在RV042ã**€**�RV042Gå′ŒRV082 VPNè∙¯ç"±å™¨ä¸Šé€šé�ŽWindowsé...�ç½®Shre VPN客æ^¶ç«¯

¢>®æ^{™™}

è™›æ"¬å°^ç'"網路(VPN)毯ä,€ç¨®& 端使ç″¨è€...通é&ŽInternetè™›æ"¬é€£ç·šå^°å°^ç″¨ç¶²è·¯ VPN

Clientæ[~]在é� 端ä,»æ©Ÿè£�ç½®ä,Šé...�ç½®çš,,軟é«″,å�¯æ��ä¾›ç°jå–®å′Œå®‰å

本æ–‡æ^a"çš,,ç>®çš,,æ^{~-}å�'æ, ¨å±•礰å¦,何ç,°é€£ç·šå^°RV042ã€�RV042Gæ^–RV082 VPNè^{.-}ç″±å™¨çš,,é>»è...¦é...�ç½®Shrew VPN客æ^¶ç«¯ã€,

æ³'æ,,∲:本æ–‡æ^a"å**∲**‡å®šæ, ¨å·²ç¶"åœ ¨Windowsé›»è...¦ä,Šä,‹è¼‰ä°†Shrew VPN客æ^¶ç«¯ã€,å**∲**¦å‰‡ï¼Œæ, ¨éœ€è¦**∲**é...�置客æ^¶ç«¯å^°ç¶²é—œVPN連線,ç,, <u>VPNè·¯ç″±å™ ¨ä,Šçš,,VPN客æ^¶ç«¯è ¨å®šé**۞** 端è ¨ªå•�éš§é�′ï¼^客æ^¶ç«¯å^°ç¶²é—œï¼‰</u>ã€,

�ç‴¨è£�ç½®

- · RV042
- · RV042G
- · RV082

軟é«"版本

· v4.2.2.08

é....�ç½®Windows上çš"Shrew VPN客æ^¶ç«[–]連ç·š

æ¥é©Ÿ1.按ä,€ä,<é>»è…¦ä,Šçš,**Shrew VPN Client**ç¨<å¼�ä,¦é-<啟å®fã€,*Show Soft VPN Access Manager*視ç^a—é–<啟:



æ¥é©Ÿ2.按ä,€ä,<「**dd**�ã€,凰ç�¾VPN Site Configurationè⊢窗:

aerielai Llier	nt Name R	esolution	Auther	nticatic 1
Remote Ho	st			
Host Name	or IP Addres	s		Port
				500
Auto Config	guration	ike confi	ig pull	~
Local Host Adapter Mo Use a virtu	ode ual adapter ar	nd assigne	:d addre	SS ¥
- Local Host Adapter Mo Use a virtu MTU	ode ual adapter ar	nd assigne	:d addre	ss 🗸
Local Host Adapter Mo Use a virtu MTU 1380	ode ual adapter ar Address	nd assigne Obtair	ed addre n Autom	ss 👻 atically
Local Host Adapter Mo Use a virtu MTU 1380	ode ual adapter ar Address Netmask	nd assigne Dbtair	ed addre	ss 👻 atically

å, jè¦**�é....�ç¹⁄**2®

æ¥é©Ÿ1.按一ä**¸General**é �籤ã€,

Remote Ho	st			
Host Name	e or IP Addres	s	F	Port
				500
Auto Confi	guration	ike confi	g pull	~
мтн		✓ Obtair	Automa	ticallu
MIU 1200	Address		n Automa	stically
	Address			
1300	Motropok			

æ³°æ,,�:*General*éf°å^†ç''''æ–¼é….�ç½®é� 端å′Œæœ¬åœ°ä¸»æ©ŸIP地å�€ã€,這ä°>引

æ¥é©Ÿ2.åœ[¨]Host Name or IP

*Address*æ¬,,ä½�ä,,è¼,å...¥é� 端ä,»æ©ŸIP地å�€ï¼Œå�³å·²é...�ç½®WANçš"IP地å�€ã

æ¥é©Ÿ3.在「Portã€�欄ä½�ä,,è¼,å...¥ç″¨æ−¼é€£ç·šçš"連ç·šåŸ è™Ÿç¢¼ã€,åœ−ä,所@

	ent Name F	fesolution	Authenti	catic
Remote H	lost			
Host Nar	ne or IP Addre:	88	P	ort
213.16.3	33.141			400
Auto Con	figuration	ike confi	g pull	~
Use a vi	rtual adapter a	ind assigne	d address	io allu
1000	6.1.1		Automat	ically
1380	Address		1	
	Netmask			

æ¥é©Ÿ4.在「Auto

*Configuration*ã**€**¢ä¸<æ<‰å¼�æ,...å−®ä¸é�,æ"‡æ‰€éœ€çš"組æ...<ã€,

·ç¦�ç″¨â€″ç¦�ç″¨é�,é ...ç¦�ç″¨ä»»ä½•自動客æ^¶ç«¯é...�ç½®ã€,

IKE Config Pull â€"

å...�許客æ^¶ç«¯å¾žé›»è...¦è¨å®šè«‹æ±,ã€,在é›»è...¦æ″¯æ�´Pull方法çš"æf...æ³�下ï

IKE Config Push â€"

伿;é>»è…¦æœ‰æ©Ÿæœf通é�Žé…�ç½®é�Žç¨‹å�'客æ^¶ç«¯æ��ä¾›è¨å®šã€,在é>»è…¦

· DHCP Over IPSec — 使客æ^¶ç«⁻有機æœf通**∲**ŽDHCP over IPSec從é›»è...¦è«‹æ±,è¨å®šã€,

Client	Name R	esolution	Authe	nticatic
te Host				
Name or	IP Addres	s		Port
16.33.14	1			400
Configura	ation	ike confi	ig pull	~
Host —		disabled ike confi	g pull	
ter Mode		tke conti dhop ovi	g push er ipsec	;
a virtual	adapter ar	nd assigne	ed addre	ess 🗸
		🗸 Obtair	n Auton	natically
30	Address			
	Netmask			
	Client te Host Name or 16.33.14 Configura Host ter Mode a virtual	Client Name R te Host Name or IP Addres 16.33.141 Configuration Host ter Mode a virtual adapter ar 30 Address	Client Name Resolution te Host Name or IP Address 16.33.141 Configuration like confi disabled like confi dhop over a virtual adapter and assigne Obtair 30 Address	Client Name Resolution Auther te Host Name or IP Address 16.33.141 Configuration ike config pull disabled ike config pull ike config pu

æ¥é©Ÿ5.從Adapter Modeä, <æ<‰é�,å−®ä,,æ ¹æ"šAuto Configurationç,ºæœ¬åœ°ä,»æ©Ÿé�,æ"‡æ‰€éœ€çš,,介é�¢å�jæ¨jå¼�ã€,

·ä¼₂¿ç"¨è™›æ"¬ä»‹é�¢å�jå′Œå^†é...�çš"地å�€ â€″ å...�許客æ^¶ç«¯ä½¿ç″¨å...·æœ‰æŒ‡å®šåœ°å�€çš"è™›æ"¬ä»‹é�¢å�jã€,

·ä½¿ç"¨è™›æ"¬ä»‹é�¢å�jå′Œéš¨æ©Ÿåœ°å�€ â€″ å...�許客æ^¶ç«¯ä½¿ç″¨å...∙有隨機地å�€çš"è™›æ"¬ä»‹é�¢å�jã€,

·ä½¿ç"¨ç�¾æœ‰ä»‹é�¢å�jå′Œç•¶å‰�地å�€ â€″ 使ç″¨ç�¾æœ‰ä»‹é�¢å�jå�Šå...¶åœ°å�€ã€,ä¸�需è¦�輸å...¥å...¶ä»–資訊ã€,

General	Client	Name R	esolution	Auther	nticatic	•
Remo	te Host					
Host	Name or	IP Addres	s		Port	
213.1	16.33.14	1			400	
Auto	Configur	ation	disabled		~	
Use	a virtual	adapter ar	nd assigne	d addre	ss 💙	
Use	a virtual a virtual	; adapter ar adapter ar	nd assigne nd assigne	d addre d addre	ss 🗸)
Use Use	a virtual an existir	adapter ar ng adapter engress	nd random and curre	address int addre	S SSS	J
		Netmask		•		

æ¥é©Ÿ6.å¦,果從æ¥é©Ÿ5çš,,Adapter Modeä,<æ<‰å¼�æ,...å-®ä,é�,æ"‡ä°†Use a Virtual Adapter and Assigned

Address,è«<在*MTU*æ¬,,ä½�ä,è¼,å...¥æœ€å¤§å,³è¼,å–®ä½�(MTU)ã€,最大å,³è¼,å–®å...fa 1380ã€,

æ¥é©Ÿ7.ï¼^å�¯é�,)è¦�通é�ŽDHCP伺æœ�器自å‹•ç�²å�–地å�€å′Œå�網掩ç Automaticallyè¦^å�–方塊ã€,æ¤é�,é ...ä,¦é�žå°�所有é...�ç½®éf½å�¯ç″¨ã€,

$$\label{eq:stable} \begin{split} & \& \ensuremath{\mathbb{R}} \ens$$

Addressï¼/Œè«‹åœ¨*Address*æ¬,,ä½�ä,è¼,å...¥é� 端客æ^¶ç«¯çš,,IP地å�€ã€,

æ¥é©Ÿ9.å¦,果從æ¥é©Ÿ5çš,,Adapter Mode ä, <æ<‰é�,å-®ä,é�,æ"‡Use a Virtual Adapter and Assigned Address ï¼Æè«<在Netmask

æ¬,,ä½�ä,è¼,å...¥é� 端客æ^¶ç«¯IP地å�€çš,,å�網掩碼ã€,

Remote Ho Host Name 213.16.33 Auto Confir	st e or IP Addres .141	s	F		
Host Name 213.16.33 Auto Confi	or IP Addres	s	F		
213.16.33 Auto Confi	141			Port	
Auto Confi	0.000			400	
1 1000 00111	guration	ike confi	g pull	~	
Use a virti	ual adapter ar	nd assigne	d addres	is 🗸	
мти		🖌 Obtair	n Automa	atically	1
1480	Address		12		
	Netmask		1		J

æ¥é©Ÿ10.按一ä¸<ã€**Œave**ã**€�**以å"²å~è¨å®šã€,

客æ^¶ç«⁻é...�ç½®

æ¥é©Ÿ1.按ä,€ä,**Client**é �籤ã€,

Firewall Options		
NAT Traversal	enable	~
NAT Traversal Port		4500
Keep-alive packet rate	15	i Secs
IKE Fragmentation	enable	~
Maximum packet size	540	Bytes
Other Options		
🗹 Enable Dead Peer Dete	ection	
🗹 Enable ISAKMP Failure	Notifications	
🗹 Enable Client Login Bar	nner	

æ³"æ,,�:在客*戶ç*«⁻éf¨å^†ï¼Œå�¯ä»¥é...�ç½®é^{~2}ç�«ç‰†é�,é ...ã€�失æ•^å°�ç‰é«″æ

æ¥é©Ÿ2.從NAT Traversalä, <æ<‰é�,å–®ä,é�,æ"‡é�©ç•¶çš"NATï¼^網路地å�€è½‰æ�>)é��æ·é�,é .. ·ç¦�ç″[¨] â€″ NATå�″定å·²ç¦�ç″[¨]ã€,

ጥٍ‴ —

åf…當網關通é�Žå�"商指礰æ"[–]æ�´æ™,æ‰�使ç"¨IKEå^†æ®µã€,

·å¼·å^¶è�‰ç¨¿â€″

NAT�定çš"è�‰ç¨¿ç‰^本ã€,å¦,果網關通é�Žå�"商æ^–檢æ,¬NAT來指

·å¼·å^¶RFC -

NAT�定çš,,RFCç‰^本ã€,å¦,果網關通é�Žå�"商æ^–檢æ,¬NAT來指礰æ"



æ¥é©Ÿ3.在NAT Traversal Portæ¬,,ä½�ä,è¼,å...¥NATçš,,UDPåŸ ã€,é �è¨å€¼ç,° 4500ã€,

æ¥é©Ÿ4.在「K*eep-alive packet rate*�欄ä½�ä,,è¼,å...¥å,³é€�ä¿�æŒ�連ç·šå°�åŒ...çš"速率值ã€,該值以ç§′ç



æ¥é©Ÿ5.在*IKE Fragmentationä*, <æ<‰æ,...å–®ä,,é�,æ"‡é�©ç•¶çš"é�,é ...ã€,

```
·ç¦�ç″¨ â€″ ä,�ä½;ç″¨IKEå^†æ®µã€,
```

ጥٍ"" —

åf…當網關通é�Žå�"商指礰æ"¯æ�´æ™,æ‰�使ç"¨IKEå^†æ®µã€,

 $\cdot \mathring{a}^{1}_{4} \cdot \mathring{a}^{\P} \hat{a} \in "c, j \in \mathbb{Z}^{p^{0}} \times \mathbb{Z}^{p^$



æ¥é©Ÿ6.åœ⁻⁻Maximum packet

*size*æ¬,,ä½�ä,ï¼^以ä½�å...fçµ,,ç,ºå–®ä½�)è¼,å...¥æœ€å¤§è³‡æ–™åŒ...大å°�ã€,å¦,æžœ

æ¥é©Ÿ7.ï¼^å�¯é�j)è‹¥è¦�å...�許é›»è...¦å'Œå®¢æ^¶ç«¯åœ¨å�¦ä,€å€‹ç"j法響應æ¹ Dead Peer Detectionè¦^å�–æ–¹åjŠã€,

æ¥é©Ÿ8.ï¼^å�¯é�j)è¦�通é�ŽVPN客æ^¶ç«¯å,³é€�æ•...障通知,è«‹é�jä,Enable ISAKMP Failure Notificationsè¦^å�–æ–¹åjŠã€,

æ¥é©Ÿ9.ï¼^å�¯é�,)è¦�在è^‡ç¶²é—œå»°ç«‹é€£ç·šæ™,ç″±å®¢æ^¶ç«¯é;¯ç¤°ç™»å...¥æ©«å Client Login èl^å�–æ–¹å;Šã€,

General Clier	nt Name Res	olution	Authentic	atic 🖣
Firewall Opt	ions			
NAT Trave	rsal	ford	ce-draft	~
NAT Trave	rsal Port			4400
Keep-alive	packet rate		17 Se	cs
IKE Fragme	entation	ford	e	~
Maximum p	acket size		520 By	tes
Other Option	ns			
🗹 Enable	Dead Peer Del	ection		
🗹 Enable	ISAKMP Failur	e Notific	ations	- 1
🗹 Enable	Client Login Ba	nner		J
· · · ·				_

æ¥é©Ÿ10.按一ä¸<ã€**Œave**ã**€�**以å"²å~è¨å®šã€,

�ç[¨]±è§£æž�é...�ç½®

æ¥é©Ÿ1.按ä,€ä, **Name Resolution**é �籤ã€,

✓ Enable DNS	🗹 Obtain Automatically
Server Address #1	
Server Address #2	
Server Address #3	
Server Address #4	
DNS Suffix	 Obtain Automatically

æ³"æ,,**\$**: Name

Resolutionéf¨å^†ç''''æ–¼é....�ç½®DNSï¼^域å��系統ï¼‱å'ŒWINï¼^Windows Internet�稱æœ�務)è¨å®šã€,

æ¥é©Ÿ2.按ä₅€ä₅<DN**&�,**é …å**�**jã€,

🖌 Enable DNS	🗹 Obtain /	Auton	natically
Server Address #1		•	
Server Address #2		-2	
Server Address #3		-22	
Server Address #4			
DNS Suffix	✔ Obtain A	Autom	natically

æ¥é©Ÿ3.é�,ä,Enable DNS以啟ç""域å��系統(DNS)ã€,

æ¥é©Ÿ4.ï¼^å�[¯]é�,)è‹¥è¦�至å‹•å�–å¾—DNS伺æœ�器ä½�å�€ï¼Œè«‹å‹¾é�,Obtain Automaticallyè¦^å�–æ–¹åjŠã€,å¦,æžœé�,æ"‡æ¤é�,é ...,請跳至æ¥é©Ÿ6ã€,

æ¥é©Ÿ5.在Server Address

#1æ¬,,ä½�ä,è¼,å...¥DNSä¼°æœ�器地å�€ã€,å¦,果有å...¶ä»–DNSä¼°æœ�器,è

Enable DNS	🗌 Obtair	n Auto	matically	
Server Address #1	213.1	6.3	3.145	
Server Address #2		8		
Server Address #3		12		
Server Address #4		181		
DNS Suffix	✓ Obtair	n Auto	matically	

æ¥é©Ÿ6.ï¼^å�[¯]é�,)è¦�自å‹•ç�²å�-DNS伺æœ�器çš,,å—尾,è«‹é�,ä,Obtain Automaticallyè¦^å�-æ-¹å¡Šã€,å¦,æžœé�,æ"‡æ¤é�,é ...,請跳至æ¥é©Ÿ8ã€,

æ¥é©Ÿ7.在「DNSå—å°¾ã��欄ä½�ä,è¼,å...¥DNSæœ�å‹™å™∵çš,,å—å°¾ã€,

æ¥é©Ÿ8.按ä,€ä,<ã€**Œave**ã**€∲**以å"²å~è¨å®šã€,

æ¥é©Ÿ9.按ä,€ä,**WINS**é **�**籤ã€,

eneral Client Name	Resolution	Auth	enticatic 4
✓ Enable WINS	🖌 Obtain	Autor	natically
Server Address #1			2
Server Address #2			

æ¥é©Ÿ10.é�,ä,Enable WINS以啟ç‴Windows Internet Name Server(WINS)ã€,

æ¥é©Ÿ11ã€,ï¼^å�¯é�,)è¦�自å‹•ç�²å�–DNS伺æœ�器地å�€ï¼Œè«‹é�,ä,Obtain Automaticallyè¦^å�–æ–¹åjŠã€,å¦,æžœé�,æ"‡æ¤é�,é ...,請跳至æ¥é©Ÿ13ã€,

æ¥é©Ÿ12.在Server Address

#1æ¬,,ä½�ä,è¼,å...¥WINSä¼°æœ�å[™]çš,,地å�€ã€,å¦,果有å...¶ä»–DNSä¼°æœ�å[™]ï *Address*æ¬,,ä½�ä,è¼,å...¥é€[™]ä°>æœ�å<[™]ä[™]çš,,地å�€ã€,

æ¥é©Ÿ13.按ä,€ä,<ã€**Gave**ã**€�**以å,,²å~è¨å®šã€,

é©—è‰

æ¥é©Ÿ1.按ä,€ä,**Authentication**é �籤ã€,

Authe	ntication N	/lethod	Hybrid R	SA + XAul	th 🗸
Loca	al Identity	Remot	e Identity	Credenti	als
Ide	ntification	Туре			
Fu	ully Qualifie	ed Doma	iin Name		~
FQ	DN String				

註:在Authenticationéf¨å^†ï¼Œæ,¨å�¯ä»¥é...�置客æ^¶ç«¯çš,,引æ•,,使å...¶åœ¨å SAæ™,處ç�†è°«ä»½é©—è‰ã€,

æ¥é©Ÿ2.從Authentication

*Method*ä, <æ<‰é�,å–®ä,é�,æ"‡é�©ç•¶çš,,谫份é©—è‰æ–¹æ³•ã€,

·æ··å�^RSA +æ"′展é©—è‰ â€" �需è¦�客æ^¶ç«¯æ†'æ"šã€,使ç"¨è€...端æœfé©—è‰é–~é�"ã€,憑æ"šå°‡æŽ¡ç"¨PEN

·æ··å�^GRP +æ"′展é©—è‰ â€" ä,�需è¦�客æ^¶ç«¯æ†'æ"šã€,ä½;ç″¨è€...端æœfé©—è‰é–~é�"ã€,æ†'è‰å°‡æŽ¡ç″¨PEN

·é>™æ–¹RSA +æ"´å±•é©—è‰ â€" 客æ^¶ç«¯å'Œç¶²é—œéƒ½éœ€è**∲**憑è‰é€²è;Œè°«ä»½é©—è‰ã€,憑è‰å°‡æŽ;ç″¨PEMæ^–PKC

·é>™æ–¹PSK +æ‴展é©—è‰ â€"

客æ^¶ç«¯å'Œç¶²é—œéf½éœ€è**∲**憑è‰é€²èjŒè°«ä»½é©—è‰ã€,憑æ"šå°‡æŽjç″¨å...±ç″¨é‡'é'°

·é>™æ–¹RSA —

客æ^¶ç«¯å'Œç¶²é—œéƒ½éœ€è**∲**憑è‰é€²èjŒè°«ä»½é©—è‰ã€,憑è‰å°‡æŽjç″¨PEMæ^–PKC

·é>™å�'PSK â€"

客æ^¶ç«¯å′Œç¶²é—œéf½éœ€è¦�憑è‰é€²è;Œè°«ä»½é©—è‰ã€,憑æ"šå°‡æŽ;ç"¨å...±ç"¨

Client	Name R	esolution	Authentication	Phase 1
Authe	ntication M	1ethod	Hybrid RSA + XA	uth 🗸
Loc	al Identity	Remo	Hybrid RSA + XA Hybrid GRP + XA	uth iuth
Ide	ntification	Туре	Mutual RSA + XA Mutual PSK + XA	uth uth
Fu	Illy Qualifie	ed Doma <mark>i</mark>	Mutual RSA	

 $acc \neg acc \circ e^{\circ} \ll a \gg \frac{1}{2} e \dots$

æ¥é©Ÿ1.按ä,€ä,**Łocal Identity**é �籤ã€,

Authe	ntication N	1ethod	Hybrid R	SA + XAu	uth '
Loca	al Identity	Remote	e Identity	Credent	ials
Ide	ntification	Туре			
Fu	Ily Qualifie	ed Domai	in Name		~
FQ	DN String				

æ³¨æ,,�:本地谫份è¨å®šå,³é**€�**å^°ç¶²é—œé€²è¡Œé©—è‰çš"IDã€,在*Local Identityéf*¨å^†ä¸ï¼Œé…�置標è~åž‹å^¥å′ŒFQDNï¼^完å…¨é™�定域å��)å—串以

æ¥é©Ÿ2.從Identification

*Type*ä,<æ<‰é�,å−®ä,é�,æ"‡ç>,應çš,æ[…]™è[~]é�,é …ã€,ä,¦é�žæ‰€æœ‰é�,é …å°�所æœ

ጨΌ…¨é™�定域å�� â€″ 本地標è~çš,,客æ^¶ç«¯æ¨™è~基於完å...¨é™�定域å��ã€,å¦,æžœé�,æ"‡æ!

·ä¼₂¿ç''''者完å…''é™�宊åŶŶå�� â€″

本地身份çš"客æ^¶ç«¯æ™è~基æ–¼ä½ç″¨è€…完å…¨é™�定域å��ã€,å¦,æžɑ

· IP地å�€ â€"

本地身份çš"客æ^¶ç«¯æ¨™è~基æ–¼IP地å�€ã€,å¦,æžœé�'ä'Use a discovered local host

·é‡'é'°è~å^¥ç¬¦è™Ϋ — 埰於金é'°è~å^¥ç¬¦è™Ÿæ[…]™è~本地客æ^¶ç«~çš,,客æ^¶ç«~è~å^¥ç¬¦è™Ÿã€,å|,æžœé�,æ"‡æ¤é�

address,將自å<•發ç�¾IP地å�€ã€,å¦,æžœé�,æ"‡æ¤é�,é ...,è«<執è;Œæ¥é©Ÿ5ï¼0

Authentication Method Hybrid RSA + XAuth Local Identity Remote Identity Credentials Identification Type Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Authentication Method Hybrid RSA + XAuth Local Identity Remote Identity Credentials Identification Type Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Authentication Method Hybrid RSA + XAuth Local Identity Remote Identity Credentials Identification Type Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Client	Name Resolution Authentication Phase
Local Identity Remote Identity Credentials Identification Type Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Local Identity Remote Identity Credentials Identification Type Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Local Identity Remote Identity Credentials	Authe	ntication Method Hybrid RSA + XAuth
Identification Type Fully Qualified Domain Name Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Identification Type Fully Qualified Domain Name Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Identification Type Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Loc	al Identity Remote Identity Credentials
Fully Qualified Domain Name Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Fully Qualified Domain Name Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Fully Qualified Domain Name Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Jer	entification Type
Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	Fully Qualified Domain Name User Fully Qualified Domain Name IP Address Key Identifier	F	ully Qualified Domain Name 🛛 🗸 🗸 🗸 🗸 🗸 🗸
IP Address Key Identifier	IP Address Key Identifier	IP Address Key Identifier	F	ally Qualified Domain Name
I Key Identiliei			IF K	Address u Identifier
				y identiliei
		Save Cance		

æ¥é©Ÿ3.åœ[•]FQDN

Stringæ¬,,ä½�ä,è¼,å...¥å®Œå...¨é™�定çš,,域å��作ç,°*DNSå*—ä,²ã€,

æ¥é©Ÿ4.åœ^{..}UFODN *String*ï¼^UFQDNå—ä,²ï¼‰æ¬,,ä½�ä,è¼,å...¥ä½¿ç″¨è€...完å...¨é™�定çš,,*域å*��(DNSå—ä,²)

æ¥é©Ÿ5.在UFQDNå—ä,²æ¬,,ä½�ä,è¼,å...¥IP地å�€ã€,

æ¥é©Ÿ6.在Key ID $String \ddot{i}/4 \acute{e}^{\dagger} \acute{e}^{\circ} ID \mathring{a} - \ddot{a}_{2} \ddot{i}/4 \\ \&\ddot{a}_{2} \dot{i}/4 \\ \&\ddot{a}_{2} \dot{a}_{3} \dot{a}_{2} \dot{a}_{3} \dot{$

æ¥é©Ÿ7.按ä,€ä,<ã€**Œave**ã€**¢**以å,,²å~è¨å®šã€,

é� ç≪¯è°«ä»½é...�ç½®

æ¥é©Ÿ1.按ä,€ä, **Remote Identity**é �¢¢±¤ã€,

address,將自動發ç�¾IP地å�€ã€,å¦,æžœé�,擇æ¤é�,é …ï¼Œè«‹åŸ·è¡Œæ¥é©Ÿ6ï¼
金鑰è~崥符號 —
埰於金鑰è~å^¥ç¬l號來標è~́é� 端客æ^¶ç«¯çš"客æ^¶ç«¯è~å^¥ç¬¦è™Ÿã€,å¦,æžœé∢

· IP地å�€ â€"
é� 端谫份çš,,客æ^¶ç«¯æ¨™è~埰æ-¼IP地å�€ã€,å¦,æžœé�,ä,Use a discovered
local host
address,將自å、•發ç�¾IP地å�€ã€,å¦,æžœé�,æ"‡æ¤é�,é ...,è«、執è;Œæ¥é©Ÿ6ï¼Q

·ä½;ç'"`者完å…¨ć™�定域å�� â€″ é� 端谫份çš"客æ^¶ç«¯æ¨™è~埰æ–¼ä½;ç″¨è€…完å…¨é™�定域å��ã€,å�ªæœ9

ጨΌ…¨é™�定域å�� â€″ é� 端標è~çš"客æ^¶ç«¯æ¨™è~埰於完å…¨é™�定域å��ã€,å�ªæœ‰åœ¨*Authe*

從PEMæ[^]-PKCS12è‰æ›,æ^a"æj[^]è‡^aå‹•æ[™]è[~]é�ç[®] 客æ[^]¶ç[®]ã€,å�^a有åœ[™]Authentication the subject in the received certificate but don't compare it with a specific valueè¦[^]å�-æ-¹åjŠä»¥è‡^a動接æ"¶è‰æ›,ã€,å¦,æžœớ,æ"‡æ¤é�,é ...,請執èjŒæ¥é©Ÿ3,ç

· ASN.1å�¯å^†è¾¨å��稱â€″

· Any é� 端客æ^¶ç«¯å�¯ä»¥æŽ¥å�—任何值æ^–ID進è;Œè°«ä»½é©—è‰ã€,

æ¥é©Ÿ2.å¾*žIdentification Type*ä, <æ<‰é�,å–®ä,é�,æ"‡ç>,應çš,,æ[…]™è~é�,é …ã€,

æ³¨æ,,�:é**�** 端谫份從網關é©—è‰IDã€,在*Remote Identity*éf¨å^†ä,,將標è~åž<å´¥é…**�**ç½®ç,°ç¢°å®šIDçš,,é©—è‰æ–¹å¼**�**ã€,

Client	Name Resolution	Authentication	Phase 1
Authe	ntication Method	Hybrid RSA + XA	uth 🗸
Loca	al Identity Remote	Identity) Creden	tials
Ide	entification Type		
Ar	1y		~

Authe	ntication Method Hybrid RSA + XAuth 🗸 🗸
Loca	Ildentity Remote Identity Credentials
Ide	ntification Type
Ar	
Ar	
AS Fu	N.1 Distinguished Name Ily Qualified Domain Name
Us	er Fully Qualified Domain Name
Κe	y Identifier

æ¥é©Ÿ3.在ASN.1 DNå—ä,²æ¬,,ä½�ä,è¼,å...¥ASN.1 DNå—ä,²ã€,

æ¥é©Ÿ4.在*FQDN* Stringæ¬,,ä½**\$**;ä,è¼,å...¥å®Œå...¨é™**\$**定çš,,域å**\$\$**;ä%Ç\$,*°DNSå*—ä,²ã€,

æ¥é©Ÿ5.在*UFQDNå—ä*,²æ¬,,ä½�ä,è¼,å...¥ä½;ç″¨è€...完å...¨é™�定çš,,域å��ï¼^DNSå—ä

æ¥é©Ÿ6.在UFQDN Stringæ¬,,ä½�ä,è¼,å...¥IPåæ°å�€ã€,

æ¥é©Ÿ7.åœ*¨Key ID String*æ¬,,ä½**@**ä,è¼,å...¥ç″¨æ−¼æ¨™è~本地客æ^¶ç«¯çš,,金é'°è~å^¥ç¬¦è™Ÿã€,

æ¥é©Ÿ8.按ä,€ä,<ã€**Œave**ã**€∲**以å,,²å~è¨å®šã€,

憑è‰é...�ç½®

æ¥é©Ÿ1.按ä,€ä,**Credentials**é �籤ã€,

Client	Name Re	esolution	Authentication	Phase 1
Authe	ntication M	lethod	Hybrid RSA + XA	uth 🗸
Loc	al Identity	Remote	Identity Creden	tials
Se	rver Certific	ate Auto	rity File	
Cli	ent Certifica	ate File		
L	0* <u>2</u> *0 148	Key File		
Cli	ent Private			
	ent Private	-		
Cli	ent Private e Shared K	ey		
Cli Pre	ent Private e Shared K	ey		
Cliv Pre	ent Private e Shared K	ey		

æ³¨æ,,�:在*Credentials*éf¨å^†ï¼Œé...**�**ç½®é **�**å...±ç″[¨] 金é'°ã€,

Client	Name R	esolution	Auther	ntication	Phase	4
Authe	ntication M	lethod	Mutual P	SK		~
Loc	al Identity	Remote	Identity	Creden	tials	
Se	rver Certific	cate Auto	rity File			
Clie	ent Certific	ate File				
B\	/042G_07(03_1105_	.pem			
Clie	ent Private	Key File			_	
Pre	e Shared K	.ey				
		••				
				1993		
			Sav	'e	Can	cel

æ¥é©Ÿ2.è¦�é�,æ"‡ä¼°æœ�器è‰æ›,æ^a"æ;`,請按ä,€ä,‹... 圖礰æ—�é,Šçš"*Server Certificate Authority*

*File*æ¬,,ä½�,ä,¦é�,æ"‡æ, [°]åœ[°] PCä,Šå,,²å[°]ä¼[°]æœ�å[™][°]è‰æ₂,æ^a"æ;[°]çš,,è^{·¯}徑ã€,

æ¥é©Ÿ3.è¦�é�¸æ"‡å®¢æ^¶ç«¯è‰æ>¸æª"æ;ˆï¼Œè«‹æŒ‰ä¸€ä¸‹... 圖ç¤⁰æ—�é,Šçš,,*Client Certificate*

*File*æ¬,,ä½�,ä,¦é�,æ"‡æ,¨åœ¨PCä,Šå,,²å˜å®¢æ^¶ç«¯è‰æ>,æ³″æ;ˆçš,,è·¯å¾′ã€,

æ¥é©Ÿ4. èl�é�,æ"‡å®¢æ^¶ç«¯ç§�é'°æª″æj^,è«‹å–®æ''Šâ€¦â€åœ–礰,ä, lé�,æ"‡æ, ¨åœ¨P

æ¥é©Ÿ5.在*PreShared Key*æ¬,,ä½�ä,è¼,å...¥é �å...±ç"¨é‡'é'°ã€,æ¤é‡'é'°æ‡‰è^‡é...�置隧é�"æ™,使ç"¨çš"金é'°ç› æ¥é©Ÿ6.按ä,€ä,<ã€**Gave**�以å,,²å~è¨å®šã€,

第1階段...�ç½®

æ¥é©Ÿ1.按ä,€ä,**Phase 1**é �籤ã€,

Proposal Parameters	8	
Exchange Type	aggressive	~
DH Exchange	group 2	×
Cipher Algorithm	auto	~
Cipher Key Length		Bits
Hash Algorithm	auto	~
Key Life Time limit	8640	O Secs
Kaul Xa Data Sait		0 Kbytes

æ³"æ,,**\$:**圓Phase

léf¨å^†ï¼Œæ,¨å�¯ä»¥é...�置引æ•,,以便å�¯ä»¥å»°ç«‹å,¶æœ‰å®¢æ^¶ç«¯ç¶²é—œçš SAã€,

æ¥é©Ÿ2.從*Exchange Type*ä, <æ<‰é�,å−®ä,é�,æ"‡é�©ç•¶çš,,金é'°ä°¤æ�>åž<å^¥ã€,

·ä¸»èl� â€″ å°�ç‰é«″çš"谫份å�—å^°ä¿�è·ã€,

·æ"»æ"Šæ€§ — å�ç‰é«″çš"谫份æ²′有ä¿�éšœã€,

Proposal Paramet	ers 🦰		
Exchange Type	aggre	essive	~
DH Exchange	main	essive	
Cipher Algorithm	auto		~
Cipher Key Lengt	h	~	Bits
Hash Algorithm	auto		~
Key Life Time limi	it	86400	Secs
Key Life Data limi	it	0	Kbytes
			_

æ¥é©Ÿ3.在DH

*Exchange*ä,<æ<‰é�,å−®ä,,é�,æ"‡åœ¨VPN連ç·šçš,,é...�置期é−"é�,æ"‡çš,,é�©ç•¶çµ,,å

æ¥é©Ÿ4.在「Cipher

*Algorithm*ã**€**¢ä,<æ<‰é�,å–®ä,,é�,æ"‡åœ¨VPN連ç·šé...�置期é–"é�,æ"‡çš"é�©ç•¶é

æ¥é©Ÿ5.在「Cipher Key

Length�ä,<æ<‰é�,å–®ä,,é�,æ"‡è^‡é...�ç½®VPN連ç·šæ™,é�,æ"‡çš"é�,é ...çš"金é'°é•·

æ¥é©Ÿ6.在「Hash

Algorithm�ä,<æ<‰é�,å–®ä,,é�,æ"‡åœ¨é...�ç½®VPN連線期é–"é�,æ"‡çš"é�,é ...ã€

æ¥é©Ÿ7.在Key Life Time

limitæ¬,,ä½�ä,,è¼,å...¥åœ¨é...�ç½®VPN連ç·šæ™,使ç″¨çš,,值ã€,

æ¥é©Ÿ8.在「é—œé�µå£½å'½è³‡æ–™é™�å^¶ã€�欄ä½�ä,,è¼,å...¥è¦�ä¿�è·çš"值ï¼′

æ¥é©Ÿ9.ï¼^å�¯é�j)é�jä,Enable Check Point Compatible Vendor IDèl^å�-æ-¹åjŠã€,

Exchange Type	aggressive	Y
DH Exchange	group 1	~
Cipher Algorithm	des	Y
Cipher Key Length	v	Bits
Hash Algorithm	md5	¥
Key Life Time limit	85400	Secs
Key Life Data limit	10	Kbyte:

æ¥é©Ÿ10.按一ä¸<ã€**Œave**ã**€�**以å"²å~è¨å®šã€,

第2階段...�ç½®

æ¥é©Ÿ1.按一ä**,Phase 2**é �籤ã€,

and Marine and States and		
Transform Algorithm	auto	~
Transform Key Length	~	Bits
HMAC Algorithm	auto	~
PFS Exchange	disabled	~
Compress Algorithm	disabled	~
Key Life Time limit	3600	Secs
Key Life Data limit	0	Kbytes

æ^{3••}æ,,**\$**:åœ^{••}Phase

2éf¨å^†ï¼Œå�¯ä»¥é...�置引æ•,,以便å�¯ä»¥å»°ç«‹å...·æœ‰é� 端客æ^¶ç«¯ç¶²é— SAã€, æ¥é©Ÿ2.在*Transform Algorithm*ä, ‹æ<‰é�,å–®ä,,é�,æ"‡åœ¨é...�ç½®VPN連線期é–"é�,æ"‡çš"é�,é ...ã€,

```
æ¥é©Ÿ3.åœ¨Transform Key
Lengthä<sub>s</sub><æ<‰é�<sub>s</sub>å−®ä<sub>s</sub>,é�<sub>s</sub>æ"‡è^‡é...�ç½®VPN連線期é–"所é�<sub>s</sub>æ"‡çš"é�<sub>s</sub>é ...çš"金é
```

```
æ¥é©Ÿ4.在「HMAC
Algorithm�ä,<æ<‰é�,å-®ä,,é�,æ"‡åœ¨é...�ç½®VPN連線期é–"é�,æ"‡çš"é�,é ...ã€
```

```
æ¥é©Ÿ5.在PFS
Exchangeä,<æ<‰é�,å–®ä,,é�,æ"‡åœ¨é...�ç½®VPN連線期é–"é�,æ"‡çš"é�,é ...ã€,
```

æ¥é©Ÿ6.在Key Life Time

*Limit*æ¬,,ä½�ä,,è¼,å...¥åœ¨é...�ç½®VPN連線期é–"使ç″¨çš"值ã€,

æ¥é©Ÿ7.在「Key Life Data

limit�欄ä½�ä,,è¼,å...¥è¦�ä¿�è·çš,,值ï¼^以å�fä½�å...fçµ,,ç,°å–®ä½�)ã€,é �è

- Proposal Par	ameters		1 Olicy	
Transform A	lgorithm	esp-3de	s	~
Transform K	ey Length		~	Bits
HMAC Algor	ithm	md5		~
PFS Exchar	ige	group 1		~
Compress Al	gorithm	deflate		~
Key Life Tim	e limit		3500	Secs
Key Life Dat	a limit		10	Kbytes

æ¥é©Ÿ8.按ä,€ä,<ã€**Œave**ã**€∲**以å,,²å~è¨å®šã€,

ç–ç•¥é...�ç½®

æ¥é©Ÿ1.按一ä**¸Policy**é �籤ã€,

	Phase 1	Phase 2 P	olicy
- IPSEC Policy	y Configuratio	on	
Policy Gene	ration Level	auto	
🗌 Maintain	Persistent S	ecurity Asso	ciations
🖌 Obtain T	opology Aut	omatically or	Tunnel All
Remo	te Network F	Resource	
5			
1. T. T.	M	odify	Delete
Add			

æ³[•]æ,,**۞:**åœ^{··}*Policy*éf[•]å^†ä¸å®šç¾©ä⁰†IPSECç–略,這æ⁻⁻客æ^¶ç«¯è^‡ä¸»æ©Ÿé€²è;Œç«™é»ž

æ¥é©Ÿ2.在Policy Generation Levelä, <æ<‰é�,å–®ä,,é�,æ"‡é�©ç•¶çš,,é�,é …ã€,

·è‡ªå<• — 自å<•碰定å¿…è¢çš"IPsecç-略級å^¥ã€,</p>

·èl�æ±, — ä,�æœfå�"商æ¯�個ç–略的å″¯ä,€å®‰å...¨é—œè�¯ã€,

·å"⁻ä,€ — ��"商æ¯�個ç-略的å″¯ä,€å®‰å...¨é—œè�¯ã€,

·å...±ç'''' ‒' 園'å¿...è¢ç´šå^¥ç″Ÿæ^�é�©ç•¶çš"ç–ç•¥ã€,

guration	
evel a	
	uto 🗸
ent Securit <mark>y</mark> ^{au} re	ito quire
y Automatica ur sh	nique bared
vork Resource	
Modify	Delete
	ent Security re y Automatic ur vork Resource

æ¥ć©Ÿ3.ï¼^å�¯ć�,)è¦�æ›´æ″¹IPSecå�″商,è«‹é�,ä,Maintain Persistent Security Associationsè¦^å�–æ–¹åjŠã€,å¦,果啟ç″¨ï¼Œå‰‡æœf在連線後直接ç,ºæ¯�個ç–ç•¥é

æ¥é©Ÿ4.ï¼^å�¯é�,)è¦�從è£�置接æ"¶è‡ªå‹•æ��供的網路æ,...單,æ^–è¦� Topology Automaticallyæ^–Tunnel

Allè¦^å�~æ-¹å¡Šã€,å¦,果未é�,ä,,則å¿...é ^手動執行é...�ç½®ã€,å¦,æžœé�,ä,æ

VF	N Site Cont	iguration	
Authentication	Phase 1 Pha	se 2 Policy	4
- IPSEC Policy	Configuration		
Policy Gene	ration Level	auto	~
🖌 Maintain	Persistent Secu	rity Associatio	ons
🖌 Obtain T	opology Automa	tically or Tuni	nel All
Remo	te Network Reso	ource	
Add	Madia	D.	alata
Auu	MODILY	De	siete
		Caula	Cancel
		Idve I	

æ¥é©Ÿ5.按ä,€ä,Addå°‡æ<"æ'2æ¢�ç>®æ–°å¢žå^°è;¨ä,ã€,凰ç�¾Topology Entryè⊢窗ã€,

Туре	Include	¥
Address		
Netmask		

æ¥é©Ÿ6.在「*ype*�下拉å¼�æ¸...å−®ä¸ï¼Œé�¸æ"‡é�©ç•¶çš"é�¸é ...ã€,

·åŒ…æ<¬ — 通�ŽVPN網關è ¨ªå•�網路ã€,

·æŽ'除 — 通�Žæœ¬åœ°é€£ç·šè¨ªå•�網路ã€,

Туре	Include 🗸 🗸
Address	Include Exclude
Netmask	

æ¥é©Ÿ7.在Addressæ¬,,ä½�ä,,è¼,å...¥RV0XXçš,,IP地å�€ã€,

æ¥é©Ÿ8.在*Netmask*æ¬,,ä½�ä,è¼,å...¥è£�ç½®çš,,å�網掩碼地å�€ã€,

Тор	ology Entry
Туре	Include 🗸 🗸
Address	192.168.1.0
Netmask	255.255.255.0

æ¥é©Ÿ9.按ä,€ä,∢「Kã€�ï¼^碰定)ã€,RV0XXçš,,IP地å�€å'Œå�網掩碼地å� Network Resourceæ,...å–®ä,ã€,

VF	N Site Cont	iguration	
Authentication	Phase 1 Pha	se 2 Policy	•
- IPSEC Policy	Configuration		
Policy Gene	ration Level	shared	~
🖌 Maintain	Persistent Secu	rity Associations	
🗌 Obtain T	opology Automa	tically or Tunnel.	All
Remo	te Network Reso	ource	
↔ 19216	68 1 0 / 255 255	255.0	
bbA	Modify	Deleti	
		0.0101	_

æ¥é©Ÿ10.按ä,€ä,**Save**,該æ"�作將使ç″¨è€...è¿″å>žå^°é; ¯ç¤°æ–°VPN連ç·šçš,,*VPN* Access Managerè⊢窗ã€,



連畚

本ç⁻€ä»‹ç´¹å¦,何在é…�置所有è¨å®šå¾Œè¨å®šVPN連ç·šã€,所需çš"ç™»å...¥

æ¥é©Ÿ1.按ä,€ä,<所需çš,,VPN連ç·šã€,

æ¥é©Ÿ2.按ä,€ä,€ã€Œonnectã€�ã€,

(B) VPN Acc	ess Mana	iger		-	
File Edit	View I	Help			
60	•	2	0		
Connect	Add	Modify	Delete		
8					
213.16.33.14	11				

 $\aa \ddagger^{a} \varsigma \diamondsuit {}^{3} 4 VPN \ Connect \grave{e} | -\varsigma^{a} - \ddot{i} {}^{1} 4 \check{s}$

w Help	
b 🤌 😑 dd Modify Delete	
S VPN Connect - 213.16.33.141 🗖 🖻 🛛	3
Connect Network	
Credentials	
Credentials Username Tunnel1	
Credentials Username Tunnel1 Password ••••••	
	w Help Add Modify Delete VPN Connect - 213.16.33.141 Connect Network Config loaded for site '213.16.33.141'

æ¥é©Ÿ3.在Usernameæ¬,,ä½�ä,è¼,å...¥VPNçš,,使ç″¨è€...å��稱ã€,

æ¥é©Ÿ4.在*Password* æ¬,,ä½**∲**ä¸è¼¸å...¥VPNä½;ç″¨è€...帳æ^¶çš"密碼ã€,

Shrew Soft VPN Connect - Cis	- • •
connect Network config loaded for site configuring client settings attached to key daemon peer configured iskamp proposal configured esp proposal configured client configured local id configured pre-shared key configured bringing up tunnel network device configured tunnel enabled	
Disconnect	Cancel

æ¥é©Ÿ6ã€,ï¼^å�¯é�,)è‹¥è¦�å�œç″¨é€£ç·šï¼Œè«‹æŒ‰ä,€ä,**‹Disconnect**ã€,

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。