ZyWALL USG シリーズ設定例

「iPhone を利用した L2TP over IPSec VPN 接続」について

構成例 iPhone を利用した L2TP over IPSec VPN 接続



- 1. ZyWALL USG の設定
 - ※ 本接続につきましては、ZyWALL USG の WAN 側 IP アドレスにグローバル固定アドレス (IP 固定サービスもしくは DynamicDNS 使用)を利用していることが前提となります。
 - (1) iPhone との接続で使用するユーザーアカウントの作成を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「Object」を選択します。
 - ③ 「User/Group」を選択します。
 - ④ 「User」タブを選択します。
 - ⑤ 「Add」をクリックして設定を行うアカウントの編集画面を開き、「User Name」、「User Type」、「Password」、「Retype」、「Description」を入力します。
 - ⑥ 「OK」ボタンを押下します。

ZyXEL ZYWAL	L USG 300	Welco	me admin 2000 ? Heip Z About 4	🕻 Site Map 🛛 Object Reference 🖵 Console 💽 CLI
CONFIGURATION	User Group Setting			? X
Network	User Configuration			
 Routing Zone DONS NAT HTTP Redirect ALG PMAC Einding Auth. Palcy Freewall VPN IPSec VPN SSL VPN L2TP VPN App Patrol AntX 	User Name: User Type: Password: Retype: Description: Authentication Timeout Settings Lease Time: Reauthentication Time:	sample user Local User Use Default Settings 1440 1440	© Use Manual Settings minutes minutes	
Device HA (2) Object (3) - HASENGROUP Address Service Schedule AAA Server det Matende	15 kurtyama 19 sample 14 Page I of I 1	₽ Show 50 ∨ items	OK Ca Local User Local User	nce Displaying 1 - 19 of 19

- (2) 接続に使用するアドレスの設定を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「Object」を選択します。
 - ③ 「Address」を選択します。
 - ④ 「Address」タブを選択します。
 - ⑤ 「Add」をクリックし、WAN 側の IP アドレスオブジェクトを作成します。
 - (ア)「Name」:任意の名称を入力します。
 - (イ)「Address Type」:「Interface IP」を選択します。
 - (ウ)「Interface」: WAN インタフェースを選択します。
 - (エ)「OK」ボタンを押下します。

📀 Add Address Rule	SUBNET	192.168.5.0 ? 🗙
Name: Address Type: Interface:	5 USG300-ge2-PPPoE INTERFACE IP ge2_ppp	v
o R_, .(1_SUBNET		OK Cancel

⑥ 「Add」をクリックし、LAN 側の IP アドレスオブジェクトを作成します。
 (ア)「Name」:任意の名称を入力します。

- (イ)「Address Type」:「SUBNET」を選択します。
- (ウ)「Network」:本構成例では、192.168.1.0 と入力します。
- (エ)「Netmask」:本構成例では、255.255.255.0と入力します。
- (オ)「OK」ボタンを押下します。

🕜 Edit Address Rule LAN	192.168.5.0 🕐 🗙	
Name: Address Type: Network: Netmask:	6 LAN_SUBNET SUBNET 192.168.1.0 255.255.255.0	
		Cancel 2

- ⑦ 「Add」をクリックし、IPSec で接続する機器に割り当てる IP アドレスオブジェクトを作成します。
 - (ア)「Name」に任意の名称を入力します。
 - (イ)「Address Type」で「Range」を選択します。
 - (ウ)「Starting IP Address」:本構成例では、192.168.10.1 と入力します。
 - (エ) 「End IP Address」:本構成例では、192.168.10.1 と入力します。
 - (オ)「OK」ボタンを押下します。

📀 Add Address Rule	SUBNET	192.168.5.0 ? 🗙
		^
Name:	C L2TP_POOL	
Address Type:	RANGE	¥ =
Starting IP Address:	192.168.10.1	
End IP Address:	192.168.10.10	
I_RPINT	RANGE	K Cancel 2
L SUBNET	INTERFACE SUBNET	de1-192 168 5 0/24

- (3) VPN Gateway の設定を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「VPN」を選択します。
 - ③ 「IPSec VPN」を選択します。
 - ④ 「VPN Gateway」タブを選択します。
 - ⑤ 設定を行う VPN Gateway を選択します。

	VPN Connection	VPN Gateway(4) Conce	ntrator	and the part of the local distance of the lo	
₩ Quick Setup	Configuration				
Hetwork	SAdd ZEC	lit 🍿 Remove 💡 Activate 🦓	Inactivate 📑 Object Refi	erence	
Routing	# Status	Name	My address	Secure Gateway	VPN Connection
	1 5 💡	Default_L2TP_VPN_GW	■ ge2_ppp	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection
+ DDNS	14 4 Page	e 1 of 1 🕨 🕅 Show	50 😽 items		Displaying 1 - 3 of 3
HTTP Redirect			, Frankl		
IP/MAC Binding Auth Policy					
	1				
+ Firewall					
• Firewall ⊡ VPN (2)					
Firewall VPN	1				

- ⑥ 「Show Advanced Settings」をクリックします。
- ⑦ 「General Settings」の「Enable」にチェックを入れ、「VPN Gateway Name」に任意の名称 を入力します。
- ⑧ 「My Address」に 1-(2)-⑤で入力した Name を選択します。
- ⑨ 「Authentication」の「Pre-Shared Key」に任意のキーを入力します。
- 10 「Phase 1 Settings」を設定します。
 - Negotiation Mode : <u>Main</u>
 - Proposal : Encryption : <u>3DES</u>
 - Proposal : Authentication : <u>SHA1</u>
 - Key Group : <u>DH2</u>
- 「OK」ボタンを押下します。

Edit VPN Gateway Default_L2TP	_VPN_0	SW			? >
Hide Advanced Settings 6					
Ceneral Settings					·
VPN Cateway Name:	0	Dofoult LOTE VEN CW	1		
vriv dateway Name.	Ø	Default_L2TP_VPN_GW			
Gateway Settings					
My Address	_				
Interface	8	ge2_ppp	Y Static	4746031131128338	μ j
Domain Name / IP					<u>}</u>
Peer Gateway Address					
Static Address		Primary 0.0.0.0			
		Secondary 0.0.0.0			
🔲 Fall back to Primary Peer G	ateway	when possible			
Fall Back Check Interval:		300	(60-86400 seconds)		
Oynamic Address			,		
A share to serve					
Authentication					
Pre-Shared Key	9	12345678			
Certificate		default	Y (See <u>My Certificates</u>	s)	
Local ID Type:		IP	*		
Content:		0.0.0.0			
Peer ID Type:		Any	~		
Content:					
			1		
Phase 1 Settings					
SA Life Time:	_	86400	(180 - 3000000 Seconds)		
Negotiation Mode:	10	Main	*		
Proposal		🗿 Add 🔜 Edit 🍵 Re	move		
	1	# Encryption -	Authentication		
		1 3DES	SHA1		
	1	2 3DES	MD5		
		3 DES	SHA1		
Key Group:		DH2	×		
NAT Traveral		DI12		J	
Extended Authentication					
Enable Extended Authentication	ı				
Server Mode		default	*		
Client Mode					
User Name:					
Password:					
					~
				ОК	Cancel

- (4) VPN Connection の設定を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「VPN」を選択します。
 - ③ 「IPSec VPN」を選択します。
 - ④ 「VPN Connection」タブを選択します。
 - ⑤ 設定を行う VPN Connection を選択します。

Z	YXEL ZYWALL U	ISG 300		Welco	me admin <u>Loqout</u>	PHelp Z Abou	t 🕴 Site Map	Pobject Reference	🖵 Console 🛛 CLI
	CONFIGURATION	VPN Connection () Global Setting Use Policy Route Ignore 'Don't Fra Configuration	VPN Gateway Co to control dynamic IPSe agment" setting in packe	ec rules					
	NAT HTTP Redirect ALG IP/MAC Binding Auth. Policy Firewall VPN (2) (3) + IPSec VPN	 Add	[Remove @ Activate Name Default_L2TP_VPN_C] of 1 ▶ ▶ Sho	VPN Gateway Default_L2TP_VPN w 50 vitems	onnect SDisconnect Encaps _GW TRANS	Diject Rel sulation Algor PORT 3DES	erence . ithm /SHA 3DES/M	Policy 15 <u>a USG300-ge2</u> Displayi	-PPPoE/ ng 1 - 3 of 3
	+ SSL VPN + L2TP VPN								

- ⑥ 「Show Advanced Settings」をクリックします。
- ⑦ 「General Settings」の「Enable」にチェックを入れ、「Connection Name」に任意の名称を 入力します。
- ⑧ 「Application Scenario」の「Remote Access(Server Role)」を選択します。
- ⑨ 「VPN Gateway」で、1-(3)-⑦で入力した VPN Gateway Name を選択します。

Edit VPN Connection Default_L2TP_VPN_Connection	? 🗙
6 Hide Advanced Settings 🛅 Create new Object 🗸	
General Settings	
⑦ ☑ Enable Connection Name:	
Nailed-Up	
Enable Replay Detection	
Enable NetBIOS broadcast over IPSec	
VPN Gateway	
Application Scenario	
Site-to-site	
Site-to-site with Dynamic Peer	
8 Remote Access (Server Role)	
Remote Access (Client Role)	
VPN Gateway:	
Manual Key	
🔘 Manual Key	
My Address:	
Secure Gateway Address:	
SPI: (256 - 4095)	×

- ⑩ 「Policy」の「Local Policy」に 1-(2)-⑤で入力した Name を選択します。
- ① 「Phase 2 Settings」を設定します。
 - Active Protocol : <u>ESP</u>
 - Encapsulation : <u>Transport</u>
 - Proposal : Encryption : <u>3DES</u>
 - Proposal : Authentication : <u>MD5</u>
 - Perfect Forward Secrecy(PFS) : none
- 12 「OK」ボタンを設定します。

licy		
.ocal policy:	USG300-ge2-PPPoE	35.13
ase 2 Settings		
A Life Time:	86400 (180 - 3000000 Seconds)	
ctive Protocol:	1) ESP 💌	
incapsulation:	Transport	
roposal	🔘 Add 🧱 Edit 🍵 Remove	
	# Encryption Authentication	
	1 3DES SHA1	
	2 3DES MD5	
	3 DES SHA1	
	(inclusion)	

- (5) L2TP VPN の設定を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「VPN」を選択します。
 - ③ 「L2TP VPN」を選択します。
 - 「L2TP VPN」タブを選択します。
 - ⑤ 「General Settings」の以下項目を設定します。
 - Enable L2TP Over IPSec にチェックを入れます。
 - VPN Connection: <u>1-(4)-⑦で入力した Connection Name</u>
 - IP Address Pool: <u>1-(2)-⑦で入力した Name</u>
 - Authentication Method : <u>default</u>
 - Allowed User: <u>1-(1)-⑤で入力した User Name</u>
 - ⑥ 「Apply」ボタンを押下します。

Z	YXEL ZYWALL	USG 300		Welcome admir	I Legout	?Help Z About ‡Site Map ⊒Object Reference ♀Console ⊂CLI
	CONFIGURATION	L2TP VPN (4)				
	T¥ Quick Setup	🔚 Create new Object 🗸				
0		General Settings				
R.	→ Zone	VPN Connection:	5	Default_L2TP_VPN_Cor	inect 🕶	
	+ DDNS + NAT	IP Address Pool:		LAN_SUBNET	*	
	HTTP Redirect	Authentication Method:		default	~	
	+ ALG + IP/MAC Binding	Allowed User:		sample	*	
	+ Auth. Policy	Keep Alive Timer:		60 (1-180 secon	ds)	
	+ Firewall	First DNS Server (Optional):		Custom Defined	~	
	+ IPSec VPN	Second DNS Server (Optional):		Custom Defined	*	
	SSL VPN BZTE VPN G	First WINS Server (Optional):				
	+ App Patrol	Second WINS Server (Optional):				

- (6) Local policy の設定を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「Network」を選択します。
 - ③ 「Routing」を選択します。
 - ④ 「Policy Route」タブを選択します。
 - ⑤ 「Add」をクリックします。
 - ⑥ 「Configuration」の「Enable」にチェックを入れ、「Description」に任意の名称を入力します。
 - ⑦「Criteria」の「Source Address」で、リモートユーザにアクセスを許可するアドレスオブジェ クト(本構成例では 1-(2)-⑥で作成した LAN_SUBNET)を選択します。「Destination Address」 で、リモートユーザに割り当てたアドレスオブジェクト(本構成例では 1-(2)-⑦で作成した L2TP_POOL)を選択します。
 - ⑧ 「Next-Hop」の「Type」で「VPN Tunnel」を選択し、「VPN Tunnel」で1-(4)-⑦で入力した Connection Name を選択します。
 - ⑨ 「OK」ボタンを押下します。

Z Edit Policy Route Show Advanced Settings		? ×
🏢 Show Advanced Settings 🔚 Create new Obje	ct.≁	
Configuration		<u>^</u>
5 🔽 Enable		
Description:	iPhone_VPN_Route (Optional)	
Criteria		
User:	any	
Incoming:	any (Excluding ZyWALL)	
Source Address:	6 LAN_SUBNET	
Destination Address:	L2TP_POOL	
DSCP Code:	any	
Schedule:	none 💌	
Service:	any	
Next-Hop		
Туре:	7 VPN Tunnel	
VPN Tunnel:	Default_L2TP_VPN_Connecti	
		OK Cancel

2. iPhone の設定

- (1) iPhone 側の VPN 設定を行います。
 - ① ホーム画面の「設定」を選択します。
 - ② 設定画面の「一般」を選択します。
 - ③ 一般画面の「ネットワーク」を選択します。
 - ④ ネットワーク画面の「VPN」を選択します。
 - ⑤ VPN 画面の「VPN 構成を追加」を選択します。
 - ⑥ RRR構成を追加画面の「L2TP」を選択し、以下項目を設定して保存します。
 - 説明:<u>任意の名称</u>
 - サーバ: 接続先のサーバ名又は IP アドレス
 - アカウント: <u>1-(1)-⑤で入力した User Name</u>
 - RSA SecurID: RSA SecurID トークンを使用する場合: オン RSA SecurID トークンを使用しない場合: オフ
 - パスワード: <u>1-(1)-⑤で入力した Password</u>
 - シークレット: <u>1-(3)-⑨で入力した Pre-Shared Key</u>
 - すべての信号を送信:<u>オン</u>



(2) 以上で設定完了となります。VPN 画面で「VPN」をオンにしてください。

3. VPN 接続している状態で、iPhone からインターネットアクセスする方法

2までの設定を行った時点では、iPhoneからLAN内へのアクセスは可能ですが、iPhoneからインターネットへのアクセスはできません。インターネットへのアクセスを許可する場合、さらに ZyWALL USG で以下の設定が必要になります。 ※iPhone 側では追加の設定は必要ありません。

- (1) Local policy の設定を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「Network」を選択します。
 - ③ 「Routing」を選択します。
 - ④ 「Policy Route」 タブを選択します。
 - ⑤ 「Add」をクリックします。
 - ⑥ 「Configuration」の「Enable」にチェックを入れ、「Description」に任意の名称を入力します。
 - ⑦ 「Criteria」の「User」でインターネットアクセスを許可するユーザ、「Incoming」で、Tunnel、 を選択し、その下に表示される「Please select one member」で1-(4)-⑦で入力した Connection Name を選択し、「Source Address」で、リモートユーザに割り当てたアドレスオブジェクト(本 構成例では1-(2)-⑦で作成したL2TP_POOL)を選択します。
 - ⑧ 「Next-Hop」の「Type」で「Trunk」を選択し、「Trunk」で外部に接続する WAN trunk を選択(本例では SYSTEM_DEFAULT_WAN_TRUNK)します。
 - ⑨ 「OK」ボタンを押下します。

🕜 Edit Policy Route		? 🗙
🏢 Show Advanced Settings	t v	
Configuration Image: Criteria	L2TP VPN to Internet (Optional)	
User: Incoming: Please select one member: Source Address:	sample Tunnel Default_L2TP_VPN_Connecti L2TP_POOL	
Destination Address:	any	
DSCP Code: Schedule:	any Y	
Service:	any	
Next-Hop		
Туре:	8 Trunk	
Trunk:	SYSTEM_DEFAULT_WAN_TR	~
		OK Cancel

- (2) DNS サーバの設定を行います。
 - ① 「CONFIGURATION」を選択します。
 - ② 「VPN」を選択します。
 - ③ 「L2TP VPN」を選択します。
 - ④ 「L2TP VPN」タブを選択します。
 - ⑤ 「General Settings」の以下項目を追加設定します。
 - First DNS Server:任意の有効な DNS サーバ
 Second DNS Server:任意の有効な DNS サーバ
 - ※First DNS Server のみ設定した場合でも動作します。 「Apply」ボタンを押下します。

Z	YXEL ZYWALL U	JSG 300	Welcome admin <u>Loqout</u>	?Help	Z About	甞 Site Map	CODject Reference	🖵 Console	C.I. (T.I.
•	CONFIGURATION	L2TP VPN							
	Ty Quick Setup	🏢 Show Advanced Settings	,						
<u></u>	Licensing Network	General Settings							
	 Interface Routing 	V Enable L2TP Over IPSec							
R,	+ Zone	VPN Connection:	Default_L2TP_VPN_Connecti	~					
	+ DDNS + NAT	IP Address Pool:	L2TP_POOL	~					
	→ HTTP Redirect	Authentication Method:	default	*					
	+ ALG + IRMAC Binding	Allowed User:	sample	~					
	+ DNS Inbound LB	Keep Alive Timer:	60 (1-180 seconds)						
		First DNS Server (Optional):	From ISP	~	ge2_pp	p 1st DNS Se	rver 💌		
	+ Firewall ⊡ VPN	Second DNS Server (Optional):	Custom Defined	~	8.8.8.8				
	→ IPSec VPN	First WINS Server (Optional):							
	 → SSL VPN → L2TP VPN 	Second WINS Server (Optional):							

以上になります。

6