

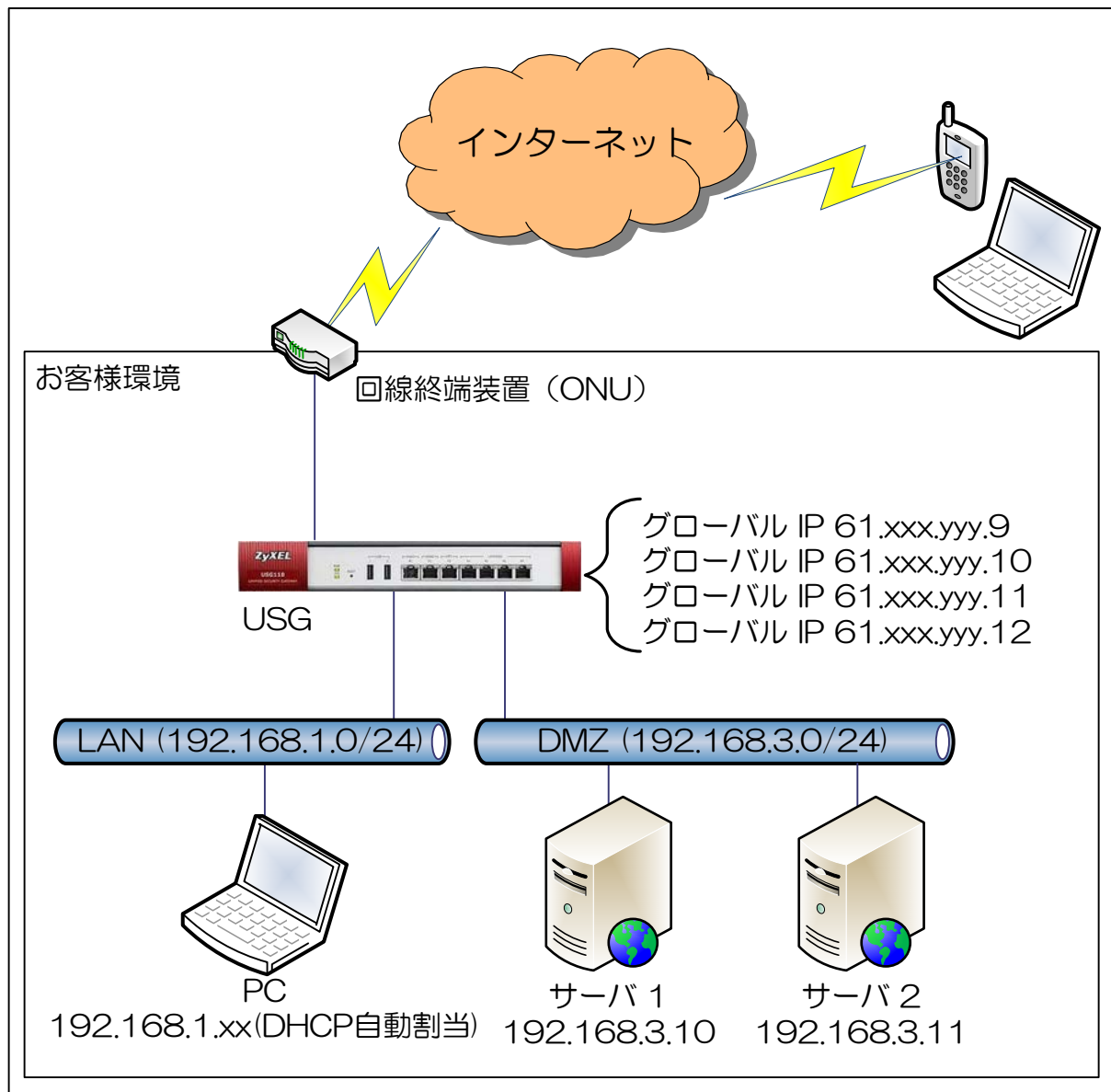
次世代ファイアウォール USG シリーズ設定例

「固定 IP アドレスサービス（複数固定 IP）を利用したサーバ構築」について

1. 使用環境

- (1) インターネット回線
フレッツ光、Bフレッツ、フレッツ ADSL といった NTT 回線 PPPoE での固定 IP サービス
 - (2) LAN IP アドレス：192.168.1.0/24 ※LAN1 初期設定のまま
 - (3) DMZ IP アドレス：192.168.3.0/24 ※DMZ 初期設定のまま
 - (4) DMZ にてグローバル IP に対応したサーバ公開
 - ① G-IP 61.xxx.yyy.9 ルータ本体（LAN1 からインターネット IP アドレス）
 - ② G-IP 61.xxx.yyy.10 DMZ-IP 192.168.3.10
 - ③ G-IP 61.xxx.yyy.11 DMZ-IP 192.168.3.11
 - ④ G-IP 61.xxx.yyy.12 DMZ-IP 192.168.3.12
- ※グローバル IP につきましては、お客様の回線契約書等で確認して下さい。

構成例：固定 IP アドレスサービスを利用した DMZ サーバ構築



2. インターネット接続設定

- (1) 初期状態より設定します。
- (2) 『クイックスタートガイド』を参照してインターネット接続設定を実施します。
 - ① Internet Access – First WAN Interface → ISP Parameters → Encapsulation に「PPP Over Ethernet」を選択します。
 - ② 「Next」ボタンを押下します。

Installation Setup Wizard

Internet Access > Internet Access Succeed > Device Registration

1 2 3

ISP Setting

I have two ISPs

Internet Access - First WAN Interface

ISP Parameters

Encapsulation: PPP Over Ethernet

IP Address Assignment

First WAN Interface: wan1_ppp

Zone: WAN

IP Address Assignment: Auto

< Back Next >

- ③ 「User Name」「Password」を入力します。
※ 「User Name」「Password」につきましては、お客様の回線契約書等で確認して下さい。
- ④ 「Nailed-Up」にチェックを入れます。
- ⑤ 「Next」ボタンを押下します。

Installation Setup Wizard

Internet Access > Internet Access Succeed > Device Registration

1 2 3

Internet Access - First WAN Interface

ISP Parameters

Encapsulation: PPPoE

Service Name: (Optional)

Authentication Type: Chap/PAP

User Name : XX@YYY.com

Password:

Retype to Confirm:

Nailed-Up

Idle timeout: 100 Seconds

IP Address Assignment

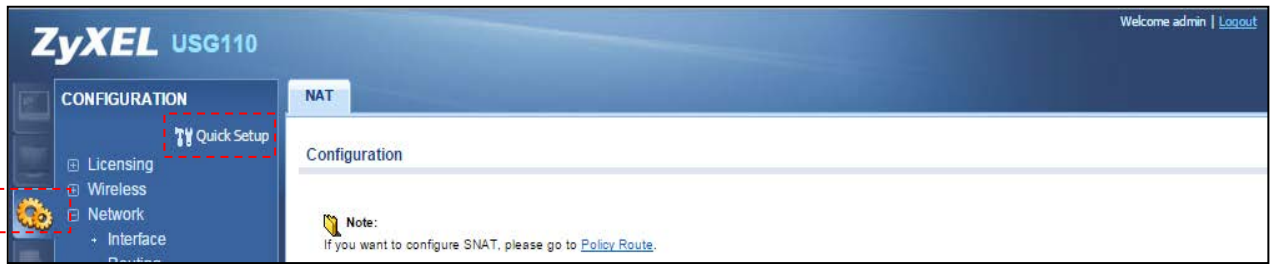
First WAN Interface: wan1_ppp

Zone: WAN

IP Address: Auto

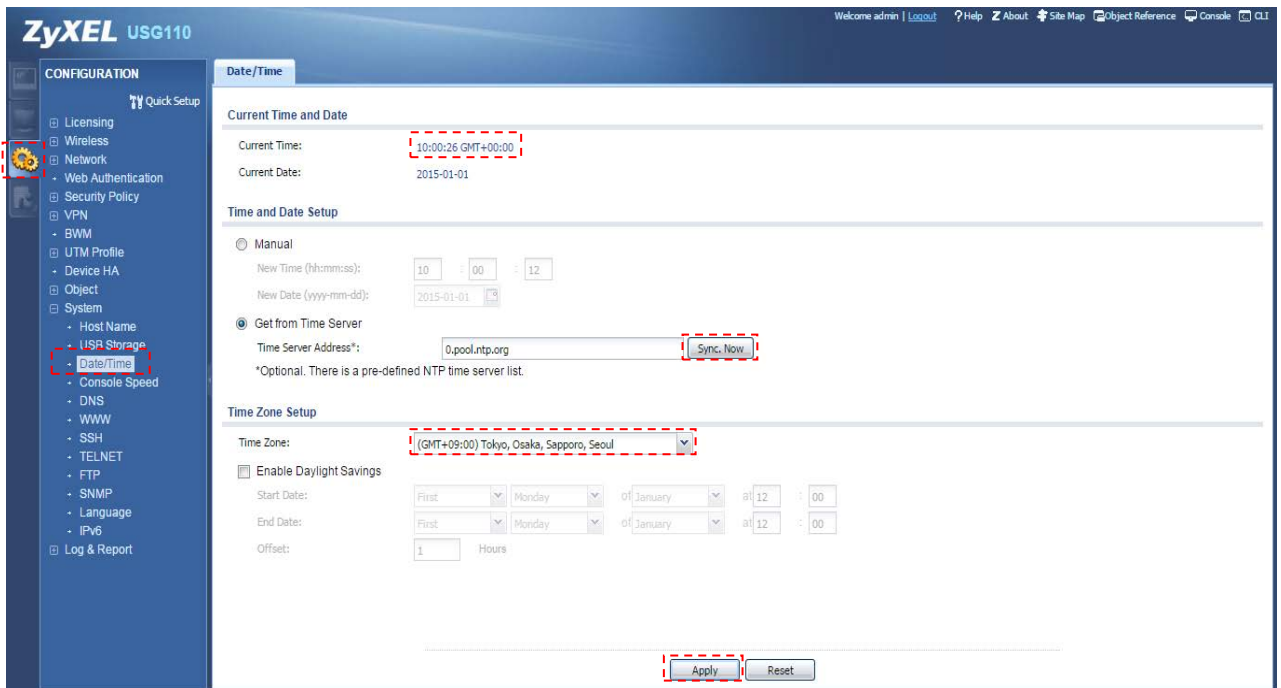
< Back Next >

※ウィザードが表示されない場合は CONFIGURATION の「Quick Setup」をクリックして下さい。



(3) Time Server 設定

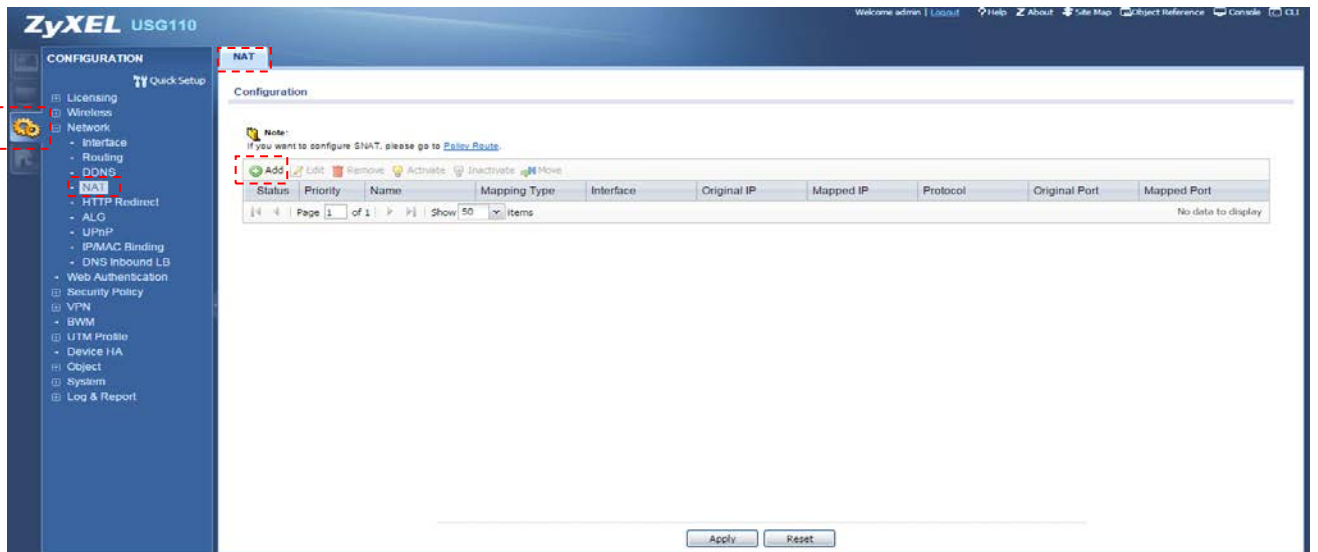
- ① 左メニューの CONFIGURATION -> System -> Date/Time を選択します。
- ② Time Zone Setup -> Time Zone にて(GMT+09:00)を選択します。
- ③ Time and Date Setup -> Get from Time Server の「Sync Now」ボタンを押下します。
- ④ Current Time and Date -> Current Time が GMT+09:00 になることを確認します。
- ⑤ 「Apply」ボタンを押下します。



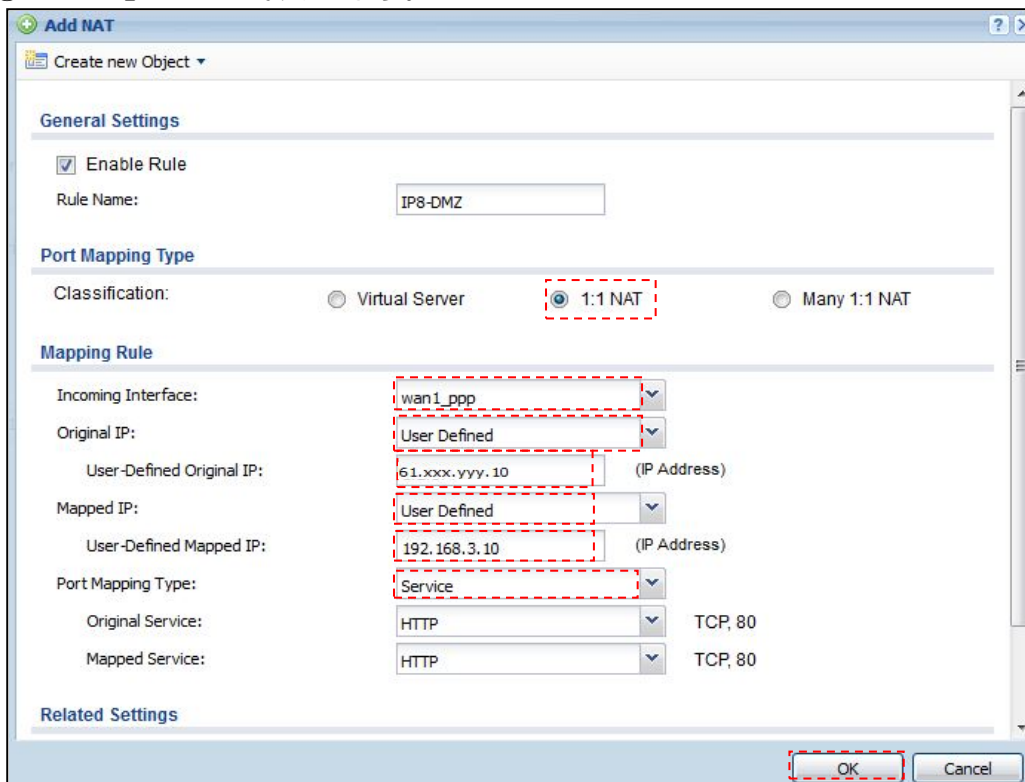
- (4) LAN1 からインターネット接続を確認します。
- (5) DMZ からインターネット接続を確認します。

3. NAT 設定

- (1) 左メニューの CONFIGURATION → Network → NAT を選択します。
- (2) 「Add」 ボタンを押下します。



- ① Port Mapping Type → Classification 「1:1 NAT」を設定します。
- ② Mapping Rule
 - Incoming Interface にて「wan1_ppp」を選択します。
 - Original IP にて「User Defined」を選択します。
 - User-Defined Original IP にて「61.xxx.yyy.10」を設定します。
 - Mapped IP にて「User Defined」を選択します。
 - User-Defined Original IP にて「192.168.3.10」を設定します。
 - Port Mapping Type にて任意の値を選択します。
- ③ 「OK」ボタンを押下します。



- ④ 必要に応じて他の G-IP についても同様に DMZ の IP アドレスの設定の追加を行います。

4. Firewall ルール追加

- (1) 左メニューの CONFIGURATION -> Security Policy-> Policy Control を選択します。
- (2) 「Add」 ボタンを押下します。

The screenshot shows the ZyXEL USG110 web interface. The left sidebar contains a 'CONFIGURATION' menu with 'Security Policy' > 'Policy Control' selected. The main content area is titled 'Policy' and shows 'General Settings' with 'Enable Policy Control' checked. Below is the 'IPv4 Configuration' section with 'Allow Asymmetrical Route' checked. A table lists existing policies, and an 'Add' button is highlighted with a red dashed box. The table has the following columns: Prior..., Status, Name, From, To, IPv4 Source, IPv4 Destinat..., Service, User, Schedule, Action, Log, UTM Profile.

Prior...	Status	Name	From	To	IPv4 Source	IPv4 Destinat...	Service	User	Schedule	Action	Log	UTM Profile
1	🔔	LAN1_Outgo...	LAN1	any (Excludi...	any	any	any	any	none	allow	no	
2	🔔	LAN2_Outgo...	LAN2	any (Excludi...	any	any	any	any	none	allow	no	
3	🔔	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no	
4	🔔	IPSec_VPN...	IPSec_VPN	any (Excludi...	any	any	any	any	none	allow	no	
5	🔔	SSL_VPN_O...	SSL_VPN	any (Excludi...	any	any	any	any	none	allow	no	
6	🔔	TUNNEL_Ou...	TUNNEL	any (Excludi...	any	any	any	any	none	allow	no	
7	🔔	LAN1_to_De...	LAN1	ZyWALL	any	any	any	any	none	allow	no	
8	🔔	LAN2_to_De...	LAN2	ZyWALL	any	any	any	any	none	allow	no	
9	🔔	DMZ_to_De...	DMZ	ZyWALL	any	any	Default_All...	any	none	allow	no	
10	🔔	WAN_to_De...	WAN	ZyWALL	any	any	Default_All...	any	none	allow	no	
11	🔔	IPSec_VPN...	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no	
12	🔔	SSL_VPN_to...	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no	
13	🔔	TUNNEL_to...	TUNNEL	ZyWALL	any	any	any	any	none	allow	no	
Def..			any	any	any	any	any	any	none	deny	log	

- ① Name に任意のルール名を入力します。
- ② From に「WAN」を選択します。
- ③ To に「DMZ」を選択します。
- ④ Destination に「DMZ_SUBNET」を選択します。
- ⑤ Service には任意の値を選択します。
- ⑥ Action を「allow」に設定します。
- ⑦ 「OK」ボタンを押下します。

Add corresponding

Create new Object ▾

Enable

Name: WAN_DMZ

Description: toDMZ_HTTP (Optional)

From: WAN ▾

To: DMZ ▾

Source: any ▾

Destination: DMZ_SUBNET ▾

Service: HTTP ▾

User: any ▾

Schedule: none ▾

Action: allow ▾

Log matched traffic: no ▾

OK Cancel

※Firewallにて許可するプロトコルは必要に応じて最小限に設定して下さい。

以上になります。