

基本設定 2/2

・基本設定 2/2 目次

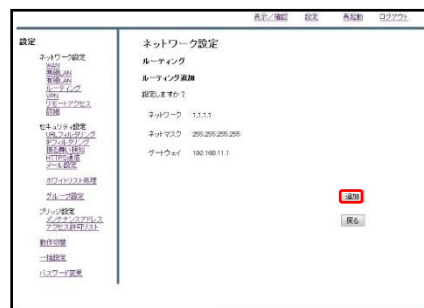
| | | |
|-----------|----------------------------|---------------------|
| 6 | <u>ルーティング設定</u> | <u>P. 3</u> |
| 7 | <u>グループ設定</u> | <u>P. 4</u> |
| 7-1 | グループ編集 | |
| 7-2 | コレダケトオス | |
| 7-3 | グループ別フィルタリング | |
| 8 | <u>ホワイトリスト申請/処理</u> | <u>P. 7</u> |
| 8-1 | ホワイトリスト申請 | |
| 8-2 | ホワイトリスト申請処理 | |
| 9 | <u>TCPMSS設定</u> | <u>P. 9</u> |
| 10 | <u>VPN接続</u> | <u>P. 10</u> |
| 10-1 | IKEv2 : VPN応答側(親)の設定 | |
| 10-2 | IKEv2 : VPN開始側(子)の設定 | |
| 10-3 | IKEv2 : VPN(MRB接続)の設定 | |
| 11 | <u>ログ閲覧</u> | <u>P. 16</u> |
| 11-1 | 閲覧できるログの確認 | |
| 11-2 | ログ閲覧時の操作 | |

6, ルーティング設定

MRBがルータとして機能する際のルーティングを設定します



①管理画面にログイン後、右上の『設定』をクリックし、左の『ルーティング』をクリックします。



④記入したIPを確認し、正しければ『追加』をクリックして作業は完了です。



②『追加』をクリックします。



③ルーティングするネットワーク情報と宛先ゲートウェイを入力し、『追加』をクリックします。

7-1, グループ編集

MRB配下の管理端末をセキュリティ設定ごとに区分します



①管理画面にログインし、右上の『設定』をクリックし、左の『グループ設定』をクリックします。



④単独で指定する場合は"IPアドレス"、範囲で指定する場合は"IPアドレス範囲"のラジオボタンをクリックし、例に習って"ルール"の記入欄にIPアドレスを記入します。



②"編集"のラジオボタンより、設定を行うグループを選択し、『編集』をクリックします。



⑤入力したIPアドレスとタイプを確認し、正しければ『追加』をクリックして設定は完了です。

※グループ割当設定を行っていないIPはデフォルトグループに所属しています。



③『追加』をクリックします。

7-2, コレダクトオス

“コレダクトオス”は許可されたIP/URL以外とは通信が出来ない特別なグループです



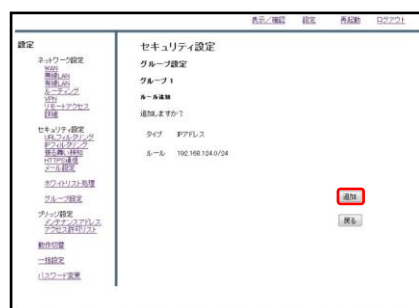
①管理画面にログインし、右上の『設定』をクリックし、左側の『グループ設定』をクリックします。



④単独で指定する場合は“IPアドレス”、範囲で指定する場合は“IPアドレス範囲”のラジオボタンをクリックし、例に習って“ルール”の記入欄にIPアドレスを記入します。



②“編集”のラジオボタンより『コレダクトオス』を選択し、『編集』をクリックします。



⑤入力したIPアドレスとタイプを確認し、正しければ『追加』をクリックして設定は完了です。



③『追加』をクリックします。

7-3、グループ別フィルタリング

グループごとのフィルタリング強度を設定します



① 右上の『設定』をクリックし、左側の『グループ設定』をクリックします。



② “編集”のラジオボタンより、設定を行うグループを選択し、『編集』をクリックします。



③ 『URLフィルタリング』『メール設定』等をクリックすることで、選択したグループのフィルタリング設定を行うことができます。

※具体的な設定方法に関しては、フィルタリング設定のページをご確認ください。

8-1, ホワイトリスト申請

Webサイトがブロックされた場合、管理者の方へ解除申請を行うことができます。

URLフィルターによりブロックされました。

| | |
|--------|---|
| サイト | http://testapp.example.jp |
| フィルター | ゲーム |
| IPアドレス | 192.168.124.13 |

サイトの再評価を申請

申請のみ状態を許可

ホワイトリストに登録を申請

サイトの再評価を行います。
承認されるまで、表示されます。
(全てのIPアドレスに反映されます。)

ご迷惑ください。
30分間アクセスの制限になります。
承認後にURLフィルターが解除されます。
(全てのIPアドレスに反映されます。)

管理員としての対応が必要です。
管理員の方にご連絡ください。
(全てのIPアドレスに反映されます。)

①Webサイトがブロックされた場合、左のような画面が表示されます。右下『ホワイトリストに登録を申請』をクリックしてください。

ブロックリクエスト設定

ホワイトリストに登録を申請しました。管理者の方にご連絡ください。

対象URL: <http://testapp.example.jp>

②左のような画面が表示されましたら、申請は完了です。管理者の方にご連絡してください。

8-2, ホワイトリスト申請処理

利用者からのWebサイトアクセス許可の申請に対して処理を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左の『ホワイトリスト処理』をクリックします。



②申請があったWebサイトに対して、ラジオボタンにより"許可"、"拒否"を選択し、『設定』をクリックします。



③対応を確認し、正しければ『設定』をクリックして処理は完了です。

9, TCPMSS設定

パケットの長さを整える設定です。ADSL
通信やひかり電話のルータが上位に存在
する場合に設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左の『詳細』をクリックします。



②TCPMSS(バイト)の記入欄を任意の値に変更し、『次へ』をクリックします。(フレッツADSL,ひかり電話利用の場合は"1414"、フレッツ光プレミアム利用の場合は"1398"を使用します。)



③入力を確認し、正しければ『確認』をクリックして設定は完了です。

10-1, VPN応答側(親)の設定

MRB同士でVPNを構築する際、固定IPを使用する側の設定です



①管理画面にログイン後、右上の『設定』をクリックし、左側の『VPN』をクリックします。



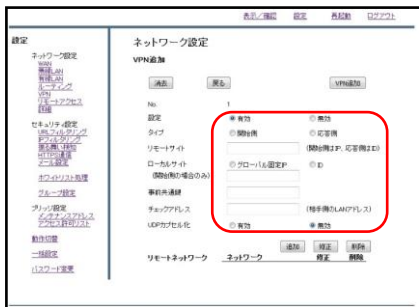
④入力が終わりましたら、下側の『追加』をクリックします。



②『追加』をクリックします。



⑤VPN相手のネットワークアドレスとネットマスクを記入し、『追加』をクリックします。



③以下の表を参考に設定項目を記入欄に入力します。

設定...有効
 タイプ...応答側
 リモートサイト...開始側と取り決めた任意のID
 ローカルサイト..."グローバル固定IP"を選択し、
 固定IPを記入
 事前共通鍵...相手側と取り決めた任意のワード
 チェックアドレス...相手側のLAN側IPアドレス
 IKEバージョン..."IKEv2"を選択
 UDPカプセル化...有効



⑦右上の『VPN追加』をクリックします。

※UDPカプセル化とは...
 NAPTを経由してVPN通信を行う際に
 NAPTによる宛先変換を可能にするための
 機能です



⑦右上の『VPN追加』をクリックします。



⑨『VPN設定』をクリックし、設定を反映させたら完了です。

10-2, VPN開始側(子)の設定

MRB同士でVPNを構築する際、固定IPを使用しない側の設定です



①管理画面にログイン後、右上の『設定』をクリックし、左側の『VPN』をクリックします。



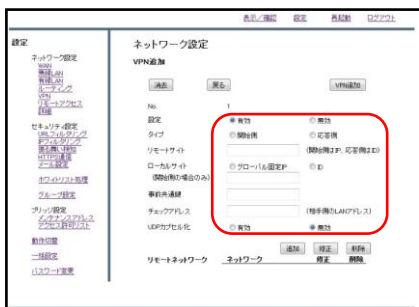
④入力が終わりましたら、下側の『追加』をクリックします。



②『追加』をクリックします。



⑤VPN相手のネットワークアドレスとネットマスクを記入し、『追加』をクリックします。



③以下の表を参考に設定項目を記入欄に入力します。

設定...有効
 タイプ...開始側
 リモートサイト...グローバル固定IP
 ローカルサイト...“ID”を選択し、
 開始側の設定したIDを記入
 事前共通鍵...相手側と取り決めた任意のワード
 チェックアドレス...相手側のLAN側IPアドレス
 IKEバージョン...“IKEv2”を選択
 UDPカプセル化...有効



⑦右上の『VPN追加』をクリックします。

※UDPカプセル化とは...
 NAPTを経由してVPN通信を行う際に
 NAPTによる宛先変換を可能にするための
 機能です



⑦右上の『VPN追加』をクリックします。



⑨『VPN設定』をクリックし、設定を反映させたら完了です。

10-3, VPN(MRB接続)の設定

MRB同士でVPNを構築する際、機械番号を使用する設定です

※MRB番号でのVPNはIPv6アドレス利用時のみ可能です



①管理画面にログイン後、右上の『設定』をクリックし、左側の『VPN』をクリックします。



④入力が終わりましたら、下側の『追加』をクリックします。



②『追加』をクリックします。



⑤VPN相手のネットワークアドレスとネットマスクを記入し、『追加』をクリックします。



③以下の表を参考に設定項目を記入欄に入力します。

設定...有効
 タイプ...MRB接続
 リモートサイト...MRBの機械番号
 ローカルサイト..."なし"を選択
 事前共通鍵...相手側と取り決めた任意のワード
 チェックアドレス...相手側のLAN側IPアドレス
 IKEバージョン..."IKEv2"を選択
 UDPカプセル化...無効



⑦右上の『VPN追加』をクリックします。

※UDPカプセル化とは...
 NAPTを経由してVPN通信を行う際に
 NAPTによる宛先変換を可能にするための機能です



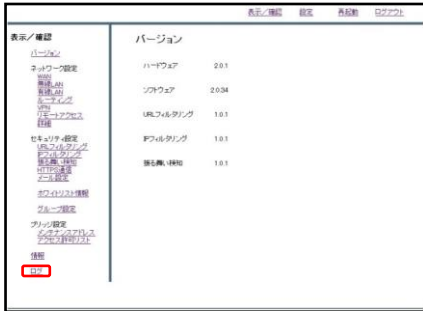
⑦右上の『VPN追加』をクリックします。



⑨『VPN設定』をクリックし、設定を反映させたら完了です。

11-1, 閲覧できるログ

MRBで検閲した通信のログを閲覧することができます



①管理画面にログイン後、
左側の『ログ』をクリックします。



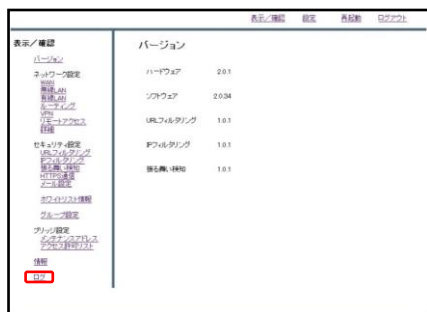
②各ボタンをクリックすることでそれぞれのログを
閲覧することができます。

③各ログの内容については以下のとおりです。

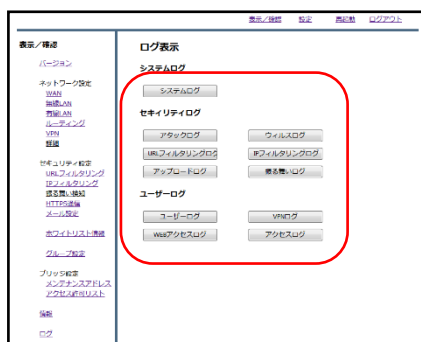
- ・ システムログ ...MRBで動作したシステムのログです。(通信のログではありません)
...外部からのアタックされた場合に記録されます
- ・ アタックログ ...ダウンロードしようとしたファイルがウイルスだった場合に記録されます
- ・ ウィルスログ ...WEB閲覧時、URLフィルタリングにて通信をブロックした場合に記録されます
- ・ URLフィルタリングログ ...WEB閲覧時、URLフィルタリングにて通信をブロックした場合に記録されます
- ・ IPフィルタリングログ ...データを外部にアップロードした際に記録されます
- ・ IPフィルタリングログ ...WEBサイト以外からの通信をブロックした際に記録されます
- ・ アップロードログ ...ユーザーがMRB管理画面にて行った操作が記録されます
- ・ 振る舞いログ ...アクセスしたWEBサイトが記録されます
- ・ ユーザーログ ...WEBサイト以外のアクセスが記録されます
- ・ WEBアクセスログ
- ・ アクセスログ

11-2, ログ閲覧時の操作

MRBで検閲した通信のログを閲覧を確認する際の操作です



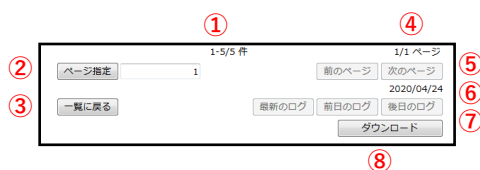
①管理画面にログイン後、左側の『ログ』をクリックします。



②閲覧したいログのボタンをクリックします。



③クリックしたボタンに対応するログが表示されます。また、『ダウンロード』をクリックすることで、現在閲覧している日付のログデータをテキスト形式でダウンロードすることができます。



④閲覧ログの操作は以下のとおりです。

- 1...現在閲覧しているログ番号/すべてのログ件数です
- 2...1ページあたり300件ごとに閲覧するログを指定できます
- 3...ログ一覧に戻ります
- 4...現在閲覧しているログページ/すべてのログページです
- 5...ログページの遷移ができます
- 6...閲覧しているログの日付です
- 7...閲覧するログの日付を変更できます
[最新のログ]は本日のログです
- 8...閲覧している日付のログをダウンロードします