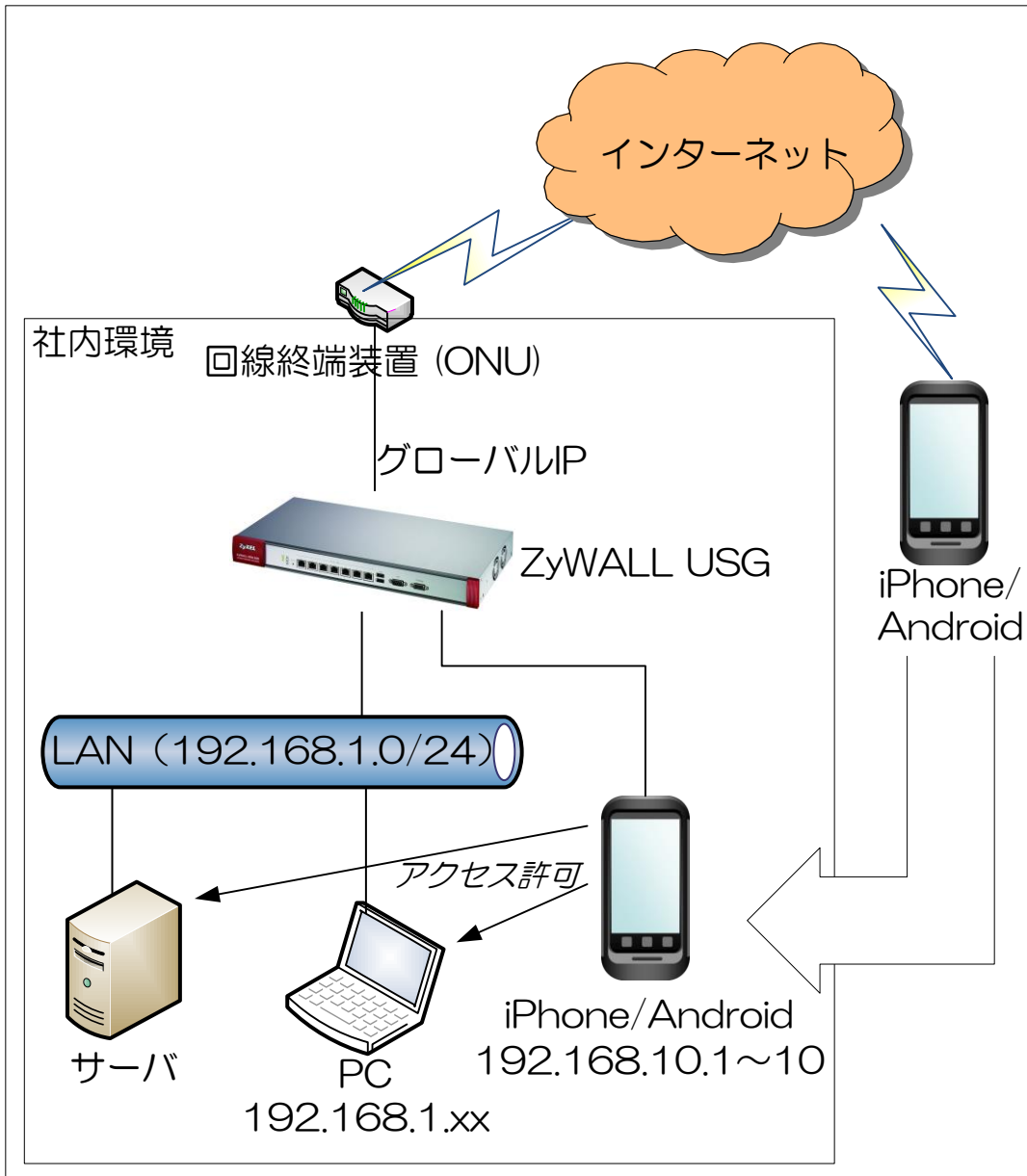


ZyWALL USG シリーズ設定例

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

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



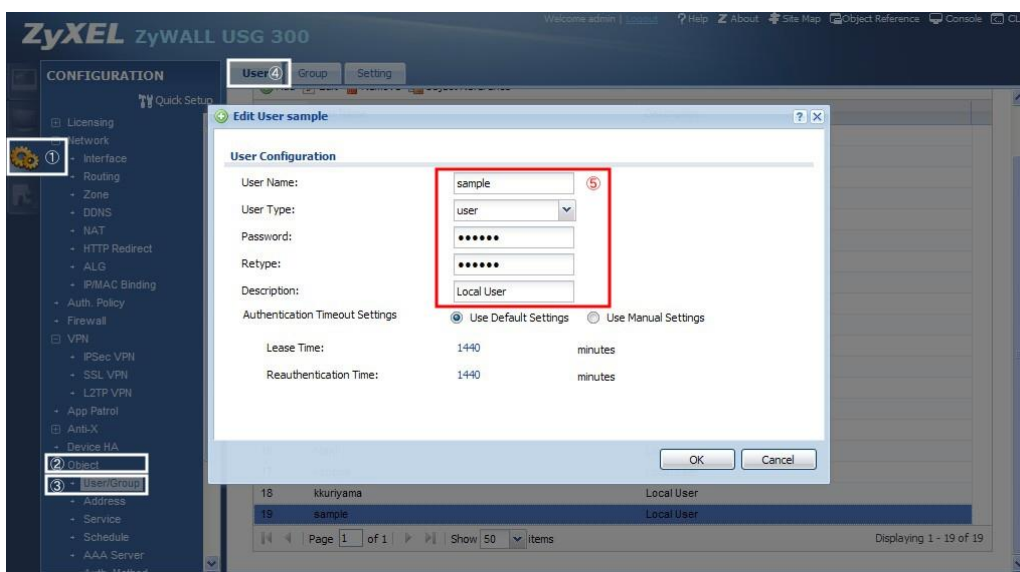
(本構成例では、Android Version 4.4.3 の Nexus 7 を使用して設定を説明します。)

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。

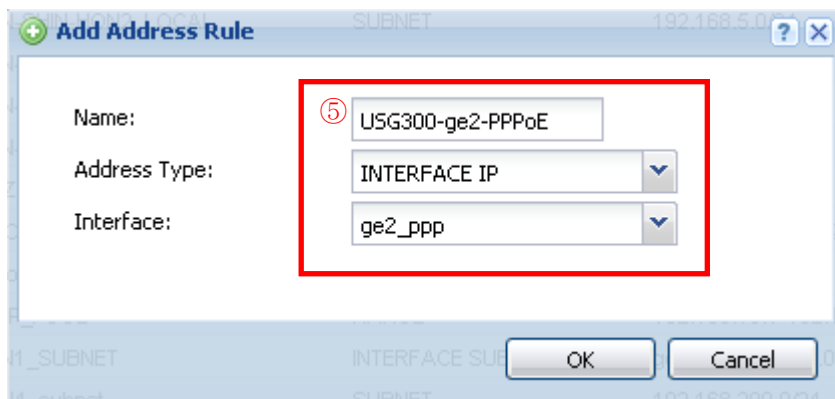
(1) Android との接続で使用するユーザーアカウントの作成を行います。

- 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。

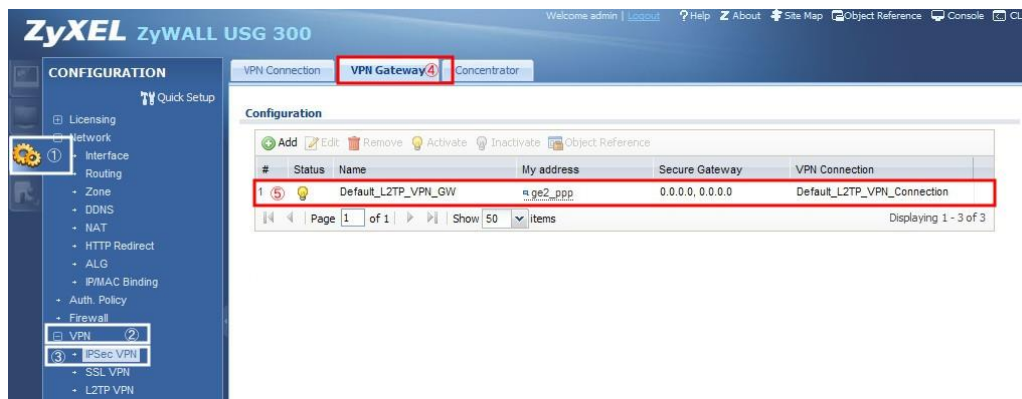
⑥

- 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、192.168.10.10 と入力します。
- (オ) 「OK」 ボタンを押下します。

⑦

(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。



- 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 : 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 -- 10.144.107.000/28 10.144.107.255/28

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

9 Pre-Shared Key 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

#	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

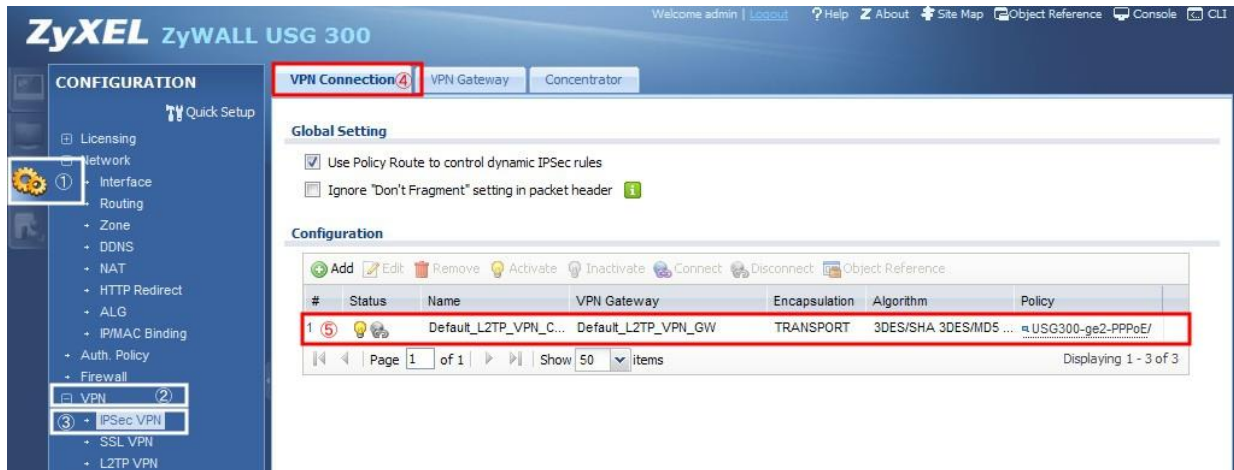
User Name:

Password:

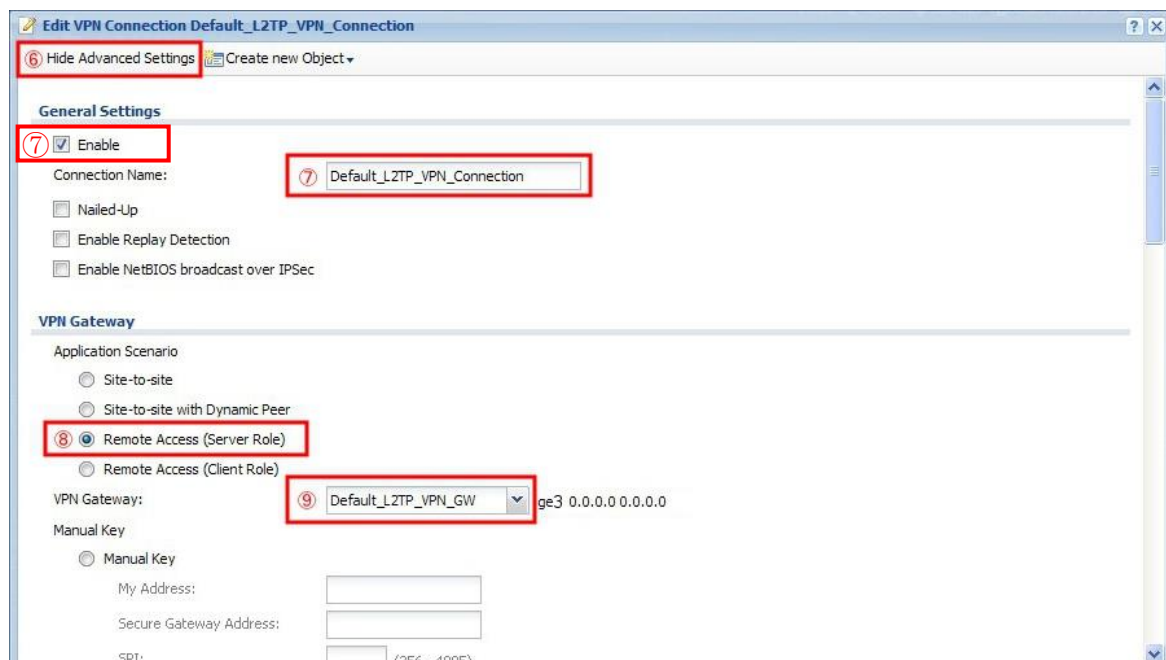
OK Cancel

(4) VPN Connection の設定を行います。

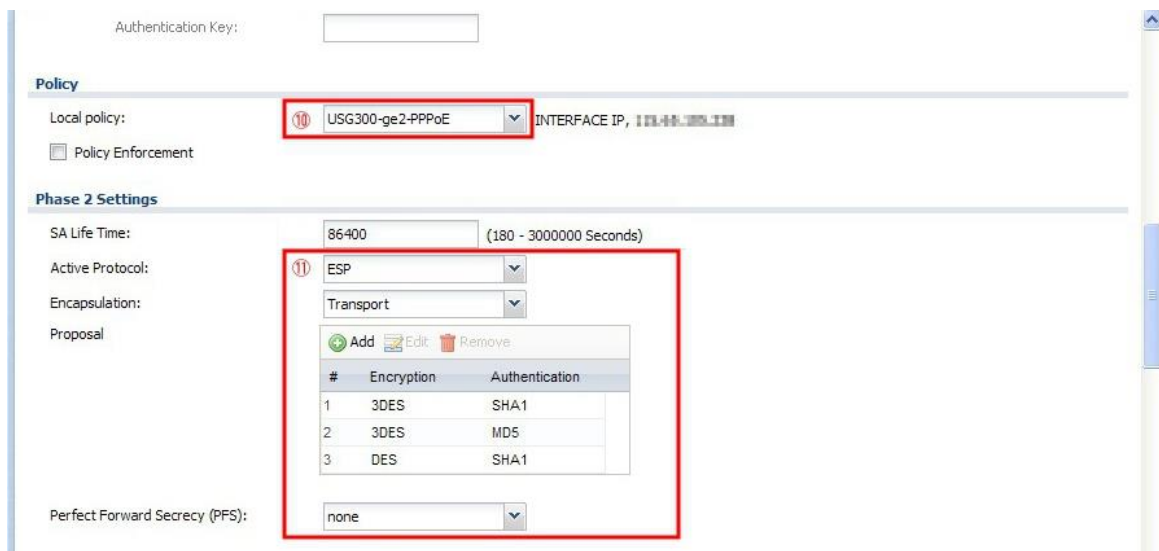
- ① 「CONFIGURATION」を選択します。
- ② 「VPN」を選択します。
- ③ 「IPSec VPN」を選択します。
- ④ 「VPN Connection」タブを選択します。
- ⑤ 設定を行うVPN Connectionを選択します。



- 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。

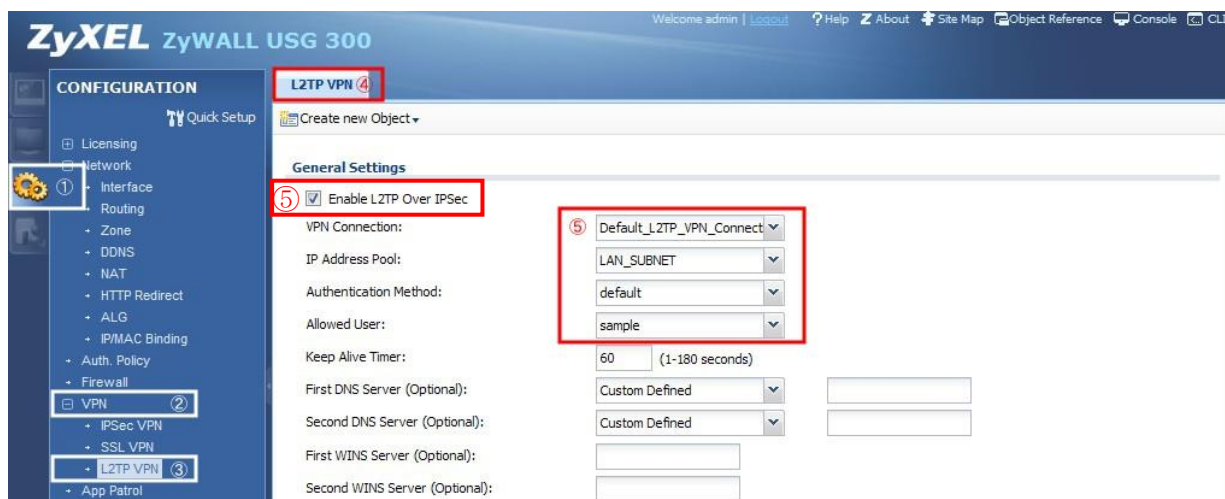


- ⑩ 「Policy」の「Local Policy」に 1-(2)-⑤で入力した Name を選択します。
- ⑪ 「Phase 2 Settings」を設定します。
 - Active Protocol : ESP
 - Encapsulation : Transport
 - Proposal : Encryption : 3DES
 - Proposal : Authentication : MD5
 - Perfect Forward Secrecy(PFS) : none
- ⑫ 「OK」ボタンを設定します。



(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。



(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。

Edit Policy Route Show Advanced Settings

Show Advanced Settings Create new Object

Configuration

⑤ Enable

Description: Android_VPN_Route (Optional)

Criteria

User: any

Incoming: any (Excluding ZyWALL)

⑥ Source Address: LAN_SUBNET

Destination Address: L2TP_POOL

DSCP Code: any

Schedule: none

Service: any

Next-Hop

⑦ Type: VPN Tunnel

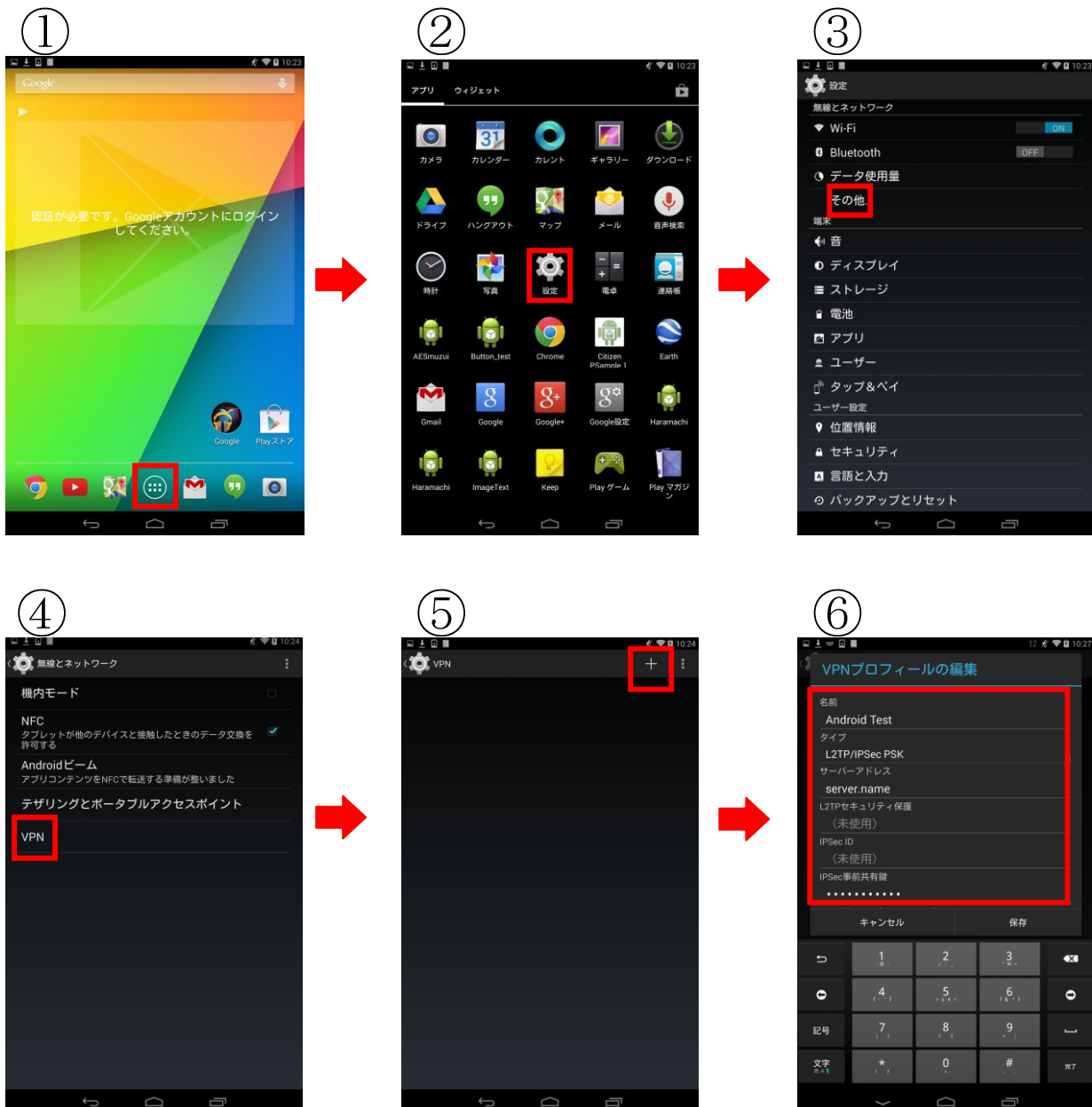
VPN Tunnel: Default_L2TP_VPN_Connecti

OK Cancel

2. Android の設定

(1) Android 側の VPN 設定を行います。

- ① ホーム画面の「アプリ一覧」を選択します。
- ② アプリ一覧画面の「設定」を選択します。
- ③ 設定画面の無線とネットワークの「その他」を選択します。
- ④ 無線とネットワーク画面の「VPN」を選択します。
 - 画面ロックを設定していない場合、「認証情報ストレージを使用するには、画面ロックの PIN またはパスワードを設定する必要があります。」との注意が表示されます。「OK」を選択して、ロック解除方法を設定してください。
- ⑤ VPN 画面の「+」を選択します。
- ⑥ VPN プロフィールの編集を行います。以下の項目を設定して保存します。
 - 名前：任意の名称を付けます。
 - タイプ：L2TP/IPSec PSK を選択します。
 - サーバーアドレス：接続先のサーバ名または IP アドレスを入力します。
 - IPSec 事前共有鍵：1-(3)-⑨で入力した Pre-Shared Key を入力します。
 - その他の項目はデフォルトのままです。



(2) VPN 接続を行います。

- ① VPN 画面を開き、2-(1) で設定した VPN 接続を選択します。
- ② ユーザー名とパスワードを入力し、「接続」を選択します。
 - ユーザー名：1-(1)-⑤で入力した User Name
 - パスワード：1-(1)-⑤で入力した Password



3. VPN 接続している状態で、Android 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、Android から LAN 内へのアクセスは可能ですが、Android 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。

※Android 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 Create new Object

Configuration

⑥ Enable

Description: L2TP VPN to Internet (Optional)

Criteria

User: ⑦ sample

Incoming: Tunnel

Please select one member: Default_L2TP_VPN_Connecti

Source Address: L2TP_POOL

Destination Address: any

DSCP Code: any

Schedule: none

Service: any

Next-Hop

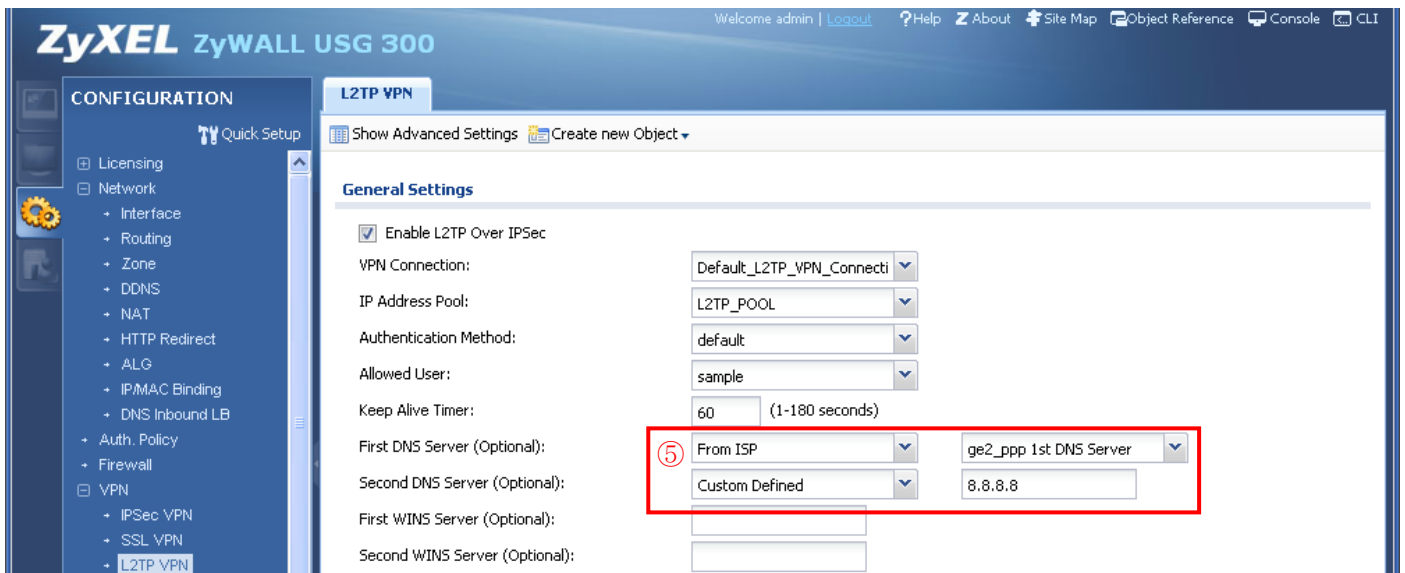
Type: ⑧ Trunk

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。
- ⑥ 「Apply」ボタンを押下します。



以上になります。