事前共有キーを使用して Windows 8 PC と ASA の間の L2TP over IPSec を設定する

内容

概要 前提条件 要件 制約事項 使用するコンポーネント 表記法 背景説明 設定 ネットワーク図 完全なトンネル設定 Adaptive Security Device Manager(ASDM)を使用したASAの設定 CLIを使用したASAの設定 Windows 8 L2TP/IPsecクライアントの設定 Split-tunnel 設定 ASAでの 設定 L2TP/IPsecクライアントの設定 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、Cisco適応型セキュリティアプライアンス(ASA)とWindows 8ネイティブ クライアント間の事前共有キーを使用して、IPsec上でレイヤ2トンネリングプロトコル(L2TP)を 設定する方法について説明します。

L2TP over Internet Protocol(IPsec)セキュリティは、L2TP Virtual Private Network(VPN)ソリュー ションを、IPsec VPNおよびファイアウォールサービスとともに1つのプラットフォームに導入し 、管理する機能を提供します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

 クライアントマシンからASAへのIP接続。接続をテストするには、クライアントエンドポイントからASAのIPアドレスをpingし、クライアントエンドポイントからASAのIPアドレスを pingします • UDPポート500および4500およびEncapsulating Security Payload(ESP)プロトコルが、接続のパス上のどこでもブロックされていないことを確認します

制約事項

- L2TP over IPsecはIKEv1のみをサポートし、IKEv2はサポートしません。
- ASA上のL2TPにより、LNSはWindows、MAC OS X、Android、およびCisco IOSなどのオペレーティングシステムに統合されたネイティブVPNクライアントと相互運用できます。 IPsecを使用するL2TPのみがサポートされ、ネイティブL2TP自体はASAではサポートされません。
- WindowsクライアントでサポートされるIPsecセキュリティアソシエーションの最小ライフタイムは300秒です。ASAのライフタイムが300秒未満に設定されている場合、Windowsクライアントはそれを無視し、300秒のライフタイムに置き換えます。
- ASAは、ローカルデータベース上で、Point-to-Point Protocol(PPP)認証Password Authentication Protocol(PAP)およびMicrosoft Challenge-Handshake Authentication Protocol(CHAP)バージョン1および2のみをサポートします。Extensible Authentication Protocol(EAP)およびCHAPは、プロキシ認証サーバによって実行されます。したがって、リ モートユーザがauthentication eap-proxyまたはauthentication chapコマンドで設定されたトン ネルグループに属し、ASAがローカルデータベースを使用するように設定されている場合、 そのユーザは接続できません。

サポートされるPPP認証タイプ

ASA上のL2TP over IPsec接続では、表に示すPPP認証タイプだけがサポートされます

	AAAサーバサ	ポートとPPP認証タイプ
AAAサーバタィ	イプ サ	・ポートされるPPP認証タイプ
LOCAL	PA	AP、MSCHAPv1、MSCHAPv2
RADIUS	PAP、CHAP	、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+		PAP、CHAP、MSCHAPv1
[LDAP]		PAP
NT		PAP
Kerberos		PAP
SDI		SDI
PPP認証タイプの	の特性	
キーワード	認証タイプ	
chap	CHAP	サーバのチャレンジに応答して、クライアントは暗号化された[chal
eap-proxy	EAP	セキュリティアプライアンスがPPP認証プロセスを外部RADIUS認識
Micr	osoft CHAP、バー	
ms-chap-v1	ジョン1	CHAPに似ていますが、CHAPのように、クリアテキストのパスワー
ms-chap-v2 Micr	osoft CHAP、バー	
	ジョン、2	
рар	PAP	認証中にクリアテキストのユーザ名とバスワードを渡し、セキュア

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いています。

• ソフトウェアバージョン9.4(1)が稼働するCisco 5515シリーズASA

• L2TP/IPSecクライアント(Windows 8)

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 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

関連製品

この設定は、Cisco ASA 5500 シリーズ セキュリティ アプライアンス 8.3(1) 以降にも使用できます。

表記法

ドキュメント表記の詳細<u>は、『シスコテクニカルティップス</u>の表記法』を参照してください

背景説明

レイヤ2トンネリングプロトコル(L2TP)は、リモートクライアントがパブリックIPネットワークを 使用して企業のプライベートネットワークサーバと安全に通信できるようにするVPNトンネリン グプロトコルです。L2TPはPPP over UDP(ポート1701)を使用してデータをトンネルします。

L2TPプロトコルは、クライアント/サーバモデルに基づいています。この機能は、L2TPネットワ ークサーバ(LNS)とL2TPアクセスコンセントレータ(LAC)の間で分割されます。 LNSは通常、 ASAなどのネットワークゲートウェイで動作しますが、LACはダイヤルアップネットワークアク セスサーバ(NAS)またはMicrosoft Windows、Apple iPhone、Androidなどのバンドルされた L2TPクライアントを備えたエンドポイントデバイスです。

設定

このセクションでは、このドキュメントで説明する機能を設定するための情報を提供します。

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、コマンド検索ツール (登録ユーザ専用)を使用してください。

注:この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティ ング可能なものではありません。これらは RFC 1918 で使用されているアドレスであり、 ラボ環境で使用されたものです。

ネットワーク図



完全なトンネル設定

Adaptive Security Device Manager(ASDM)を使用したASAの設定

次のステップを実行します。

ステップ1:ASDMにログインし、[Wizards] > [VPN Wizards] > [Ipsec (IKEv1) Remote Access VPN Wizard] に移動します。

🔂 Cis	🧧 Cisco ASDM 7.2 for ASA - 10.106.44.216						
File	View To	ools	Wizards	Window Help			
<u></u>	Home 🖓	Conf	f Startup Wizard Back 🚺		k 🔿 Forward 🦻 Help		
~	VPN Wizards			Site-to-site VPN Wizard			
Devi	ice List		Hi	gh Availability and Scalability Wizard	- -	AnyConnect VPN Wizard	
🖶 Add 📋 Delete		Un	Unified Communication Wizard		Clienthers CCL VDN1//Great		
Find:		_	01	ined communication wizard		Clientless SSL VPIN Wizard	
	10 105 13	0.63	Packet Capture Wizard IPsec (IKEv1) Remote Access VPN Wizard				

ステップ2:[Remote Access VPN setup]ウィンドウが表示されます。ドロップダウンリストから、 VPNトンネルを終端するインターフェイスを選択します。この例では、外部インターフェイスは WANに接続されているため、このインターフェイスでVPNトンネルを終端します。[Enable inbound IPSec sessions to bypass **interface access lists]ボックスをオンのままにします。グルー プポリシーとユーザごとの許可アクセスリストは、チェックされたトラフィックに適用さ**れ、ク ライアントが内部リソースにアクセスできるように外部インターフェイスで新しいアクセスリス トを設定する必要はありません。[next] をクリックします。



ステップ3:この図に示すように、PAPはセキュアではなく、他の認証タイプはLOCAL認証デー タベースでサポートされていないため、PAPをPAPとしてL2TP over IPSec、MS-CHAP-V1、MS-CHAP-CHAP-V2 [Next] をクリックします。

🔄 VPN Wizard	×
VPN Wizard	Remote Access Client (Step 2 of)
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
SET ISP	VPN Client Type:
	Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product
Home	Microsoft Windows client using L2TP over IPsec
Corporate	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
The said	PAP CHAP MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
	Specify if the client will send tunnel group name as - username@tunnelgroup.
THUILIN	Client will send tunnel group name as username@tunnelgroup.
TTT	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
- B-	
	< Back Next > Finish Cancel Help

ステップ4:認証方式として**Pre-shared-keyを選択し**て、クライアント側でも同じである必要があ る事前共有キーを入力し、次の図に示すようにNextをクリックします。

📑 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
VPN WIZARU	Which Clear Authentication Method and Tunnel Group Name (Step 3 or) The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client. Authentication Method Pre-shared key Pre-shared Key: Clsc0@123 Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK) Tunnel Group For VPN clients using L2TP over IPsec with pre-shared key authentication, DefaultRAGroup tunnel group name to used. Tunnel Group Name: DefaultRAGroup
	< Back Next > Finish Cancel Help

ステップ5:L2TP over IPsec接続を試行するユーザを認証する方法を指定します。外部AAA認証サ ーバまたは独自のローカルデータベースを使用できます。ASAのロー**カル・データベースに対し** てクライアントを認証する場合は、[Authenticate using the local user database]を選択し、 [Next]をクリック**します。**

注:外部AAAサーバを使用してユーザを認証するに<u>は、「VPNユーザのRADIUS認証</u>の設定」を参照してください。

🔄 VPN Wizard					
VPN Wizard	Client Authentication (Step 4 of)				
Branch Branch Branch Home Branch Home Branch	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.				
	< Back Next > Finish Cancel Help				

ステップ6:ユーザ認証用にローカルデータベースに新しいユーザを追加するには、ユーザ名とパ スワードを入力し、[ADD]をクリックします。それ以外の場合は、データベース内の既存のユー ザアカウントを使用できます(次の図を参照)。[next] をクリックします。

🕞 VPN Wizard		in the second se	×
VPN Wizard	User Accounts (Step 5 of 11) Add new users into the user auther or to remove them from the databa Users/AAA > User Accounts in the r User to Be Added Username: test	ntication database. To edit existin ise, go to Configuration > Device main ASDM window.	ng entries in the database Management >
	Password (optional): Confirm Password (optional):	Oelete < Back Next >	inish Cancel Help

ステップ7:ドロップダウンリストから、クライアントへのIPアドレスの割り当てに使用するアド レスプールを選択します。新しいアドレスプールを作成するには、次の図に示すように[New]をク リックします。

C VPN Wizard		J
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Franch Franch Franch Franch Franch	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporate Network	Tunnel Group Name : DefaultRAGroup	
THE SHA	Pool Name: New	
	Pool Settings	
THUIM	Range Start Address:	
Think	Range End Address:	
	Subnet Mask:	
	< Back Next > Finish Cancel Help	

- ステップ8:[**Add IPv4 Pool**]ダ**イアログボックス**が表示されます。
 - 1. 新しい IP アドレス プールの名前を入力します。
 - 2. 最初と最後の IP アドレスを入力します。
 - 3. サブネットマスクを入力し、 **OK**.

is VPN Wizard		23
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Franch Soft	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote clients.	VPN
Home	🖬 Add IPv4 Pool	
Corporate Network	Name: Address-pool	
Ection 10	Starting IP Address: 192.168.1.1	
	Ending IP Address: 192.168.1.254	
LUU III	Subnet Mask: 255.255.255.0	
The	OK Cancel Help	
	Subjections.	
	< Back Next > Finish Cancel	Help

ステップ9 : プール設定を確認し、[**Next**]をクリック**します。**

VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch Franch Former	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate Network	Tunnel Group Name : DefaultRAGroup
Frank JAN	Pool Name: Address-pool New
	Pool Settings
THUM	Range Start Address: 192.168.1.1
T	Range End Address: 192.168.1.254
	Subnet Mask: 255.255.0
	< Back Next > Finish Cancel Help

ステップ10:クライアントにプッシュする属性を設定するか、空のままにして[**Next**]をクリック **します。**

T VPN Wizard		×
VPN Wizard	Attributes Pushed to Client (Optional)(Step 7 of 11)
Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blar		ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate Natwork	Tunnel Group:	DefaultRAGroup
No.	Primary DNS Server:	8.8.8
	Secondary DNS Server:	4.4.4.2
-Tunt	Primary WINS Server:	
-I-I-I	Secondary WINS Server:	
	Default Domain Name:	cisco.com
		< Back Next > Finish Cancel Help

ステップ 11:一部のクライ**アント・プラットフォームでこの機能がサポートされてい**ないため、 [Enable Perfect Forwarding Secrecy (PFS)]ボックスがオフになっていることを確認します。スプ リットトンネリングを有効にすると、リモートユーザが上記で定義したリソースに同時に暗号化 アクセスでき、インターネットボックスへの暗号化されていないアクセスはオフです。これは、 クライアントマシンからのすべてのトラフィック(インターネットトラフィックを含む)が ASAに送信されます。[next] をクリックします。

VPN Wizard		
VPN Wizard	IPsec Settings (Optional) (Step 8 of 11)	
Branch Frank	Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN. To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the Exempt Networks field blank.	
Corporate Network	Interface: outside Exempt Networks: .	
	 Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet. Enable Perfect Forwarding Secrecy (PFS) Diffie-Hellman Group: 	
	< <u>Back</u> <u>Next</u> > <u>Finish</u> <u>Cancel</u> <u>Help</u>	

ステップ12:サマリー情報を確認し、[完了]をクリック**します。**



CLIを使用したASAの設定

ステップ1:IKEフェーズ1ポリシーパラメータを設定します。

このポリシーは、ピア間の制御トラフィックを保護するために使用されます(つまり、事前共有 キーとフェーズ2ネゴシエーションを保護します)

ciscoasa(config)#crypto ikev1 policy 10 ciscoasa(config-ikev1-policy)#authentication pre-share ciscoasa(config-ikev1-policy)#encryption 3des

- ciscoasa(config-ikev1-policy)#hash sha
- ciscoasa(config-ikev1-policy)#group 2
- ciscoasa(config-ikev1-policy)#lifetime 86400
- ciscoasa(config-ikev1-policy)#exit

ステップ2:トランスフォームセットを設定します。

データトラフィックを保護するために使用されるIKEフェーズ2ポリシーパラメータが含まれてい ます。Windows L2TP/IPsecクライアントはIPsecトランスポートモードを使用するため、モード をtransportに設定します。デフォルトはトンネルモードです

ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport ステップ3:ダイナミックマップを設定します。

WindowsクライアントがISPまたはローカルDHCPサーバ(モデムなど)の前にダイナミックIPア

ドレスを取得すると、ASAはピアのIPアドレスを認識しないため、ASA側のスタティックピアの 設定に問題が生じます。そのため、ダイナミッククリプト設定にアプローチする必要があります 。クライアントからのIPSecネゴシエーションの結果として、すべてのパラメータが必ずしも定 義されず、欠落しているパラメータが後で動的に学習されます。

ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

ステップ4:ダイナミックマップをスタティック暗号マップにバインドし、暗号マップを適用して、外部インターフェイスでIKEv1を有効にします

ダイナミック暗号マップはインターフェイスに適用できないため、スタティック暗号マップにバ インドします。ASAが最初に他の暗号マップを評価できるように、ダイナミック暗号セットは、 暗号マップセット内で最も低い優先順位の暗号マップである必要があります(つまり、最も高い シーケンス番号が必要です)。他の(スタティック)マップエントリが一致しない場合にのみ、 ダイナミッククリプトマップセットが検査されます。

ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map ciscoasa(config)#crypto map outside_map interface outside ciscoasa(config)#crypto ikev1 enable outside ステップ5:IPアドレスプールの作成

IPアドレスがリモートVPNクライアントに動的に割り当てられるアドレスのプールを作成します。ASAで既存のプールを使用するには、この手順を無視します。

ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0 ステップ6:グループボリシーの設定

グループポリシーを内部として識別します。つまり、属性がローカルデータベースから取得され ます。

ciscoasa(config)#group-policy L2TP-VPN internal

注:L2TP/IPsec接続は、デフォルトのグループポリシー(DfltGrpPolicy)またはユーザ定義の グループポリシーで設定できます。どちらの場合も、L2TP/IPsecトンネリングプロトコル を使用するようにグループポリシーを設定する必要があります。デフォルトのグループポリ シーのVPNプロトコル属性にI2tp-ipsecを設定します。このグループポリシーは、vpnprotocol属性が設定されていない場合、ユーザ定義のグループポリシーに継承されます。

vpn tunnel protocol(vpn tunnel protocol)(この例ではl2tp-ipsec)、ドメイン名、DNSおよび WINSサーバのIPアドレス、および新しいユーザアカウントなどの属性を設定します

- ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
- ciscoasa(config-group-policy)#default-domain value cisco.com

AAAの使用に加えて、デバイスのユーザ名とパスワードを設定します。ユーザがMicrosoft CHAPバージョン1またはバージョン2を使用するL2TPクライアントであり、ASAがローカルデー タベースに対して認証するように設定されている場合は、mschapキーワードを含める必要があり ます。たとえば、username <username> password <password> mschap。

ciscoasa(config)#group-policy L2TP-VPN attributes

ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2

tunnel-groupコマンドを使用してトンネルグループを作成し、IPアドレスをクライアントに割り当 てるために使用するローカルアドレスプール名を指定します。認証方式が事前共有キーの場合、 トンネルグループ名はDefaultRAGroupである必要があります。これは、クライアントにトンネル グループを指定するオプションがなく、デフォルトのトンネルグループのみに到達するためです 。default-group-policyコマンドを使用して、グループポリシーをトンネルグループにバインドし ます

ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes ciscoasa(config-tunnel-general)#address-pool Address-pool ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN ciscoasa(config-tunnel-general)#exit

注:事前共有キーベースの認証が実行される場合は、デフォルトの接続プロファイル(トン ネルグループ)、DefaultRAGroupを設定する必要があります。証明書ベースの認証を実行 すると、証明書の識別子に基づいてユーザ定義接続プロファイルを選択できます

tunnel-group ipsec-attributesコマンドを使用して、事前共有キーを設定するためにipsecattributeコンフィギュレーションモードに入ります。

ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key C!sc0@123 ciscoasa(config-tunnel-ipsec)#exit

tunnel group ppp-attributesモードから**authentication typeコマンドを**使用して、PPP認証プロトコ ルを設定します。AAAサーバがローカルデータベースとして設定されている場合、CHAPはサポ ートされないため、デフォルトで有効になっているCHAPを無効にします。

ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes ciscoasa(config-ppp)#no authentication chap ciscoasa(config-ppp)#authentication ms-chap-v2 ciscoasa(config-ppp)#exit ステップ8:NAT免除の設定

クライアントが内部インターフェイスに接続された内部リソースにアクセスできるように、 NAT免除を設定します(この例では、内部リソースは内部インターフェイスに接続されています)。

ciscoasa(config)#object network L2TP-Pool ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0 ciscoasa(config-network-object)#exit ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp route-lookup 完全な設定例

crypto ikev1 policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 exit crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map crypto map outside_map interface outside crypto ikev1 enable outside ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0 group-policy L2TP-VPN internal group-policy L2TP-VPN attributes vpn-tunnel-protocol l2tp-ipsec default-domain value cisco.com username test password test mschap exit tunnel-group DefaultRAGroup general-attributes address-pool Address-pool default-group-policy L2TP-VPN exit tunnel-group DefaultRAGroup ipsec-attributes ikev1 pre-shared-key C!sc0@123 exit tunnel-group DefaultRAGroup ppp-attributes no authentication chap authentication ms-chap-v2 exit object network L2TP-Pool subnet 192.168.1.0 255.255.255.0

exit nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp route-lookup

Windows 8 L2TP/IPsecクライアントの設定

1.コントロールパネルを開き、[ネットワークと共有センター]を選択します。



2. [新しい接続またはネットワークの設定]オプションを選択します。

Image: Set also Set also Set also NomeGroup Internet Options Windows Firewall	¥	Network and Sharing Center	- 🗆 🗙	
Control Panel Home Change adapter settings Change advanced sharing settings Network 2 Public network Connections: Change vour networking settings	🛞 🌛 👻 🕇 💺 « All Control P	anel Items 🔸 Network and Sharing Center	✓ ♂ Search Control Panel	
Change adapter settings Change advanced sharing settings Public network Public network Access type: No Internet access Connections: © Etherne Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Image: Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information. See also HomeGroup Internet Options Windows Firewall	Control Panel Home	View your basic network information and set up connections		
Change advanced sharing settings Network 2 Access type: No Internet access Public network Connections: Etheme Etheme Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Image your networking settings Set up a hew connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Image your network problems Diagnose and repair network problems, or get troubleshooting information. See also HomeGroup Internet Options Windows Firewall	Change adapter settings	View your active networks		
Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Image: Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information. See also HomeGroup Internet Options Windows Firewall	Change advanced sharing settings	Network 2 Public network	Access type: No Internet access Connections:	
See also HomeGroup Internet Options Windows Firewall		Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information.		
HomeGroup Internet Options Windows Firewall	See also			
Windows Firewall	HomeGroup			
	Windows Firewall			

3. 「ワークプレイス**に接続」オプションを選択**し、「次へ」をクリ**ックしま**す。

	- '	×	
📀 🔮 Set Up a Connection or Network			
Choose a connection option			
Connect to the Internet Set up a broadband or dial-up connection to the Internet.			
Set up a new network Set up a new router or access point.			
Connect to a workplace Set up a dial-up or VPN connection to your workplace.			
Next	_	Concol	1
Next		Cancel	

4. [Use my Internet connection (VPN)]オプションをクリックします。



5. ASAのWANインターフェイスまたはFQDNのIPアドレスと、ローカルで有効なVPNアダプタの 任意の名前を入力し、[**Create**]をクリック**します。**

			-		^
€	Connect to a Workpl	ace			
	Type the Internet addre	ess to connect to			
	Your network administrator o	an give you this address.			
	Internet address:	172.16.1.2			
	Destination name:	L2TP VPN			
	Use a smart card				
	 Remember my creder 	ntials			
	Allow other people to This antion allows are	use this connection			
	This option allows any	yone with access to this computer to use this connection.			
		Creat	e	Cano	:el

6. [ネットワークと共有センター]で、ウィンドウの左ペイン**にある[アダ**プタ設定の変更]オプショ ンを選択します。



7. L2TP VPN用に最近作成したアダプタを右クリックし、[Properties]を選択します。



8. [Security] タブに移動し、[Type of VPN]で[**Layer 2 Tunneling Protocol with IPsec** (L2TP/IPsec)]を選択して、[Advanced settings]をクリックします。

L2TP VPN Properties					
General Options Security Networking Sharing					
Type of VPN:					
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec) ✓					
Data encryption:					
Require encryption (disconnect if server declines)					
Authentication					
O Use Extensible Authentication Protocol (EAP)					
\checkmark					
Properties					
O Allow these protocols					
Unencrypted password (PAP)					
Challenge Handshake Authentication Protocol (CHAP)					
Microsoft CHAP Version 2 (MS-CHAP v2)					
Automatically use my Windows logon name and password (and domain, if any)					
OK Cancel					

9. tunnel-group **DefaultRAGroup**で指定した事前共有キーを入力し、[**OK**]をク**リックします**。この 例では、事前共有キーとしてC!sc0@123が使用されています。

Advanced Properties
L2TP
Use preshared key for authentication Key: C!sc0@123
 ◯ Use certificate for authentication ✓ Verify the Name and Usage attributes of the server's certificate
OK Cancel

10. [Allow these protocols]で認証方式を選択し、[**Microsoft CHAP Version 2 (MS-CHAP v2)]チェ ックボックスだけがオンになっていることを確認**し、[**OK**]をクリック**します**。

General Options Security Networking Sharing Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec) Advanced settings Advanced settings Data encryption: Require encryption (disconnect if server declines) Authentication Use Extensible Authentication Protocol (EAP) Properties Image: Allow these protocols Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any)	L2TP VPN Propertie	es ×
Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec) Advanced settings Data encryption: Require encryption (disconnect if server declines) Authentication Use Extensible Authentication Protocol (EAP) Properties Allow these protocols Allow these protocols Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any)	General Options Security Networking Sh	aring
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec) Advanced settings Data encryption: Require encryption (disconnect if server declines) Authentication Use Extensible Authentication Protocol (EAP) Properties Image: Allow these protocols Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Image: Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any)	Type of VPN:	
Advanced settings Data encryption: Require encryption (disconnect if server declines) Authentication Use Extensible Authentication Protocol (EAP) Properties Image: Allow these protocols Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any)	Layer 2 Tunneling Protocol with IPsec (L2TP)	/IPsec) ∨
Require encryption (disconnect if server declines) Authentication Use Extensible Authentication Protocol (EAP) Properties Image: Allow these protocols Image: Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Image: Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any)	Data encryption:	Advanced settings
Authentication Use Extensible Authentication Protocol (EAP) Properties Allow these protocols Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any)	Require encryption (disconnect if server decli	nes) 🗸 🗸
 Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any) 	Use Extensible Authentication Protocol (E	AP)
	 Unencrypted password (PAP) Challenge Handshake Authentication Microsoft CHAP Version 2 (MS-CHAP) Automatically use my Windows log password (and domain, if any) 	Protocol (CHAP) v2) on name and

11. [Network Connections]で、[L2TP VPN adapter]を右クリックし、[**Connect/Disconnect**]を選択 します。



12. [Networks]アイコンがポップアップし、[L2TP VPN connection]をクリックします。

P	Network Connections	Networks	
🔄 🄄 🔻 🛉 🖳 « Network and In	ternet → Network Connections v 🖒		
Organize Start this connection	Rename this connection Delete this connection »	Connections	
Ethernet Network 2	L2TP VPN Disconnected	Network 2	Limited 『テ
vmxnet3 Ethernet Adapter	WAN Miniport (L2TP)	L2TP VPN	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
			<u>C</u> onnect

13.ユーザーの資格証明を入力し、「OK」をクリ**ックします**。

Networks
Connecting to 172.16.1.2
Network Authentication
User name
Password
Domain:
OK Cancel

必要なパラメータが両端で一致すると、L2TP/IPsec接続が確立されます。



Split-tunnel 設定

スプリットトンネリングは、暗号化する必要があるサブネットまたはホストのトラフィックを定 義するために使用できる機能です。これには、この機能に関連付けられたアクセスコントロール リスト(ACL)の設定が含まれます。このACLで定義されたサブネットまたはホストのトラフィック は、クライアントエンドからのトンネルを介して暗号化され、これらのサブネットのルートが PCルーティングテーブルにインストールされます。ASAはクライアントからのDHCPINFORMメ ッセージを代行受信し、サブネットマスク、ドメイン名、クラスレススタティックルートで応答 します。

ASAでの設定

ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0

ciscoasa(config)# group-policy DefaultRAGroup attributes ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT ciscoasa(config-group-policy)# intercept-dhcp 255.255.255 enable

L2TP/IPsecクライアントの設定

1. L2TP VPNアダプタを右クリックし、[Properties]を選択します。



2. [Networking]タブに移動し、[Internet Protocol Version 4 (TCP/IPv4)]を選択して[Properties]をク リックし**ます。**

L2TP VPN Properties	×
General Options Security Networking Sharing	
This connection uses the following items: Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 4 (TCP/IPv4) Image: File and Printer Sharing for Microsoft Networks	
Client for Microsoft Networks	
Install Oescription]
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
OK Cance	

3.「詳細」オプション**をクリッ**クします。

Internet Protocol Version 4 (1	CP/IPv4) Properties ? ×
General	
You can get IP settings assigned aut supports this capability. Otherwise, yo administrator for the appropriate IP se	omatically if your network ou need to ask your network attings.
Obtain an IP address automatic	ally
Use the following IP address: -	
IP address:	* * *
O Use the following DNS server a Preferred DNS server:	ddresses:
Alternate DNS server:	
	Advanced
	OK Cancel

4. [Use default gateway on remote network]オプションのチェックを外し、[OK]をクリックします。

	Advanced TCP/IP Settings	?	×
IP Settings	DNS WINS		
This check network ar that canno network.	box only applies when you are connected to a lo d a dial-up network simultaneously. When check be sent on the local network is forwarded to the	ocal ked, data dial-up	
Use o	efault gateway on remote network ble class based route addition		
Auton	atic metric		
Interfact	e metric:		
	ОК	Can	icel

確認

ここでは、設定が正常に機能しているかどうかを確認します。

注:アウトプット インタープリタ ツール(登録ユーザ専用)は、特定の show コマンドを サポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

• show crypto ikev1 sa:ピアにおける現在のIKE SAをすべて表示します。

ciscoasa# show crypto ikev1 sa

IKEv1 SAs:

Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1

1 IKE Peer:

10.1.1.2

Type : user Role : responder Rekey : no

State : MM_ACTIVE

● show crypto ipsec sa :現在ピアにあるすべての IPsec SA を表示します。

ciscoasa# show crypto ipsec sa interface: outside Crypto map tag:

outside_dyn_map

, seq num: 10, local addr: 172.16.1.2

local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

17/1701

)

remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

17/1701

)

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

dynamic allocated peer ip(ipv6): 0.0.0.0

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

```
#TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0
  local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
  path mtu 1500, ipsec overhead 58(36), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: E8AF927A
  current inbound spi : 71F346AB
inbound esp sas:
  spi: 0x71F346AB (1911768747)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport, IKEv1, }
     slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
     sa timing: remaining key lifetime (kB/sec): (237303/3541)
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x0000000 0x0000003
outbound esp sas:
  spi: 0xE8AF927A (3903820410)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport, IKEv1, }
     slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
     sa timing: remaining key lifetime (kB/sec): (237303/3541)
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x0000000 0x0000001
• show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverlpSec - L2TP over IPsec接続の詳細情報を表示します。
```

ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed

```
Username
          : test
```

Index : 1

Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

Protocol	:	IKEv1 IPsec L2T	POverIP	sec		
License	:	Other VPN				
Encryption	:	IKEv1: (1)3DES	IPsec:	(1)3DES	L2TPOverIPsec:	(1)none
Hashing	:	IKEv1: (1)SHA1	IPsec:	(1)SHA1	L2TPOverIPsec:	(1)none
Bytes Tx	:	1574		Bytes Rx	: 12752	
Pkts Tx	:	29		Pkts Rx	: 118	
Pkts Tx Drop	:	0		Pkts Rx I	Drop : 0	

```
Group Policy : L2TP-VPN
```

Tunnel Group : DefaultRAGroup

Duration : 0h:04m:05s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a6a2577000010005557d3a0 Security Grp : none IKEv1 Tunnels: 1 IPsec Tunnels: 1

IKEv1:

L2TPOverIPsec Tunnels: 1

Tunnel ID : 1.1 UDP Src Port : 500 UDP Dst Port : 500 Auth Mode : preSharedKeys Hashing : SHA1 IKE Neg Mode : Main Encryption : 3DES Rekey Int (T): 28800 Seconds Rekey Left(T): 28555 Seconds D/H Group : 2 Filter Name :

IPsec:

Tunnel ID :	1.2		
Local Addr :	172.16.1.2/255.255.255	.255/17/1701	
Remote Addr :	10.1.1.2/255.255.255.2	55/17/1701	
Encryption :	3DES	Hashing :	SHA1
Encapsulation:	Transport		
Rekey Int (T):	3600 Seconds	Rekey Left(T):	3576 Seconds
Rekey Int (D):	250000 K-Bytes	Rekey Left(D):	250000 K-Bytes
Idle Time Out:	30 Minutes	Idle TO Left :	29 Minutes
Bytes Tx :	1574	Bytes Rx :	12752
Pkts Tx :	29	Pkts Rx :	118

L2TPOverIPsec:

Tunnel ID : 1.3

Username : test

Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

ites

ASDMで、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions]の下に、VPNセッションに関する 一般情報が表示されます。L2TP over IPsecセッションは、IPsec (IKEv1) Remote Access > Protocol > L2TP Over IPsecでフィルタリングできます。

File View Tools Wizards Wind	dow	Help										Type topic to search Go	ababa
🔥 Home 🗞 Configuration [Mo	j hone alg Configuration 🔁 Nontorna 🔄 Sere 🗞 Astron 🧟 Bad. 🕐 Formed 🦿 Help												
Device List 🗗 🕂 🗡		Monitoring > VPN > VPN Statistics > Sessions											
🗣 Add 📋 Delete 🚿 Connect													
Find: Go		Type Active			Cumulative			Peak Concurrent			Inactive		
■ 10.105.130.63 ▲ ■ 10.105.130.92 ■ ■ 10.105.130.98 ■ ■ 10.105.130.98 ■ ■ 10.105.130.102 ■ ■ 10.105.130.211 ■		IKEv1 IPsec/L2TF	P IPsec			1				15	1		
■ 10.105.130.214 ■ 10.105.130.225 ▼PN ■ ₽		Filter By: IPsec	(IKE v 1) Remote Access 🔹] [Pro	tocol	▼] [LZTP Over IPsec	• Filter							
VPN Statistics Sessions		Username	Group Policy Connection Profile	Assigned IP Address Public(Peer) IP Address	Protocol Encryption	Login Time Duration		Client(Peer) Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token			Details
VPN Clutter Loads Crypto Statistics Compression Statistics Compression Statistics Global Int// Proc Statistics MAC Seasion Summary VAN Mapping Seasions VAN Mapping Seasions VAN Mapping Seasions VAN Seasions		test	DefaultRAGroup DefaultRAGroup	192, 168, 1, 1 64, 103, 236, 179	(RE+1 IPsec L ZTPC/ver/Psec (RE+1: (1)3DES IPseci (1.)	05:45:13 UTC Sat May 9 20 0h:03m1238	015	Mcrosoft 6.1	1422 24688	Unknown			Ping

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

注:debug コマンドを使用する前に、「<u>デバッグ コマンドの重要な情報」を参照してくだ</u> <u>さい。</u>

注意:ASA では、さまざまなデバッグ レベルを設定できます。デフォルトでは、レベル 1 が使用されます。デバッグ レベルを変更すると、デバッグの冗長性が高くなる場合があり ます。特に実稼働環境では、注意して変更してください。

VPNトンネルに関する問題をトラブルシュ**ートするには、次の**debugコマンドを注意して使用し てください

debug crypto ikev1:IKEに関するデバッグ情報を表示します

• debug crypto ipsec: IPSecに関するデバッグ情報を表示します

正常なL2TP over IPSec接続のデバッグ出力を次に示します。

May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (2) + VENDOR (13) + VENDOR (2) + VENDOR

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group Description: Rcv'd: Unknown Cfg'd: Group 2 May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group Description: Rcv'd: Unknown Cfg'd: Group 2 May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended capabilities payload May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124 May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260 May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1]IP = 10.1.1.2,

Connection landed on tunnel_group DefaultRAGroup

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for Responder... May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304 May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR

```
+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keepalives (type = None) May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds. May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500 May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300 May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

PSec SA Proposal # 2, Transform # 1 acceptable

```
Matches global IPSec SA entry # 10
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
  SCB: 0xE1C00540,
  Direction: inbound
  SPI
         : 0x7AD72E0D
  Session ID: 0x00001000
  VPIF num : 0x0000002
  Tunnel type: ra
  Protocol
            : esp
  Lifetime : 240 seconds
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine:
SPI = 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick
mode
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,
```

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd QM pkt: msg id = 0000001 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160 May 18 04:17:18 [IKEv1]IF = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + NONE (0) total length : 52 May 18 04:17:18 [IKEv1]EF = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + NONE (0) total length : 52 May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key! May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0; encrypt_rule=0000000; tunnelFlow_rule=0000000 May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key! IPSEC: New embryonic SA created @ 0x00007fffelc75c00, SCB: 0xE13ABD20, Direction: outbound SPI : 0x8C14FD70 Session ID: 0x00001000 VPIF num : 0x0000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x8C14FD70 IPSEC: Creating outbound VPN context, SPI 0x8C14FD70 Flags: 0x00000205 SA : 0x00007fffe1c75c00 SPI : 0x8C14FD70 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x0AC609F9 Channel: 0x00007fffed817200 IPSEC: Completed outbound VPN context, SPI 0x8C14FD70 VPN handle: 0x000000000028d4 IPSEC: New outbound encrypt rule, SPI 0x8C14FD70 Src addr: 172.16.1.2 Src mask: 255.255.255.255 Dst addr: 10.1.1.2 Dst mask: 255.255.255.255

Src ports

Upper: 1701

Lower: 1701

Op : equal

Dst ports

Upper: 1701

Lower: 1701

Op : equal

Protocol: 17

```
Use protocol: true
  SPI: 0x0000000
  Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
  Src addr: 172.16.1.2
  Src mask: 255.255.255.255
  Dst addr: 10.1.1.2
  Dst mask: 255.255.255.255
   Src ports
    Upper: 0
    Lower: 0
    Op : ignore
   Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x8C14FD70
  Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User () Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
  Direction: inbound
   SPI
        : 0x7AD72E0D
  Session ID: 0x00001000
  VPIF num : 0x0000002
  Tunnel type: ra
  Protocol : esp
            : 240 seconds
   Lifetime
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x00000206
   SA
      : 0x00007fffe13ab260
  SPI : 0x7AD72E0D
  MTU : 0 bytes
  VCID : 0x0000000
   Peer : 0x000028D4
   SCB : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x0000205
   SA : 0x00007fffe1c75c00
   SPI : 0x8C14FD70
  MTU : 1500 bytes
  VCID : 0x0000000
   Peer : 0x00004174
```

```
SCB : 0x0AC609F9
  Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
  VPN handle: 0x000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 1701
    Lower: 1701
    Op : equal
  Dst ports
    Upper: 1701
    Lower: 1701
    Op : equal
   Protocol: 17
  Use protocol: true
  SPI: 0x0000000
  Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
   Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0x7AD72E0D
  Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
```

Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 2 COMPLETED

(msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1 Windowsクライアントで一般的に発生するVPN関連のエラーの一部を次の表に示します

エラー コード

考えられる解決策

691 入力したユーザ名とパスワードが正しいことを確認します

789,835 クライアントマシンに設定されている事前共有キーがASAと同じであることを確認します non 1. VPNタイプが[Layer 2 Tunneling Protocol (L2TP)]に設定されていることを確認します

- 800 2.事前共有キーが正しく設定されていることを確認します
- 809 UDPポート500、4500(クライアントまたはサーバのいずれかがNATデバイスの背後にある場合

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- ・一般的な L2L およびリモート アクセス IPsec VPN のトラブルシューティング方法について
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>