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

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 背景説明 リモート アクセス VPN **IPSec** ネットワーク図 設定 VPN 終端およびパススルー WLC への VPN パススルーの設定 VPN Server の設定 VPN Client の設定 確認 トラブルシュート 関連情報

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

<u>要件</u>

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

<u>使用するコンポーネント</u>

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いています。

- ・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:ルータをVPNサーバとして機能させるには、基本的なIPsecをサポートする機能セットを実行 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ました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>表記法</u>

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。

<u>リモート アクセス VPN</u>

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、『<u>IPSec の設定</u>』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、<u>Command Lookup</u> <u>Tool(登録</u>ユーザ専用)を使用してください。

<u>ネットワーク図</u>

このドキュメントでは、次の構成を使用します。

- •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:ライブネットワークでは、このデフォルトゲートウェイは、WLCを他のネットワークやインターネットに接続する即時ルータの着信インターフェイスを指している必要があります。
- 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している必要があります。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。



<u>設定</u>

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 <u>AP (LAP)の登録</u>』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。

Cisco - Microsoft Inter	net Explorer	NAKITAR	and a state of the	(ara na isa da ara	ringinen zinais:		analyningeneing		_ PX
File Edit View Favorites	Tools Help	Sec. 1	100000000000						unis 🍽 🖓
Cisco Svorcan							Save Co	nfiguration Ping	Logout Refresh
A.A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	come Mascall combrad of all all of a state
WLANS	WLANs >	New						< Back	Apply
WLANS WLANS	WLAN ID		1 🛩						
AP Groups VLAN	WLAN SS	ID	vpnclient						
CLAINPACCALIS.									
2 Done								🔒 🔮 📾	ternet

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。

Cisco - Microsoft Interne	t Explorer				
File Edit View Favorites	Tools Help				Unis 🎽 🧖
Cinco Sverzma				Save Configurat	ion Ping Logout Refres
AA	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	
WLANS WLANS WLANS AP Groups VLAN	7920 Phone Support Broadcast SSID Aironet IE Allow AAA Override Client Exclusion DHCP Server	Chent CAC Limit A Chent CAC Limit A Enabled Enabled Enabled Enabled Coverride	P CAC Limit Velue (secs)	* Web Policy cannot with IPsec and L2TP ** When client excli- value of zero means administrative overn clients) *** CKIP is not sup	be used in combination usion is enabled, a timeout infinity(will require ide to reset excluded ported by 10xx APs
	DHCP Addr. Assignment Interface Name MFP Version Required MFP Signature Generation H-REAP Local Switching * H-REAP Local Switching FORTRESS authentication Radius Servers	Required management i (Global MFP Disabled) ord supported with IPSEC, s.) L2TP, PPTP, CRANITE and		
	Server 1 Server 2 Server 3 WPA1+WPA2 Parameters	Authentication Servers	Accounting Servers		
	WPA1 Policy WPA1 Encryption WPA2 Policy Auth Key Mgmt PSK format	AES TKIP PSK V asci V			

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

Cisco - Microsoft Interne	t Explorer			
File Edit View Favorites	Tools Help	<mark>n ha distant na sana an</mark> an	a shina ku shi a shina i	Links 🎽 🦓
Cinca Svarema			Save Configura	ation Ping Logout Refresh
A. A.	MONITOR WLANS CO	INTROLLER WIRELESS SECURITY MANAGEMENT	r commands hel	P
WLANS	WLANs > Edit			< Back Apply
WLANs	WLAN ID	1		
WLANS AP Groups VLAN	WLAN SSID	vpnclient		
	General Policies		Security Policies	
	Radio Policy	All V	1	WD41 (WD42
	Admin Status	✓ Enabled	Layer 2 Security	WPA1+WPA2
	Session Timeout (secs)	0		MAC Filtering
	Quality of Service (QoS)	Silver (best effort)	Layer 3 Security	None 👻
	WMM Policy	Disabled 💌		None White Parce Through
	7920 Phone Support	Client CAC Limit 🔄 AP CAC Limit		ALL LESS THOMAST.
	Broadcast SSID	Enabled		
	Aironet IE	Enabled	* Web Policy canno with IPsec and L2T	ot be used in combination P.
	Allow AAA Override	Enabled	** When client exc	lusion is enabled, a timeout
	Client Exclusion	Enabled ** 60 Timeout Value (secs) value of zero means infinity(will require administrative override to reset exclusion of the sect exclu		
	DHCP Server	🔄 Override	*** CKIP is not su	pported by 10xx APs
	DHCP Addr. Assignment	Required		
	Interface Name	management 💌		
	MFP Version Required	1		
	MFP Signature Generation	✔ (Global MFP Disabled)		
	H-REAP Local Switching			
	* H-REAP Local Switching FORTRESS authentication	not supported with IPSEC, L2TP, PPTP, CRANITE and s.		
	Radius Servers			
		Authentication Servers Accounting Servers		5
Done				🔒 🌒 Internet

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。

Cisco - Microsoft Interne	t Explorer				
File Edit View Favorites	Tools Help				Unis 🎽 🦂
Cisco Systems				Save Configuration	Ping Logout Refrest
<u>A.</u>	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	
WLANS WLANS AP Groups VLAN	Allow AAA Override Client Exclusion DHCP Server DHCP Addr. Assignment Interface Name MFP Version Required MFP Signature Generation H-REAP Local Switching * H-REAP Local Switching FORTRESS authentication Radius Servers	Enabled Enabled ** 60 Timeout Override Required management 1 (Global MFP Disabled not supported with IPSEC, s.	Value (secs))) L2TP, PPTP, CRANITE and	 ** When client exclusion value of zero means infi administrative override clients) *** CKIP is not support 	n is enabled, a timeout inity(will require to reset excluded led by 10xx APs
	Server 1 Server 2 Server 3 WPA1+WPA2 Parameters WPA1 Policy WPA1 Encryption WPA2 Policy Auth Key Mgmt PSK format VPN Pass Through	Authentication Servers	Accounting Servers		

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。



<u>VPN Server の設定</u>

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

注: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の間にIP到達可能性がない場合、トンネルは確立されません。

注:このドキュメントでは、ユーザがネットワークでダイナミックルーティングを有効にする方 法を認識していることを前提としています。

Cisco 3640 ルータ
vonrouter# 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
1
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
1
aaa authorization network employee local
aaa session-id common
1
resource policy
1
memory-size iomem 10
!
!
ip cef
no ip domain lookup
1
1
1
1
1
!
1
1
1
1
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
1
!--- 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-gueue
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:一部のシスコソフトウェアでは、CCOユーザ名とパスワードを使用してログインする必要が あります。

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。

Status: Disconnected VPN Client - Version 4.8.0	01.0300	
Connection Entries Status Certificates Log Options Help		
Connect New Import Modify Delete		Cisco Systems
Connection Entry	Host	Transport
1		
Not connected.		T

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。

🧔 status: Disconnected VPN	Client - Version 4.8.01.0300	_
Connection Entries Status Certificat	es Log Options Help	
Connect New Import	Modify Delete	Cisco Systems
VPN Client Create New VP	N Connection Entry	Transact
Connection Entry: vpn		Transport
Description		
Host 192.168.1.11		
Authentication Transport Backup	Servers Dial-Up	
Group Authentication	C Mutual Group Authentication	
Name: employee		
Password:		.
Confirm Password:		
C Certificate Authentication		
Name:	<u>*</u>	
Send CA Certificate Chain		
Prove Harry Providence A		

注:ここで設定する[Group Name]と[Password]は、VPNサーバで設定したものと同じにす 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。* 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。

Status: Disconnected VPN Client - Version 4.8.	.01.0300	🖃 🗖 🔀
Connection Entries Status Certificates Log Options Help		
Cancel Connect New Import Modify Del	lete	CISCO SYSTEMS
Connection Entries Certificates Log		
Connection Entry	Host	Transport
nav	192.168.1.11	IPSec/UDP
VPN Client Connecting to "vpn"		
Securing communications channel		
Connect History		
Initializing the connection Contacting the security gateway at 192.168.1.11 Negotiating security policies Securing communications channel)
Close Cancel Co	nnect	

注:このVPNトンネルを確立するには、VPN Clientとサーバの間に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。

Status: C	onnected VPN Clie	nt - Version 4.8.01	.0300	
Connection En	tries Status Certificates	s Log Options Help		
Disconnect	New Import	Modify Delet		CISCO SYSTEMS
Connection Er	Itries Certificates Lo	og	Hot	Transport
a	VDD		192,168,1,11	IPSec/UDP

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。

inging 10.0.0.20 with eply from 10.0.0.20: b eply from 10.0.0.20: b	32 bytes of data ytes=32 time=37r ytes=32 time=37r ytes=32 time=37r ytes=32 time=37r ytes=32 time=37r ytes=32 time=37r ytes=32 time=37r ytes=32 time=37r ytes=32 time=37r	a: as IIL=255 as IIL=255	
Tunnel Details Route Details Address Information Client: 10.0.0.57 Client: 192.168.1.11 Bytes Received: 1800 Sent: 8435 Packets Encrypted: 79 Decrypted: 30 Discarded: 32 Bypassed: 35	Firewall Connection Informat Entry: Time: Crypto Encryption: Authentication: Transport Transparent Tunnel Local LAN: Compression:	ion vpn 0 day(s), 00:08:58 168-bit 3-DES HMAC-MD5 ing:Inactive Disabled None Reset Close	•

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と表示されています。これは、 フェーズ1ネゴシエーションが成功した後、VPNサーバが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るアドレスです。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はVPNパススルー用に設定されているため、クライアントはパススルー用に設定された VPNゲートウェイ(ここでは192.168.1.11 VPNサーバ)に接続されたセグメントにのみアクセスで きます。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。

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。 注:<u>debug</u> 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。

<u>トラブルシュート</u>

「**確認**」セクションで説明した debug および <u>show</u> 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
                                hash MD5
*Aug 28 10:37:29.515: ISAKMP:
*Aug 28 10:37:29.515: ISAKMP:
                                default group 2
                                auth pre-share
*Aug 28 10:37:29.515: ISAKMP:
*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。以下が一例です。

```
_____
_____
*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,
```

```
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)暗号化の概要
 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

- <u>Cisco Easy VPN に関する Q&A</u>
- 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
- ・<u>Wireless LAN Controller での ACL の設定例</u>
- ・<u>Wireless LAN Controller (WLC)に関する FAQ</u>
- ・<u>ワイヤレスに関するサポート ページ</u>
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>