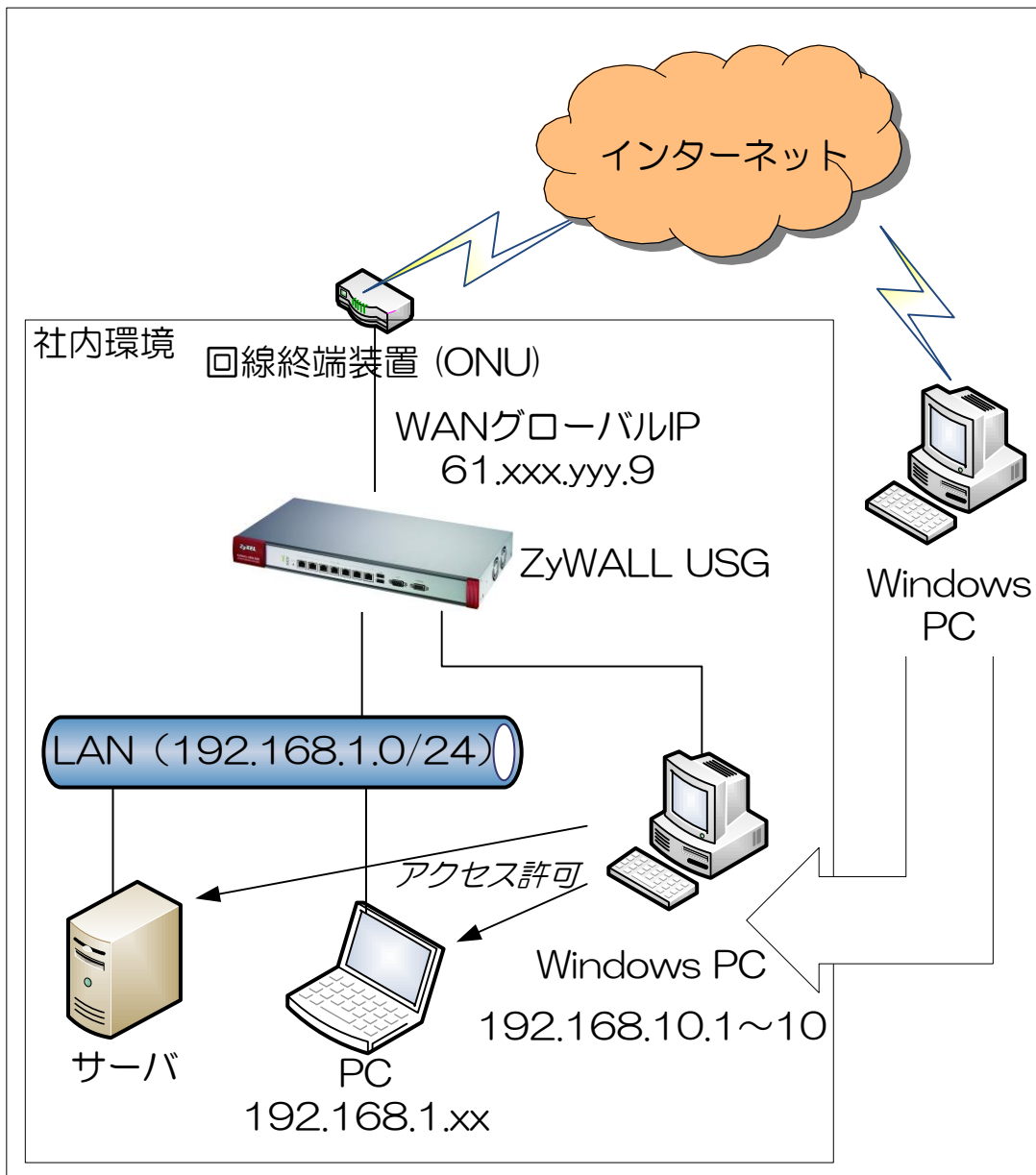


ZyWALL USG シリーズ設定例

「Windows OS での VPN 接続 (L2TP over IPSec VPN 接続)」について

構成例 Windows OS での VPN 接続

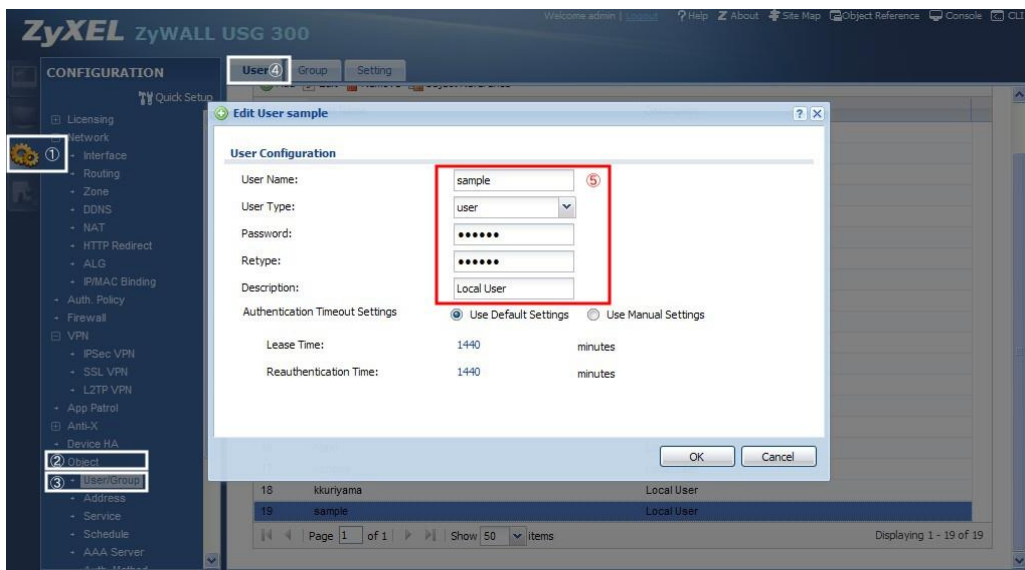


1. ZyWALL USG の設定

※ 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。

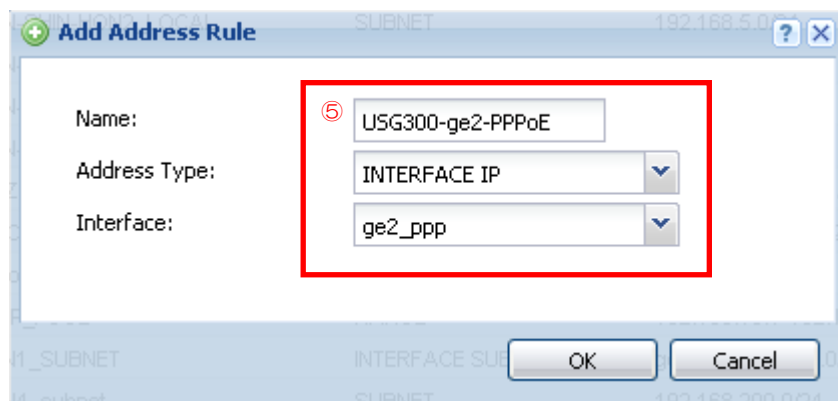
(1) Windows PC との接続で使用するユーザーアカウントの作成を行います。

- 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。

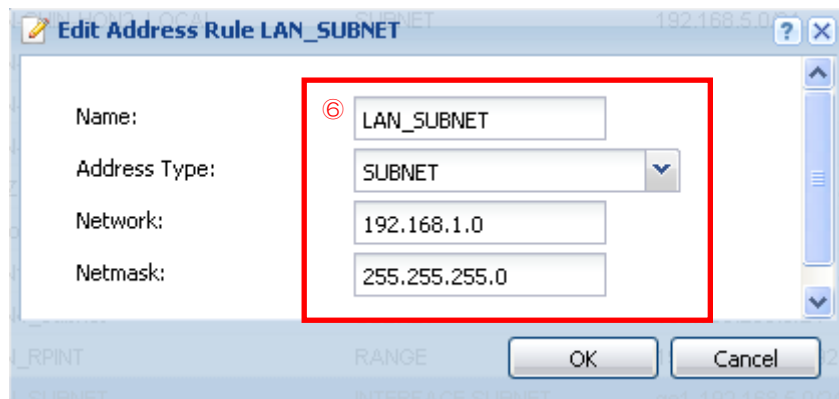


(2) 接続に使用するアドレスの設定を行います。

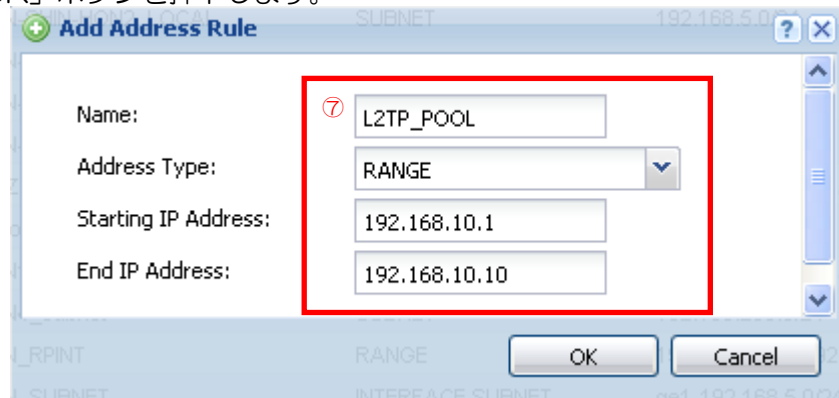
- ① 「CONFIGURATION」を選択します。
- ② 「Object」を選択します。
- ③ 「Address」を選択します。
- ④ 「Address」タブを選択します。
- ⑤ 「Add」をクリックし、WAN 側の IP アドレスオブジェクトを作成します。
 - (ア) 「Name」: 任意の名称を入力します。
 - (イ) 「Address Type」: 「INTERFACE IP」を選択します。
 - (ウ) 「Interface」: WAN インタフェースを選択します。
 - (エ) 「OK」ボタンを押下します。



- 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。

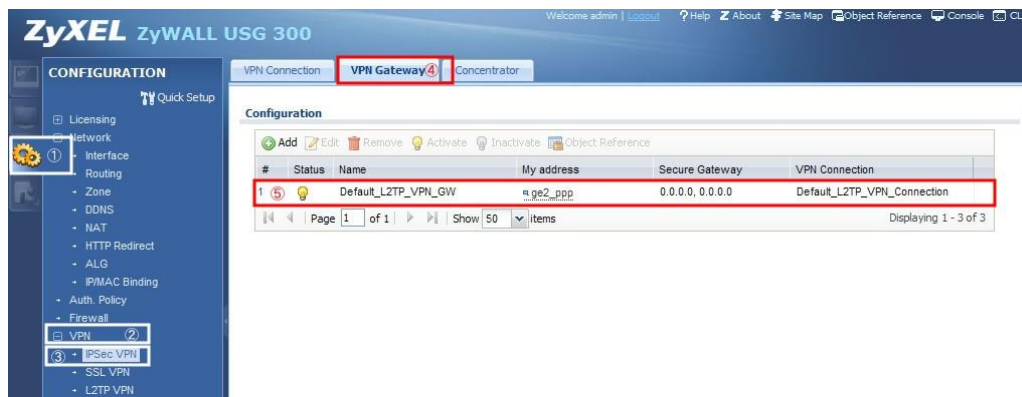


- ⑦ 「Add」をクリックし、IPSec で接続する機器に割り当てる IP アドレスオブジェクトを作成します。
- (ア) 「Name」に任意の名称を入力します。
 - (イ) 「Address Type」で「RANGE」を選択します。
 - (ウ) 「Starting IP Address」：本構成例では、192.168.10.1 と入力します。
 - (エ) 「End IP Address」：本構成例では、192.168.10.10 と入力します。
 - (オ) 「OK」ボタンを押下します。



(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

General Settings

☒ Enable

VPN Gateway Name:
Default_L2TP_VPN_GW

Gateway Settings

My Address

☒ Interface
ge2_ppp
Static -- 12.144.47.000/28 12.144.255.255

☐ 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
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: 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

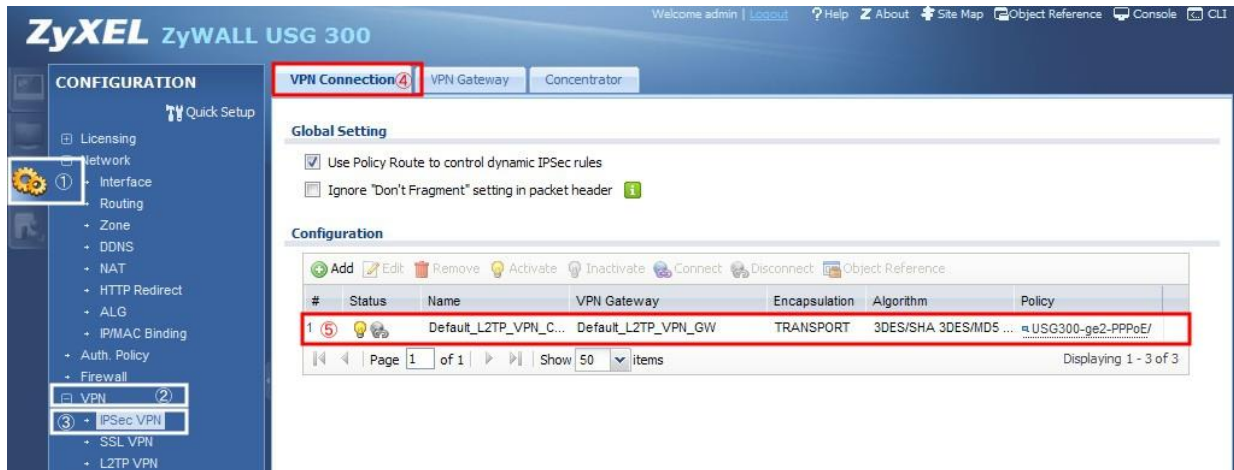
☐ Client Mode

User Name:
Password:

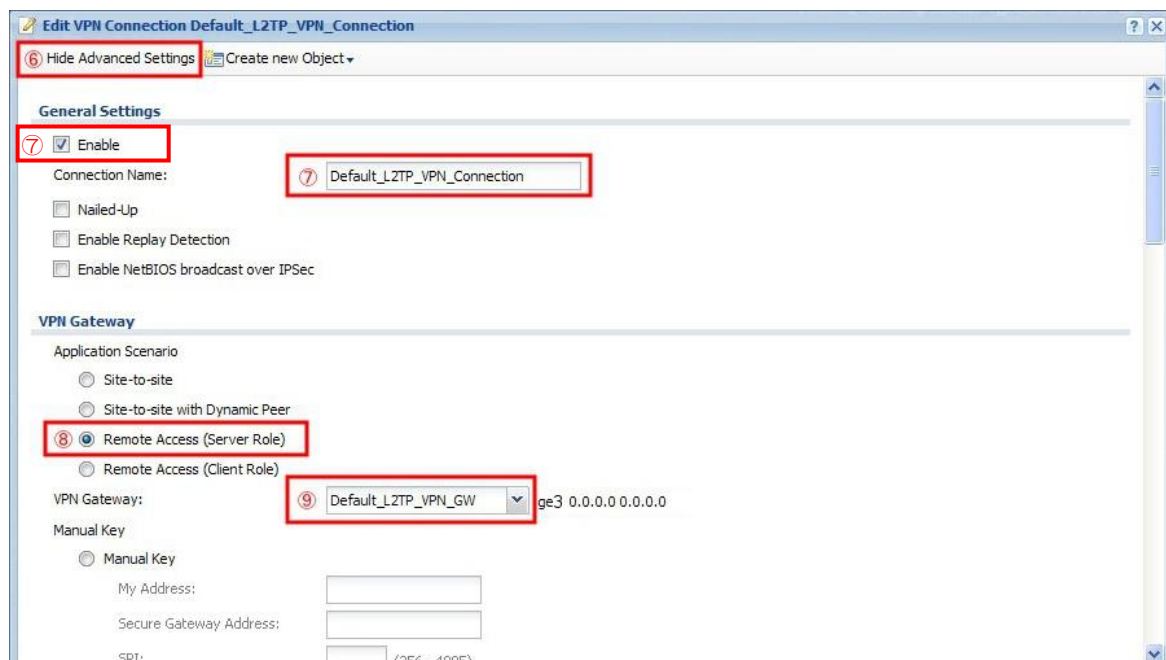
OK Cancel

(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。

Authentication Key:

Policy

Local policy: ⑪ USG300-ge2-PPPoE INTERFACE IP, 172.16.1.1

☐ Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ⑪ ESP

Encapsulation: Transport

Proposal

#	Encryption	Authentication
1	3DES	SHA1
2	3DES	MD5
3	DES	SHA1

Perfect Forward Secrecy (PFS): none

(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。

ZyXEL ZyWALL USG 300

Welcome admin | [Logout](#) | [Help](#) | [About](#) | [Site Map](#) | [Object Reference](#) | [Console](#) | [CLI](#)

CONFIGURATION

Quick Setup

Create new Object

L2TP VPN ④

General Settings

⑤ ☒ Enable L2TP Over IPsec

VPN Connection: ⑤ Default_L2TP_VPN_Connection

IP Address Pool: L2TP_POOL

Authentication Method: default

Allowed User: sample

Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

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。

Edit Policy Route Show Advanced Settings

Show Advanced Settings Create new Object

Configuration

⑥ ☒ Enable

Description: Windows_VPN_Route (Optional)

Criteria

User: any

Incoming: any (Excluding ZyWALL)

⑦ Source Address: LAN_SUBNET

Destination Address: L2TP_POOL

DSCP Code: any

Schedule: none

Service: any

Next-Hop

⑧ Type: VPN Tunnel

VPN Tunnel: Default_L2TP_VPN_Connecti

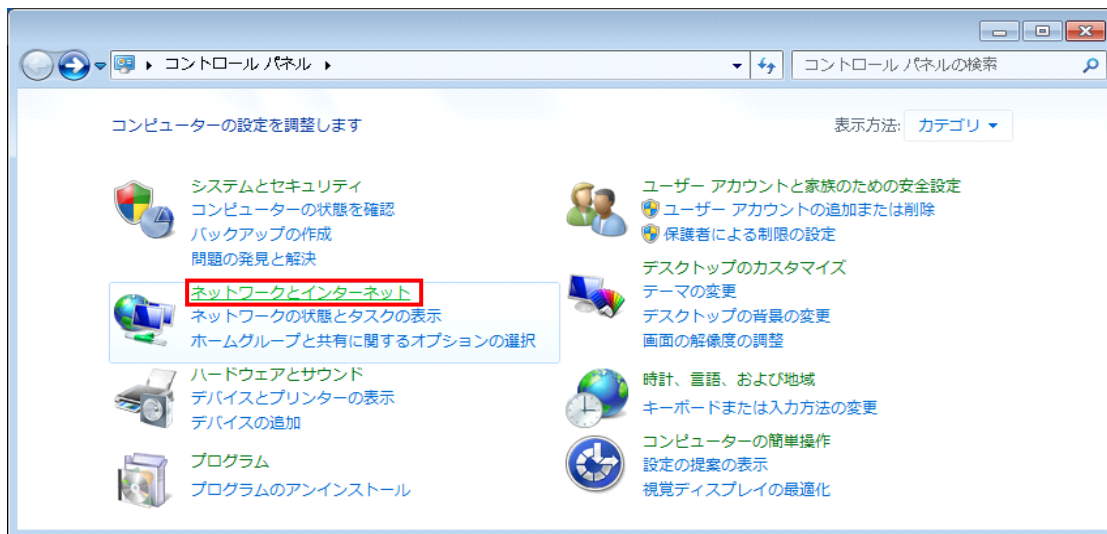
OK Cancel

2. Windows PC の設定

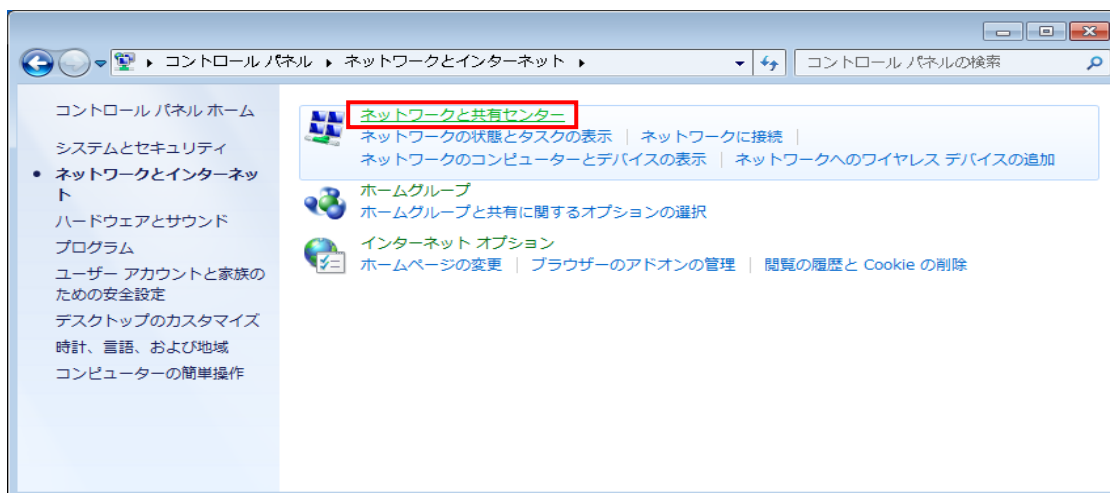
(1) Windows 側の VPN 設定を行います。

※操作方法については Windows 7 での設定例となります。その他の OS については読み替えて操作してください。

① コントロールパネルを開き、「ネットワークとインターネット」を選択します。



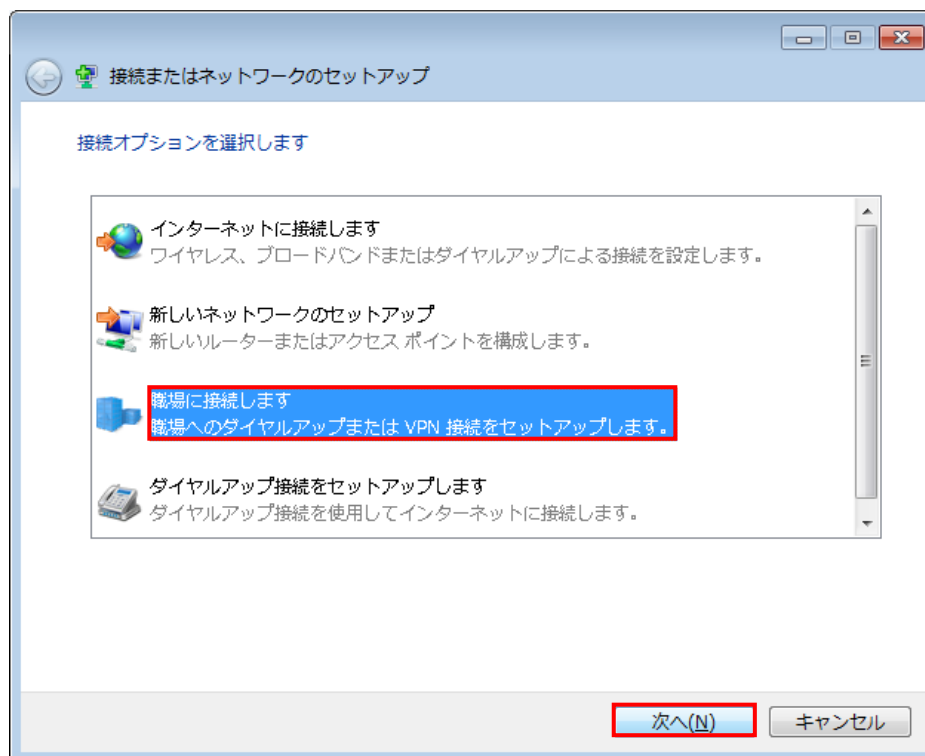
② 「ネットワークと共有センター」を選択します。



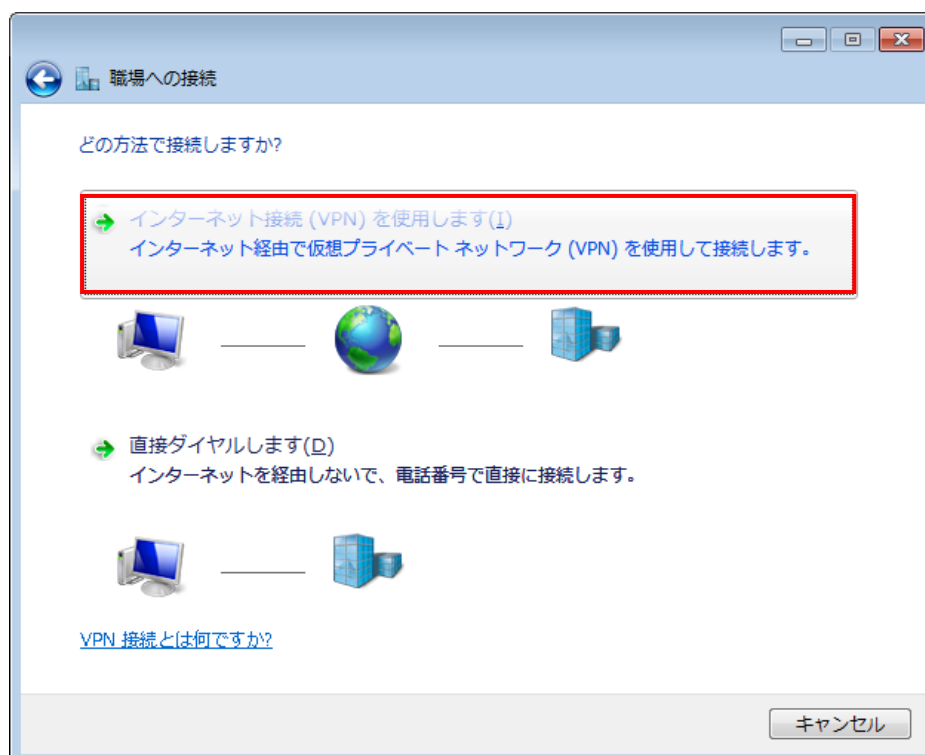
③ 「新しい接続またはネットワークのセットアップ」を選択します。



- ④ 「職場に接続します」を選択して、「次へ」を押下します。



- ⑤ 「インターネット接続 (VPN) を使用します」を選択します。



⑥ 以下の項目を設定後、「次へ」を押下します。

- ①インターネットアドレス：接続先のサーバ名または、IP アドレス
- ②接続先の名前：任意の名称
- ③「今は接続しない。自分が後で接続できるようにセットアップのみを行う」にチェックをします。

職場への接続

接続に使用するインターネット アドレスを入力してください

このアドレスは、ネットワーク管理者より受け取ることができます。

① インターネット アドレス(I): 61.xxx.yyy.9

② 接続先の名前(E): VPN 接続

☐ スマート カードを使用する(S)

☐ 他の人がこの接続を使うことを許可する(A)
このオプションによって、このコンピューターにアクセスがあるすべての人がこの接続を使えるようになります。

③ ☒ 今は接続しない。自分が後で接続できるようにセットアップのみを行う(D)

次へ(N) キャンセル

⑦ 以下の項目を設定後、「作成」を押下します。

- ①ユーザー名：1-(1)-⑤で入力した User Name
- ②パスワード：1-(1)-⑤で入力した Password

職場への接続

ユーザー名およびパスワードを入力してください

① ユーザー名(U): sample

② パスワード(P): ●●●●●●

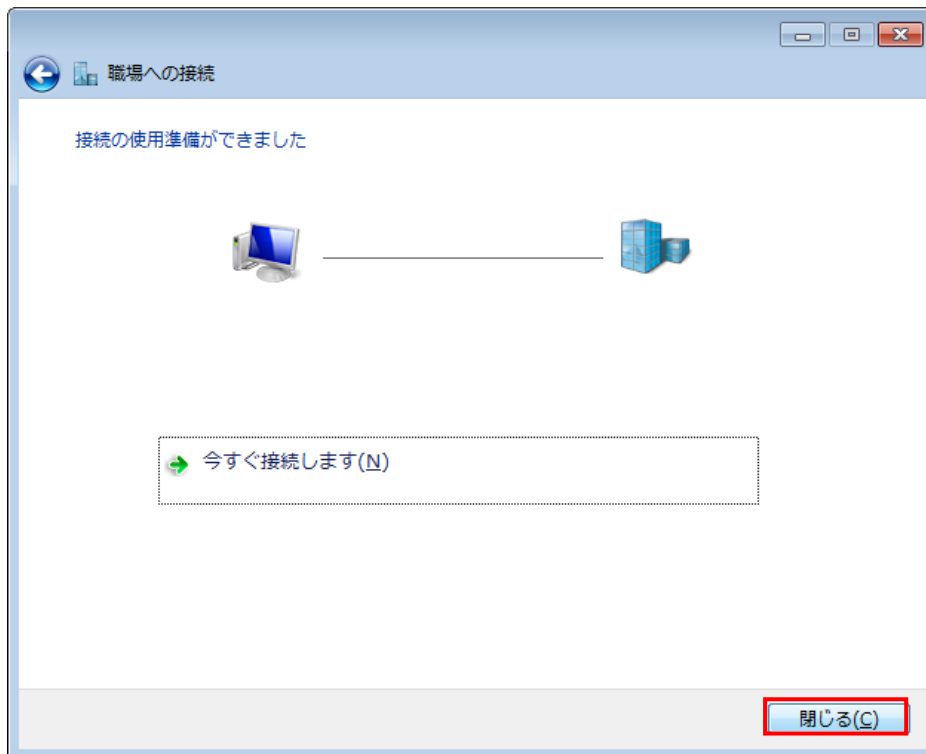
☐ パスワードの文字を表示する(S)

☐ このパスワードを記憶する(R)

ドメイン (オプション)(D):

作成(C) キャンセル

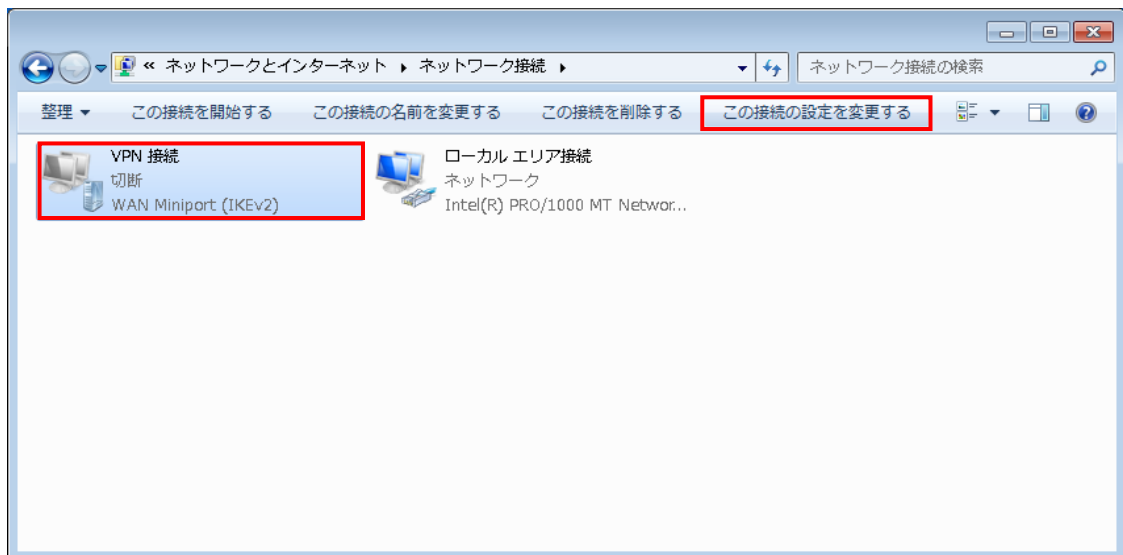
- ⑧ 「閉じる」を押下します。



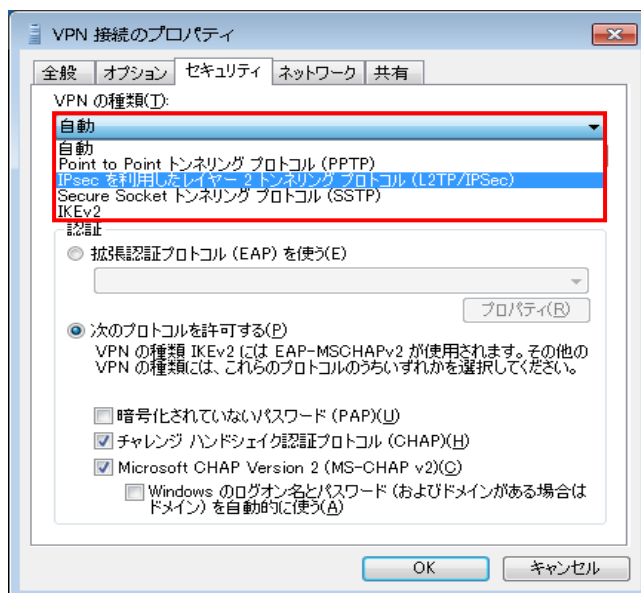
- ⑨ ネットワークと共有センターから「アダプターの設定の変更」を選択します。



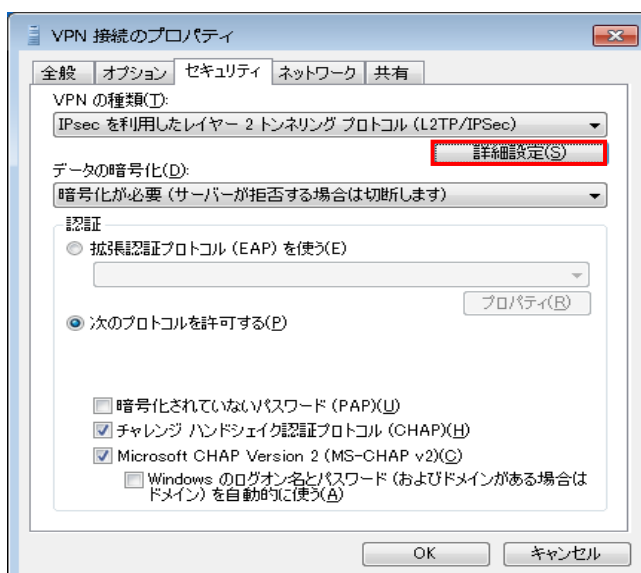
- ⑩ 「VPN接続」を選択して、「この接続の設定を変更する」を押下します。



- ⑪ セキュリティタブの「VPN の種類」で
「IPSec を利用したレイヤー 2 トンネリングプロトコル (L2TP/IPSec)」を選択します。

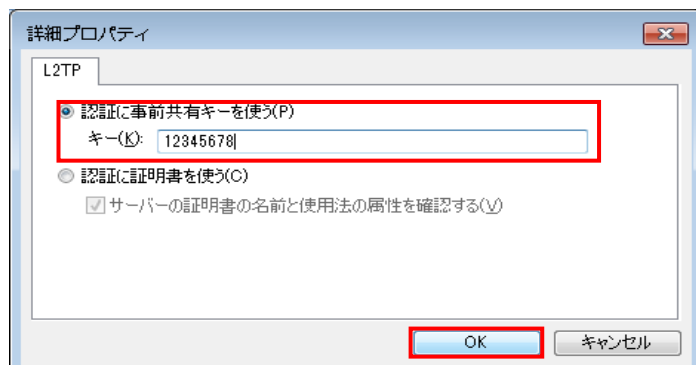


- ⑫ セキュリティタブの「詳細設定」を押下します。

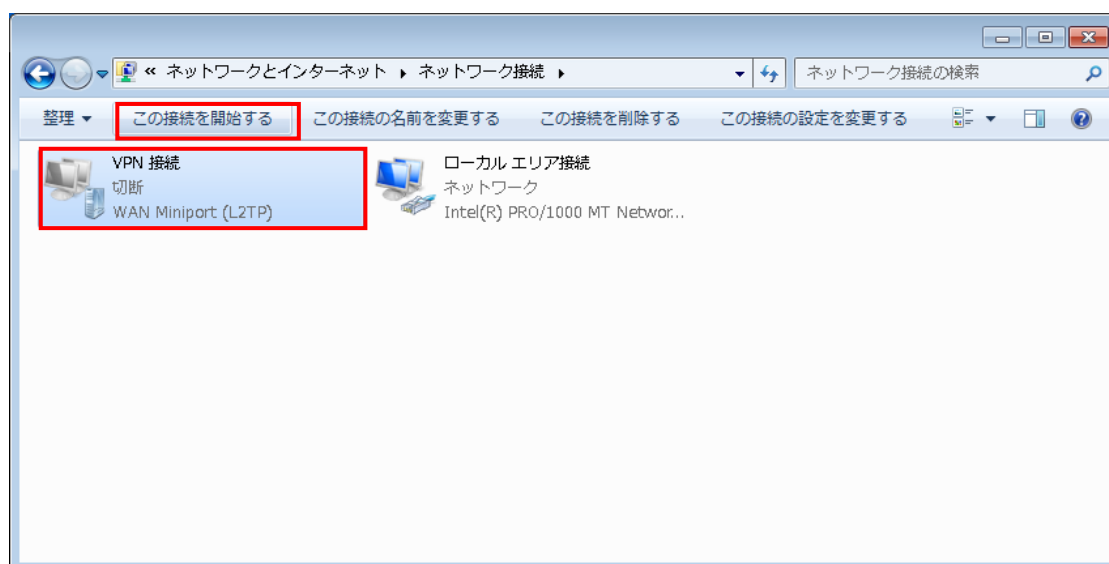


- ⑬ 「認証に事前共有キーを使う」を選択して、事前共有キーを入力後、「OK」を押下します。さらに VPN 接続のプロパティのウィンドウも「OK」を押下して閉じます。

・事前共有キー：1-(3)-⑨で入力した Pre-Shared Key



- ⑭ VPN接続を選択して、「この接続を開始する」を押下します。



- ⑮ ユーザー名とパスワードを入力して、「接続」を押下します。



(2) L2TP over IPsec VPN で接続されます。

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

2. 『Windows PC の設定』までの設定を行った時点では、Windows PC から LAN 内へのアクセスは可能ですが、Windows PC 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。
※Windows PC 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: ⑥ 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

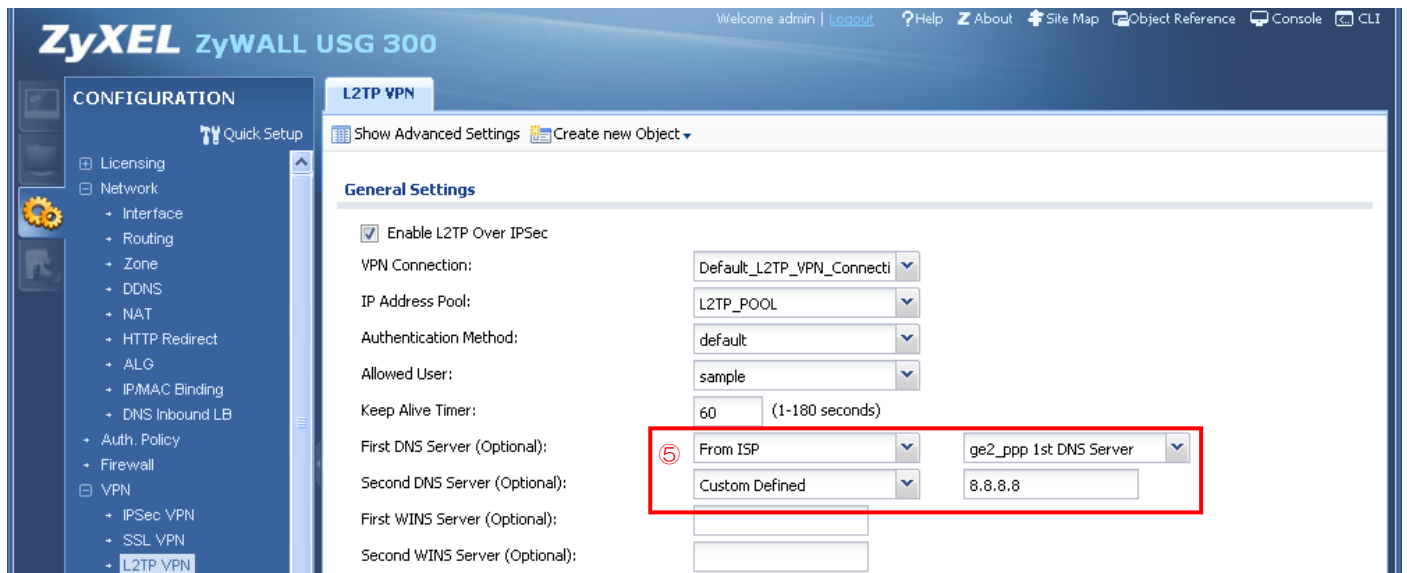
Type: ⑧ Trunk

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