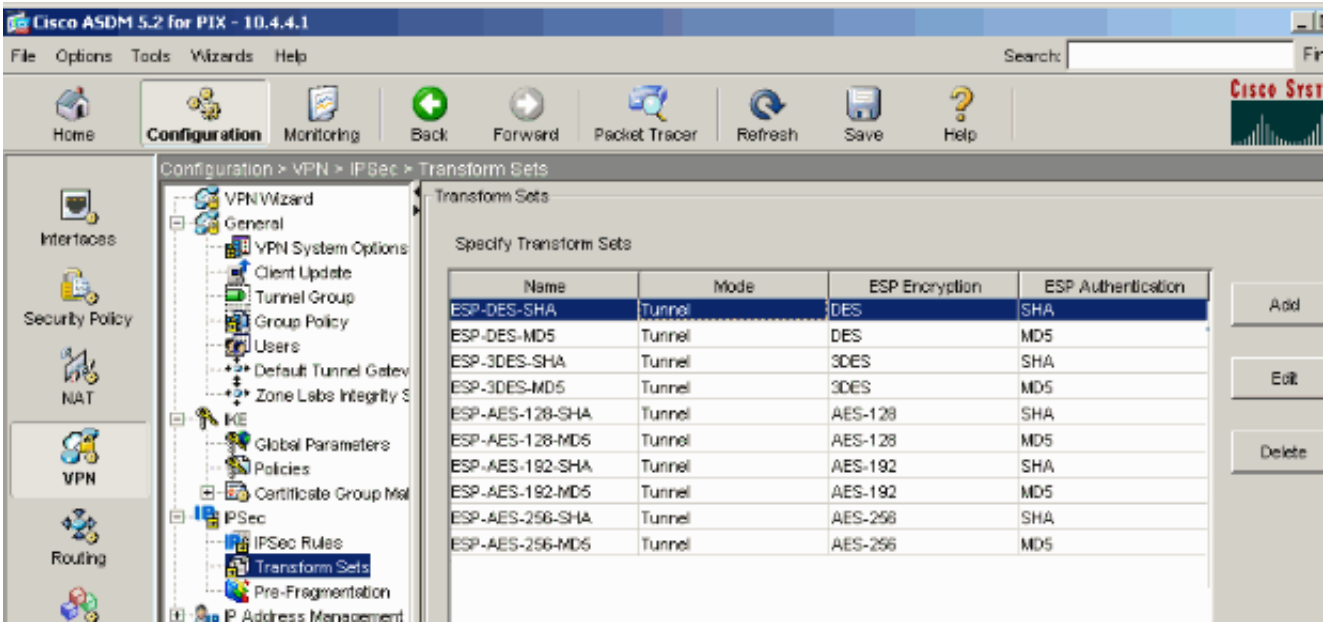
```
encrypted


 vpn-tunnel-protocol l2tp-ipsec

http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

!--- Identifies the IPsec encryption and hash algorithms
!--- to be used by the transform set. crypto ipsec
transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac

!--- Since the Windows 2000 L2TP/IPsec client uses IPsec
transport mode, !--- set the mode to transport. !--- The
default is tunnel mode. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 mode transport




!--- Specifies the transform sets to use in a dynamic
crypto map entry. crypto dynamic-map outside_dyn_map 20
set transform-set TRANS_ESP_3DES_MD5

!--- Requires a given crypto map entry to refer to a
pre-existing !--- dynamic crypto map. crypto map
outside_map 20 ipsec-isakmp dynamic outside_dyn_map

!--- Applies a previously defined crypto map set to an
outside interface. crypto map outside_map interface
outside

crypto isakmp enable outside
crypto isakmp nat-traversal 20

!--- Specifies the IKE Phase I policy parameters. crypto
isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400

!--- Creates a tunnel group with the tunnel-group
command, and specifies the local !--- address pool name
used to allocate the IP address to the client. !---
Associate the AAA server group (VPN) with the tunnel
group.


tunnel-group DefaultRAGroup general-attributes
 address-pool clientVPNpool
 authentication-server-group vpn

!--- Link the name of the group policy to the default
tunnel !--- group from tunnel group general-attributes
mode. default-group-policy DefaultRAGroup

!--- Use the tunnel-group ipsec-attributes command !---
in order to enter the ipsec-attribute configuration
```

```
mode. !--- Set the pre-shared key. !--- This key should
be the same as the key configured on the Windows
machine.


tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key *

!--- Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode.


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

telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:e1e0730fa260244caa2e2784f632accd
: end
```

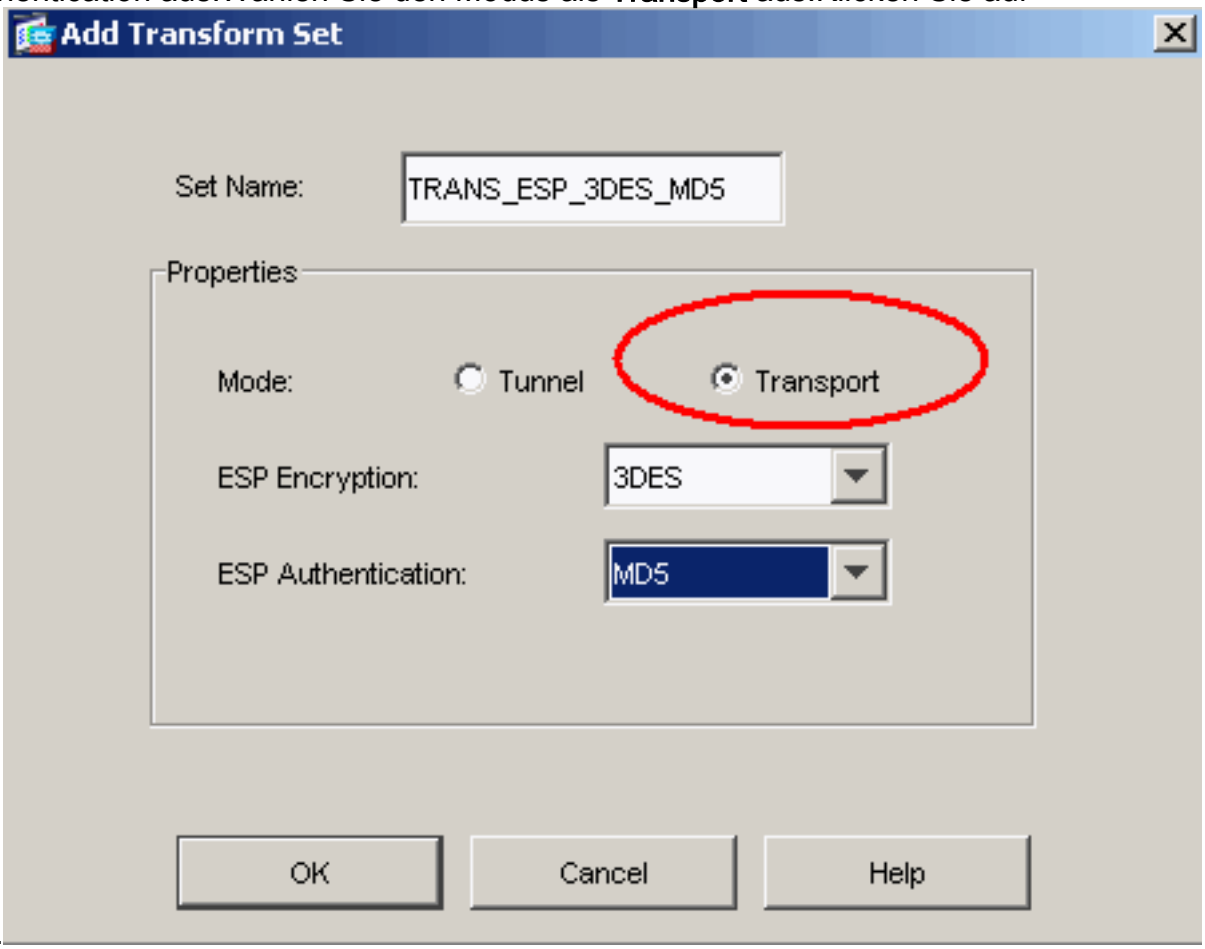
L2TP mithilfe der ASDM-Konfiguration

Gehen Sie wie folgt vor, um die Sicherheits-Appliance so zu konfigurieren, dass sie L2TP-over-IPsec-Verbindungen akzeptiert:

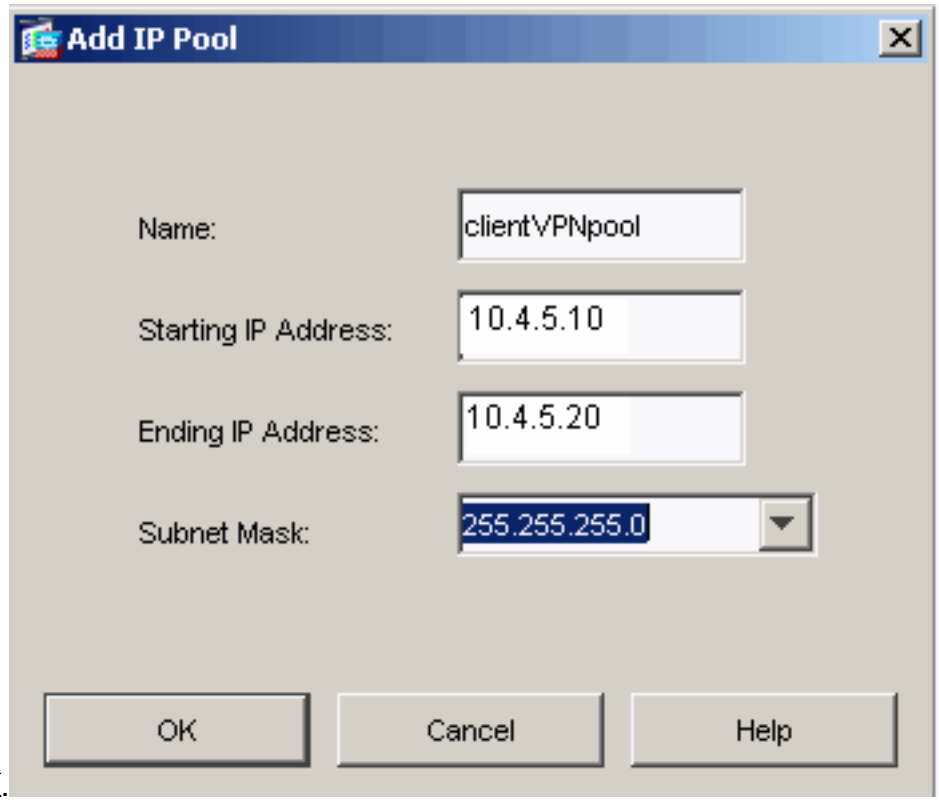
1. Fügen Sie einen IPsec-Transformationssatz hinzu, und geben Sie IPsec für die Verwendung des Transportmodus statt des Tunnelmodus an. Wählen Sie dazu **Configuration > VPN > IPSec > Transform Sets** aus, **und** klicken Sie auf **Add**. Der Bereich "Transform Sets" wird angezeigt.



2. Gehen Sie wie folgt vor, um einen Transformationssatz hinzuzufügen:Geben Sie einen Namen für den Transformationssatz ein.Wählen Sie die Methoden ESP Encryption und ESP Authentication aus.Wählen Sie den Modus als **Transport** aus.Klicken Sie auf **OK**.

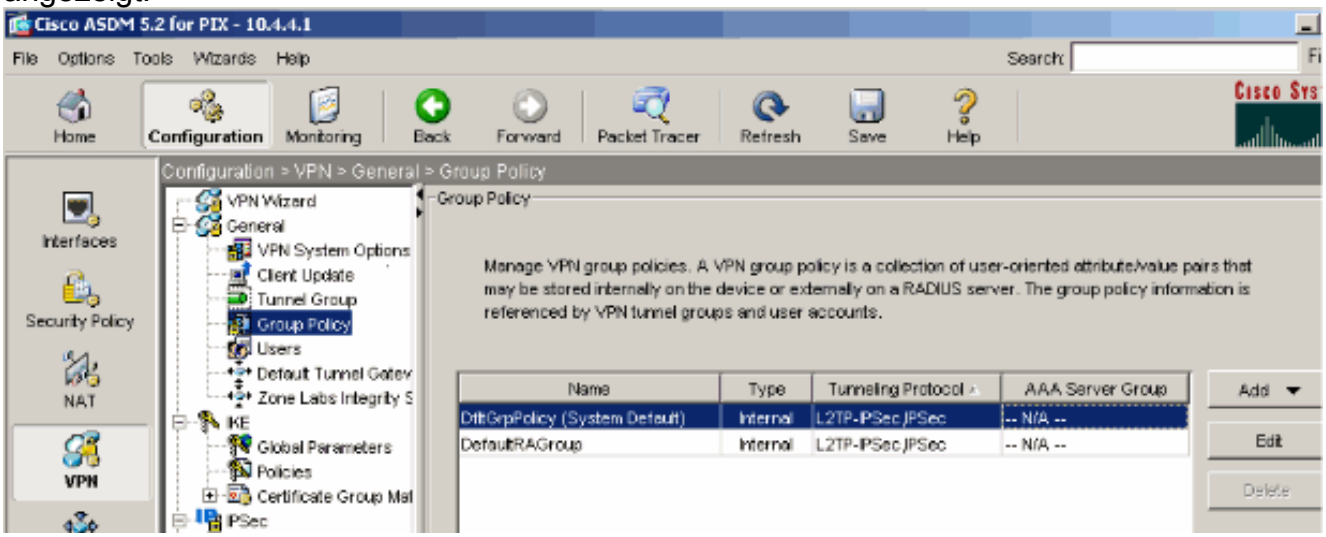


3. Führen Sie diese Schritte aus, um eine Methode für die Adresszuweisung zu konfigurieren. In diesem Beispiel werden IP-Adressen-Pools verwendet.Wählen Sie **Configuration > VPN > IP Address Management > IP Pools aus**.Klicken Sie auf **Hinzufügen**. Das Dialogfeld "IP-Pool hinzufügen" wird angezeigt.Geben Sie den Namen des neuen IP-Adresspools ein.Geben Sie die Start- und End-IP-Adressen ein.Geben Sie die Subnetzmaske ein, und klicken Sie auf

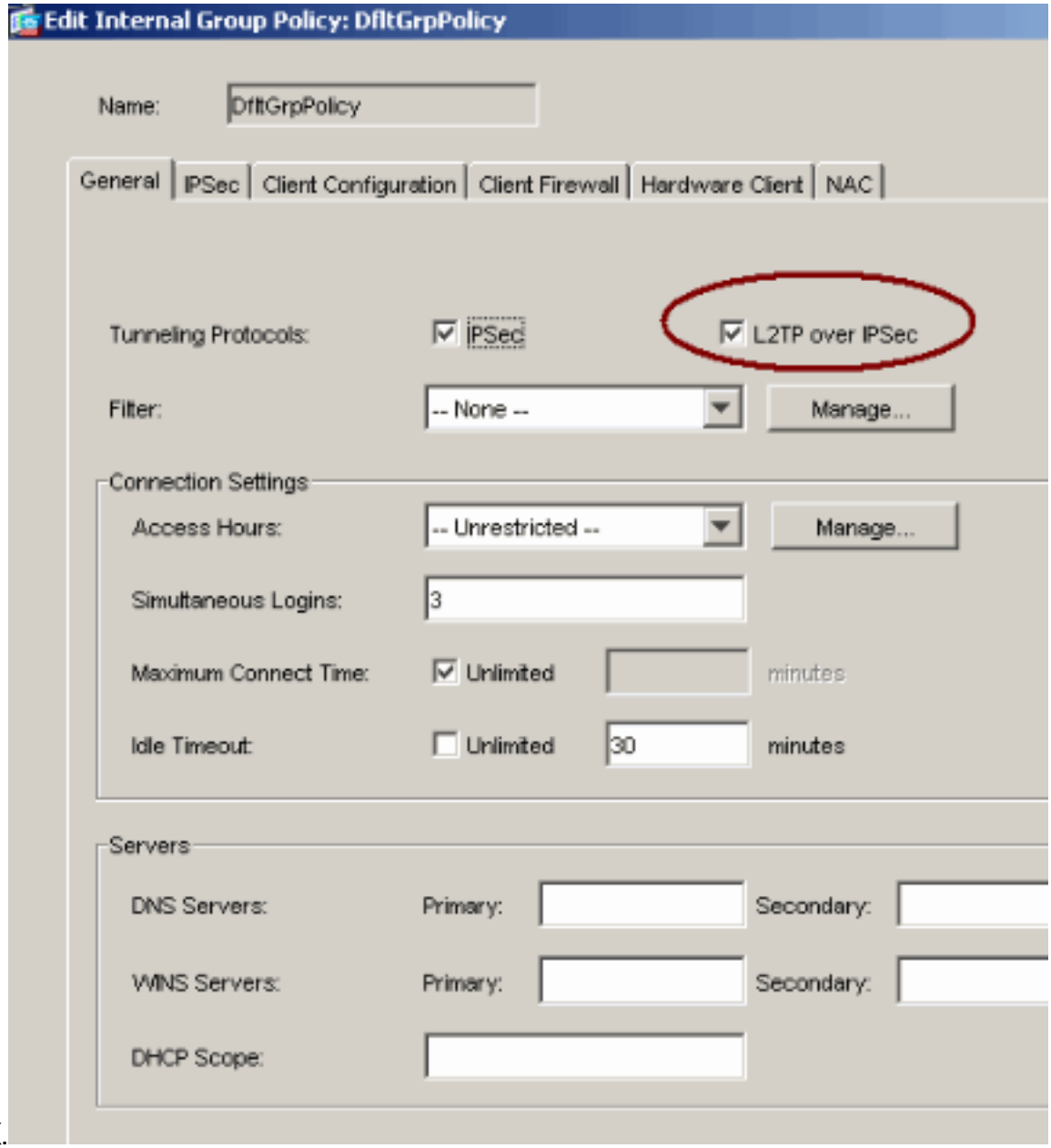


OK.

4. Wählen Sie **Configuration > VPN > General > Group Policy (Konfiguration > VPN > Allgemein > Gruppenrichtlinie)**, um L2TP over IPsec als gültiges VPN-Tunneling-Protokoll für die Gruppenrichtlinie zu konfigurieren. Der Bereich "Gruppenrichtlinie" wird angezeigt.

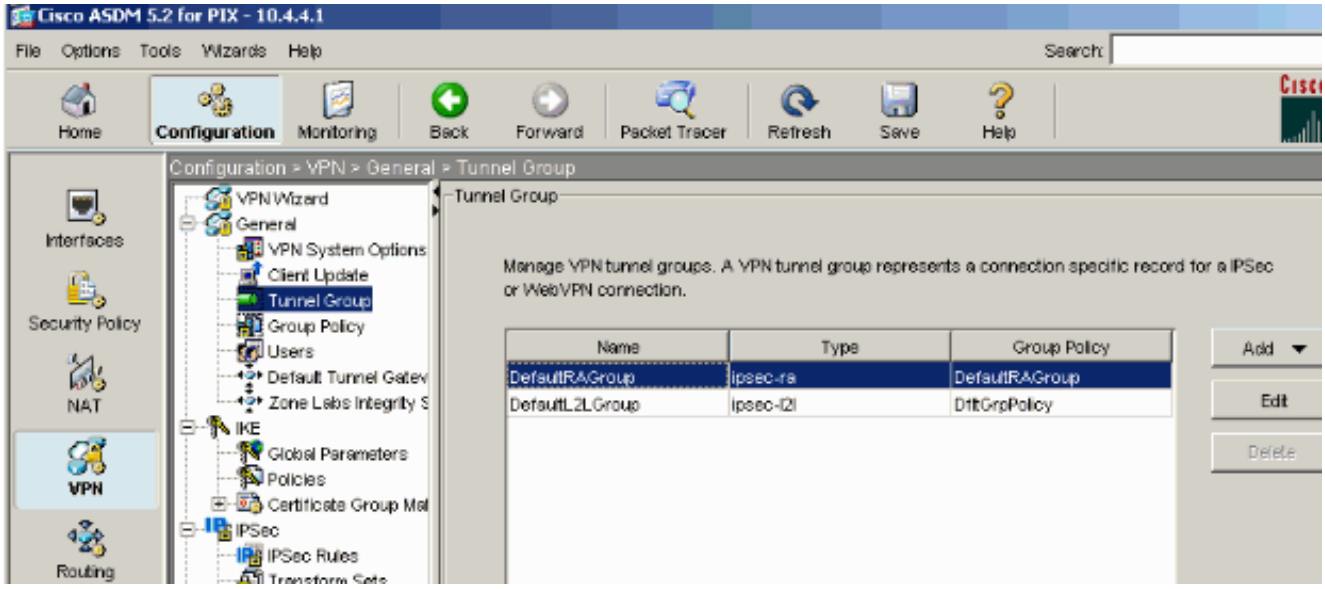


5. Wählen Sie eine Gruppenrichtlinie (DiffGrpPolicy) aus, und klicken Sie auf **Bearbeiten**.Das Dialogfeld "Gruppenrichtlinie bearbeiten" wird angezeigt. Aktivieren Sie **L2TP über IPSec**, um das Protokoll für die Gruppenrichtlinie zu aktivieren, und klicken Sie dann auf

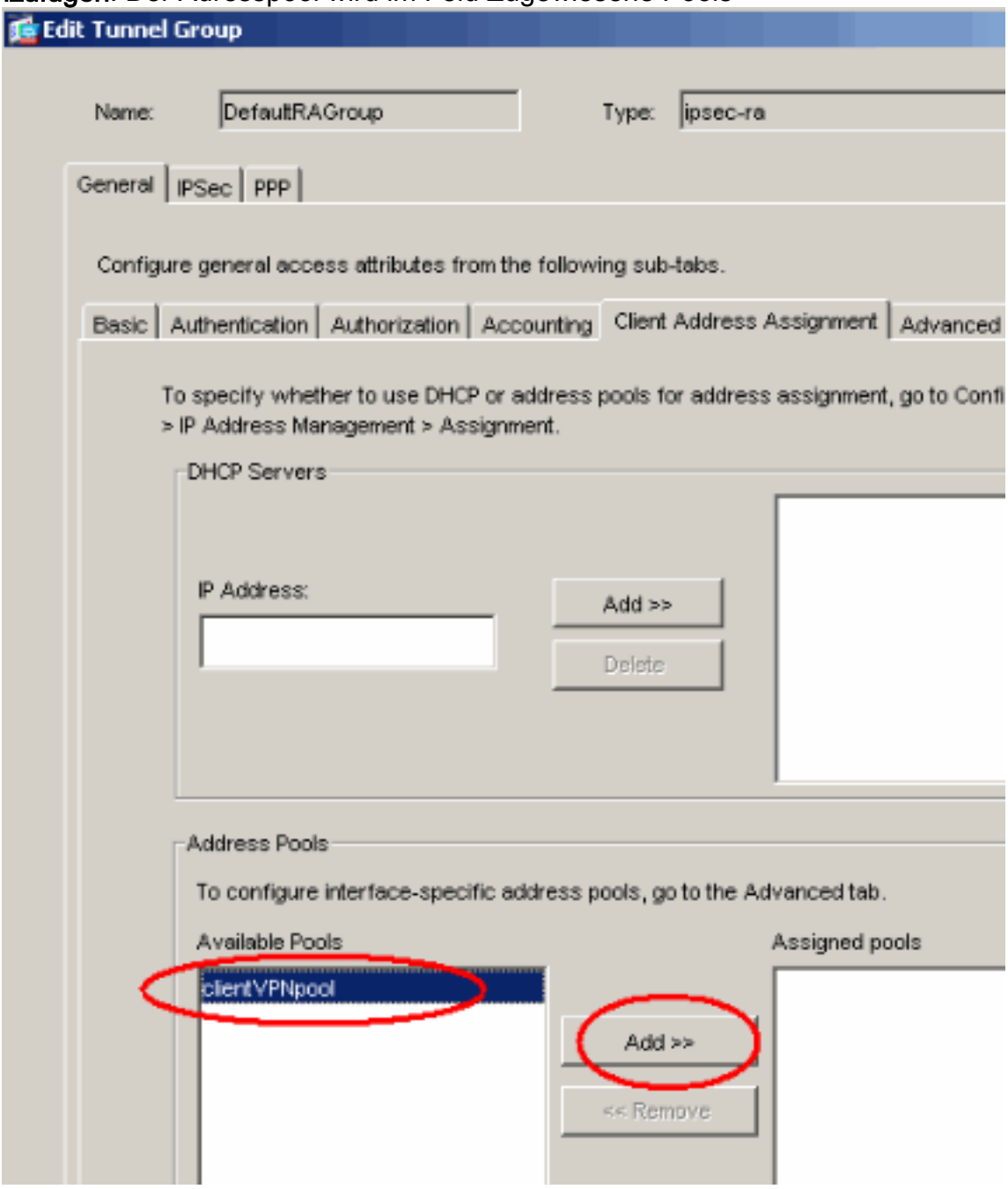


OK.

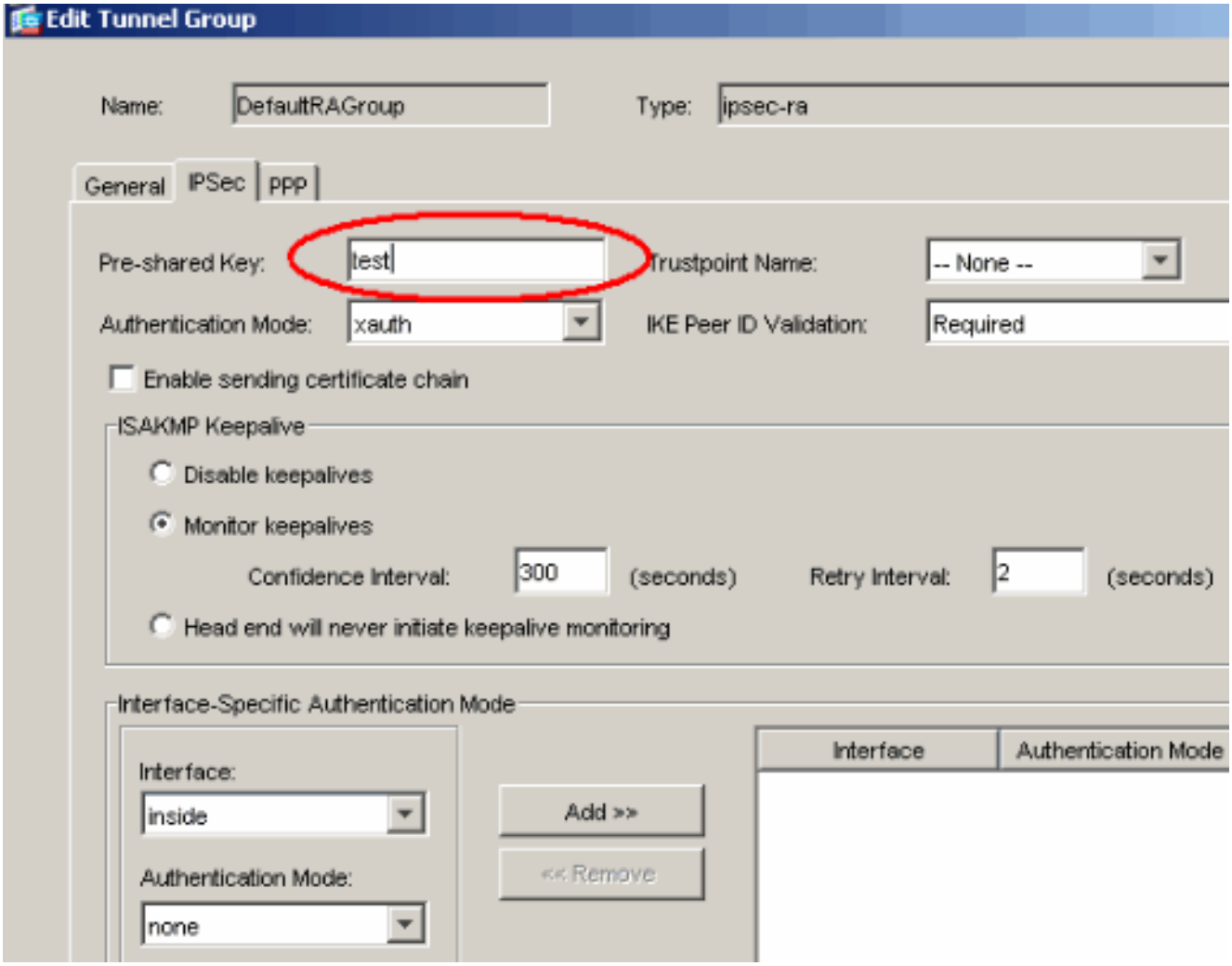
6. Gehen Sie wie folgt vor, um den IP-Adresspool einer Tunnelgruppe zuzuweisen:Wählen Sie **Configuration > VPN > General > Tunnel Group (Konfiguration > VPN > Allgemein > Tunnelgruppe)**.Wenn der Bereich "Tunnelgruppe" angezeigt wird, wählen Sie in der Tabelle eine Tunnelgruppe (DefaultRAGroup) aus.Klicken Sie auf **Bearbeiten**.



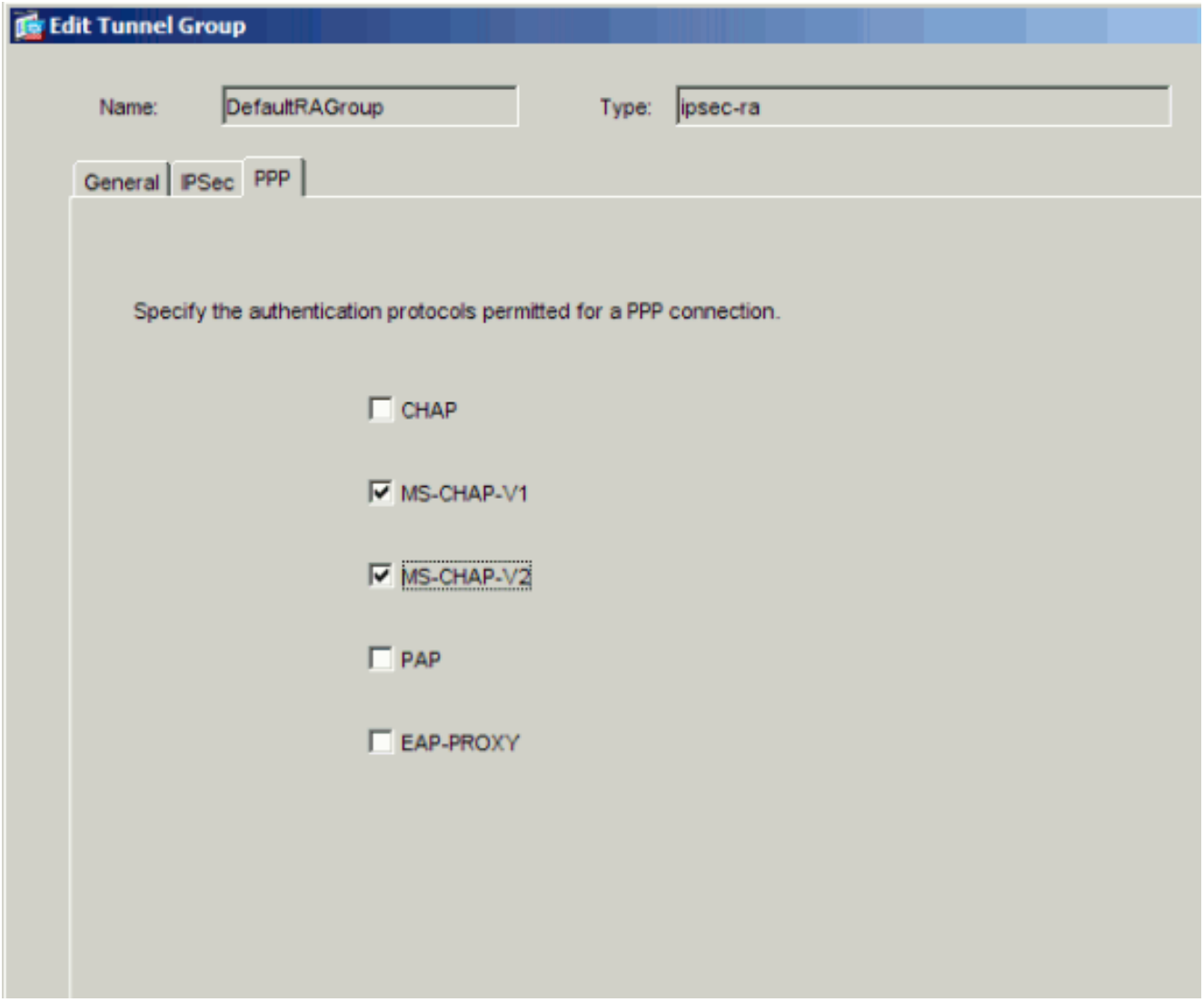
7. Gehen Sie wie folgt vor, wenn das Fenster "Edit Tunnel Group" (Tunnelgruppe bearbeiten) angezeigt wird:Klicken Sie auf der Registerkarte Allgemein auf die Registerkarte Client Address Assignment (Client-Adressenzuweisung).Wählen Sie im Bereich "Address Pools" (Adresspools) einen Adresspool aus, der der Tunnelgruppe zugewiesen werden soll.Klicken Sie auf **Hinzufügen**. Der Adresspool wird im Feld Zugewiesene Pools angezeigt.



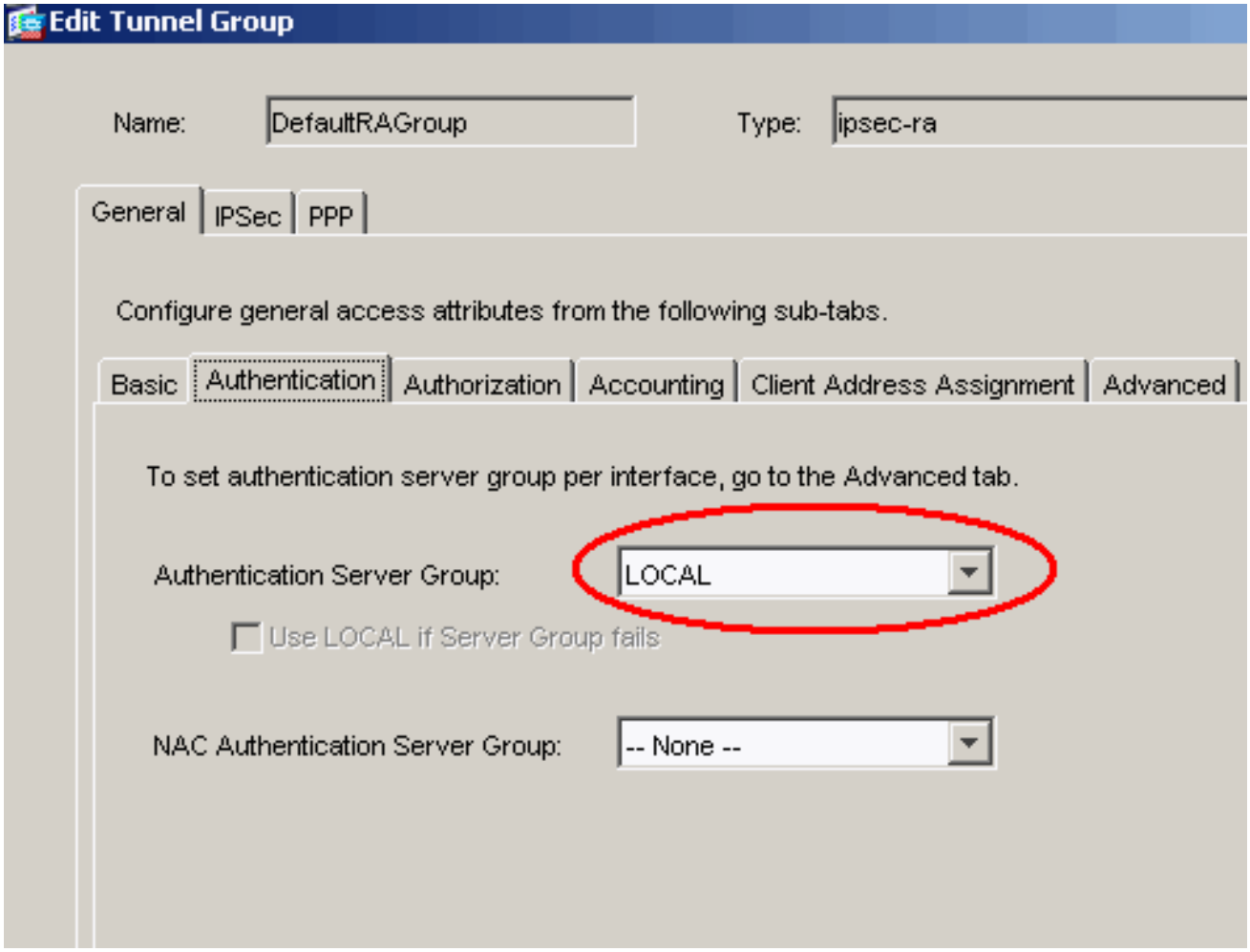
8. Um den Pre-Shared Key festzulegen, gehen Sie zur Registerkarte IPSec, geben Sie Ihren **Pre-shared Key ein** und klicken Sie auf **OK**.



9. L2TP über IPsec verwendet PPP-Authentifizierungsprotokolle. Geben Sie auf der PPP-Registerkarte der Tunnelgruppe die Protokolle an, die für PPP-Verbindungen zulässig sind. Wählen Sie zur Authentifizierung das **MS-CHAP-V1**-Protokoll
aus.



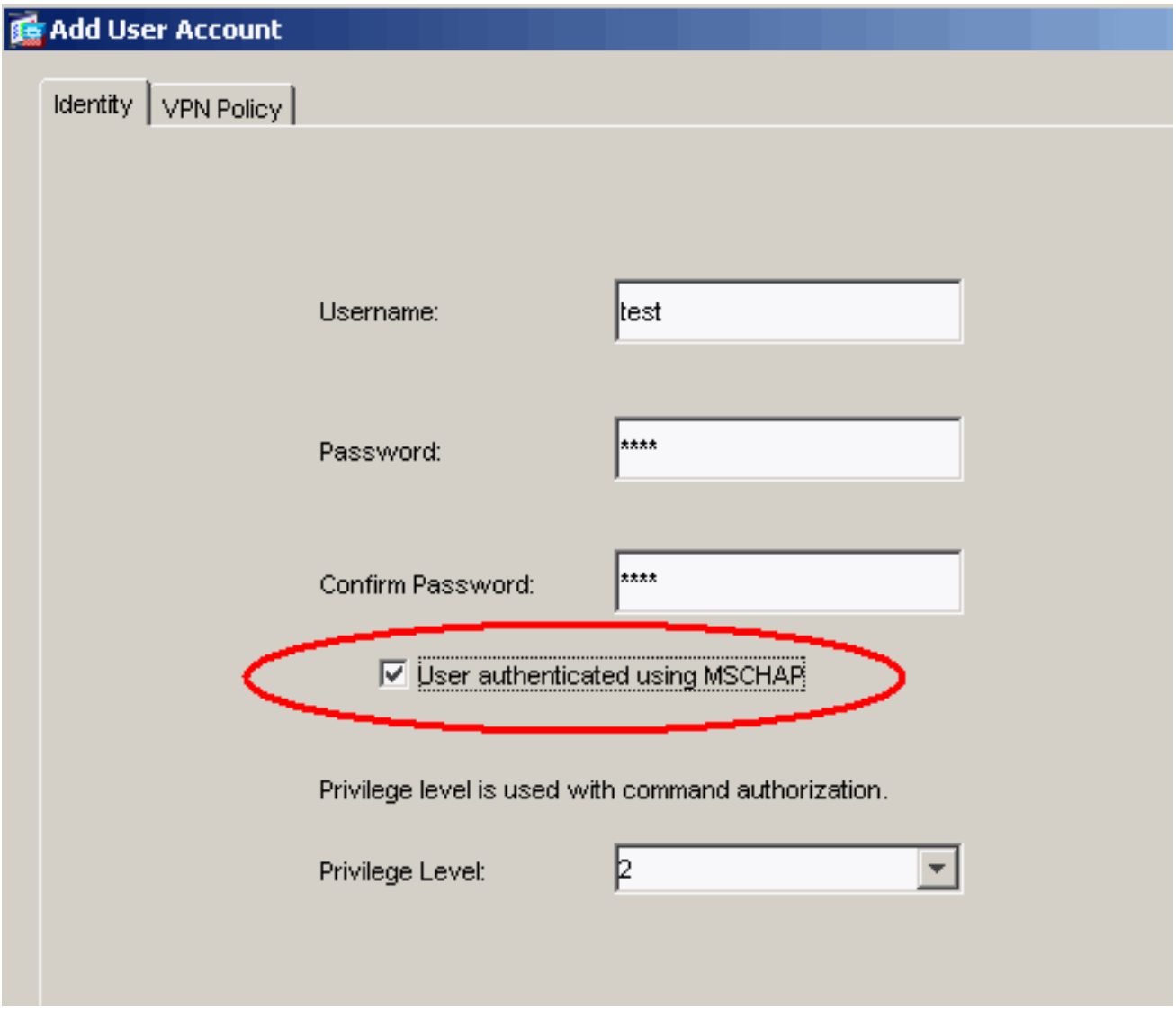
10. Geben Sie eine Methode zum Authentifizieren von Benutzern an, die L2TP über IPsec-Verbindungen versuchen.Sie können die Sicherheits-Appliance so konfigurieren, dass sie einen Authentifizierungsserver oder eine eigene lokale Datenbank verwendet. Gehen Sie dazu zur Registerkarte Authentifizierung der Tunnelgruppe. Die Sicherheits-Appliance verwendet standardmäßig ihre lokale Datenbank. Die Dropdown-Liste "Authentication Server Group" (Authentifizierungsserver-Gruppe) zeigt LOCAL an. Um einen Authentifizierungsserver zu verwenden, wählen Sie einen aus der Liste aus.**Hinweis:** Die Sicherheits-Appliance unterstützt nur die PPP-Authentifizierungen PAP und Microsoft CHAP Version 1 und 2 in der lokalen Datenbank. EAP und CHAP werden von Proxy-Authentifizierungsservern durchgeführt. Wenn ein Remote-Benutzer einer Tunnelgruppe angehört, die mit EAP oder CHAP konfiguriert ist, und die Sicherheits-Appliance für die Verwendung der lokalen Datenbank konfiguriert ist, kann dieser Benutzer keine Verbindung herstellen.



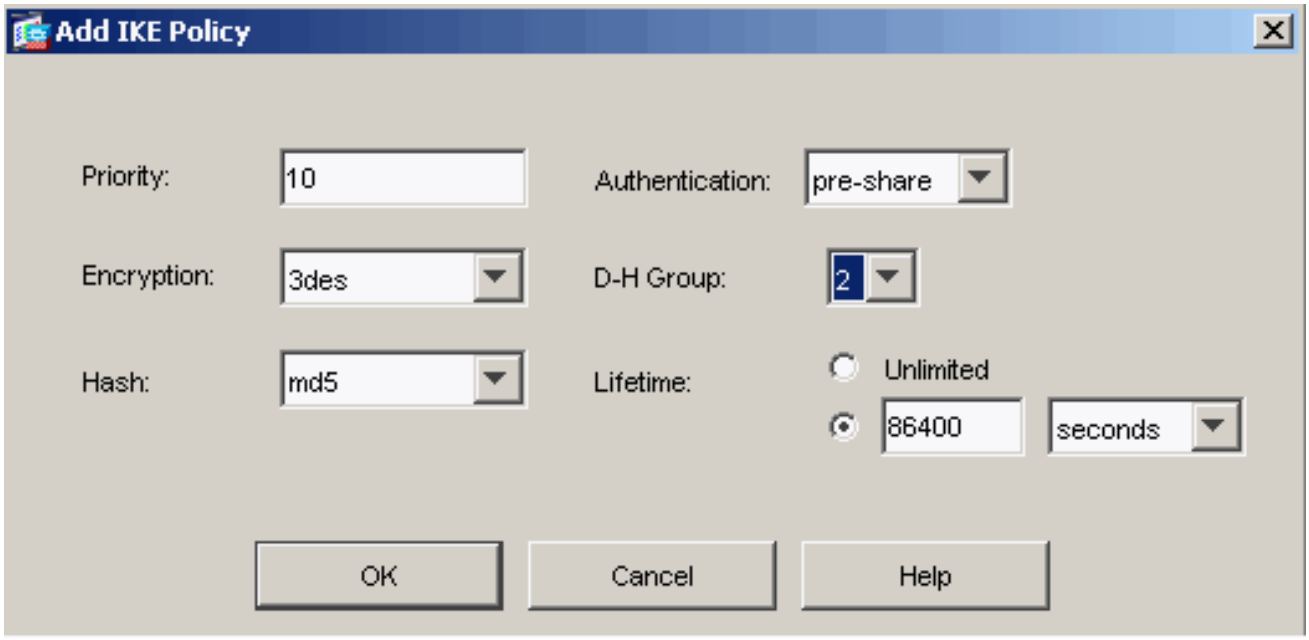
Hinweis: Wählen Sie **Configuration > VPN > General > Tunnel Group (Konfiguration > VPN > Allgemein > Tunnel-Gruppe** aus, um zur Tunnelgruppenkonfiguration zurückzukehren, sodass Sie die Gruppenrichtlinie mit der Tunnelgruppe verknüpfen und Tunnelgruppen-Switching aktivieren können (optional). Wenn das Fenster Tunnelgruppe angezeigt wird, wählen Sie die Tunnelgruppe aus, und klicken Sie auf **Bearbeiten**.**Hinweis:** Mit Tunnelgruppen-Switching kann die Sicherheits-Appliance verschiedene Benutzer zuordnen, die L2TP über IPsec-Verbindungen mit verschiedenen Tunnelgruppen herstellen. Da jede Tunnelgruppe über eine eigene AAA-Servergruppe und IP-Adresspools verfügt, können Benutzer mithilfe von Methoden authentifiziert werden, die für ihre Tunnelgruppe spezifisch sind. Anstatt nur einen Benutzernamen zu senden, sendet der Benutzer einen Benutzernamen und einen Gruppennamen im Format username@group_name. "@" steht für ein Trennzeichen, das Sie konfigurieren können, und der Gruppenname ist der Name einer Tunnelgruppe, die auf der Sicherheits-Appliance konfiguriert ist.**Hinweis:** Die Tunnelgruppen-Switching-Funktion wird durch die Verarbeitung von Strip-Gruppen aktiviert. Dadurch kann die Sicherheits-Appliance die Tunnelgruppe für Benutzerverbindungen auswählen, indem sie den Gruppennamen aus dem vom VPN-Client angegebenen Benutzernamen abruft. Die Sicherheits-Appliance sendet dann nur den Benutzerteil des Benutzernamens zur Autorisierung und Authentifizierung. Andernfalls (wenn deaktiviert) sendet die Sicherheits-Appliance den gesamten Benutzernamen, einschließlich des Bereichs. Um die Tunnelgruppen-Switching zu aktivieren, aktivieren Sie **die** Option **Bereich vom Benutzernamen entfernen, bevor Sie ihn an den AAA-Server weiterleiten**, und aktivieren Sie **die Option Gruppe aus Benutzernamen entfernen, bevor Sie sie an den AAA-Server weiterleiten**. Klicken Sie anschließend auf **OK**.

11. Gehen Sie wie folgt vor, um einen Benutzer in der lokalen Datenbank zu erstellen:Wählen

Sie **Konfiguration > Eigenschaften > Geräteverwaltung > Benutzerkonten aus**.Klicken Sie auf **Hinzufügen**.Wenn der Benutzer ein L2TP-Client ist, der Microsoft CHAP-Version 1 oder 2 verwendet und die Sicherheits-Appliance für die Authentifizierung über die lokale Datenbank konfiguriert ist, müssen Sie **User Authenticated using MSCHAP** aktivieren, um die MSCHAP zu aktivieren.Klicken Sie auf
OK.



12. Wählen Sie **Configuration > VPN > IKE > Policies (Konfiguration > VPN > IKE > Richtlinien) aus,** und klicken Sie auf **Add**, um eine IKE-Richtlinie für Phase I zu erstellen. Klicken Sie auf **OK**, um
fortzufahren.



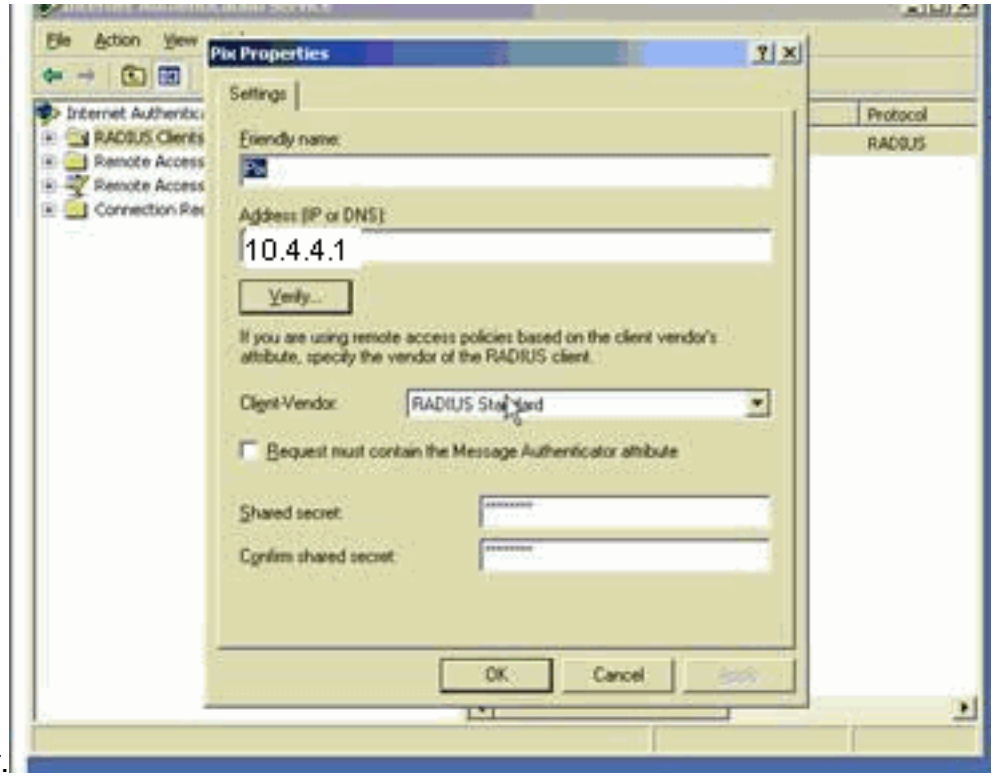
13. (Optional) Wenn Sie erwarten, dass mehrere L2TP-Clients hinter einem NAT-Gerät L2TP über IPsec-Verbindungen zur Sicherheits-Appliance herstellen, müssen Sie NAT-Traversal aktivieren, damit ESP-Pakete ein oder mehrere NAT-Geräte durchlaufen können. Gehen Sie wie folgt vor, um dies zu tun:Wählen Sie **Configuration > VPN > IKE > Global Parameters (Konfiguration > VPN > IKE > Globale Parameter)**.Stellen Sie sicher, dass **ISAKMP** auf einer Schnittstelle aktiviert ist.Aktivieren Sie **IPSec über NAT-T aktivieren**.Klicken Sie auf **OK**.

Microsoft Windows 2003 Server mit IAS-Konfiguration

Führen Sie diese Schritte aus, um den Microsoft Windows 2003-Server mit IAS zu konfigurieren.

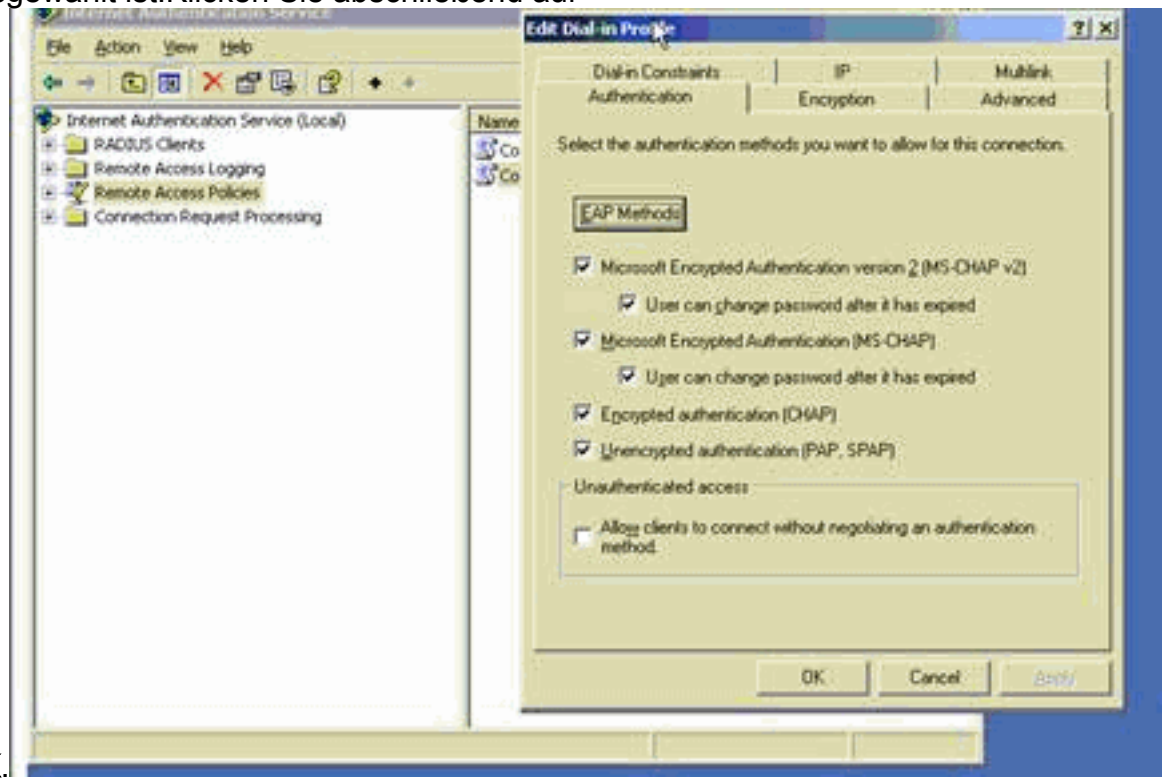
Hinweis: Bei diesen Schritten wird davon ausgegangen, dass IAS bereits auf dem lokalen Computer installiert ist. Falls nicht, fügen Sie dies über **Systemsteuerung > Software hinzu**.

1. Wählen Sie **Verwaltung > Internet Authentication Service** und klicken Sie mit der rechten Maustaste auf **RADIUS Client**, um einen neuen RADIUS-Client hinzuzufügen. Nachdem Sie die Clientinformationen eingegeben haben, klicken Sie auf **OK**.Dieses Beispiel zeigt einen Client mit dem Namen "Pix" und einer IP-Adresse von 10.4.4.1. Der Client-Anbieter ist auf **RADIUS-Standard** festgelegt, und der gemeinsame geheime Schlüssel ist



radiuskey.

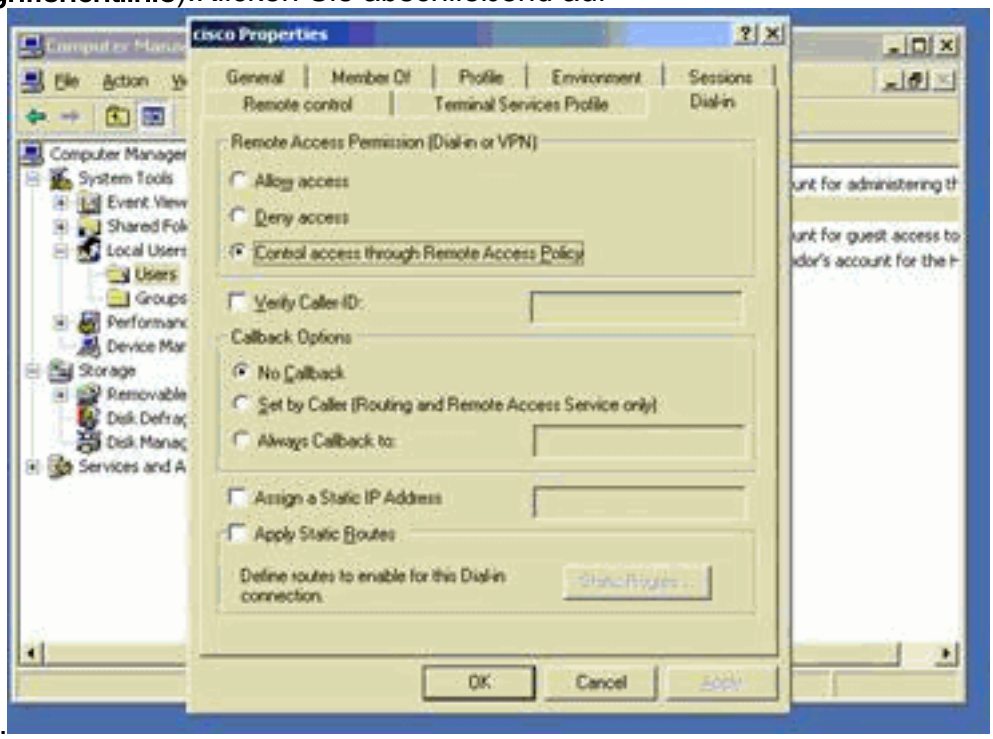
2. Wählen Sie **Remotezugriffsrichtlinien aus**, klicken Sie mit der rechten Maustaste auf **Verbindungen zu anderen Zugriffsservern**, und wählen Sie **Eigenschaften aus**.
3. Stellen Sie sicher, dass die Option **Remote-Zugriffsberechtigungen erteilen** aktiviert ist.
4. Klicken Sie auf **Profil bearbeiten**, und überprüfen Sie diese Einstellungen:Aktivieren Sie auf der Registerkarte Authentifizierung die Option **Uncrypted Authentication (PAP, SPAP)**.Stellen Sie sicher, dass auf der Registerkarte Verschlüsselung die Option **Keine Verschlüsselung** ausgewählt ist.Klicken Sie abschließend auf



OK.

5. Wählen Sie **Verwaltung > Computerverwaltung > Systemprogramme > Lokale Benutzer und Gruppen**, klicken Sie mit der rechten Maustaste auf **Benutzer** und wählen Sie **Neue Benutzer**, um dem lokalen Computerkonto einen Benutzer hinzuzufügen.
6. Fügen Sie einen Benutzer mit dem Cisco Kennwort **password1 hinzu**, und überprüfen Sie die

Profilinformationen:Stellen Sie auf der Registerkarte Allgemein sicher, dass die Option **Kennwort nie abgelaufen** anstelle der Option Kennwort ändern muss aktiviert ist.Wählen Sie auf der Registerkarte Dial-in (Einwählen) die Option **Allow access (Zugriff zulassen)** (oder belassen Sie die Standardeinstellung für den **Steuerungszugriff über Remote-Zugriffsrichtlinie**).Klicken Sie abschließend auf



OK.

Erweiterte Authentifizierung für L2TP über IPSec mit Active Directory

Verwenden Sie diese Konfiguration auf der ASA, damit die Authentifizierung für die L2tp-Verbindung vom Active Directory aus erfolgen kann:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup
ppp-attributes
ciscoasa(config-ppp)# authentication pap
```

Gehen Sie auf dem L2tp-Client auch zu **Erweiterte Sicherheitseinstellungen (Benutzerdefiniert)** und wählen Sie nur die Option für **unverschlüsseltes Kennwort (PAP)**.

Überprüfung

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Einige Befehle des Typs **show werden vom Tool** Output Interpreter unterstützt (nur für registrierte Kunden), mit dem sich Analysen der Ausgabe von Befehlen des Typs show abrufen lassen.

- **show crypto ipsec sa** - Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.

```
pixfirewall#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1
```

```
      access-list 105 permit ip host 172.16.1.1 host 192.168.0.2
      local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0)
      remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701)
      current_peer: 192.168.0.2, username: test
      dynamic allocated peer ip: 10.4.5.15

#pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
       #pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 23, #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
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C16F05B8

    inbound esp sas:
      spi: 0xEC06344D (3959829581)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 3, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 3335
         IV size: 8 bytes
         replay detection support: Y

outbound esp sas:
      spi: 0xC16F05B8 (3245278648)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 3, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 3335
         IV size: 8 bytes
         replay detection support: Y
```

- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-SAs in einem Peer an.

```
pixfirewall#show crypto isakmp sa

   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: 192.168.0.2
    Type    : user            Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

- **show vpn-sessiondb** - Enthält Protokollfilter, die Sie verwenden können, um detaillierte Informationen über L2TP über IPsec-Verbindungen anzuzeigen. Der vollständige Befehl aus dem globalen Konfigurationsmodus ist **show vpn-sessoindb detailliertes Remote-Filterprotokoll l2tpOverIPsec**.Dieses Beispiel zeigt die Details einer einzelnen L2TP-over-IPsec-Verbindung:

```
pixfirewall#show vpn-sessiondb detail remote filter protocol L2TPOverIPSec

Session Type: Remote Detailed

Username     : test
Index        : 1
Assigned IP  : 10.4.5.15             Public IP    : 192.168.0.2
Protocol     : L2TPOverIPSec         Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 1336                  Bytes Rx     : 14605
Client Type  :                       Client Ver   :
```

```
Group Policy : DefaultRAGroup
Tunnel Group : DefaultRAGroup
Login Time   : 18:06:08 UTC Fri Jan 1 1993
Duration     : 0h:04m:25s
Filter Name  :
NAC Result   : N/A
Posture Token:

IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1


IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28536 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 172.16.1.1/255.255.255.255/17/1701
  Remote Addr  : 192.168.0.2/255.255.255.255/17/1701
  Encryption   : 3DES                   Hashing      : MD5
  Encapsulation: Transport
  Rekey Int (T): 3600 Seconds           Rekey Left(T): 3333 Seconds
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Bytes Tx     : 1336                   Bytes Rx     : 14922
  Pkts Tx      : 25                     Pkts Rx      : 156


L2TPOverIPSec:
  Session ID   : 3
  Username     : test
  Assigned IP  : 10.4.5.15
  Encryption   : none                   Auth Mode    : msCHAPV1
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Bytes Tx     : 378                    Bytes Rx     : 13431
  Pkts Tx      : 16                     Pkts Rx      : 146
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration. Ein Beispiel für eine Debugausgabe wird ebenfalls angezeigt.

Befehle zur Fehlerbehebung

Bestimmte Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **Ausgabe von** Befehlen anzeigen können.

Hinweis: Lesen Sie die wichtigen Informationen zu Debug-Befehlen und IP-Sicherheitsfehlerbehebung - Verwenden von Debugbefehlen, bevor Sie **Debug**-Befehle verwenden.

- **debug crypto ipsec 7**: Zeigt die IPsec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp 7**: Zeigt die ISAKMP-Verhandlungen von Phase 1 an.

Beispielausgabe für Debugging

PIX-Firewall

```
PIX#debug crypto isakmp 7
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess
age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V
ID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform
# 2 acceptable  Matches global IKE entry # 2
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID
+ extended capabilities payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa
yload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo
ad
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS V
endor ID payload (version: 1.0.0, capabilities: 20000001)
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco
 ASA GW VID
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
aultRAGroup
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing keys for Responder...
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (
13) + VENDOR (13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
aultRAGroup
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previ
ously allocated memory for authorization-dn-attributes
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
```

```
cting ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting dpd vid payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length :
80

!--- Phase 1 completed succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP =
192.168.0.2, PHASE 1 COMPL
ETED
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection:
None
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer do
es not support keep-alives (type = None)
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
g P1 rekey timer: 21600 seconds.
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NONE (0) total length : 164
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo
te Proxy Host data in ID Payload:  Address 192.168.0.2, Protocol 17, Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca
l Proxy Host data in ID Payload:  Address 172.16.1.1, Protocol 17, Port 1701

!--- PIX identifies the L2TP/IPsec session. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP
= 192.168.0.2, L2TP/IPSec se
ssion detected.
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed
old sa not found by addr
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Pe
er configured for crypto map: outside_dyn_map
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing IPSec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPSec S
A Proposal # 1, Transform # 1 acceptable  Matches global IPSec SA entry # 20
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesti
ng SPI!
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
 SPI from key engine: SPI = 0xce9f6e19

!--- Constructs Quick mode in Phase 2. Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP
= 192.168.0.2, oakley
constucting quick mode
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting blank hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting IPSec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting IPSec nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
```

```
cting proxy ID
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi
tting Proxy Id:
  Remote host: 192.168.0.2  Protocol 17  Port 1701
  Local host:  172.16.1.1  Protocol 17  Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting qm hash payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b
84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N
ONE (0) total length : 144
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading
 all IPSEC SAs
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing Quick Mode Key!
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing Quick Mode Key!
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego
tiation complete for User ()  Responder, Inbound SPI = 0xce9f6e19, Outbound SPI
= 0xd08f711b
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
 a KEY_ADD msg for SA: SPI = 0xd08f711b
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher
: received KEY_UPDATE, spi 0xce9f6e19
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
g P2 rekey timer: 3059 seconds.
```

!--- Phase 2 completes succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.1 68.0.2> mask <0xFFFFFFFF> port <1701> PIX#**debug crypto ipsec 7**

```
pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09
    Rule ID: 0x028D78D8
IPSEC: Deleted inbound permit rule, SPI 0x71933D09
    Rule ID: 0x02831838
IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09
    Rule ID: 0x029134D8
IPSEC: Deleted inbound VPN context, SPI 0x71933D09
    VPN handle: 0x0048B284
IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA
    Rule ID: 0x028DAC90
IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA
    Rule ID: 0x02912AF8
IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA
    VPN handle: 0x0048468C
IPSEC: New embryonic SA created @ 0x01BFCF80,
    SCB: 0x01C262D0,
    Direction: inbound
    SPI      : 0x45C3306F
    Session ID: 0x0000000C
    VPIF num  : 0x00000001
    Tunnel type: ra
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: New embryonic SA created @ 0x0283A3A8,
    SCB: 0x028D1B38,
    Direction: outbound
    SPI      : 0x370E8DD1
    Session ID: 0x0000000C
    VPIF num  : 0x00000001
    Tunnel type: ra
```

```
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x370E8DD1
IPSEC: Creating outbound VPN context, SPI 0x370E8DD1
    Flags: 0x00000205
    SA   : 0x0283A3A8
    SPI  : 0x370E8DD1
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x028D1B38
    Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
    VPN handle: 0x0048C164
IPSEC: New outbound encrypt rule, SPI 0x370E8DD1
    Src addr: 172.16.1.1
    Src mask: 255.255.255.255
    Dst addr: 192.168.0.2
    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 0x370E8DD1
    Rule ID: 0x02826540
IPSEC: New outbound permit rule, SPI 0x370E8DD1
    Src addr: 172.16.1.1
    Src mask: 255.255.255.255
    Dst addr: 192.168.0.2
    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: 0x370E8DD1
    Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x370E8DD1
    Rule ID: 0x028D78D8
IPSEC: Completed host IBSA update, SPI 0x45C3306F
IPSEC: Creating inbound VPN context, SPI 0x45C3306F
    Flags: 0x00000206
    SA   : 0x01BFCF80
    SPI  : 0x45C3306F
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x0048C164
    SCB  : 0x01C262D0
    Channel: 0x01693F08
IPSEC: Completed inbound VPN context, SPI 0x45C3306F
    VPN handle: 0x0049107C
```

```
IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1
    Flags: 0x00000205
    SA   : 0x0283A3A8
    SPI  : 0x370E8DD1
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0049107C
    SCB  : 0x028D1B38
    Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
    VPN handle: 0x0048C164
IPSEC: Completed outbound inner rule, SPI 0x370E8DD1
    Rule ID: 0x02826540
IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1
    Rule ID: 0x028D78D8
IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    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 0x45C3306F
    Rule ID: 0x02831838
IPSEC: New inbound decrypt rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    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: 0x45C3306F
    Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F
    Rule ID: 0x028DAC90
IPSEC: New inbound permit rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    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: 0x45C3306F
    Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F
    Rule ID: 0x02912E50
```

Fehlerbehebung mit ASDM

Sie können ASDM verwenden, um die Protokollierung zu aktivieren und die Protokolle anzuzeigen.

1. Wählen Sie **Konfiguration > Eigenschaften > Protokollierung > Protokollierung Setup**, wählen Sie **Protokollierung aktivieren aus**, und klicken Sie auf **Übernehmen**, um die Protokollierung zu aktivieren.
2. Wählen Sie **Monitoring > Logging > Log Buffer > On Logging Level aus**, wählen Sie **Logging Buffer aus**, und klicken Sie auf **View**, um die Protokolle anzuzeigen.

Problem: Häufige Unterbrechungen

Leerlauf/Sitzungs-Timeout

Wenn die Zeitüberschreitung im Leerlauf auf 30 Minuten festgelegt ist (Standardeinstellung), bedeutet dies, dass der Tunnel verworfen wird, nachdem kein Datenverkehr 30 Minuten lang durch ihn fließt. Der VPN-Client wird unabhängig von der Einstellung der Leerlaufzeitüberschreitung nach 30 Minuten getrennt und erhält die Fehlermeldung `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Konfigurieren Sie Leerlaufzeitüberschreitung und Sitzungs-Timeout so, dass der Tunnel immer aktiv ist und der Tunnel nicht verworfen wird.

Geben Sie den Befehl **vpn-idle-timeout** im Konfigurationsmodus für Gruppenrichtlinien oder im Konfigurationsmodus für Benutzernamen ein, um die Zeitüberschreitungsdauer für den Benutzer zu konfigurieren:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-idle-timeout none
```

Konfigurieren Sie mit dem Befehl **vpn-session-timeout** im Konfigurationsmodus für Gruppenrichtlinien oder im Konfigurationsmodus für Benutzernamen eine maximale Zeit für VPN-Verbindungen:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-session-timeout none
```

Fehlerbehebung in Windows Vista

Gleichzeitiger Benutzer

Mit L2TP/IPsec in Windows Vista wurden Architekturänderungen eingeführt, die verhindern, dass

mehrere Benutzer gleichzeitig mit einem Head-End-PIX/ASA verbunden werden können. Dieses Verhalten tritt unter Windows 2K/XP nicht auf. Cisco hat für diese Änderung ab Version 7.2(3) eine Lösung implementiert.

Vista-PC kann keine Verbindung herstellen

Wenn der Windows Vista-Computer nicht in der Lage ist, den L2TP-Server zu verbinden, dann überprüfen Sie, ob Sie NUR mschap-v2 unter den ppp-Attributen auf der DefaultRAGroup konfiguriert haben.

Zugehörige Informationen

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- Cisco Security Appliances der Serie PIX 500
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Produkt-Support für die Cisco PIX Firewall
- Cisco Secure PIX Firewall - Befehlsreferenzen
- RADIUS-Support-Seite
- Support-Seite für IPSec-Aushandlung/IKE-Protokolle
- Anforderungen für Kommentare (RFCs)
- Layer-2-Tunnelprotokoll (L2TP)
- Technischer Support und Dokumentation für Cisco Systeme