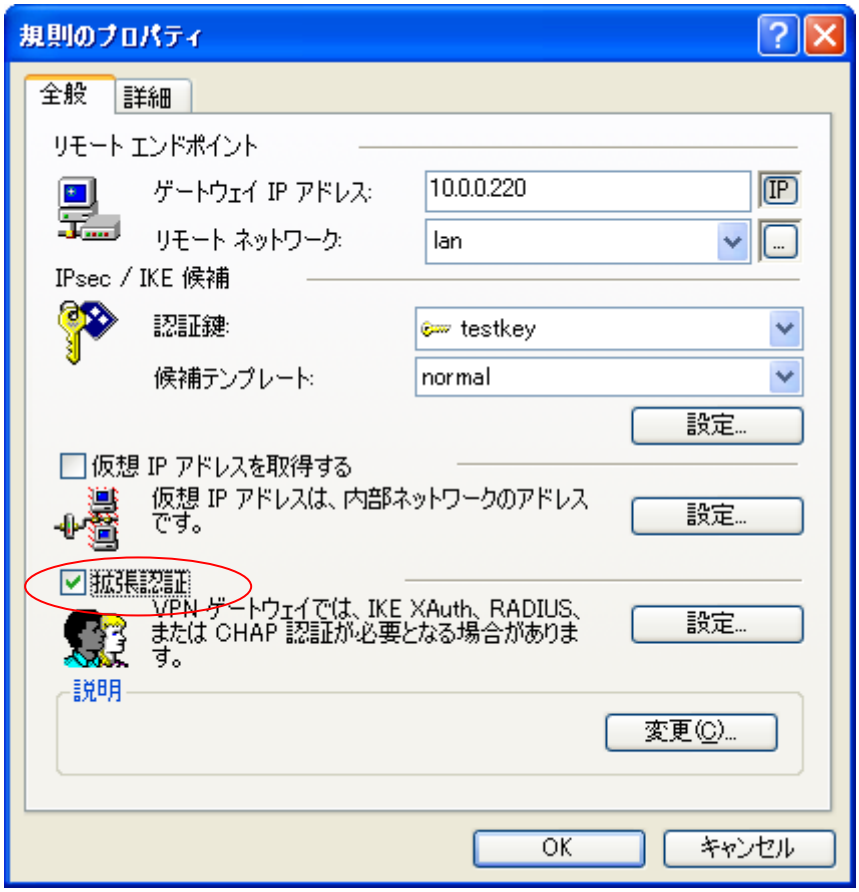
3-2. XAuth を利用したユーザ認証

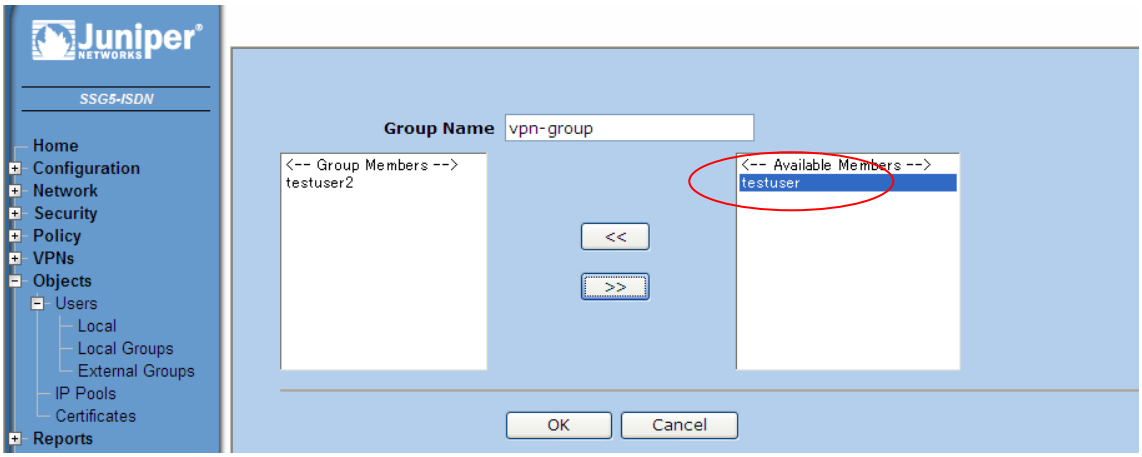
オプションで VPN 接続時に ID とパスワードを必要とするユーザ認証を行うことが可能です。

・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。

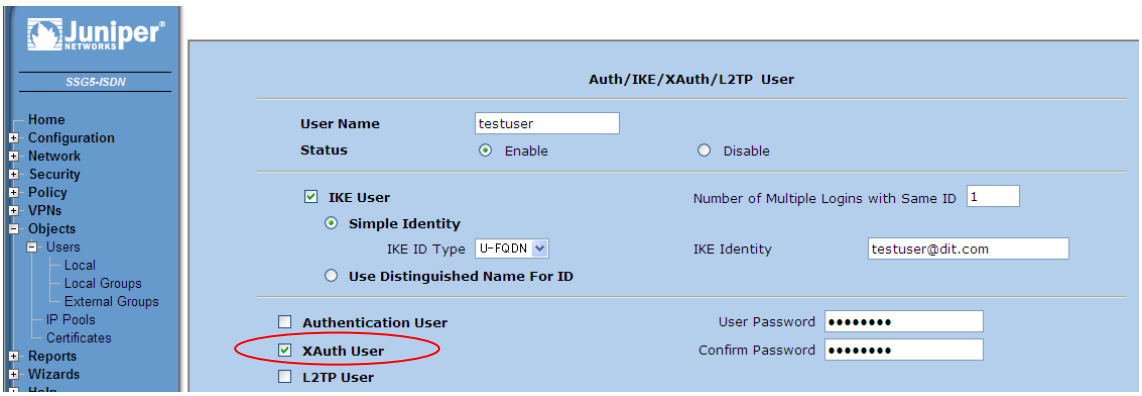


・SSG では各ユーザ設定の変更、及びフェーズ 1 にあたる設定を変更する必要があります。

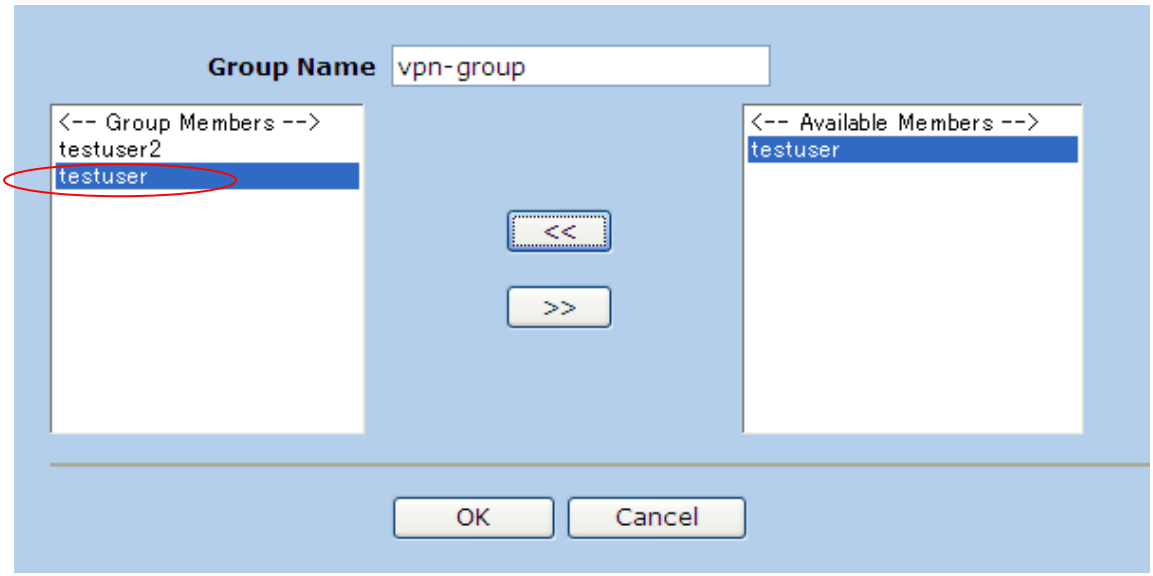
・左欄の Objects -> Users -> Local Groups を選択し、変更したいユーザをグループから一旦外して OK を選択します。



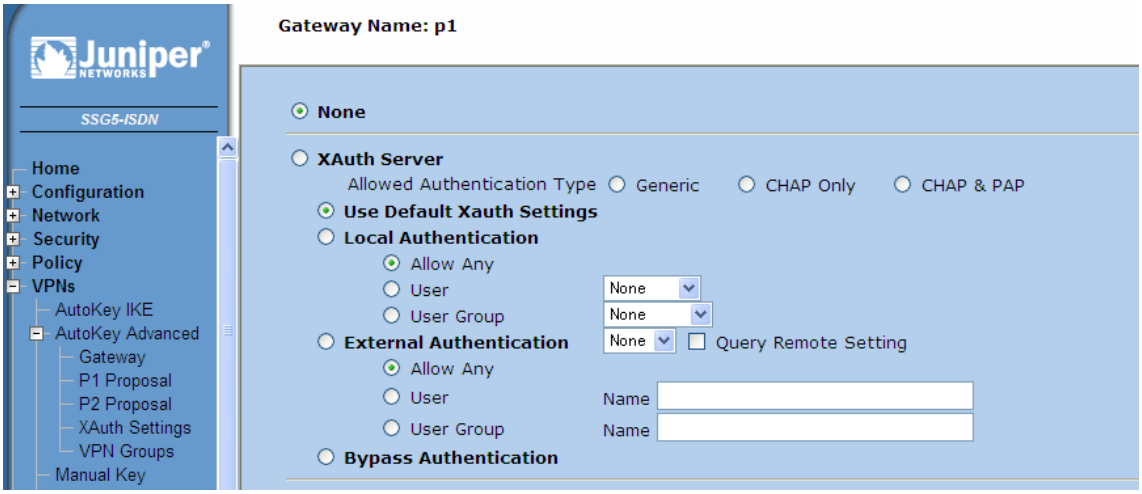
・同じく Users -> Local から当該ユーザを Edit で選択し、XAuth User にチェックを入れるとともに User Password の欄にパスワードを設定します。



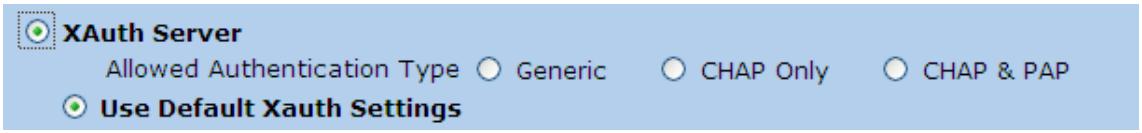
・再度、Local Groups から該当するグループを選択し、ユーザをグループに再度追加します。



・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。

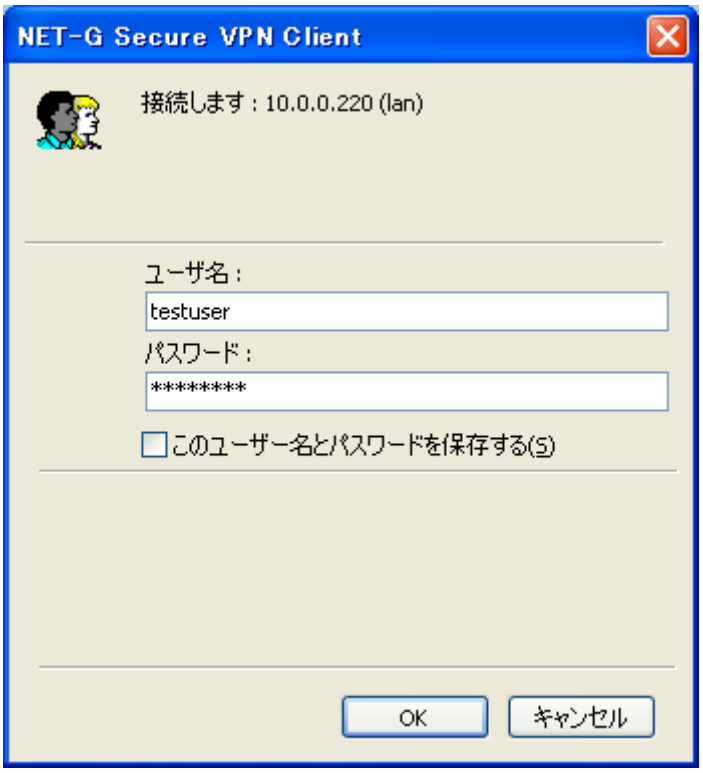


XAuth Server にチェックを入れ、OK で終了します。



・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。



・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.