

CentreCOM AR260S 設定例

PPPoEインターネット接続環境における2点間IPsec VPN (両側アドレス固定)
AR260S同士でのIPsec VPN

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の間を IPsec (ESP) のトンネルで接続します。

各拠点は、インターネットサービスプロバイダー (ISP) から次の情報を提供されているものとします。

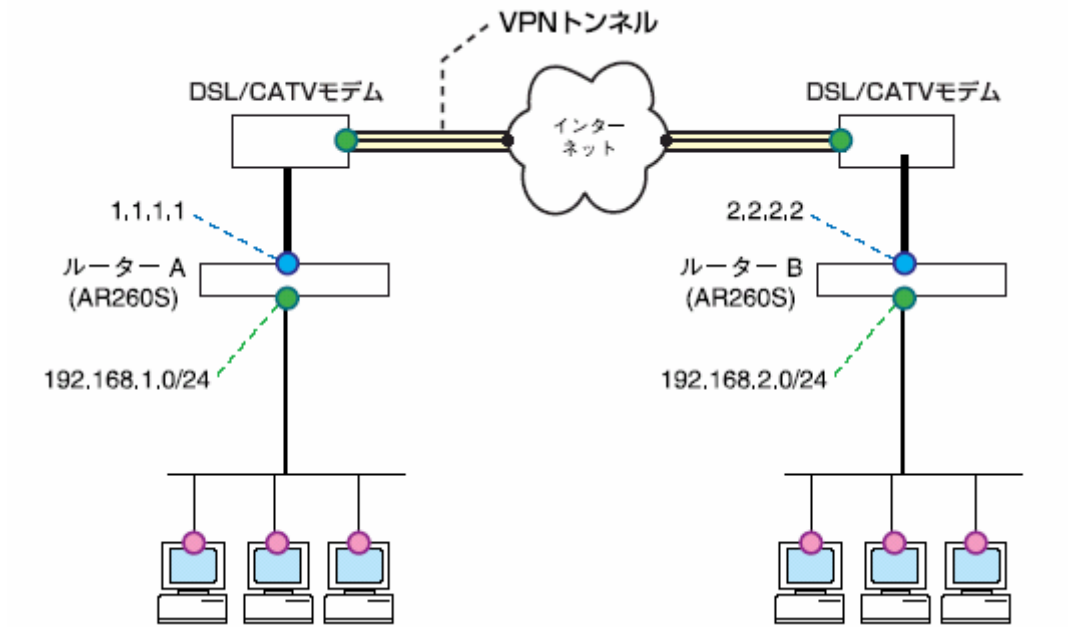
表1：ISP から提供された情報

	ルーターA	ルーターB
PPP ユーザー名	userA@ispA	userB@ispB
PPP パスワード	isppasswdA	isppasswdB
PPPoE サービス名	なし	なし
使用できる IP アドレス	1.1.1.1/32	2.2.2.2/32
接続形態	端末型 (アドレス1個固定)	端末型 (アドレス1個固定)

以下、ルーターA、Bの基本設定についてまとめます。

表2：ルーターA、Bの基本設定

	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	1.1.1.1/32	2.2.2.2/32
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。

- トンネリング対象の packets に NAT が適用されないよう Inbound/Outbound アクセスルールを設定します。

IPsec 関連の設定は次のようになります。

表 3 : 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	Main モード
事前共有鍵	secret (文字列)
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

表 4 : 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	1.1.1.1/32 (A) ・ 2.2.2.2/32 (B)
VPN 無通信監視	無効
キープ SA	無効
PFS グループ	使用しない

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

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	userA@ispA
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
<input type="button" value="適用"/> <input type="button" value="ヘルプ"/>	

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。

・キープ SA：

PPPoEセッションが切断されたときに、確立中のIPsec SA 保持する機能です。有効時はPPPoEセッションが切断されても有効期限まで SA を保持します。

・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。

・ローカルゲートウェイ：

VPN 通信パケットを送受信するローカルのインターフェースを指定します。

・リモートゲートウェイ：

VPN 接続先ルーター（対向ルーターのWAN 側）の IP を指定します。

・IKE交換モード：

両側IPアドレス固定の場合、通常「Main」を選択します。Mainモードは、両側IPが固定の場合に使用することが可能です。

- IKE暗号化/認証アルゴリズム：
対向のARルーターとIKE 暗号化/認証アルゴリズムを合わせて設定する必要があります。「全て」を選択することも可能です。
- IPsec 暗号化/認証アルゴリズム：
対向のARルーターとIPsec 暗号化/認証アルゴリズムを合わせて設定する必要があります。「全て」を選択することも可能です。
- 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	ポリシー名	vpn	<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			
キープSA			<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	ppp0e0				
リモートゲートウェイ	種類	IPアドレス				
	IPアドレス	2.2.2.2				
IKE設定						
IKE交換モード			<input checked="" type="radio"/> Main <input 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"/>						
サイト間アクセスルール						
	ID	ポリシー名	ローカル/リモートネットワーク	トンネル終端	鍵管理方式	IPSec 状況
	1	vpn	192.168.1.0/24 192.168.2.0/24	2.2.2.2	事前共有鍵	トンネル 有効

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			
<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"/>
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						
				追加	変更	削除	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	<input type="text" value="192.168.2.1"/>
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"/>	

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	<input type="text" value="PPPoE"/> <input type="button" value="切断"/>
セッションID	<input type="text" value="PPPoE:0"/> <input type="button" value="切断"/>
デフォルトゲートウェイ	<input type="text" value="PPPoE:0"/>
Unnumbered PPPoE	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
ホスト名	<input type="text" value="AR260S"/> (オプション)
ユーザー名	<input type="text" value="userB@ispB"/>
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ー)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
プライマリDNSサーバー	<input type="text"/> (オプション)
セカンダリDNSサーバー	<input type="text"/> (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="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
<input type="button" value="適用"/> <input type="button" value="ヘルプ"/>	

- 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。

・キープ SA：

PPPoEセッションが切断されたときに、確立中のIPsec SA 保持する機能です。有効時はPPPoEセッションが切断されても有効期限まで SA を保持します。

・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。

・ローカルゲートウェイ：

VPN 通信パケットを送受信するローカルのインターフェースを指定します。

・リモートゲートウェイ：

VPN 接続先ルーター（対向ルーターのWAN 側）の IP を指定します。

・IKE交換モード：

両側IPアドレス固定の場合、通常「Main」を選択します。Mainモードは、両側IPが固定の場合に使用することが可能です。

- ・IKE暗号化/認証アルゴリズム：
対向のARルーターとIKE 暗号化/認証アルゴリズムを合わせて設定する必要があります。「全て」を選択することも可能です。
- ・IPsec 暗号化/認証アルゴリズム：
対向のARルーターとIPsec 暗号化/認証アルゴリズムを合わせて設定する必要があります。「全て」を選択することも可能です。
- ・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	ポリシー名	vpn	<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			
キープSA			<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	1.1.1.1				
IKE設定						
IKE交換モード			<input checked="" type="radio"/> Main <input 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	
			追加	変更	削除	ヘルプ
サイト間アクセスルール						
	ID	ポリシー名	ローカル/リモートネットワーク	トンネル終端	鍵管理方式	IPSec 状況
 	1	vpn	192.168.2.0/24 192.168.1.0/24	1.1.1.1	事前共有鍵	トンネル 有効

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 通信が可能かどうか確認してください。

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。

以下の表示のようになっていれば、VPN は確立されております。

ルーターAの「VPN 統計情報」

VPN Statistics							
Global IPsec SA Statistics							
AH Packets	0						
ESP Packets	14						
Triggers	0						
Packets Dropped	0						
Packets Passed	18						
IKE Statistics							
IKE Phase1 Negotiations Done	1						
Failed IKE Negotiations Done	0						
Quick Mode Negotiations Performed	1						
Number of ISAKMP SAs	1						
ESP Statistics							
Active Inbound ESP SAs	1						
Active Outbound ESP SAs	1						
Total Inbound ESP SAs	1						
Total Outbound ESP SAs	1						
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
	1.1.1.1	2.2.2.2	500	500	Done	Identity Protection	No
IPsec SA							
	SPI	Protocol	Source IP	Destination IP			
	 2064723132	ESP	2.2.2.2	1.1.1.1			
	 3516026403	ESP	1.1.1.1	2.2.2.2			
更新							



ルーターBの「VPN 統計情報」

VPN Statistics							
Global IPsec SA Statistics							
AH Packets						0	
ESP Packets						374	
Triggers						10	
Packets Dropped						0	
Packets Passed						518	
IKE Statistics							
IKE Phase1 Negotiations Done						6	
Failed IKE Negotiations Done						2	
Quick Mode Negotiations Performed						36	
Number of ISAKMP SAs						1	
ESP Statistics							
Active Inbound ESP SAs						1	
Active Outbound ESP SAs						1	
Total Inbound ESP SAs						36	
Total Outbound ESP SAs						36	
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
	2.2.2.2	1.1.1.1	500	500	Done	Identity Protection	Yes
IPsec SA							
	SPI	Protocol	Source IP	Destination IP			
	2064723132	ESP	2.2.2.2	1.1.1.1			
	3516026403	ESP	1.1.1.1	2.2.2.2			
更新							

更新日 2005 年 2 月 22 日

