FutureNet XR Series ⇔ DOVPN

接続設定ガイド

Ver 1.0.0

センチュリー・システムズ株式会社

目次

は	じめに	3
改	版履歷	4
1.	基本設定例	5
	1-1. 構成例	5
	1-2. 設定例	6 6
	121. ビジダ ル ダ (AII) 1-2-2. VPN クライアント (携帯端末)	0
2.	センター経由での IPsec 通信設定例	. 18
	2-1. 構成例	. 18
	2-2. 設定例	. 19
	2-2-1. センタールータ (XR_A)	. 19
	2-2-2. 拠点ルータ (XR_B)	. 23
	2-2-3. VPN クライアント(携帯端末)	. 25
3.	サポートデスクへのお問い合わせ	. 31
	3-1. サポートデスクへのお問い合わせに関して	. 31
	9-9 井平 トニュカのブ利田に開して	91

はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- DOVPN は日立ビジネスソリューション株式会社の日本における登録商標です。
- Windows は、米国マイクロソフト社の米国およびその他の国における登録商標です。
- 本書に記載されている会社名,製品名は、各社の商標および登録商標です。
- DOVPN のインストール方法および詳細な操作方法につきましては、DOVPN「取扱説明書」をご覧ください。
- 本ガイドは、以下のFutureNet XR 製品に対応しております。
 - XR-510/C
 - XR-540/C
 - XR-730/C
 - ・ XR-1100 シリーズ
- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は XR-510/C Ver3.5.0, DOVPN は Ver2.1βをベースに作成しております。IPsec および IPsec KeepAlive において、ご使用されている製品およびファームウェアのバージョンによっては、一部機能および設定画面が異なっている場合もありますので、その場合は各製品のユーザーズガイドを参考に、適宜読みかえてご参照および設定を行って下さい。
- 本書を利用し運用した結果発生した問題に関しましては、一切責任を負いかねますのでご了承下さい。

改版履歴

Version	更新内容	
1.0.0	初版	

1. 基本設定例

携帯端末にインストールして使用する VPN クライアント「DOVPN」を利用することにより、外出先などの リモートからも IPsec によるインターネッ VPN が利用可能です。この設定例では、携帯端末でのセンタ ーLAN 側へのリモートアクセスを実現しています。

1-1. 構成例



1-2. 設定例

1-2-1. センタールータ (XR)

ポイント

VPN クライアントをインストールした携帯端末と IPsec 接続するための設定を行います。 VPN クライアントをインストールした携帯端末は動的 IP アドレスを取得しているため、IKE モードとし てアグレッシブモードを使用しています。

〈〈インタフェース設定〉〉

[Ethernet0の設定]

● 固定アド	レスで使用	101 1
IP アドレス	192.168.10.1	
ネットマスク	255.255.255.0]
MTU	1500	

Ethernet0 に関する設定をします。

※IPアドレスの設定を変更した場合、その設定した IPアドレスが即反映されます。

[Ethernet1の設定]

● 固定アド	レスで使用	
IP アドレス	0	
ネットマスク	255.255.255.0	
мти	1500	

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定1]

ユーザロ	test1@centurysys
パスワード	test1pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

接続先の選択	●接統先1 ●接統先2 ●接統先3 ●接統先4 ●接統先5
接続ポート	O Ether0 O Ether1 O Ether2 O BRI(54K) O BRI MP(128K) O Leased Line(64K) O Leased Line(128K) O RS2320
接統形態	○ 手動接続 ● 常時接続 ● スケジューラ接続
RS232C/BRI接続タイプ	 ● 通常 ○ On-Demand接続
ドマスカレード	○無効 ◎ 有効
ステートフルパケット インスペウション	○ 無効 ● 有効 □ DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◎ 有効

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、XR 配下の端末からのルータ経由でのインターネットアクセスも可能になっています。

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	ICMP type/code	送信元MADアドレス	LOG
рррО	パケット受信時	許可 💌	udp 💌		500		500			
рррО	パケット受信時	許可 💌	esp 💌							

IKE パケット, ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

インターフェー スのIPアドレス	10.10.10.1	
上位ルータのIPアドレス	%ррр0	
インターフェー スのID		(例:@xr.centurysys)

XRの WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	VPN_Client
リモート IP アドレス	0. 0. 0. 0
インタフェースの ID	@dovpn
モード	Aggressive
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DH グループ	Group2
ライフタイム	3600(秒)
事前共有鍵(Pre Shared Key)	ipseckey

IKE/ISAKMPポリシー名	VPN_Client
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	0.0.0.0
上位ルータのIPアドレス	
インターフェー スのレ	@dovpn (例:@xt.centurysys)
モードの設定	aggressive モード 💌
	1∰目 group2-aes128-sha1 💌
	2番目 使用しない 💌
transformu) as a	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)

VPN クライアントに対する IKE/ISAKMP ポリシーを設定します。

XR における ID の設定では"@"を付けますが、DOVPN では、"@"を付けない形式で設定してください。 DOVPN でも"@"を付けて設定すると接続できません。

鍵の設定	
 PSKを使用する PSAを使用する (X500を使用する場合は PSAL設定してください) 	i pseckey

事前共有鍵(PSK)として「ipseckey」を設定しています。

[IPsec ポリシーの設定 1]

○ 使用する ○ 使用しない ◎ Responderとして使用する ○ On-Dermandで使用する

VPN クライアントの IP アドレスが不定のため、「Responder として使用する」を選択します。

設定項目	パラメータ
使用する IKE ポリシー名	VPN_Client (IKE1)
本装置の LAN 側のネットワークアドレス	192. 168. 10. 0/24
相手側の LAN 側のネットワークアドレス	空欄
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS (DH グループ)	使用する(Group2)
ライフタイム	28800(秒)
DISTANCE	1

使用するIKEポリシー名の選択	VPN_Client (IKE1) 💌
本装置側のL4N側のネットワークアドレス	192.168.10.0/24 (第1:192.168.00/24)
相手側のLAN側のネットワークアドレス	(例:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	 使用する 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SADライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

VPN クライアントに対して IPsec 通信を行う IP アドレスの範囲を設定します。 携帯端末が動的 IP のため、「相手側の LAN 側のネットワークアドレス」について、この項目を"空欄"に 設定します。

【IPsec サーバ】

Pseott—11	停止	⊙起動
-----------	----	-----

IPsec サーバ機能を起動します。

1-2-2. VPN クライアント(携帯端末)

ポイント

DOVPN をインストールした携帯端末と XR との IPsec 接続になります。 本設定例では、IKE モードとしてアグレッシブモードを使用しています。

<<ポリシーの新規作成>>

NOVPN				X
Log in	Policy	•		
Status				
 ■ 				
		TRIAL		
Option	S	A	Tools	

DOVPN を起動すると、上記画面が表示されます。

DOVPN	X
Log in Policy	
Status	
Execute after login	
Settings	
Conne Edit s	
Policy New TRIAL	
<u>D</u> elete A	Tools

「Option」をタップし、リストから「Policy」->「New」を選択します。

N DOVPN		ok
New Policy Name	xr	
ОК	A	Cancel

「New Policy Name」の項目でポリシー名を設定します。 本設定例では「xr」と設定しています。 設定後、「OK」をタップします。

<<Gatewayの設定>>

NOVPN			×
Save Gateway Gateway Gateway type	/ay 🔻	Cancel	
Gateway address KeyMobile / PKI Perfect forward sec	10.10.10.1		
		A	

「Gateway type」でプルダウンメニューより「NetScreen Series」をタップします。

「Gateway address」の項目には、XRの WAN 側 IP アドレスを設定します。本設定例では「10.10.10.1」を設定しています。

「KeyMobile/PKI」の項目は、チェックの必要はありません。

「Perfect forward secrecy (PFS)」の項目は、PFSを使用する場合は、チェックします。本設定例では チェックをしています。 <<Account の設定>>

POVPN			X
Save	ount 👻	Cancel	
Account Extended authen	tication (XAUTH)		
Generic Xauth		~	
Group name			
Group password			
User name	dovpn		
User password	****		
		A	

XAUTH は使用しないため、「Extended authentication」の項目は、チェックの必要はありません。 「User name」の項目では、XRの IKE/ISAKMP 設定で設定したインタフェースの ID を設定します。 本設定例では、「dovpn」を設定しています。

「User password」の項目では、XRの IKE/ISAKMP 設定で設定した Pre shared key(PSK)を設定します。 本設定例では、「ipseckey」を設定しています。

<<IKE Proposalsの設定>>

NOVPN		×
Save IKE F	Proposals 👻 Cancel	
The Proposals		
Group	Group 2 (DH1024) 🛛 🔫	
Cipher	AES128 👻	
Hash	SHA 👻	
Lifetime (s)	3600	
	<u> </u>	

IKE Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」,「Cipher」は「AES128」,「Hash」は「SHA」を選択して います。

また IKE Lifetime も設定可能です。

本設定例では、「3600秒」を設定しています。

<<IPSec Proposalsの設定>>

NOVPN		X
Save IPSec	Cancel	
Group	Group 2 (DH1024) 👻	
Cipher	AES128 🗸	
Hash	SHA 🔻	
Lifetime (s)	3600	
	A	

IPSec Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」,「Cipher」は「AES128」,「Hash」は「SHA」を選択して います。

また IKE Lifetime も設定可能です。

本設定例では、「3600秒」を設定しています。

<<Subnets の設定>>

POVPN		×
Save	ets 🔻 Cancel	
[Subnets		
Subnet 1 IP	192.168.10.0	
Subnet 1 mask	255.255.255.0	
Subnet 2 IP	0.0.0.0	
Subnet 2 mask	0.0.0.0	
Subnet 3 IP	0.0.0.0	
Subnet 3 mask	0.0.0.0	
	<u>_</u>	

ここでは IPsec 経由でアクセスしたいネットワークを設定します。

本設定例では対向XRのLAN側ネットワークアドレス「192.168.10.0」, サブネットマスク「255.255.255.0」 を設定しています。

NOVPN					×
Save	ts 🔻	Cancel]		
[Subnets			1		
Subnet 1 IP	192.168.10.0				
Subnet 1 mask	255.255.255.0				
Subnet 2 IP	0.0.0.0				
Subnet 2 mask	0.0.0.0				
Subnet 3 IP	0.0.0.0		3		
Subnet 3 mask	0.0.0.0				
The second s		A	-		

設定完了後、「Save」をタップします。

P DOVPN
Save Subnets Cancel
Subnets
Subnet 1 IP
保存 - ×r Subnet 1 m
Subnet 2 IF パリシーを保存しますか?
Subnet 2 m
Subnet 3 IF はい いいえ
Subnet 3 mask
Δ

「Save」タップ後、「ポリシーを保存しますか?」と表示されますので、「はい」をタップします。

POVPN
Save Subnets Cancel
Subnet 1 ma Subnet 2 IP Subnet 2 ma Subnet 2 ma ポリシーを保存しました。
Subnet 3 IP Subnet 3 mask 0.0.0.0

これで設定完了です。

<<IPsec の接続>>



先ほど作成したポリシー「xr」が選択されている状態で「Log in」をタップすることにより IPsec 接続 を開始します。

ログイン中(接続完了)の場合、ウインドウが以下のように変わります。



なおログアウト中は以下の表示になります。



また VPN ウインドウではログイン中の場合、以下のように表示されます。

N DOVPN	×
Log out Policy Xr	*
Status	
Done Aggressive Mode Initiating Quick Mode Sending 92 bytes to 10.10.10.1:500 at 14: Sending 300 bytes to 10.10.10.1:500 at 14 Received 300 bytes from 10.10.10.1:500 at Done Quick Mode Sending 60 bytes to 10.10.10.1:500 at 14: Login successful!	▲ 228 4:22 11 1 = 228 ▼
Power off timer disabled	▶ IIII FRIAL
Options	Tools

2. センター経由での IPsec 通信設定例

本設定例では、DOVPNのデフォルトルートをセンター側 XR とすることでセンター経由で拠点側 LAN へも アクセス可能とし、インターネットアクセスもセンター側 XR 経由でアクセスします。

また本設定例では、XR に関しましては IPsec 設定に関してのみ記載(センター側のみ DNS サーバ設定あ り)しております。その他の設定に関しましては、インターネット VPN 設定例集 IPsec 編の「IPsec を 利用したセンター経由インターネット接続例」をご参照下さい。

2-1. 構成例



2-2. 設定例

2-2-1. センタールータ(XR_A)

ポイント

XR_B(拠点)および携帯端末と IPsec 接続するための設定を行います。

XR_B(拠点)および携帯端末は動的 IP のため、IKE モードとしてアグレッシブモードを使用しています。 携帯端末が IPsec 経由で名前解決ができるように、DNS キャッシュ機能を起動しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定1]

インターフェースのIPアドレス	10.10.10.1	
上位ルータのIPアドレス	%ррр0	
インターフェースのID		(例:@xr.centurysys)

XRの WAN 側インタフェースの IP アドレス,および上位ルータの IP アドレスを設定します。PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_B
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	0.0.0.0
上位ルータのIPアドレス	
インターフェー スのID	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード 💌
	1番目 group2-aes128-sha1 💌
	2番目 使用しない 💌
transformU)ag.p.	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 彩 (1081~28800秒まで)

XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定		
 PSKを使用する PSAを使用する (v500を使用する場合は PSAL設定してください) 	ipseckey1	

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

🔘 使用する 🔍 使用しない 💿 Responderとして使用する 🔍 On-Demandで使用する

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B(IKE1)
本装置側のL4V側のネットワークアドレス	0.0.0/0 (第192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (第1:192.168.0.0/24)
FH2のTransFormの選択	aes128-sha1 💌
PFS	⊙ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IKE/ISAKMPの設定2]

IKE/ISAKMPポリシー名	VPN_Client	
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	0.0.0.0	
上位ルータのIPアドレス		
インターフェー スのレ	@dovpn (例:@xr.centurysys)	
モードの設定	aggressive モード 💌	
	1∰目 group2-aes128-sha1 💌	
	2番目 使用しない 💌	
transformU)aste	3番目 使用しない 🔽	
	4番目 使用しない 💌	

VPN クライアントに対する IKE/ISAKMP ポリシーを設定します。

XR における ID の設定では"@"を付けますが、DOVPN 側では、"@"を付けない形式で設定してください。 DOVPN でも"@"を付けて設定すると接続できません。

鍵の設定		
 PSKを使用する PSAを使用する (0500を使用する場合は RSAに設定してくたさい) 	ipseckey2	

事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

○ 使用する ○ 使用しない ⊙ Responderとして使用する ○ On-Demandで使用する

VPN クライアントの IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	VPN_Client (IKE2) 💌
本装置側のL4N側のネオワークアドレス	0.0.0.0/0 (第:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	(例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1 💌
PFS	⊙ 使用する ○ 使用しない
DH Groupの選択(PFS使用時に有効)	eroup2
SADライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 0~255まで)

VPN クライアントに対して IPsec 通信を行う IP アドレスの範囲を設定します。 携帯端末が動的 IP のため、「相手側の LAN 側のネットワークアドレス」について、この項目を"空欄"に 設定します。

【IPsec サーバ】



IPsec サーバ機能を起動します。

【DNS キャッシュ】

DNSキヤッパノユ	○停止	⊙起動	
-----------	-----	-----	--

携帯端末が IPsec 経由で名前解決ができるように、DNS キャッシュ機能を起動します。

2-2-2. 拠点ルータ(XR_B)

ポイント

XR_A(センター)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、IKE モードとしてアグレッシブモードを使用しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

インターフェー スのIPアドレス	%ррр0	
上位ルータのIPアドレス		
インターフェー スのID	@ipsec1	(例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」, インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMPの設定1]

IKE/ISAKMPポリシー名	XR_A
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	10.10.10.1
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	aggressive モード 💌
	1番目 group2-aes128-sha1 💌
	2番目 使用しない 💌
transformu) as a	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 科 (1081~28800科まで)

XR_A(センター)に対する ISAKMP ポリシーの設定を行います。

鍵の設定		
 PSKを使用する PSAを使用する (x509を使用する場合は RSAに設定してくたさい) 	ipseckey1	

事前共有鍵(PSK)として「ipseckey1」を設定します。

[IPsec ポリシーの設定 1]

● 使用する
 ● 使用しない
 ○ Responderとして使用する
 ○ On-Demandで使用する

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) 💌		
本装置側のL4N側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)		
相手側のLAN側のネットワークアドレス	0.0.0/0 (例:192.168.0.0/24)		
FH2のTransFormの選択	aes128-sha1 💌		
PFS	⊙ 使用する ○ 使用しない		
DH Groupの選択(FFS使用時に有効)	group2		
SADライフタイム	28800 秒 (1081~86400秒まで)		
DISTANCE	1 (1~255まで)		

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。 この例では、IPsec 通信を行う宛先 IP アドレスを「0.0.0.0/0」に設定しています。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option1 <u>米</u>	動作option 2 <u>米</u>	interface	backup SA
1		192.168.20.1	192.168.10.1	30	3	60			ipsec0 💌	

XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsec#-15	○停止	⊙起動	

IPsec サーバ機能を起動します。

2-2-3. VPN クライアント(携帯端末)

ポイント

DOVPN をインストールした携帯端末と XR_A (センター) で IPsec 接続を行います。

XR_A(センター)経由で拠点およびインターネット側への通信をするため、Subnets 設定で「0.0.0.0/0」 を設定しています。

また IPsec 経由での名前解決用に DNS 設定を行っています。

本設定例では、IKE モードとしてアグレッシブモードを使用しています。

<<ポリシーの新規作成>>

NOVPN		×
Log in	Policy 🔽	
Status		
	~	
	TRIAL	
Option	5 <u>A</u>	Tools

DOVPN を起動すると、上記画面が表示されます。

DOVPN	×
Log in Policy	
Status	
A	
<u>Execute after login</u>	
Settings	
<u>Conne</u> <u>Edit</u> s	
Policy New TRIAL	
<u>D</u> elete	Tools

「Option」をタップし、リストから「Policy」->「New」を選択します。

NOVPN		ok
New Policy Name	xr	
ОК	A	Cancel

「New Policy Name」の項目でポリシー名を設定します。 ここでは「xr」と設定しています。 設定後、「OK」をタップします。

<<Gatewayの設定>>

NOVPN			×
Save Gateway Gateway Gateway type	/ay 🔻	Cancel	
Gateway address KeyMobile / PKI Perfect forward sec	10.10.10.1		
		A	

「Gateway type」でプルダウンメニューより「NetScreen Series」をタップします。

「Gateway address」の項目には、XRの WAN 側 IP アドレスを設定します。本設定例では「10.10.10.1」を設定しています。

「KeyMobile/PKI」の項目は、チェックの必要はありません。

「Perfect forward secrecy (PFS)」の項目は、PFSを使用する場合は、チェックします。本設定例では チェックをしています。 <<Account の設定>>

NOVPN			X
Save	int 🔻	Cancel	
Account Extended authentication (XAUTH)			
Generic Xauth		∇	
Group name			
Group password			
User name	dovpn		
User password	****		
		A	

XAUTH は使用しないため、「Extended authentication」の項目は、チェックの必要はありません。 「User name」の項目では、XRの IKE/ISAKMP 設定で設定したインタフェースの ID を設定します。 本設定例では、「dovpn」を設定しています。

「User password」の項目では、XRの IKE/ISAKMP 設定で設定した Pre shared key(PSK)を設定します。 本設定例では、「ipseckey2」を設定しています。

<<IKE Proposalsの設定>>

NOVPN		×				
Save IKE P	Save IKE Proposals Cancel					
IKE Proposais						
Group	Group 2 (DH1024) 👻					
Cipher	AES128 👻					
Hash	SHA 👻					
Lifetime (s)	3600					
	A					

IKE Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」,「Cipher」は「AES128」,「Hash」は「SHA」を選択して います。

また IKE Lifetime も設定可能です。

本設定例では、「3600」秒を設定しています。

<<IPSec Proposalsの設定>>

NOVPN		×
Save IPSec	CProposals Cancel	
Group	Group 2 (DH1024) 👻	
Cipher	AES128 -	
Hash	SHA 🔻	
Lifetime (s)	3600	
	A	

IPSec Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」,「Cipher」は「AES128」,「Hash」は「SHA」を選択して います。

また IKE Lifetime も設定可能です。

本設定例では、「3600」秒を設定しています。

<<Subnets の設定>>

N DOVPN		X
Save Subr	nets	
[Subnets		
Subnet 1 IP	0.0.0.0	
Subnet 1 mask	0.0.0.0	
Subnet 2 IP	0.0.0.0	
Subnet 2 mask	0.0.0.0	
Subnet 3 IP	0.0.0.0	
Subnet 3 mask	0.0.0.0	
	<u>.</u>	

ここでは IPsec 経由でアクセスしたいネットワークを設定します。

本設定例ではセンター側 LAN, 拠点側 LAN およびインターネットアクセスを IPsec 経由で行いますので、 「Subnet 1 IP」および「Subnet 1 mask」は「0.0.0.0」と設定します。 <<DNS/WINS の設定>>

NOVPN			×
Save DNS/ DNS/WINS Query DNS	WINS 🔻 C	ancel	
Primary DNS	192.168.10.1		
Secondary DNS	0.0.0.0		
Primary WINS	0.0.0.0		
Secondary WINS	0.0.0.0		
Domain suffix			
		4	

ここでは DNS サーバの設定をします。

本設定例ではセンター側 XR で DNS 機能を有効にしていますので、Primary DNS サーバの IP アドレスと して「192.168.10.1」を設定しています。

NOVPN			×
Save DNS/V	VINS 🔻	Cancel	
Query DNS			
Primary DNS	192.168.10.1		
Secondary DNS	0.0.0.0		
Primary WINS	0.0.0.0		
Secondary WINS	0.0.0.0		
Domain suffix			
		A	

設定完了後、「Save」をタップします。

POVPN				
Save Subnets Cancel				
Subnets				
Subnet 1 IP				
Subnet 1 m				
Subnet 2 IF (ポリシーを保存しますか?				
Subnet 2 m				
Subnet 3 IF はい いいえ				
Subnet 3 mask 10.0.0.0				
A				

「Save」タップ後、「ポリシーを保存しますか?」と表示されますので、「はい」をタップします。

POVPN
Save Subnets Cancel Subnets Subnet 1 IP 192.168.10.0 Subnet 1 Im 成功 ok Subnet 2 IP ボリシーを保存しました。 Subnet 3 IP Subnet 3 mask

これで設定完了です。

<<IPsec の接続>>

POVPN		×
Log in Po	licy 🛛 🕶	
Status		
	<u> </u>	
▲ III	► ►	
	TRIAL	
Options	<u>A</u>	Tools

先ほど作成したポリシー「xr」が選択されている状態で「Log in」をタップすることにより IPsec 接続 を開始します。

ログイン中(接続完了)の場合、ウインドウが以下のように変わります。



3. サポートデスクへのお問い合わせ

3-1. サポートデスクへのお問い合わせに関して

XR 製品に関してサポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応 させて頂くことが可能ですので、ご協力をお願い致します。

- ご利用頂いている XR の製品名およびバージョン番号
- ご利用頂いているネットワーク構成
- 不具合の内容および不具合の再現手順(何を行った場合にどのような問題が発生したのかをできる だけ具体的にお知らせ下さい)
- VPN クライアントと接続する、または接続している XR の設定ファイル, ログ, IPsec のステータス 情報(取得方法に関しましては、ご利用頂いている製品のユーザーズガイドをご参照下さい)
- DOVPN を XR 製品以外でご利用頂く場合に関しましては、ご購入された代理店および販売店様へお問い合わせ下さい。

3-2. サポートデスクのご利用に関して

電話サポート

電話番号:0422-37-8926

電話での対応は以下の時間帯で行います。

月曜日 ~ 金曜日 10:00 AM - 5:00 PM

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail: <u>support@centurysys.co.jp</u>

FAXサポート

FAX 番号:0422-55-3373

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため 停止する場合があります。 その際は弊社ホ ームページ等にて事前にご連絡いたします。

FutureNet XR Series ⇔ DOVPN 接続設定ガイド

Ver1.0.0

2008年3月

発行 センチュリー・システムズ株式会社 2008 CENTURYSYSTEMS INC.ALL rights reserved.