

PPPoE マルチセッションによる端末型インターネット接続 + CUG サービス接続(端末型)

PPPoE セッションを 2 本使い、インターネットサービスプロバイダ(以下 ISP)への接続と CUG(Closed Users Group)サービス(NTT 東日本のフレッツ・グループアクセス(ライト)および NTT 西日本のフレッツ・グループ(ベーシックメニュー))の「端末型払い出し」を同時に利用します。CUG サービス網を介してルーター間に IPsec(ESP)トンネルを構築します。パケットの振り分けはスタティックな経路制御により行います。また、各拠点からのインターネット向け通信も可能とします。

ISP からは、次の情報が提供されているものとします。

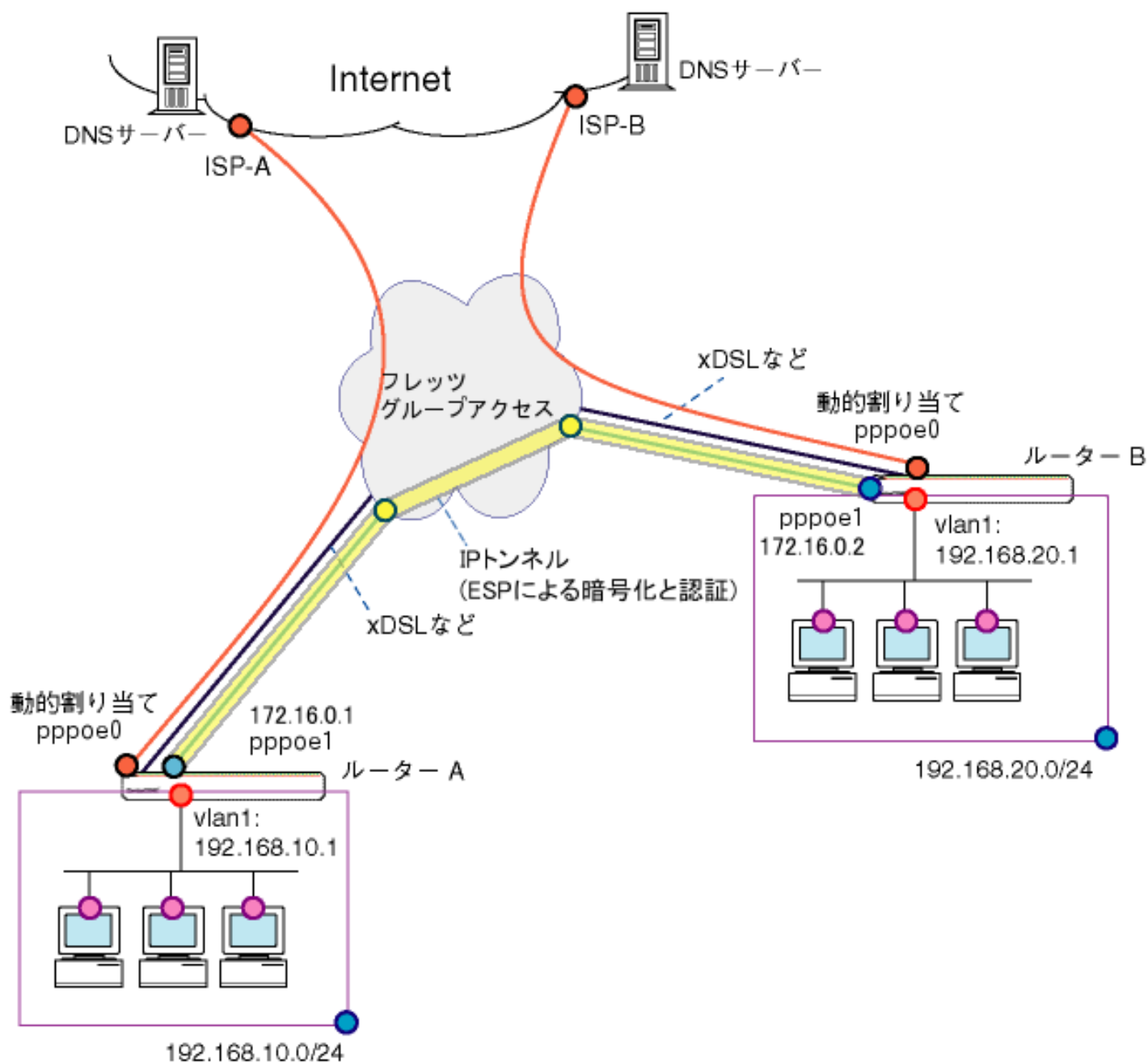
	ルーターA	ルーターB
PPP ユーザー名	user1@example	user2@example
PPP パスワード	password	password
IP アドレス	グローバルアドレス 1 個 (動的割り当て)	グローバルアドレス 1 個 (動的割り当て)
DNS サーバー	接続時に通知される	接続時に通知される

CUG サービスからは、次の情報が提供されているものとします。

	ルーターA	ルーターB
ユーザーID (PPP ユーザー名)	router1	router2
パスワード (PPP パスワード)	password	password
IP アドレス	172.16.0.1/32	172.16.0.2/32

各ルーターは以下のように設定するものとします。

	ルーターA	ルーターB
WAN 側 IP アドレス	自動取得 (172.16.0.1/32 を取得)	自動取得 (172.16.0.2/32 を取得)
LAN 側 IP アドレス	192.168.10.1/24	192.168.20.1/24
VPN 接続設定		
ローカルセキュアグループ ～リモートセキュアグループ	192.168.10.0/24 ～192.168.20.0/24	192.168.20.0/24 ～192.168.10.0/24
ローカルゲートウェイ	pppoe0	pppoe0
リモートゲートウェイ	172.16.0.2	172.16.0.1
IKE 設定		
交換モード	メイン	メイン
事前共有鍵	secret	secret
暗号化認証アルゴリズム	3DES & SHA1-DH2	3DES & SHA1-DH2
IPsec 設定		
暗号化認証アルゴリズム	ESP 3DES HMAC SHA1	ESP 3DES HMAC SHA1
PFS グループ	なし	なし



本構成における設定のポイントは、次の通りです。

- スタティックルーティングにより、グループ内の他ユーザー宛パケット(対向ルータの LAN 側宛)と、それ以外のインターネット宛パケットの転送先を振り分けます。
- CUGサービス網上に IPsec (ESP) トンネルを構築し、拠点間の複数クライアント間通信を実現します。

※ 本設定例は ルーターAへの設定内容を想定しています。ルーターBの設定を行う場合は

※ 文中の「ルーターBは～」をご参照ください。

<手順1>

IP アドレスを自動取得するよう設定したPCを接続し、Webブラウザを起動します。
Web ブラウザから「<http://192.168.1.1/>」を開くとユーザー名、パスワードを求められますのでユーザー名「manager」、パスワード「friend」を入力すると、次の画面が表示されます。



The screenshot shows the web interface for CentreCOM AR260S V2. The title bar includes the Allied Telesis logo and the version number 'CentreCOM® AR260S V2 Version 1.0.0'. On the left is a navigation menu with options like '設定/保存', 'セットアップウィザード', 'システム情報', 'LAN', 'WAN', 'ルーティング', 'ARP', 'ファイアウォール/NAT', 'VPN', 'ログ', 'システム管理', '再起動', and 'ログアウト'. The main content area displays 'CentreCOM® AR260S V2' and a 'セットアップウィザード' (Setup Wizard) dialog box with the text: 'このセットアップウィザードで本製品の基本設定を行うことができます。セットアップを始めるには「次へ」ボタンをクリックしてください。' Below the dialog is a '次へ' (Next) button. At the bottom right, it says 'アライドテレシス株式会社' and 'Copyright © 2006 Allied Telesis Holdings K.K. All rights reserved.'

次に、左側のメニューから[LAN]-[IP]を選択します。

[IP アドレス]を 192.168.10.1 (ルーター-B は 192.168.20.1)に変更して[適用]を押します。



The screenshot shows the 'LAN側IP設定' (LAN Side IP Configuration) page. It has three input fields: 'IPアドレス' (IP Address) with the value '192.168.10.1' circled in red, 'サブネットマスク' (Subnet Mask) with '255.255.255.0', and 'ダイレクトブロードキャスト転送' (Direct Broadcast Forwarding) with radio buttons for '有効' (Enabled) and '無効' (Disabled). There are '適用' (Apply) and 'ヘルプ' (Help) buttons. Below this is a table titled '現在の設定' (Current Settings) showing the current IP address as '192.168.1.1' and subnet mask as '255.255.255.0'.

現在の設定	
IPアドレス	192.168.1.1
サブネットマスク	255.255.255.0

[適用]を押した後 1 分ほどお待ち頂き、PC を再起動します。PC が起動完了したら、再度 Web ブラウザを起動して「<http://192.168.10.1/>」(ルーター-Bは <http://192.168.20.1/>)を開きます。

<手順2>

左側のメニューから[LAN]-[DHCP]を選択します。

[開始 IP アドレス]を 192.168.10.223 から 192.168.10.10(ルーターBは 192.168.20.10)に変更して [適用]を押します。

DHCPサーバ設定			
IPアドレスプール	始点IPアドレス	終点IPアドレス	
	<input type="text" value="192.168.10.10"/>	<input type="text" value="192.168.10.254"/>	
サブネットマスク	デフォルトゲートウェイ	リース期限	
255.255.255.0	192.168.10.1	<input type="text" value="00:12:00"/> (dd 日: hh 時間: mm 分)	
プライマリDNSサーバ		セカンダリDNSサーバ	
<input type="text" value="192.168.10.1"/> (オプション)		<input type="text"/> (オプション)	
プライマリWINSサーバ		セカンダリWINSサーバ	
<input type="text"/> (オプション)		<input type="text"/> (オプション)	
<input type="button" value="適用"/>		<input type="button" value="ヘルプ"/>	

<手順3>

左側のメニューから[WAN]-[WAN]を選択します。

[WAN 設定]の[接続モード]に PPPoE を選択し、[デフォルトゲートウェイ]を pppoe0 とします。

・ pppoe0 の設定

pppoe0 の[ユーザ名][パスワード]に、ISP から通知されたユーザーID/パスワードを設定して[適用]を押します。

セッションID pppoe0	<input type="button" value="接続"/>	<input type="button" value="切断"/>
アンナナバード PPPoE <input type="radio"/> 有効 <input checked="" type="radio"/> 無効	IPアドレス <input type="text"/> (オプション)	
ユーザ名 <input type="text" value="user1@example"/>	パスワード <input type="password" value="●●●●●●●●"/>	
サービス名 <input type="text"/> (オプション)	AC(アクセスコンセントレータ名) <input type="text"/> (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	DNS問い合わせドメイン <input type="text"/> (オプション)	
MSSクランプ <input checked="" type="radio"/> 有効 <input type="radio"/> 無効	クランプ値 <input type="text" value="40"/> バイト	MSS値 <input type="text" value="1414"/> バイト
接続オプション <input type="radio"/> ダイアルオンデマンド <input checked="" type="radio"/> キーブアライブ <input type="radio"/> 無効	エコー送信間隔 <input type="text" value="60"/> 秒	
<input type="button" value="適用"/>		

※ その他のパラメータは、初期状態のままで問題ございません。

• pppoe1の設定

pppoe1 の[ユーザ名][パスワード]に CUG サービスから通知されたユーザーID/パスワードを設定します。
[クランプ値]を 40 から 120 に変更し、[適用]を押します。

セッションID pppoe1	<input type="button" value="接続"/>	<input type="button" value="切断"/>
アンナナバード PPPoE <input type="radio"/> 有効 <input checked="" type="radio"/> 無効	IPアドレス <input type="text"/>	
ユーザ名 <input type="text" value="router1"/>	パスワード <input type="password" value="●●●●●●●●"/>	
サービス名 <input type="text"/> (オプション)	AC(アクセスコンセントレータ名) <input type="text"/> (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	DNS問い合わせドメイン <input type="text"/> (オプション)	
MSSクランプ <input checked="" type="radio"/> 有効 <input type="radio"/> 無効	クランプ値 <input type="text" value="120"/> バイト	MSS値 <input type="text" value="1334"/> バイト
接続オプション <input type="radio"/> ダイアルオンデマンド <input checked="" type="radio"/> キーブアライブ <input type="radio"/> 無効	エコー送信間隔 <input type="text" value="60"/> 秒	
<input type="button" value="適用"/>		

※ その他のパラメータは、初期状態のまま問題ございません。

<手順 4>

左側のメニューの[ルーティング]から[スタティックルーティング設定]を開きます。
 [宛先ネットワークアドレス]を 192.168.20.0(ルーターBは 192.168.10.0)に、
 [宛先ネットマスク]を 255.255.255.0 に設定します。

[ゲートウェイ]は インターフェース を選択し、pppoe1 を選んで[追加]を押します。



次に [宛先ネットワークアドレス]を 172.16.0.2(ルーターBは 172.16.0.1)に、
 [宛先ネットマスク]を 255.255.255.255 に設定します。

[ゲートウェイ]は インターフェース を選択し、pppoe1 を選んで[追加]を押します。



画面下部の[ルーティングテーブル]にて、以下のスタティックルートが追加されているかご確認ください。

ルーターA の場合:

[宛先ネットワークアドレス] 172.16.0.2 [宛先ネットマスク] 255.255.255.255 [インターフェース] pppoe1
 [宛先ネットワークアドレス] 192.168.20.0 [宛先ネットマスク] 255.255.255.0 [インターフェース] pppoe1

ルーターB の場合:

[宛先ネットワークアドレス] 172.16.0.1 [宛先ネットマスク] 255.255.255.255 [インターフェース] pppoe1
 [宛先ネットワークアドレス] 192.168.10.0 [宛先ネットマスク] 255.255.255.0 [インターフェース] pppoe1

<手順5>

左側のメニューから[ファイアウォール/NAT]-[ファイアウォール]を選択します。
 [pppoe1(WAN)] タブを開き、[アクセスリスト設定]に次の設定を行います。

[方向] Inbound

[動作] 通過

[優先度] 1

[送信元]-[タイプ] サブネット

[サブネット] 192.168.20.0(ルーターB の場合 192.168.10.0) [マスク] 255.255.255.0

[宛先]-[タイプ] サブネット

[サブネット] 192.168.10.0(ルーターB の場合 192.168.20.0) [マスク] 255.255.255.0

[送信元ポート] すべて

[宛先ポート] すべて

[プロトコル] すべて

[ログ] 無効

設定が完了したら、[追加]を押します。

アクセスリスト設定			
ID	新規作成		
方向	動作	優先度	
Inbound	通過	1	
送信元	タイプ	サブネット	マスク
	サブネット	192.168.20.0	255.255.255.0
宛先	タイプ	サブネット	マスク
	サブネット	192.168.10.0	255.255.255.0
送信元ポート	タイプ		
	すべて		
宛先ポート	タイプ		
	すべて		
プロトコル	プロトコル		
	すべて		
ログ	<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="ヘルプ"/>			

<手順6>

左側のメニューから[ファイアウォール/NAT]-[NAT 設定]を選択します。

[pppoe1(WAN)] タブを開き、「NAT 設定リスト」にある既存の項目を選択し[削除]を押します。

「削除します。よろしいですか?」と表示されますので、「OK」を押します。



NAT 設定リスト		
送信元	変換	宛先
<input checked="" type="radio"/> すべて	pppoe1	すべて

削除

<手順7>

左側のメニューから[VPN]-[VPN 接続]を選択し、[VPN 接続設定]を次の内容で設定します。

[ポリシー名] vpn 、有効
 [キープ SA] 無効
 [DF ビット設定] クリア
 [ローカルセキュアグループ]-[種類] サブネット
 [アドレス] 192.168.10.0(ルーターBの場合は 192.168.20.0)
 [マスク] 255.255.255.0
 [リモートセキュアグループ]-[種類] サブネット
 [アドレス] 192.168.20.0(ルーターBの場合は 192.168.10.0)
 [マスク] 255.255.255.0
 [ローカルゲートウェイ] pppoe1
 [リモートゲートウェイ]-[種類] IP アドレス
 [IP アドレス] 172.16.0.2(ルーターBの場合は 172.16.0.1)
 [内部 NAT] 無効 [フェーズ 2 ローカル ID] 空欄

VPN接続設定			
ID	1		
ポリシー名	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 <input type="text" value="vpn"/>		
キープSA	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効		
DFビット設定	<input type="radio"/> コピー <input type="radio"/> セット <input checked="" type="radio"/> クリア		
ローカルセキュアグループ	種類	アドレス	マスク
	<input type="text" value="サブネット"/>	<input type="text" value="192.168.10.0"/>	<input type="text" value="255.255.255.0"/>
リモートセキュアグループ	種類	アドレス	マスク
	<input type="text" value="サブネット"/>	<input type="text" value="192.168.20.0"/>	<input type="text" value="255.255.255.0"/>
ローカルゲートウェイ	インターフェース		
	<input type="text" value="pppoe1"/>		
リモートゲートウェイ	種類	IPアドレス	
	<input type="text" value="IPアドレス"/>	<input type="text" value="172.16.0.2"/>	
内部NAT	フェーズ2ローカルID		
<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	<input type="text"/> 例: 192.168.1.1/32		

※ ファームウェアバージョンが 2.0.0 の場合は[キープアライブ(DPD)]という項目も表示されますので、
 ※ 「有効」に設定してください。


次に、[IKE 設定]を設定します。

[IKE 交換モード] メイン

[事前共有鍵] secret

[IKE 暗号化/認証アルゴリズム] 3DES & SHA1-DH2

[有効期限] 3600 秒(1 時間)



IKE設定

IKE交換モード
 メイン アグレッシブ

事前共有鍵

IKE暗号化/認証アルゴリズム
 3DES & SHA1-DH2

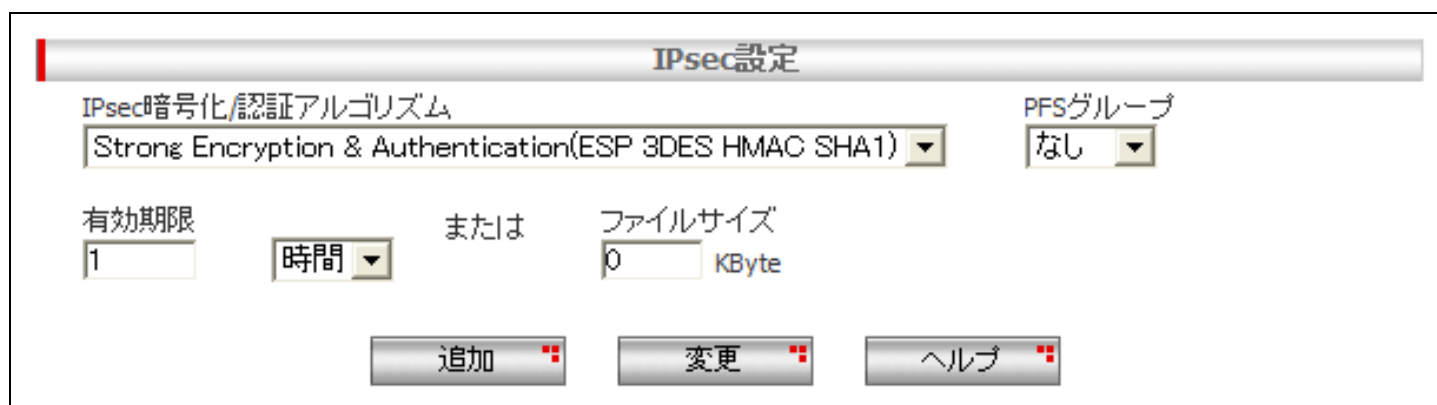
有効期限
 1 時間

次に、[IPsec 設定]を設定して[追加]を押します。

[IPsec 暗号化/認証アルゴリズム] Strong Encryption & Authentication(ESP 3DES HMAC SHA1)

[PFS グループ] なし

[有効期限] 3600 秒(1 時間)



IPsec設定

IPsec暗号化/認証アルゴリズム
 Strong Encryption & Authentication(ESP 3DES HMAC SHA1)

PFSグループ
 なし

有効期限
 1 時間

または
 ファイルサイズ
 0 KByte

追加 変更 ヘルプ

<手順8>

画面左上の[設定保存]を押します。

設定保存ボタン下の「設定が保存されていません」という表示が消えれば設定完了です。

設定例は以上です。