

# 2

## VPNサーバーの 設定

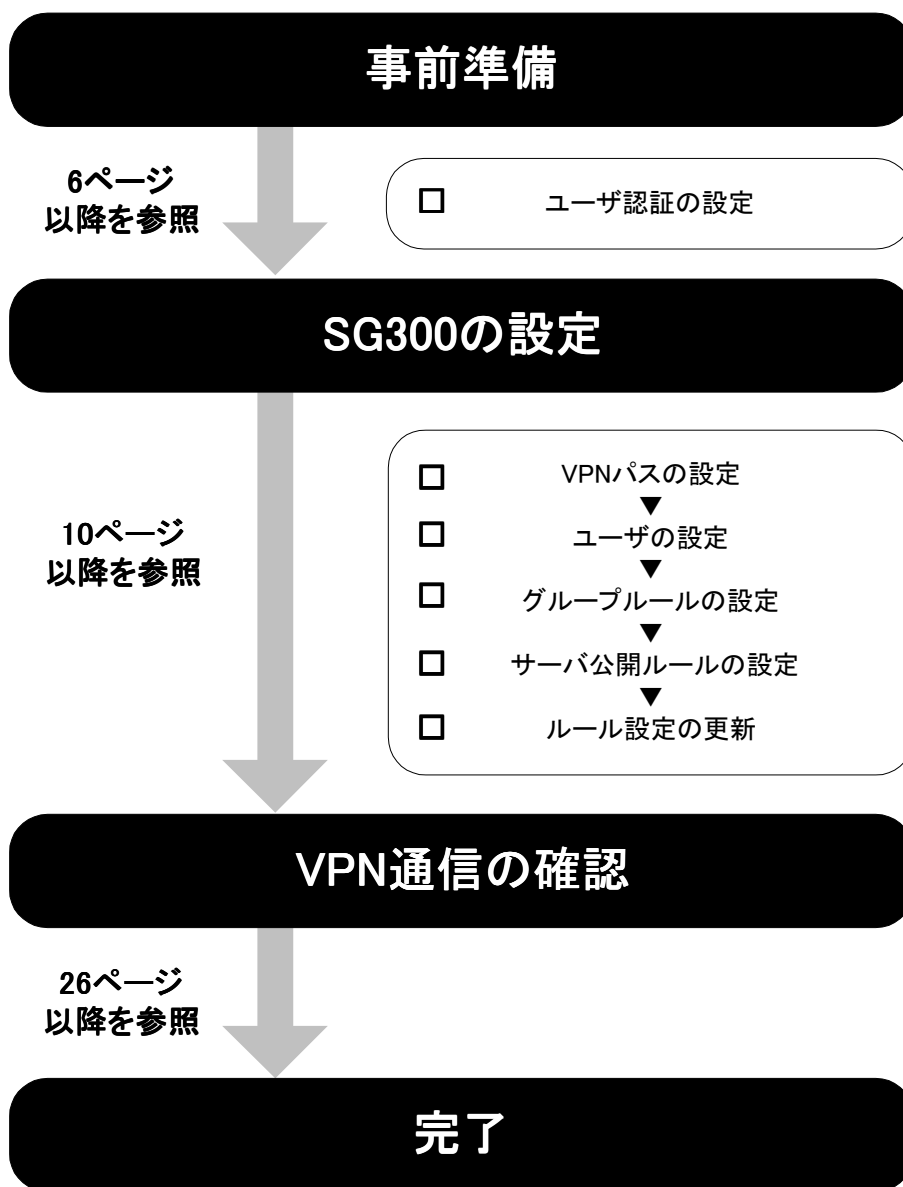


本章では、SG300側で行うリモートアクセスVPNの設定について、順番に説明します。

作業の流れ (→6ページ) .....	SG300側での作業の流れをフロー図で説明します。
SG300の設定 (→10ページ) .....	VPN構築に必要な設定方法について説明します。
VPN通信の確認 (→26ページ) .....	VPN通信が正しく行われているかをログで確認する方法について説明します。

# 作業の流れ

リモートアクセスVPN環境を構築する場合、SG300側では図のような流れで作業を行います。



# 事前準備

リモートアクセスVPN環境を構築するには、ユーザ認証が必須となります。そのため、VPN設定前の事前準備として、かんたん設定でユーザ認証が利用できるように設定しておく必要があります。



チェック

本書では、リモートアクセスVPNを利用するユーザをuser\_tokyoとし、ユーザ (user\_tokyo)が所属するグループをvpn\_groupとしています。  
ユーザの設定の詳細はP14「ユーザの設定」を参照してください。

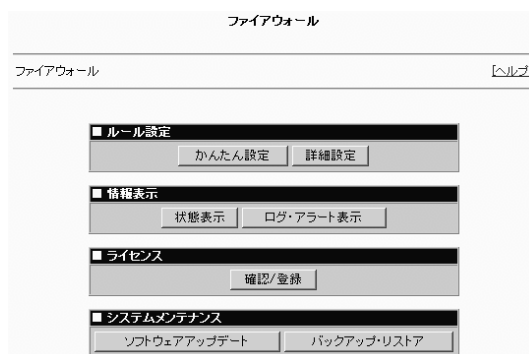
## ユーザ認証の設定

かんたん設定でユーザ認証を利用可能にします。

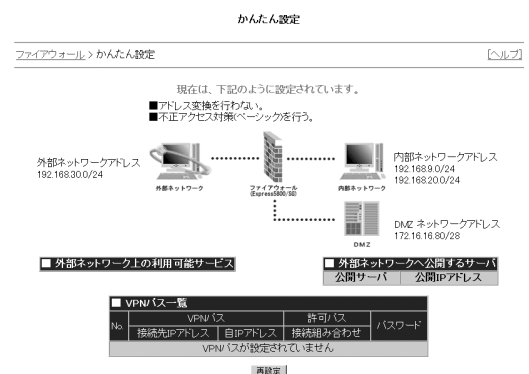
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。  
ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[かんたん設定]をクリックする。  
設定内容確認画面が表示されます。

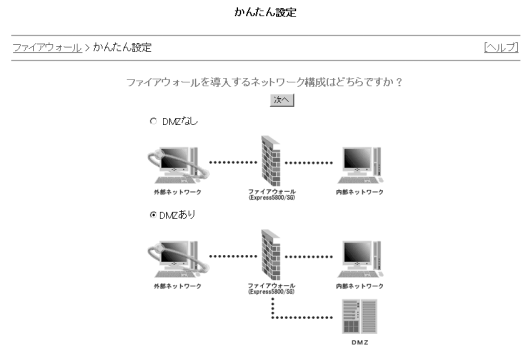


3. [再設定]をクリックする。  
ネットワークの構成の選択画面が表示されます。



4. [次へ]をクリックする。

同様にユーザ認証の利用選択画面が表示されるまで、[次へ]をクリックする。  
ユーザ認証の利用選択画面が表示されま  
す。

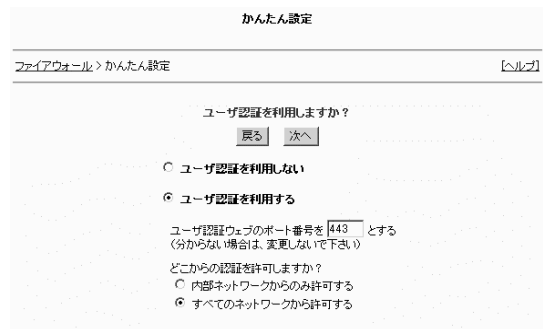


ヒント

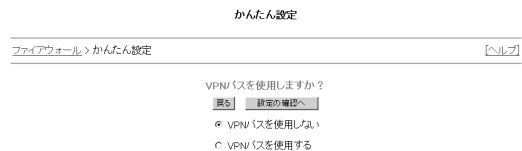
ネットワークの構成選択画面からユーザ認証の利用選択画面までの遷移は以下のとおり  
です。

ネットワークの構成選択画面→インタフェース選択画面→ウェブサーバ公開の設定画面  
→メールサーバ公開の設定画面→ファイル転送サーバ公開の設定画面→ネームサーバ公  
開の設定画面→その他の公開サーバの設定画面→外部ネットワーク利用サービス選択の  
画面→より強固な不正アクセス対策の設定画面→ユーザ認証の利用選択画面

5. 「ユーザ認証を利用する」のラジオボタ  
ンと「すべてのネットワークから許可す  
る」のラジオボタンを選択し、[次へ]をク  
リックする。  
VPN利用選択画面が表示されます。



6. [設定の確認へ]をクリックする。  
設定内容確認画面が表示されます。



- [設定]をクリックする。  
ルール適用画面が表示されます。

かんたん設定

ヘルプ

ファイアウォール > かんたん設定

下記のように設定してよろしいですか？

アドレス変換を行う。  
 不正アクセス対策バナーを表示を行う。

外部ネットワークアドレス 192.168.30.0/24

内部ネットワークアドレス 192.168.0/24

DMZ ネットワークアドレス 172.16.16.0/25

■ 外部ネットワーク上の利用可能サービス		■ 外部ネットワークへ公開するサーバ	
サービス	内部IPアドレス	公開サーバ	公開IPアドレス
ウェブサービス(HTTP/HTTPS)		ウェブサーバ (HTTP)	192.168.30.51
メールサービス(SMTP)		メールサーバ (SMTP)	192.168.30.52
ファイル転送サービス(FTP)		ファイル転送サーバ (FTP)	192.168.30.53
ネームサービス(DNS)		ネームサーバ (DNS)	192.168.30.54
時刻同期サービス(NTP)		その他のサーバ	192.168.30.5
			192.168.30.5
			192.168.30.6

■ VPN サービス一覧			
No.	VPN ID	許可IP	パスワード
	接続先IPアドレス	自己IPアドレス	接続組み合わせ
1	192.168.80.1	192.168.30.93	192.168.20.0/24:192.168.100.0/24 *****
2	192.168.150.1	192.168.30.93	192.168.20.0/24:192.168.160.0/24 *****

戻る | やり直し | 設定

- [かんたん設定を終了]をクリックする。  
ファイアウォールメニュー画面に戻ります。

かんたん設定

ヘルプ

ファイアウォール > かんたん設定

下記のように設定しました。

アドレス変換を行う。  
 不正アクセス対策バナーを表示を行う。

外部ネットワークアドレス 192.168.30.0/24

内部ネットワークアドレス 192.168.0/24

DMZ ネットワークアドレス 172.16.16.0/25

■ 外部ネットワーク上の利用可能サービス		■ 外部ネットワークへ公開するサーバ	
サービス	内部IPアドレス	公開サーバ	公開IPアドレス
ウェブサービス(HTTP/HTTPS)		ウェブサーバ (HTTP)	192.168.30.51
メールサービス(SMTP)		メールサーバ (SMTP)	192.168.30.52
ファイル転送サービス(FTP)		ファイル転送サーバ (FTP)	192.168.30.53
ネームサービス(DNS)		ネームサーバ (DNS)	192.168.30.54
時刻同期サービス(NTP)			

■ VPN サービス一覧			
No.	VPN ID	許可IP	パスワード
	接続先IPアドレス	自己IPアドレス	接続組み合わせ
2	192.168.30.1	192.168.30.93	192.168.7.0/24:192.168.20.0/24 *****
2	192.168.30.1	192.168.30.93	192.168.7.0/24:192.168.30.93/32 *****

かんたん設定を終了

- 以上で、事前準備は終了しました。

# SG300の設定

リモートアクセスVPN環境を構築するためには、SG300(tokyo)側で以下の項目を設定しておく必要があります。

- VPNパスの設定
- ユーザ設定
- グループルールの設定
- サーバ公開ルールの設定

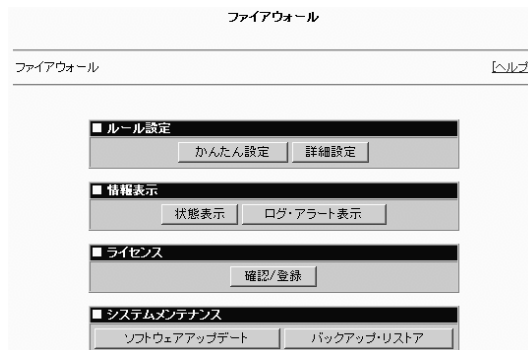
## VPNパスの設定

VPN環境を構築するためには、まずは、VPNパス（自動鍵交換：トランスポートモード）の設定を行います。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。  
ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。  
詳細設定メニュー画面が表示されます。



3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。  
VPN情報一覧画面が表示されます。



4. 「一覧の末尾にVPNパス（自動鍵交換：トランスポートモード）を『追加』をクリックする。
- VPNパス追加画面（自動鍵）が表示されます。

5. VPNパス追加画面（自動鍵）に表示される各項目を設定する。

	項目	設定内容
VPNパス	接続先IPアドレス	202.247.5.0/24
	自IPアドレス	202.247.5.136
	暗号化／認証	AES128 & MD5
	有効期間	3600
	共有秘密鍵	パスワード（プリシェアードシークレット）
	暗号化／認証（AH）	チェックしない
	暗号化／認証（ESP:暗号アルゴリズム）	AES128
	暗号化／認証（ESP:認証アルゴリズム）	HMAC MD5
	鍵の有効期間	28800
オプション	PFS (Perfect Forward Secrecy) の有効	チェックする
	IPSecで鍵更新を行う	チェックする

VPNパス設定

ファイアウォール > 詳細設定 > VPNパス設定 [ヘルプ]

一覧の末尾にVPNパス(共有鍵交換)を [追加]  
 一覧の末尾にVPNパス(自動鍵交換:トンネルモード)を [追加]  
 一覧の末尾にVPNパス(自動鍵交換:トランスポートモード)を [追加] 1頁に表示するレコード  
 選択したVPNパスを [削除] [20] 件 [戻検]  
 条件中 件目を表示 ← 前の件 | 次の件 →

VPNパス	許可パス	モード	鍵交換方式
接続先IPアドレス	自IPアドレス	接続組み合わせ	

VPNパスが設定されていません

全選択/解除 ← 前の件 | 次の件 →

■ VPNパス(自動鍵交換:トランスポートモード)

VPNパス

接続先IPアドレス 202.247.5.0/24  
 自IPアドレス 202.247.5.136  
 暗号化/認証 AES128 & MD5  
 有効期間(秒) 3600 (1200~28800)

Phase 1

共有秘密鍵  
 パスワード(プリシェアードシークレット)  
 \*\*\*\*\*  
 ※接続先VPN機器と同じ接続パスワード(英数字を組み合わせ、8文字以上500文字以内)  
 RSA鍵 [鍵IDの確認]  
 自ファイアウォールのRSA公開鍵を取得する [鍵の出力]  
 接続先VPN機器から取得した鍵ファイルを設定する [参照]

Phase 2

暗号化/認証 AH:  使用する(認証方式はMD5)  
 ESP:  
 暗号アルゴリズム AES128  
 認証アルゴリズム HMAC MD5  
 鍵の有効期間(秒) 28800 (1200~86400)

オプション  
 PFS(Perfect Forward Secrecy)の有効  
 IPSecで鍵更新を行う  
 [適用]



接続先 IPアドレスにはクライアント側のネットワークアドレスを指定します。



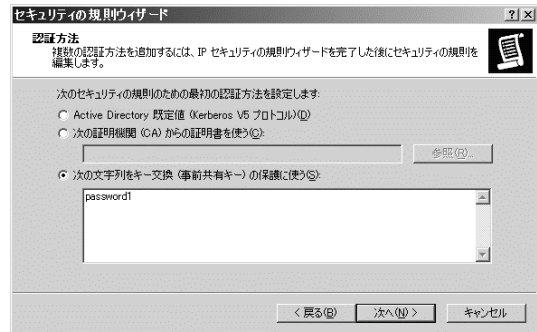
共有秘密鍵でパスワードを選択した場合、クライアントのパスワードと同じ文字列でなければなりません。

Windows XP（クライアント側）では、セキュリティ規則作成時の「認証方法」でパスワードを設定します。

パスワードは必ず英数字を組み合わせ、8文字以上500文字以内で入力します。

（右記の例では「password1」と記しています。）

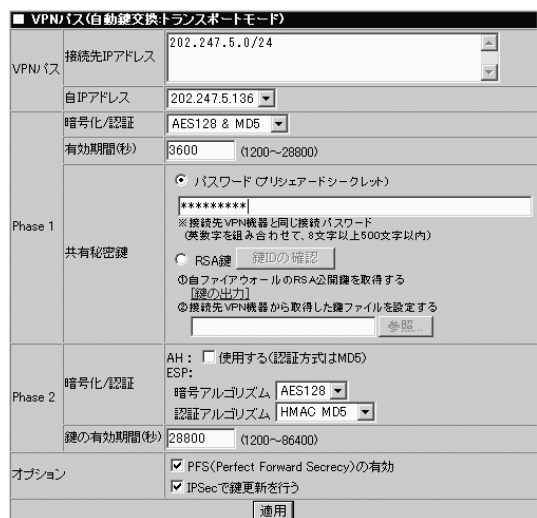
設定の詳細は『リモートアクセスVPNの設定（クライアント編）』P10「セキュリティ規則の作成」手順12を参照してください。



以上の設定項目はP4「VPN構築の前提条件」にあわせて一例として説明しています。接続先IPアドレス、自IPアドレス等は、適宜お客様の環境にあわせて設定してください。

## 6. [適用]をクリックする。

VPNパス登録結果画面（自動鍵）が表示されます。

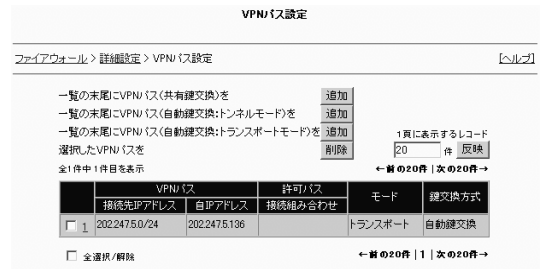




7. [VPNパス設定に戻る]をクリックする。  
追加したVPNパスが反映されたVPNパス設定画面が表示されます。



8. 追加したVPNパスが反映されていることを確認し、[詳細設定]をクリックする。  
詳細設定メニュー画面が表示されます。  
引き続きユーザの設定を行います。



# ユーザの設定

ユーザの作成、所属するグループの登録の各設定を行います。

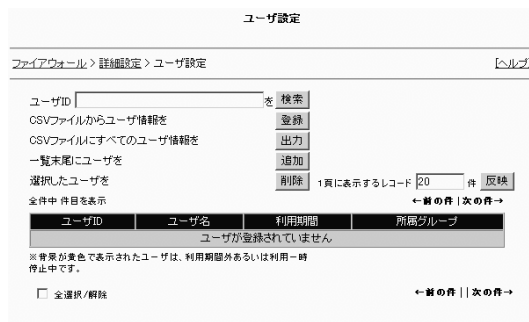
## ユーザの作成

ユーザの作成を行います。

1. 詳細設定メニューの「ユーザ設定」から  
[ユーザ設定]をクリックする。  
ユーザ情報一覧画面が表示されます。



2. 「一覧末尾にユーザを『追加』」をクリックする。  
ユーザ情報登録画面が表示されます。



3. ユーザ情報登録画面に表示される各項目  
を設定する。

項目	設定内容
ユーザ名	user_tokyo
ユーザID	user_tokyo
パスワード	6文字から256文字までの英数文字列
再パスワード	(上記と同じ文字列を入力)
備考	(空白)
利用期間	(任意の期間を指定)



項目	設定内容
利用を一時停止する	チェックしない

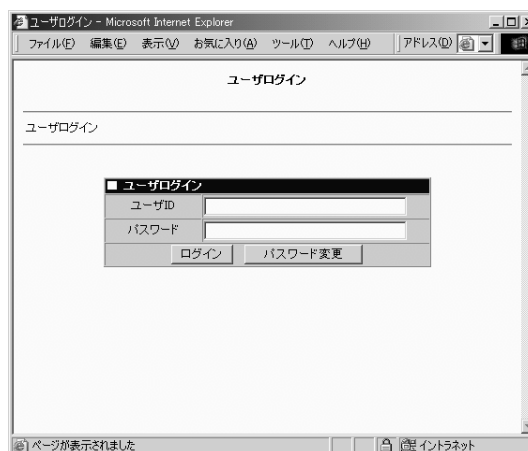


クライアント（Windows XP側）がインターネット経由で企業内ネットワークへアクセスする場合、まず、「ユーザログイン」が表示され、本項目で設定したユーザIDとパスワードの入力が必要になります。

本書では、リモートアクセスVPNを利用するユーザIDを

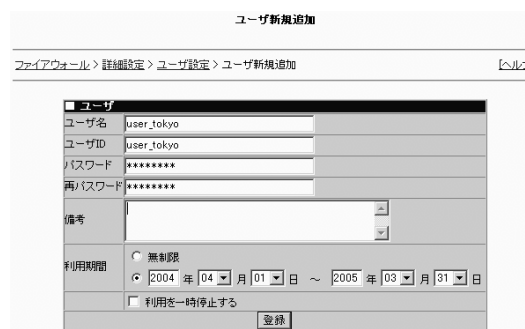
「user\_tokyo」とし、パスワードは英数文字列で6文字以上256文字以内としています。

詳細は『リモートアクセスVPNの設定（クライアント編）』P19「ユーザ認証」手順2を参照してください。



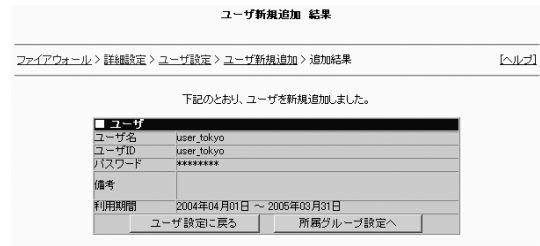
#### 4. [登録]をクリックする。

ユーザ情報登録結果画面が表示されます。



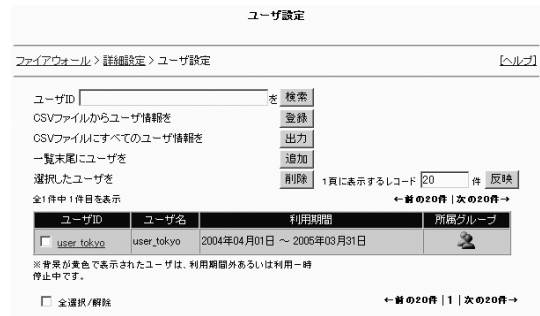
5. ユーザ情報登録結果画面の[ユーザ設定に戻る]をクリックする。

ユーザ情報一覧画面に戻ります。新しく登録されたユーザ情報が一覧に反映された形で表示されます。



6. ユーザ情報一覧画面を確認し、[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。引き続きユーザの設定（グループの作成）を行います。



## グループの作成

ここでは、グループの作成を行います。

7. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

グループ情報一覧画面が表示されます。

8. 「一覧末尾にグループを『追加』」をクリックする。

グループ情報登録画面が表示されます。

9. グループ情報登録画面に表示される各項目を入力する。

項目	設定内容
グループ名	vpn_group
利用期間	任意の期間を指定
備考	(空白)



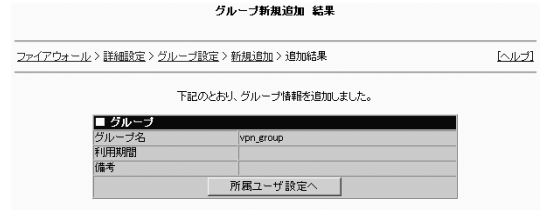
チェック

本書では、リモートアクセスVPNを利用するユーザをuser\_tokyoとし、ユーザ (user\_tokyo) が所属するグループをvpn\_groupとしています。

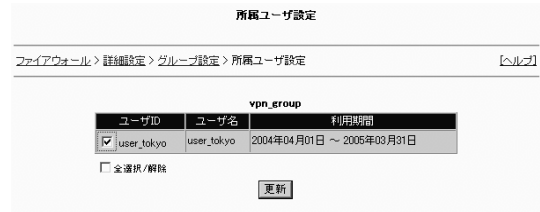
10. [登録]をクリックする。

グループ情報登録結果画面が表示されます。

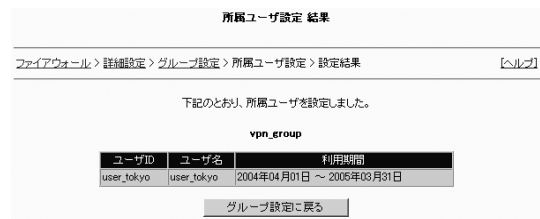
- 1 1. [所属ユーザ設定へ]をクリックする。  
所属ユーザ選択画面が表示されます。



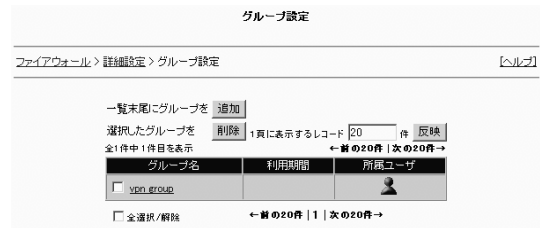
- 1 2. 先ほど作成したユーザ (user\_tokyo) のチェックボックスをチェックし、[更新] をクリックする。  
所属ユーザ登録結果画面が表示されます。



- 1 3. [グループ設定に戻る]をクリックする。  
グループ情報一覧画面に戻ります。新しく登録されたグループ情報が一覧に反映された形で表示されます。



- 1 4. グループ情報一覧画面を確認し、[詳細設定]をクリックする。  
詳細設定メニュー画面が表示されます。  
引き続きグループルールの作成を行います。



# グループルールの設定

グループルールを作成します。

1. 詳細設定メニューの「ルール設定」から[グループ設定]をクリックする。

グループ情報一覧画面が表示されます。

詳細設定

ファイアウォール > 詳細設定 [ヘルプ]

■ ルール設定

サイト共通ルール グループルール サーバ公開ルール 流入量制限ルール

アドレスグループ サービス

最終更新日: 2004年06月21日 17時25分34秒

最終更新状態に戻す 編集結果を適用

■ ユーザ設定

ユーザ設定 ロックアウト設定 グループ設定

■ VPN設定

VPNパス設定 VPNパラメータ設定

■ ログアラート設定

ログアラートファイル設定 アラートアクション設定

2. 「一覧末尾にグループルールを『追加』」をクリックする。

グループ選択画面が表示されます。

ルール設定(グループ)

ファイアウォール > 詳細設定 > ルール設定(グループ) [ヘルプ]

かみたん設定(ネットワーク構成)の確認

ルールの追加・削除・更新を行った場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックしてください。

一覧末尾にグループルールを 追加 削除

選択したルールを 1頁に表示するグループ 20 件 戻換

条件中 件目を表示 < 前の件 | 次の件 >

No.	発信元	宛先	通信種別	処理	記録
グループルールが登録されていません。					

全選択/解除 < 前の件 | 次の件 >

3. ルールを追加するグループ名 (vpn\_group) のラジオボタンをクリックし、「選択したグループのグループルールを『追加』」をクリックする。

選択したグループのルール一覧画面が表示されます。

グループ選択

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループ選択 [ヘルプ]

選択したグループのグループルールを 追加

グループ名	利用期間
<input checked="" type="radio"/> vpn_group	

4. 「一覧末尾に『追加』」をクリックする。個別ルール追加画面が表示されます。

グループルール

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール [ヘルプ]

vpn\_group

■ 認証有効時間

60 分

一覧末尾に 追加 削除

選択したルールを 削除

No.	発信元	宛先	通信種別	処理	記録
グループルールが登録されていません。					

全選択/解除

トランスポートVPNパスを 変更

VPNパス	モード	鍵交換方式
接続先IPアドレス	自IPアドレス	

トランスポートVPNパスが選択されていません。

登録

5. 個別ルール追加画面に表示される各項目を設定する。

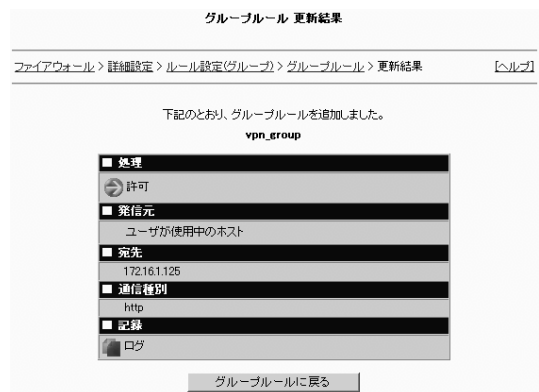
項目	設定内容
宛先	ユーザ指定（ラジオボタン）、172.16.1.125（テキストボックス）
通信種別	ユーザ指定（ラジオボタン）、http（テキストボックス）
記録	ログ



6. [登録]をクリックする。  
個別ルール追加画面が表示されます。



7. [グループルールに戻る]をクリックする。  
追加したルールが反映された、選択したグループのルール一覧画面が表示されます。



8. 「トランスポートVPNパスを『変更』」をクリックする。  
トランスポートVPNパス選択画面が表示されます。





9. 表示されるトランスポートVPNパスの中から先ほど設定したVPNパスのチェックボックスをチェックし、[登録]をクリックする。
- 選択したグループルールの一覧画面に戻ります。

項目	チェック内容
接続先IPアドレス	202.247.5.0/24
自IPアドレス	202.247.5.136
モード	トランスポートモード
鍵交換方式	自動鍵

10. 「認証有効時間」のテキストボックスに、ユーザ認証の後、ルールを有効にしておく時間を入力する。
- (右記の例では60[分]としています。)

11. [登録]をクリックする。
- グループルール登録結果画面が表示されます。

トランスポートVPNパス選択

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール > トランスポートVPNパス選択 [ヘルプ](#)

グループルールに登録するトランスポートVPNパスを選択してください。

VPNパス	モード	鍵交換方式
<input checked="" type="checkbox"/> 1 202.247.5.0/24	202.247.5.136	トランスポートモード

全選択/解除

グループルール

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール [ヘルプ](#)

vpn\_group

■ 認証有効時間

60 分

一覧末尾に

選択したルールを

No.	宛信元	宛先	通信種別	処理	記録
グループルールが登録されていません。					

全選択/解除

トランスポートVPNパスを

VPNパス	モード	鍵交換方式
<input type="checkbox"/> 1 202.247.5.0/24	202.247.5.136	トランスポートモード

トランスポートVPNパスが選択されていません。

グループルール

ファイアウォール > 詳細設定 > ルール設定(グループ) > グループルール [ヘルプ](#)

vpn\_group

■ 認証有効時間

60 分

一覧末尾に

選択したルールを

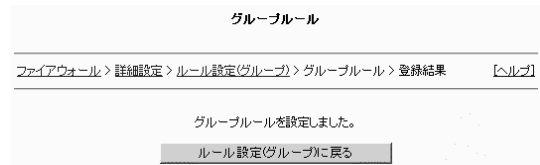
No.	宛信元	宛先	通信種別	処理	記録
<input type="checkbox"/> 1	ユーザが使用中のホスト	172.16.1.125	http		

全選択/解除

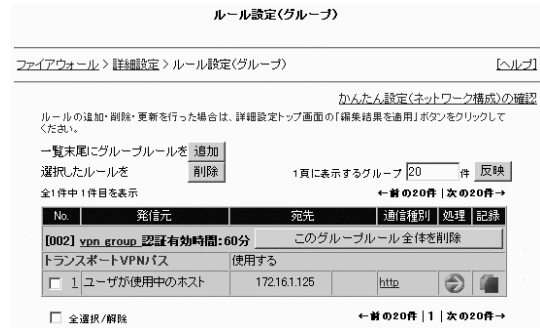
トランスポートVPNパスを

VPNパス	モード	鍵交換方式
<input checked="" type="checkbox"/> 1 202.247.5.0/24	202.247.5.136	トランスポートモード

12. [ルール設定(グループ)に戻る]をクリックする。  
グループ情報一覧画面が表示されます。



13. グループ情報一覧画面を確認し、[詳細設定]をクリックする。  
詳細設定メニュー画面が表示されます。  
引き続きサーバ公開ルールの設定を行います。



# サーバ公開ルールの設定

サーバ公開ルールを作成します。

1. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

サーバ公開ルール一覧画面が表示されま  
す。

2. 「一覧末尾にルールを『追加』」をクリックする。

サーバ公開ルール追加画面が表示されま  
す。

3. サーバ公開ルール追加画面に表示される  
各項目を設定する。

項目	設定内容
外部公開IPアドレス	202.247.5.136
内部IPアドレス	172.16.1.125
ポート	TCP (外部80→内部80)
記録	ログ

4. [登録]をクリックする。

サーバ公開ルール登録結果画面が表示されます。

ルール設定追加

ファイアウォール > 詳細設定 > ルール設定(サーバ公開) > ルール設定更新 [ヘルプ]

■ 外部公開IPアドレス  
202.247.5.136

■ 内部IPアドレス  
 172.16.1.125  
 アドレス変換しない

■ ポート  
 ポートの指定をしない  
 TCP 外部 80 → 内部 80  
 UDP 外部 → 内部

■ 記録  
 しない  
 ログ

登録

5. [ルール設定(サーバ公開)に戻る]をクリックする。

追加したルールが反映されたサーバ公開ルール一覧画面が表示されます。

ルール設定追加結果

ファイアウォール > 詳細設定 > ルール設定(サーバ公開) > ルール設定追加 > ルール設定追加結果 [ヘルプ]

下記のとおり、ルール設定(サーバ公開)追加に成功しました。

■ 外部公開IPアドレス  
202.247.5.136

■ 内部IPアドレス  
172.16.1.125

■ ポート  
TCP 80→80

■ 記録  
ログ

ルール設定(サーバ公開)に戻る

6. サーバ公開ルール一覧画面を確認し、[詳細設定]をクリックする。

詳細設定メニュー画面が表示されます。  
引き続きルール設定の更新を行います。

ルール設定(サーバ公開)

ファイアウォール > 詳細設定 > ルール設定(サーバ公開) [ヘルプ]

かんたん設定(ネットワーク構成)の確認

ルールへの追加・削除・更新を行った場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックください。

一覧末尾のルールを [追加](#)  
選択したルールを [削除](#)

No.	公開IPアドレス	ポート	内部IPアドレス	ポート	記録
1	202.247.5.136	tcp/80	172.16.1.125	80	

全選択/解除

■ オプション  
 ウェブサーバをウェブ専用フィルタ経由で公開する。(ウェブ専用フィルタ設定)  
 メールサーバをメール専用フィルタ経由で公開する。(メール専用フィルタ設定)

確定

# ルール設定の更新

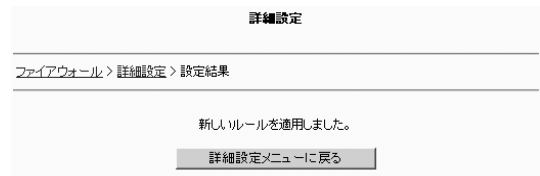
最後に、今までの設定を更新します。

1. 詳細設定メニューの「ルール設定」から[編集結果を適用]をクリックする。

詳細設定結果画面が表示されます。



2. 新しく追加したルールが Express5800/SG300に適用されます。



# VPN通信の確認

ここでは、VPNパス間で暗号通信が正常に行えているかどうかを確認する方法について説明します。

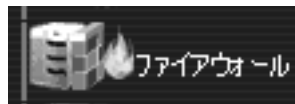
VPNパス間で暗号通信ができているかどうかは、実際にVPNの対象となる通信を行った後、通信ログを参照することで確認します。確認手順を以下に示します。



ヒント

VPNクライアントの設定の詳細は、「リモートアクセスVPNの設定（クライアント編）」を参照してください。

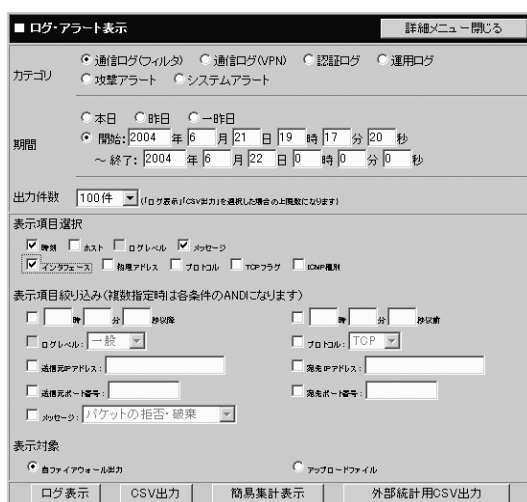
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。  
ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。  
ログ・アラート表示画面が表示されます。



3. 「詳細メニュー開く」をクリックし、ログ・アラート表示画面に表示される各項目を入力する。

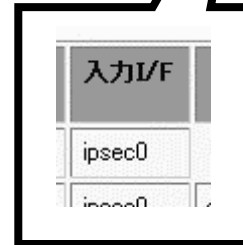


項目	設定内容
カテゴリ	通信ログ（フィルタ）
期間	VPNの対象となる通信を行った期間を指定
出力件数	（任意の件数を指定）
表示項目選択	時刻、メッセージ、インタフェース
表示項目絞り込み	VPNの対象となる通信を絞り込む条件を指定 （特に指定しなくても可）
表示対象	自ファイアウォール出力

#### 4. [ログ表示]をクリックする。

ログ表示画面が表示されます。右図の通り、VPN通信に該当するグループルールやサーバ公開ルールの出力の「入力I/F」欄に、ipsecという文字列が表示されていれば設定は成功です。

時刻	メッセージ	発信元IPアドレス	宛先IPアドレス	宛先ポート番号	入力I/F	出力I/F
2004/06/21 19:17:20.672	サーバ公開ルールが有効になりました。	202.247.51.71	202.247.51.136	80	ipsec0	
2004/06/21 19:17:20.672	ルール #632-e1 の有効化が完了しました。	202.247.51.71	202.247.51.136	80	ipsec0	eth0
2004/06/21 19:17:20.682	サーバ公開ルールが有効になりました。	202.247.51.71	202.247.51.136	80	ipsec0	
2004/06/21 19:17:20.682	ルール #632-e1 の有効化が完了しました。	202.247.51.71	202.247.51.136	80	ipsec0	eth0
2004/06/21 19:17:20.692	サーバ公開ルールが有効になりました。	202.247.51.71	202.247.51.136	80	ipsec0	
2004/06/21 19:17:20.692	ルール #632-e1 の有効化が完了しました。	202.247.51.71	202.247.51.136	80	ipsec0	eth0



ヒント

「入力I/F」欄にethという文字列が表示されている場合は、VPN通信が行われていません。再度、これまでの各設定を見直してください。

VPN通信に関するエラー情報は、ログ・アラート表示画面でカテゴリとして[通信ログ (VPN)]のラジオボタンを選択し、[ログ表示]をクリックすることで確認できます。