3-2. XAuth を利用したユーザ認証

オプションで VPN 接続時に ID とパスワードを必要とするユーザ認証を行うことが可能です。

・Secure VPN Client では以下の拡張認証のチェックを有効にするだけです。

規則のプロパティ 🔹 💽 🔀			
全般	羊糸田		
ሀቺ-ኑ:	エンドポイント ――		
	ゲートウェイ IP アドレス:	10.0.0.220	P
J.	リモート ネットワーク:	lan	✓ …
IPsec /	IKE 候補		
?	認証鍵:	🕬 testkey	~
0	候補テンプレート	normal	*
			設定
🗌 仮想	見IP アドレスを取得する		
-	仮想 IP アドレスは、内部ネ です。	ットワークのアドレス	設定
☑菰弭			
		XAuth、RADIUS、 となる場合がありま	
6/L ⁴ /1			変更(<u>C</u>)
		ОК	キャンセル

・SSG では各ユーザ設定の変更、及びフェーズ1にあたる設定を変更する必要があります。

・左欄の Objects -> Users -> Local Groups を選択し、変更したいユーザをグループから一 旦外して OK を選択します。

SSG5-ISDN	Group Name vpn-group
Configuration Network Centry Centry Delicy VPNs Objects Users Local Local Centry External Groups External Groups	< Group Members> testuser2 <<
	OK Cancel

・同じく Users -> Local から当該ユーザを Edit で選択し、XAuth User にチェックを入れ るとともに User Password の欄にパスワードを設定します。

SSG5-ISDN	A	uth/IKE/XAuth/L2TP User
Home	User Name testuser	
Network	Status 💿 Enable	O Disable
 + Security + Policy + VPNs 	☑ IKE User	Number of Multiple Logins with Same ID 1
- Objects - Users - Local	IKE ID Type U-FODN V	IKE Identity testuser@dit.com
- Local Groups - External Groups - IP Pools	Authentication User	User Password
Certificates Reports Wizards Kolp	XAuth User	Confirm Password

・再度、Local Groups から該当するグループを選択し、ユーザをグループに再度追加します。

Von-droup	
vpn group	< Available Members>
	testuser
>>	
OK Cancel]
	vpn-group >> OK Cancel

・ついで、左欄のメニューのVPNsからフェーズ1の設定変更を行います。VPNs -> AutoKey Advanced -> Gateway を選択、Configure から XAuth を選択します。

		Gateway Name: p1
	SSG5-ISDN	⊙ None
+ +	- Home - Configuration - Network	 XAuth Server Allowed Authentication Type O Generic CHAP Only CHAP & PAP Use Default Xauth Settings
•	- Security - Policy	Local Authentication O Allow Any
	VPNs AutoKey IKE AutoKey Advanced Gateway	User None User Group None External Authentication None O allow Apy Query Remote Setting
	 P1 Proposal P2 Proposal XAuth Settings VPN Groups Manual Key 	O User Name O User Group Name O Bypass Authentication

XAuth Server にチェックを入れ、OK で終了します。

XAuth Server
 Allowed Authentication Type O Generic O CHAP Only O CHAP & PAP
 Use Default Xauth Settings

・以上の設定でユーザ認証が有効となりました。

・Secure VPN Client のタスクトレイアイコンから実際に接続を行うと下記のようにユーザ 名とパスワードを求められますので設定したユーザ名とパスワードを用いて接続を行うこ とが可能です。

NET-G Secure VPN Client 🛛 🔀		
	接続します:10.0.0.220 (lan)	
	ユーザ名: testuser パスワード: ******* このユーザー名とパスワードを保存する(<u>5</u>)	
	<u>ок</u> <i>キャンセル</i>	

・以下はユーザ認証が成功した際の SSG のログです。

Date / Time	Level	Description
2010-05-24 14:58:54	info	IKE 10.0.0.200 Phase 2 msg ID 4ed9a365: Completed negotiations with SPI 5b64604d, tunnel ID 32786, and lifetime 3600 seconds/409600 KB.
2010-05-24 14:58:54	info	IKE 10.0.0.200 Phase 2 msg ID 4ed9a365: Responded to the peer's first message.
2010-05-24 14:58:54	info	IKE 10.0.0.200: XAuth login was passed for gateway p1, username testuser, retry: 0, Client IP Addr 0.0.0.0, IPPool name: , Session-Timeout: 0s, Idle-Timeout: 0s.
2010-05-24 14:58:53	info	IKE 10.0.0.200 Phase 1: Completed Aggressive mode negotiations with a 28800-second lifetime.
2010-05-24 14:58:53	info	IKE 10.0.0.200 Phase 1: Completed for user testuser.
2010-05-24 14:58:53	info	IKE<10.0.0.200> Phase 1: IKE responder has detected NAT in front of the remote device.
2010-05-24 14:58:53	info	IKE 10.0.0.200 Phase 1: Responder starts AGGRESSIVE mode negotiations.