

PPPoE による LAN 型インターネット接続（スタティック NAT によるサーバー公開）

PPPoE を使ってインターネットサービスプロバイダー（以下 ISP）に接続します。グローバルアドレスを 8 個、16 個などのブロック単位で固定的に割り当てられる LAN 型接続の設定例です。この例では、ISP から割り当てられたアドレスをルーターやホストに直接割り当てず、LAN 側コンピューターはプライベートアドレスで運用します。クライアントはダイナミック ENAT 経由でインターネットにアクセスさせます。また、ファイアウォールを使って外部からのアクセスを原則拒否しつつ、スタティック NAT を使って特定のサーバーだけを外部に公開します。

ISP からは次の情報を提供されているものとします。

表 1：ISP から提供された情報

| | |
|---------------|------------------------------|
| PPP ユーザー名 | user@isp |
| PPP パスワード | isppasswd |
| PPPoE サービス名 | 指定なし |
| 使用できる IP アドレス | 4.4.4.0/29 (4.4.4.0～4.4.4.7) |
| DNS サーバー | 自動取得（端末に設定） |

ルーターには、次のような方針で設定を行います。

- LAN 側はすべてプライベートアドレスで運用します。LAN 側のクライアントがインターネットにアクセスできるよう、ダイナミック ENAT を使用します。グローバルアドレスには、4.4.4.1 を使います。
- LAN 側のサーバーにもプライベートアドレスを割り当てますが、外部からアクセスさせるため、スタティック NAT を使って外からはグローバルアドレスを持っているように見せかけます。変換ルールは次のとおりとします。
 - Web サーバー：192.168.10.2 4.4.4.2
 - SMTP サーバー：192.168.10.3 4.4.4.3
 - DNS サーバー：192.168.10.4 4.4.4.4

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。
- 外部からのアクセスは基本的にすべて遮断しますが、スタティック NAT で公開している Web サーバー（4.4.4.2 の TCP80 番）、SMTP サーバー（4.4.4.3 の TCP25 番）、DNS サーバー（4.4.4.4 の TCP/UDP53 番）へのアクセスだけは特例として許可します。

以下、ルーターの基本設定についてまとめます。

表 2：ルーターの基本設定

| | |
|---------------------|-----------------|
| WAN 側物理インターフェース | WAN |
| WAN 側（ppp0）IP アドレス | Unnumbered |
| LAN 側（vlan1）IP アドレス | 192.168.10.1/24 |
| DHCP サーバー機能 | 使わない |
| DNS リレー機能 | 使わない |

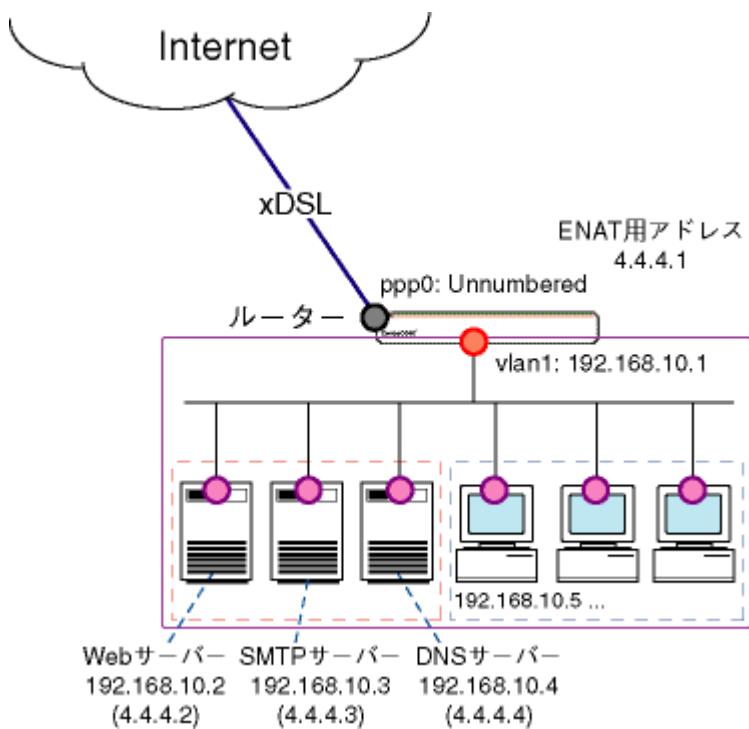


図 1 ネットワーク構成図

ルーターの設定

1.メニューから「LAN」 「LAN」の順にクリックし、LAN側 IP アドレスの設定を行います。

| LAN側IP設定 | |
|--|--|
| IPアドレス | <input type="text" value="192.168.10.1"/> |
| サブネットマスク | <input type="text" value="255.255.255.0"/> |
| <input type="button" value="適用"/> <input type="button" value="ヘルプ"/> | |

以下のメッセージが表示されますので、「OK」ボタンをクリックします。端末の IP アドレスを 192.168.10.100 など変更後のアドレスにあわせて設定し、変更後の AR260S の IP アドレス (192.168.10.1) に接続し直して下さい。



2.メニューから「WAN」 「WAN」の順にクリックします。セッション ID : PPPoE0 を選択し、インターネット接続の設定を行います。

WAN 側 IP はグローバル IP を 8 個取得する Unnumbered 接続となりますが、スタティック NAT を使用する場合は、「Unnumbered PPPoE」は「無効」にします。

| WAN設定 | |
|--|--|
| 接続モード | PPPoE |
| セッションID | PPPoE.0 <input type="button" value="接続"/> |
| デフォルトゲートウェイ | PPPoE.0 |
| Unnumbered PPPoE | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| ホスト名 | AR260S (オプション) |
| ユーザー名 | user@isp |
| パスワード | ***** |
| サービス名 | (オプション) |
| AC(アクセスコンセントレーター)名 | (オプション) |
| DNSオプション | <input type="radio"/> 固定設定 <input checked="" type="radio"/> 自動取得 |
| プライマリDNSサーバー | (オプション) |
| セカンダリDNSサーバー | (オプション) |
| MSSクランプ | <input type="radio"/> 無効 <input checked="" type="radio"/> 有効 MSSの値 40 Bytes |
| 接続オプション | <input type="radio"/> ダイヤルオンデマンド <input checked="" type="radio"/> キーブアライブ <input type="radio"/> 無効 エコー送信間隔 60 秒 |
| <input type="button" value="適用"/> <input type="button" value="ヘルプ"/> | |

3.メニューから「ファイアウォール」 「ポリシーリスト」 「NAT プール」の順にクリックし、スタティック NAT の設定を行います。

3-1. 192.168.10.2 は、4.4.4.2 へスタティック NAT を行う「NAT プール」を作成します。

| NATプール設定 | | |
|--|--------------|--------------|
| <input type="button" value="プールの新規追加"/> | | |
| プール名 | WebServer | |
| プールタイプ | スタティックNAT | |
| 変換前のIPアドレス | 始点IPアドレス | 192.168.10.2 |
| | 終点IPアドレス | 192.168.10.2 |
| NAT IPアドレス | 始点NAT IPアドレス | 4.4.4.2 |
| | 終点NAT IPアドレス | 4.4.4.2 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | | |

3-2. 192.168.10.3 は、4.4.4.3 ヘスタティック NAT を行う「NAT プール」を作成します。

| NATプール設定 | | |
|--|--------------|--------------|
| プールの新規追加 ▼ | | |
| プール名 | SMTP_Server | |
| プールタイプ | スタティックNAT ▼ | |
| 変換前のIPアドレス | 始点IPアドレス | 192.168.10.3 |
| | 終点IPアドレス | 192.168.10.3 |
| NAT IPアドレス | 始点NAT IPアドレス | 4.4.4.3 |
| | 終点NAT IPアドレス | 4.4.4.3 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | | |









3-3. 192.168.10.4 は、4.4.4.4 ヘスタティック NAT を行う「NAT プール」を作成します。

| NATプール設定 | | |
|--|--------------|--------------|
| プールの新規追加 ▼ | | |
| プール名 | DNS_Server | |
| プールタイプ | スタティックNAT ▼ | |
| 変換前のIPアドレス | 始点IPアドレス | 192.168.10.4 |
| | 終点IPアドレス | 192.168.10.4 |
| NAT IPアドレス | 始点NAT IPアドレス | 4.4.4.4 |
| | 終点NAT IPアドレス | 4.4.4.4 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | | |

3-4. ダイナミック ENAT を行う「NAT プール」を作成します。LAN 側のプライベート IP アドレスを、ISP から与えられたグローバル IP アドレス 4.4.4.1 に変換する「NAT プール」を作成します。

| NATプール設定 | |
|--|---------|
| プールの新規追加 ▼ | |
| プール名 | ENAT |
| プールタイプ | ENAT ▼ |
| NAT IPアドレス | 4.4.4.1 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

3-1 から 3-4 まで終了すると、「NAT プールリスト」は以下のように表示されます。

| NATプールリスト | | | | | | |
|---|---|-------------|---------------|----------|--------------------------------|-------------------|
| | プール名 | NATタイプ | NAT IPアドレス | インターフェース | 範囲指定 | NAT範囲指定 |
|  |  | WebServer | スタティック NAT | | 192.168.10.2 - 192.168.10.2 | 4.4.4.2 - 4.4.4.2 |
|  |  | SMTP_Server | スタティック NAT | | 192.168.10.3 - 192.168.10.3 | 4.4.4.3 - 4.4.4.3 |
|  |  | DNS_Server | スタティック NAT | | 192.168.10.4 - 192.168.10.4 | 4.4.4.4 - 4.4.4.4 |
|  |  | ENAT | ENAT | 4.4.4.1 | | |

4.メニューから「ファイアウォール」「Outboundアクセス」の順にクリックします。Outboundアクセス設定では、内部から外部へ出る場合の設定を行います。

4-1. 192.168.10.2 は、4.4.4.2へスタティック NAT を行うように設定します。

| Outboundアクセス制御設定 | |
|--|--|
| ID | 新規追加 |
| アクション | 通過 |
| 優先度 | 1 |
| 送信元 | タイプ IPアドレス IPアドレス 192.168.10.2 |
| 宛先 | タイプ 全て |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ 全て |
| プロトコル | 全て |
| NAT | NATプール プール WebServer |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

4-2. 192.168.10.3 は、4.4.4.3へスタティック NATを行うように設定します。

| Outboundアクセス制御設定 | |
|--|--|
| ID | 新規追加 |
| アクション | 通過 |
| 優先度 | 1 |
| 送信元 | タイプ IPアドレス IPアドレス 192.168.10.3 |
| 宛先 | タイプ 全て |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ 全て |
| プロトコル | 全て |
| NAT | NATプール プール SMTP_Server |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

4-3. 192.168.10.4 は、4.4.4.4へスタティックNATを行うように設定します。

| Outboundアクセス制御設定 | |
|--|--|
| ID | 新規追加 |
| アクション | 通過 |
| 優先度 | 1 |
| 送信元 | タイプ IPアドレス IPアドレス 192.168.10.4 |
| 宛先 | タイプ 全て |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ 全て |
| プロトコル | 全て |
| NAT | NATプール プール DNS_Server |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

4-4. スタティックNATに該当しない端末は、ENATを行うように設定します。ENATの設定は、スタティックNATの設定より優先度を低くする必要があります。

デフォルトでインターフェースNATを使用する設定が入っておりますので、PPPoE0を使用するインターフェースNATの設定から、ENATを使用する設定に変更してください。

| Outboundアクセス制御設定 | |
|--|--|
| ID | 4 |
| アクション | 通過 |
| 優先度 | 4 |
| 送信元 | タイプ 全て |
| 宛先 | タイプ 全て |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ 全て |
| プロトコル | 全て |
| NAT | NATプール プール ENAT |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

| Outboundアクセス制御リスト | | | | | |
|-------------------|--------------|----|----------|-------------|-------|
| ID | 送信元 | 宛先 | プロトコル | NAT | アクション |
| 1 | 192.168.10.4 | 全て | 全て,全て,全て | DNS_Server | 通過 |
| 2 | 192.168.10.3 | 全て | 全て,全て,全て | SMTP_Server | 通過 |
| 3 | 192.168.10.2 | 全て | 全て,全て,全て | WebServer | 通過 |
| 4 | 全て | 全て | 全て,全て,全て | ENAT | 通過 |

ENATと併用する場合、スタティックNATの優先度(IDが優先度を表しています)をENATより高く(小さい値)設定してください。優先度の順番を間違えるとサーバー公開できない問題が発生してしまいます。

5.メニューから「ファイアウォール」「inboundアクセス」の順にクリックします。Inboundアクセス制御設定では外部から内部へのアクセスに関する設定を行います。ここでは、サーバー公開の設定を行います。

5-1.インターネット側から「4.4.4.2」のTCP/80番宛の通信は「192.168.10.2」に転送する設定を行います。ここではサービスで指定していますが、ポート番号での指定も可能です。

| Inboundアクセス制御設定 | |
|--|--|
| ID | 1 |
| アクション | 通過 |
| 優先度 | 1 |
| 送信元 | タイプ 全て |
| 宛先 | タイプ IPアドレス IPアドレス 4.4.4.2 |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ サービス サービス HTTP |
| NAT | IPアドレス IPアドレス 192.168.10.2 |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

5-2.インターネット側から「4.4.4.3」のTCP/25番宛の通信は「192.168.10.3」に転送する設定を行います。ここではサービスで指定していますが、ポート番号での指定も可能です。

| Inboundアクセス制御設定 | |
|--|--|
| ID | 新規追加 |
| アクション | 通過 |
| 優先度 | 1 |
| 送信元 | タイプ 全て |
| 宛先 | タイプ IPアドレス IPアドレス 4.4.4.3 |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ サービス サービス SMTP |
| NAT | IPアドレス IPアドレス 192.168.10.3 |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

5-3. インターネット側から「4.4.4.4」のTCP/53番宛の通信は「192.168.10.4」に転送する設定を行います。DNSは、AR260Sのサービスリストに設定されていないため、ポート番号で指定します。（サービスリストに新規追加し、サービスで指定することも可能です。）

| Inboundアクセス制御設定 | |
|--|--|
| ID | 新規追加 |
| アクション | 通過 |
| 優先度 | 1 |
| 送信元 | タイプ 全て |
| 宛先 | タイプ IPアドレス IPアドレス 4.4.4.4 |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ ポート指定 ポート番号 53 |
| プロトコル | TCP |
| NAT | IPアドレス IPアドレス 192.168.10.4 |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

5-4. インターネット側から「4.4.4.4」のUDP/53番宛の通信は「192.168.10.4」に転送する設定を行います。DNSは、AR260Sのサービスリストに設定されていないため、ポート番号で指定します。（サービスリストに新規追加し、サービスで指定することも可能です。）

| Inboundアクセス制御設定 | |
|--|--|
| ID | 新規追加 |
| アクション | 通過 |
| 優先度 | 1 |
| 送信元 | タイプ 全て |
| 宛先 | タイプ IPアドレス IPアドレス 4.4.4.4 |
| 送信元ポート | タイプ 全て |
| 宛先ポート | タイプ ポート指定 ポート番号 53 |
| プロトコル | UDP |
| NAT | IPアドレス IPアドレス 192.168.10.4 |
| ログ | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| <input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="削除"/> <input type="button" value="ヘルプ"/> | |

5-1 から 5-4 まで終了すると、「Inbound アクセス制御リスト」は以下のように表示されます。

| Inboundアクセス制御リスト | | | | | | |
|------------------|-----|---------|--------------|--------------|-------|--|
| ID | 送信元 | 宛先 | プロトコル | NAT | アクション | |
| 1 | 全て | 4.4.4.4 | UDP,全て,53 | 192.168.10.4 | 通過 | |
| 2 | 全て | 4.4.4.4 | TCP,全て,53 | 192.168.10.4 | 通過 | |
| 3 | 全て | 4.4.4.3 | SMTP(TCP,25) | 192.168.10.3 | 通過 | |
| 4 | 全て | 4.4.4.2 | HTTP(TCP,80) | 192.168.10.2 | 通過 | |

6.メニューから「システム管理」 「サービスの有効/無効」の順にクリックします。「ファイアウォール」を有効にします。(デフォルトで有効になっております。)

| サービスの有効/無効 | |
|----------------|--|
| ファイアウォール | <input checked="" type="radio"/> 有効 <input type="radio"/> 無効 |
| VPN | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| DNSリレー | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| DHCP | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| SNTP | <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 |
| リセットスイッチによる初期化 | <input checked="" type="radio"/> 有効 <input type="radio"/> 無効 |

メモ

1.メニューから「ファイアウォール」 「統計情報」の順にクリックします。ファイアウォールの接続情報を確認することができます。以下の情報では、internet 側 (WAN 側) からのアクセスに関する情報が出力されていることが確認できます。

| Active Connections | | | | | | | |
|--------------------|----------|------------------------|---------------------|-------------------|-------------|-----------|----------|
| Source Network | Protocol | Source IP-Port | Destination IP-Port | NAT IP-Port | Life (Secs) | Bytes Out | Bytes In |
| LAN | TCP | 192.168.10.100 - 1387 | 192.168.10.1 - 80 | 0.0.0.0 - 0 | 20 | 0 | 0 |
| LAN | TCP | 192.168.10.100 - 1385 | 192.168.10.1 - 80 | 0.0.0.0 - 0 | 20 | 0 | 0 |
| LAN | TCP | 192.168.10.100 - 1386 | 192.168.10.1 - 80 | 0.0.0.0 - 0 | 20 | 0 | 0 |
| LAN | TCP | 192.168.10.100 - 1388 | 192.168.10.1 - 80 | 0.0.0.0 - 0 | 600 | 0 | 0 |
| LAN | UDP | 192.168.10.100 - 1052 | 192.168.10.1 - 53 | 0.0.0.0 - 0 | 48 | 0 | 0 |
| Internet | TCP | 200.200.200.100 - 1364 | 4.4.4.2 - 80 | 192.168.10.2 - 80 | 528 | 45110 | 2554 |
| Internet | TCP | 200.200.200.100 - 1360 | 4.4.4.2 - 80 | 192.168.10.2 - 80 | 420 | 0 | 0 |
| Internet | TCP | 200.200.200.100 - 1363 | 4.4.4.2 - 80 | 192.168.10.2 - 80 | 516 | 65504 | 3257 |

| Total Connections Count | | | |
|-------------------------|-----|------|--------|
| TCP | UDP | ICMP | Others |
| 7 | 1 | 0 | 0 |

更新日 2005年06月08日