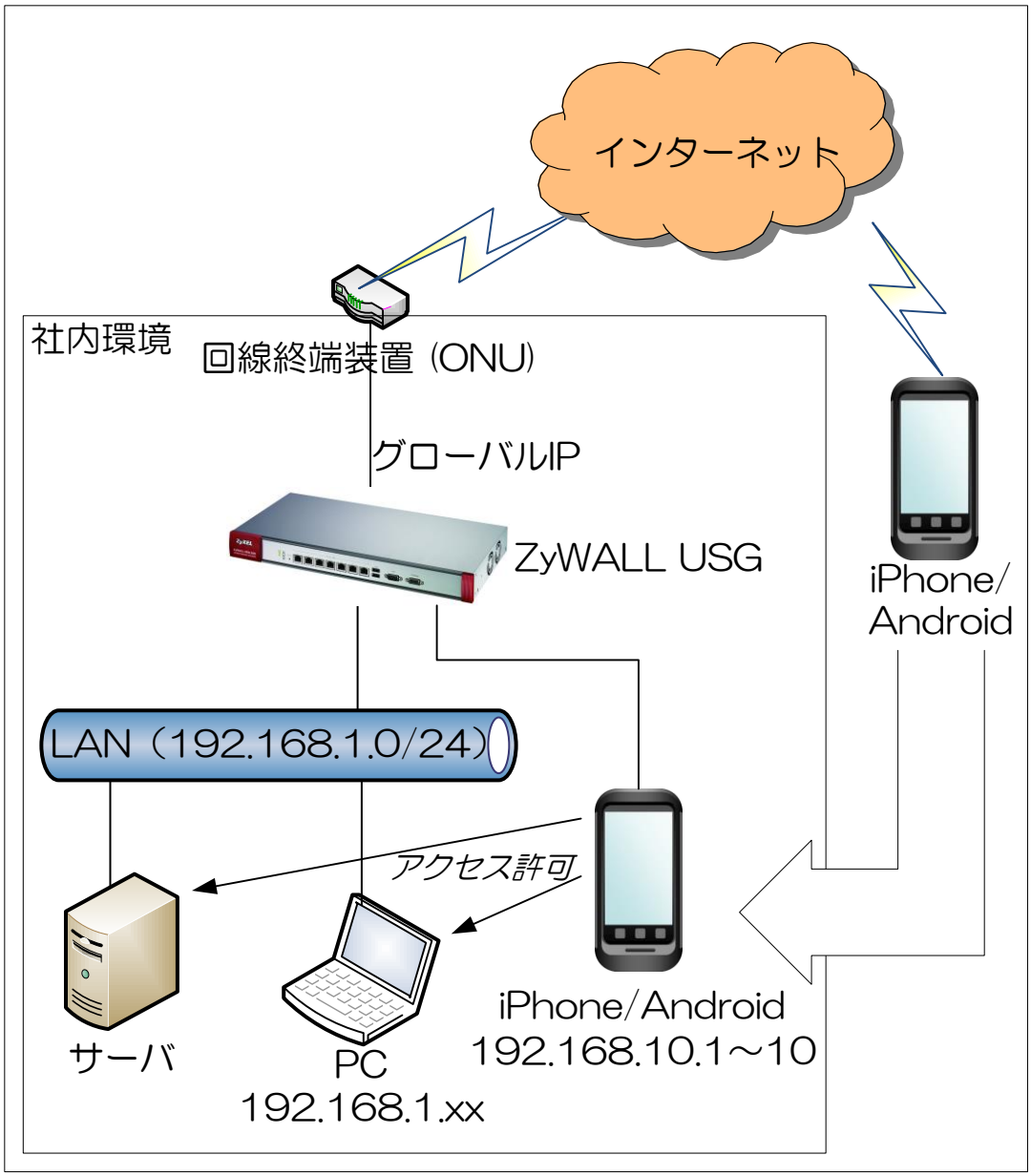
ZyWALL USG シリーズ設定例

「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

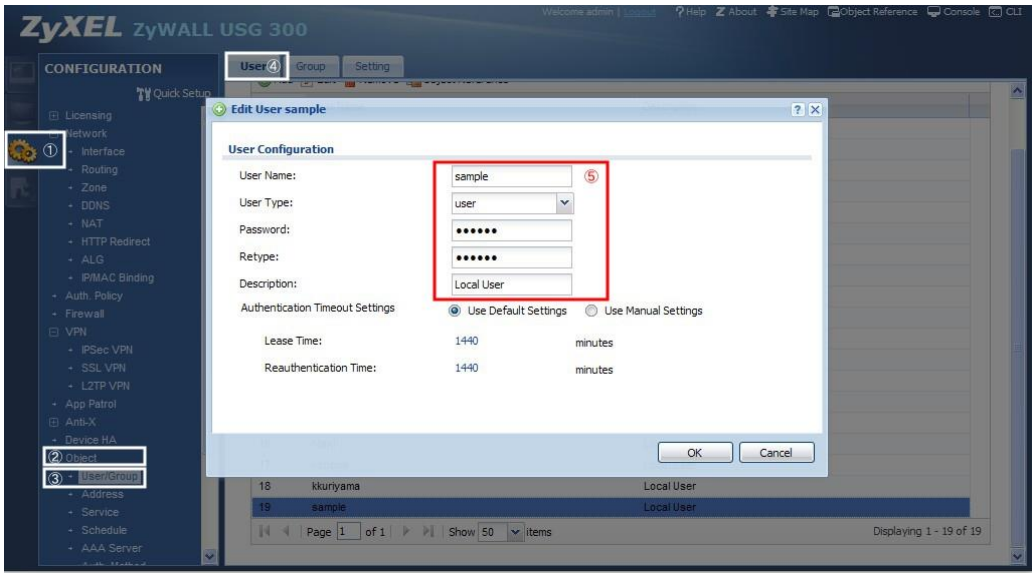


1. ZyWALL USG の設定

※ 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。

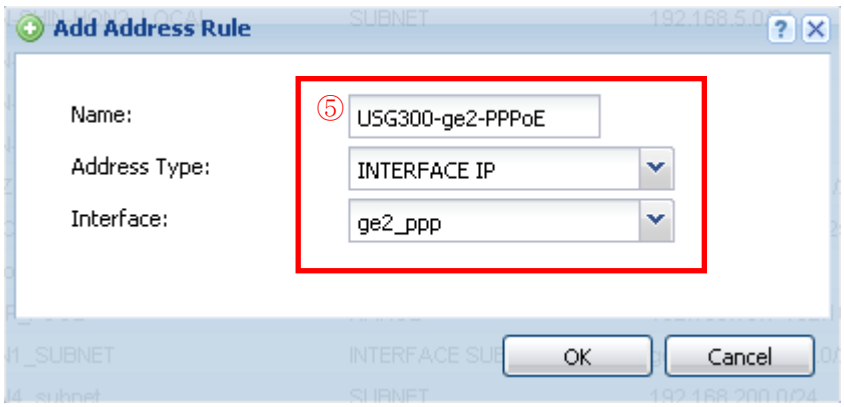
(1) iPhone との接続で使用するユーザーアカウントの作成を行います。

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。



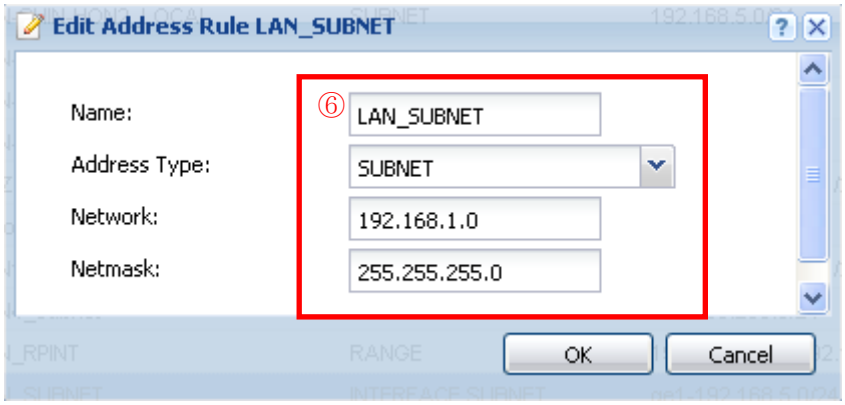
(2) 接続に使用するアドレスの設定を行います。

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。

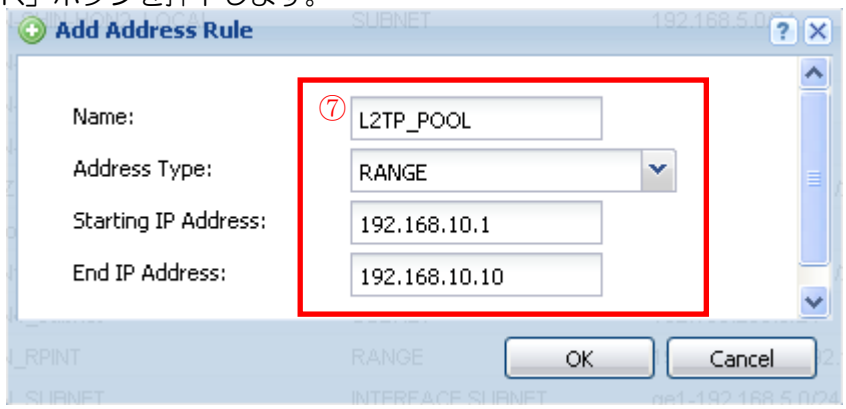


⑥ 「Add」をクリックし、LAN 側の IP アドレスオブジェクトを作成します。
(ア) 「Name」:任意の名称を入力します。

(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。

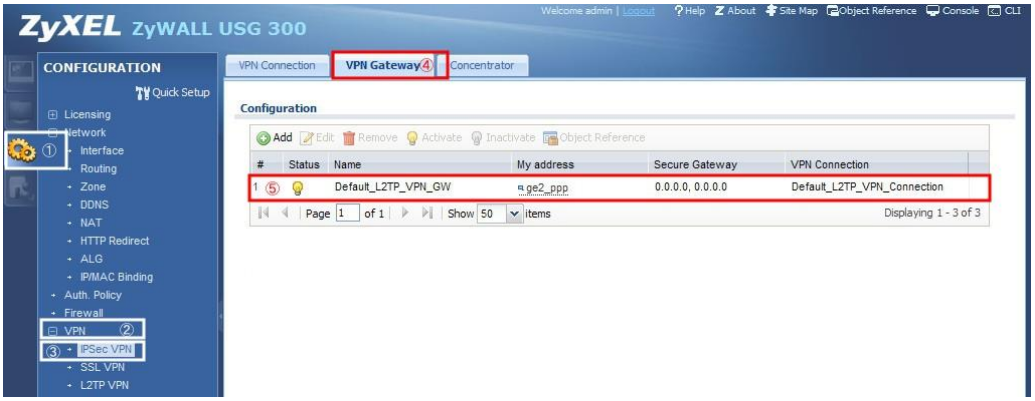


⑦ 「Add」をクリックし、IPSec で接続する機器に割り当てる IP アドレスオブジェクトを作成します。
(ア) 「Name」に任意の名称を入力します。
(イ) 「Address Type」で「Range」を選択します。
(ウ) 「Starting IP Address」: 本構成例では、192.168.10.1 と入力します。
(エ) 「End IP Address」: 本構成例では、192.168.10.1 と入力します。
(オ) 「OK」ボタンを押下します。



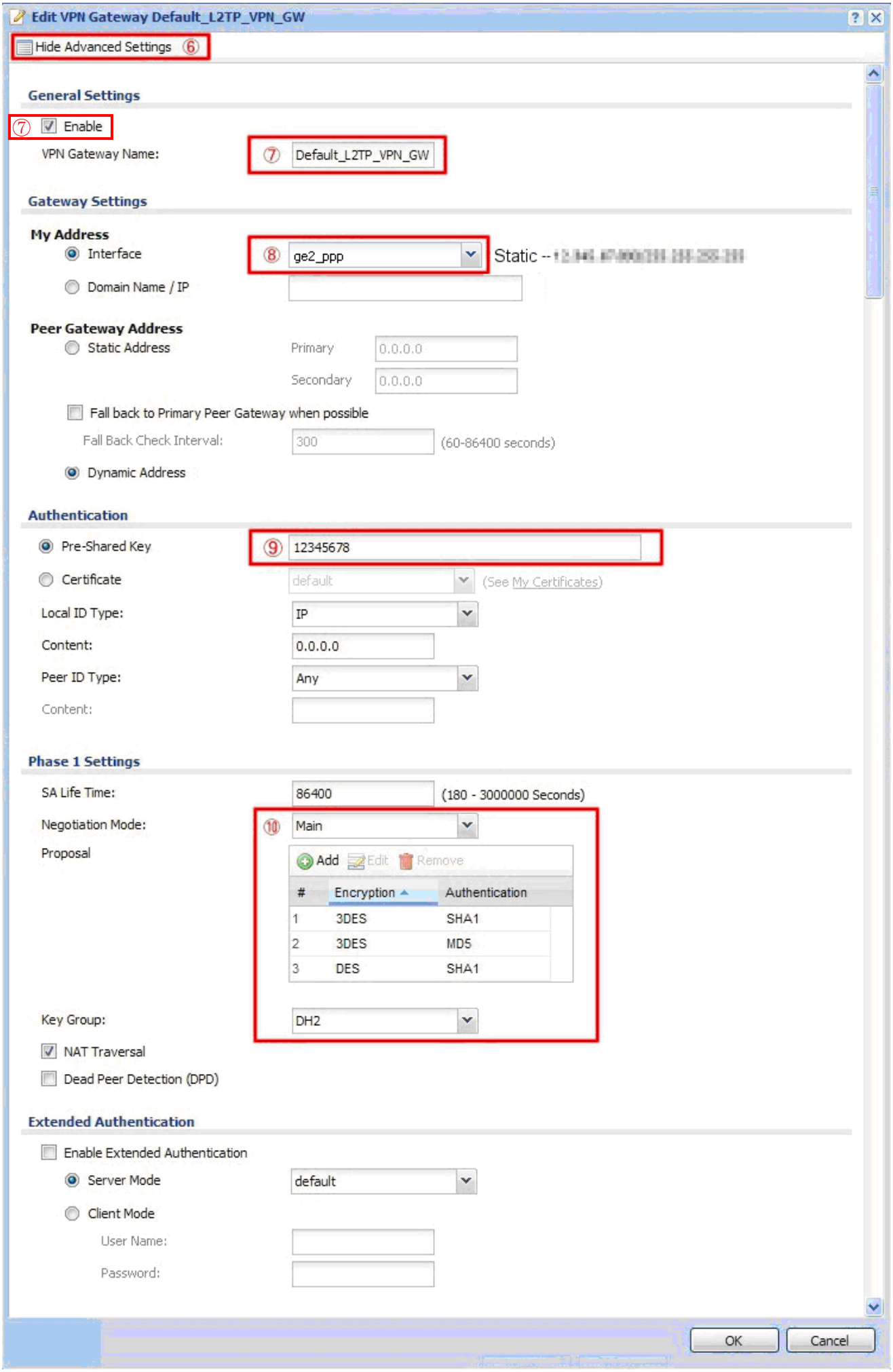
⑶ VPN Gateway の設定を行います。

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。



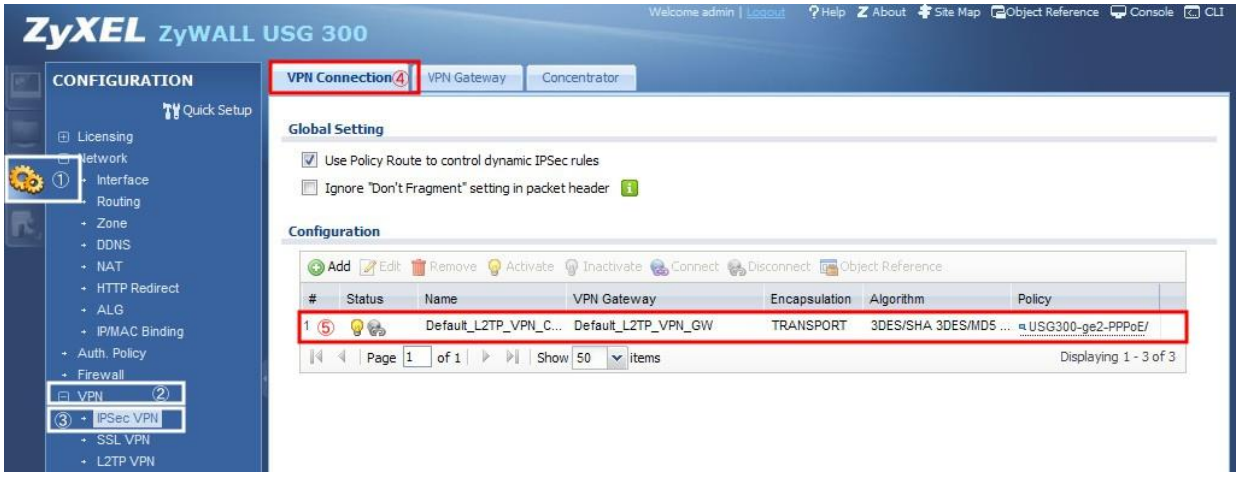
⑥ 「Show Advanced Settings」をクリックします。
⑦ 「General Settings」の「Enable」にチェックを入れ、「VPN Gateway Name」に任意の名称を入力します。
⑧ 「My Address」に 1-⑵-⑤で入力した Name を選択します。
⑨ 「Authentication」の「Pre-Shared Key」に任意のキーを入力します。
⑩ 「Phase 1 Settings」を設定します。
- Negotiation Mode：Main
- Proposal：Encryption：3DES
- Proposal：Authentication：SHA1
- Key Group：DH2

⑪ 「OK」ボタンを押下します。

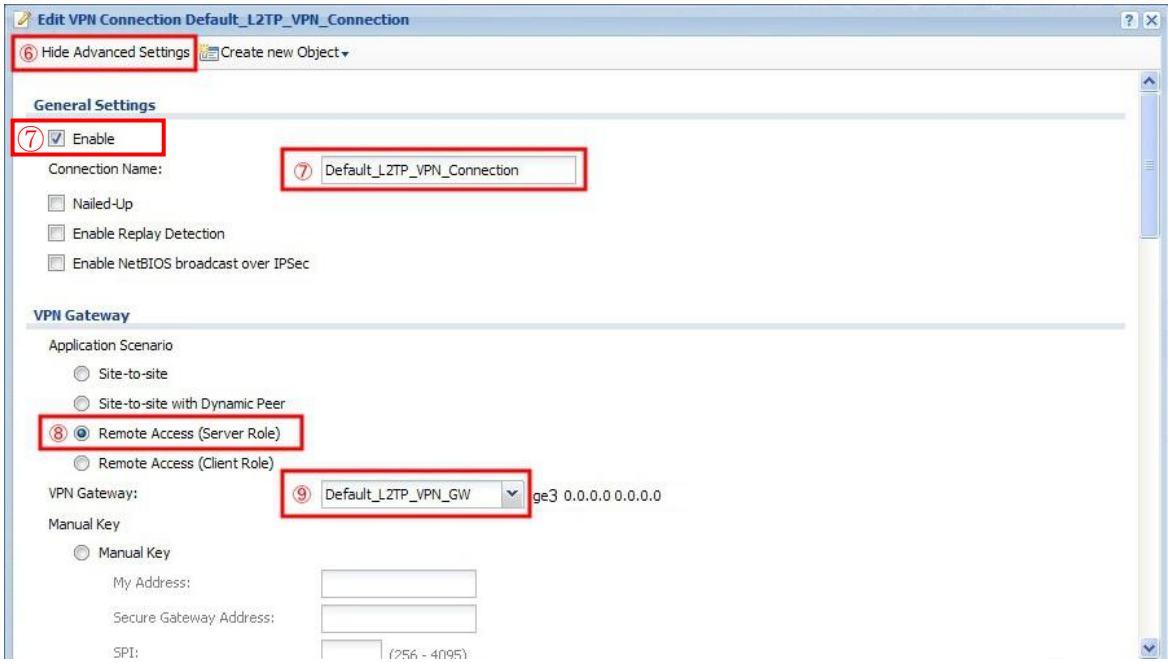

Edit VPN Gateway Default_L2TP_VPN_GW
Hide Advanced Settings ⑥
General Settings
⑦ Enable
VPN Gateway Name:
⑦ Default_L2TP_VPN_GW
Gateway Settings
My Address
Interface
⑧ ge2_ppp
Static --
Domain Name / IP
Peer Gateway Address
Static Address
Primary
0.0.0.0
Secondary
0.0.0.0
Fall back to Primary Peer Gateway when possible
Fall Back Check Interval:
300
(60-86400 seconds)
Dynamic Address
Authentication
Pre-Shared Key
⑨ 12345678
Certificate
default
(See My Certificates)
Local ID Type:
IP
Content:
0.0.0.0
Peer ID Type:
Any
Content:
Phase 1 Settings
SA Life Time:
86400
(180 - 3000000 Seconds)
Negotiation Mode:
⑩ Main
Proposal
Add
Edit
Remove
Encryption Authentication
1 3DES SHA1
2 3DES MD5
3 DES SHA1
Key Group:
DH2
NAT Traversal
Dead Peer Detection (DPD)
Extended Authentication
Enable Extended Authentication
Server Mode
default
Client Mode
User Name:
Password:
OK
Cancel

⑷ 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。

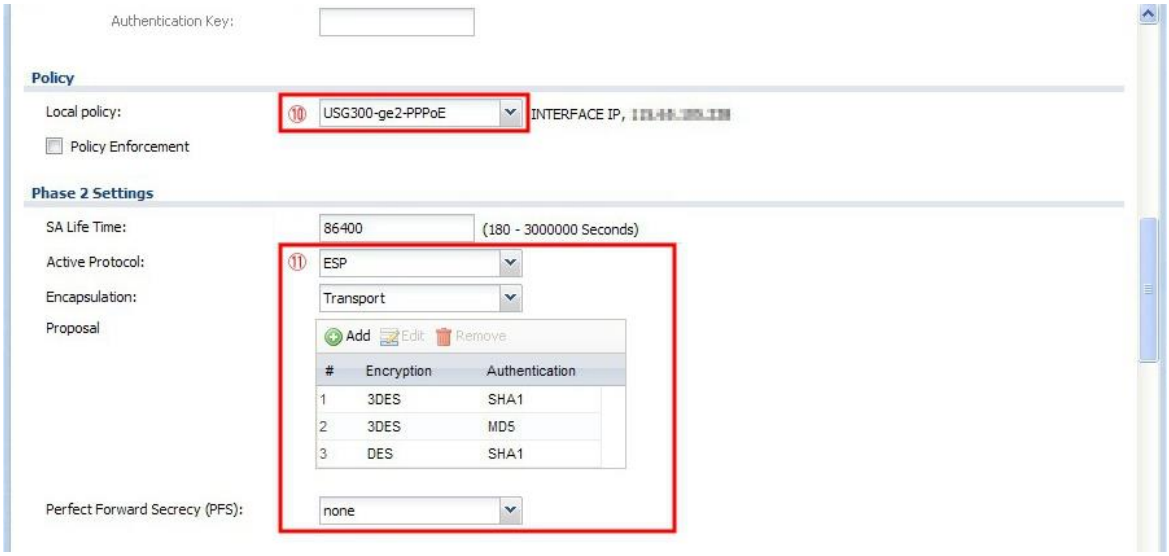


⑥ 「Show Advanced Settings」をクリックします。
⑦ 「General Settings」の「Enable」にチェックを入れ、「Connection Name」に任意の名称を入力します。
⑧ 「Application Scenario」の「Remote Access(Server Role)」を選択します。
⑨ 「VPN Gateway」で、1-⑶-⑦で入力した VPN Gateway Name を選択します。



⑩　「Policy」の「Local Policy」に 1-(2)-⑤で入力した Name を選択します。
⑪　「Phase 2 Settings」を設定します。
- Active Protocol：ESP
- Encapsulation：Transport
- Proposal：Encryption：3DES
- Proposal：Authentication：MD5
- Perfect Forward Secrecy(PFS)：none

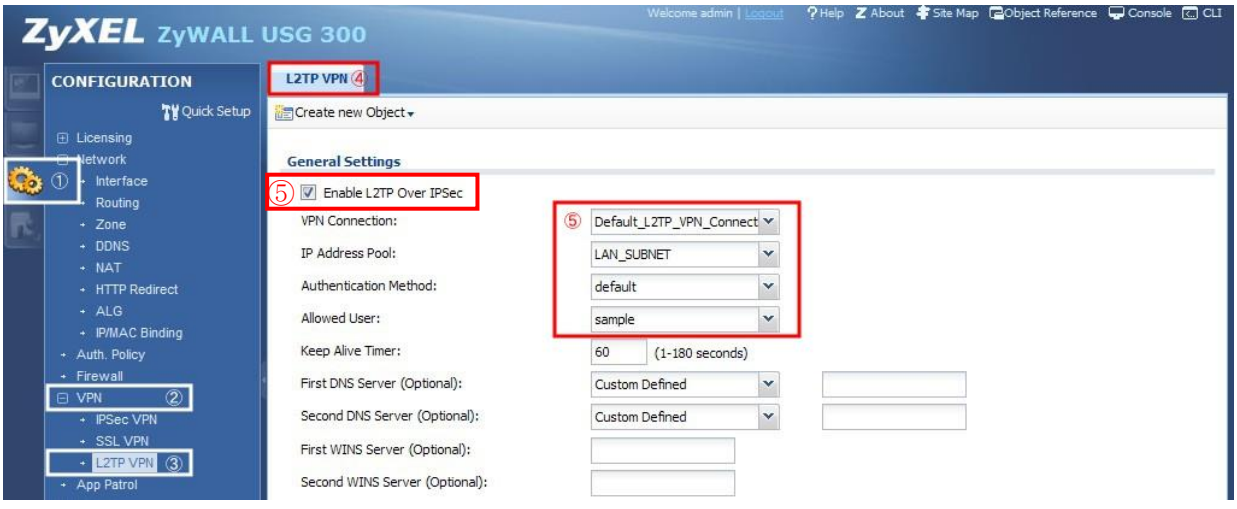
⑫　「OK」ボタンを設定します。



(5) L2TP VPN の設定を行います。

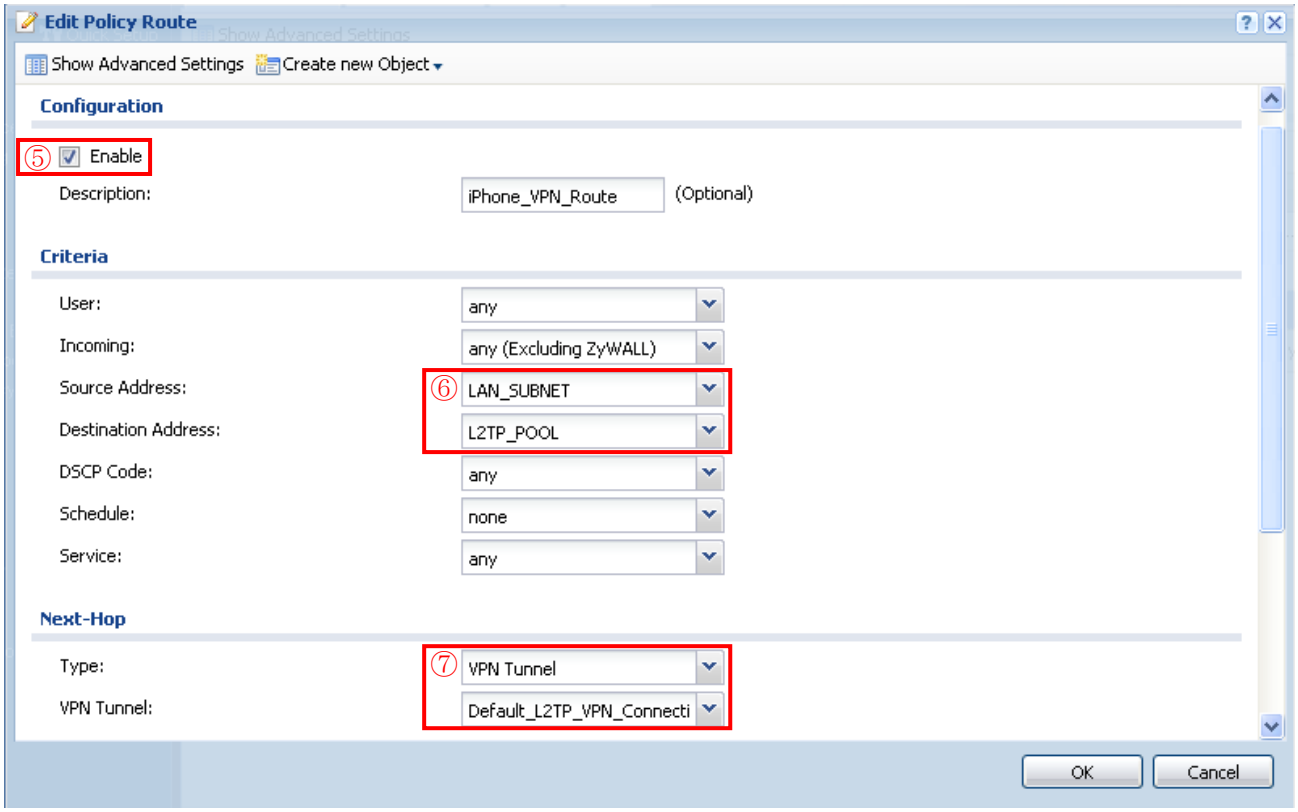
①　「CONFIGURATION」を選択します。
②　「VPN」を選択します。
③　「L2TP VPN」を選択します。
④　「L2TP VPN」タブを選択します。
⑤　「General Settings」の以下項目を設定します。
- Enable L2TP Over IPSec にチェックを入れます。
- VPN Connection：1-(4)-⑦で入力した Connection Name
- IP Address Pool：1-(2)-⑦で入力した Name
- Authentication Method：default
- Allowed User：1-(1)-⑤で入力した User Name

⑥　「Apply」ボタンを押下します。



⑹ 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-⑵-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-⑵-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-⑷-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。



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：任意の名称
- サーバ：接続先のサーバ名又は IP アドレス
- アカウント：1-(1)-⑤で入力した User Name
- 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：1-(1)-⑤で入力した Password
- シークレット：1-(3)-⑨で入力した Pre-Shared Key
- すべての信号を送信：オン

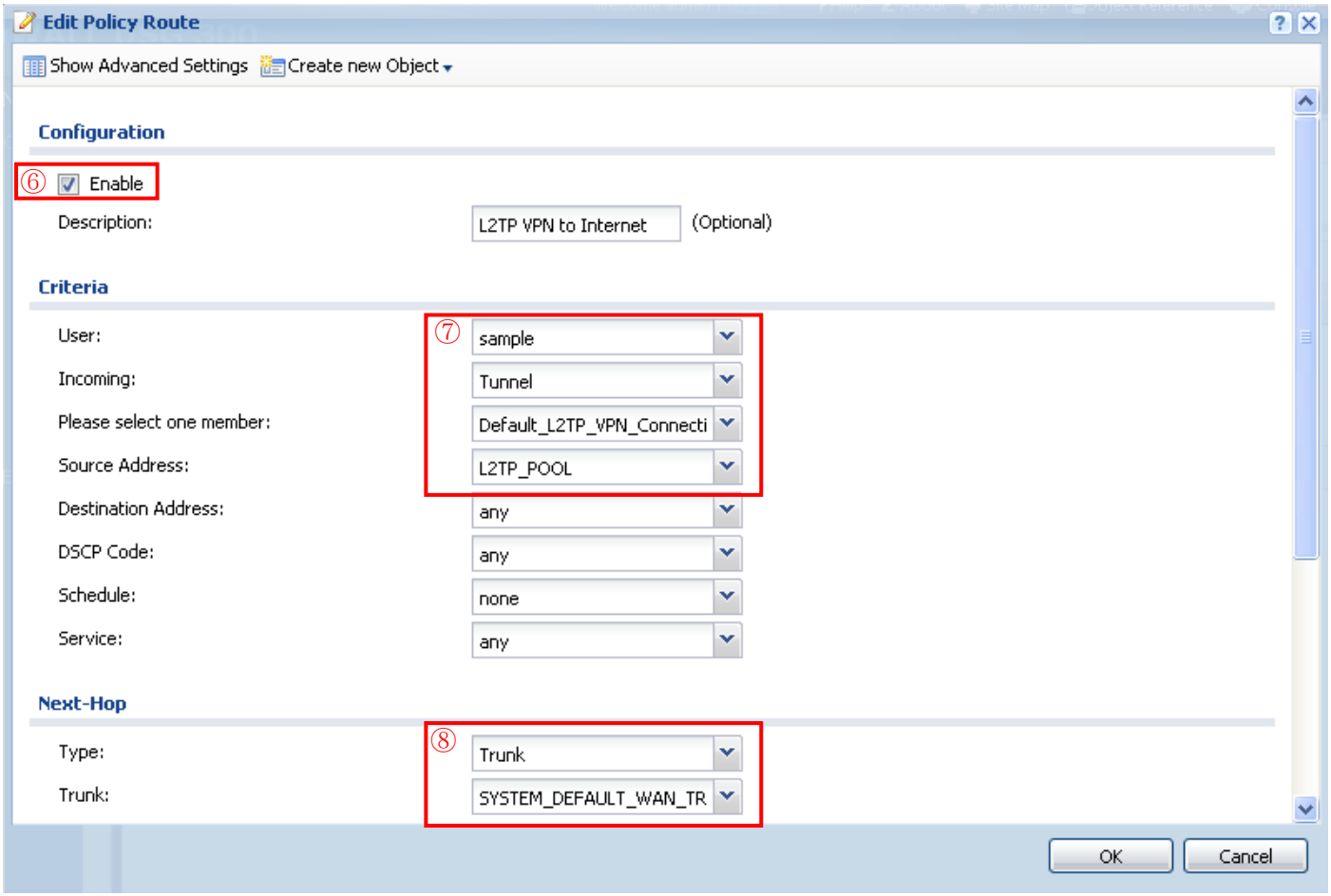
（2）以上で設定完了となります。VPN 画面で「VPN」をオンにしてください。

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。

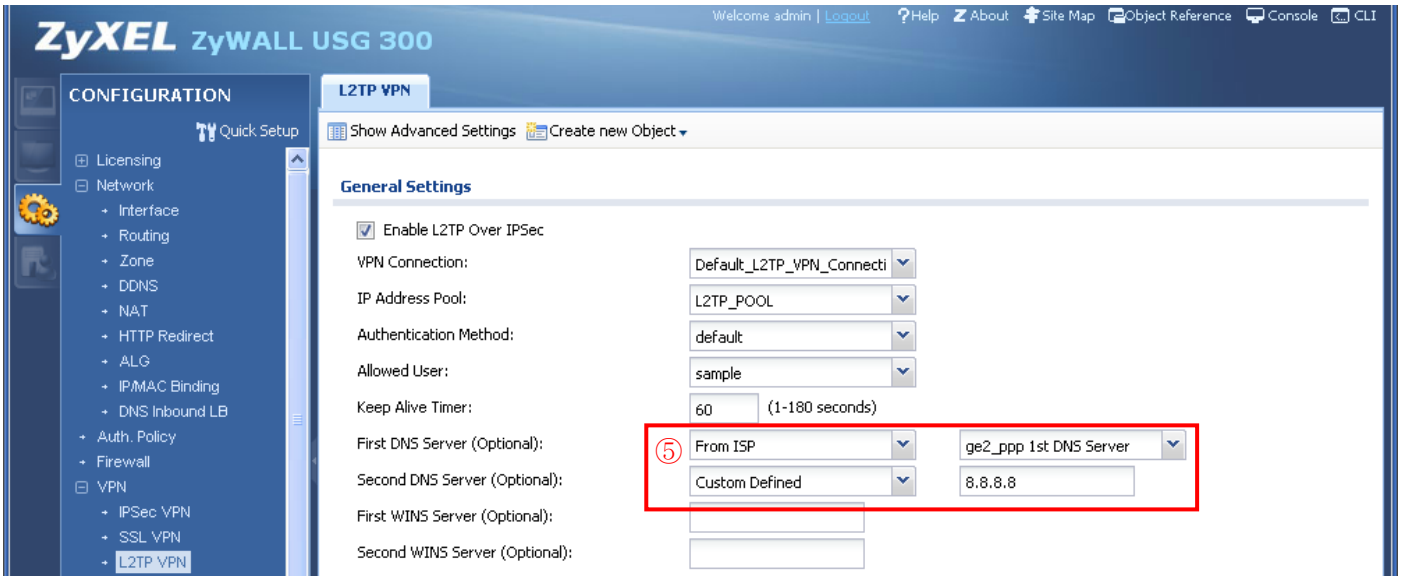


⑵ DNS サーバの設定を行います。

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。

⑥ 「Apply」ボタンを押下します。



以上になります。