WLC を使用したワイヤレス LAN 上のクライアント VPN の設定例

目次

概要

このドキュメントでは、ワイヤレス環境における Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の概念を紹介します。 このドキュメントでは、ワイヤレス クライアントと VPN サーバ間に Wireless LAN Controller（WLC; ワイヤレス LAN コントローラ）を経由する VPN トンネルを配備する際の、関連する設定を説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- WLC に関する知識と WLC の基本的なパラメータの設定方法に関する知識
- Wi-Fi Protected Access（WPA）の概念に関する知識
- VPN および VPN のタイプに関する基本的な知識
- IPSec に関する知識
- 使用可能な暗号アルゴリズム、認証アルゴリズム、ハッシュ アルゴリズムに関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 4.0.179.8 が稼働する Cisco 2006 WLC
- Cisco 1000 シリーズ Lightweight アクセス ポイント（LAP）
- Cisco IOS® ソフトウェア リリース 12.4(8) が稼働する Cisco 3640
- Cisco VPN Client バージョン 4.8

注: このドキュメントでは、VPN サーバとして Cisco 3640 ルータを使用します。 より高度なセキュリティ機能をサポートするために、専用 VPN サーバを使用することもできます。

注: ルータが VPN サーバとして動作するためには、ルータで基本的な IPSec をサポートするフィーチャ セットを稼働する必要があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

VPN は、インターネットなどの公共の電気通信インフラストラクチャを使用したプライベート ネットワーク内で、データを安全に送信するために使用する、プライベート データ ネットワークです。 VPN は、トンネリング プロトコルおよびセキュリティ手順を使用して、データ プライバシーを維持します。

リモート アクセス VPN

リモート アクセス VPN の設定は、モバイル ユーザなどの VPN ソフトウェア クライアントが、VPN サーバの背後にある中央のネットワーク リソースに安全にアクセスできるようにするために使用されます。 Cisco では、これらの VPN サーバを Cisco Easy VPN Server、クライアントを Cisco Easy VPN Remote デバイスとも呼びます。

Cisco IOS ルータ、Cisco PIX セキュリティ アプライアンス、Cisco VPN 3002 ハードウェア クライアント、および Cisco VPN Client が Cisco Easy VPN Remote デバイスとなります。 これらのデバイスは、Cisco Easy VPN Server からの VPN トンネル接続上で、セキュリティ ポリシーを受信するために使用されます。 これにより、リモート サイトでの設定要件を最小に抑えることができます。 Cisco VPN Client は、PC、ラップトップなどにインストールできるソフトウェア クライアントです。

Cisco IOS ルータ、Cisco PIX セキュリティ アプライアンス、および Cisco VPN 3000 コンセントレータが Cisco Easy VPN Server となります。

このドキュメントでは、ラップトップ上で稼働する Cisco VPN Client ソフトウェアを VPN Client、Cisco 3640 IOS ルータを VPN サーバとして使用します。 このドキュメントでは、IPSec 標準を使用してクライアントとサーバ間に VPN トンネルを確立します。

IPsec

IPSec は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）が策定したオープン スタンダードのフレームワークです。 IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。

IPSec により、ネットワークでは IP パケット レベルでデータの暗号化が実行されます。これにより、標準ベースの堅牢なセキュリティ ソリューションが提供されます。 IPSec の主要なタスクは、保護されていない接続上で機密情報のやり取りを可能にすることです。 IPSec では、情報が傍受されたり、盗聴されたりすることを防ぐために、暗号化が使用されます。 ただし、暗号化を効果的に使用するためには、送信者と受信者の両者が、情報の暗号化および復号化の両方に使用される秘密を共有する必要があります。

IPSec は、共有秘密を秘密交換できるように、2 つのフェーズで動作します。

- フェーズ 1：2 つの IPSec ピア間で安全なチャネルを確立するために必要なセキュリティ パラメータのネゴシエーションを処理します。 通常、フェーズ 1 は Internet Key Exchange（IKE; インターネット キー エクスチェンジ）プロトコルを使用して実装されます。 リモート IPSec ピアで IKE を実行できない場合は、事前共有キーを使用した手動設定を使用して、フェーズ 1 を完了できます。
- フェーズ 2：フェーズ 1 で確立された安全なトンネルを使用して、実際にユーザ データを送信するために必要なセキュリティ パラメータを交換します。 IPSec の両フェーズで使用される安全なトンネルは、各 IPSec エンド ポイントで使用される Security Association（SA; セキュリティ アソシエーション）に基づいています。 SA は、両方のエンド ポイントで同意して使用される認証および暗号化のタイプなどの、セキュリティ パラメータを記述します。

フェーズ 2 で交換されるセキュリティ パラメータは IPSec トンネルを作成するために使用され、作成されたトンネルは VPN Client とサーバ間のデータ転送に使用されます。

IPSec とその設定についての詳細は、『IPSec の設定』を参照してください。

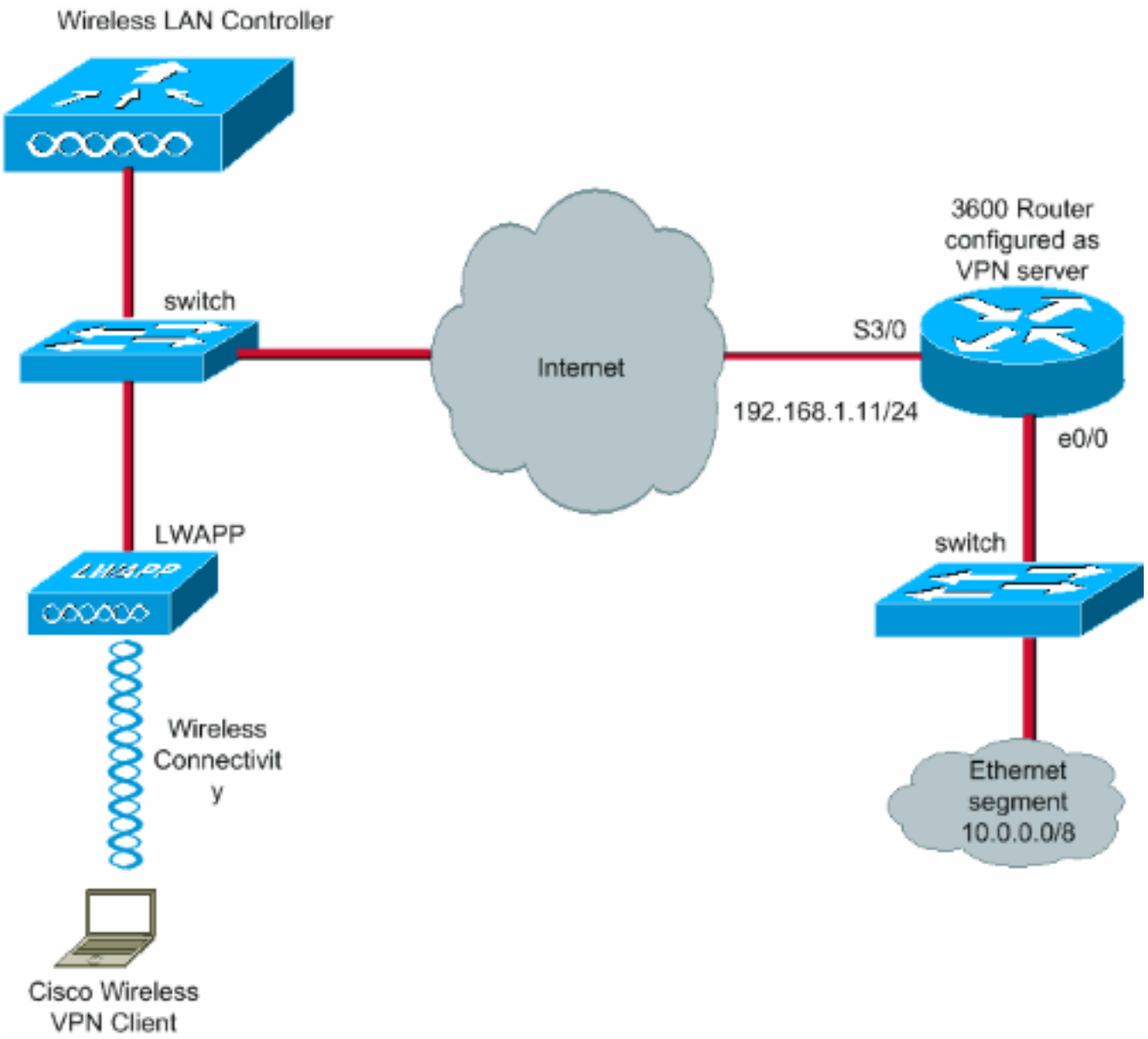
VPN Client とサーバ間に VPN トンネルが確立すると、*VPN サーバで定義されているセキュリティ ポリシーはクライアントに送信されます*。 これにより、クライアント側での設定要件を最小に抑えることができます。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次の設定を使用します。

- WLC の管理インターフェイス IP アドレス：172.16.1.10/16
- WLC の AP マネージャ インターフェイス IP アドレス：172.16.1.11/16
- デフォルト ゲートウェイ：172.16.1.20/16**注:** 実稼働中のネットワークでは、このデフォルト ゲートウェイは、WLC を他のネットワークおよびインターネット（またはそのいずれか）に接続する直接ルータの着信インターフェイスを指す必要があります。
- VPN サーバ 3/0 の IP アドレス：192.168.1.11/24**注:** この IP アドレスは、VPN サーバ側で VPN トンネルを終端するインターフェイスを指す必要があります。 この例では、VPN サーバで VPN トンネルを終端するインターフェイスは s3/0 です。
- VPN サーバでの LAN セグメントでは、IP アドレスの範囲 10.0.0.0/8 が使用されます。



設定

WLAN 集中型アーキテクチャでは、ラップトップなどのワイヤレス VPN Client が VPN サーバとの VPN トンネルを確立できるようにするために、クライアントに Lightweight Access Point (LAP; Lightweight アクセス ポイント) を関連付け、LAP を WLC に登録する必要があります。 このドキュメントでは、『ワイヤレス LAN コントローラ (WLC) への Lightweight AP (LAP) の登録』で説明されている、ローカル サブネットのブロードキャスト ディスカバリ プロセスを使用して WLC に登録済みの LAP を扱います。

次の手順では、VPN に WLC を設定します。

VPN 終端およびパススルー

バージョン 4 よりも前の Cisco 4000 シリーズ WLC では、IPSec VPN 終端 (IPSec サポート) と呼ばれる機能がサポートされています。 この機能により、これらのコントローラは、コントローラ上で直接 VPN Client セッションを終端できます。 要約すると、この機能により、コントローラ自体が VPN サーバとして動作できるようになります。 ただし、このようにするためには、別途 VPN 終端ハードウェア モジュールをコントローラ上にインストールする必要があります。

次のコントローラでは、IPSec VPN サポートは利用できません。

- Cisco 2000 シリーズ WLC
- バージョン 4.0 以降で稼働するすべての WLC

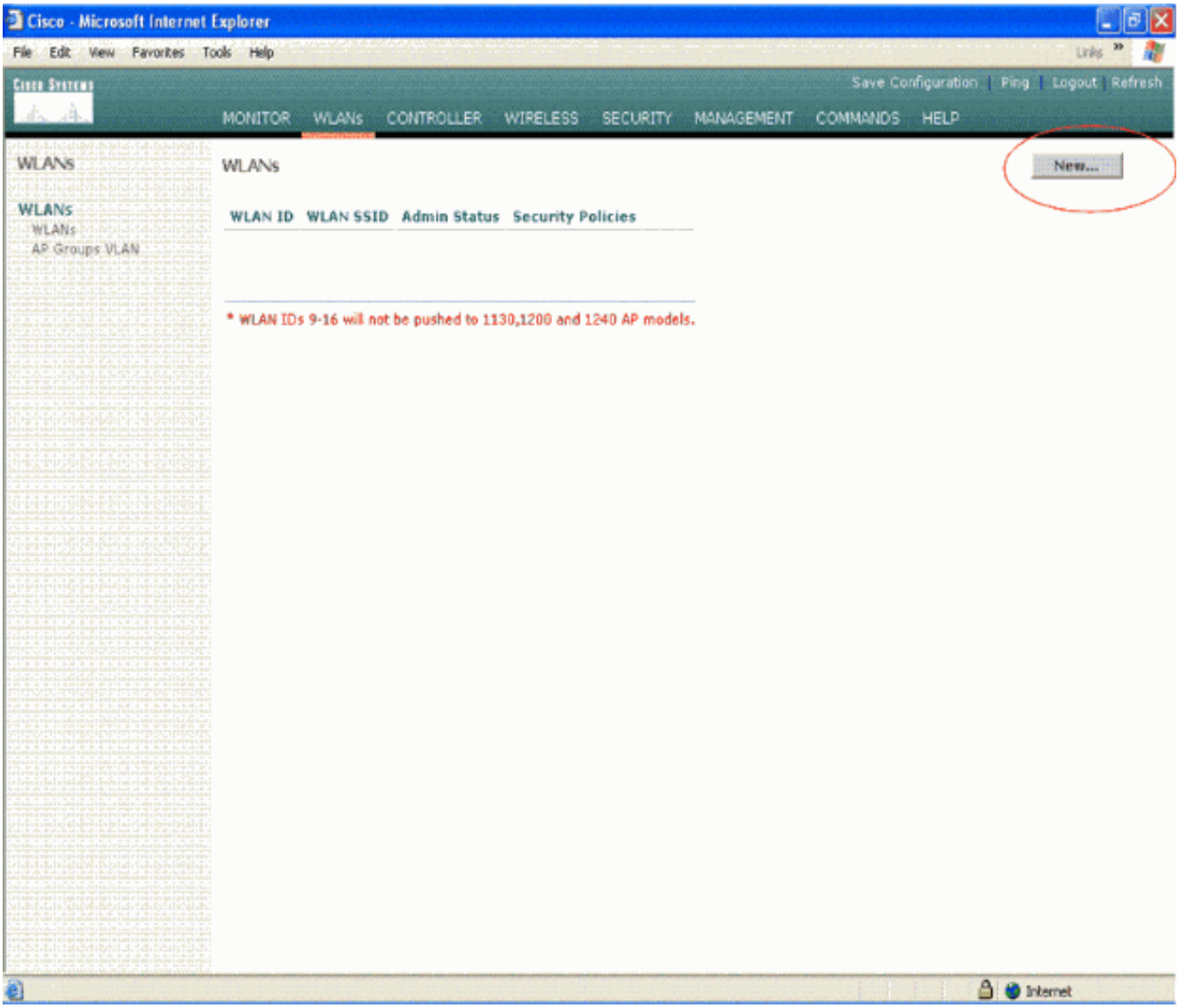
このため、4.0 より後のバージョンでサポートされる VPN 機能は、VPN パススルーのみです。この機能は、Cisco 2000 シリーズ WLC でもサポートされています。

VPN パススルーは、クライアントが特定の VPN サーバだけを使用してトンネルを確立できるようにする機能です。 そのため、設定済みの VPN サーバおよび別の VPN サーバやインターネットに安全にアクセスする必要がある場合に、コントローラ上で VPN パススルーがイネーブルにされていると、トンネルが確立できなくなります。 このような要件がある場合は、VPN パススルーをディセーブルにする必要があります。 ただし、適切な ACL を作成し、対応する WLAN に適用した場合は、WLC がパススルーとして動作し、複数の VPN ゲートウェイに到達するように WLC を設定できます。 このような、冗長性を持たせるために複数の VPN ゲートウェイに到達できるようにするシナリオでは、VPN パススルーをディセーブルにし、VPN ゲートウェイへのアクセスを許可する ACL を作成し、その ACL を WLAN に適用します。

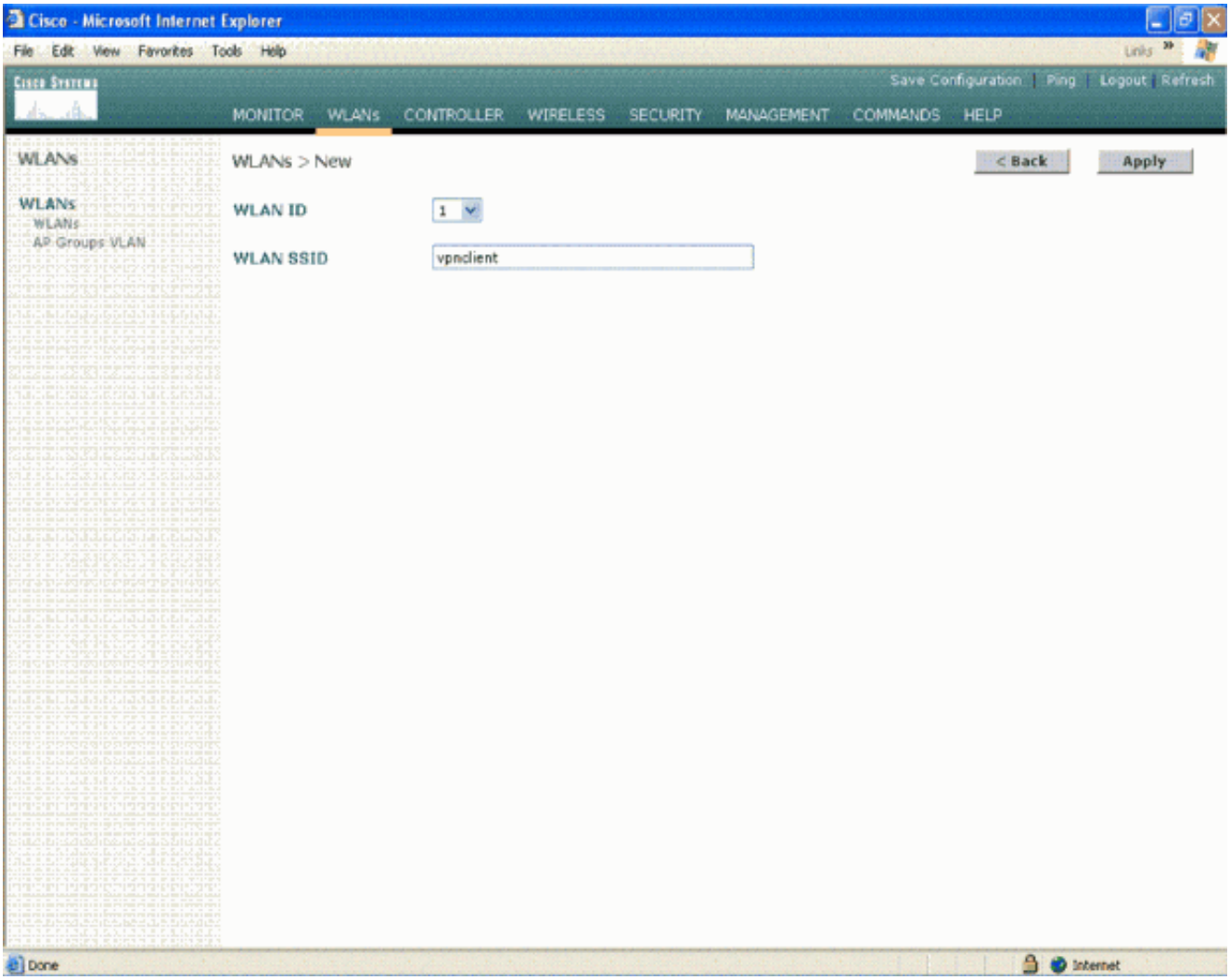
WLC への VPN パススルーの設定

次の手順を実行して、VPN パススルーを設定します。

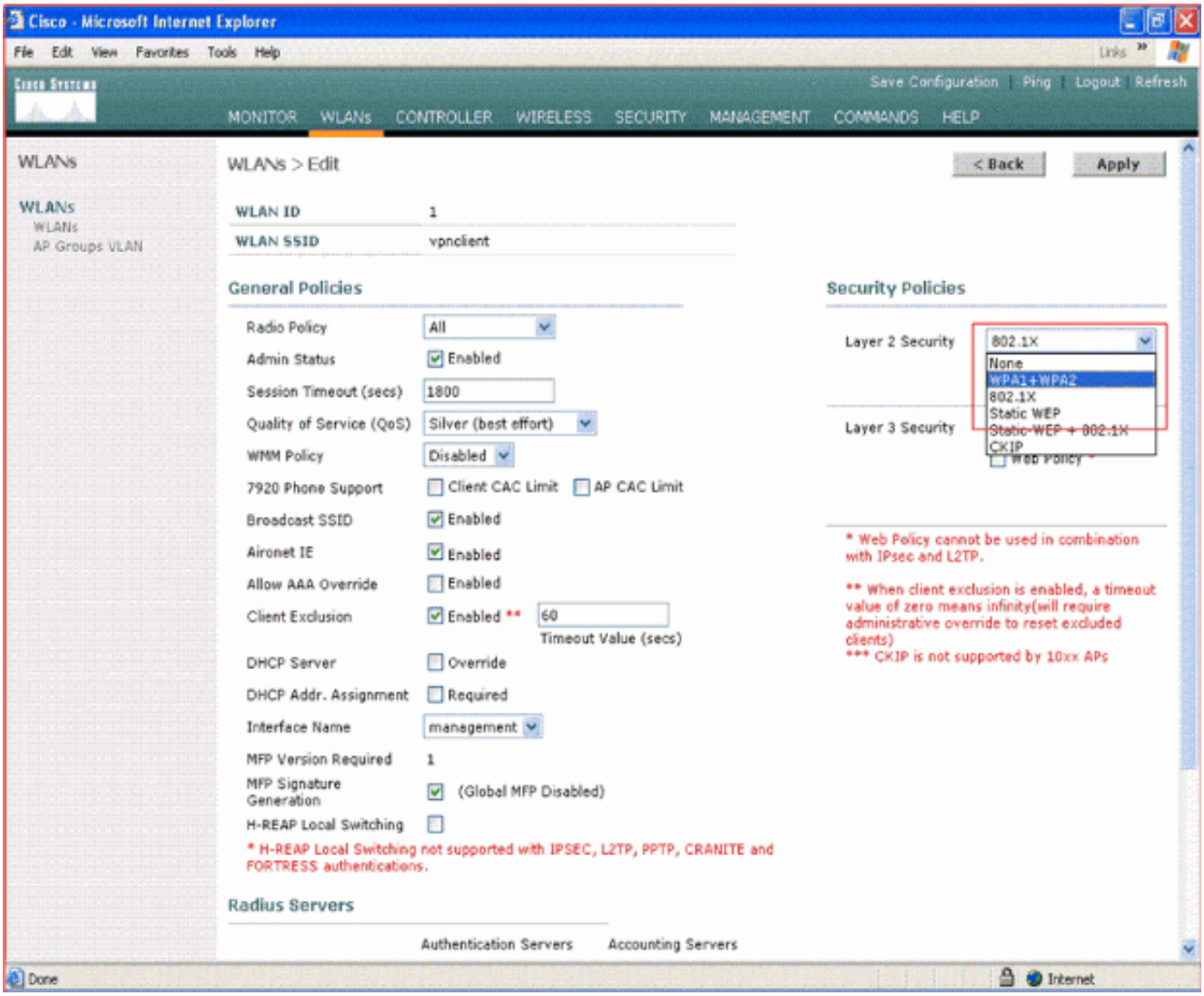
1. WLC の GUI で [WLANs] をクリックして、[WLANs] ページに移動します。
2. [New] をクリックして新規の WLAN を作成します。



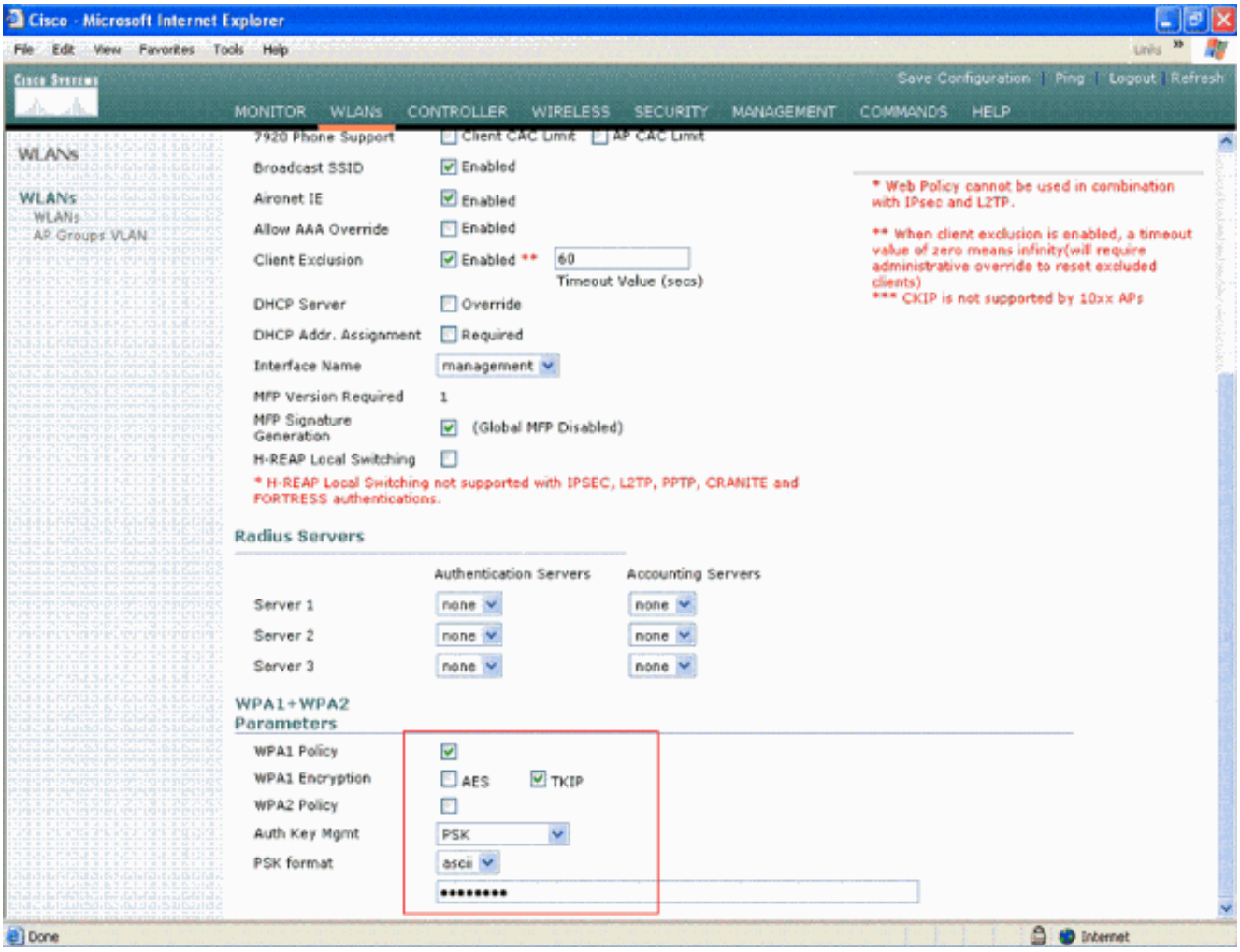
3. この例では、WLAN SSID は **vpnclient** と命名されています。 [Apply] をクリックします。



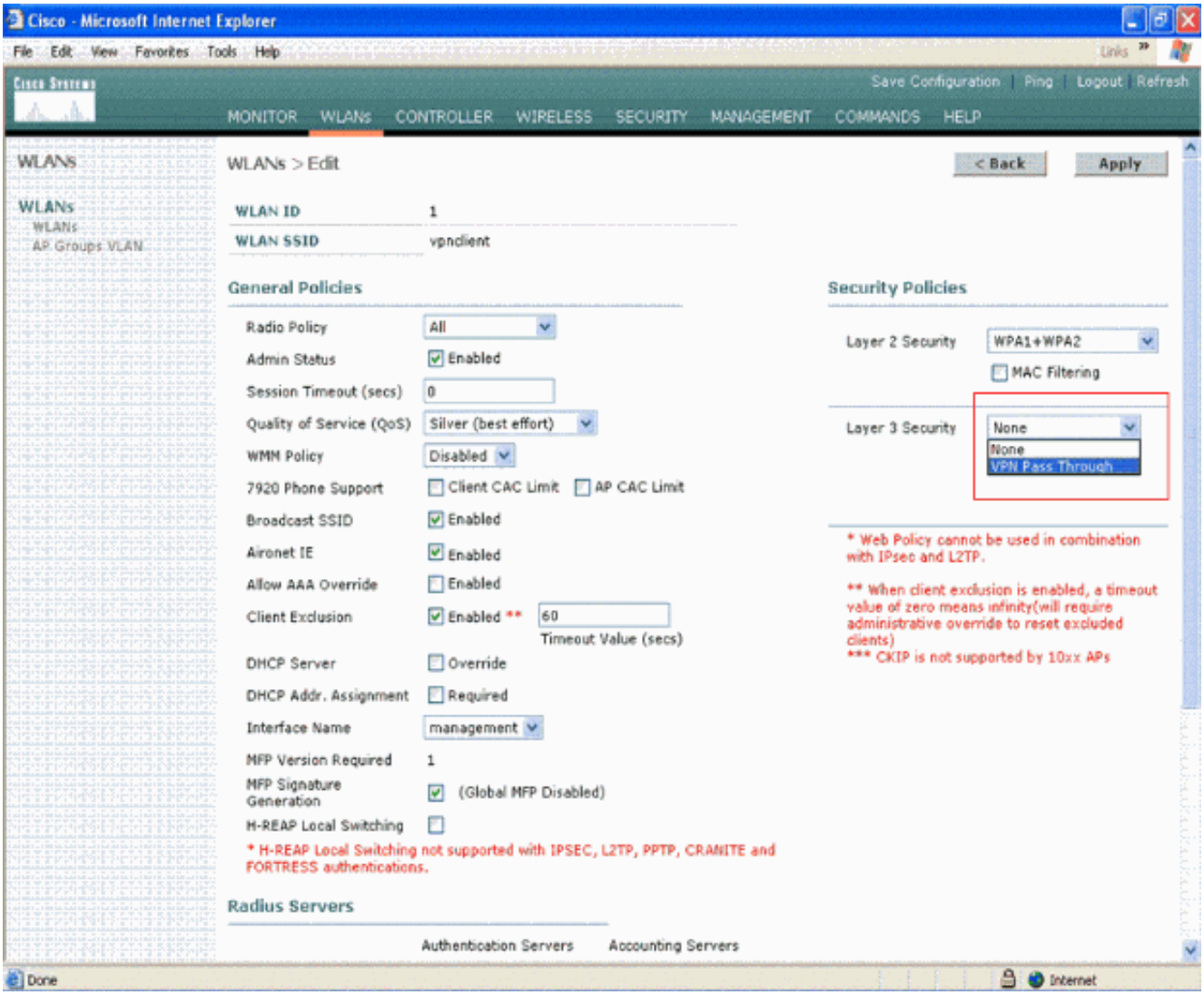
4. vpnclient SSID にレイヤ 2 セキュリティを設定します。 *この設定はオプション*です。この例では、セキュリティ タイプに **WPA1+WPA2** を使用します。



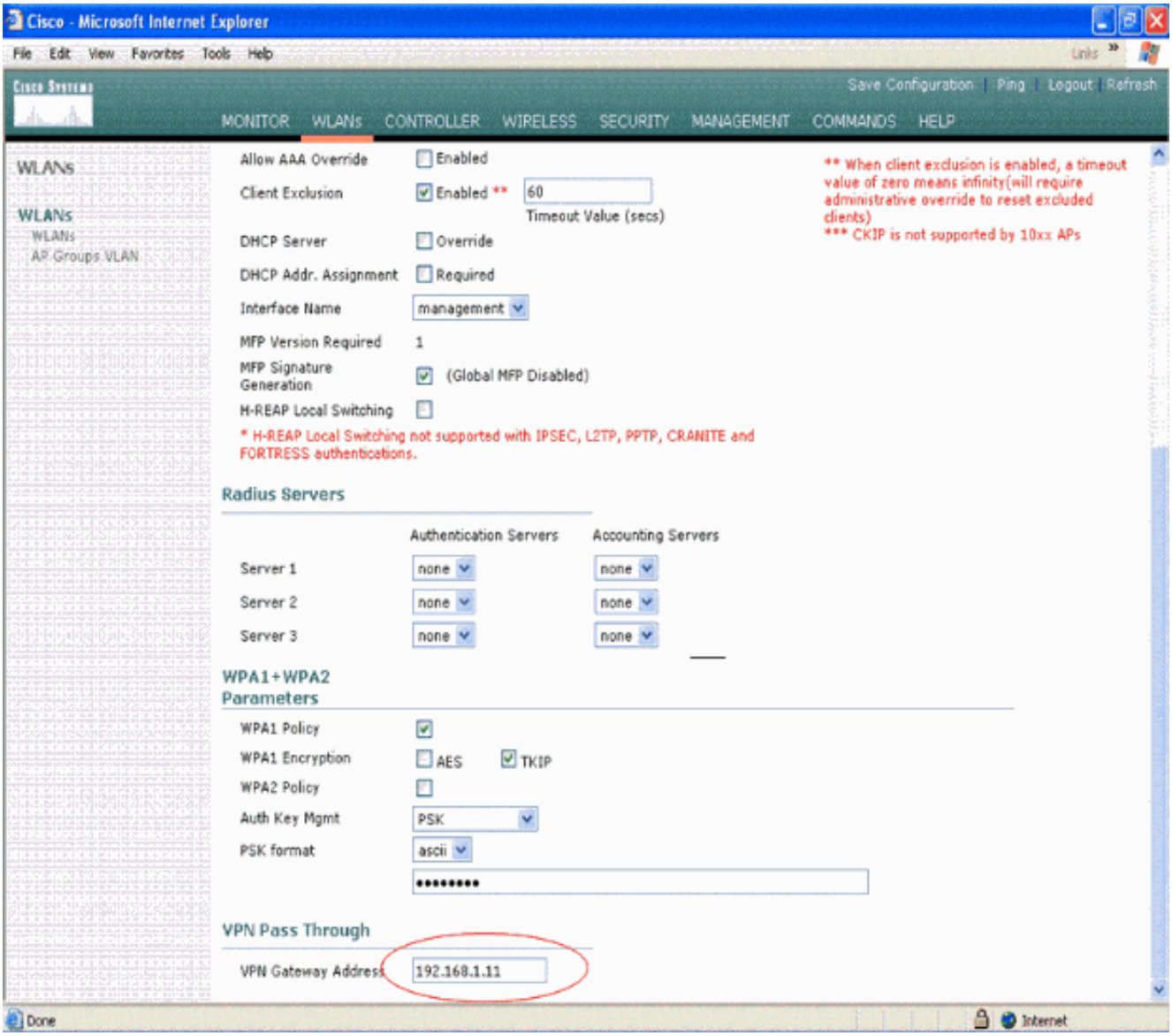
5. 使用する WPA ポリシーと認証キー管理タイプを設定します。この例では、認証キー管理に **Pre-Shared Key (PSK; 事前共有キー)** を使用します。 [PSK] を選択したら、[PSK Format] で [ASCII] を選択し、PSK 値を入力します。 この SSID に属するクライアントをこの WLAN に関連付けるために、この PSK 値は、ワイヤレス クライアントの SSID 設定の PSK 値と同じ値にする必要があります。



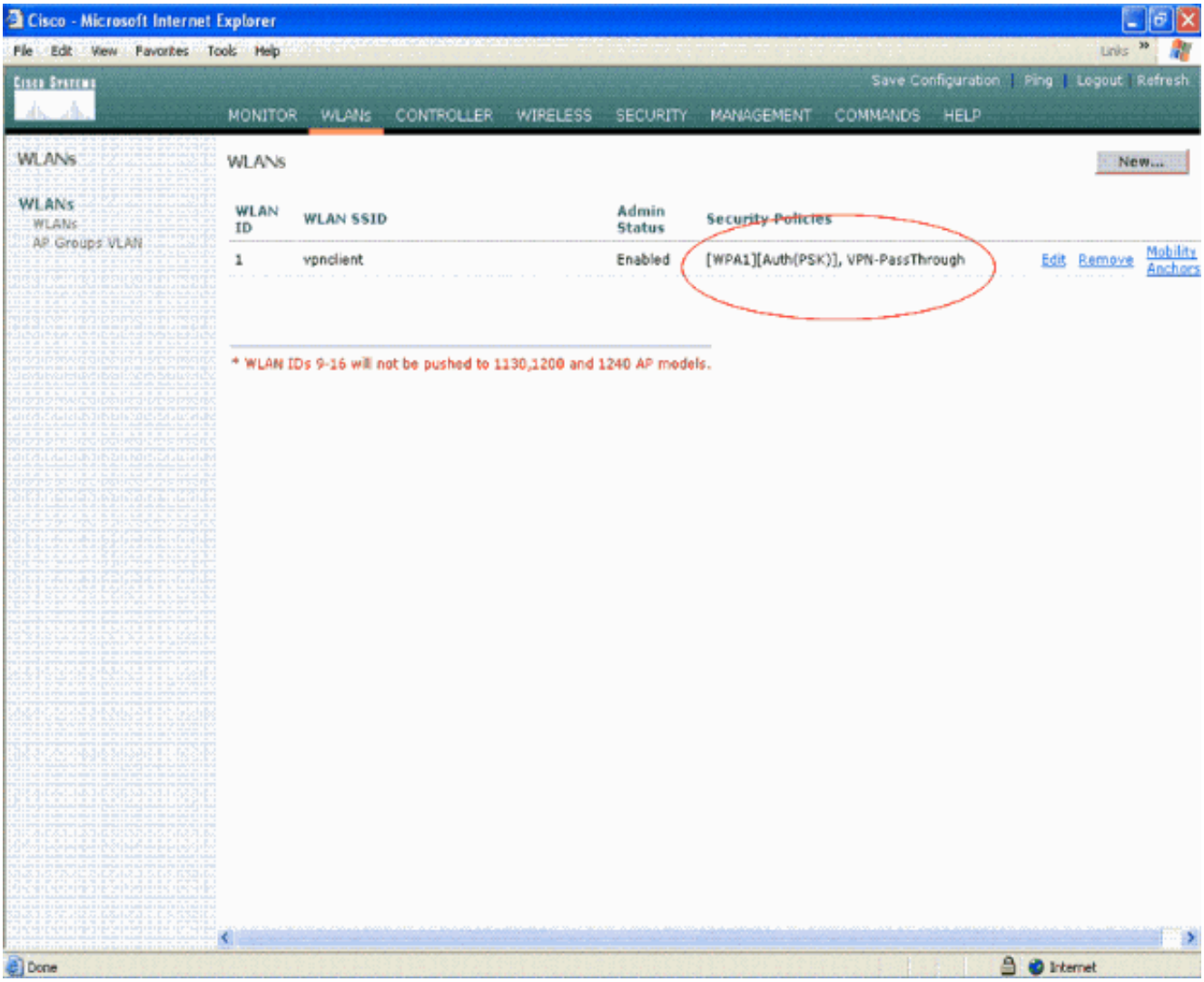
6. [Layer 3 Security] で [VPN Pass-through] を選択します。 次に例を示します。



7. Layer 3 Security として VPN Pass-through を選択したら、次の例のように [VPN Gateway Address] を追加します。このゲートウェイ アドレスは、サーバ側で VPN トンネルを終端するインターフェイスの IP アドレスとする必要があります。 この例では、設定するゲートウェイ アドレスは、VPN サーバでの s3/0 インターフェイスの IP アドレス（192.168.1.11/24）です。



8. [Apply] をクリックします。 *vpnclient* という名前の WLAN に VPN Pass-through が設定されました。



VPN Server の設定

この設定では、Cisco 3640 ルータを VPN サーバとして示します。

注: 説明を簡単にするため、この設定ではスタティック ルーティングを使用してエンド ポイント間の IP 到達可能性を維持します。 到達可能性を維持するためには、Routing Information Protocol（RIP; ルーティング情報プロトコル）、Open Shortest Path First（OSPF）などのあらゆるダイナミック ルーティング プロトコルを使用できます。

注: クライアントとサーバ間に IP 到達可能性がない場合は、トンネルを確立できません。

注: このドキュメントでは、ユーザはネットワークでダイナミック ルーティングをイネーブルにする方法を知っていることを前提とします。

Cisco 3640 ルータ

```
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
```

注: この例では、グループ認証のみを使用します。 個別ユーザ認証は使用しません。

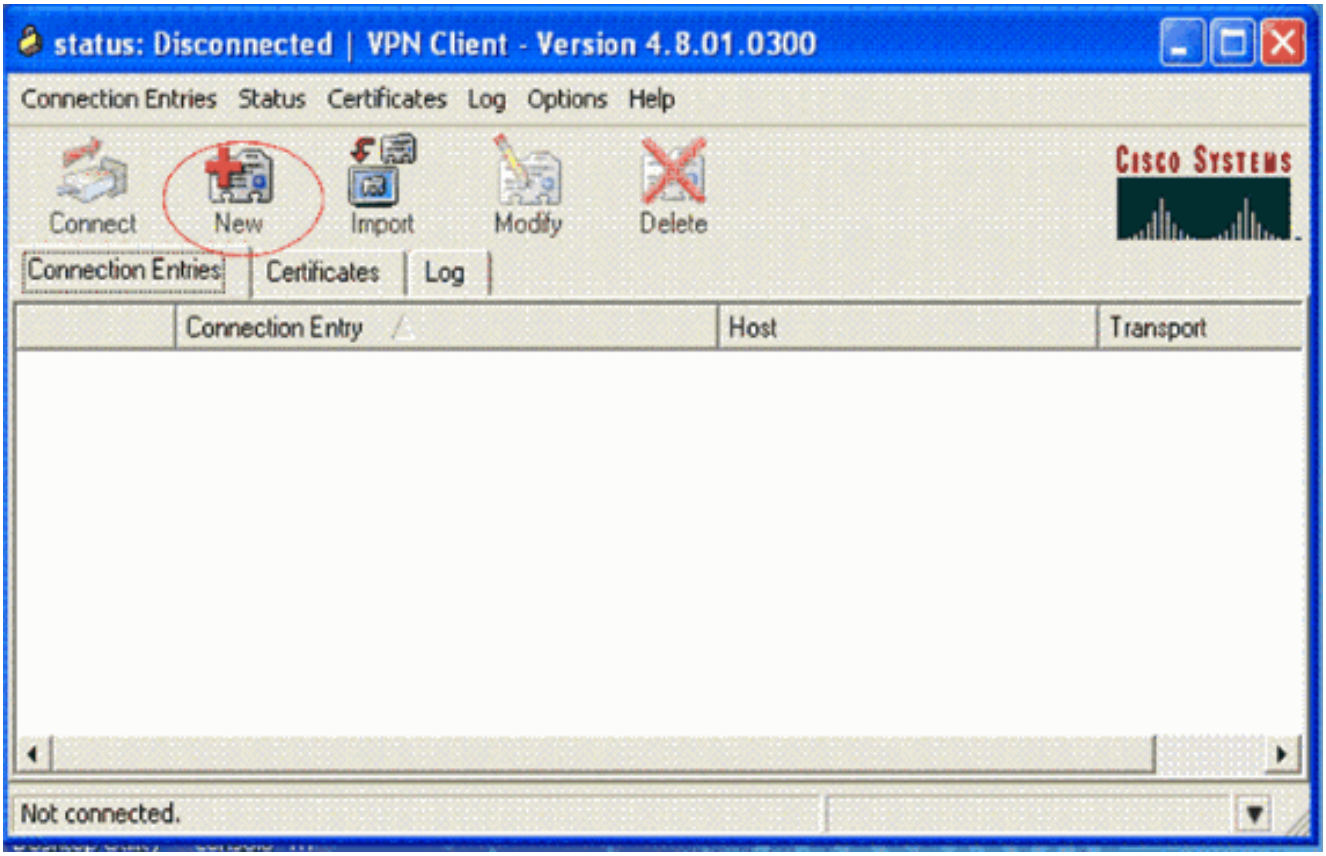
VPN Client の設定

VPN Client ソフトウェアは Cisco.com Software Center でダウンロードできます。

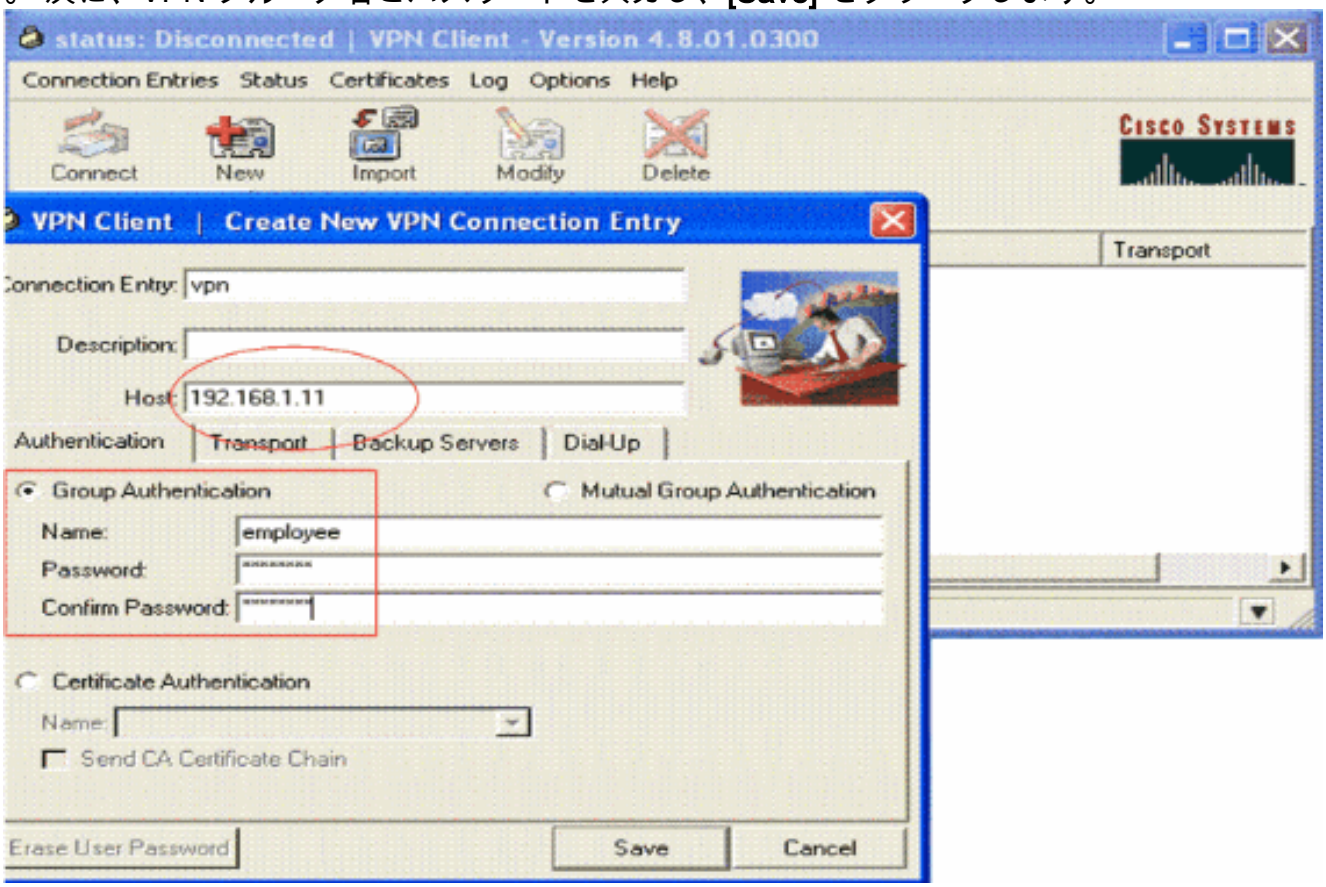
注: 一部の Cisco ソフトウェアでは、CCO ユーザ名およびパスワードでのログインが必要です。

次の手順を実行して、VPN Client を設定します。

1. ワイヤレス クライアント（ラップトップ）で [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] を選択し、VPN Client にアクセスします。 この場所は、VPN Client のデフォルトのインストール場所です。
2. [New] をクリックして、[Create New VPN Connection Entry] ウィンドウを開きます。



3. 接続エントリの名前と説明を入力します。 この例では *vpn* を使用しています。[Description] フィールドはオプションです。 [Host] ボックスに VPN サーバの IP アドレスを入力します。 次に、VPN グループ名とパスワードを入力し、**[Save]** をクリックします。



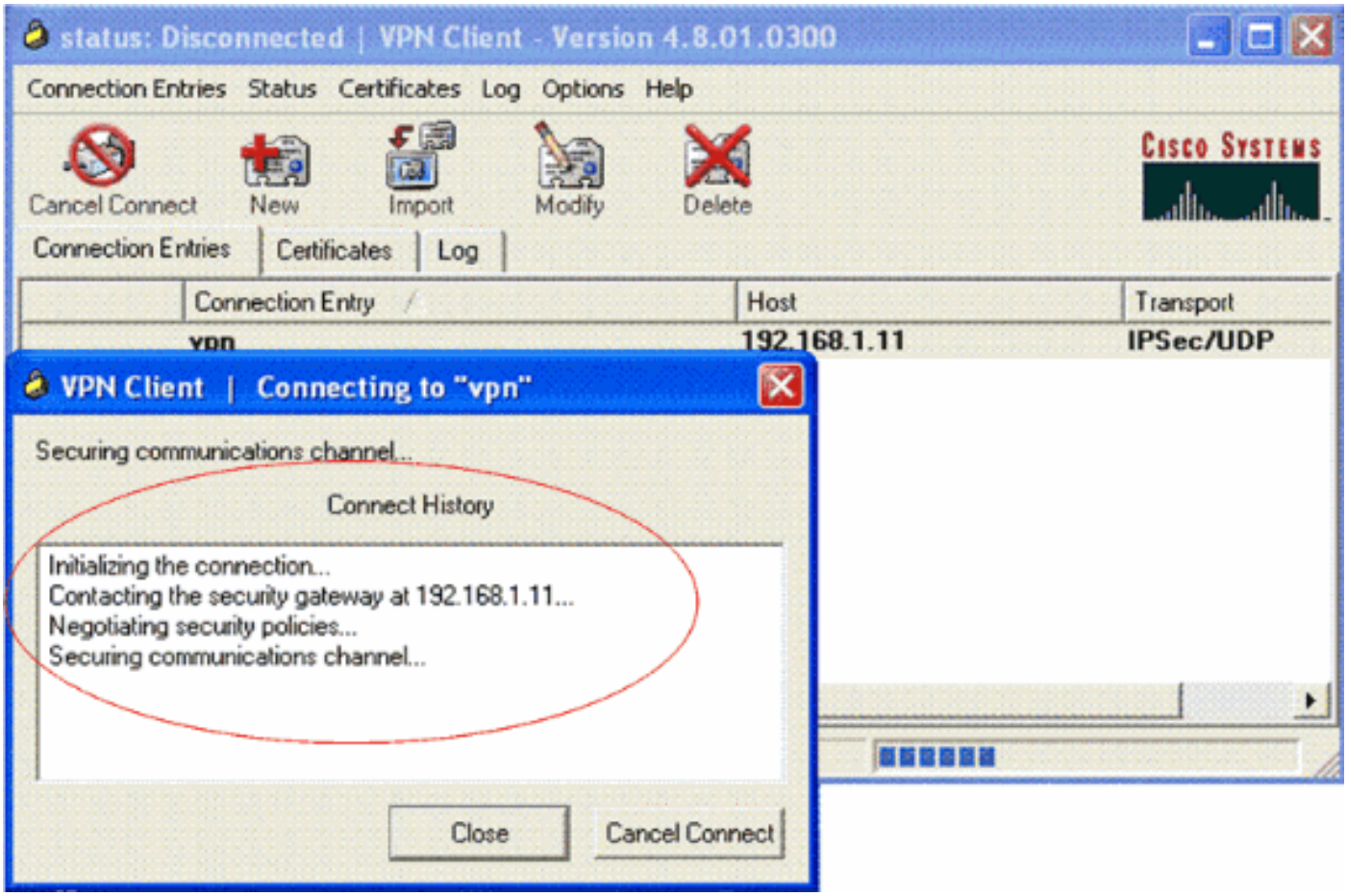
注: ここで設定するグループ名およびパスワードは、VPN サーバに設定されているものと同じにする必要があります。 この例では、名前は *employee*、パスワードは *cisco123* を使用します。

確認

この構成を確認するには、ワイヤレス クライアントの SSID **vpnclient** に、WLC に設定されているものと同じセキュリティ パラメータを設定し、クライアントをこの WLAN に関連付けます。複数のドキュメントで、ワイヤレス クライアントに新しいプロファイルを設定する方法を説明しています。

ワイヤレス クライアントを関連付けたら、VPN Client に移動し設定した接続をクリックします。次に、VPN Client のメイン ウィンドウで [Connect] をクリックします。

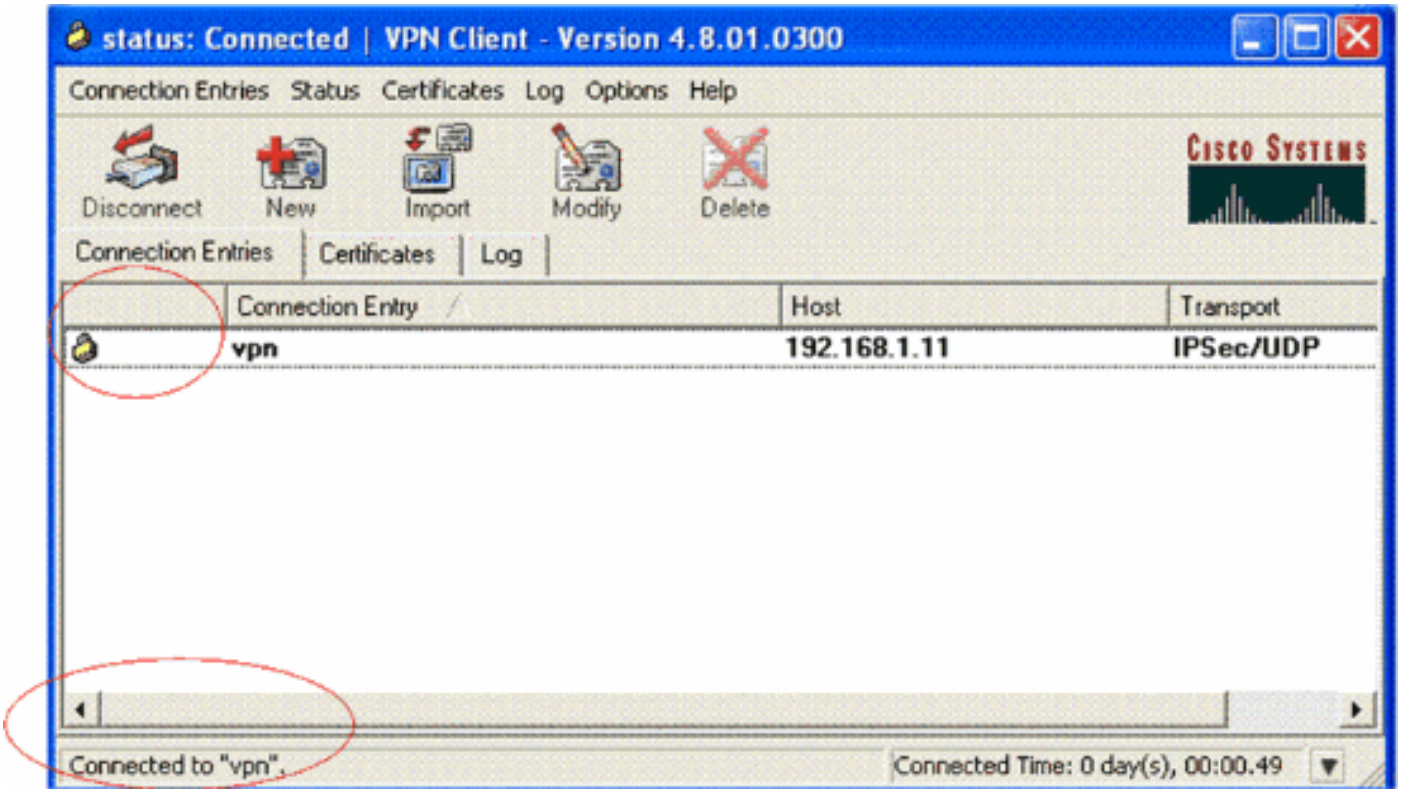
クライアントとサーバ間でネゴシエーションされている、フェーズ 1 およびフェーズ 2 のセキュリティ パラメータが表示されます。



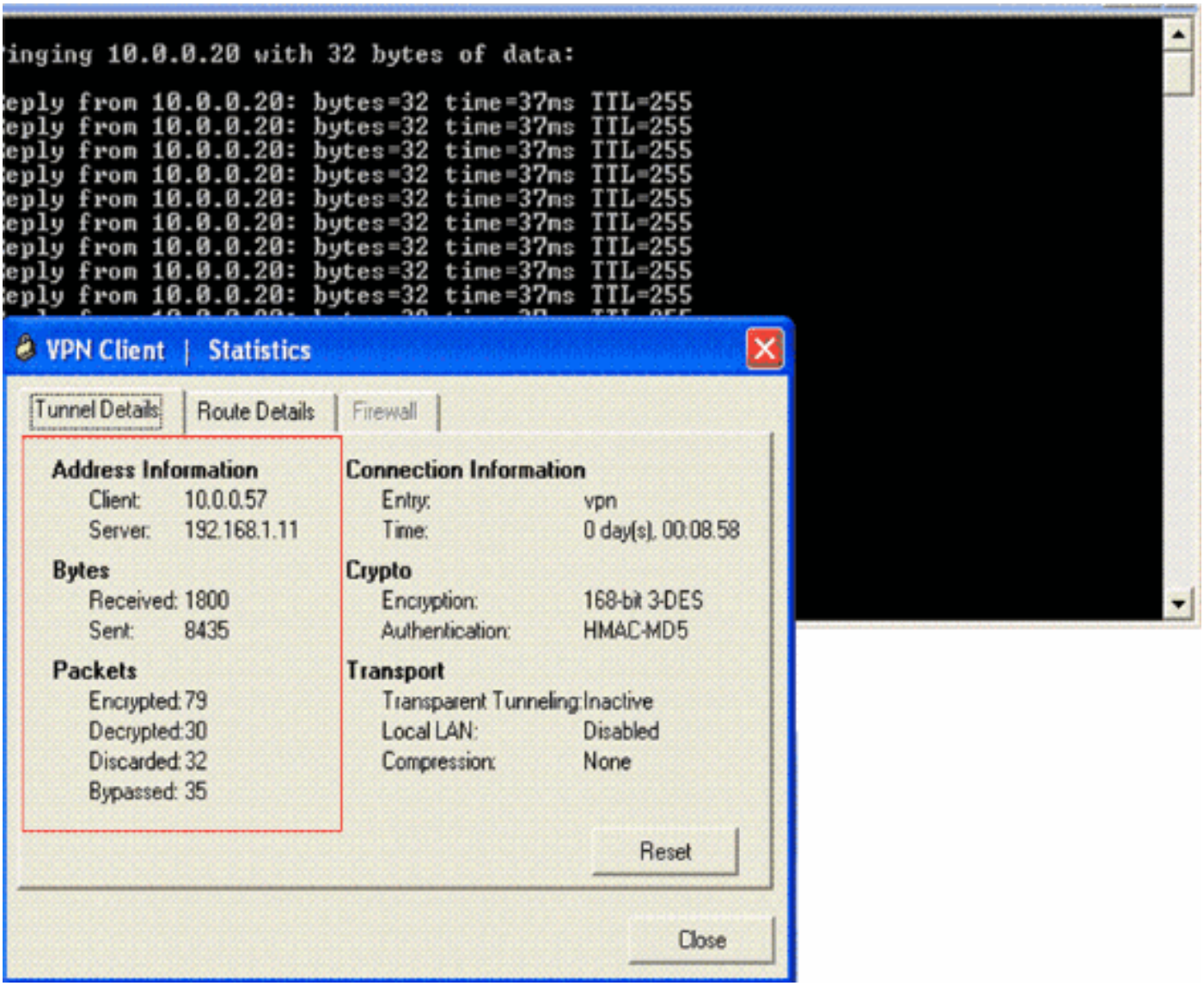
注: この VPN トンネルを確立するには、VPN Client およびサーバ間に IP 到達可能性が必要です。 VPN Client がセキュリティ ゲートウェイ (VPN サーバ) と通信できない場合は、トンネルが確立されていません。クライアント側には次のメッセージを示すアラート ボックスが表示されます。

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

クライアントとサーバの間に VPN トンネルが正しく確立されたことを確認するには、確立された VPN Client の横にロック アイコンが作成されたことを確認します。 また、ステータス バーにも **Connected to "vpn"** と表示されます。 次に例を示します。



また、VPN Client からサーバ側の LAN セグメントに、またサーバ側の LAN セグメントから VPN Client に正常にデータを送信できることを確認します。 VPN Client のメイン メニューで [Status] > [Statistics] を選択します。 ここでは、トンネルを経由してパススルーされた暗号化および復号化パケットの統計情報を確認できます。



このスクリーンショットでは、クライアント アドレスが 10.0.0.57 であることが確認できます。これは、フェーズ 1 ネゴシエーションが成功した後に、VPN サーバにより、VPN サーバのローカルに設定されたプールからクライアントに割り当てられたアドレスです。 トンネルが確立したら、VPN サーバにより、VPN サーバのルート テーブル内の IP アドレスが、この割り当てられた DHCP に自動的に追加されます。

また、クライアントからサーバにデータが転送される間は暗号化パケットの数が増加し、サーバからクライアントにデータが転送される間は復号化パケットの数が増加することが確認できます。

注: WLC には VPN パススルーが設定されているため、クライアントは、パススルーが設定された VPN ゲートウェイ (ここでは 192.168.1.11 の VPN サーバ) に接続したセグメントだけにアクセスできるようになります。 これにより、その他すべてのトラフィックがフィルタリングされます。

同一の設定でその他の VPN サーバを設定し、VPN Client で VPN サーバへの新しい接続エントリを設定することで、上記の状態を確認できます。 この VPN サーバでトンネルの確立を試行すると、今度は失敗します。 これは、WLC によりこのトラフィックがフィルタリングされ、VPN パススルーが設定された VPN ゲートウェイ アドレスへのトンネルだけが許可されるためです。

また、VPN サーバの CLI でも設定を確認できます。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

VPN サーバで使用されているこれらの **show** コマンドは、トンネル状態の確認に役立つ場合があります。

- **show crypto session** コマンドは、トンネル状態の確認に使用します。 次に、このコマンドの出力例を示します。`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`
- **show crypto isakmp policy** は、設定されたフェーズ 1 パラメータを表示するために使用します。

トラブルシューティング

「**確認**」セクションで説明した **debug** および show コマンドもトラブルシューティングに使用できます。

- **debug crypto isakmp**
- **debug crypto ipsec**
- **show crypto session**

- VPN サーバの **debug crypto isakmp** コマンドでは、クライアントとサーバ間のフェーズ 1 ネゴシエーション プロセス全体が表示されます。 次に、フェーズ 1 ネゴシエーションの成功例を示します。`----------`
  `----------`
  `----------`
  `*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`**
- VPN サーバの **debug crypto ipsec** コマンドでは、成功したフェーズ 1 IPSec ネゴシエーションと VPN トンネルの作成が表示されます。 次に例を示します。`----------`
  `----------`
  `----------`
  `----------`
  `----------`

```
*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
```

関連情報

- IPセキュリティ（IPSec）暗号化入門
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- IPsec ネットワーク セキュリティの設定
- Cisco Easy VPN に関する Q&A
- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0
- Wireless LAN Controller での ACL の設定例
- Wireless LAN Controller（WLC）に関する FAQ
- ワイヤレスに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems