ClientVPN via draadloos LAN met Configuratievoorbeeld van WLC

Inhoud

Inleiding

Dit document introduceert het concept Virtual Private Network (VPN) in een draadloze omgeving. Het document legt de configuraties uit die betrokken zijn bij de implementatie van een VPN-tunnel tussen een draadloze client en een VPN-server via een draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Kennis van WLC's en hoe u de WLC-fundamentele parameters kunt configureren
- Kennis van Wi-Fi Protected Access (WAP) concepten
- Basiskennis van VPN en de soorten VPN
- Kennis van IPsec
- Basiskennis van de beschikbare encryptie-, verificatie- en hashingalgoritmen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco WLC 2006 met versie 4.0.179.8
- Cisco 1000 Series lichtgewicht access point (LAP)
- Cisco 3640 dat Cisco IOS-softwarerelease 12.4(8) draait
- Cisco VPN-clientversie 4.8

Opmerking: Dit document gebruikt een 3640 router als een VPN-server. Om meer geavanceerde beveiligingsfuncties te ondersteunen, kunt u ook een speciale VPN-server gebruiken.

Opmerking: om een router als VPN-server op te kunnen zetten, moet deze een functieset uitvoeren die basisIPsec ondersteunt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Een VPN is een privaat datanetwerk dat wordt gebruikt om de gegevens veilig binnen een privaat netwerk door te geven via de openbare telecommunicatie-infrastructuur zoals het internet. Dit VPN handhaaft de gegevensprivacy door het gebruik van een tunneling protocol en veiligheidsprocedures.

Remote Access VPN

Een configuratie voor externe toegang van VPN wordt gebruikt om VPN-softwareclients zoals mobiele gebruikers veilig toegang te bieden tot gecentraliseerde netwerkbronnen die achter een VPN-server wonen. In Cisco terminologie worden deze VPN servers en cliënten ook de Cisco Easy VPN server en het Cisco Easy VPN Remote-apparaat genoemd.

Een Cisco Makkelijk VPN-apparaat kan Cisco IOS-routers, Cisco PIX-security applicaties, Cisco VPN 3002 hardwareclients en Cisco VPN-client zijn. Ze worden gebruikt om beveiligingsbeleid te ontvangen op een VPN-tunnelverbinding van een Cisco Easy VPN-server. Dit minimaliseert de configuratie vereisten op de verre locatie. De Cisco VPN-client is een softwareclient die op pc's, laptops enzovoort kan worden geïnstalleerd.

Een Cisco Makkelijk VPN-server kan Cisco IOS-routers, Cisco PIX-security applicaties en Cisco VPN 3000 Concentrators zijn.

Dit document gebruikt Cisco VPN-clientsoftware die op een laptop draait als de VPN-client en Cisco 3640 IOS-router als VPN-server. Het document gebruikt de IPsec-standaard om een VPN-tunnel tussen een client en een server op te zetten.

IPsec

IPsec vormt een raamwerk van open standaarden die zijn ontwikkeld door de Internet Engineering Task Force (IETF). IPsec biedt beveiliging voor de transmissie van gevoelige informatie via onbeschermde netwerken zoals het internet.

IPsec biedt een encryptie van netwerkgegevens op het IP-pakketniveau, dat een robuuste veiligheidsoplossing biedt die op standaarden is gebaseerd. De belangrijkste taak van IPsec is het toestaan van de uitwisseling van privé informatie via een onveilige verbinding. IPsec gebruikt encryptie om informatie tegen interceptie of afluisteren te beschermen. Om encryptie echter efficiënt te kunnen gebruiken, moeten beide partijen een geheim delen dat wordt gebruikt voor zowel encryptie als decryptie van de informatie.

IPsec functioneert in twee fasen om de vertrouwelijke uitwisseling van een gedeeld geheim mogelijk te maken:

- Fase 1 — hanteert de onderhandeling van veiligheidsparameters vereist om een veilig kanaal tussen twee IPsec peers te creëren. Fase 1 wordt in het algemeen uitgevoerd door middel van het Internet Key Exchange-protocol (IKE). Als de externe IPsec-peer geen IKE kan uitvoeren, kunt u handmatige configuratie met vooraf gedeelde toetsen gebruiken om fase 1 te voltooien.
- Fase 2 — Gebruikt de beveiligde tunnel ingesteld in Fase 1 om de veiligheidsparameters uit te wisselen die nodig zijn om gebruikersgegevens daadwerkelijk te verzenden. De veilige tunnels die in beide fasen van IPsec worden gebruikt zijn gebaseerd op veiligheidsassociaties (SAs) gebruikt op elk eindpunt van IPsec. SAs beschrijven de veiligheidsparameters, zoals het type van authenticatie en encryptie dat beide eindpunten overeenkomen te gebruiken.

De in fase 2 uitgewisselde veiligheidsparameters worden gebruikt om een IPsec-tunnel te maken die op haar beurt wordt gebruikt voor gegevensoverdracht tussen de VPN-client en de server.

Raadpleeg IPsec configureren voor meer informatie over IPsec en de configuratie ervan.

Zodra een VPN-tunnelverbinding tussen de VPN-client en de server tot stand is gebracht, *worden het beveiligingsbeleid dat op de VPN-server is gedefinieerd naar de client verzonden*. Dit minimaliseert de configuratie-eisen aan de clientzijde.

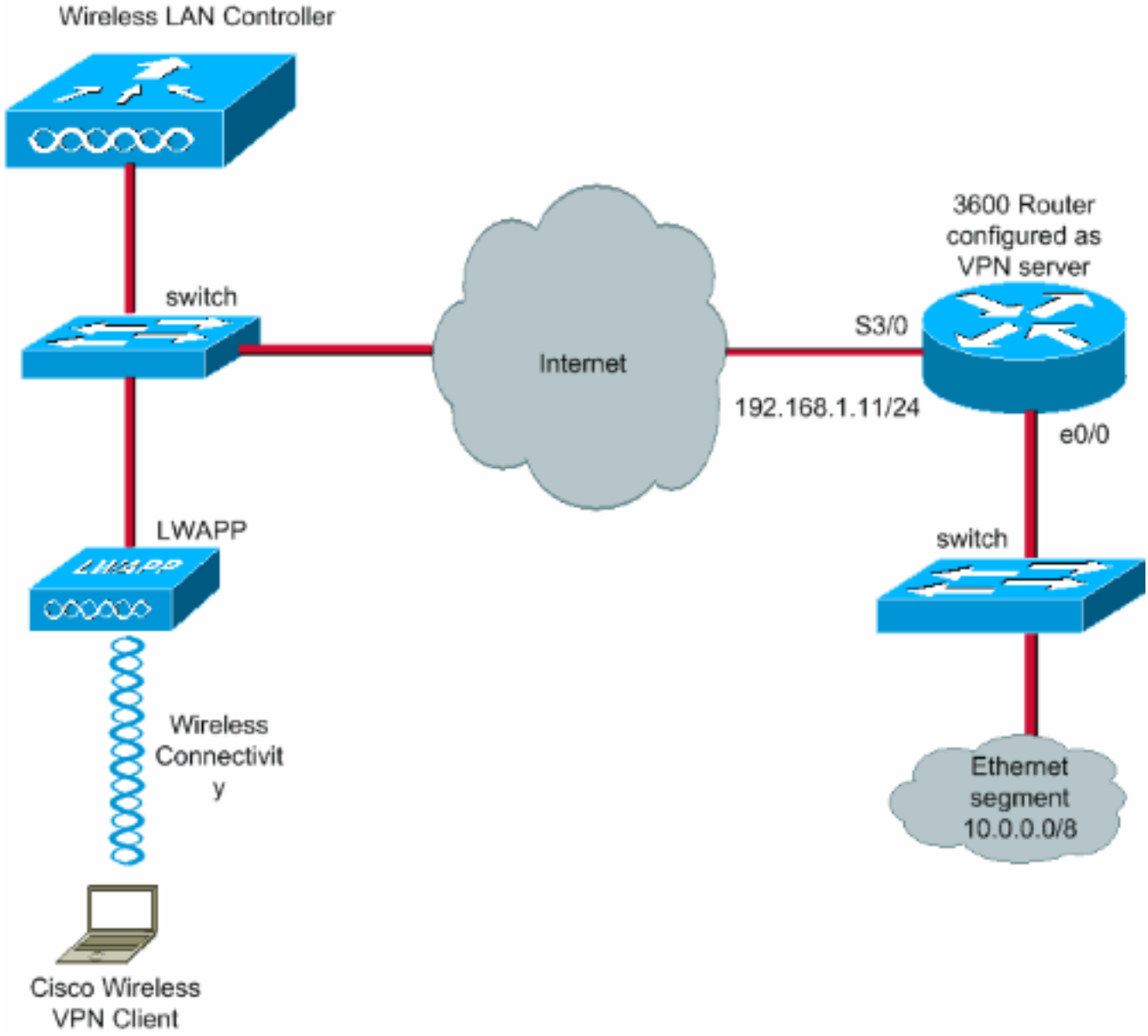
N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Dit document gebruikt deze configuraties:

- IP-adres van de beheerinterface voor het WLC-172.16.1.10/16
- AP-Manager interface IP adres van WLC-172.16.1.11/16
- Standaard gateway—172.16.1.20/16**Opmerking:** In een bewegend netwerk moet deze standaardgateway naar de inkomende interface van de onmiddellijke router wijzen die de WLC met de rest van het netwerk en/of met internet verbindt.
- IP-adres van de VPN-server s3/0-192.168.1.11/24**Opmerking:** Dit IP-adres moet naar de interface wijzen die de VPN-tunnel aan de VPN-serverkant beëindigt. In dit voorbeeld is s3/0 de interface die de VPN-tunnel op de VPN-server beëindigt.

- Het LAN-segment op de VPN-server gebruikt het IP-adresbereik van 10.0.0.0/8.



Configureren

In een WLAN-gecentraliseerde architectuur is het, om een draadloze VPN-client zoals een laptop in staat te stellen een VPN-tunnel aan te leggen met een VPN-server, noodzakelijk dat de client wordt gekoppeld aan een lichtgewicht access point (LAP) dat op zijn beurt bij een WLC moet worden geregistreerd. Dit document heeft de LAP zoals reeds geregistreerd met de WLC met behulp van het lokale SUBNET broadcast-proces dat is uitgelegd in Lichtgewicht AP (LAP)-registratie naar een draadloze LAN-controller (WLC).

De volgende stap is het configureren van de WLC voor VPN.

VPN-beëindiging en -doorvoer

Met Cisco 4000 Series WLCs eerder dan versie 4 wordt een functie die IPsec VPN-beëindiging (IPsec-ondersteuning) wordt genoemd ondersteund. Deze optie stelt deze controllers in staat om VPN-clientsessies rechtstreeks op de controller te beëindigen. Samengevat stelt deze optie de controller in staat om als VPN-server op te treden. Maar dit betekent dat er een afzonderlijke VPN-terminatie hardwaremodule moet worden geïnstalleerd in de controller.

Deze ondersteuning van IPsec VPN is niet beschikbaar in:

- Cisco WLC 2000 Series-switches
- Alle WLC's die versie 4.0 of hoger uitvoeren

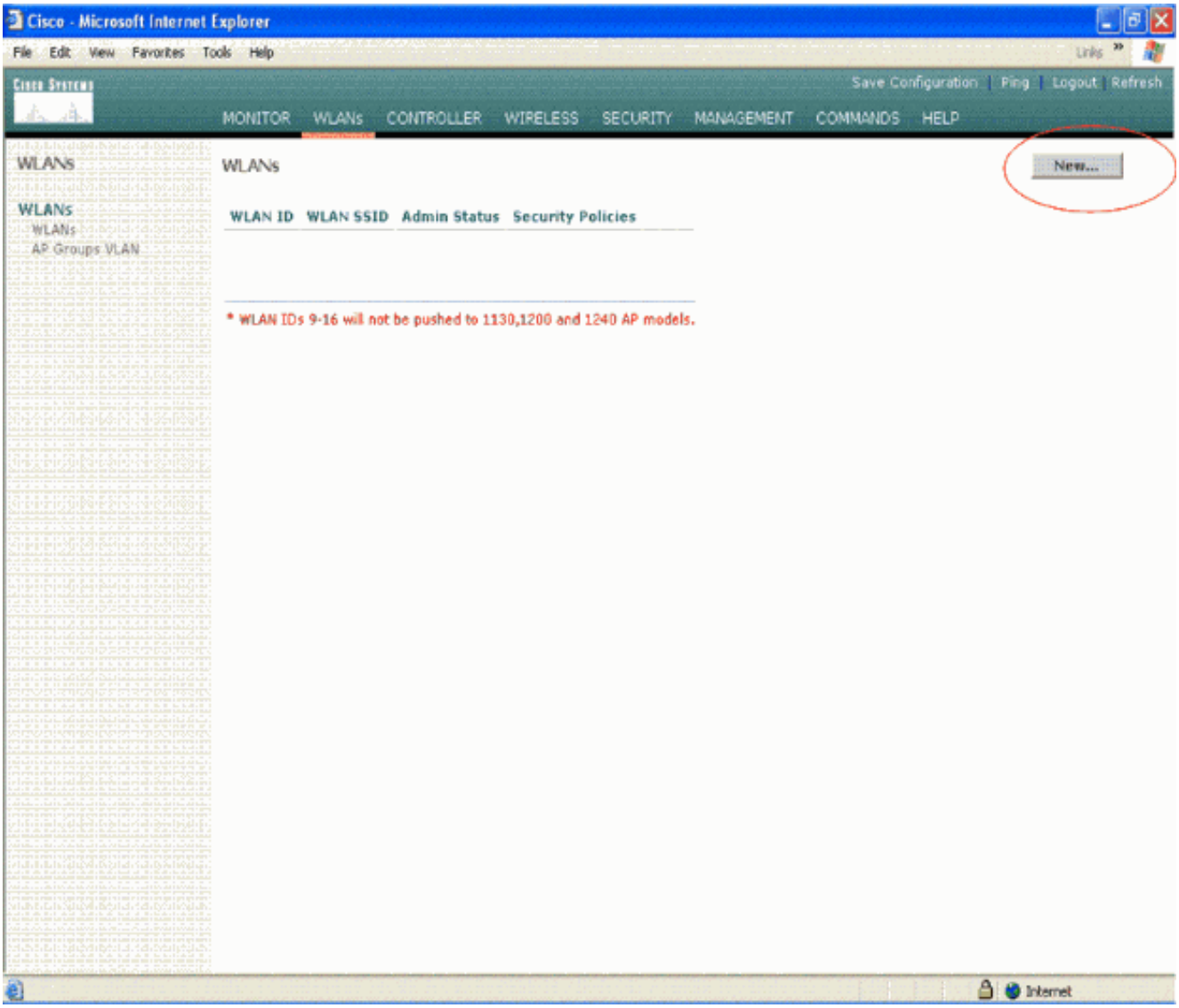
Daarom is de enige functie van VPN die in versies later dan 4.0 wordt ondersteund VPN Pass-Through. Deze optie wordt ook ondersteund in Cisco 2000 Series WLC.

VPN Pass-Through is een functie waarmee een client een tunnel kan aanleggen alleen met een specifieke VPN-server. Dus als u veilig toegang moet hebben tot de geconfigureerde VPN-server, maar ook tot een andere VPN-server of het internet, is dit niet mogelijk met de VPN Pass-Through ingeschakeld op de controller. Onder dergelijke vereisten moet u VPN-doorloop uitschakelen. Maar de WLC kan worden geconfigureerd om als passthrough te fungeren om meerdere VPN-gateways te bereiken wanneer een geschikte ACL wordt gecreëerd en toegepast op de corresponderende WLAN. Dus onder dergelijke scenario's waar u meerdere VPN gateways voor redundantie wilt bereiken, maak VPN passthrough uit en creëer ACL die toegang tot de VPN gateways toestaat en ACL op WLAN toepassen.

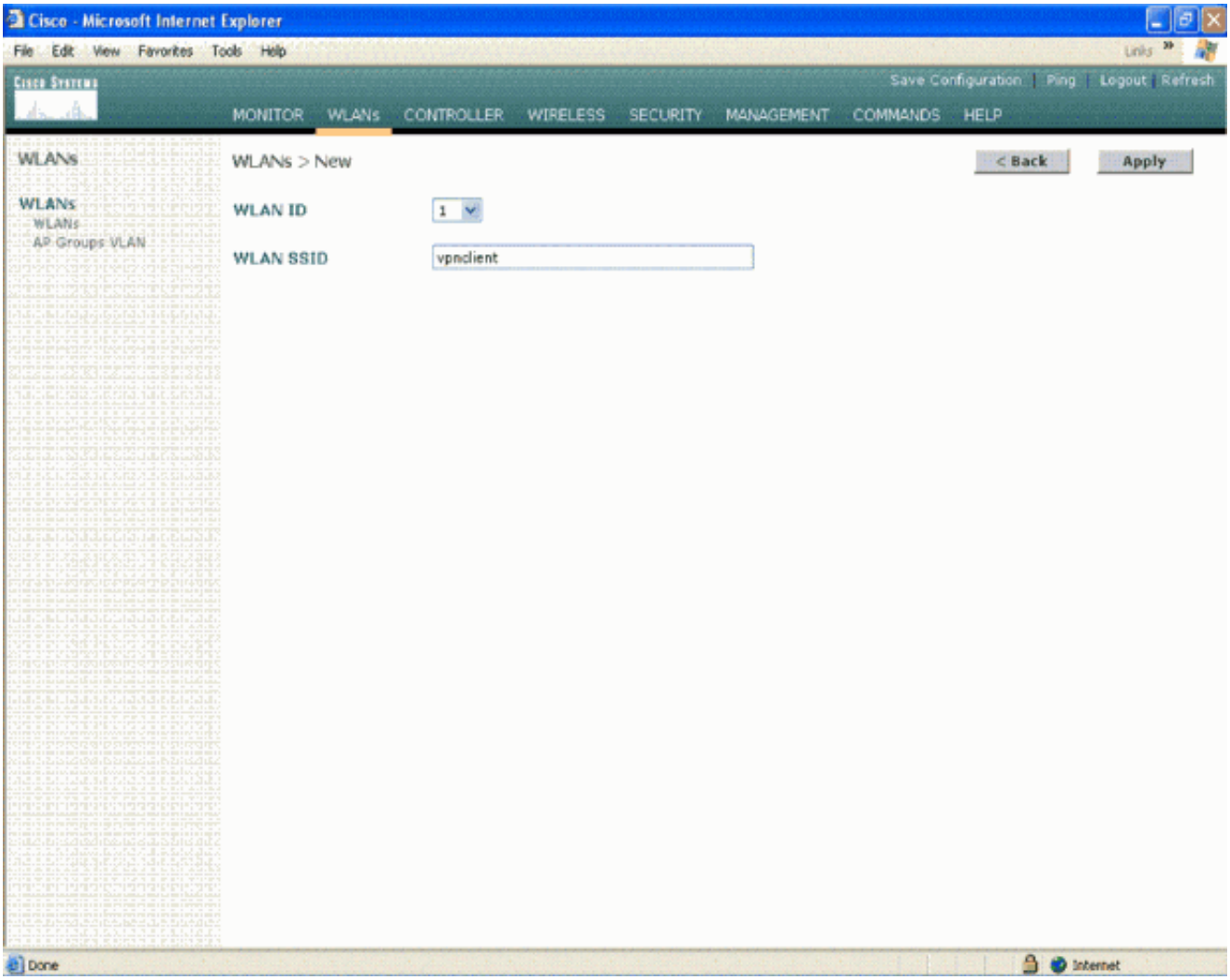
Configureer de WLC voor VPN-doorvoer

Voltooi deze stappen om VPN-doorvoer te configureren.

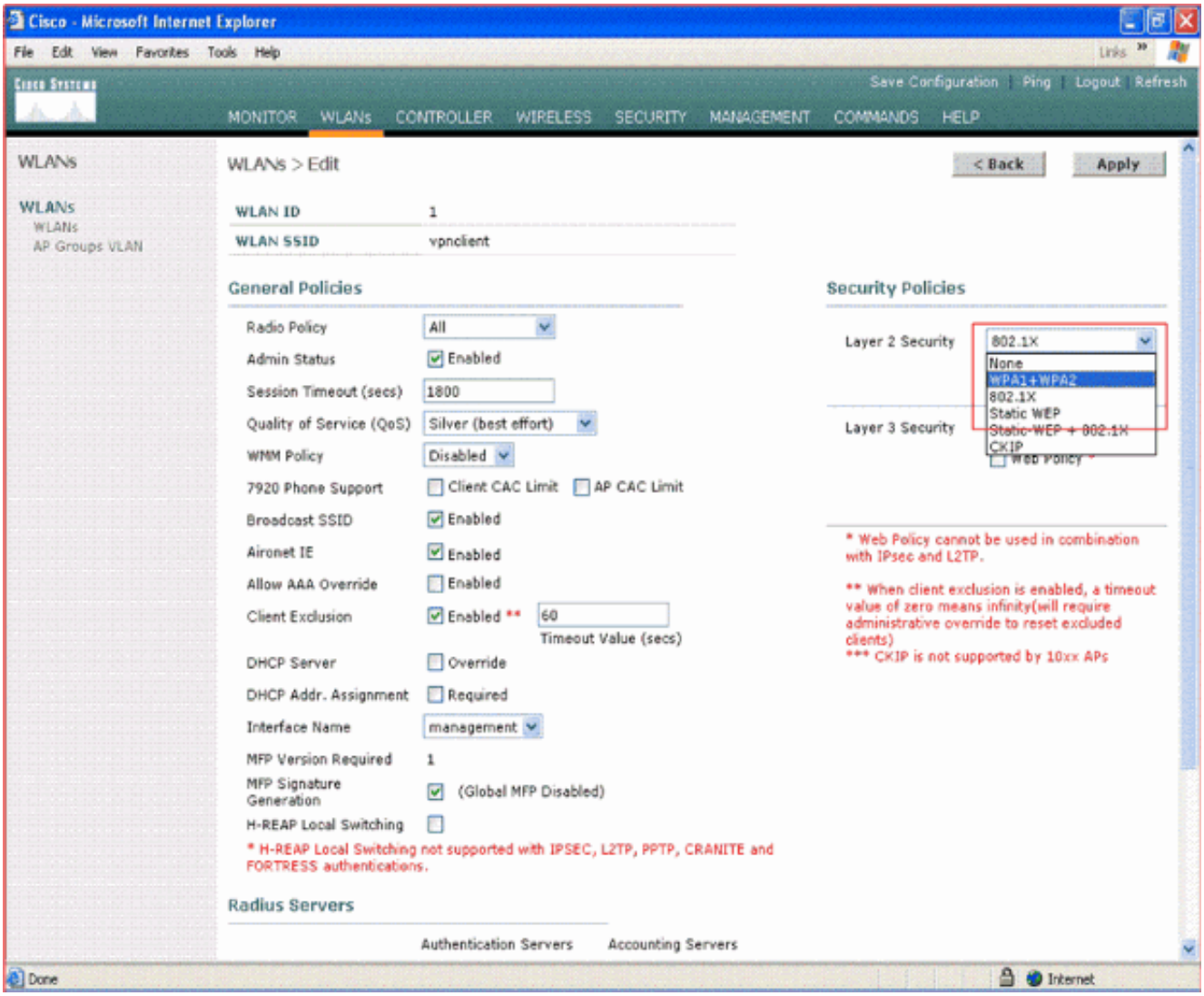
1. Klik vanuit de WLC GUI op **WLAN** om naar de WLAN's pagina te gaan.
2. Klik op **Nieuw** om een nieuw WLAN te maken.



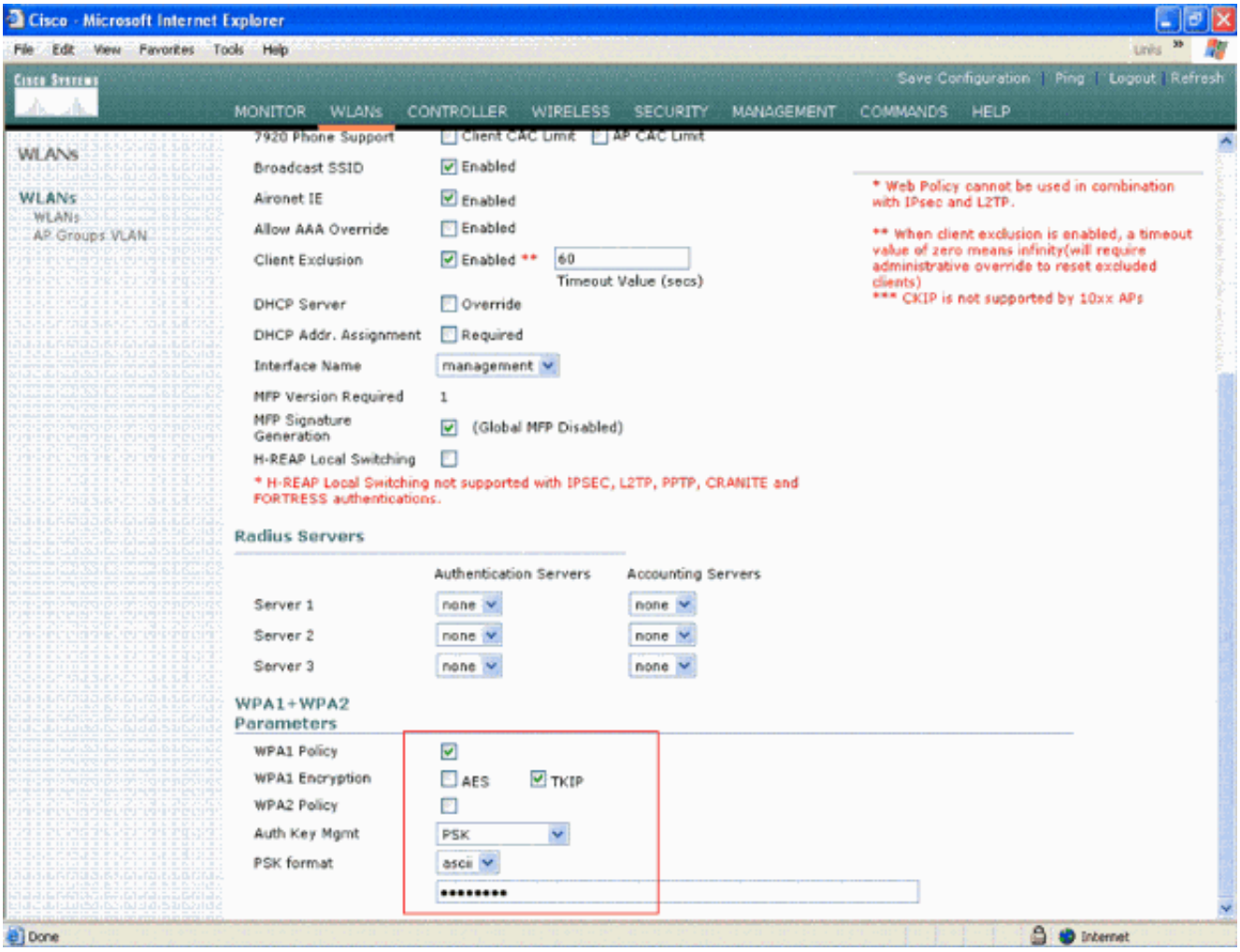
3. WLAN SSID wordt in dit voorbeeld als **VPN-client** genoemd. Klik op Apply (Toepassen).



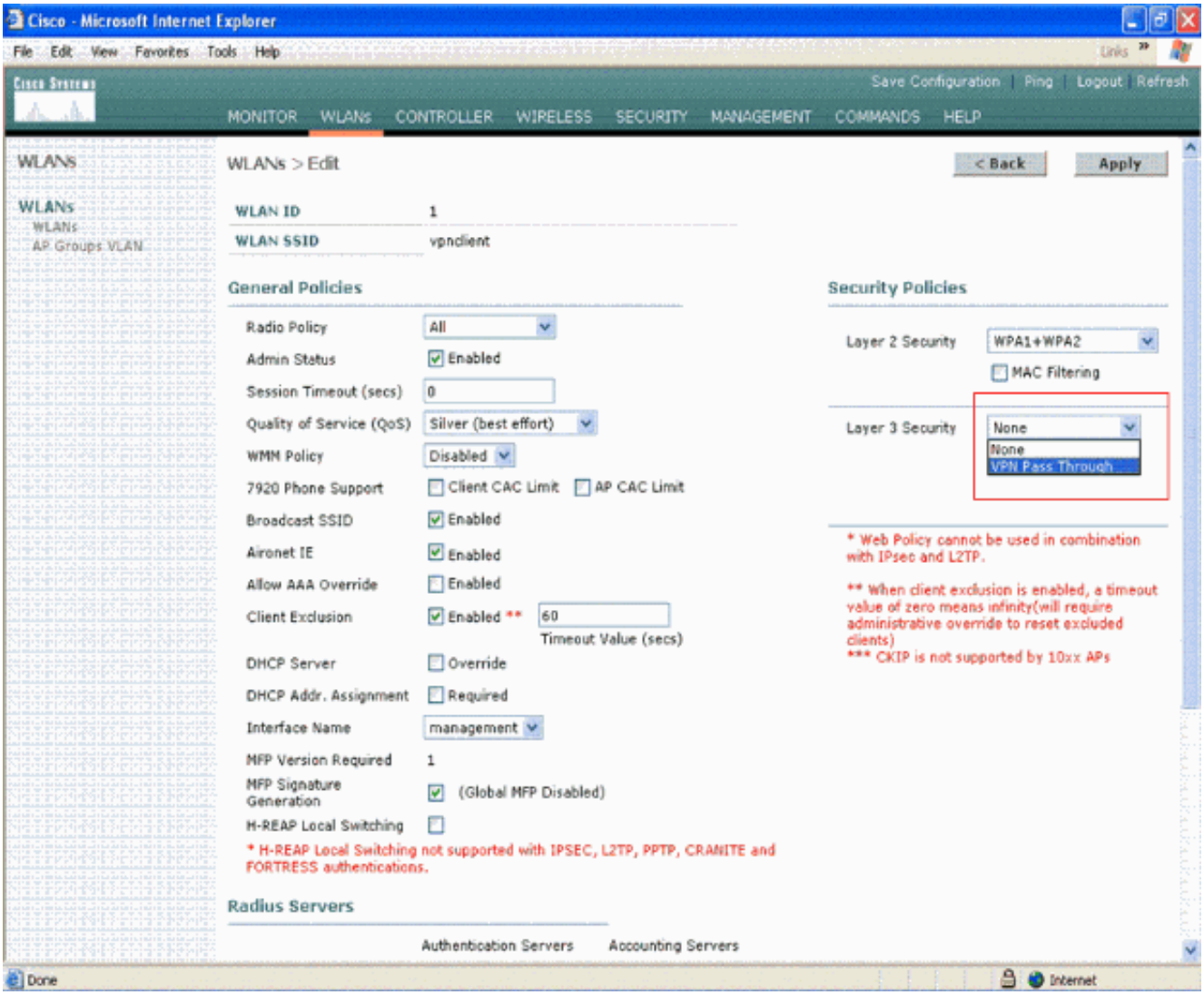
4. Configureer de VPN-client SSID met Layer 2 beveiliging. *Dit is optioneel.*Dit voorbeeld gebruikt **WAP1+WAP2** als beveiligingstype.



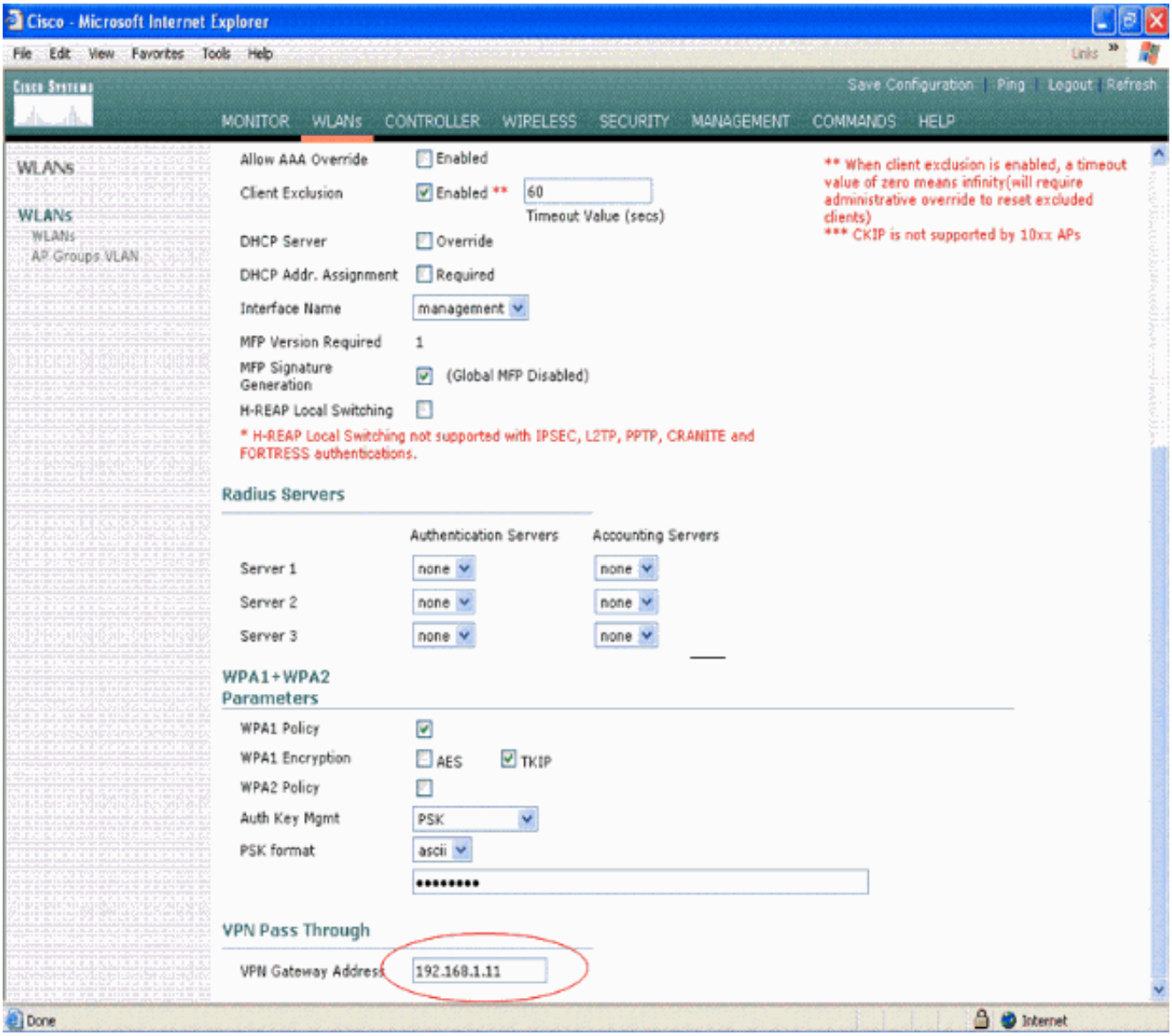
5. Configureer het WAP-beleid en het type verificatiesleutel.Dit voorbeeld gebruikt **Pre-Shared Key (PSK)** voor het beheer van de echtheidskenmerken. Als PSK eenmaal is geselecteerd, selecteert u **ASCII** als de PSK-indeling en typt u de PSK-waarde. Deze waarde zou in de configuratie van SSID van de draadloze client hetzelfde moeten zijn om de klanten die aan deze SSID behoren met deze WLAN te associëren.



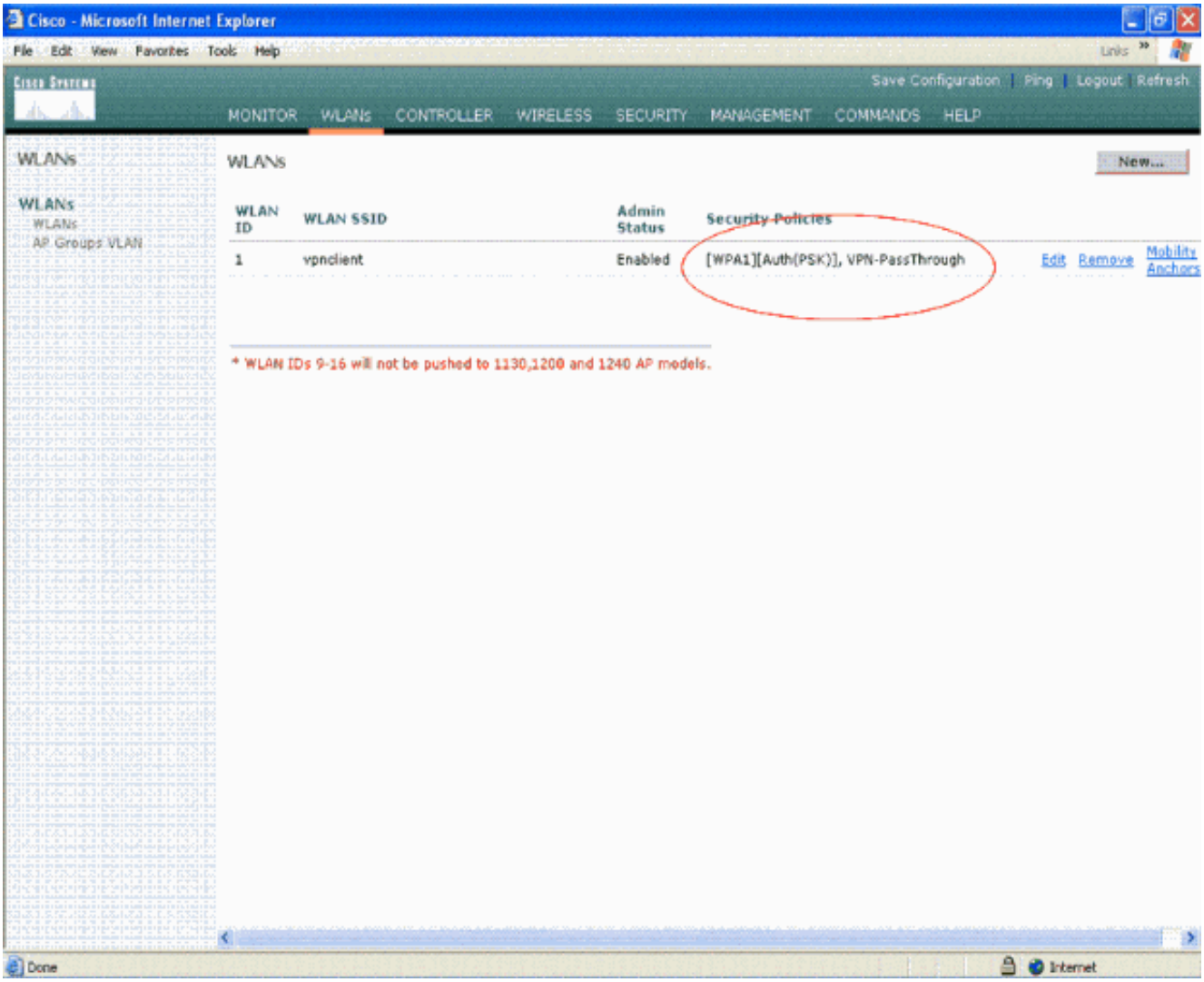
6. Selecteer **VPN Pass-Through** als Layer 3 Security. Hier is het voorbeeld.



7. Wanneer VPN-doorloop is geselecteerd als Layer 3-beveiliging, voegt u het VPN-gatewayadres toe zoals in dit voorbeeld wordt weergegeven.Dit gateway-adres moet het IP-adres van de interface zijn dat de VPN-tunnel aan de serverkant beëindigt. In dit voorbeeld, is het IP adres van de s3/0 interface (192.168.1.11/24) op de server van VPN het te configureren
adres.



8. Klik op **Apply** (Toepassen). De WLAN-*client* is nu geconfigureerd voor VPN-doorvoer.



VPN-serverconfiguratie

Deze configuratie toont Cisco 3640 router als de VPN-server.

Opmerking: Voor eenvoud gebruikt deze configuratie statische routing om IP-bereikbaarheid tussen de eindpunten te behouden. U kunt elk dynamisch routingprotocol gebruiken zoals Routing Information Protocol (RIP), Open Snelste pad eerst (OSPF), enzovoort om bereikbaarheid te behouden.

Opmerking: De tunnel is niet ingesteld als er geen IP-bereikbaarheid tussen de client en de server is.

N.B.: Dit document gaat ervan uit dat de gebruiker weet hoe u dynamische routing in het netwerk kunt inschakelen.

Cisco 3640 router

```
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
```

Toelichting: Dit voorbeeld gebruikt alleen de groepsidentificatie. Het maakt geen gebruik van individuele gebruikersauthenticatie.

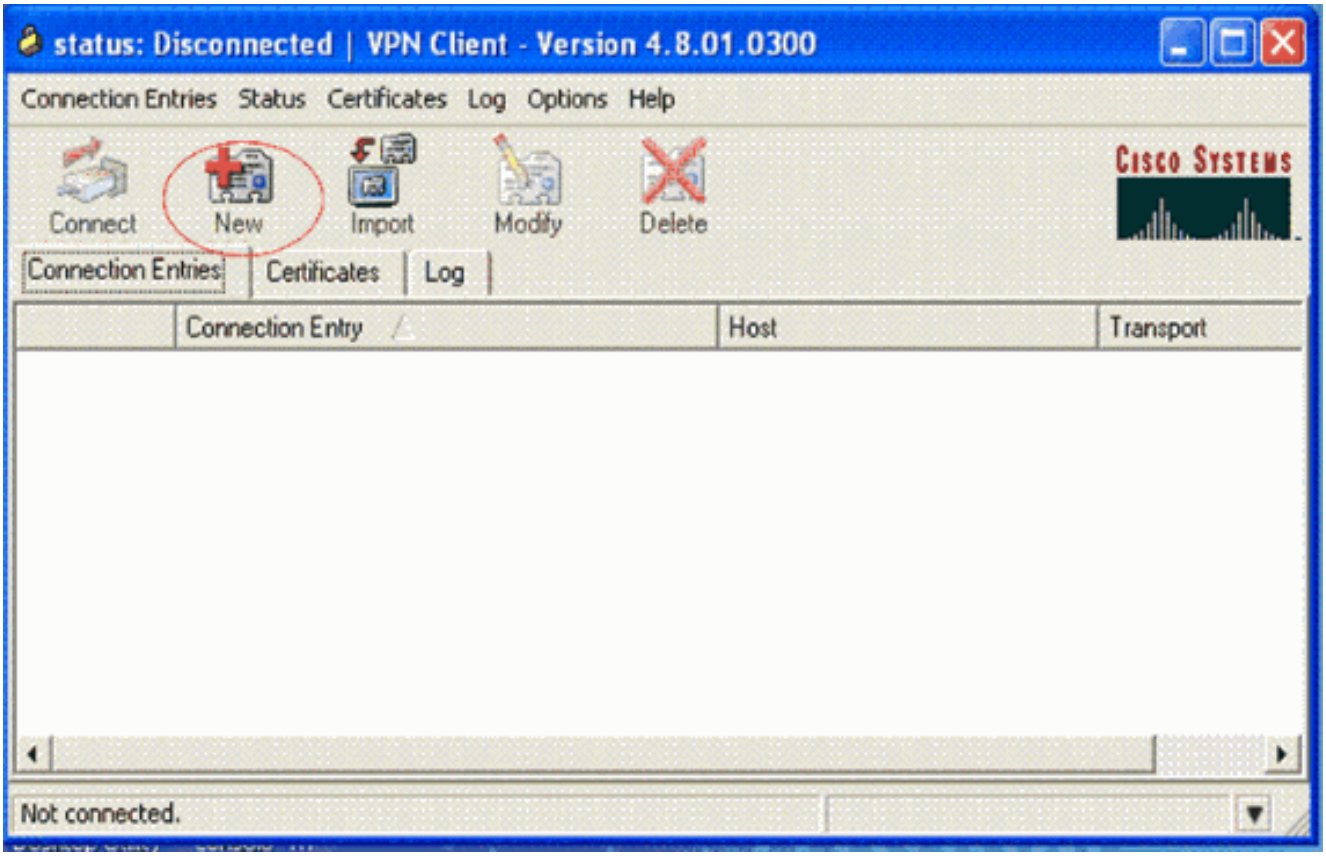
VPN-clientconfiguratie

U kunt een software VPN-client downloaden van het Cisco.com Software Center.

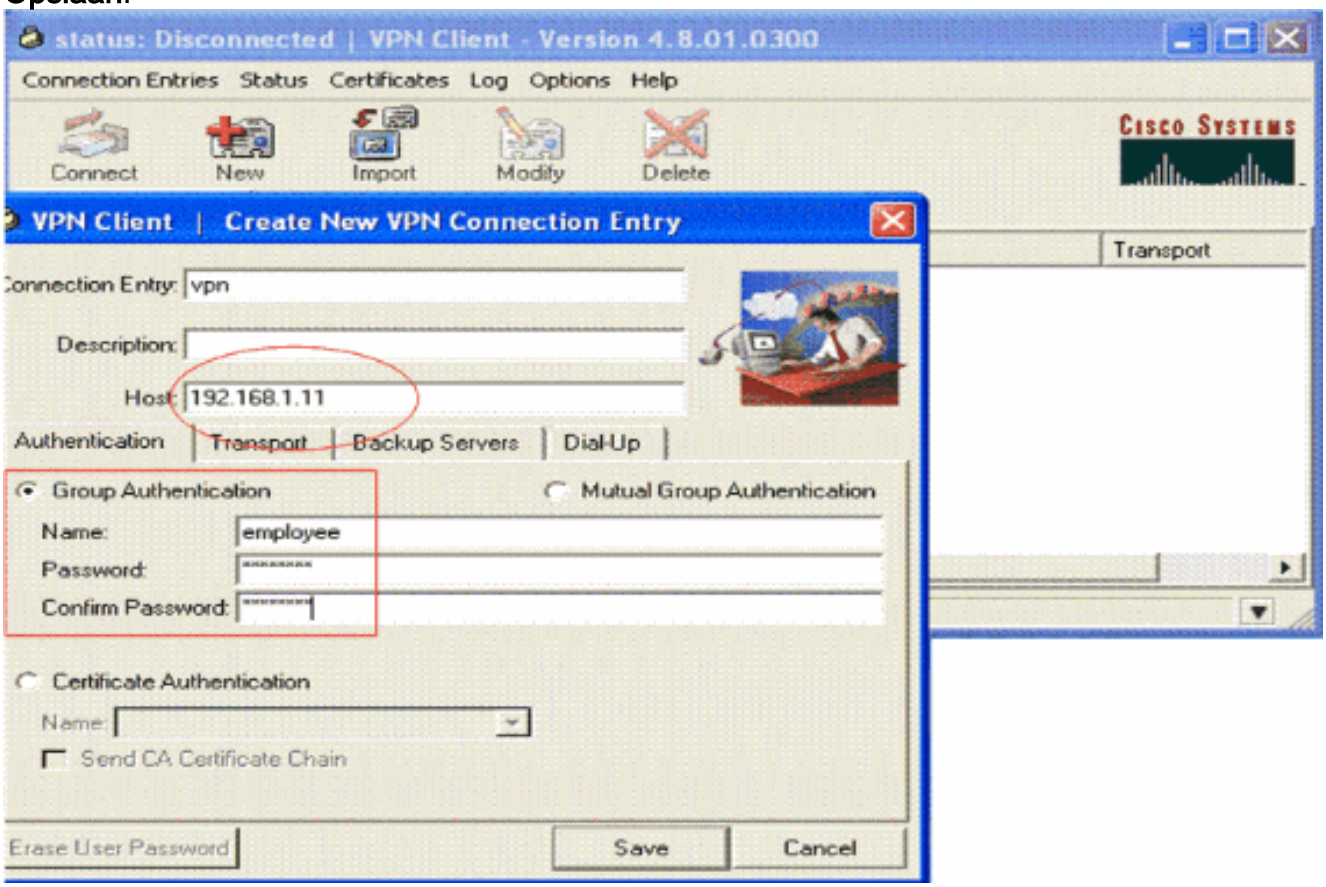
N.B.: Voor sommige software van Cisco dient u met een CCO-gebruikersnaam en -wachtwoord in te loggen.

Voltooi deze stappen om de VPN-client te configureren.

1. Kies **Start > Programma's > Cisco Systems VPN-client > VPN-client** om toegang tot de VPN-client te krijgen. Dit is de standaardlocatie waar de VPN-client is geïnstalleerd.
2. Klik op **Nieuw** om het venster Nieuwe VPN-verbinding maken te starten.



3. Voer de naam van de verbindingsbocht in samen met een beschrijving. In dit voorbeeld *wordt gebruikgemaakt van vpn*.Het veld Description is optioneel. Voer het IP-adres van de VPN-server in het hostvak. Typ vervolgens de VPN-groepsnaam en het wachtwoord en klik op
Opslaan.



Opmerking: De groepsnaam en het wachtwoord dat hier wordt ingesteld, moeten gelijk zijn aan de naam en het wachtwoord die in de VPN-server zijn ingesteld. Dit voorbeeld gebruikt

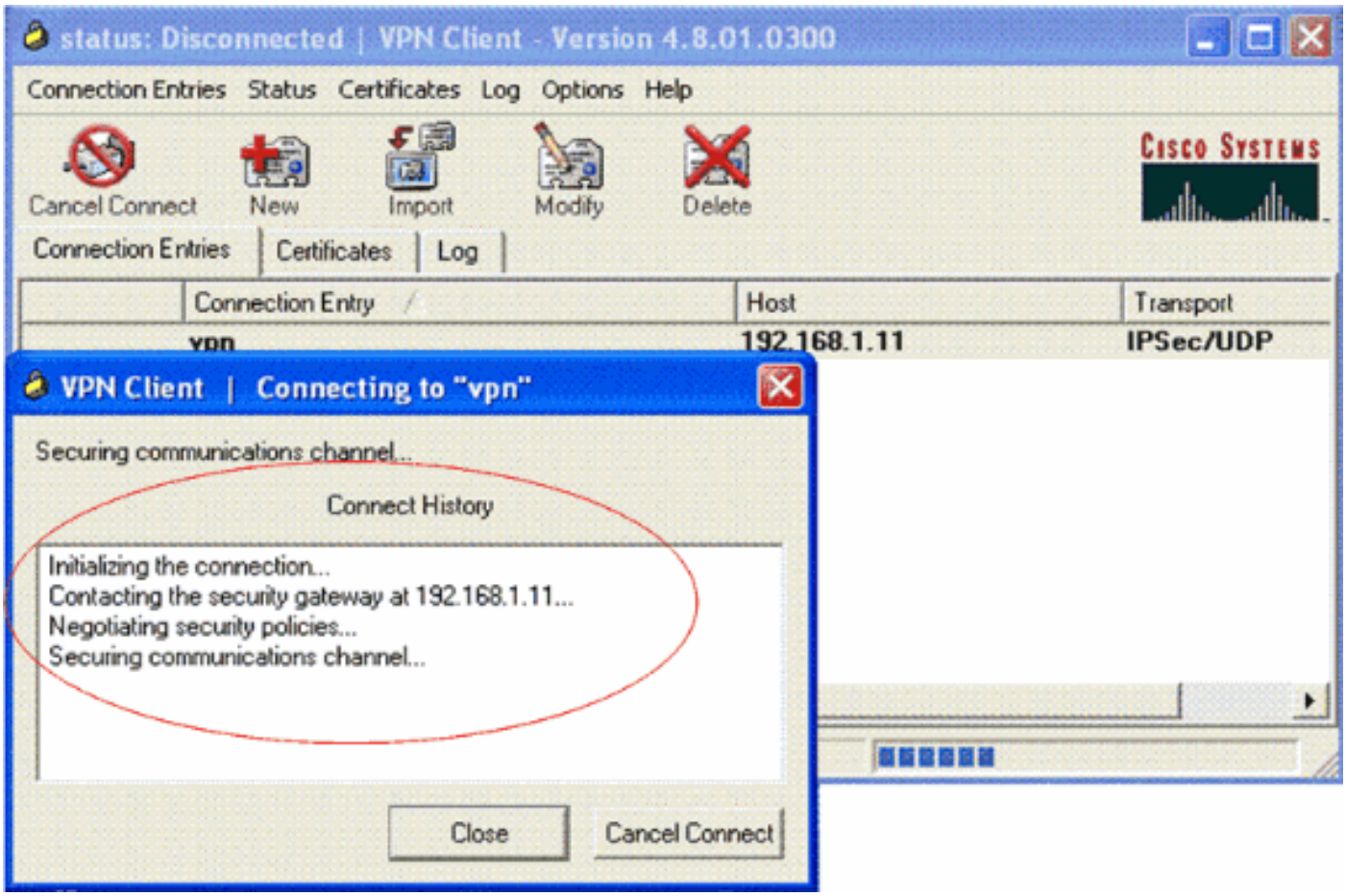
de *medewerker* van de Naam en Wachtwoord *cisco123.*

Verifiëren

Om deze configuratie te verifiëren, moet u de SSID-**client** in de draadloze client configureren met dezelfde beveiligingsparameters die in de WLC zijn geconfigureerd en de client koppelen aan deze WLAN. Er zijn verschillende documenten die uitleggen hoe u een draadloze client met een nieuw profiel kunt configureren.

Nadat de draadloze client is gekoppeld, gaat u naar de VPN-client en klikt u op de verbinding die u hebt ingesteld. Klik vervolgens op **Connect** vanuit het hoofdvenster van VPN-client.

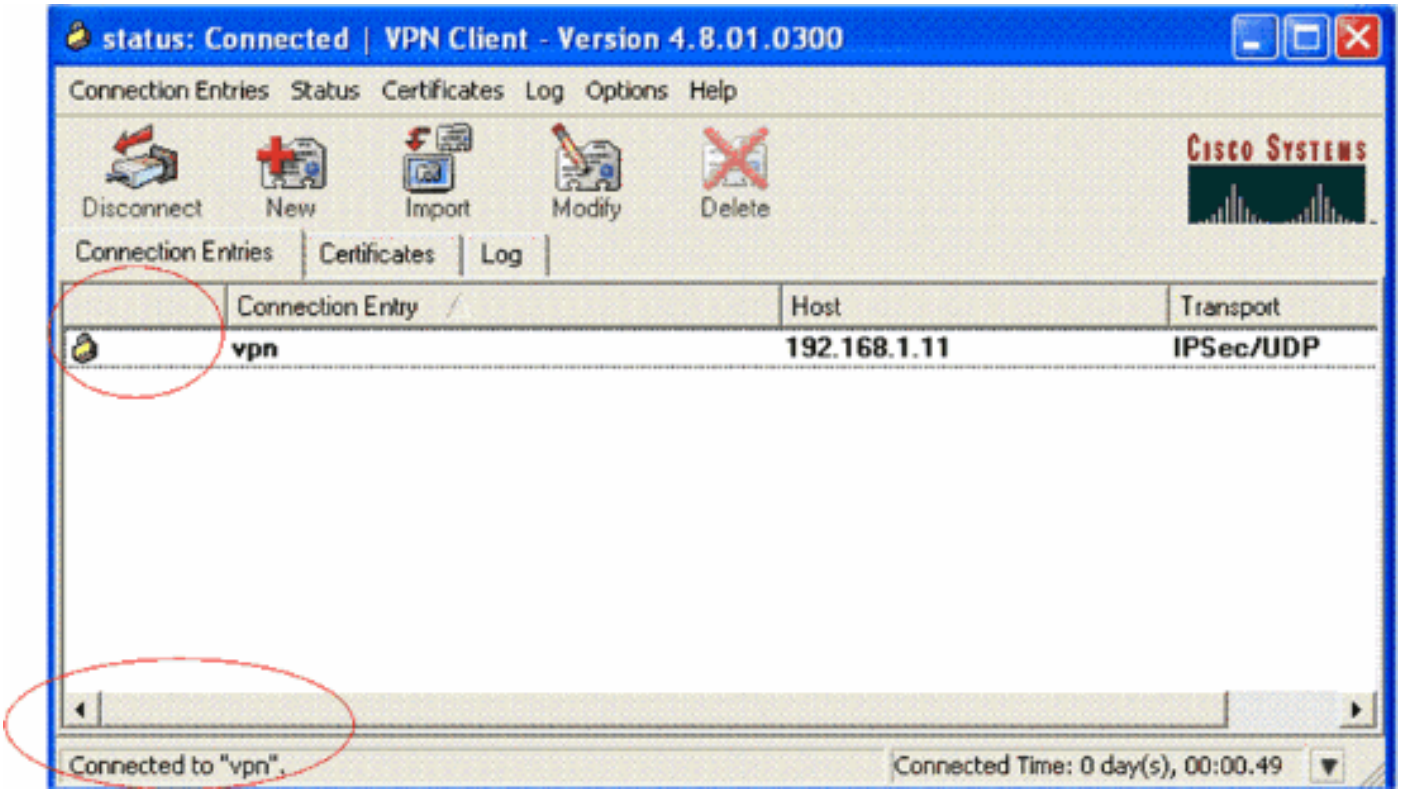
U kunt de beveiligingsparameters fase 1 en fase 2 zien die tussen de client en de server zijn onderhandeld.



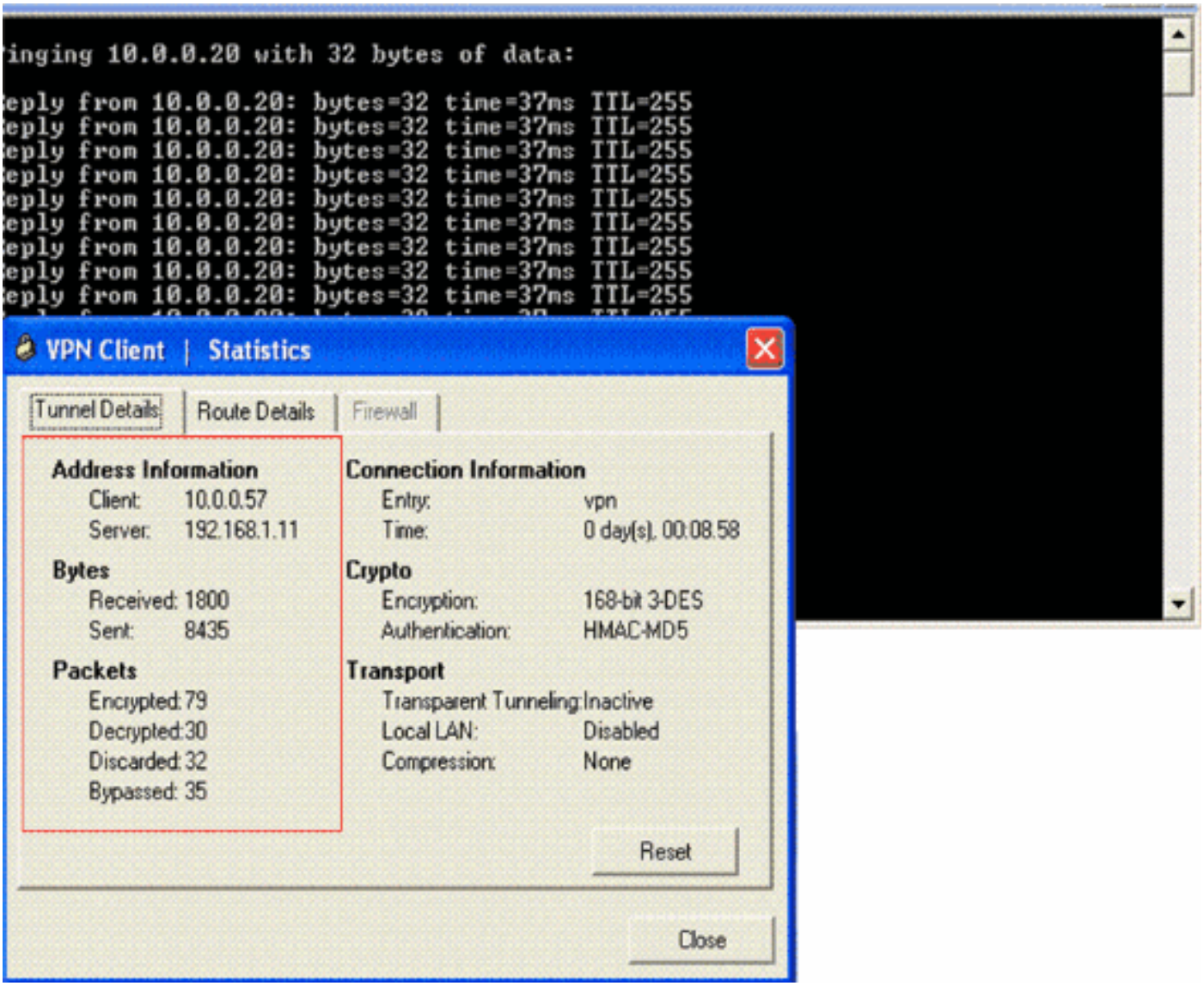
Opmerking: om deze VPN-tunnel in te stellen, moeten de VPN-client en de server IP-bereikbaarheid tussen de tunnels hebben. Als de VPN-client geen contact kan opnemen met de beveiligingsgateway (VPN-server) is de tunnel niet aangelegd en wordt er aan de clientzijde een waarschuwing met dit bericht weergegeven:

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

Om ervoor te zorgen dat een VPN-tunnel goed tussen de client en de server tot stand is gebracht, kunt u een vergrendelingspictogram vinden dat naast de ingestelde VPN-client is gemaakt. De statusbalk geeft ook **aan dat er een verbinding is met "VPN"**. Hierna volgt een voorbeeld.



Zorg er ook voor dat u gegevens met succes kunt verzenden naar het LAN-segment aan de serverkant van de VPN-client en omgekeerd. Kies in het hoofdmenu van VPN Client de optie **Status > Statistieken**. Daar vind je de statistieken van de gecodeerde en gedecrypteerde pakketten die door de tunnel worden doorgegeven.



In dit screenshot kunt u het clientadres zien als 10.0.57. Dit is het adres dat de VPN-server aan de client toekent vanuit de lokaal geconfigureerd pool na succesvolle onderhandeling over fase 1. Zodra de tunnel wordt gevestigd, voegt de server van VPN automatisch een route aan dit toegewezen IP adres van DHCP toe in zijn routingtabel.

U kunt ook het aantal versleutelde pakketten zien toenemen terwijl de gegevens van de client naar de server worden overgebracht en het aantal gedecrypteerde pakketten tijdens een omgekeerde gegevensoverdracht toeneemt.

Opmerking: Aangezien de WLC voor VPN Pass-Through is geconfigureerd, geeft de client toegang tot alleen het segment dat is aangesloten op de VPN-gateway (hier is het 192.168.1.11 VPN-server) die voor Pass-Through is geconfigureerd. Dit filtreert al het andere verkeer.

U kunt dit verifiëren door een andere VPN-server met dezelfde configuratie te configureren en een nieuwe verbinding-ingang voor deze VPN-server aan te passen aan de VPN-client. Wanneer je een tunnel probeert op te zetten met deze VPN server, dan is dat niet succesvol. Dit komt doordat de WLC dit verkeer filters en alleen een tunnel naar het VPN-gateway-adres toestaat dat voor VPN Pass-Through is geconfigureerd.

U kunt de configuratie ook controleren vanuit de CLI van de VPN-server.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten.

Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

Deze **tonen** opdrachten die in de VPN server gebruikt worden kunnen ook nuttig zijn om u te helpen de tunnelstatus te controleren.

- De opdracht **show crypto sessie** wordt gebruikt om de tunnelstatus te controleren. Hier is een voorbeelduitvoer van deze opdracht.

```
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
```

- Het **beleid van de showcrypto isakmp** wordt gebruikt om de geconfigureerde Fase 1-parameters te bekijken.

Problemen oplossen

De opdrachten **debug** en **show** die in de sectie verify zijn uitgelegd, kunnen ook voor probleemoplossing worden gebruikt.

- **debug van crypto isakmp**
- **crypto ipsec debug**
- **show crypto sessie**

- De **debug crypto** opdracht **van** de **tekenherkenning** op de VPN-server toont het gehele fase 1 onderhandelingsproces tussen de client en de server. Hier is een voorbeeld van een succesvolle fase 1 onderhandeling.

```
------------------------------------------------------------------
 ----------------------------------------------------------
------------------------------------------------------------
*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
```

- De **debug crypto ipsec** opdracht op de VPN server toont de succesvolle Fase 1 IPsec onderhandeling en de creatie van de VPN-tunnel. Hierna volgt een voorbeeld:

```
------------------------------------------------------------------------
 ------------------------------------------------------------------------
------------------------------------------------------------------------
*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
```

Gerelateerde informatie

- Inleiding over IP Security (IPsec) encryptie
- Ondersteuning van IPsec-onderhandeling/IKE-protocol
- IPsec-netwerkbeveiliging configureren
- Cisco Makkelijk VPN-v&A
- Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.0
- Configuratievoorbeeld van ACL's op draadloze LAN-controllers
- WLC FAQ (draadloze LAN-controller)
- Draadloze ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems