Esempio di configurazione di Client VPN over Wireless LAN con WLC

Sommario

Introduzione

Questo documento introduce il concetto di VPN (Virtual Private Network) in un ambiente wireless. Il documento spiega le configurazioni coinvolte nella distribuzione di un tunnel VPN tra un client wireless e un server VPN tramite un controller WLC.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza dei WLC e come configurare i parametri base del WLC
- Conoscenza dei concetti di Wi-Fi Protected Access (WPA)
- Conoscenze base di VPN e dei suoi tipi
- Conoscenza di IPsec
- Conoscenze base degli algoritmi di crittografia, autenticazione e hashing disponibili

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 2006 WLC con versione 4.0.179.8
- Cisco serie 1000 Lightweight Access Point (LAP)
- Cisco 3640 con software Cisco IOS® versione 12.4(8)
- Cisco VPN Client versione 4.8

Nota: questo documento utilizza un router 3640 come server VPN. Per supportare funzioni di sicurezza più avanzate, è inoltre possibile utilizzare un server VPN dedicato.

Nota: per funzionare come server VPN, un router deve eseguire un set di funzionalità che supporta il protocollo IPsec di base.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Una VPN è una rete di dati privata che viene utilizzata per trasmettere in modo sicuro i dati all'interno di una rete privata attraverso l'infrastruttura di telecomunicazione pubblica come Internet. Questa VPN mantiene la privacy dei dati tramite l'uso di un protocollo di tunneling e le procedure di sicurezza.

VPN ad accesso remoto

Una configurazione VPN ad accesso remoto viene utilizzata per consentire ai client software VPN, ad esempio gli utenti mobili, di accedere in modo sicuro alle risorse di rete centralizzate che risiedono dietro un server VPN. Nella terminologia Cisco, questi server e client VPN sono chiamati anche server Cisco Easy VPN e dispositivo remoto Cisco Easy VPN.

Un dispositivo remoto Cisco Easy VPN può essere un router Cisco IOS, un'appliance di sicurezza Cisco PIX, client hardware Cisco VPN 3002 e un client VPN Cisco. Vengono utilizzati per ricevere i criteri di sicurezza su una connessione tunnel VPN da un server Cisco Easy VPN. In questo modo si riducono al minimo i requisiti di configurazione della postazione remota. Cisco VPN Client è un client software che può essere installato su PC, laptop e così via.

Un server Cisco Easy VPN può essere un router Cisco IOS, un'appliance di sicurezza Cisco PIX e un concentratore Cisco VPN 3000.

In questo documento viene usato il software Cisco VPN Client che viene eseguito su un laptop come client VPN e il router Cisco 3640 IOS come server VPN. Nel documento viene usato lo

standard IPsec per stabilire un tunnel VPN tra un client e un server.

IPSec

IPsec è una struttura di standard aperti sviluppata dalla Internet Engineering Task Force (IETF). IPsec fornisce la sicurezza per la trasmissione di informazioni sensibili su reti non protette, ad esempio Internet.

IPsec fornisce la crittografia dei dati di rete a livello di pacchetto IP, offrendo una soluzione di sicurezza solida basata su standard. La funzione principale di IPSec è consentire lo scambio di informazioni private su una connessione non protetta. IPsec utilizza la crittografia per proteggere le informazioni da intercettazioni o intercettazioni. Tuttavia, per utilizzare la crittografia in modo efficiente, entrambe le parti devono condividere un segreto utilizzato sia per la crittografia che per la decrittografia delle informazioni.

IPsec opera in due fasi per consentire lo scambio confidenziale di un segreto condiviso:

- Fase 1 - Gestisce la negoziazione dei parametri di sicurezza necessari per stabilire un canale sicuro tra due peer IPsec. La fase 1 viene in genere implementata tramite il protocollo IKE (Internet Key Exchange). Se il peer IPsec remoto non è in grado di eseguire IKE, è possibile utilizzare la configurazione manuale con chiavi già condivise per completare la fase 1.
- Fase 2 - Utilizza il tunnel protetto stabilito nella Fase 1 per scambiare i parametri di sicurezza necessari per la trasmissione effettiva dei dati utente. I tunnel sicuri utilizzati in entrambe le fasi di IPsec si basano sulle associazioni di sicurezza (SA) utilizzate in ciascun endpoint IPsec. Le associazioni di protezione descrivono i parametri di sicurezza, ad esempio il tipo di autenticazione e crittografia che entrambi gli endpoint concordano di utilizzare.

I parametri di sicurezza scambiati nella fase 2 vengono usati per creare un tunnel IPsec che a sua volta viene usato per il trasferimento di dati tra il client VPN e il server.

Per ulteriori informazioni su IPsec e la relativa configurazione, fare riferimento a Configurazione di IPsec.

Una volta stabilito un tunnel VPN tra il client VPN e il server, *i criteri di sicurezza definiti nel server VPN vengono inviati al client*. Ciò riduce al minimo i requisiti di configurazione sul lato client.

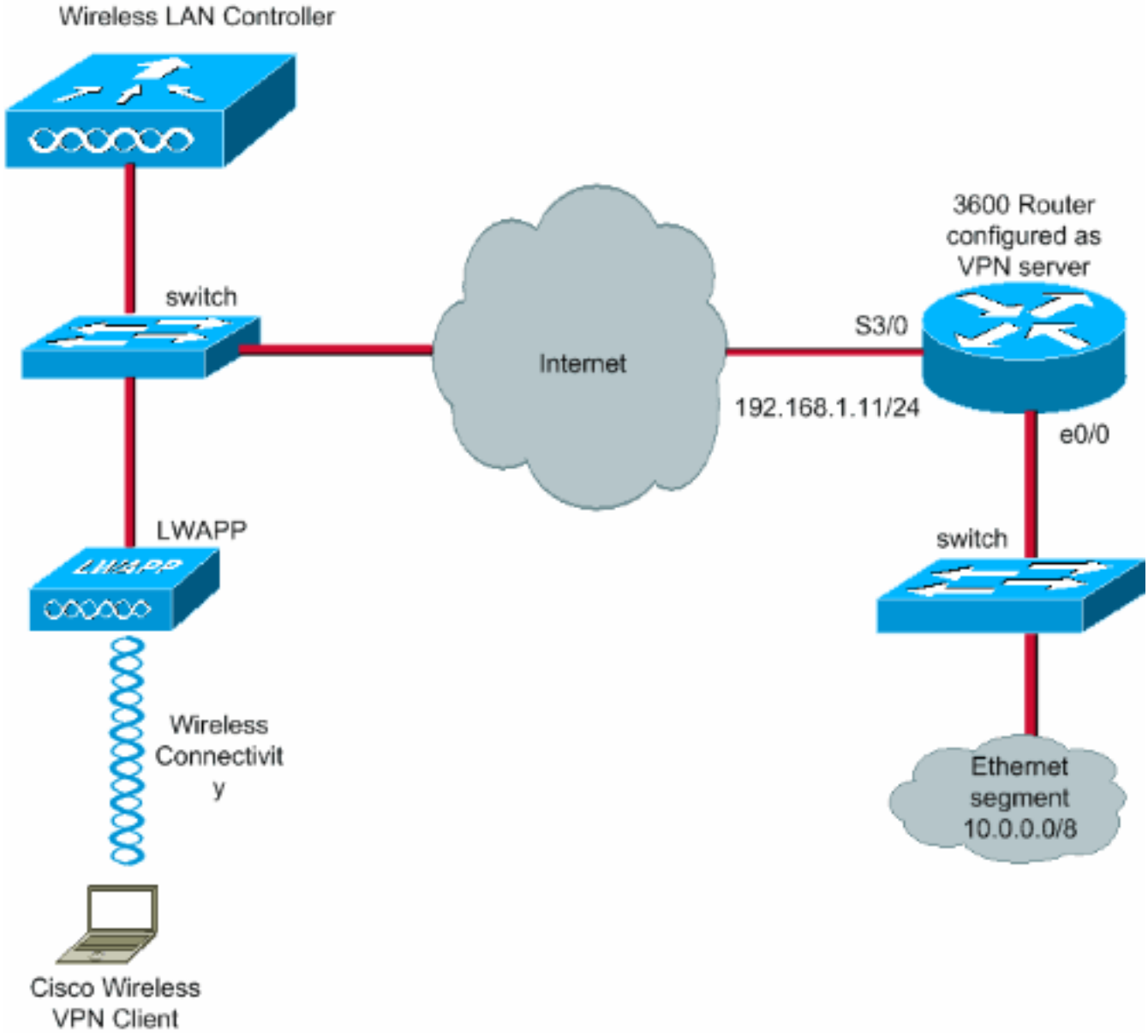
Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento vengono usate queste configurazioni:

- Indirizzo IP dell'interfaccia di gestione del WLC—172.16.1.10/16
- Indirizzo IP dell'interfaccia AP-manager del WLC—172.16.1.11/16
- Gateway predefinito: 172.16.1.20/16**Nota:** in una rete live, questo gateway predefinito deve puntare all'interfaccia in entrata del router immediato che connette il WLC al resto della rete e/o a Internet.
- Indirizzo IP del server VPN s3/0—192.168.1.11/24**Nota:** questo indirizzo IP deve puntare all'interfaccia che termina il tunnel VPN sul lato server VPN. Nell'esempio, s3/0 è l'interfaccia che termina il tunnel VPN sul server VPN.

- Il segmento LAN sul server VPN utilizza l'intervallo di indirizzi IP di 10.0.0.0/8.



Configurazione

In un'architettura centralizzata WLAN, per consentire a un client VPN wireless, ad esempio un laptop, di stabilire un tunnel VPN con un server VPN, è necessario che il client venga associato a un Lightweight Access Point (LAP), che a sua volta deve essere registrato su un WLC. Questo documento ha il LAP già registrato sul WLC usando il processo di rilevamento delle trasmissioni nella subnet locale spiegato in Registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC).

Il passaggio successivo è configurare il WLC per VPN.

Terminazione e pass-through VPN

Sui Cisco serie 4000 WLC precedenti alla versione 4, è supportata una funzione chiamata IPsec VPN terminal (supporto IPsec). Questa funzionalità consente a questi controller di terminare le sessioni client VPN direttamente sul controller. In breve, questa funzionalità consente al controller stesso di agire come server VPN. Tuttavia, è necessario installare un modulo hardware di terminazione VPN separato nel controller.

Questo supporto VPN IPsec non è disponibile in:

- Cisco serie 2000 WLC
- Qualsiasi WLC che esegue la versione 4.0 o successive

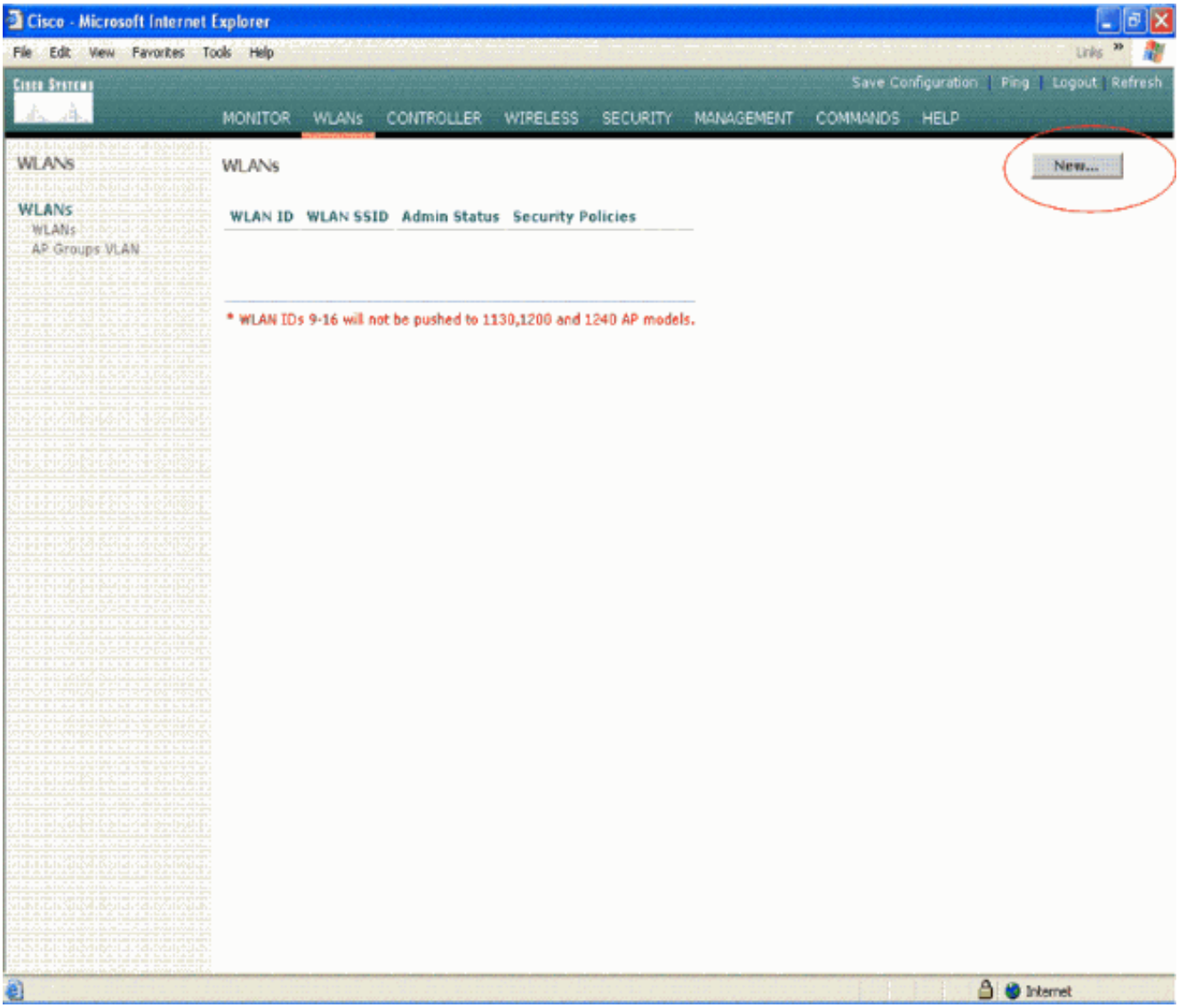
Pertanto, l'unica funzionalità VPN supportata nelle versioni successive alla 4.0 è VPN Pass-through. Questa funzione è supportata anche nei Cisco serie 2000 WLC.

Pass-through VPN è una funzionalità che consente a un client di stabilire un tunnel solo con un server VPN specifico. Pertanto, se è necessario accedere in modo sicuro al server VPN configurato nonché a un altro server VPN o a Internet, ciò non è possibile con il pass-through VPN abilitato sul controller. In base a tali requisiti, è necessario disabilitare il pass-through VPN. Tuttavia, il WLC può essere configurato in modo da funzionare come pass-through per raggiungere più gateway VPN quando viene creato e applicato un ACL appropriato alla WLAN corrispondente. Pertanto, in questi scenari in cui si desidera raggiungere più gateway VPN per la ridondanza, disabilitare il pass-through VPN e creare un ACL che consenta l'accesso ai gateway VPN e applicare l'ACL alla WLAN.

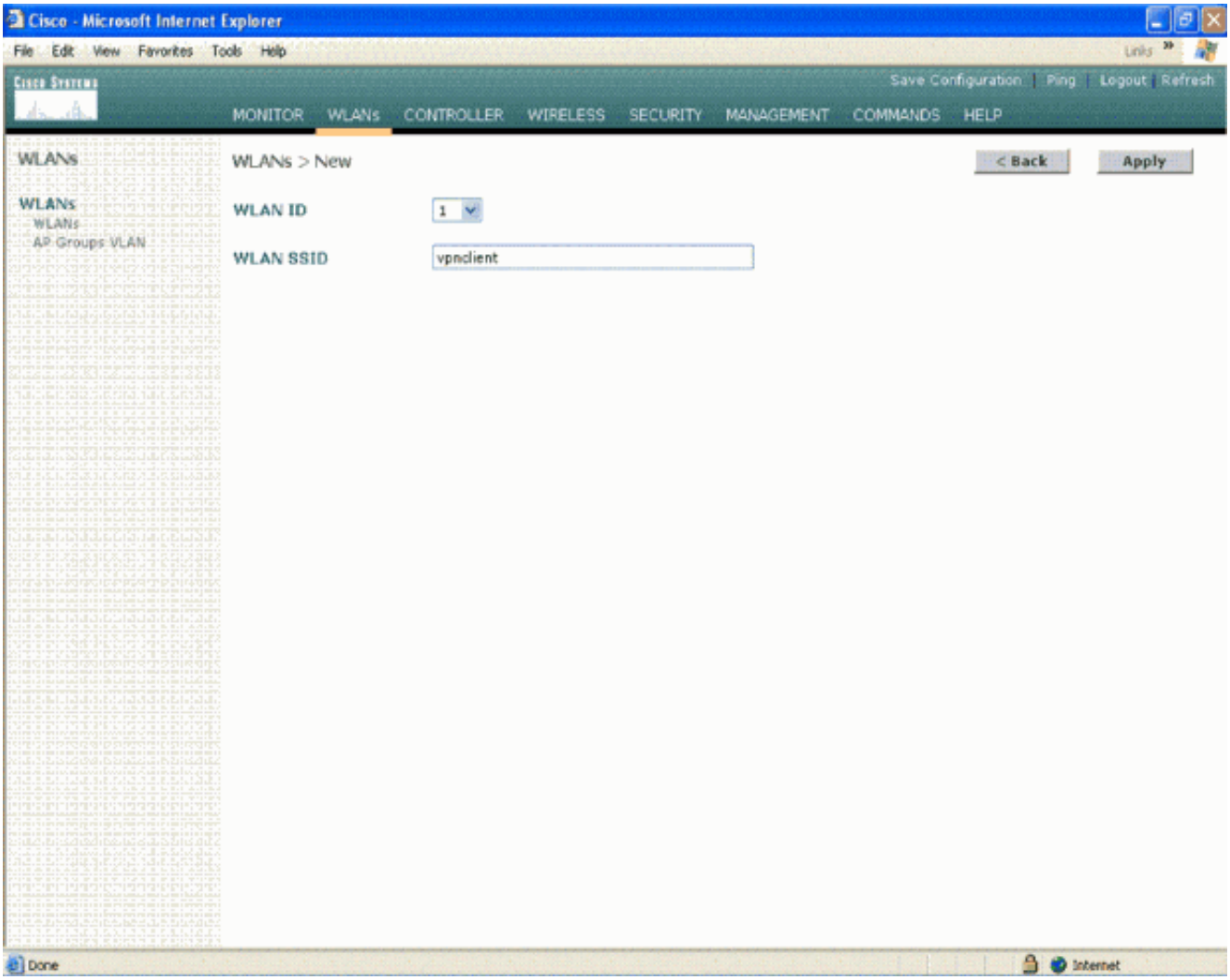
Configurare il WLC per il pass-through VPN

Completare questa procedura per configurare il pass-through VPN.

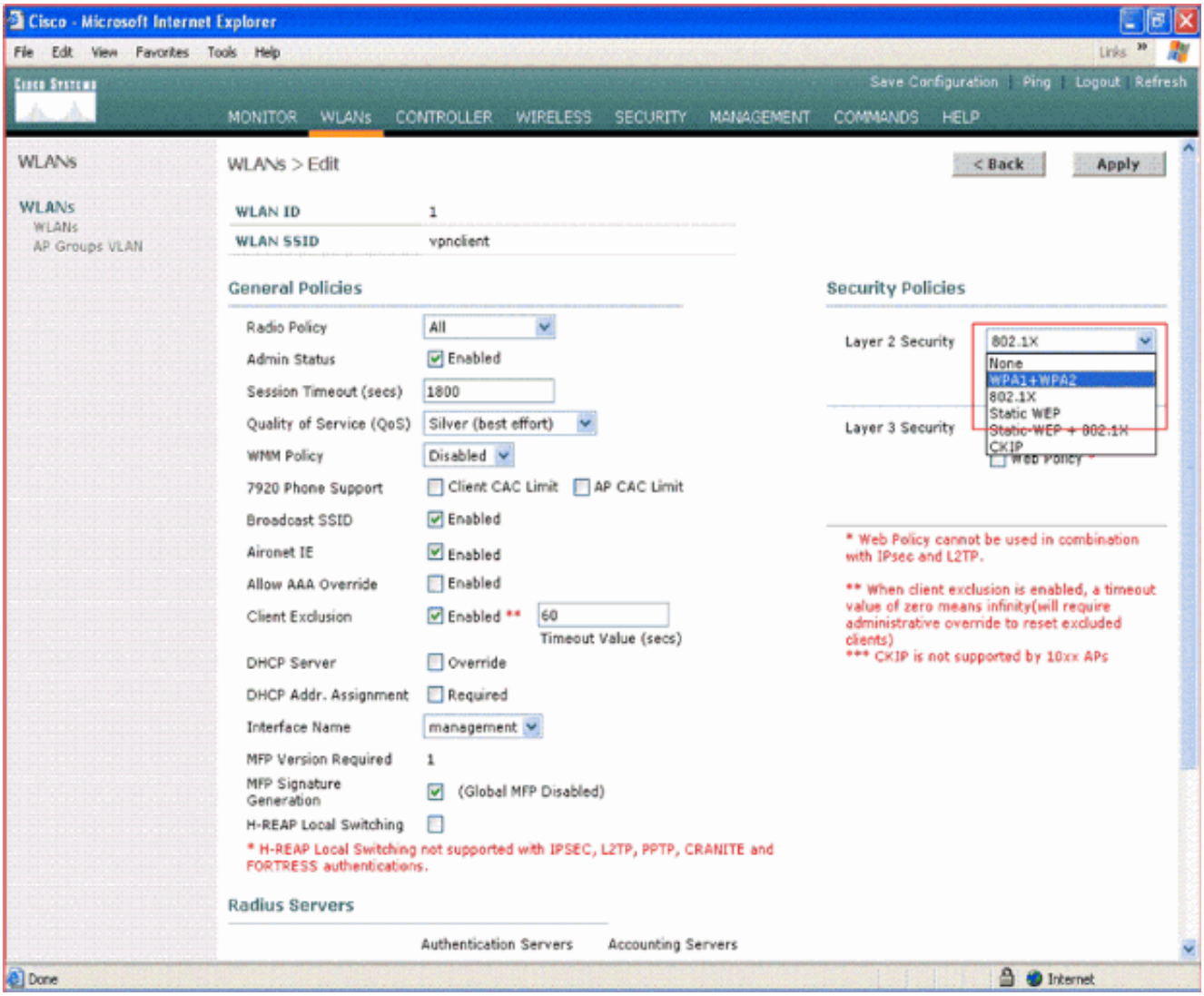
1. Dall'interfaccia utente del WLC, fare clic su **WLAN** per andare alla pagina WLAN.
2. Per creare una nuova WLAN, fare clic su **New** (Nuovo).



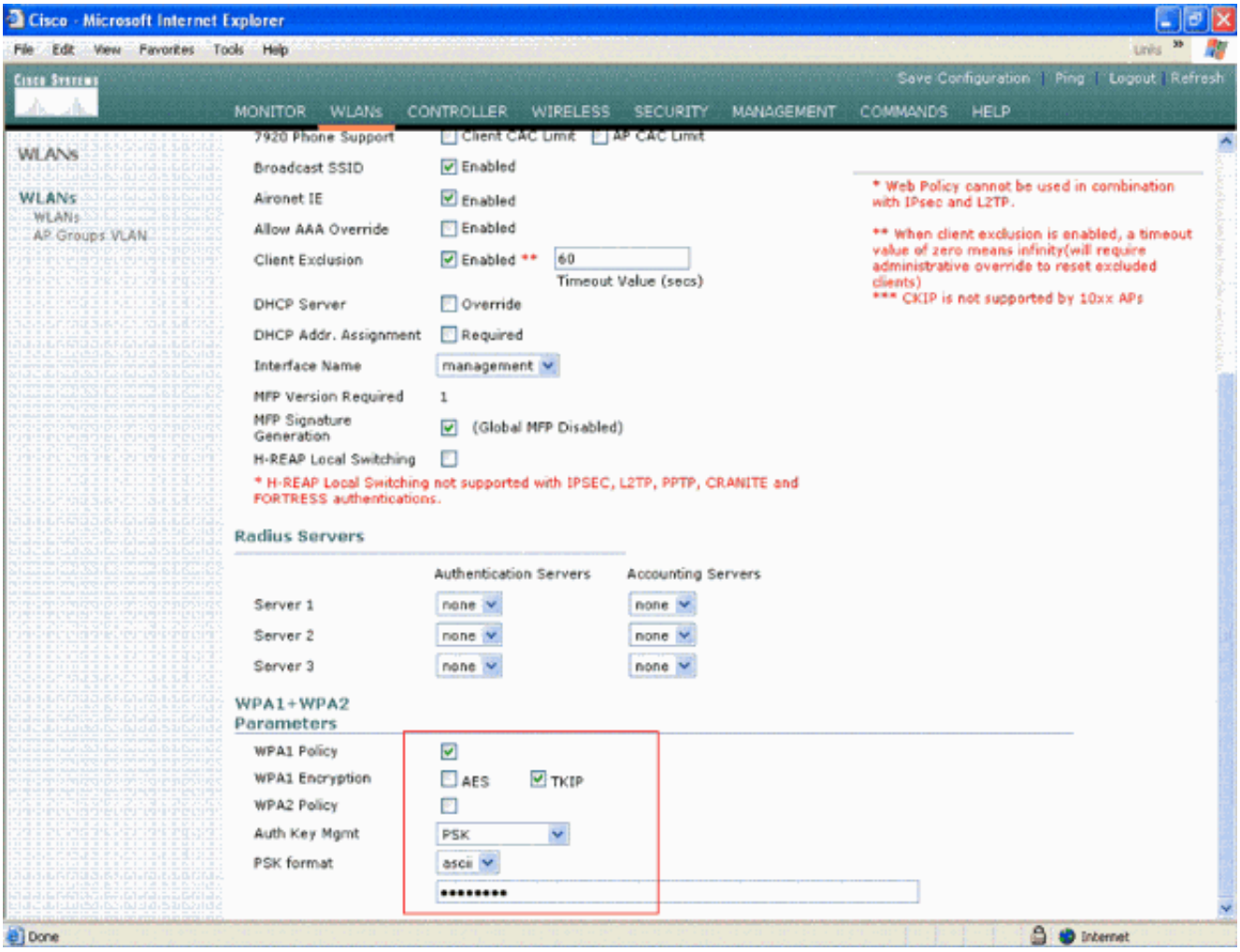
3. Nell'esempio, il nome dell'SSID della WLAN è **vpnclient**. Fare clic su Apply (Applica).



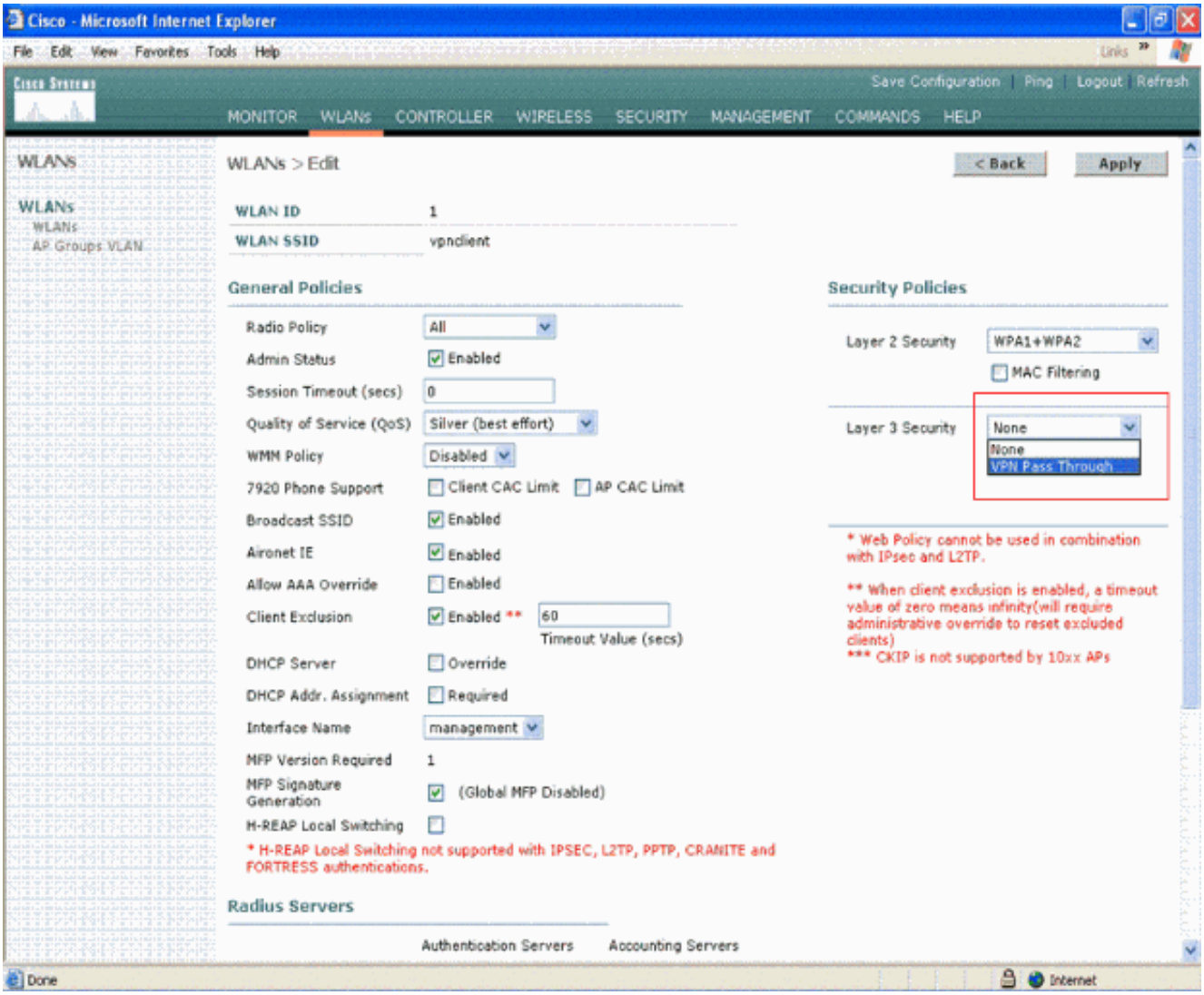
4. Configurare il SSID vpnclient con la sicurezza di layer 2. *Questa operazione è facoltativa.*In questo esempio viene utilizzato **WPA1+WPA2** come tipo di protezione.



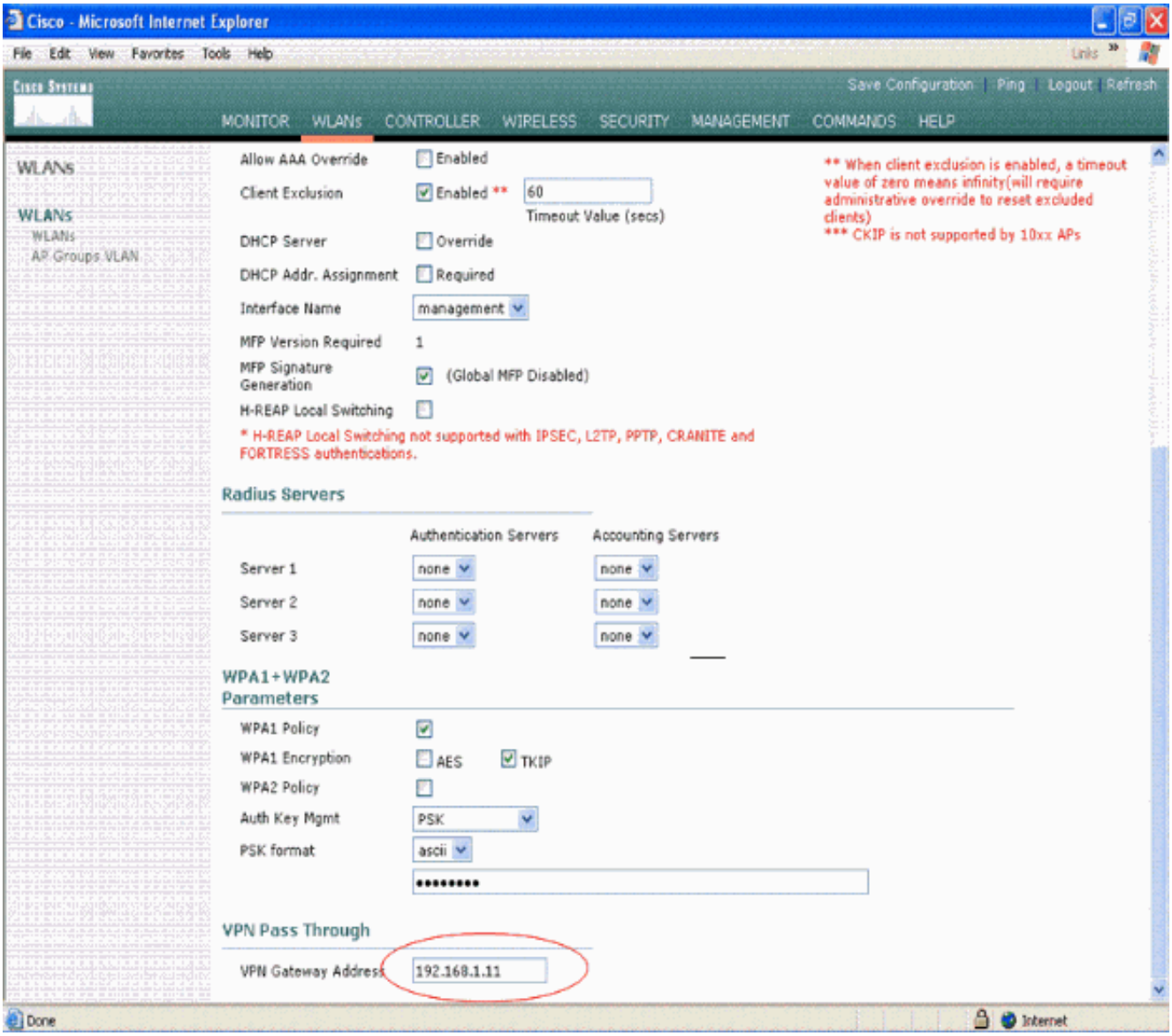
5. Configurare il criterio WPA e il tipo di gestione della chiave di autenticazione da utilizzare.In questo esempio viene utilizzata la **chiave già condivisa (PSK)** per la gestione delle chiavi di autenticazione. Dopo aver selezionato PSK, selezionare **ASCII** come formato PSK e digitare il valore PSK. Affinché i client che appartengono a questo SSID possano essere associati alla WLAN, questo valore deve essere uguale nella configurazione SSID del client wireless.



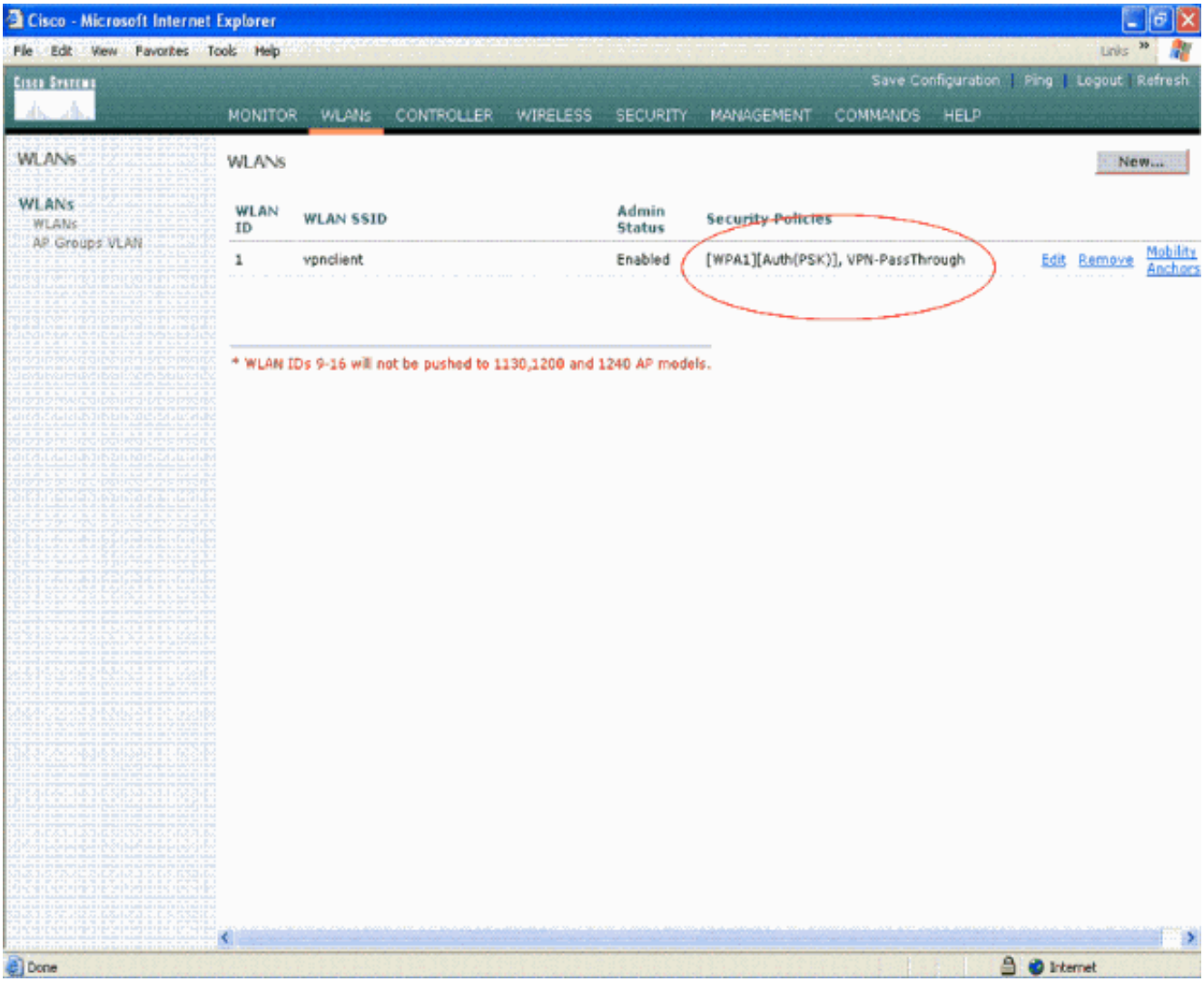
6. Selezionare **VPN Pass-through** come sicurezza di livello 3. Ecco l'esempio.



7. Dopo aver selezionato VPN Pass-through come protezione di livello 3, aggiungere l'indirizzo del gateway VPN come mostrato nell'esempio.L'indirizzo del gateway deve essere l'indirizzo IP dell'interfaccia che termina il tunnel VPN sul lato server. Nell'esempio, l'indirizzo IP dell'interfaccia s3/0 (192.168.1.11/24) sul server VPN è l'indirizzo del gateway da configurare.



8. Fare clic su **Apply** (Applica). La WLAN chiamata *vpnclient* è ora configurata per il pass-through
VPN.



Configurazione server VPN

Questa configurazione mostra il router Cisco 3640 come server VPN.

Nota: per semplicità, questa configurazione utilizza l'indirizzamento statico per mantenere la raggiungibilità dell'IP tra gli endpoint. Per mantenere la raggiungibilità, è possibile utilizzare qualsiasi protocollo di routing dinamico, ad esempio RIP (Routing Information Protocol), OSPF (Open Shortest Path First) e così via.

Nota: il tunnel non viene stabilito se non è possibile raggiungere l'indirizzo IP tra il client e il server.

Nota: in questo documento si presume che l'utente sia a conoscenza del modo in cui abilitare il routing dinamico nella rete.

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
```

Nota: in questo esempio viene utilizzata solo l'autenticazione di gruppo. Non utilizza l'autenticazione dei singoli utenti.

Configurazione client VPN

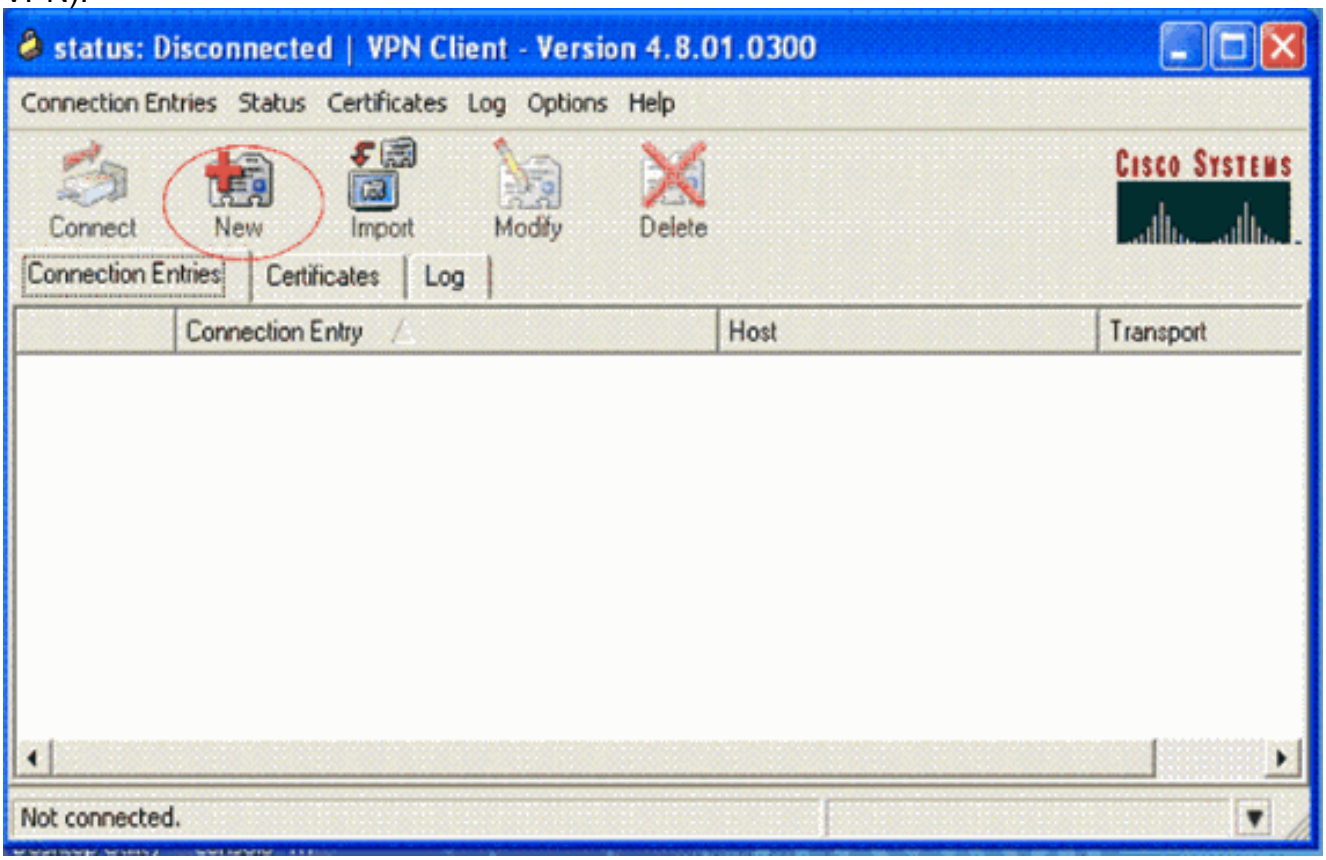
Èpossibile scaricare un client VPN software dal Cisco.com Software Center.

Nota: alcuni software Cisco richiedono di eseguire il login con un nome utente e una password CCO.

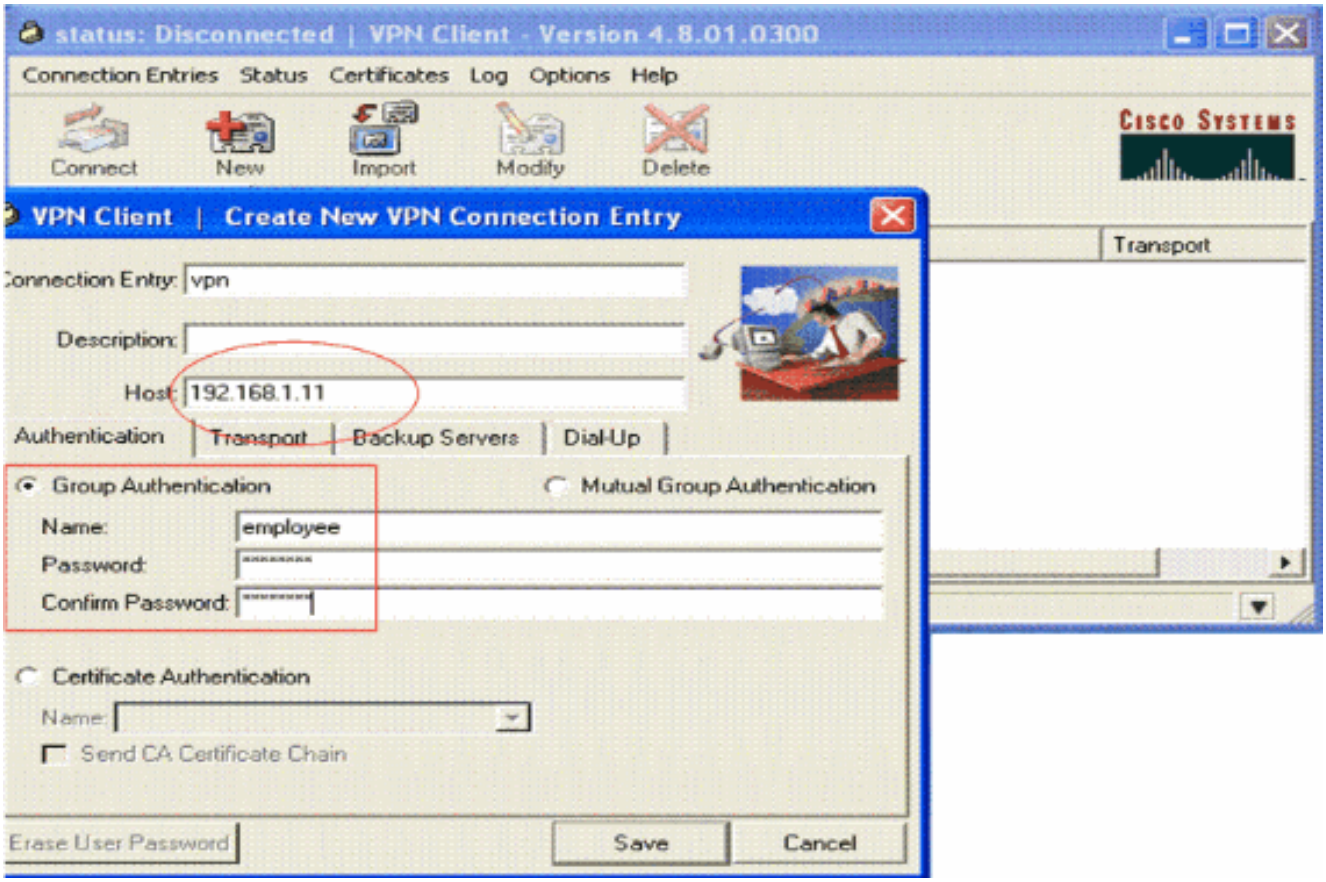
Completare questa procedura per configurare il client VPN.

1. Dal client wireless (laptop), scegliere **Start > Programmi > Cisco Systems VPN Client > VPN Client** per accedere al client VPN. Questa è la posizione predefinita in cui è installato il client VPN.
2. Fare clic su **New** per avviare la finestra Create New VPN Connection Entry (Crea nuova voce di connessione

VPN).



3. Immettere il nome della voce di connessione insieme a una descrizione. In questo esempio *viene utilizzato vpn*.Il campo Descrizione è facoltativo. Immettere l'indirizzo IP del server VPN nella casella Host. Immettere il nome e la password del gruppo VPN e fare clic su **Salva**.



Nota: il nome del gruppo e la password configurati in questa finestra devono corrispondere a quelli configurati nel server VPN. In questo esempio vengono utilizzati il nome *employee* e la

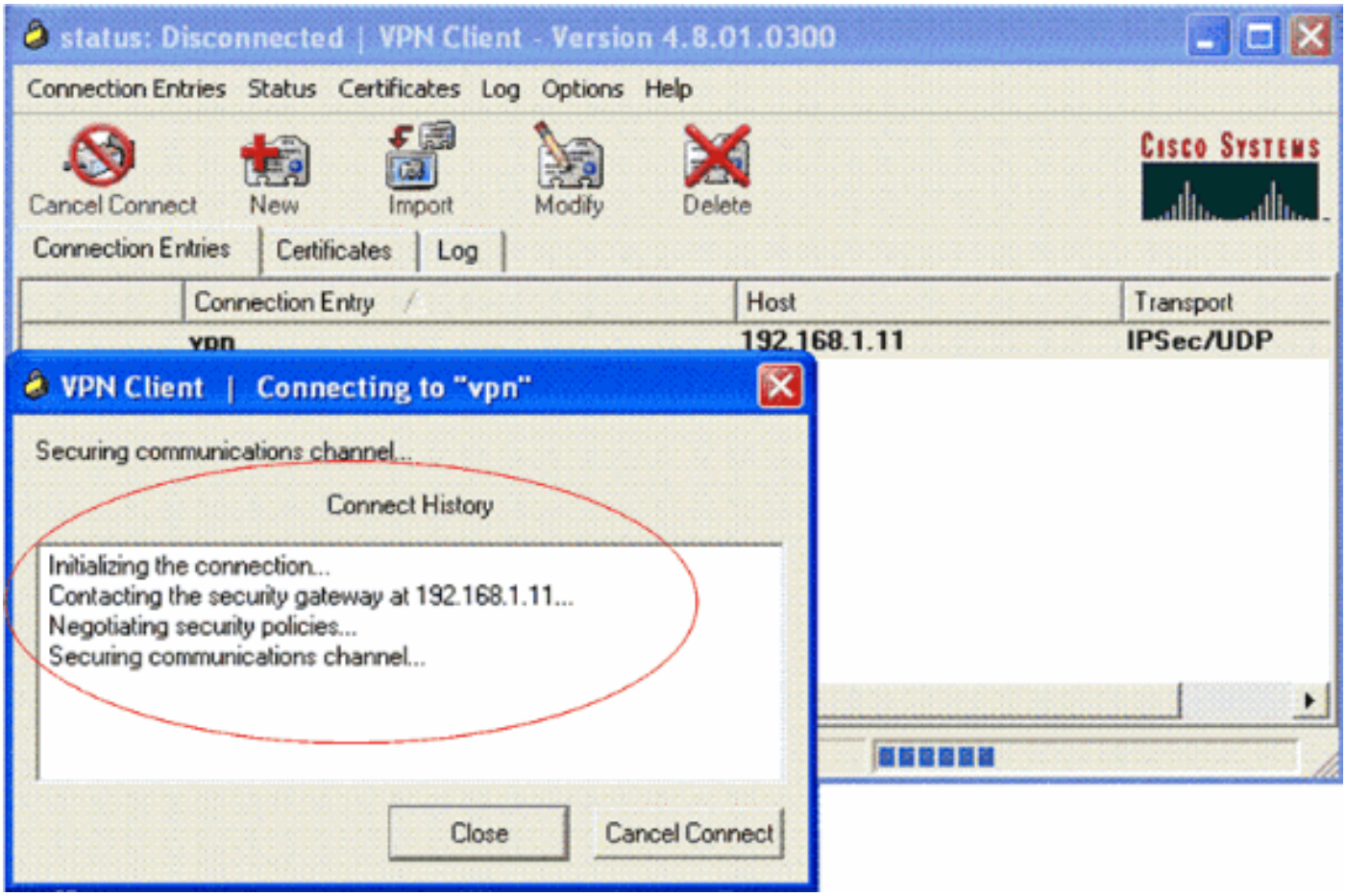
password *cisco123*.

Verifica

Per verificare questa configurazione, configurare il client **vpnSSID** nel client wireless con gli stessi parametri di sicurezza configurati nel WLC e associare il client alla WLAN. Sono disponibili diversi documenti che spiegano come configurare un client wireless con un nuovo profilo.

Una volta associato il client wireless, passare al client VPN e fare clic sulla connessione configurata. Quindi fare clic su **Connect** (Connetti) nella finestra principale VPN Client.

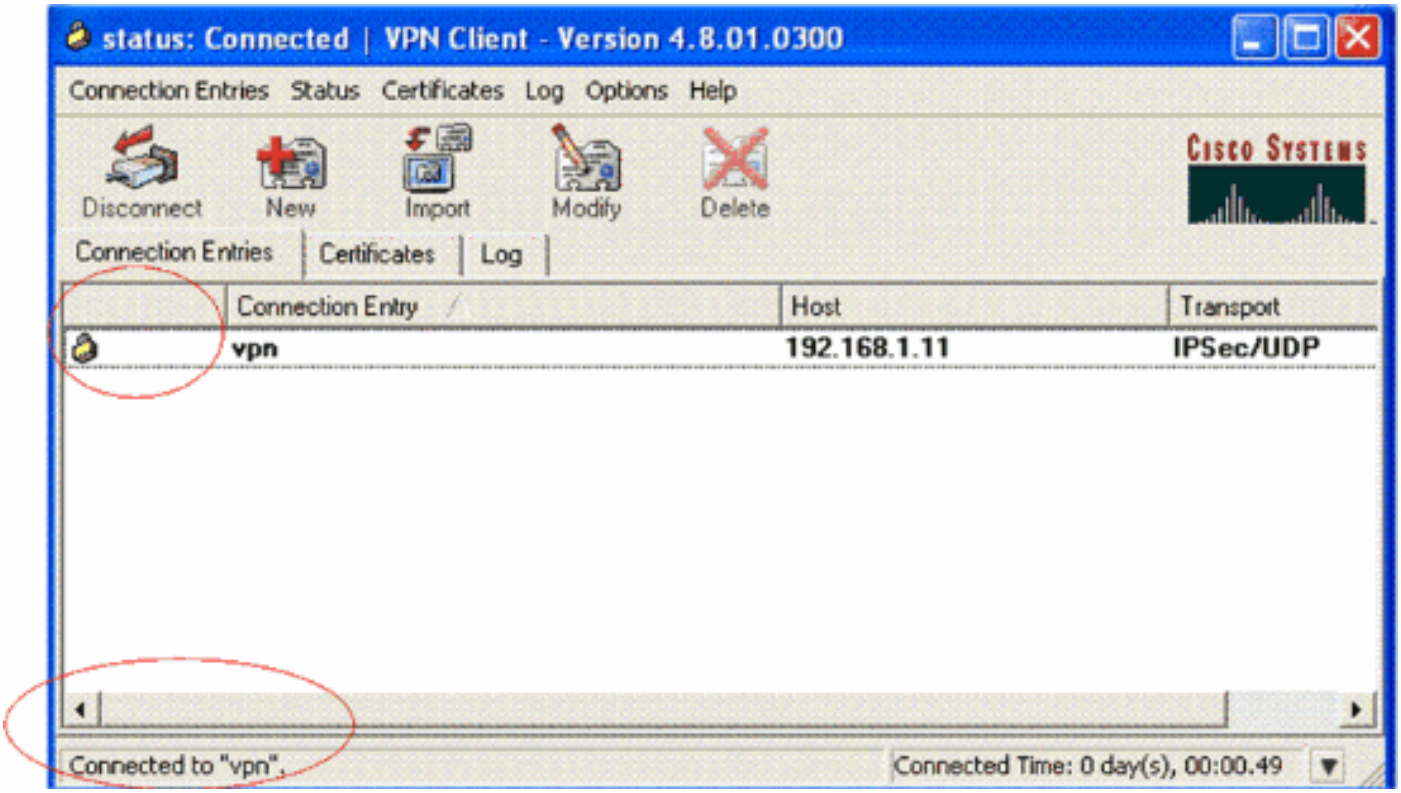
Èpossibile visualizzare i parametri di sicurezza Fase 1 e Fase 2 negoziati tra il client e il server.



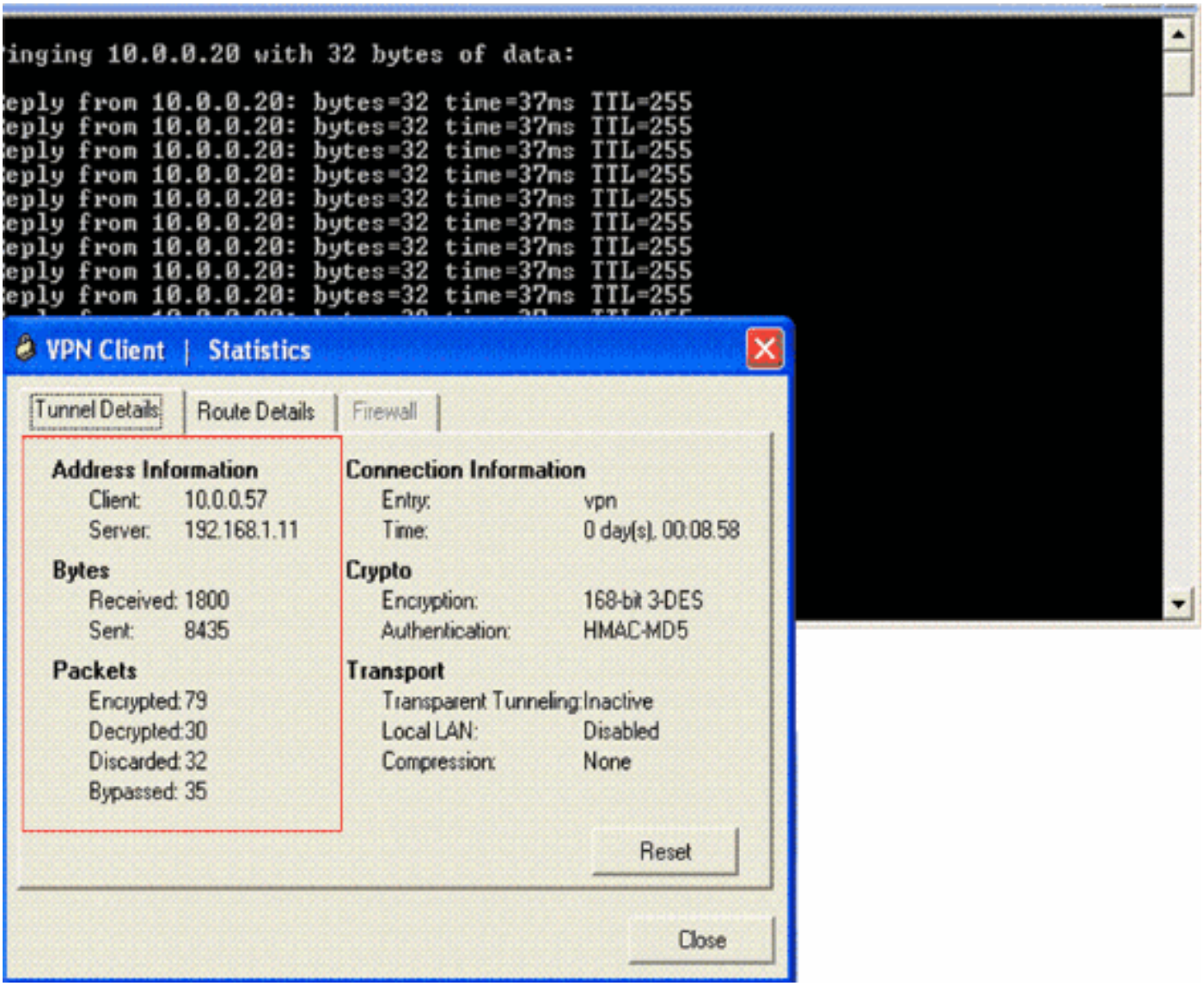
Nota: per stabilire questo tunnel VPN, il client VPN e il server devono avere una raggiungibilità IP tra loro. Se il client VPN non è in grado di contattare il gateway di sicurezza (server VPN), il tunnel non viene stabilito e sul lato client viene visualizzata una finestra di avviso con questo messaggio:

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

Per garantire che un tunnel VPN sia stabilito correttamente tra il client e il server, è possibile trovare un'icona a forma di lucchetto creata accanto al client VPN stabilito. La barra di stato indica anche **Connesso a "vpn"**. Ecco un esempio.



Verificare inoltre di essere in grado di trasmettere correttamente i dati al segmento LAN sul lato server dal client VPN e viceversa. Dal menu principale di VPN Client, scegliere **Stato > Statistiche**. Qui è possibile trovare le statistiche dei pacchetti crittografati e decrittografati che vengono passati attraverso il tunnel.



In questa schermata è possibile visualizzare l'indirizzo del client come 10.0.0.57. Si tratta dell'indirizzo che il server VPN assegna al client dal pool configurato localmente dopo la negoziazione della fase 1 riuscita. Una volta stabilito il tunnel, il server VPN aggiunge automaticamente una route all'indirizzo IP DHCP assegnato nella relativa tabella di route.

Èinoltre possibile verificare l'aumento del numero di pacchetti crittografati durante il trasferimento dei dati dal client al server e l'aumento del numero di pacchetti decrittografati durante un trasferimento inverso dei dati.

Nota: poiché il WLC è configurato per il pass-through VPN, consente al client di accedere solo al segmento connesso al gateway VPN (in questo caso, il server VPN è 192.168.1.11) configurato per il pass-through. In questo modo viene filtrato tutto il resto del traffico.

Èpossibile verificare questa condizione configurando un altro server VPN con la stessa configurazione e configurando una nuova voce di connessione per questo server VPN nel client VPN. Ora, quando si tenta di stabilire un tunnel con questo server VPN, non è possibile. Infatti, il WLC filtra questo traffico e consente un tunnel solo all'indirizzo del gateway VPN configurato per il pass-through VPN.

Èinoltre possibile verificare la configurazione dalla CLI del server VPN.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare

l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

I comandi **show** usati nel server VPN possono essere utili anche per verificare lo stato del tunnel.

- Il comando **show crypto session** viene usato per verificare lo stato del tunnel. Di seguito è riportato un esempio di output di questo comando.

```
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
```

- Il criterio **show crypto isakmp** viene usato per visualizzare i parametri configurati per la fase 1.

Risoluzione dei problemi

Per la risoluzione dei problemi, è possibile usare anche i comandi **debug** e **show** spiegati nella sezione Verifica.

- **debug crypto isakmp**
- **debug crypto ipsec**
- **mostra sessione crittografica**

- Il comando **debug crypto isakmp** sul server VPN visualizza l'intero processo di negoziazione in fase 1 tra il client e il server. Di seguito è riportato un esempio di negoziazione riuscita per la fase 1.

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

- Il comando **debug crypto ipsec** sul server VPN visualizza la negoziazione IPsec della fase 1 riuscita e la creazione del tunnel VPN. Di seguito è riportato un esempio:

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

Informazioni correlate

- Introduzione alla crittografia di protezione IP (IPsec)
- Negoziazione IPsec/pagina di supporto del protocollo IKE

- Configurazione della protezione di rete IPsec
- Cisco Easy VPN - Domande e risposte
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0
- Esempio di configurazione degli ACL sui controller LAN wireless
- Domande frequenti sui Wireless LAN Controller (WLC)
- Pagina di supporto wireless
- Documentazione e supporto tecnico – Cisco Systems