BROADBAND GATE

Linux エンジン搭載ブロードバンドルータ

FutureNet XR シリーズ

IPsec 経由で SNMP 情報を取得する設定

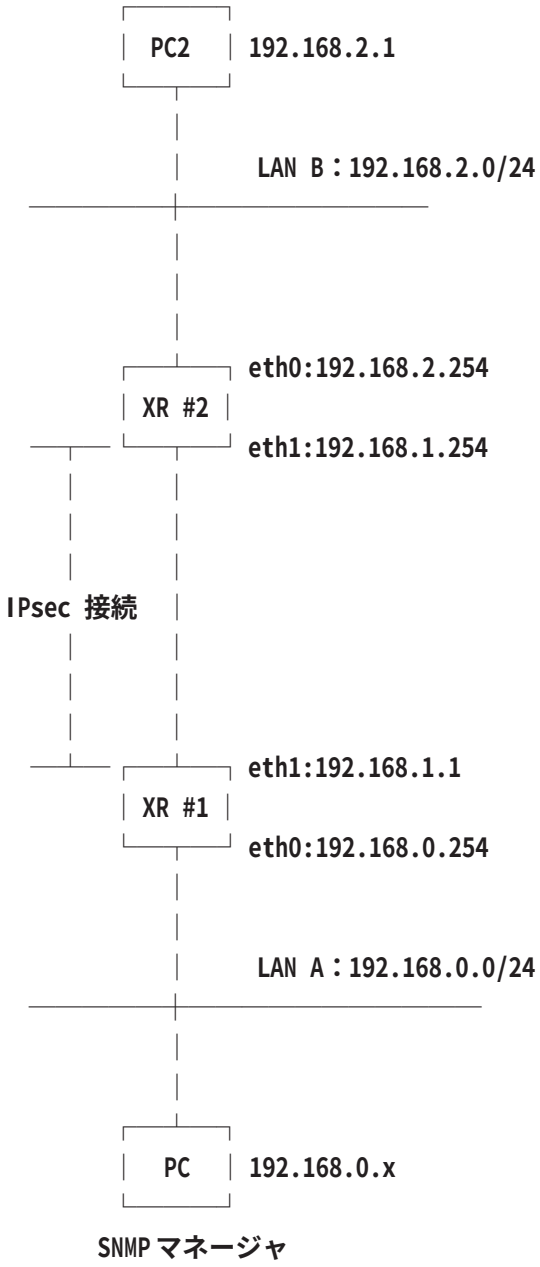
センチュリー・システムズ 株式会社

IPsec 設定ガイド

IPsec 経由で SNMP 情報を取得する設定

ネットワーク構成

XR #1 と XR # 2 との間で Ipsec トンネルを生成し、SNMP マネージャ(PC1)が XR #2 から IPsec 経由で SNMP 情報を取得可能とします。



運用条件

・SNMP マネージャは 192.168.0.0/24 内の PC とします。

・XR #2 は SNMP エージェントとなります。

・XR #1 - XR #2 間で IPsec を確立し、XR #2 の MIB 情報は IPsec トンネルを経由して、192.168.0.0/24 内の SNMP マネージャで取得します。

・どちらの XR とも、PPPoE 接続します。

IPsec 設定条件

・PSK 共通鍵方式で認証します。

・main モードで接続します。

・共通鍵は「ipseckey」とします。

・XR #1、XR #2 ともに固定的に IP アドレスが割り当てられるものとします。

・IP アドレス等は図中の表記を使うものとします。

設定方法

◆XR #1 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU 値の設定　必要に応じて設定します。
○NAT Traversal の設定　「使用しない」
○VirtualPrivate 設定　「空欄」
○鍵の表示　「空欄」

「本装置側の設定 1」

○インタフェースの IP アドレス　「192.168.1.1」
○上位ルータの IP アドレス　「%ppp0」
○インタフェース ID　「空欄」

インターフェースのIPアドレス	192.168.1.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	（例：@xr.centurysys）

「IKE/ISAKMP ポリシーの設定 1」

○ IKE/ISAKMP ポリシー名　「任意で入力」
○接続する本装置側の設定　「本装置側の設定 1」
○インタフェースの IP アドレス　「192.168.1.254」
○上位ルーターの IP アドレス　「空欄」
○インタフェースの ID　「空欄」
○モードの設定　「main モード」
○Transform の設定　1 番目「すべてを送信する」
　2～4 番目は「使用しない」
○ IKE のライフタイム　「任意で設定」
○鍵の表示　「PSK を使用する」を選択し、「ipseckey」を入力します。

IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	192.168.1.254
上位ルータのIPアドレス	
インターフェースのID	（例：@xr.centurysys）
モードの設定	main モード
transformの設定	1番目 すべてを送信する 2番目 使用しない 3番目 使用しない 4番目 使用しない
IKEのライフタイム	3600 秒（1081～28800秒まで）
鍵の設定	
◉ PSKを使用する ○ RSAを使用する (X509を使用する場合は RSAに設定してください)	ipseckey

「IPsec ポリシーの設定 1」

○「使用する」を選択
○使用する IKE ポリシー名の選択　「IKE1」
○本装置側の LAN 側のネットワークアドレス
　「192.168.0.0/24」
○相手側の LAN 側のネットワークアドレス
　「192.168.1.254/32」
○ PH2 の Transform の設定　「すべてを送信する」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「指定しない」
○ SA のライフタイム　「任意で設定」

◉ 使用する ○ 使用しない ○ Responderとして使用する ○ On-Demandで使用する	
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.1.254/32 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	◉ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)

相手側の LAN 側のネットワークアドレスは、リモート側装置の **”WAN 側 IP アドレス /32”** として設定します。

「IPsec ポリシーの設定 2」

○「使用する」を選択
○使用する IKE ポリシー名の選択　「IKE1」
○本装置側の LAN 側のネットワークアドレス
　「192.168.0.0/24」
○相手側の LAN 側のネットワークアドレス
　「192.168.2.0/24」
○ PH2 の Transform の設定　「すべてを送信する」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「指定しない」
○ SA のライフタイム　「任意で設定」

◉ 使用する ○ 使用しない ○ Responderとして使用する ○ On-Demandで使用する	
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.2.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	◉ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)

◆XR #2 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU 値の設定　必要に応じて設定します。
○NAT Traversal の設定　「使用しない」
○VirtualPrivate 設定　「空欄」
○鍵の表示　「空欄」

「本装置側の設定 1」

○インタフェースの IP アドレス　「192.168.1.254」
○上位ルータの IP アドレス　「%ppp0」
○インタフェース ID　「空欄」

インターフェースのIPアドレス	192.168.1.254
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例：@xr.centurysys)

「IKE/ISAKMP ポリシーの設定 1」

○ IKE/ISAKMP ポリシー名　「任意で入力」
○接続する本装置側の設定　「本装置側の設定 1」
○インタフェースの IP アドレス　「192.168.1.1」
○上位ルーターの IP アドレス　「空欄」
○インタフェースの ID　「空欄」
○モードの設定　「main モード」
○ Transform の設定　1 番目「すべてを送信する」
2～4 番目は「使用しない」
○ IKE のライフタイム　「任意で設定」
○鍵の表示　「PSK を使用する」を選択し、「ipseckey」を入力します。

IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	192.168.1.1
上位ルータのIPアドレス	
インターフェースのID	(例：@xr.centurysys)
モードの設定	main モード
transformの設定	1番目 すべてを送信する 2番目 使用しない 3番目 使用しない 4番目 使用しない
IKEのライフタイム	3600 秒 (1081～28800秒まで)
鍵の設定	
PSKを使用する RSAを使用する (X509を使用する場合はRSAに設定してください)	ipseckey

「IPsec ポリシーの設定 1」

○「使用する」を選択
○使用する IKE ポリシー名の選択　「IKE1」
○本装置側の LAN 側のネットワークアドレス
「192.168.1.254/32」
○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」
○ PH2 の Transform の設定　「すべてを送信する」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「指定しない」
○ SA のライフタイム　「任意で設定」

使用する / 使用しない / Responderとして使用する / On-Demandで使用する	
使用するIKEポリシー名の選択	IKE1
本装置側のLAN側のネットワークアドレス	192.168.1.254/32 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する / 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)

本装置の LAN 側のネットワークアドレスは、本装置の”WAN 側 IP アドレス /32”として設定します。

「IPsec ポリシーの設定 2」

○「使用する」を選択
○使用する IKE ポリシー名の選択　「IKE1」
○本装置側の LAN 側のネットワークアドレス
「192.168.2.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」
○ PH2 の Transform の設定　「すべてを送信する」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「指定しない」
○ SA のライフタイム　「任意で設定」

使用する / 使用しない / Responderとして使用する / On-Demandで使用する	
使用するIKEポリシー名の選択	IKE1
本装置側のLAN側のネットワークアドレス	192.168.2.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する / 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400秒まで)

これらの設定で、LAN A と LAN B 間の VPN 接続、ならびに LAN A から XR #2 の SNMP 情報を VPN 経由で取得できます。

ステートフルパケットインスペクション機能が有効か、明示的にフィルタ設定をしているときは、IPsec 用の入力フィルタ設定をしてください。

注意点

IPsec 経由で SNMP 情報を取得する場合、対向側装置の IP アドレスは固定 IP アドレスでなければなりません。対向側装置が動的 IP アドレスの場合は、IPsec 経由での SNMP 情報取得ができません。

XR シリーズ IPsec 経由で SNMP 情報を取得する設定ガイド 1981
2003 年 8 月版
発行 センチュリー・システムズ株式会社