

PPPoE インターネット接続環境における 2 点間 IPsec VPN (片側アドレス不定・AR260S 同士)

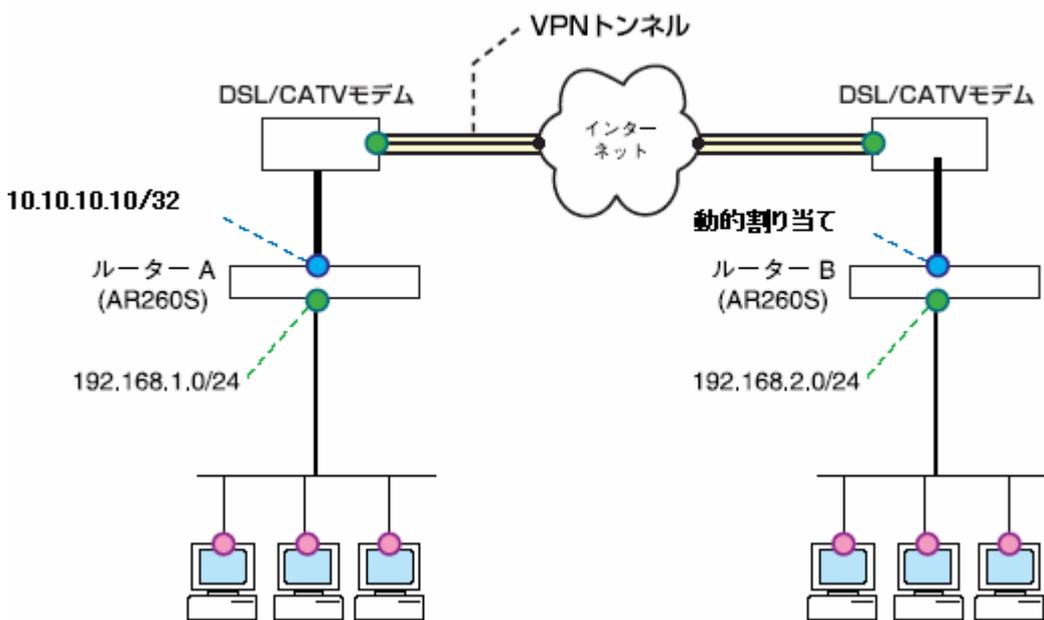
PPPoE でインターネットに接続している 2 つの拠点を IPsec で結ぶ VPN 構築例です。この例では、グローバルアドレス 1 個を固定的に割り当てられているサイトと、グローバルアドレス 1 個を動的に割り当てられるサイトの間を IPsec (ESP) のトンネルで接続します。

各拠点は、ISP から次の情報を提供されているものとして扱います。

	ルーターA	ルーターB
PPP ユーザー名	pppoe1@ispA	pppoe2@ispB
PPP パスワード	pppoe1AAA	pppoe2BBB
PPPoE サービス名	isp1	isp1
使用できる IP アドレス	10.10.10.10/32	グローバルアドレス 1 個を接続時に割り当て
接続形態	端末型(アドレス 1 個固定)	端末型(アドレス 1 個不定)

以下、ルーターA、B の基本設定についてまとめます。

	ルーターA	ルーターB
WAN 側物理インターフェース	WAN	WAN
WAN 側 IP アドレス	10.10.10.10/32	動的割り当て (ppp0)
LAN 側 IP アドレス	192.168.1.1/24	192.168.2.1/24



上図構成において IPsec VPN を構築するときのポイントは次のとおりです。

- ・ ルーターB のアドレスが不定なため、ルーターA からルーターB に接続することはできません。常にルーターB から接続を開始することになります。
- ・ ルーターB のアドレスが不定なため、IKE フェーズ1 では Aggressive モードを使い、ルーターB の ID として文字列 (名前) を使用します。
- ・ トンネリング対象のパケットに NAT が適用されないように Outbound/Inbound アクセスの設定をします。

IPsec 関連の設定は次のようになります。

IKE 設定

ルーター間の認証方式	事前共有鍵 (pre-shared key)
IKE 交換モード	Aggressive モード
事前共有鍵	test (文字列)
ルーターA の認証 ID	未定義
ルーターB の認証 ID	vpn_sc
ISAKMP メッセージの暗号化方式	全て (デフォルト)
ISAKMP メッセージの認証方式	全て (デフォルト)
ISAKMP SA の有効期限 (時間)	デフォルト値を使用
ISAKMP SA の有効期限 (Kbyte 数)	デフォルト値を使用

IPsec 設定

セキュリティープロトコル	全て
暗号化方式	全て
認証方式	全て
IPsec SA の有効期限 (時間)	デフォルト値を使用
IPsec SA の有効期限 (Kbyte 数)	デフォルト値を使用
トンネリング対象 IP アドレス	192.168.1.0/24 192.168.2.0/24
トンネル終端アドレス	10.10.10.10 (A) ・不定 (B)
VPN 無通信監視	無効

ルーターA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	192.168.1.1
サブネットマスク	255.255.255.0
<input type="button" value="適用"/> <input type="button" value="ヘルプ"/>	

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

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、端末の IP アドレスを取得しなおしてから、AR260S の変更後のアドレスに接続します。



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設定	
接続モード	PPPoE
セッションID	PPPoE:0 <input type="button" value="切断"/>
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	pppoe1@ispA
パスワード	●●●●●●●●
サービス名	isp1 (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"/> ダイアルオンデマンド <input checked="" type="radio"/> キープアライブ <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「システム管理」 「サービスの有効 / 無効」の順にクリックし、VPN を有効にします。VPN 機能を使用する場合、「サービスの有効 / 無効」にて VPN を有効にしてから、VPN 接続設定を行う必要があります。

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 checked="" type="radio"/> 有効 <input type="radio"/> 無効
DNSリレー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
DHCP	<input checked="" type="radio"/> 有効 <input 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

4.メニューから「VPN」 「VPN 接続」の順にクリックし、VPN 接続設定を行います。VPN 接続設定にてポリシーを作成する前に、「サービスの有効 / 無効」にて VPN サービスを有効にしておいてください。

各パラメーターについて以下に説明いたします。

・VPN 無通信監視:

VPN 通信が「無通信時間」指定した時間発生しなかった場合に、IPsec SA を削除する機能です。

・ローカルセキュアグループ:

ポリシーの適用対象となるパケットのローカル側 IP アドレスを指定します。

・リモートセキュアグループ:

ポリシーの適用対象となるパケットのリモート側 IP アドレスを指定します。

・リモートゲートウェイ:

VPN 接続先の IP アドレスが不定である場合、「全て」を選択します。

・ローカル ID:

IKE モードにて「Aggressive」を選択した場合にのみ表示されます。おもに、自分の IP が不定の場合に指定します。

・リモート ID:

IKEモードにて「Aggressive」を選択した場合にのみ表示されます。おもに、リモートゲートウェイのIPが不定の場合に指定します。この例では相手のIPアドレスが不定なため、リモートIDで相手の認証IDを指定します。

・IKE交換モード:

片側IPアドレス不定の場合、「Aggressive」を選択します。「Aggressive」は、おもにリモートゲートウェイのIPアドレスが片側不定の場合に選択します。

・IKE暗号化/認証アルゴリズム:

AR260S同士であれば、「全て」でも接続可能です。

・IPsec 暗号化/認証アルゴリズム:

AR260S 同士であれば、「全て」でも接続可能です。

・PFS グループ:

PFS 機能を使用するかどうかを指定します。未定義は使用しません。

VPN接続設定	
ID	1:vpn_ip1
ポリシー名	vpn_ip1
	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	優先度 1
VPN無通信監視	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
ローカルセキュアグループ	種類 サブネット
	アドレス 192.168.1.0
	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 192.168.2.0
	マスク 255.255.255.0
ローカルゲートウェイ	インターフェース pppoe0
リモートゲートウェイ	種類 全て
ローカルID	種類 未定義
リモートID	種類 FQDN
	FQDN vpn_sc
IKE設定	
IKE交換モード	<input type="radio"/> Main <input checked="" type="radio"/> Aggressive
事前共有鍵	****
IKE暗号化認証アルゴリズム	全て
有効期限	3600 秒
IPSec設定	
IPSec暗号化認証アルゴリズム	全て
PFSグループ	未定義
有効期限	3600 秒 または 75000 KByte
<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.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。ファイアウォールを有効にしている場合は、ファイアウォールでISAKMP/IPsecのパケットが遮断されないように、Inbound/Outbound アクセス制御設定にて、アクセスを透過する設定が必要になります。

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	サブネット			
	アドレス	192.168.2.0			
	マスク	255.255.255.0			
宛先	タイプ	サブネット			
	アドレス	192.168.1.0			
	マスク	255.255.255.0			
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	未定義				
ログ	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効				
VPN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効				
				追加	変更
				削除	ヘルプ
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	192.168.2.0 - 255.255.255.0	192.168.1.0 - 255.255.255.0	全て,全て,全て	未定義	通過

6.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。ファイアウォールを有効にしている場合は、ファイアウォールでISAKMP/IPsecのパケットが遮断されないように、Inbound/Outboundアクセス制御設定にて、アクセスを透過する設定が必要になります。

Outbound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: サブネット アドレス: 192.168.1.0 マスク: 255.255.255.0
宛先	タイプ: サブネット アドレス: 192.168.2.0 マスク: 255.255.255.0
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	未定義
ログ	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
VPN	<input checked="" type="radio"/> 有効 <input 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	192.168.1.0 - 255.255.255.0	192.168.2.0 - 255.255.255.0	全て,全て,全て	未定義	通過	
2	全て	全て	全て,全て,全て	pppoe0	通過	

Outboundアクセスルールにはデフォルトでポリシーが設定されています。(ID:2 の設定がデフォルトポリシーになります。)このポリシーが設定されていることで、LAN側からインターネットへ向けたパケットのIPアドレスは全てpppoe0インターフェースのIP アドレスに変換され、インターネット通信が可能になります。VPNパケットを透過するアクセスルールはデフォルトポリシーより優先度を高く設定する必要があります。

ルーターB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	192.168.2.1
サブネットマスク	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、端末の IP アドレスを取得しなおしてから、AR260S の変更後のアドレスに接続します。



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設定	
接続モード	PPPoE
セッションID	PPPoE:0 <input type="button" value="切断"/>
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	pppoe2@isp8
パスワード	*****
サービス名	isp1 (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 <input type="text" value="40"/> Bytes
接続オプション	<input type="radio"/> ダイアルオンデマンド <input checked="" type="radio"/> キープアライブ <input type="radio"/> 無効 エコー送信間隔 <input type="text" value="60"/> 秒
<input type="button" value="適用"/> <input type="button" value="ヘルプ"/>	

3.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、VPN を有効にします。VPN 機能を使用する場合、「サービスの有効 / 無効」にて VPN を有効にしてから、VPN 接続設定を行う必要があります。

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 checked="" type="radio"/> 有効 <input type="radio"/> 無効
DNSリレー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
DHCP	<input checked="" type="radio"/> 有効 <input 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

4.メニューから「VPN」 「VPN 接続」の順にクリックし、VPN 接続設定を行います。VPN 接続設定にてポリシーを作成する前に、「サービスの有効 / 無効」にて VPN サービスを有効にしておいてください。

各パラメーターについて以下に説明いたします。

・VPN 無通信監視:

VPN 通信が「無通信時間」指定した時間発生しなかった場合に、IPsec SA を削除する機能です。

・ローカルセキュアグループ:

ポリシーの適用対象となるパケットのローカル側 IP アドレスを指定します。

・リモートセキュアグループ:

ポリシーの適用対象となるパケットのリモート側 IP アドレスを指定します。

・リモートゲートウェイ:

VPN 接続先の IP アドレスが不定である場合、「全て」を選択します。

・ローカル ID:

IKEモードにて「Aggressive」を選択した場合にのみ表示されます。おもに、自分のIPが不定の場合に指定します。この例では自分のIPアドレスが不定なため、ローカルIDで自分の認証IDを指定します。

・リモートID:

IKEモードにて「Aggressive」を選択した場合にのみ表示されます。おもに、リモートゲートウェイのIPが不定の場合に指定します。

・IKE交換モード:

片側IPアドレス不定の場合、「Aggressive」を選択します。「Aggressive」は、おもにリモートゲートウェイのIPアドレスが片側不定の場合に選択します。

・IKE暗号化/認証アルゴリズム:

AR260S同士であれば、「全て」でも接続可能です。

・IPsec 暗号化/認証アルゴリズム:

AR260S 同士であれば、「全て」でも接続可能です。

・PFS グループ:

PFS 機能を使用するかどうかを指定します。未定義は使用しません。

VPN基本設定	
ID	1:vpn_ip0
ポリシー名	vpn_ip0
	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	優先度 1
VPN無通信監視	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
ローカルセキュアグループ	種類 サブネット アドレス 192.168.2.0 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 192.168.1.0 マスク 255.255.255.0
ローカルゲートウェイ	インターフェース pppoe0
リモートゲートウェイ	種類 IPアドレス IPアドレス 10.10.10.10
ローカルID	種類 FQDN FQDN vpn_sc
リモートID	種類 未定義
IKE設定	
IKE交換モード	<input type="radio"/> Main <input checked="" type="radio"/> Aggressive
事前共有鍵	****
IKE暗号化認証アルゴリズム	全て
有効期限	3600 秒
IPSec設定	
IPSec暗号化認証アルゴリズム	全て
PFSグループ	未定義
有効期限	3600 秒 または 75000 KByte
<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.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。ファイアウォールを有効にしている場合は、ファイアウォールでISAKMP/IPsecのパケットが遮断されないように、Inbound/Outbound アクセス制御設定にて、アクセスを透過する設定が必要になります。

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	サブネット	アドレス	192.168.1.0	マスク	255.255.255.0
宛先	タイプ	サブネット	アドレス	192.168.2.0	マスク	255.255.255.0
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	未定義					
ログ	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効					
VPN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効					
			追加	変更	削除	
ヘルプ						
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	192.168.1.0 - 255.255.255.0	192.168.2.0 - 255.255.255.0	全て,全て,全て	未定義	通過	

6.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。ファイアウォールを有効にしている場合は、ファイアウォールでISAKMP/IPsecのパケットが遮断されないように、Inbound/Outbound アクセス制御設定にて、アクセスを透過する設定が必要になります。

Outbound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: サブネット アドレス: 192.168.2.0 マスク: 255.255.255.0
宛先	タイプ: サブネット アドレス: 192.168.1.0 マスク: 255.255.255.0
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	未定義
ログ	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
VPN	<input checked="" type="radio"/> 有効 <input 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	192.168.2.0 - 255.255.255.0	192.168.1.0 - 255.255.255.0	全て 全て 全て	未定義	通過
2	全て	全て	全て 全て 全て	pppoe0	通過

Outboundアクセスルールにはデフォルトでポリシーが設定されています。(ID:2 の設定がデフォルトポリシーになります。)このポリシーが設定されていることで、LAN側からインターネットへ向けたパケットのIPアドレスは全て pppoe0インターフェースのIP アドレスに変換され、インターネット通信が可能になります。VPNパケットを透過するアクセスルールはデフォルトポリシーより優先度を高く設定する必要があります。

メモ

上記設定が終了したら、VPN 通信が可能かご確認ください。メニューから「VPN」「統計情報」の順にクリックし、VPN トラフィックの確認をします。IKE SA、IPSec SA を確認し、VPN が確立されているか確認してください。

以下のように表示されていれば、VPN は確立しています。

VPN Statistics							
Global IPSec SA Statistics							
AH Packets	0						
ESP Packets	45						
Triggers	0						
Packets Dropped	0						
Packets Passed	51						
IKE Statistics							
IKE Phase1 Negotiations Done	2						
Failed IKE Negotiations Done	0						
Quick Mode Negotiations Performed	2						
Number of ISAKMP SAs	1						
ESP Statistics							
Active Inbound ESP SAs	1						
Active Outbound ESP SAs	1						
Total Inbound ESP SAs	2						
Total Outbound ESP SAs	2						
AH Statistics							
Active Inbound AH SAs	0						
Active Outbound AH SAs	0						
Total Inbound AH SAs	0						
Total Outbound AH SAs	0						
IKE SA							
	Local ID	Remote ID	Local Port	Remote Port	Phase1 Status	Exchange Type	Initiator
	10.10.10.10	vpn_sc	500	500	Done	Aggressive	No
IPSec SA							
	SPI	Protocol	Source IP	Destination IP			
	3490621792	ESP	10.10.10.10	20.20.20.20			
	2376325393	ESP	20.20.20.20	10.10.10.10			
更新							

更新日 2005 年 10 月 26 日