Client VPN over Wireless LAN mit WLC-Konfigurationsbeispiel

Inhalt

Einleitung

In diesem Dokument wird das Konzept des Virtual Private Network (VPN) in einer Wireless-Umgebung vorgestellt. In diesem Dokument werden die Konfigurationen erläutert, die bei der Bereitstellung eines VPN-Tunnels zwischen einem Wireless-Client und einem VPN-Server über einen Wireless LAN-Controller (WLC) erforderlich sind.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Kenntnis der WLCs und Konfiguration der WLC-Basisparameter
- Kenntnisse über Wi-Fi Protected Access (WPA)-Konzepte
- Grundkenntnisse des VPN und seiner Typen
- Kenntnis von IPsec

- Grundkenntnisse der verfügbaren Verschlüsselungs-, Authentifizierungs- und Hashing-Algorithmen

Verwendete Komponenten

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

- Cisco 2006 WLC mit Version 4.0.179.8
- Cisco Lightweight Access Point (LAP) der Serie 1000
- Cisco 3640 mit Cisco IOS® Softwareversion 12.4(8)
- Cisco VPN Client Version 4.8

Hinweis: In diesem Dokument wird ein 3640-Router als VPN-Server verwendet. Um erweiterte Sicherheitsfunktionen zu unterstützen, können Sie auch einen dedizierten VPN-Server verwenden.

Hinweis: Damit ein Router als VPN-Server fungieren kann, muss er ein Feature-Set ausführen, das grundlegende IPsec-Funktionen unterstützt.

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.

Konventionen

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

Hintergrundinformationen

Ein VPN ist ein privates Datennetzwerk, das verwendet wird, um die Daten sicher innerhalb eines privaten Netzwerks über die öffentliche Telekommunikationsinfrastruktur, z. B. das Internet, zu übertragen. Dieses VPN schützt den Datenschutz durch Verwendung eines Tunneling-Protokolls und von Sicherheitsverfahren.

VPN für Remote-Zugriff

Mit einer VPN-Konfiguration für den Remote-Zugriff können VPN-Software-Clients wie mobile Benutzer sicher auf zentralisierte Netzwerkressourcen zugreifen, die sich hinter einem VPN-Server befinden. In Cisco Terminologie werden diese VPN-Server und -Clients auch als Cisco Easy VPN-Server und Cisco Easy VPN Remote-Gerät bezeichnet.

Ein Cisco Easy VPN Remote-Gerät kann Cisco IOS-Router, Cisco PIX Security Appliances, Cisco VPN 3002 Hardware-Clients und der Cisco VPN-Client sein. Sie werden verwendet, um Sicherheitsrichtlinien über eine VPN-Tunnelverbindung von einem Cisco Easy VPN-Server zu erhalten. Dadurch werden die Konfigurationsanforderungen am Remote-Standort minimiert. Der Cisco VPN Client ist ein Software-Client, der auf PCs, Laptops usw. installiert werden kann.

Ein Cisco Easy VPN-Server kann Cisco IOS-Router, Cisco PIX Security Appliances und Cisco

VPN 3000 Concentrators sein.

In diesem Dokument wird die Cisco VPN Client-Software verwendet, die auf einem Laptop als VPN-Client und Cisco 3640 IOS-Router als VPN-Server ausgeführt wird. Das Dokument verwendet den IPsec-Standard, um einen VPN-Tunnel zwischen einem Client und einem Server einzurichten.

IPsec

IPsec ist ein Framework offener Standards, das von der Internet Engineering Task Force (IETF) entwickelt wurde. IPsec bietet Sicherheit für die Übertragung vertraulicher Informationen über ungeschützte Netzwerke wie das Internet.

IPsec bietet Netzwerkdatenverschlüsselung auf IP-Paketebene, was eine robuste, standardbasierte Sicherheitslösung darstellt. Die Hauptaufgabe von IPsec besteht darin, den Austausch privater Informationen über eine unsichere Verbindung zu ermöglichen. IPsec verwendet Verschlüsselung, um Informationen vor dem Abfangen oder Abhören zu schützen. Um die Verschlüsselung effizient zu nutzen, sollten beide Parteien jedoch ein Geheimnis teilen, das sowohl für die Verschlüsselung als auch für die Entschlüsselung der Informationen verwendet wird.

IPsec arbeitet in zwei Phasen, um den vertraulichen Austausch eines gemeinsam genutzten Geheimtitels zu ermöglichen:

- Phase 1 - behandelt die Aushandlung von Sicherheitsparametern, die zum Einrichten eines sicheren Kanals zwischen zwei IPsec-Peers erforderlich sind. Phase 1 wird im Allgemeinen über das Internet Key Exchange (IKE)-Protokoll implementiert. Wenn der Remote-IPsec-Peer IKE nicht ausführen kann, können Sie die manuelle Konfiguration mit vorinstallierten Schlüsseln verwenden, um Phase 1 abzuschließen.
- Phase 2 - Verwendet den in Phase 1 eingerichteten sicheren Tunnel zum Austausch der Sicherheitsparameter, die für die tatsächliche Übertragung von Benutzerdaten erforderlich sind. Die in beiden Phasen von IPsec verwendeten sicheren Tunnel basieren auf Sicherheitszuordnungen (Security Associations, SAs), die an jedem IPsec-Endpunkt verwendet werden. SAs beschreiben die Sicherheitsparameter, z. B. die Art der Authentifizierung und Verschlüsselung, die beide Endpunkte verwenden.

Die in Phase 2 ausgetauschten Sicherheitsparameter werden zur Erstellung eines IPsec-Tunnels verwendet, der wiederum für die Datenübertragung zwischen dem VPN-Client und dem Server verwendet wird.

Weitere Informationen zu IPsec und seiner Konfiguration finden Sie unter Konfigurieren von IPsec.

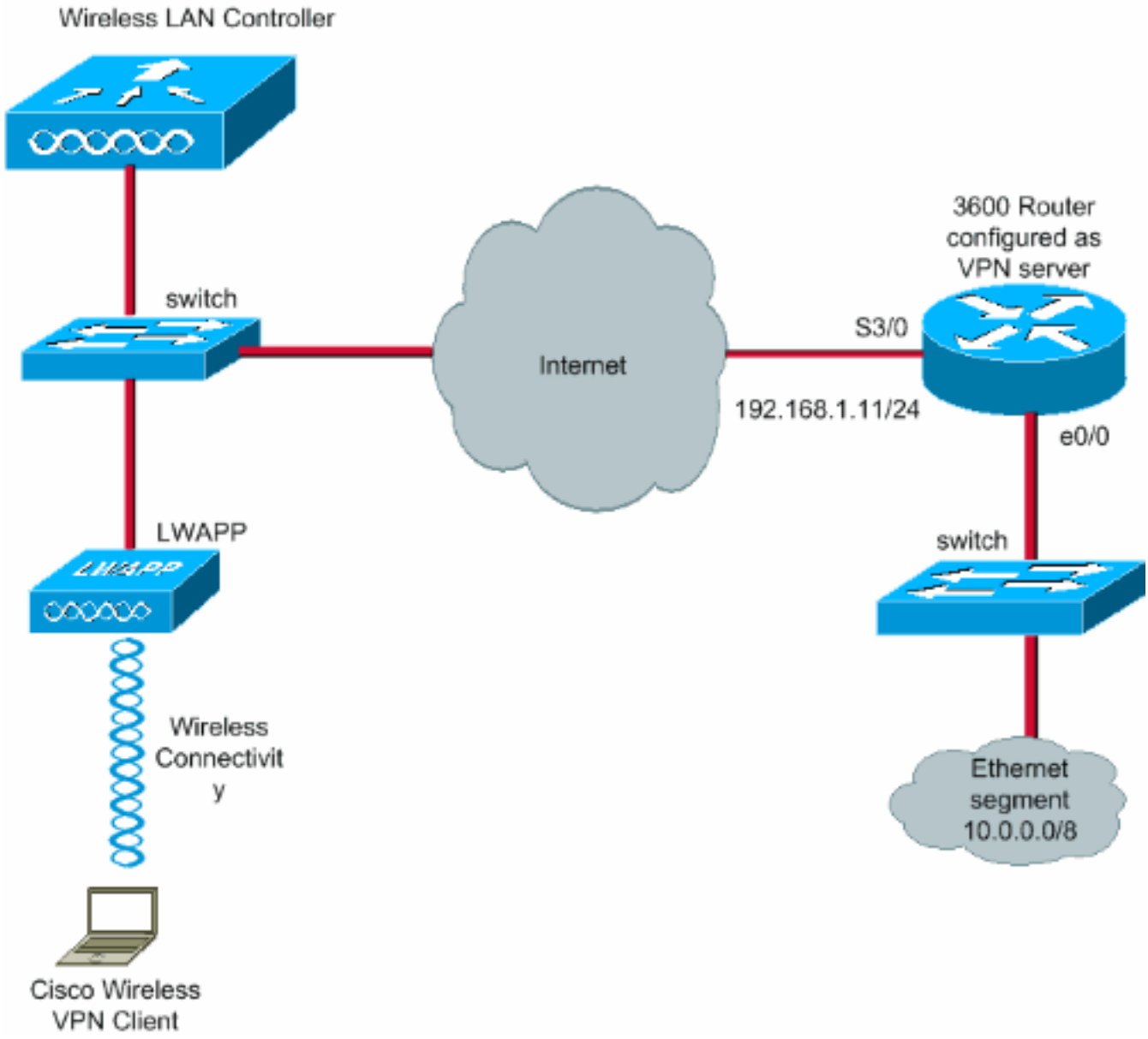
Sobald ein VPN-Tunnel zwischen dem VPN-Client und dem Server eingerichtet ist, *werden die vom VPN-Server definierten Sicherheitsrichtlinien an den Client gesendet*. Dadurch werden die Konfigurationsanforderungen auf Client-Seite minimiert.

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

Netzwerkdiagramm

In diesem Dokument werden folgende Konfigurationen verwendet:

- IP-Adresse der Verwaltungsschnittstelle des WLC: 172.16.1.10/16
- IP-Adresse der AP-Manager-Schnittstelle des WLC: 172.16.1.11/16
- Standard-Gateway - 172.16.1.20/16**Hinweis:** In einem Live-Netzwerk sollte dieses Standard-Gateway auf die eingehende Schnittstelle des sofortigen Routers verweisen, der den WLC mit dem restlichen Netzwerk und/oder mit dem Internet verbindet.
- IP-Adresse des VPN-Servers s3/0 - 192.168.1.11/24**Hinweis:** Diese IP-Adresse sollte auf die Schnittstelle verweisen, die den VPN-Tunnel auf der Seite des VPN-Servers terminiert. In diesem Beispiel ist s3/0 die Schnittstelle, die den VPN-Tunnel am VPN-Server terminiert.
- Das LAN-Segment des VPN-Servers verwendet den IP-Adressbereich 10.0.0.0/8.



Konfigurieren

In einer zentralisierten WLAN-Architektur muss der Client mit einem Lightweight Access Point (LAP) verbunden werden, der wiederum bei einem WLC registriert werden muss, um einem Wireless-VPN-Client wie einem Laptop den Aufbau eines VPN-Tunnels mit einem VPN-Server zu ermöglichen. Dieses Dokument enthält die LAP, die bereits beim WLC registriert wurde. Hierzu wird der lokale Subnetz-Broadcast Discovery-Prozess verwendet, der in der Lightweight AP (LAP)-Registrierung bei einem Wireless LAN Controller (WLC) erläutert wird.

Im nächsten Schritt wird der WLC für VPN konfiguriert.

VPN-Terminierung und -Passthrough

Bei Cisco WLCs der Serie 4000 vor Version 4 wird eine Funktion mit dem Namen IPsec VPN Termination (IPsec-Unterstützung) unterstützt. Diese Funktion ermöglicht es diesen Controllern, VPN-Client-Sitzungen direkt auf dem Controller zu beenden. Zusammenfassend lässt sich feststellen, dass der Controller selbst als VPN-Server agieren kann. Hierfür muss jedoch ein separates Hardwaremodul für die VPN-Terminierung im Controller installiert sein.

Diese IPsec-VPN-Unterstützung ist in folgenden Ländern nicht verfügbar:

- Cisco WLC der Serie 2000
- Alle WLCs mit Version 4.0 oder höher

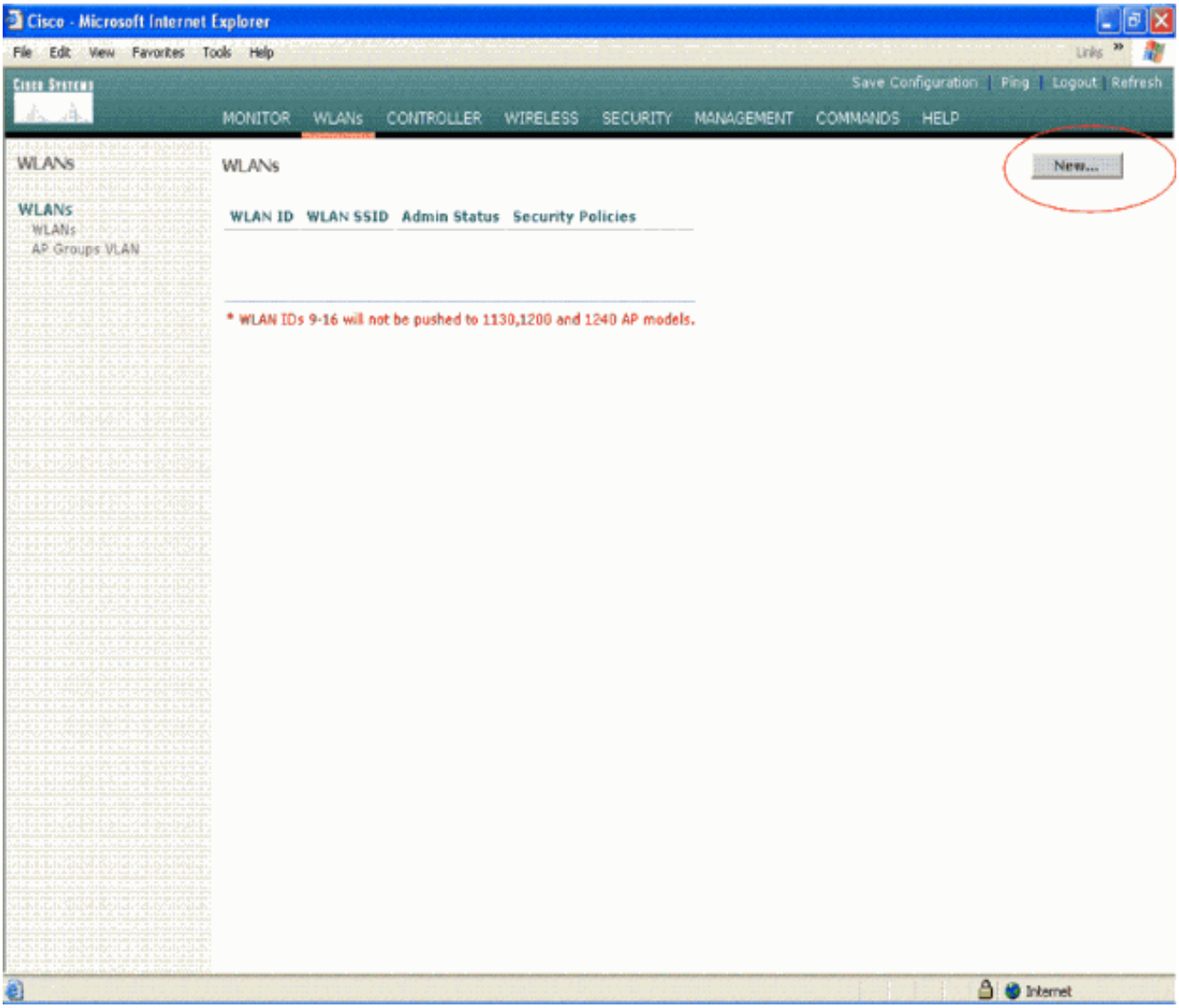
Daher wird in Versionen nach Version 4.0 nur noch VPN-Passthrough unterstützt. Diese Funktion wird auch vom Cisco WLC der Serie 2000 unterstützt.

VPN-Passthrough ist eine Funktion, mit der ein Client nur einen Tunnel mit einem bestimmten VPN-Server einrichten kann. Wenn Sie also sicher auf den konfigurierten VPN-Server sowie auf einen anderen VPN-Server oder das Internet zugreifen müssen, ist dies bei aktiviertem VPN-Passthrough auf dem Controller nicht möglich. Unter diesen Voraussetzungen müssen Sie VPN-Passthrough deaktivieren. Der WLC kann jedoch so konfiguriert werden, dass er als Passthrough fungiert, um mehrere VPN-Gateways zu erreichen, wenn eine entsprechende ACL erstellt und auf das entsprechende WLAN angewendet wird. In solchen Szenarien, in denen Sie mehrere VPN-Gateways erreichen möchten, um für Redundanz zu sorgen, deaktivieren Sie den VPN-Passthrough-Modus, und erstellen Sie eine ACL, die den Zugriff auf die VPN-Gateways ermöglicht und die ACL auf das WLAN anwendet.

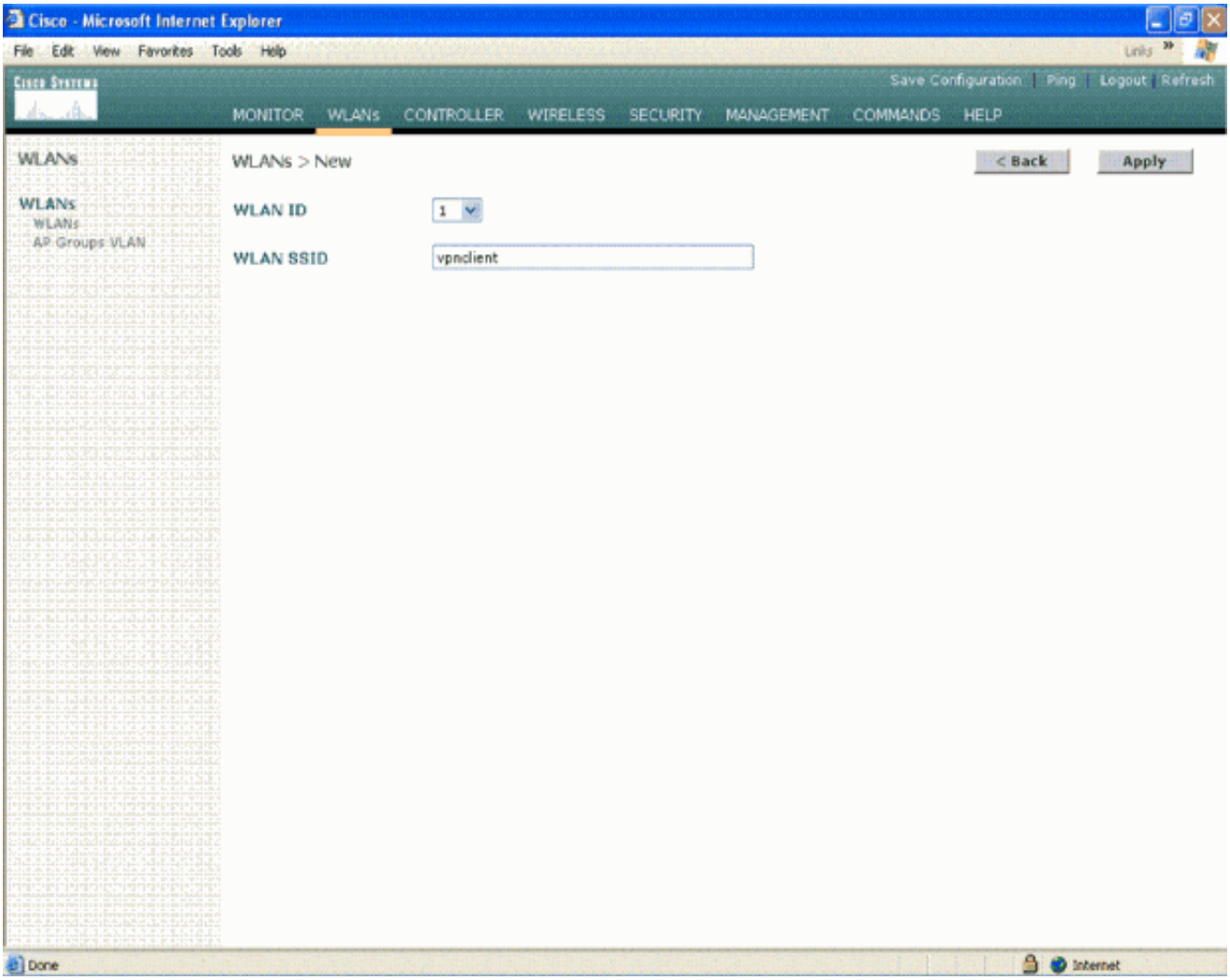
Konfigurieren des WLC für VPN-Passthrough

Führen Sie diese Schritte aus, um den VPN-Passthrough zu konfigurieren.

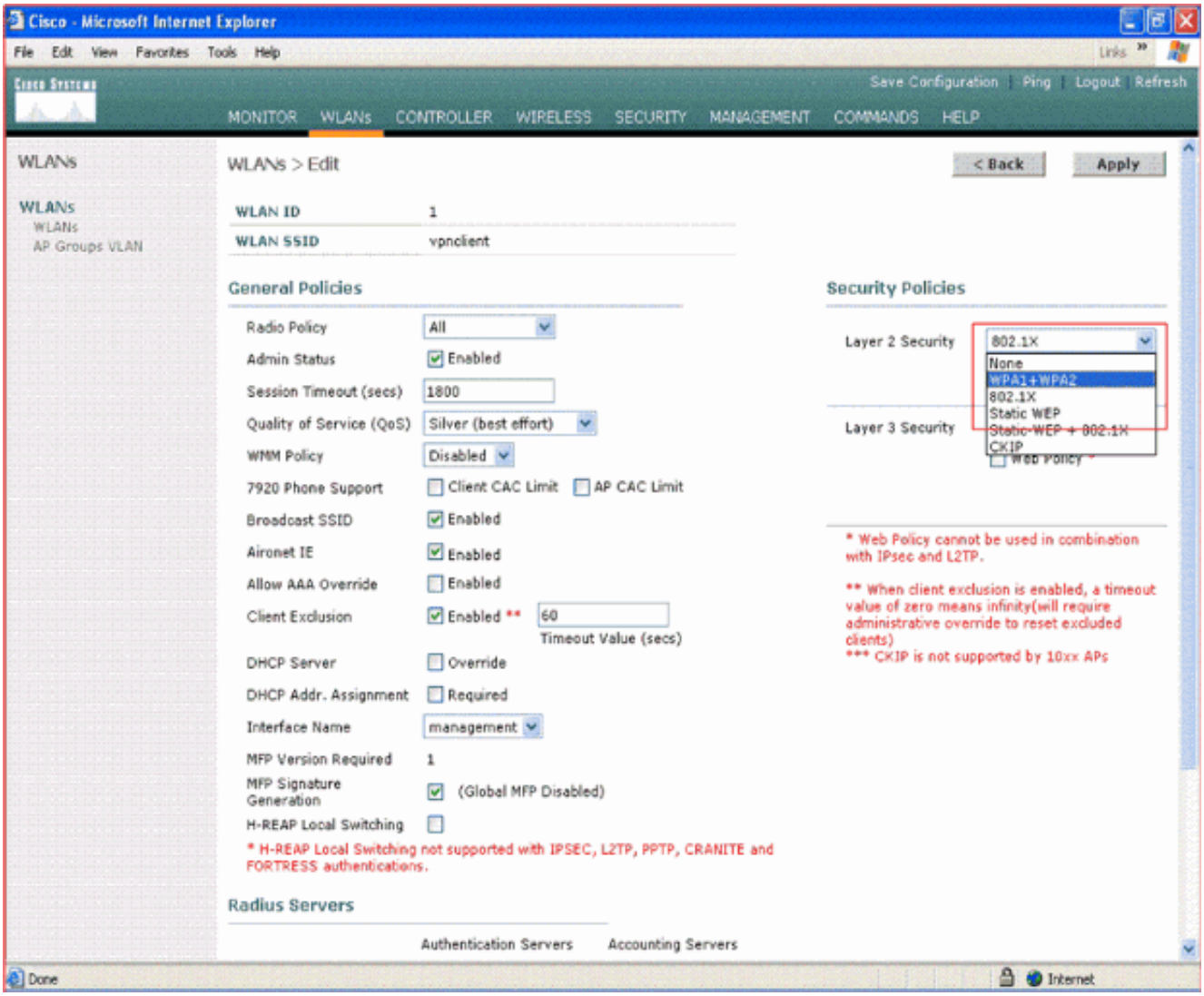
1. Klicken Sie in der WLC-GUI auf **WLAN**, um zur Seite WLANs zu gelangen.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu erstellen.



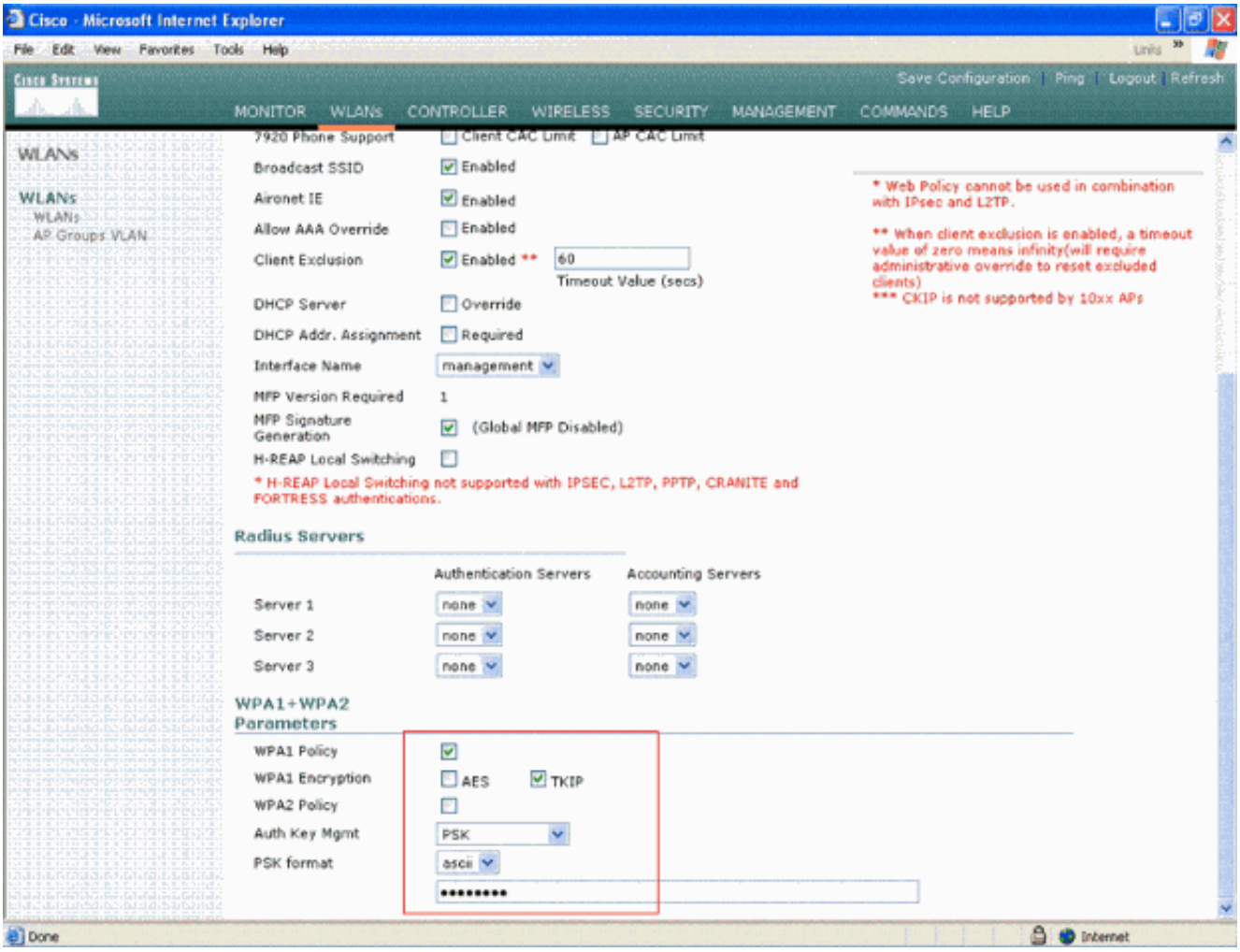
3. Die WLAN-SSID wird in diesem Beispiel als **vpnclient** bezeichnet. Klicken Sie auf Apply (Anwenden).



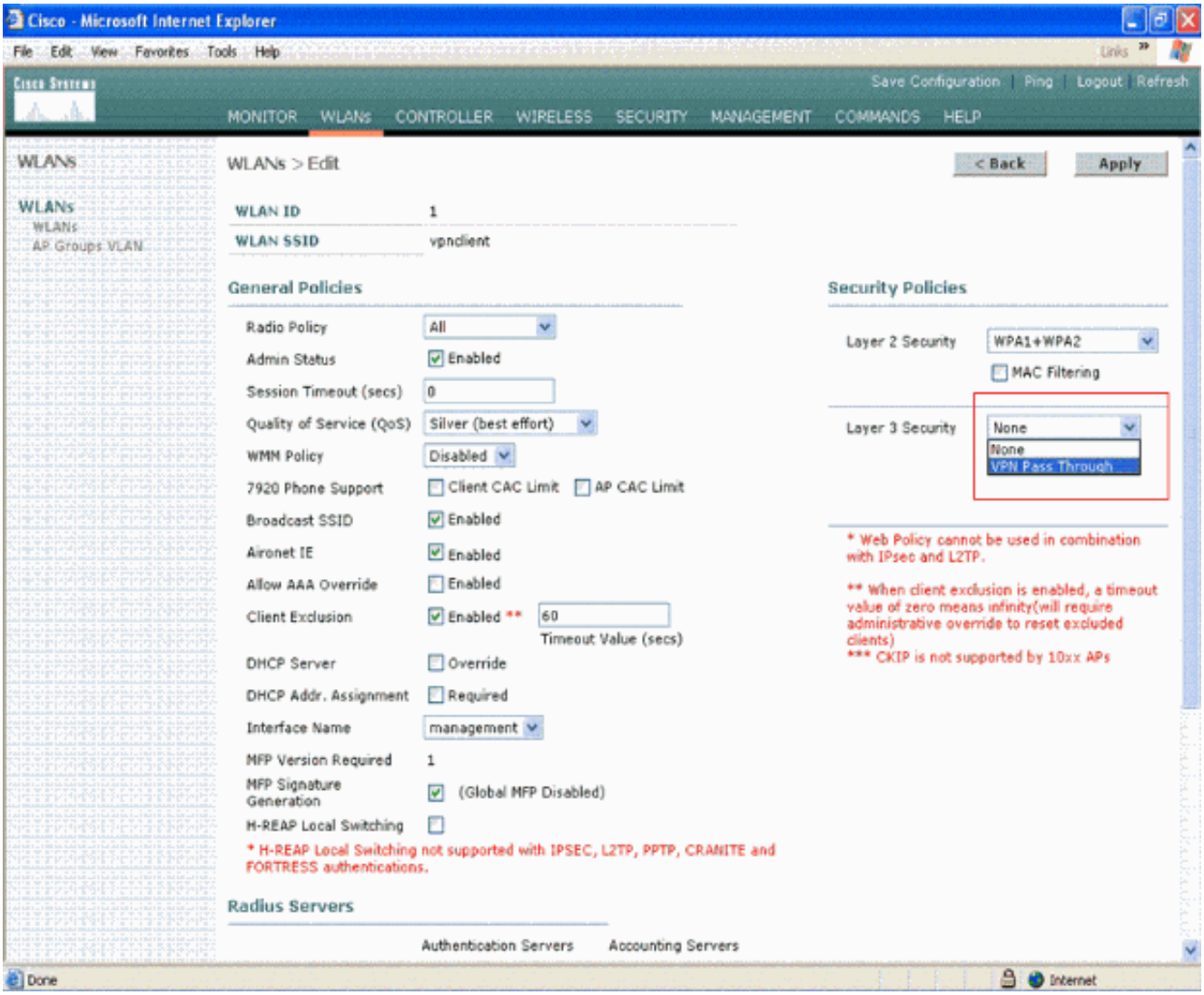
4. Konfigurieren Sie die vpnclient-SSID mit Layer-2-Sicherheit. *Dies ist optional.*In diesem Beispiel wird **WPA1+WPA2** als Sicherheitstyp verwendet.



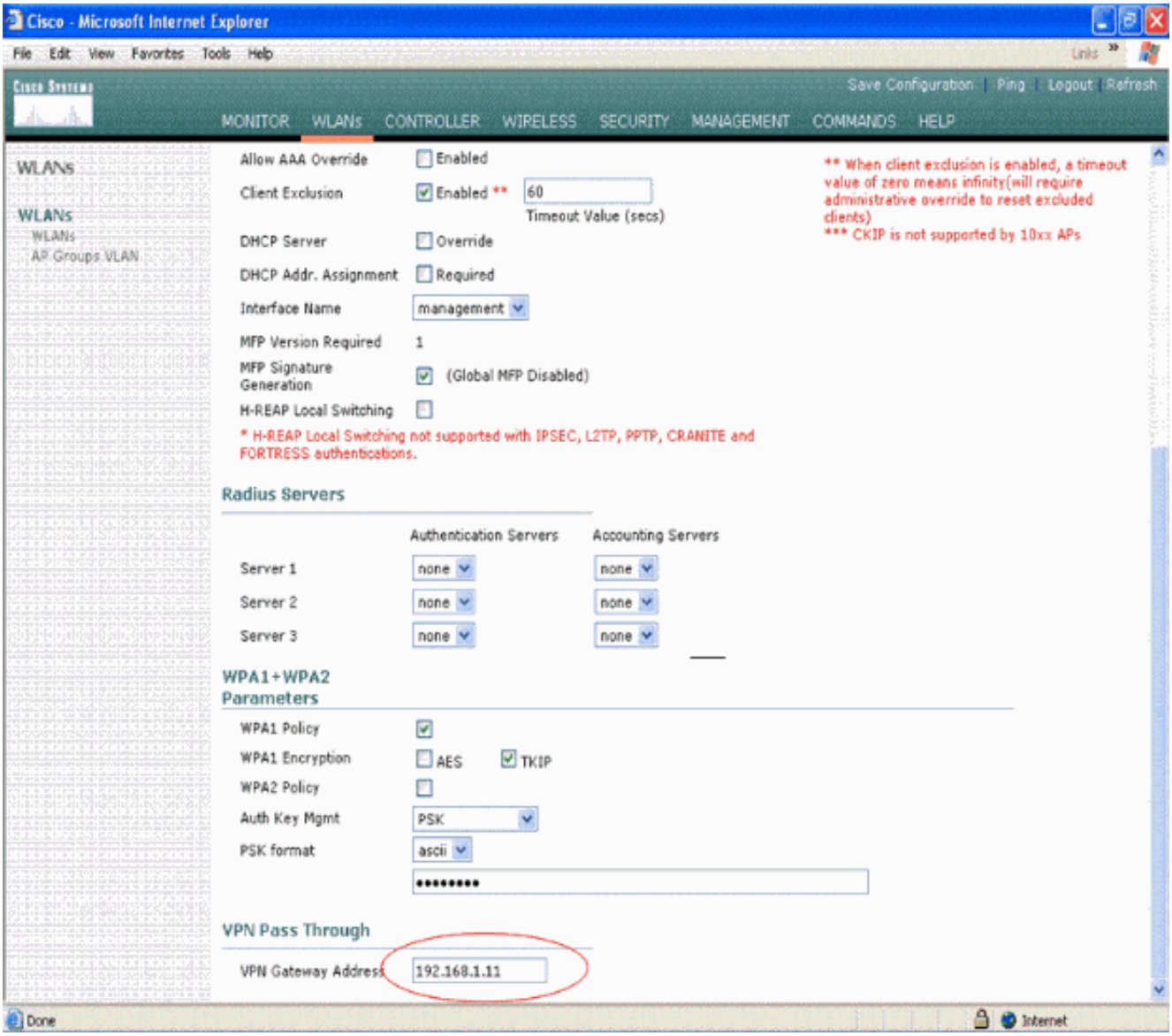
5. Konfigurieren Sie die zu verwendende WPA-Richtlinie und den zu verwendenden Authentifizierungsschlüssel-Managementtyp.In diesem Beispiel wird **PSK (Pre-Shared Key)** für die Verwaltung von Authentifizierungsschlüsseln verwendet. Wenn PSK ausgewählt ist, wählen Sie **ASCII** als PSK-Format aus, und geben Sie den PSK-Wert ein. Dieser Wert sollte in der SSID-Konfiguration des Wireless-Clients identisch sein, damit die Clients, die zu dieser SSID gehören, eine Verbindung zu diesem WLAN herstellen.



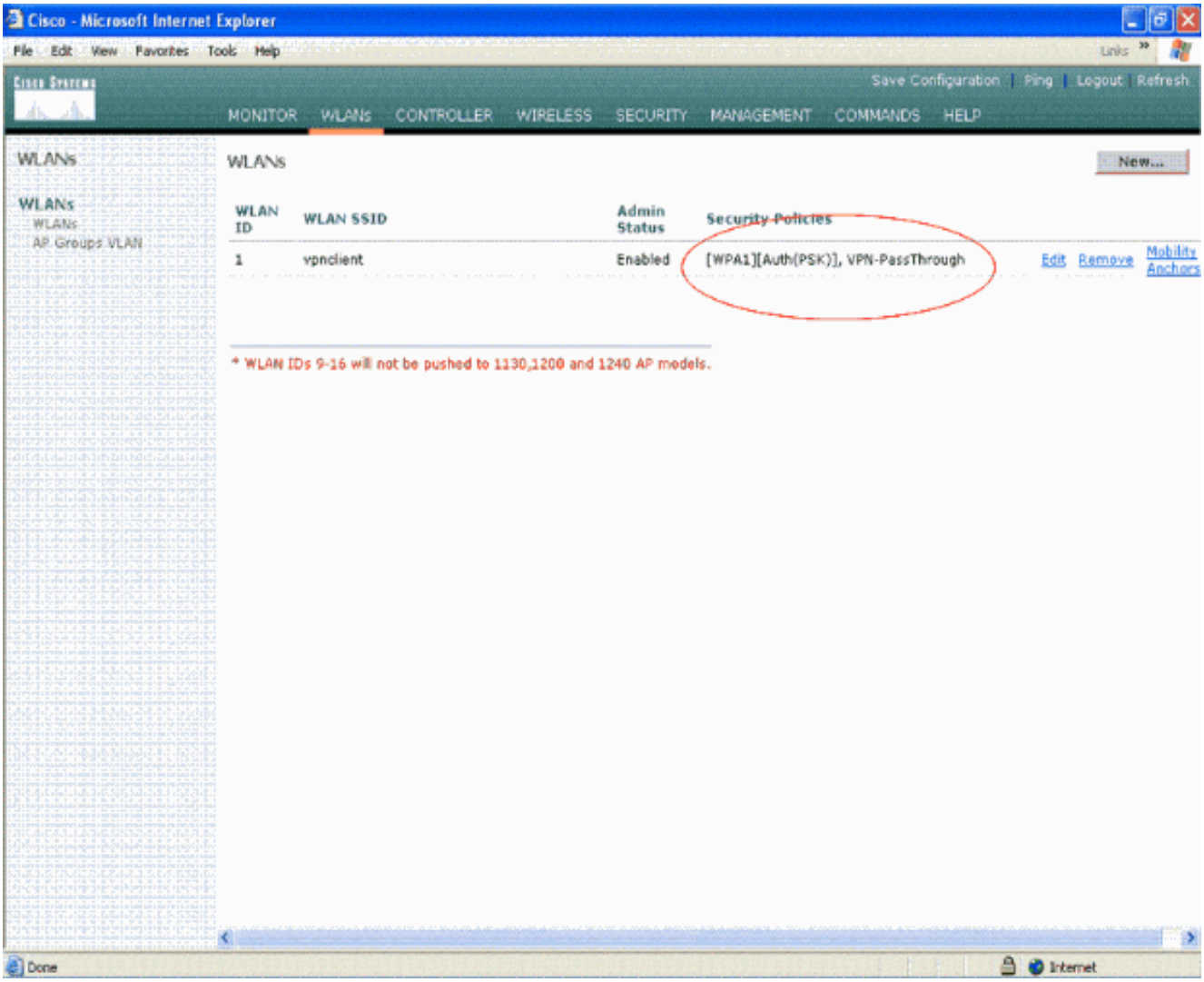
6. Wählen Sie **VPN-Passthrough** als Layer-3-Sicherheit aus. Hier ist das Beispiel.



7. Wenn VPN-Passthrough als Layer-3-Sicherheit ausgewählt ist, fügen Sie die VPN-Gateway-Adresse wie im folgenden Beispiel gezeigt hinzu.Diese Gateway-Adresse sollte die IP-Adresse der Schnittstelle sein, die den VPN-Tunnel am Server terminiert. In diesem Beispiel ist die IP-Adresse der s3/0-Schnittstelle (192.168.1.11/24) am VPN-Server die Gateway-Adresse, die konfiguriert werden
soll.



8. Klicken Sie auf **Apply** (Anwenden). Das WLAN mit dem Namen *vpnclient* ist jetzt für VPN-Passthrough
konfiguriert.



VPN-Serverkonfiguration

Diese Konfiguration zeigt den Cisco 3640 Router als VPN-Server.

Hinweis: Zur Vereinfachung verwendet diese Konfiguration statisches Routing, um die IP-Erreichbarkeit zwischen den Endpunkten aufrechtzuerhalten. Sie können jedes dynamische Routing-Protokoll wie Routing Information Protocol (RIP), Open Shortest Path First (OSPF) usw. verwenden, um die Erreichbarkeit aufrechtzuerhalten.

Hinweis: Der Tunnel wird nicht eingerichtet, wenn zwischen Client und Server keine IP-Erreichbarkeit besteht.

Hinweis: In diesem Dokument wird davon ausgegangen, dass der Benutzer weiß, wie dynamisches Routing im Netzwerk aktiviert wird.

Cisco Router 3640

```
vpnrouter#show running-config

Building configuration...

Current configuration : 1623 bytes
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1
!--- Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiation. hash md5
!--- Choose the hash algorithm to be md5. authentication
pre-share
!--- The authentication method selected is pre-shared.
group 2
!--- With the group command, you can declare what size
modulus to !--- use for Diffie-Hellman calculation.
Group 1 is 768 bits long, !--- and group 2 is 1024 bits
long.


crypto isakmp client configuration group employee key
cisco123 pool mypool
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!--- Create a dynamic map and apply the transform set
that was created. !--- Set reverse-route for the VPN
server. crypto dynamic-map mymap 10 set transform-set
```

```
myset reverse-route
!
crypto map clientmap isakmp authorization list employee
!--- Create the crypto map.
crypto map clientmap client configuration address crypto
map clientmap 10 ipsec-isakmp dynamic mymap
!
!--- Apply the employee group list that was created
earlier.



!
!
!
!
interface Ethernet0/0
 ip address 10.0.0.20 255.0.0.0
 half-duplex
!
interface Serial3/0
 ip address 192.168.1.11 255.255.255.0
 clock rate 64000
 no fair-queue
 crypto map clientmap
!--- Apply the crypto map to the interface. ! interface
Serial3/1 no ip address shutdown ! interface Serial3/2
no ip address shutdown ! interface Serial3/3 no ip
address shutdown ! interface Serial3/4 no ip address
shutdown ! interface Serial3/5 no ip address shutdown !
interface Serial3/6 no ip address shutdown ! interface
Serial3/7 no ip address shutdown ip local pool mypool
10.0.0.50 10.0.0.60
!--- Configure the Dynamic Host Configuration Protocol
!--- (DHCP) pool which assigns the tunnel !--- IP
address to the wireless client. !--- This tunnel IP
address is different from the IP address !--- assigned
locally at the wireless client (either statically or
dynamically). ip http server no ip http secure-server !
ip route 172.16.0.0 255.255.0.0 192.168.1.10 ! ! ! !
control-plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0
line vty 0 4 ! ! end ip subnet-zero . . . ! end
```

Hinweis: In diesem Beispiel wird nur die Gruppenauthentifizierung verwendet. Es wird keine individuelle Benutzerauthentifizierung verwendet.

VPN-Client-Konfiguration

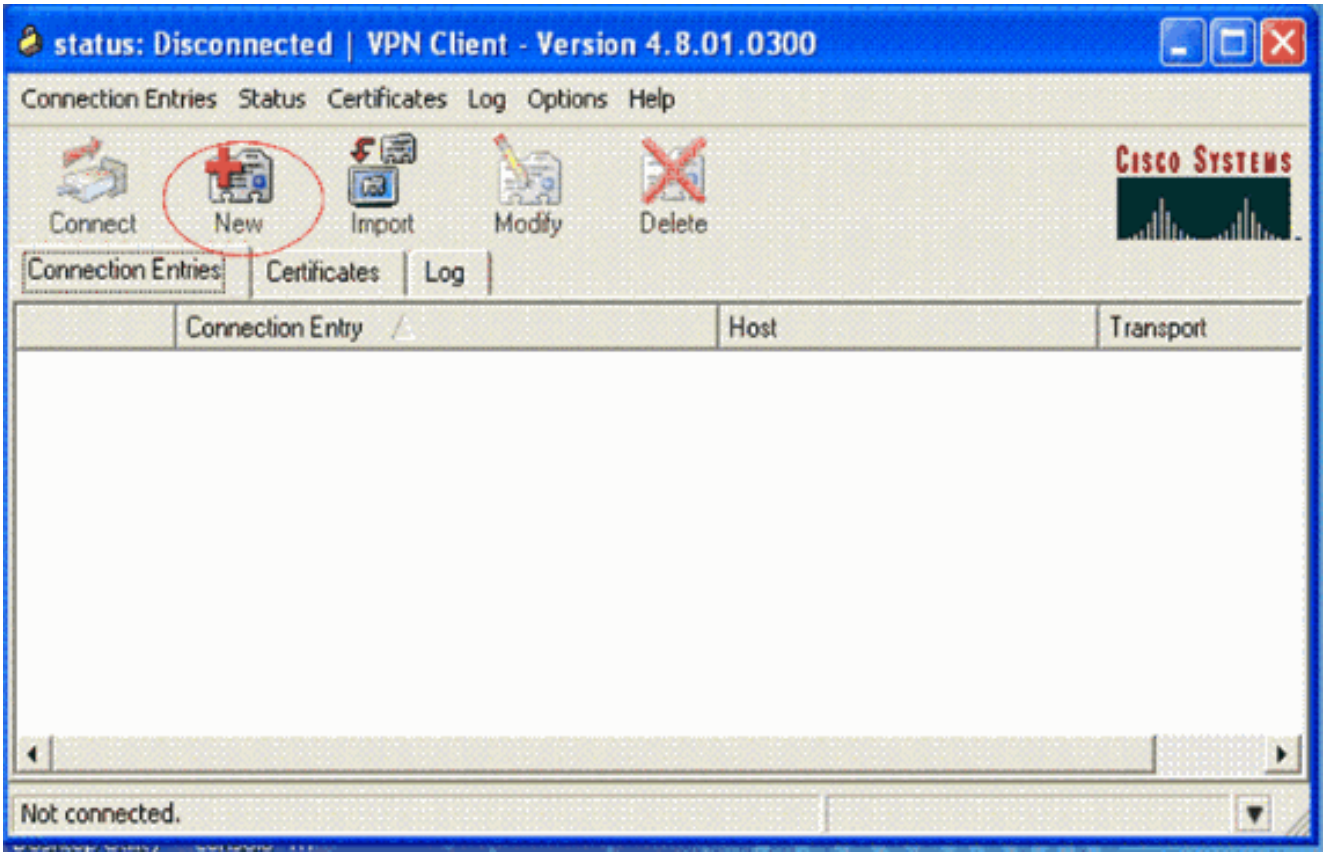
Ein Software-VPN-Client kann vom Cisco.com Software Center heruntergeladen werden.

Hinweis: Bei einigen Cisco Software müssen Sie sich mit einem CCO-Benutzernamen und -Kennwort anmelden.

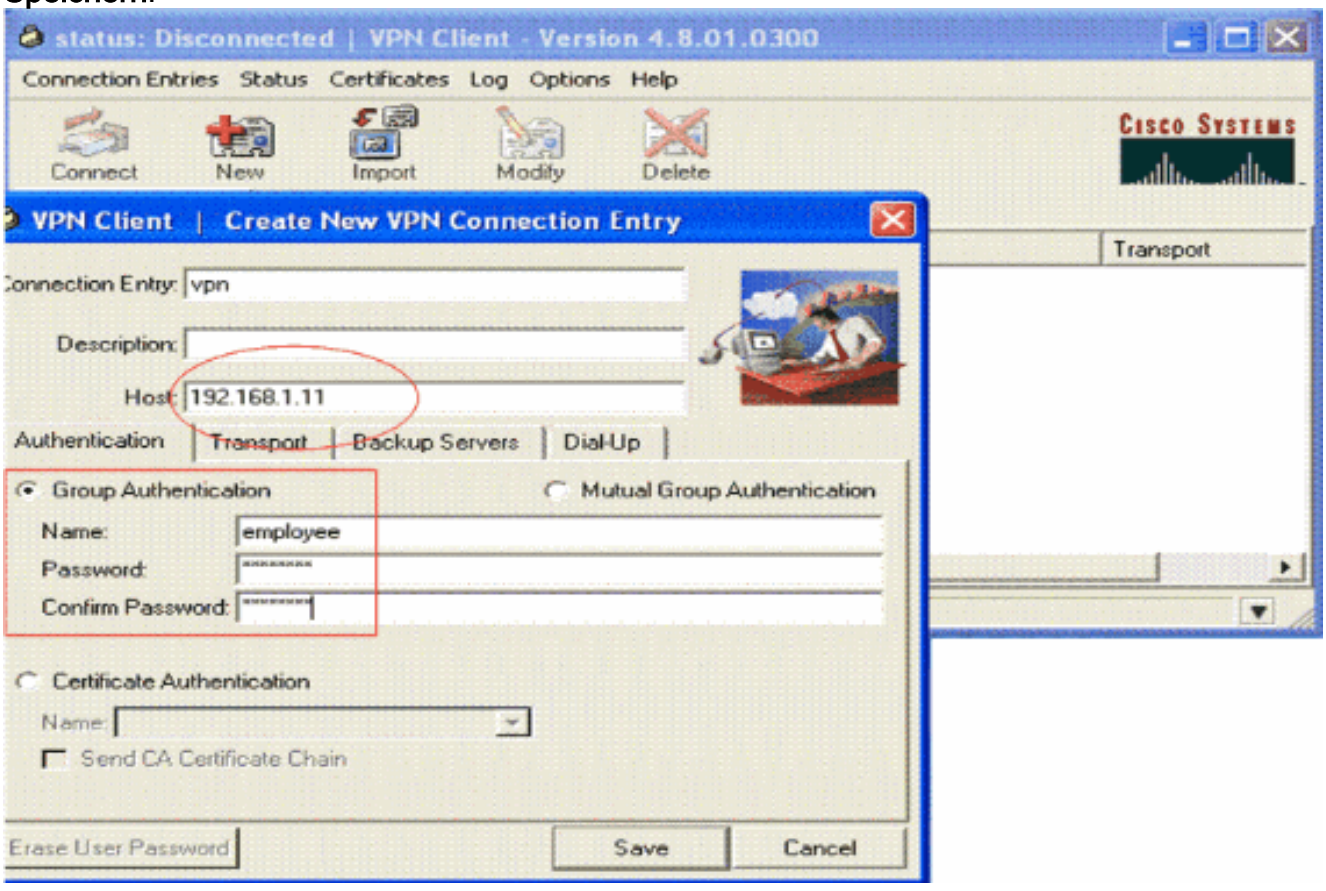
Führen Sie diese Schritte aus, um den VPN-Client zu konfigurieren.

1. Wählen Sie als Wireless-Client (Laptop) **Start > Programme > Cisco Systems VPN Client > VPN Client** aus, um auf den VPN Client zuzugreifen. Dies ist der Standardspeicherort, an dem der VPN-Client installiert ist.
2. Klicken Sie auf **Neu**, um das Fenster Create New VPN Connection Entry (Neue VPN-

Verbindung erstellen) zu öffnen.



3. Geben Sie den Namen des Verbindungseintrags und eine Beschreibung ein. In diesem Beispiel *wird esvpn verwendet*.Das Feld Beschreibung ist optional. Geben Sie die IP-Adresse des VPN-Servers in das Feld Host ein. Geben Sie dann den VPN-Gruppennamen und das VPN-Kennwort ein, und klicken Sie auf **Speichern**.



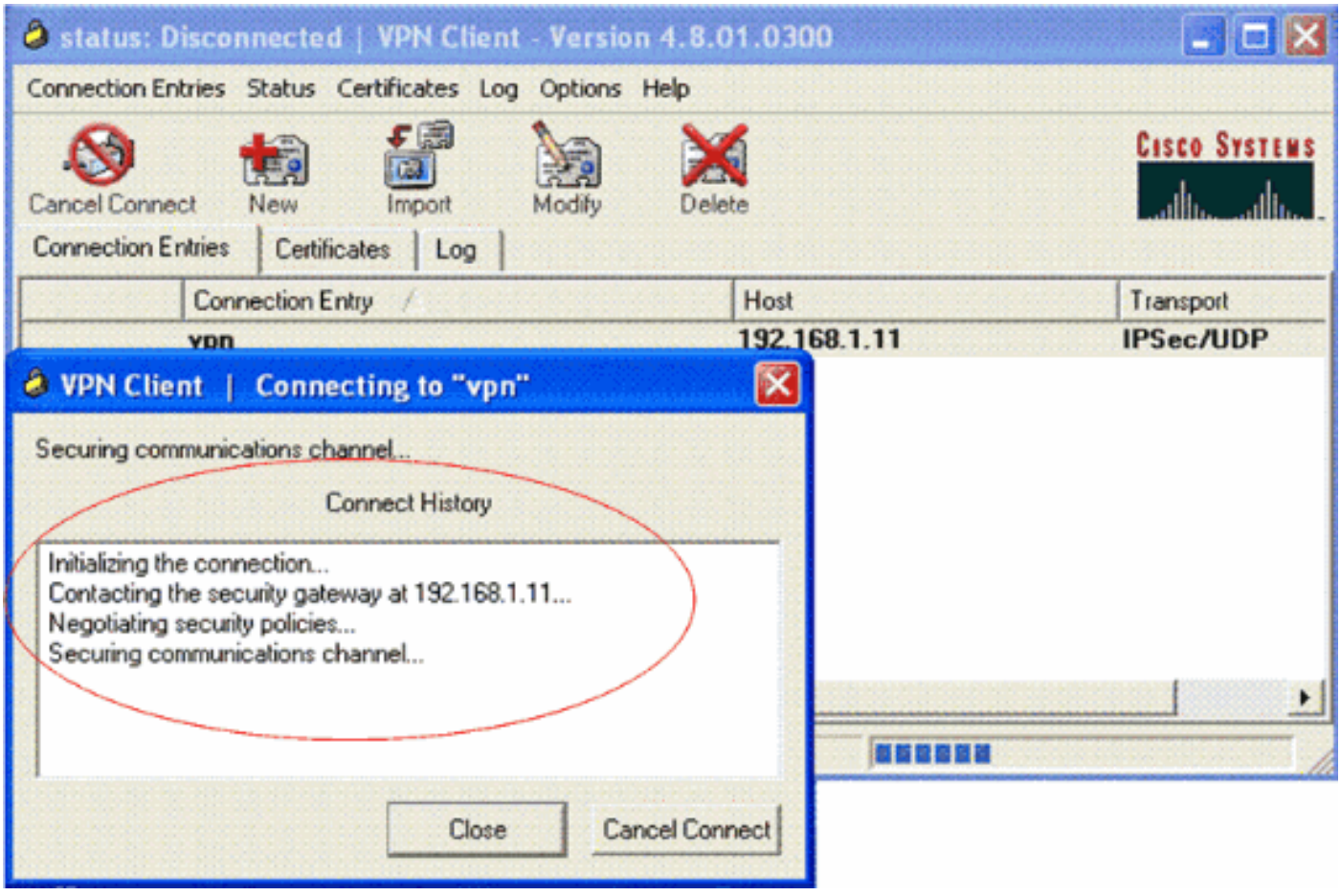
Hinweis: Der hier konfigurierte Gruppenname und das hier konfigurierte Kennwort müssen mit dem im VPN-Server konfigurierten identisch sein. In diesem Beispiel wird der Name des *Mitarbeiters* und das Kennwort *cisco123* verwendet.

Überprüfung

Um diese Konfiguration zu überprüfen, konfigurieren Sie den SSID-**VPN-Client** im Wireless-Client mit denselben Sicherheitsparametern, die im WLC konfiguriert sind, und ordnen den Client diesem WLAN zu. Es gibt mehrere Dokumente, in denen die Konfiguration eines Wireless-Clients mit einem neuen Profil erläutert wird.

Wenn der Wireless-Client zugeordnet ist, gehen Sie zum VPN-Client, und klicken Sie auf die von Ihnen konfigurierte Verbindung. Klicken Sie anschließend im Hauptfenster des VPN-Clients auf **Verbinden**.

Sie sehen die zwischen dem Client und dem Server ausgehandelten Sicherheitsparameter für Phase 1 und Phase 2.

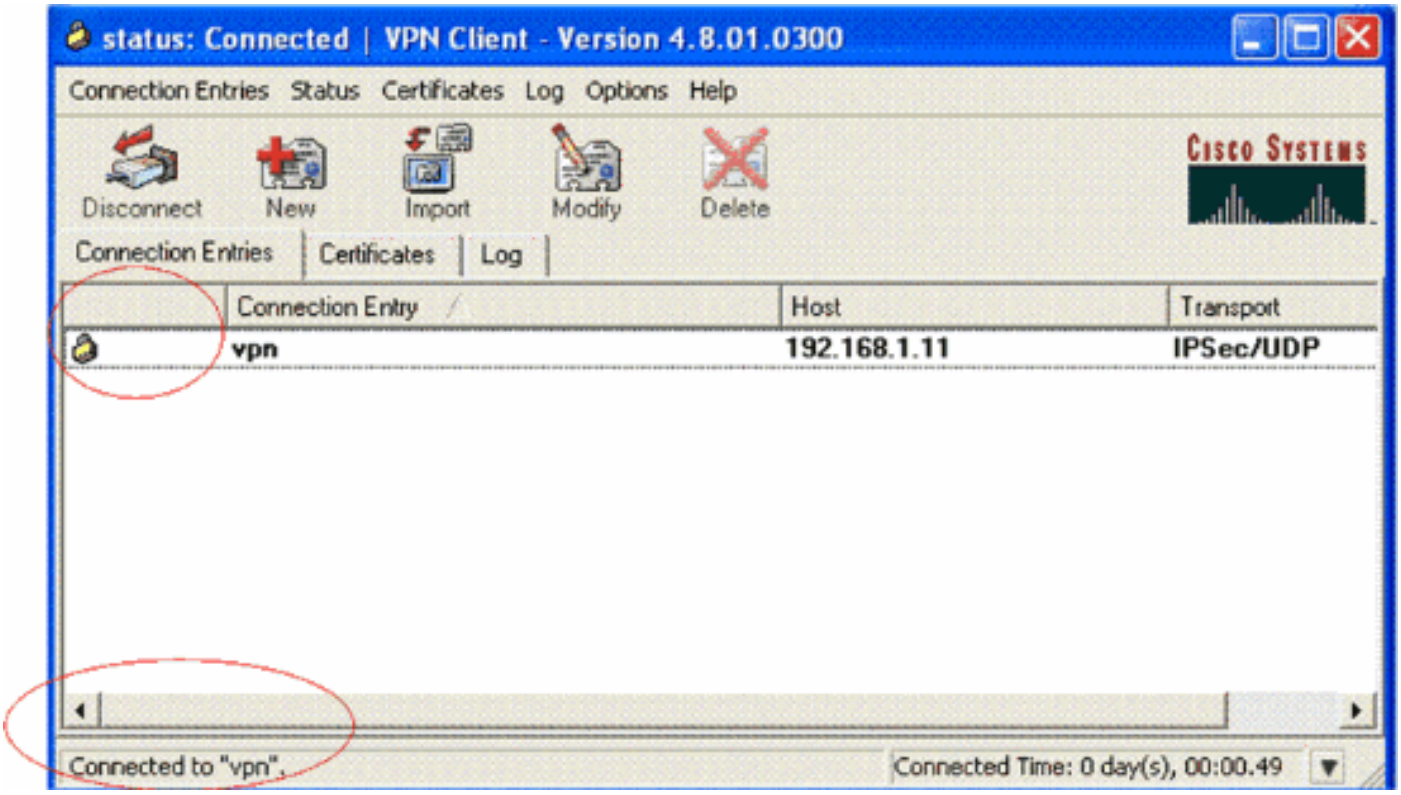


Hinweis: Um diesen VPN-Tunnel einzurichten, müssen der VPN-Client und der Server IP-Erreichbarkeit zwischen ihnen haben. Wenn der VPN-Client das Sicherheits-Gateway (VPN-Server) nicht kontaktieren kann, ist der Tunnel nicht eingerichtet, und auf der Clientseite wird ein Warnfeld mit der folgenden Meldung angezeigt:

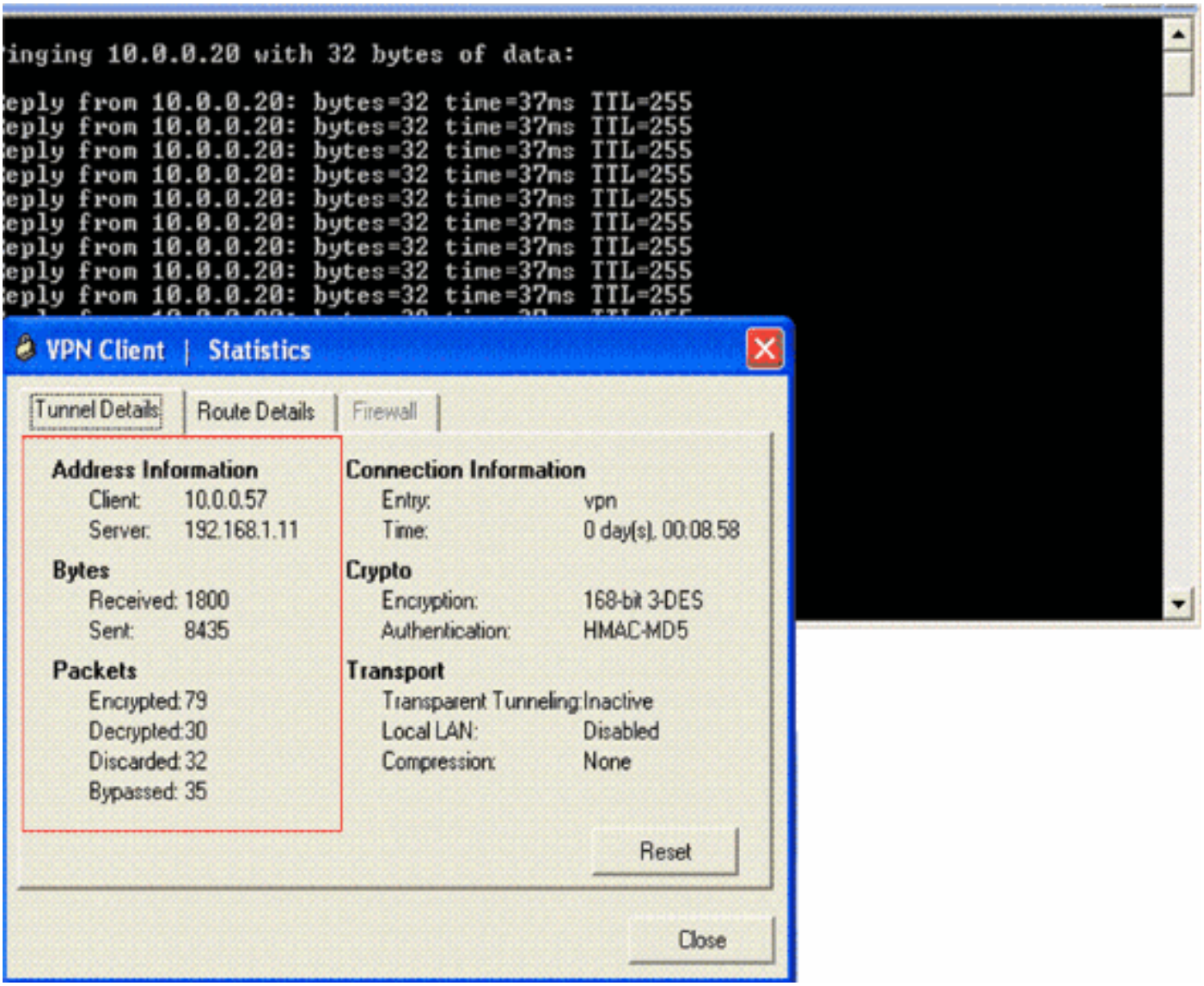
```
Reason 412: The remote peer is no longer responding
```

Um sicherzustellen, dass zwischen Client und Server ein VPN-Tunnel ordnungsgemäß eingerichtet ist, können Sie ein Sperrsymbol finden, das neben dem eingerichteten VPN-Client

erstellt wird. Die Statusleiste zeigt auch **Verbunden mit "vpn"** an. Hier ein Beispiel.



Stellen Sie außerdem sicher, dass Sie die Daten vom VPN-Client aus erfolgreich an das LAN-Segment auf Serverseite übertragen können und umgekehrt. Wählen Sie im Hauptmenü des VPN-Clients **Status > Statistics (Status > Statistik)**. Dort finden Sie die Statistiken der verschlüsselten und entschlüsselten Pakete, die durch den Tunnel weitergeleitet werden.



In diesem Screenshot sehen Sie die Client-Adresse als 10.0.0.57. Dies ist die Adresse, die der VPN-Server dem Client aus seinem lokal konfigurierten Pool nach erfolgreicher Phase-1-Aushandlung zuweist. Sobald der Tunnel eingerichtet ist, fügt der VPN-Server dieser zugewiesenen DHCP-IP-Adresse in der Routing-Tabelle automatisch eine Route hinzu.

Sie sehen auch, wie die Anzahl der verschlüsselten Pakete zunimmt, während die Daten vom Client zum Server übertragen werden, und wie die Anzahl der entschlüsselten Pakete während einer umgekehrten Datenübertragung zunimmt.

Hinweis: Da der WLC für den VPN-Passthrough-Modus konfiguriert ist, kann der Client nur auf das Segment zugreifen, das mit dem VPN-Gateway verbunden ist (hier ist dies der 192.168.1.11-VPN-Server), der für den Pass-Through konfiguriert wurde. Dadurch wird der gesamte andere Datenverkehr gefiltert.

Sie können dies überprüfen, indem Sie einen anderen VPN-Server mit derselben Konfiguration konfigurieren und einen neuen Verbindungseintrag für diesen VPN-Server auf dem VPN-Client konfigurieren. Wenn Sie jetzt versuchen, einen Tunnel zu diesem VPN-Server einzurichten, ist dieser nicht erfolgreich. Der Grund hierfür ist, dass der WLC diesen Datenverkehr filtert und einen Tunnel nur zur für den VPN-Passthrough konfigurierten VPN-Gateway-Adresse zulässt.

Sie können die Konfiguration auch über die CLI des VPN-Servers überprüfen.

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

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Diese **show**-Befehle, die auf dem VPN-Server verwendet werden, können auch hilfreich sein, um Ihnen bei der Überprüfung des Tunnelstatus zu helfen.

- Der Befehl **show crypto session** dient zur Überprüfung des Tunnelstatus. Hier ist eine Beispielausgabe dieses Befehls.

```
Crypto session current status

Interface: Serial3/0
Session status: UP-ACTIVE
Peer: 172.16.1.20 port 500
  IKE SA: local 192.168.1.11/500 remote 172.16.1.20/500

Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58
        Active SAs: 2, origin: dynamic crypto map
```

- Die **show crypto isakmp-Richtlinie** wird verwendet, um die konfigurierten Parameter für Phase 1 anzuzeigen.

Fehlerbehebung

Zur Fehlerbehebung können auch die im Abschnitt Überprüfen erläuterten Befehle **debug** und **show** verwendet werden.

- **debuggen crypto isakmp**
- **debuggen crypto ipsec**
- **Kryptositzung anzeigen**

- Der Befehl **debug crypto isakmp** auf dem VPN-Server zeigt den gesamten Verhandlungsprozess für Phase 1 zwischen Client und Server an. Dies ist ein Beispiel für eine erfolgreiche Phase-1-Aushandlung.

```
------------------------------------------------------------------
 ----------------------------------------------------------
----------------------------------------------------------------
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 14
   against priority 1 policy
*Aug 28 10:37:29.515: ISAKMP:      encryption DES-CBC
*Aug 28 10:37:29.515: ISAKMP:      hash MD5
*Aug 28 10:37:29.515: ISAKMP:      default group 2
*Aug 28 10:37:29.515: ISAKMP:      auth pre-share
*Aug 28 10:37:29.515: ISAKMP:      life type in seconds
*Aug 28 10:37:29.515: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
*Aug 28
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):SA authentication status:
authenticated
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process initial contact,
  bring down existing phase 1 and 2 SA's with local 192.168.1.11
  remote 172.16.1.20 remote port 500
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to
```

```
  the address pool: 10.0.0.57
*Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address 10.0.0.57 to pool
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact, deleting SA
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade
  1583442981 to QM_IDLE
*Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY
  RESPONDER_LIFETIME protocol 1
spi 1689265296, message ID = 1583442981
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending packet to
  172.16.1.20 my_port 500 peer_port 500 (R) QM_IDLE
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):purging node 1583442981
*Aug 28 10:37:29.967: ISAKMP: Sending phase 1 responder lifetime 86400

*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Old State = IKE_R_AM2
  New State = IKE_P1_COMPLETE
```

- Der Befehl **debug crypto ipsec** auf dem VPN-Server zeigt die erfolgreiche Phase 1-IPsec-Aushandlung und Erstellung des VPN-Tunnels an. Hier ein Beispiel:

```
-------------------------------------------------------------------------
 -------------------------------------------------------------------------
-------------------------------------------------------------------------
*Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages
*Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA
from 192.168.1.11 to 172.16.1.20 for prot 3
*Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for
  peer or rekeying for peer 172.16.1.20
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added
  10.0.0.58 255.255.255.255 via 172.16.1.20 in IP DEFAULT TABLE with tag 0
*Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F
*Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58,
  dest_port 0

*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.11, sa_proto= 50,
    sa_spi= 0x8538A817(2235082775),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.20, sa_proto= 50,
    sa_spi= 0xFFC80936(4291299638),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
```

Zugehörige Informationen

- Einführung in die IP-Sicherheit (IPsec)-Verschlüsselung
- Support-Seite für IPsec-Aushandlung/IKE-Protokoll
- Konfigurieren der IPsec-Netzwerksicherheit
- Fragen und Antworten zu Cisco Easy VPN
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0
- Konfigurationsbeispiel für ACLs in Wireless LAN-Controllern
- Häufig gestellte Fragen zum Wireless LAN Controller (WLC)
- Wireless-Support-Seite
- Technischer Support und Dokumentation für Cisco Systeme