RV320およびRV325 VPNルータシリーズのシステムログの設定

目的

システムログは、ネットワークイベントの記録です。ログは、ネットワークの動作を理解するために使用される重要なツールです。ネットワーク管理とネットワークのトラブルシューティングに役立ちます。

この記事では、記録するログの種類、RV32x VPNルータシリーズのログの表示方法、およびSMS、システムログサーバ、または電子メールを介して受信者にログを送信する方法について説明します。

該当するデバイス

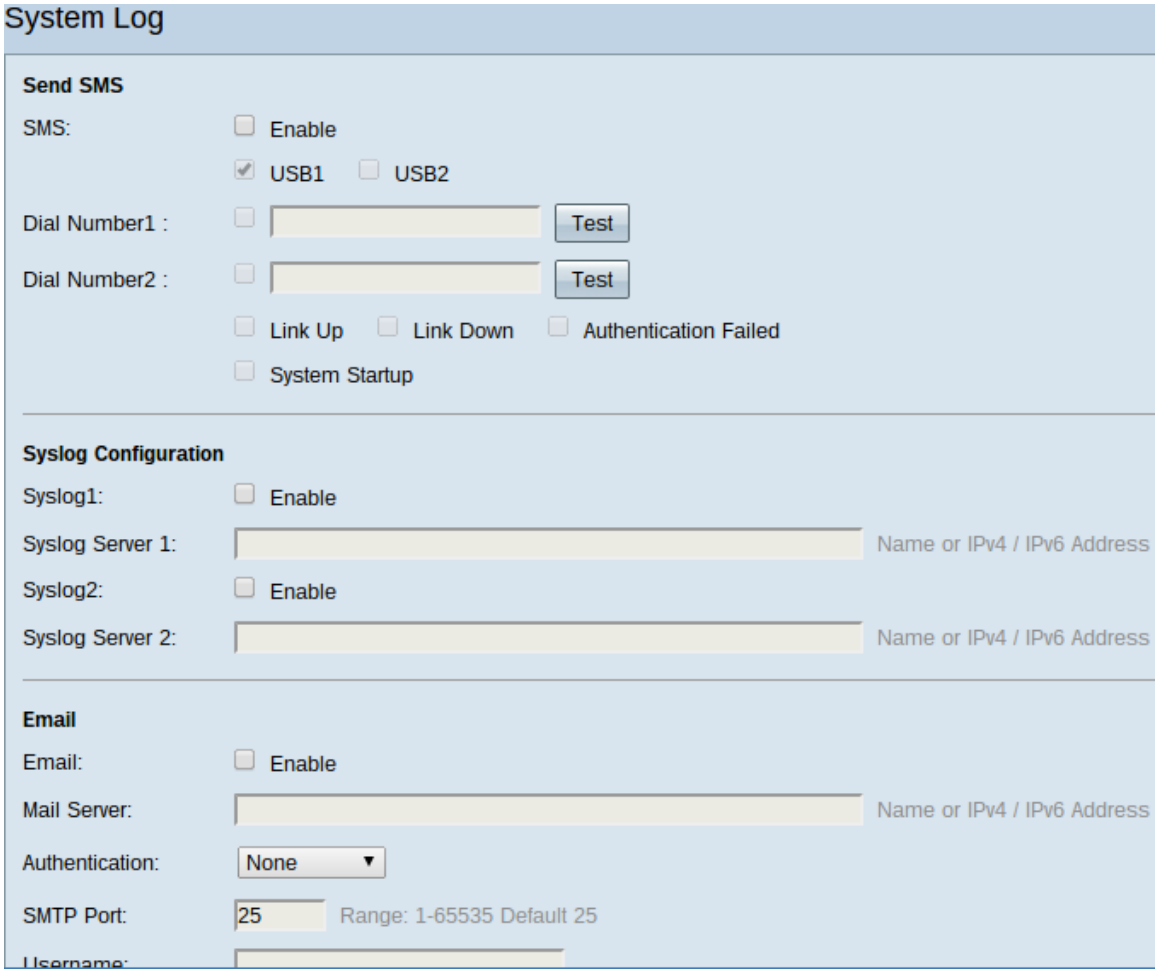
- RV320デュアルWAN VPNルータ
- RV325ギガビットデュアルWAN VPNルータ

[Software Version]

- v1.1.0.09

システムログの設定

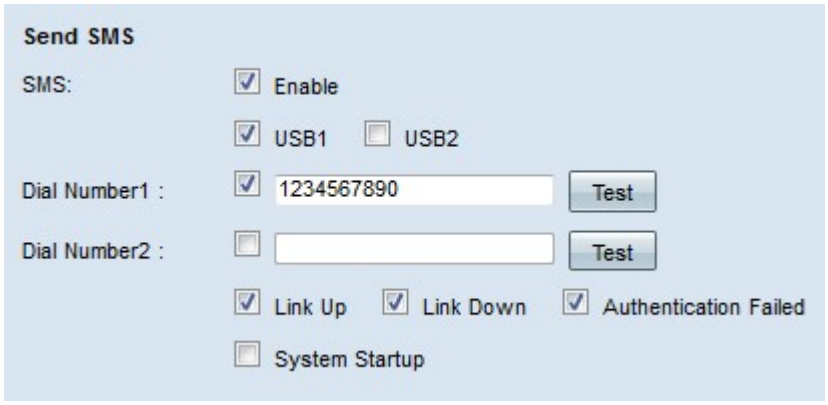
ステップ1:Web構成ユーティリティにログインし、**[Log] > [System Log]を選択します。**「システム・*ログ*」ページが開きます。



「システムログ」ページについては、次のセクションを*参照*してください。

- SMSによるシステムログ:SMSを介してシステムログを電話機に送信する方法。
- システムログサーバのシステムログ：システムログをシステムログサーバに送信する方法。
- Email System Logs：システムログを電子メールアドレスに送信する方法。
- ログ設定：ログに保存されるメッセージの種類を設定する方法。
- システムログの表示：デバイスのシステムログを表示する方法。
- View Outgoing Log Table：発信パケットのみに関連するシステムログを表示する方法。
- View Incoming Log Table：着信パケットのみに関連するシステムログを表示する方法。

SMSによるシステムログ



ステップ1:[SMS]フィールドの[**Enable**]をオンにして、ショートメッセージサービス(SMS)メッセージを使用してシステムログをクライアントに送信します。

ステップ2:3G USBモデムが接続されているUSBポートのチェックボックスをオンにします。

ステップ3:[Dial Number1（ダイヤル番号1）]フィールドのチェックボックスをオンにし、メッセージの送信先の電話番号を入力します。

注：[Test] をクリックして、ダイヤル番号1への接続をテストします。設定済みの番号がテストメッセージを受信しない場合は、[Dial Number1]フィールドに電話番号が正しく入力されていることを確認します。

ステップ4:（オプション）[Dial Number2（ダイヤル番号2）]フィールドのチェックボックスをオンにし、メッセージの送信先の電話番号を入力します。

注：[Test] をクリックして、番号2への接続をテストします。設定済みの番号がテストメッセージを受信しない場合は、[Dial Number2]フィールドに電話番号が正しく入力されていることを確認します。

ステップ5：ログの送信をトリガーするイベントのチェックボックスをオンにします。

- Link Up — RV320への接続が確立されました。
- Link Down — RV320への接続がダウンしています。
- Authentication Failed：認証に失敗しました。
- システムの起動：ルータが起動します。

ステップ6:[Save]をクリックします。SMSを介したシステムログが設定されます。

システムログサーバのシステムログ

ステップ1:[Syslog1]フィールドの[Enable] をオンにして、システムログをシステムログサー

バに送信します。

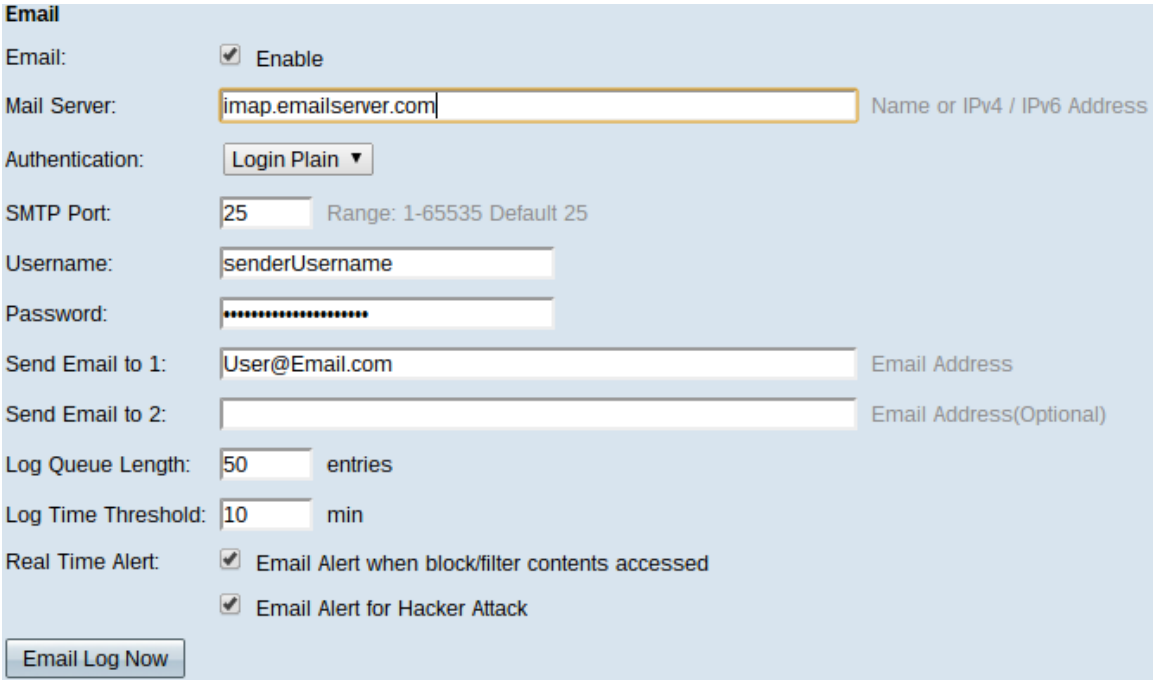
ステップ2：システムログサーバのホスト名またはIPアドレスを[Syslog Server 1]フィールドに入力します。

ステップ3:（オプション）別のシステムログサーバにログを送信するには、[Syslog2]フィールドの[**Enable**]をオンにします。

ステップ4:[Syslog2]フィールドでチェックボックスをオンにした場合は、[Syslog Server 2]フィールドにシステムログサーバのホスト名またはIPアドレスを入力します。

ステップ5:[Save]をクリックします。システムログサーバ経由のシステムログが設定されます。

Eメールシステムログ



ステップ1:[Email]フィールドの[Enable] をオンにして、システムログを電子メールで受信者に送信します。

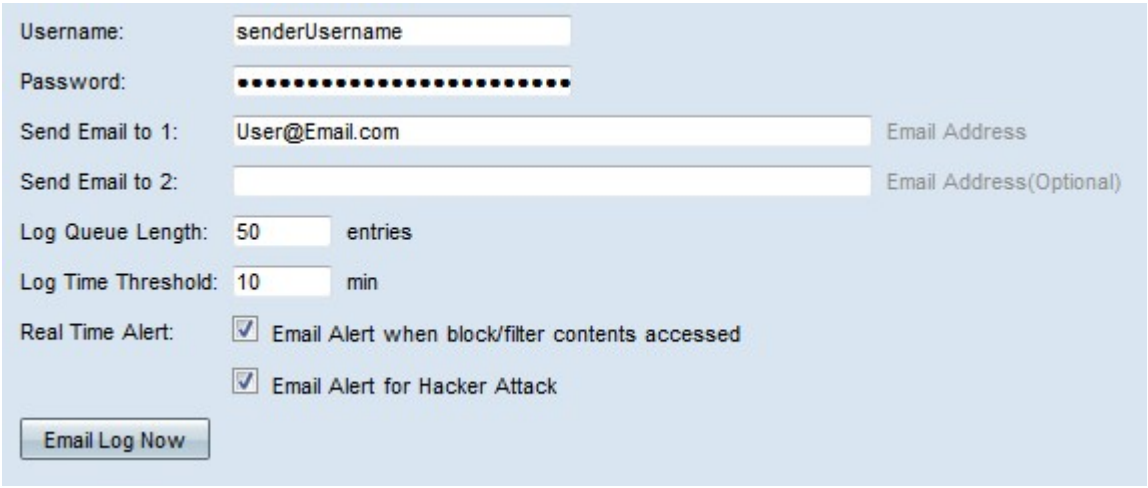
ステップ2:[Mail Server]フィールドにメールサーバのドメイン名またはIPアドレスを入力します。

ステップ3:[Authentication]フィールドで、メールサーバが使用する認証のタイプを選択します。

- None：メールサーバは認証を使用しません。
- Login Plain：メールサーバはプレーンテキスト形式の認証を使用します。
- TLS：メールサーバはTransport Layer Security(TLS)を使用して、クライアントとサーバが認証情報を安全に交換できるようにします。
- SSL：メールサーバはSecure Sockets Layer(SSL)を使用して、クライアントとサーバが認証情報を安全に交換できるようにします。

ステップ4：メールサーバが使用するシンプルメール転送プロトコル(SMTP)ポートを

[SMTPポート(SMTP Port)]フィールドに入力します。SMTPは、電子メールをIPネットワーク経由で送信できるようにするプロトコルです。



ステップ5:[Username]フィールドに電子メール送信者のユーザ名を入力します。

ステップ6:[Password]フィールドに電子メール送信者のパスワードを入力します。

ステップ7:[Send Email to 1]フィールドに電子メール受信者の電子メールアドレスを入力します。

ステップ8:（オプション）[Send Email to 2]フィールドに、ログメールの送信先となる追加の電子メールアドレスを入力します。

ステップ9:[Log Queue Length（ログキューの長さ）]フィールドに、メール受信者にログを送信する前に行う必要があるログエントリの数を入力します。

ステップ10:[Log Time Threshold]フィールドに、デバイスが電子メールにログを送信する間隔を入力します。

ステップ11:[Real Time Alert]フィールドの最初のチェックボックスをオンにすると、ブロックまたはフィルタリングされたユーザがルータにアクセスしようとするときに、すぐに電子メールが送信されます。

ステップ12:[Real Time Alert]フィールドの2番目のチェックボックスをオンにして、ハッカーがDenial of Service(DOS)攻撃を使用してルータにアクセスしようとしたときに、すぐに電子メールを送信します。

注：[Email Log Now]をクリックすると、すぐにログが送信されます。

ステップ13:[Save]をクリックします。電子メールによるシステムログが設定されます。

ログ設定

ステップ1：ログエントリをトリガーするイベントのチェックボックスをオンにします。

・ アラートログ：これらのログは、攻撃または攻撃の試みが発生したときに作成されます。

- Syn Flooding:SYN要求は、ルータが処理できる速度を超えて受信されます。

- IPスプーフィング：RV320は、偽造された送信元IPアドレスを持つIPパケットを受信しました。

- Unauthorized Login Attempt：ネットワークへのログオンの拒否に失敗しました。

- Ping of Death：異常なサイズのpingが、ターゲットデバイスをクラッシュさせようとしたインターフェイスに送信されました。

- Win Nuke:WinNukeと呼ばれるリモート分散型サービス拒否攻撃(DDOS)が、ターゲットデバイスをクラッシュさせようとしてインターフェイスに送信されました。

・ 一般ログ：これらのログは、一般的なネットワーク操作が発生したときに作成されます。

- Deny Policies – ルータの設定済みポリシーに基づいて、ユーザへのアクセスが拒否されました。

- Authorized Login：ユーザがネットワークへのアクセスを許可されました。

– システムエラーメッセージ：システムエラーが発生しました。

- Allow Policies：ルータの設定されたポリシーに基づいて、ユーザにアクセスが許可されています。

- Kernel – すべてのカーネルメッセージをログに含めます。カーネルは、起動時にメモリにロードされるオペレーティングシステムの最初の部分です。カーネルメッセージは、カーネルに関連付けられたログです。

- Configuration Changes：ルータの設定が変更されました。

- IPSECおよびPPTP VPN:IPSECおよびPPTP VPNのネゴシエーション、接続、または切断が発生しました。

- SSL VPN:SSL VPNのネゴシエーション、接続、切断が発生しました。

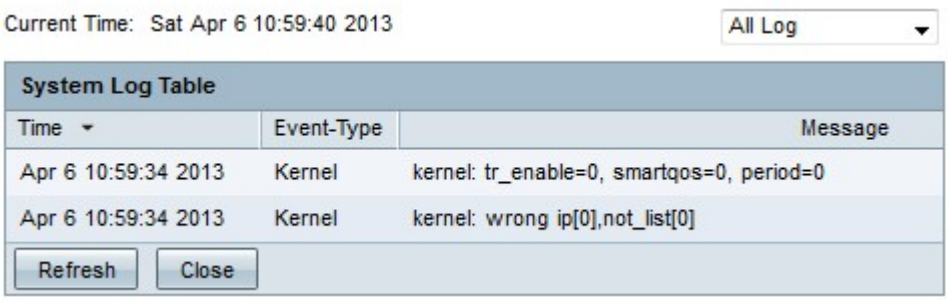
– ネットワーク：WANまたはDMZインターフェイスで物理接続が確立されたか、失われました。

ステップ2:[Save]をクリックします。ログ設定が設定されます。

注：現在のログをクリアするには、[Clear Log]をクリックします。

システムログの表示

ステップ1：システムログテーブルを表示するには、[システムログの表示]をクリックします。[システムログテーブル]ウィンドウが表示されます。



ステップ2:（オプション）ドロップダウンリストから、表示するログのタイプを選択します。

- All Log – すべてのログメッセージを含みます。
- システムログ：システムエラーメッセージのみが含まれます。
- ファイアウォール/DoSログ：アラートログのみを含みます。
- VPNログ：IPSecおよびPPTP VPNログとSSL VPNログのみが含まれます。
- ネットワークログ：ネットワークログのみを含みます。
- カーネルログ：カーネルメッセージのみを含みます。
- ユーザログ：拒否ポリシー、許可ポリシー、許可ログイン、設定変更ログのみを含む
- SSLログ：SSL VPNログのみを含みます。

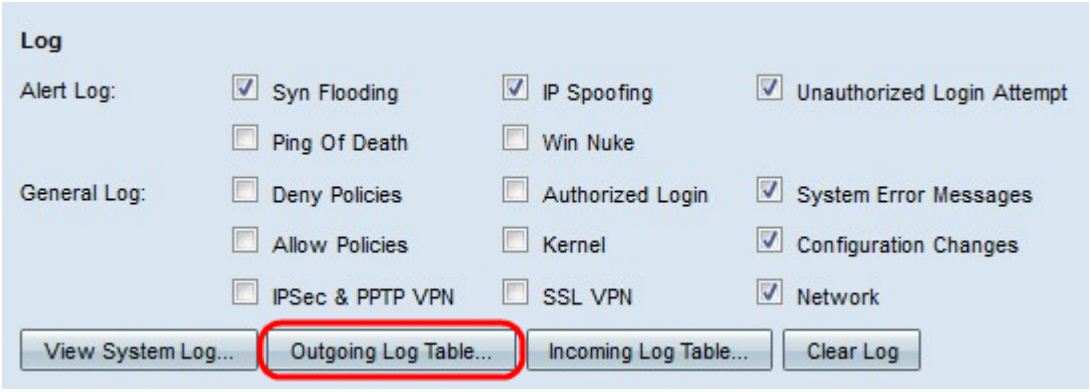
システムログテーブルには、次の情報が表示されます。

- Time – ログが作成された時刻。
- Event-Type：ログのタイプ。

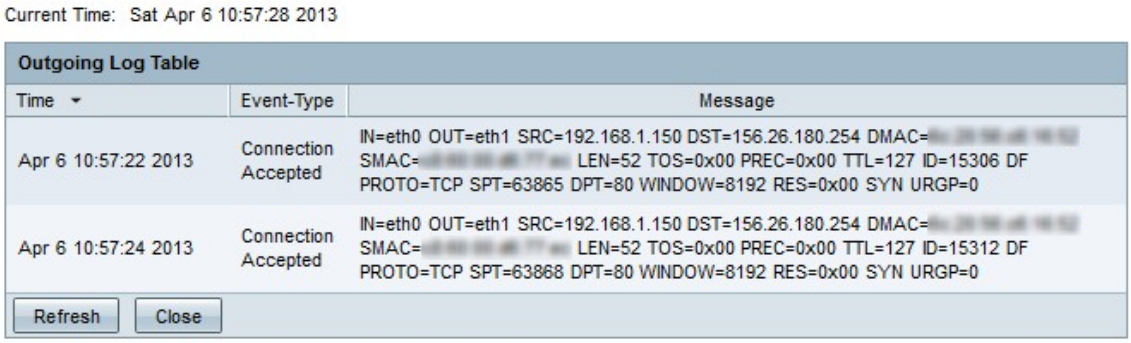
・メッセージ：ログに対応する情報。これには、ポリシーのタイプ、送信元IPアドレス、送信元MACアドレスが含まれます。

注：[更新]をクリックして、ログテーブルを更新します。

発信ログテーブルの表示



ステップ1:[Outgoing Log Table]をクリックして、発信パケットのみに関連するログテーブルを表示します。[Outgoing *Log Table]ウィンドウが*表示されます。



[Outgoing Log Table]には、次の情報が表示されます。

・ Time – ログが作成された時刻。

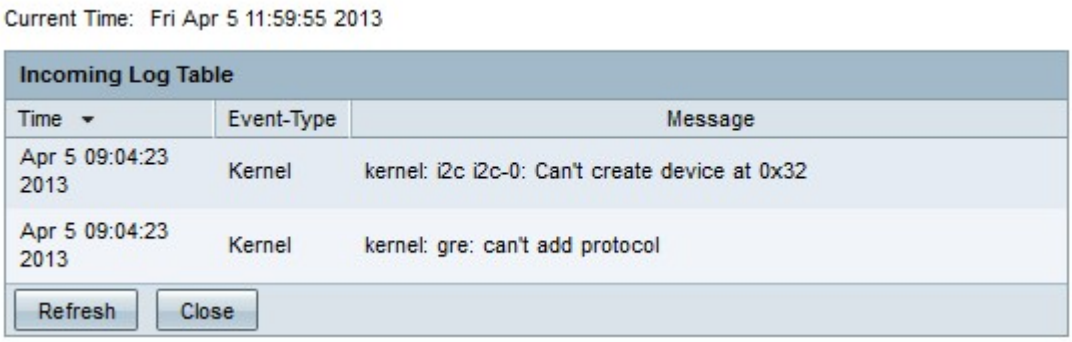
・ Event-Type：ログのタイプ。

・メッセージ：ログに対応する情報。これには、ポリシーのタイプ、送信元IPアドレス、送信元MACアドレスが含まれます。

注：[更新]をクリックして、ログテーブルを更新します。

受信ログテーブルの表示

ステップ1:[着信ログテーブル(Incoming Log Table)]をクリックして、着信パケットのみに関連するログテーブルを表示します。[着信ログテーブル]ウィンドウが表示されます。



[着信ログテーブル(Incoming Log Table)]には、次の情報が表示されます。

- Time – ログが作成された時刻。
- Event-Type：ログのタイプ。
- メッセージ：ログに対応する情報。これには、ポリシーのタイプ、送信元IPアドレス、送信元MACアドレスが含まれます。

注：[更新]をクリックして、ログテーブルを更新します。