D-Link DSR-500/1000/1000AC

Unified Services VPN Router

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物的損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠危険

⃠ 禁止 **分解・改造をしない**
火災、やけど、けが、感電などの原因となります。

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

⃠ 禁止 **水をかけたり、ぬらしたりしない**
内部に水が入ると、火災、感電、故障の原因となります。

⃠ 禁止 **水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない**
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止 **各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く**
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止 **油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない**
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止 **内部に金属物や燃えやすいものを入れない**
火災、感電、故障の原因となります。

⃠ 禁止 **砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない**
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止 **電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない**
火災、やけど、けが、感電、故障の原因となります。

⚠警告

⃠ 禁止 **落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない**
故障の原因となります。

⃠ 禁止 **発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない**
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼ください。

⃠ 禁止 **表示以外の電圧で使用しない**
火災、感電、または故障の原因となります。

⃠ 禁止 **たこ足配線禁止**
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

❗ **設置、移動のときは電源プラグを抜く**
火災、感電、または故障の原因となります。

⃠ 禁止 **雷鳴が聞こえたら、ケーブル / コード類にはさわらない**
感電の原因となります。

⃠ 禁止 **ケーブル / コード類や端子を破損させない**
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障の原因となります。

❗ **本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する**
火災、感電、または故障の原因となります。

⃠ 禁止 **各光源をのぞかない**
光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。

⃠ 禁止 **各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする**
火災、やけど、けが、感電または故障の原因となります。

⃠ 禁止 **使用中に布団で覆ったり、包んだりしない**
火災、やけどまたは故障の原因となります。

❗ **ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る**
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。

⃠ 禁止 **カメラのレンズに直射日光などを長時間あてない**
素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。

❗ **無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する**
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。

⃠ 禁止 **本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない**
火災、または故障の原因となります。

❗ **耳を本体から離してご使用ください**
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。

❗ **無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する**
医療電気機器に悪影響を及ぼすおそれがあります。

❗ **高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない**
電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。

❗ **ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する**
破損部や露出部に触れると、やけど、けが、感電の原因となります。

❗ **ペットなどが本機に噛みつかないように注意する**
火災、やけど、けがなどの原因となります。

⃠ 禁止 **コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない**
火災、やけど、感電または故障の原因となります。

⃠ 禁止 **AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない**
発火、発熱、感電または故障の原因となります。

⚠警告

- ACアダプタもしくは電源プラグについたほこりは、拭き取る
  ほこりが付着した状態で使用すると、
  火災、やけど、感電または故障の原因となります。
- ACアダプタや電源ケーブルをコンセントに
  さしこむときは、確実に差し込む
  確実に差し込まないと、火災、やけど、
  感電もしくは故障の原因となります。
- 接続端子が曲がるなど変形した場合は、直ちに使用を中止する。
  また、変形をもとに戻しての使用も行わない
  端子のショートにより、火災、やけど、けが、
  感電または故障の原因となります。
- 各種接続端子を機器本体に接続する場合、斜めに差したり、
  差した状態で引っ張ったりしない
  火災、やけど、感電または故障の原因となります。
- 使用しない場合は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  電源プラグを差したまま放置すると、火災、やけど、
  感電または故障の原因となります。
- お手入れの際は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  抜かずに行うと、火災、やけど、感電または故障の原因となります。
- 禁止 SDやMicroSDカード、USBメモリの使用中は、
  カードやメモリを取り外したり、本製品の電源を切ったりしない
  データの消失、機器本体の故障の原因となります。
- 禁止 磁気カードや磁気を帯びたものを本製品に近づけない
  磁気カードのデータが消えてしまうおそれもしくは
  機器本体の誤作動の原因となります。
- ディーリンクジャパンが販売している無線機器は
  国内専用のため、海外で使用しない
  海外では国によって電波使用制限があるため、
  本製品を使用した場合、罰せられる場合があります。
  海外から持ち込んだディーリンク製品や並行輸入品を
  日本国内で使用する場合も同様に、罰せられる場合があります。

⚠注意

- 禁止 乳幼児の手の届く場所では使わない
  やけど、ケガまたは感電の原因となります。
- 静電気注意
  コネクタや電源プラグの金属端子に触れたり、
  帯電したものを近づけますと故障の原因となります。
- 禁止 コードを持って抜かない
  コードを無理に曲げたり、引っ張ると、
  コードや機器本体の破損の原因となります。
- 禁止 振動が発生する場所では使用しない
  故障の原因となります。
- 付属品の使用は取扱説明書に従う
  本製品の付属品は、取扱説明書に従い、
  他の製品に使用しないでください。機器の破損の原因となります。
- 禁止 破損したまま使用しない
  火災、やけどまたはけがの原因となります。
- 禁止 ぐらついた台の上や傾いた場所などの
  不安定な場所や高所には置かない
  落下して、けがなどの原因となります。
- 禁止 子供が使用する場合は、保護者が取扱いの方法を教え、
  誤った使い方をさせない
  けがや故障などの原因となります。
- 本製品を長時間連続使用する場合は、
  温度が高くなることがあるため、注意する。
  また、使用中に眠ってしまうなどして、
  意図せず長時間触れることがないようにする
  温度の高い部分に直接長時間触れると
  お客様の体質や体調によっては肌の赤みや
  かゆみ、かぶれ、低温やけどの原因となります。
- 禁止 コンセントにつないだ状態で、ACアダプタや
  電源コンセントに長時間触れない
  やけど、感電の原因となります。
- 一般の電話機やコードレス電話、テレビ、ラジオなどを
  お使いになっている近くで使用しない
  近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、
  なるべく離れた場所で使用してください。
- 禁止 D-Linkが指定したオプション品がある場合は、
  指定オプションを使用する
  不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。
この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。
さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

無線 LAN について

業界標準に基づく弊社の無線 LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これらを使用して時間や場所に関わらず必要なデータにアクセスすることができます。
WLAN は家庭やオフィス環境のみならず、空港やコーヒーショップ、または大学など公共の施設においても幅広く利用されるようになってきました。この WLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。
ノート型やデスクトップ型 PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線ネットワークと同じアプリケーションを利用できるようになりました。

WLAN 技術を利用するさまざまな理由

可動性
WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。

低い実現コスト
WLAN は設置、管理、変更、移転のすべてが簡単です。このような WLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします

簡単な設置と拡張
煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。

低コストのソリューション
無線 LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。本製品は設定可能な複数のモードで多機能性を提供し、コスト削減を行います。

柔軟性
配置する無線 LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから大規模なインフラネットワークまで、自由自在に構築することができます。

世界基準対応の技術
無線機器は、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n および IEEE 802.11ac に準拠しています。

● EEE 802.11ac 規格

IEEE 802.11ac 規格の無線通信速度は、最大 1300Mbps までと高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。

● EEE 802.11n 規格

IEEE 802.11n 規格は、従来の IEEE 802.11a、IEEE 802.11b および IEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大 300Mbps までと高速化され、2.4GHz 帯および 5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。
これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ない MPEG 形式の映像の視聴などが可能になります。OFDM(Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うことができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロストーク（干渉）の発生を抑えることが可能です。
IEEE 802.11n 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。
WPA/WPA2 には企業向けの「 Enterprise」とホームユーザ向けの「Personal」の 2 種類があります。「WPA-Personal」と「WPA2-Personal」はユーザ認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「 Pre-Shared Key（ 事前共有鍵）」の定義を行うという点で WEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認され条件が満たされた時にアクセスが認められます。
「WPA-Enterprise」と「 WPA2-Enterprise」は既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。
ネットワーク管理者は、RADIUS サーバ上で 802.1X を使用し、無線 LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」または「 WPA2-Enterprise」を実装した無線 LAN にアクセスする場合、ユーザはユーザ名とパスワードの入力を要求されます。ユーザがネットワーク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危険にさらすことは避けることができます。
EAP（ Extensible Authentication Protocol）は Windows OS に実装されています。802.1X の機能を使用する際には、ネットワークにおけるすべてのデバイスの EAP タイプを同一にする必要があります。

重要
最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

無線に関するご注意

電波に関するご注意

本製品は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。

以下の注意をよくお読みになりご使用ください。

● 本製品を以下の場所では使用しないでください。

- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。
- 電気製品、AV 機器、OA 機器などの磁気を帯びているところや電磁波が発生しているところで使用すると下記のような影響があります。
    - 時期や電気雑音の影響を受けると雑音が大きくなったり、通信ができなくなったりすることがあります。
    - テレビ、ラジオなどに近いと受信障害の原因となったり、テレビ画面が乱れたりすることがあります。
    - 近くに複数の無線 LAN アクセスポイントが存在し、同じチャネルを使用していると、正しく検索できない場合があります。

● 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局) 並びにアマチュア無線局 (免許を必要とする無線局) が運用されています。

● 本製品を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。

● 万一、本製品から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。

● その他、本製品から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 /OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定 小電力無線局並びにアマチュア無線局の帯域を回避可能

5GHz 帯使用に関するご注意

無線 LAN の 5.2/5.3GHz（W52/W53）をご利用になる場合、電波法の定めにより屋外ではご利用になれません。

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

● 通信内容を盗み見られる

悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。

- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

● 不正に侵入される

悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。

- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。
セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
https://www.dlink-jp.com/support/info/product-assurance-provision.html

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。
https://www.dlink-jp.com/support

目次

安全にお使いいただくために 2
ご使用上の注意 4
静電気障害を防止するために 4
電源の異常 4
無線 LAN について 5
WLAN 技術を利用するさまざまな理由 5
無線に関するご注意 6

はじめに 12

本マニュアルの対象者 13
表記規則について 13
製品名 / 品番一覧 13

第 1 章　本製品のご利用にあたって 14

製品概要 14
ポート 14
前面パネル 15
LED 表示 16
背面パネル 17

第 2 章　製品の設置 18

パッケージの内容 18
ネットワーク接続前の準備 18
製品の設置 19
アンテナの取り付け（DSR-1000AC） 19
19 インチラックへの取り付け 19
電源の投入 20
ネットワークへの接続 20

第 3 章　基本設定について 21

Web GUI 画面へのログイン 21
LAN IP アドレスの設定 22
DHCP サーバの設定 23
日付 / 時刻の設定 24
インターネット接続設定 26
ワイヤレスネットワーク接続（DSR-1000AC のみ） 28
ユーザアカウント作成 29
セキュリティ / VPN ウィザード 30
ダイナミック DNS ウィザード（DDNS） 33

第 4 章　LAN 設定（Network） 34

LAN（LAN 設定） 35
LAN Settings（IPv4 ネットワーク用 LAN 設定） 35
LAN DHCP Reserved IPs（LAN DHCP 予約 IP アドレスの設定） 37
IP/MAC Binding（IP/MAC バインディング） 39
IGMP Setup（IGMP 設定） 40
UPnP Setup（UPnP 設定） 40
VLAN（VLAN 設定） 42
VLAN Settings（VLAN 設定） 42
Port VLAN（ポート VLAN / ワイヤレス VLAN） 45

第 5 章　ネットワーク設定（Network） 47

Internet（インターネット接続設定） 48
WAN1 Settings（WAN1 設定） 48
WAN2 / DMZ Setting（WAN2 / DMZ 設定） 59
WAN3 Setting（WAN3 / 3G インターネット設定（未サポート）） 61
WAN Mode（WAN モード設定） 62
SIM Card Authentication（SIM カード認証（未サポート）） 66
Routing Mode（ルーティングモード設定） 67
IP Aliasing（IP エイリアス設定） 69
DMZ Settings（DMZ 設定） 70
DMZ DHCP Reserved IPs（DMZ DHCP の予約 IP 設定） 71
Dynamic DNS（ダイナミック DNS 設定） 72
Traffic Management（トラフィック管理） 73

Jumbo Frames（ジャンボフレーム設定）....80
Routing（ルーティング設定）....81
Static Routes（スタティックルート）....81
RIP（RIP 設定）....82
OSPF（OSPF 設定）....83
Protocol Binding（プロトコルバインディング）....85
IPv6（IPv6 ネットワーク設定）....86
IP Mode（IP モード設定）....86
IPv6 Wan1 Settings（IPv6 ネットワークにおける WAN1 設定）....87
IPv6 Wan2 Settings（IPv6 ネットワークにおける WAN2 設定）....89
Static Routing（IPv6 スタティックルーティング設定）....89
OSPFv3（OSPFv3 設定）....90
6 to 4 Tunneling（6 to 4 トンネル設定）....91
ISATAP Tunnels（ISATAP トンネル設定）....91
Teredo Tunnel（Teredo トンネル設定）....92
IPv6 LAN Settings（IPv6 LAN 設定）....93
IPv6 Tunnels Status（IPv6 トンネルステータス）....98

第 6 章　無線設定（Wireless）（DSR-1000AC のみ）　99

General（一般設定）....100
Access Points（アクセスポイント）....100
Profiles（無線プロファイル）....103
Radio Settings（無線帯域の詳細設定）....105
Advanced（高度な設定）....107
WMM（WMM 設定）....107
WDS（WDS 設定）....108
Advanced Settings（詳細設定）....109
WPS（WPS 設定）....110

第 7 章　VPN 設定（VPN）　112

IPSec VPN（IPSec VPN の設定）....113
Policies（IPSec VPN ポリシーの設定）....113
Tunnel Mode（トンネルモード）....116
DHCP Range（IP アドレス範囲の設定）....118
Certificate（認証証明書）....119
Easy VPN Setup（VPN セットアップ）....122
One To One Mapping（One To One マッピング）....122
PPTP VPN（PPTP VPN 設定）....123
PPTP Server（PPTP VPN サーバ設定）....123
PPTP Client（PPTP クライアント）....124
PPTP Active Users（PPTP アクティブユーザリスト）....125
L2TP VPN（L2TP VPN 設定）....126
L2TP Server（L2TP VPN サーバ設定）....126
L2TP Client（L2TP VPN クライアント）....127
L2TP Active Users（L2TP アクティブユーザリスト）....128
SSL VPN（SSL VPN 設定）....129
SSL VPN 対応 OS/ ブラウザー覧 129
SSL VPN Server Policy（SSL VPN ポリシー設定）....130
Portal Layouts（ポータルレイアウトの作成）....131
Resources（ネットワークリソース）....133
SSL VPN Client（SSL VPN クライアント設定）....137
Client Routes（SSL VPN クライアントルート設定）....138
OpenVPN（OpenVPN 設定）....139
OpenVPN 設定....139
OpenVPN Certificates（Open VPN 証明書）....141
OpenVPN Server Policy（Open VPN サーバポリシー）....145
Local Networks（ローカルネットワーク設定）....146
Remote Networks（リモートネットワーク設定）....147
OmniSSL Client Configuration（OmniSSL クライアント設定）....148
OmniSSL Portal Layouts（OmniSSL ポータルレイアウト）....149
GRE（GRE 設定）....150
GRE Tunnels（Gre トンネル設定）....150

第 8 章　セキュリティ設定（Security）　152

Authentication（認証設定）....153
Internal User Database（内部ユーザデータベース）....153
External Auth Server（外部認証）....160
Radius Accounting（Radius アカウンティング設定）....166
Login Profiles（ログインプロファイル）....168
Services Route Management（サービスルート管理）....170
DUA External CP Web（DUA 外部キャプティブポータル Web サーバ）....171
Web Content Filter（Web コンテンツフィルタリング）....172
Static Filtering（スタティックフィルタリング）....172
Dynamic Filtering（ダイナミックフィルタリング）....175
URL Filtering ACL（URL フィルタリング ACL）....177
Firewall（ファイアウォール設定）....178
Firewall Rules（ファイアウォールルールの設定）....178
Schedule（ファイアウォールスケジュール設定）....181
Blocked Clients（クライアントブロック設定）....182
Custom Services（カスタムサービスの設定）....183
ALGs（ALG サポート）....184
VPN Passthrough（VPN パススルー）....188
Dynamic Port Forwarding（ダイナミックポートフォワーディング）....189
Attack Checks（攻撃のチェック）....191
Intel® AMT（インテル ® アクティブ・マネジメント・テクノロジー）....192
IPS（侵入防止システム）....193
App Control Policy（アプリケーションコントロールポリシー）....194
Application Control（アプリケーションコントロール）....194

第 9 章　メンテナンス（Maintenance）　199

Administration（システム管理設定）....200
System Setting（システム名の設定）....200
Data and Time（システムの日時設定）....200
Session Settings（セッションタイムアウトの設定）....201
License Update（WCF ライセンスのアップデート）....202
USB Share Ports（USB 共有ポートの設定）....203
SMS Service（SMS サービス（未サポート））....204
Package Manager（パッケージマネージャ）....206
Set Language（言語設定）....209
Web GUI Management（Web GUI 管理）....210
Management（管理設定）....211
Remote Management（リモート管理）....211
SNMP（SNMP の使用）....212
Diagnostics（診断ツール）....216
Power Saving（省エネ設定）....222
DDP Client（DDP クライアント設定）....223
Firmware & Config（ファームウェアとコンフィグ）....224
Firmware Upgrade（ファームウェアアップグレード）....224
Backup/Restore（コンフィグレーションのバックアップとリストア）....227
Soft Reboot（再起動／工場出荷時設定の復元）....229
Logs Settings（ログ設定）....231
Log Facilities（ログファシリティ）....231
Routing Logs（ルーティングログ）....232
Sytem Log（System ログ）....234
Remote Logging（リモートログ）....235
SMS Logging（SMS ログ（未サポート））....238

第 10 章　ステータス情報（Status）　239

Dashboard（ダッシュボード画面）....240
System Information（システム状態の参照）....242
Device（デバイス状態の参照）....242
All Logs（ログ）....247
USB Status（USB ステータス）....248
Network Information（ネットワーク情報の参照）....249
DHCP クライアントの参照....249
CaptivePortal Sessions（キャプティブポータルセッションの参照）....250
Active Sessions（アクティブセッションの参照）....251
Active VPNs（VPN セッションの参照）....251
Interfaces Statistics（インタフェースの統計）....254
Wireless Clients（無線クライアントの参照）....255
Wireless Statistics（無線の統計情報）....255
Device Statistics（デバイス統計情報）....256
LAN Clients（LAN クライアント）....256
Session Limiting Status（セッション制限ステータス）....257

第 11 章　トラブルシューティング　258

インターネット接続....258
日付と時間....260
LAN の接続性をテストするために Ping する....260
ご使用の PC からルータまでの LAN パスをテストする....260
ご使用の PC からリモートデバイスまでの LAN パスをテストする....261
工場出荷時設定へのリセット....261

付録　262

【付録 A】用語解説....262
【付録 B】工場出荷時設定....263
【付録 C】ポートフォワーディングとファイアウォール設定に利用可能な標準サービス....263
【付録 D】ログメッセージ....264

はじめに

本マニュアルでは、DSR-500/1000/1000AC の設置および操作方法について説明します。
各パラメータの説明については、本製品の Web GUI 上にあるオンラインヘルプ もご参照ください。

「第 1 章　本製品のご利用にあたって」
- 本製品の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

「第 2 章　製品の設置」
- 本製品の基本的な設置方法と接続方法について説明します。

「第 3 章　基本設定について」
- 製品を使用する上で必要な基本的設定について説明します。

「第 4 章　LAN 設定（Network）」
- 本製品の LAN、WAN の設定方法について説明します。

「第 5 章　ネットワーク設定（Network）」
- 本製品のインターネットへの接続、設定方法について説明します。

「第 6 章　無線設定（Wireless）（DSR-1000AC のみ）」
- 本製品の無線アクセスポイント設定、無線プロファイル、無線帯域設定、WMM、WDS などについて説明します。

「第 7 章　VPN 設定（VPN）」
- ゲートウェイルータ間、またはリモート PC クライアント間の安全な通信のための VPN 機能について説明します。

「第 8 章　セキュリティ設定（Security）」
- 本製品のネットワークの安全を確保するための多くのセキュリティ機能について説明します。

「第 9 章　メンテナンス（Maintenance）」
- 本製品のメンテナンス作業について説明します。

「第 10 章　ステータス情報（Status）」
- 本製品とネットワークのステータス情報ついて説明します。

「第 11 章　トラブルシューティング」
- 本製品のインストールと操作で発生する問題への解決策を提供します。

「付録」
- 工場出荷時設定、ログメッセージなどを記載しています。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	Web GUI 上の UI 名を示します。	「OK」をクリックし、設定を適用します。
青字	参照先または URL を示します。	「Web GUI 画面へのログイン」をご参照ください。
Menu Name > Menu Option	メニュー構造を示します。	**Device > Port > Port Properties** は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

1.
製品名 / 品番一覧

製品名	品番
DSR-500	DSR-500/B1
DSR-1000	DSR-1000/B1
DSR-1000AC	DSR-1000AC

第 1 章　本製品のご利用にあたって

ここでは、本製品の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

- 「製品概要」
- 「ポート」
- 「前面パネル」
- 「背面パネル」

製品概要

DSR-500/1000/1000AC は、SOHO などの小規模ビジネスにおいて、無線 LAN AP（1000AC のみ）と VPN をオールインワンで提供可能な 802.11ac 対応ワイヤレス VPN ルータです。高速ワイヤレス通信に対応する IEEE 802.11ac により、通常の有線ネットワーク通信と同等の通信環境を構築することができます。最適なネットワークセキュリティは各種 VPN 機能、IPSecurity（IPSec）、Point-to-Point Tunneling Protocol（PPTP）、Layer2 Tunneling Protocol（L2TP）、そして Secure Sockets Layer（SSL）等の機能によって提供されています。さらに SSL VPN トンネル機能を利用して、時間や場所を気にせずリモートアクセスすることが可能です。

多彩な管理機能

DSR-500/1000/1000AC は、ポリシーベースサービスマネージメント機能を提供するデュアル WAN ギガビットイーサネットを搭載しており、生産性を最大に発揮します。フェイルオーバ機能はネットワーク通信を切断することなく、ネットワークトラフィックのデータを維持することができ、WAN ロードバランシング機能は WAN インタフェースから送信されるトラフィックを調整し、システムパフォーマンスを最適化します。2 ポートあるうちの 1 つの WAN ポートを DMZ のポートとして設定し、LAN からサーバを隔離することも可能です。

高速ワイヤレスネットワーク（DSR-1000AC）

DSR-1000AC は、IEEE802.11ac/a/b/g/n の無線標準規格に準拠しており、2.4GHz もしくは 5GHz の周波数帯域を使用することができ、既に構築済みのワイレスネットワークにも柔軟に対応することが可能です。最新の IEEE802.11ac に対応し、高速なワイヤレスネットワークを構築することができます。

優れた VPN 機能

Virtual Pivate Network（VPN）機能により、モバイル端末を使用しているユーザや支店からも安全にネットワークへ接続することができ、同時に 15（DSR-500）、25（DSR-1000/1000AC）の SSL VPN トンネルをそれぞれに管理することができます。会社のデータベース等へ接続することができるリモートアクセス権限をモバイルユーザに割当てることで、瞬時に必要なデータを取得し、外出先で様々な対応を迅速にとることが可能となり、作業効率を上げていくことが可能です。

IPv6 対応

DSR-500/1000/1000AC は、IPv6/WAN ネットワークへの接続に対応するとともに、PPPoE（IPv6）や IPv6 スタティックルートなど様々な IPv6 機能を搭載し、IPv6 ネットワークへの移行に柔軟に対応できます。

D-Link Green 省電力機能

「D-Link Green 省電力機能」は、リンクダウン時とケーブル長に応じて、自動で消費電力を削減する仕組みです。これにより環境への配慮、製品寿命の延命化、発熱の抑制、運用時のコスト削減を実現します。

ポート

DSR シリーズは以下のポートを搭載しています。

ポート	DSR-500	DSR-1000	DSR-1000AC
10BASE-T/100BASE-TX/1000BASE-T ポート	WAN x 2、LAN x 4（10/100/1000 Mbps）		
コンソールポート	1		
USB ポート	1	2	2

前面パネル

前面パネルの各部名称と機能について説明します。

DSR-500

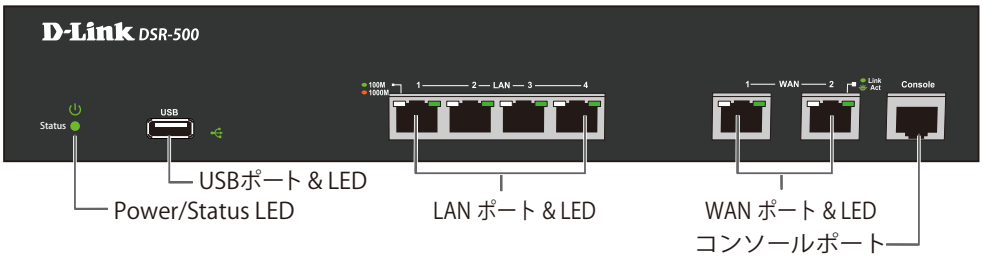

図 1-1　前面パネル（DSR-500）

DSR-1000

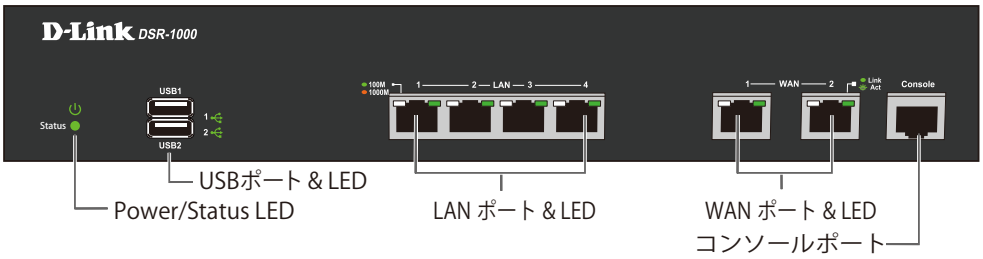

図 1-2　前面パネル（DSR-1000）

DSR-1000AC

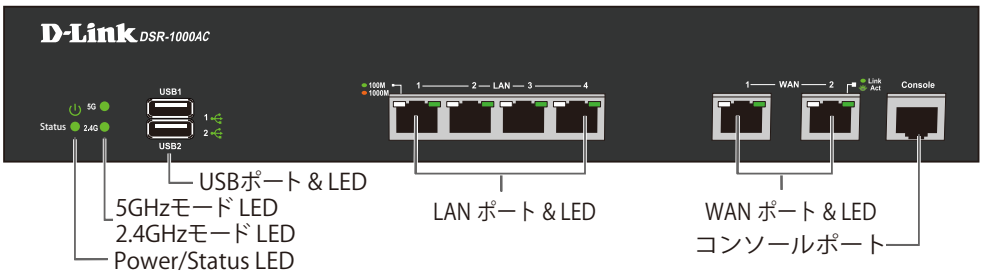

図 1-3　前面パネル（DSR-1000AC）

機能	説明
Power / Status LED 5GHz / 2.4GHz モード LED*	LED の点灯状態で本製品の状態を示します。 LED 表示については「」を参照してください。
USB ポート / LED	USB ポートには、USB2.0/USB1.1 対応フラッシュディスクやハードディスクを接続できます。 注意　3G 機器は未サポートです。
LAN ポート	UTP ケーブルを使用し、スイッチやハブなどのイーサネットデバイスと接続します。
WAN ポート	UTP ケーブルを使用し、ケーブルモデムまたは DSL モデムに接続します。 WAN2 ポートは、DMZ ポートとしても設定可能です。
コンソールポート	RJ45-to-DB9 コンソールケーブルを接続し、CLI（コマンドラインインタフェース）にアクセスします。

* DSR-1000AC のみ

LED 表示

本製品の LED 表示について説明します。

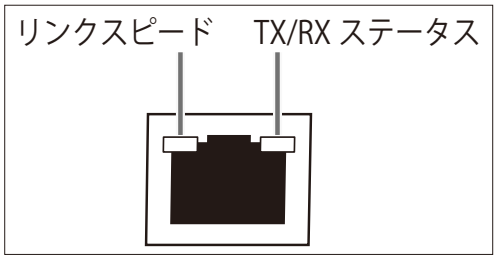

図 1-4　WAN/LAN LED

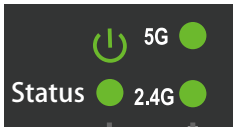

図 1-5　Power/Status、無線モード（5G/2.4G）LED

図 1-6　USB LED

LED	状態	色	状態説明
Power	点灯	緑	製品に電源が供給され正常に動作しています。
	点滅	緑	システムにファームウェアアップグレードの失敗などの不具合が生じています。
	消灯	―	製品に電源が供給されていません。
Status	点灯	橙	製品の起動中です。
	点滅	橙	製品がクラッシュしているか、またはリカバリモード中です。
	消灯	―	製品が正常に動作しています。
5GHz※（DSR-1000AC）	点灯	緑	5GHz 無線 LAN による通信が可能な状態です。
	点滅	緑	5GHz 無線 LAN によりデータを送受信しています。
	消灯	―	5GHz 無線 LAN による通信が不可能な状態です。
2.4GHz※（DSR-1000AC）	点灯	緑	2.4GHz 無線 LAN による通信が可能な状態です。
	点滅	緑	2.4GHz 無線 LAN によりデータを送受信しています。
	消灯	―	2.4GHz 無線 LAN による通信が不可能な状態です。
リンクスピード（WAN / LAN）	点灯	橙	1000Mbps でリンクが確立しています。
	点灯	緑	100Mbps でリンクが確立しています。
	消灯	―	ポートは 10Mbps で動作中です。
TX/RX ステータス（WAN / LAN）	点灯	緑	リンクが確立しています。
	点滅		データを送受信しています。
	消灯	―	リンクが確立していません。
USB	点灯	緑	USB デバイスが接続しています。
	点滅		USB デバイスとのデータ送受信を行っています。
	消灯		USB デバイスが接続していません。

* DSR-1000AC のみ

背面パネル

背面パネルの各部名称と機能について説明します。

DSR-500/1000

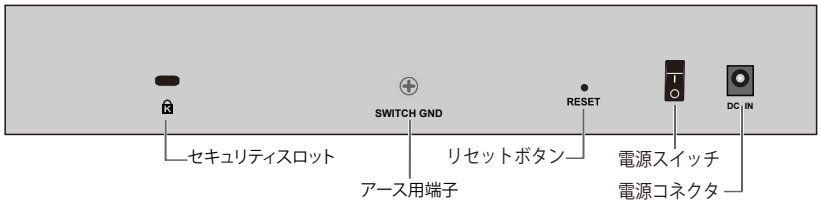

図 1-7　背面パネル図（DSR-500/1000）

DSR-1000AC

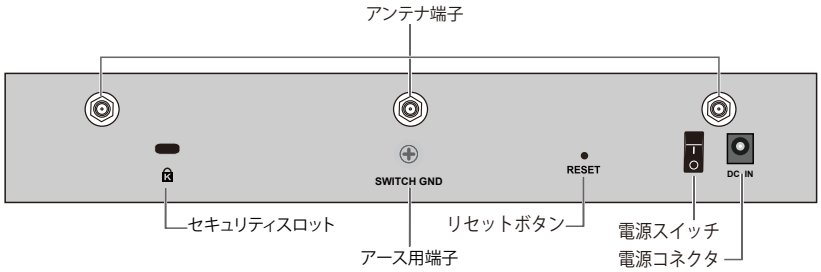

図 1-8　背面パネル図（DSR-1000AC）

部位	機能
セキュリティスロット	市販のセキュリティロックの取り付けが可能です。
アース用端子	アース線を接続し、接地を行います。
リセットボタン	本製品を工場出荷時設定にリセットします。
電源コネクタ	付属の AC ケーブルを接続します。
電源スイッチ	電源の ON、OFF を行います。
アンテナ端子（DSR-1000AC）	DSR-1000AC に付属のアンテナを接続します。

第 2 章　製品の設置

- 「パッケージの内容」
- 「ネットワーク接続前の準備」
- 「製品の設置」
- 「電源の投入」
- 「ネットワークへの接続」

パッケージの内容

本製品を箱から取り出したら、以下の同梱物があることを確認してください。
万一、不足しているものや損傷を受けているものがありましたら、ご購入いただいた代理店にお問い合わせください。

- 本体
- AC 電源アダプタ
- ネットワークケーブル
- RJ45/DB9 変換ケーブル
- ラックマウントキット
- ゴム足
- CD-ROM
- アンテナ× 3 （DSR-1000AC のみ）
- GNU GPL ライセンスノート
- PL シート

ネットワーク接続前の準備

製品の設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

- 製品は、しっかりとした水平面で耐荷重性のある場所に設置してください。
- 製品の上に重いものを置かないでください。
- 本製品から 1.82m 以内の電源コンセントを使用してください。
- 電源アダプタが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本製品の周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 16cm 以上の空間を保つようにしてください。
- 製品は動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- 製品は強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- 製品を水平面に設置する際は、製品底面に同梱のゴム足を取り付けてください。ゴム製の足は製品のクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

設置にあたってのご注意
本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になりますが、壁や天井など無線信号が通過する物体の数や厚さ、場所などにより、動作範囲が制約を受ける場合があります。一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

1. 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。一枚の壁や天井の影響により、本製品の動作範囲は 1 ～ 30 メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。
2. ネットワークデバイス間の直線距離にご注意ください。厚さ 50 センチの壁を 45 度の角度で無線信号が通過する時、通り抜ける壁の厚みは約 1 メートルになります。2 度の角度で通過すると、通り抜ける厚みは 14 メートルになります。信号が障害物をなるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。
3. 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線 LAN デバイスや無線 LAN アダプタ使用のコンピュータの設置は、信号がなるべく乾式壁か開放された戸口などを通るような位置に設置してください。
4. 周波数ノイズを発生する電気機器や家電製品からは、最低でも 1、2 メートル離してデバイスを設置してください。
5. 2.4GHz のコードレス電話または X-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz 電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。
6. 必ず付属の AC 電源アダプタをご使用ください。

製品の設置

アンテナの取り付け（DSR-1000AC）

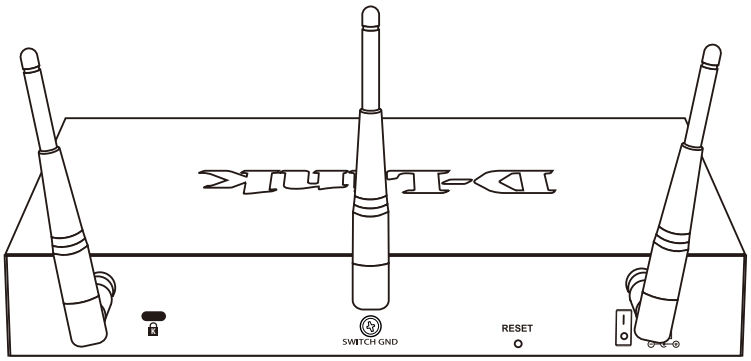

図 2-9　アンテナの取り付け

1. 付属の 3 本のアンテナを本体のアンテナ端子に取り付けます。取り付けの際には、アンテナは折り曲げずに本体のアンテナ接合部に接続し、右方向に締めます。
2. 取り付け後に折り曲げます。
3. 電波状況に合わせてアンテナの向きを変更します。

19 インチラックへの取り付け

以下の手順に従って本製品を標準の 19 インチラックに設置します。

ブラケットの取り付け

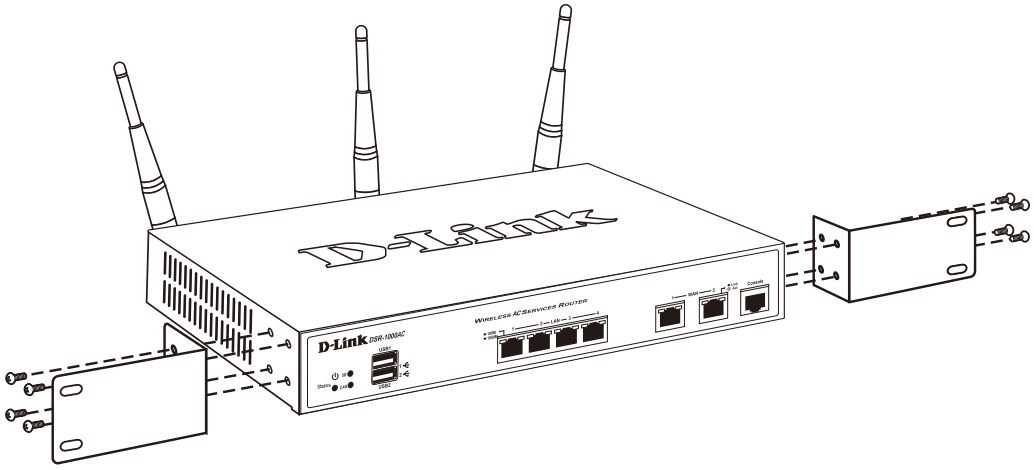

図 2-10図 2-2　ブラケットの取り付け

ラックマウントキットに付属のネジを使用して、本製品にブラケットを取り付けます。完全にブラケットが固定されていることを確認し、本製品を以下の通り標準の 19 インチラックに固定します。

19 インチラックに本製品を取り付ける

警告 前面、側面にスタビライザを取り付けないで製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム / コンポーネントを取り付けた後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つだけとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

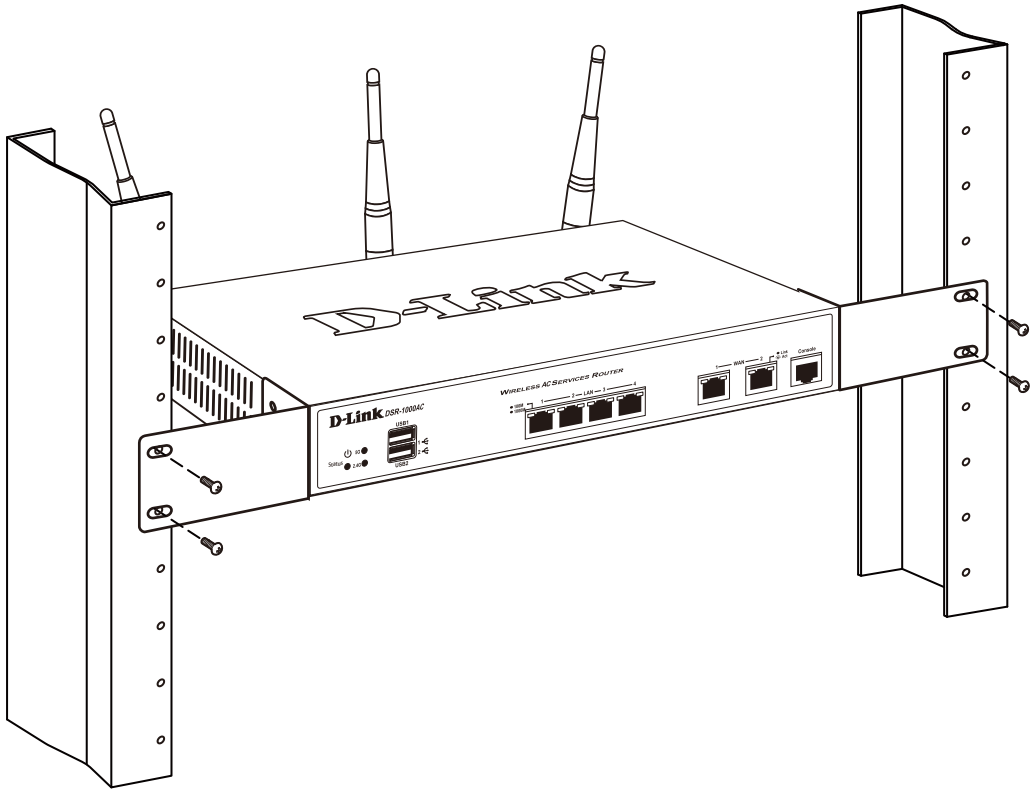

図 2-11図 2-3　製品のラックへの設置

電源の投入

1. 電源アダプタを本製品の電源コネクタに接続します。電源アダプタのプラグを電源コンセントに接続します。
2. 本製品の電源スイッチを「ON」にします。本製品に電源が供給されると、Power LED が緑色に点灯します。

ネットワークへの接続

本製品の物理的なネットワークへの接続について説明します。

1. 外部ルータ、またはモデムと本製品の WAN ポートをイーサネットケーブルで接続します。WAN ポートは WAN のネットワークセグメントに属することになります。
2. LAN セグメントに属するスイッチ、または PC と本製品の LAN ポートをイーサネットケーブルで接続します。
3. CLI での設定を行う場合は、付属のコンソールケーブルを使用し、コンソールポートを管理 PC を接続します。

第 3 章　基本設定について

Web GUI 画面へのログイン方法、IP アドレスの設定方法など、基本的な設定について説明します。

- 「Web GUI 画面へのログイン」
- 「LAN IP アドレスの設定」
- 「DHCP サーバの設定」
- 「日付 / 時刻の設定」
- 「インターネット接続設定」
- 「ワイヤレスネットワーク接続（DSR-1000AC のみ）」
- 「ユーザアカウント作成」
- 「セキュリティ / VPN ウィザード」
- 「ダイナミック DNS ウィザード（DDNS）」

Web GUI 画面へのログイン

本製品の設定は、本製品と UTP ケーブルで接続した PC から行うことができます。Web ブラウザを使用して、本製品の Web GUI にアクセスしてください。
対応している Web ブラウザ：Internet Explorer/Firefox/Chrome/Safari

1. UTP ケーブルを使用し、LAN ポートと設定用 PC を接続します。
2. 本製品と設定用 PC の IP アドレスが同じサブネット内にあることを確認します。（本製品の IP アドレスの初期値：192.168.10.1）
3. Web ブラウザを起動します。
4. 本製品の IP アドレスをアドレスバーに入力し、Enter キーを押します。

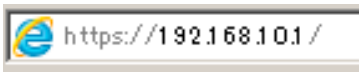

図 3-1　アドレス入力画面

注意　本製品の IP アドレスが初期値から変更されている場合は、変更後のアドレスを入力します。

5. ログイン画面で「Username」と「Password」を入力します。

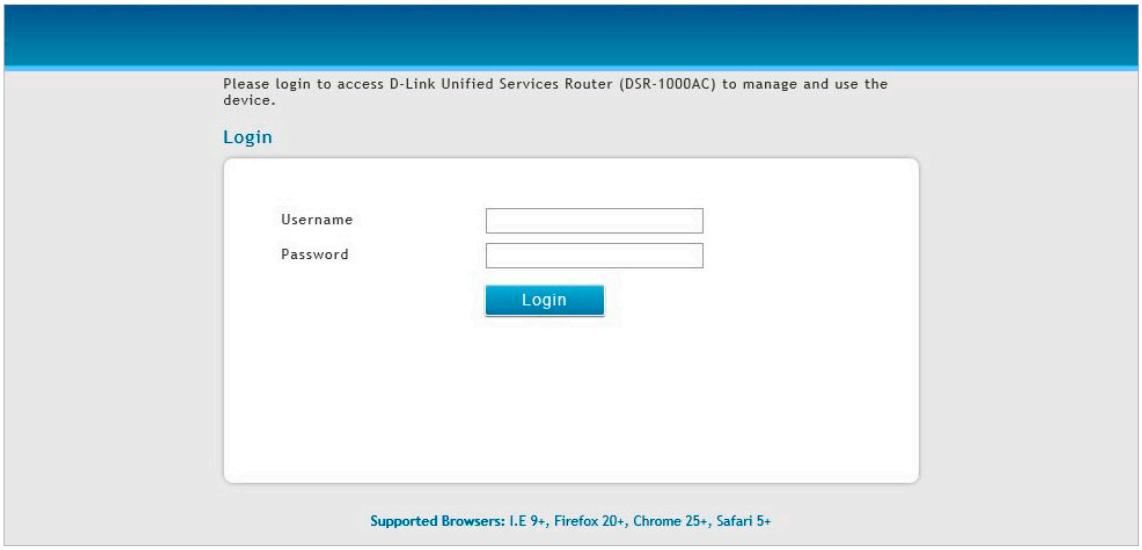

図 3-2　Login 画面

「Username」と「Password」の初期値は「admin」です。

Web GUI のログインパスワードを変更する場合は、**Security > Authentication > Internal User Database > Users タブ**画面で設定を行います。詳細は「ユーザ情報の編集」を参照してください。

6. 「Login」をクリックします。
7. **Status > Dashboard** 画面がトップページとして表示されます。

LAN IP アドレスの設定

LAN IP アドレスの設定方法について説明します。

1. **Network > LAN > LAN Settings** をクリックし、以下の画面を表示します。

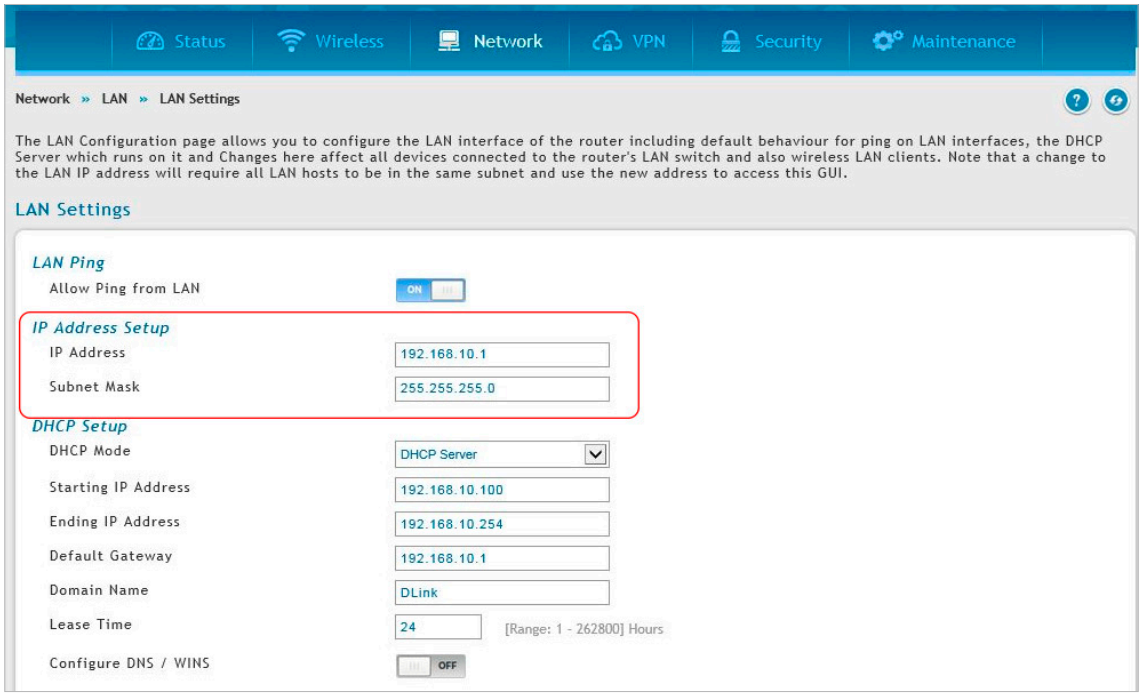

図 3-3　LAN Settings 画面（IP Address Setup）

2. 「IP Address Setup」で、新しい IP アドレスを入力します。
3. 必要に応じて、サブネットマスクを変更します
4. 「Save」をクリックし、設定を適用します。

注意 IP アドレスを変更して「Save」をクリックすると、Web GUI が応答しなくなります。
変更後の IP アドレスを使用し、再度 Web GUI にログインしてください。

DHCP サーバの設定

DHCP サーバの設定方法について説明します。

1. **Network > LAN > LAN Settings** をクリックし、以下の画面を表示します。

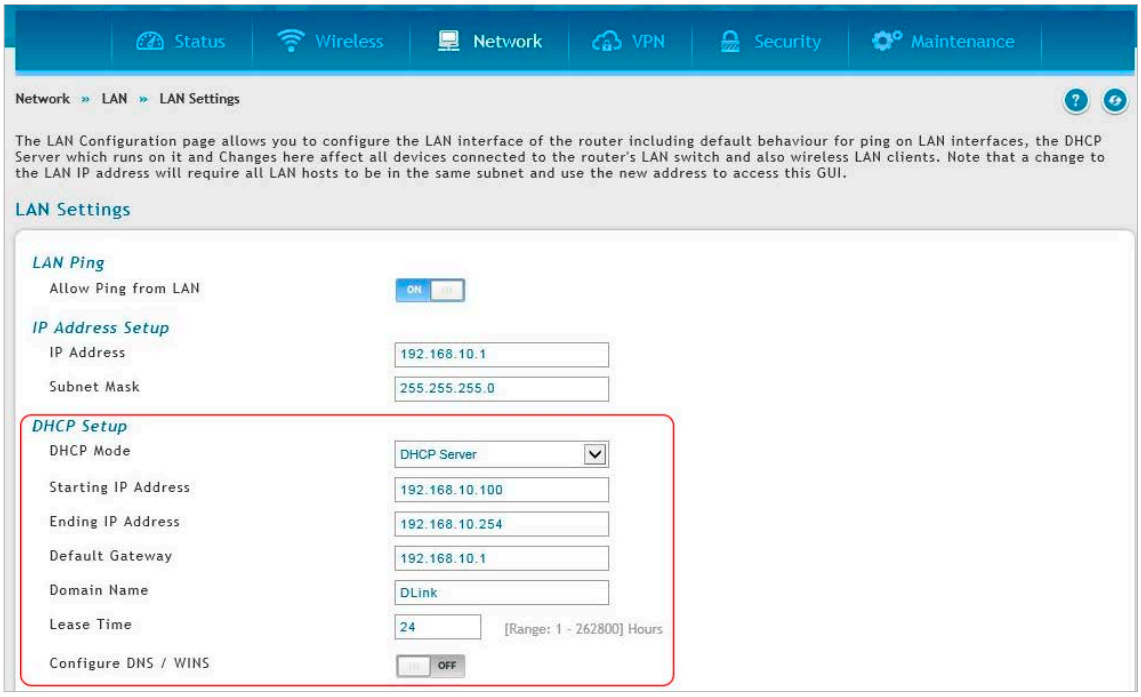

図 3-4　LAN Settings 画面（DHCP Setup）

2. 「DHCP Setup」セクションの「DHCP Mode」で、DHCP のモードを「None」「DHCP Server」「DHCP Relay」から選択します。

注意 「DHCP Relay」を選択すると、LAN 上の DHCP クライアントは異なるサブネットにある DHCP サーバから IP アドレスリースと対応する情報を受け取ることができます。これにより LAN クライアントが DHCP 要求を行うとリレーゲートウェイ IP アドレスを通してアクセス可能なサーバに送られます。

3. 必要に応じて以下の項目を設定します。

項目	説明
Starting / Ending IP Address	DHCP アドレスプールの開始 IP アドレスと終了アドレスを入力します。 LAN に参加する新規の DHCP クライアントには、「Starting IP Address」（開始 IP アドレス）と「Ending IP Address」（終了 IP アドレス）で指定した範囲内の IP アドレスが割り当てられます。 開始 IP アドレスと終了 IP アドレスは、ルータの LANIP アドレスと同じサブネット内である必要があります。 ・開始アドレスの初期値：192.168.10.100 ・終了アドレスの初期値：192.168.10.254
Default Gateway	デフォルトゲートウェイを入力します。 初期値はルータの LAN IP アドレス（192.168.10.1）です。 ネットワークのゲートウェイがこのルータでない場合は、LAN サブネット内の任意の有効な IP に設定することができます。 設定した IP アドレスはデフォルトゲートウェイとして DHCP サーバから DHCP クライアントに付与されます。
Domain Name	識別に使用するネットワークのドメイン名を入力します。
Lease Time	IP アドレスがクライアントにリースされる期間を入力します。 ・設定可能範囲：1-262800（時） ・初期値：24（時）
Configure DNS/WINS	「ON」を選択した場合、DNS/WINS サーバの IP アドレスを入力します。

4. 「Save」をクリックし、設定を適用します。

日付 / 時刻の設定

日付 / 時刻の設定方法について説明します。

1. 「Wizard」をクリックします。

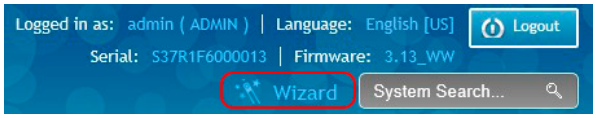

図 3-5　Wizard button 画面

2. 「Date and Time Wizard」内の「Run」をクリックします。

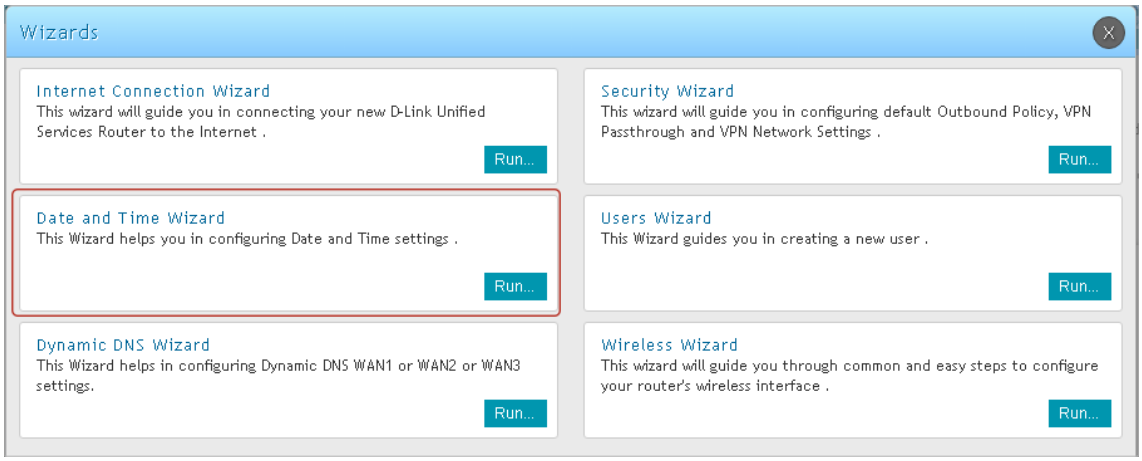

図 3-6　Wizards 画面

3. 地図から設定する地域を選択　→「City」からタイムゾーンを選択します。

4. サマータイムを有効にする場合は「Daylight Saving」を「ON」にします。

5. 「Next」をクリックします。

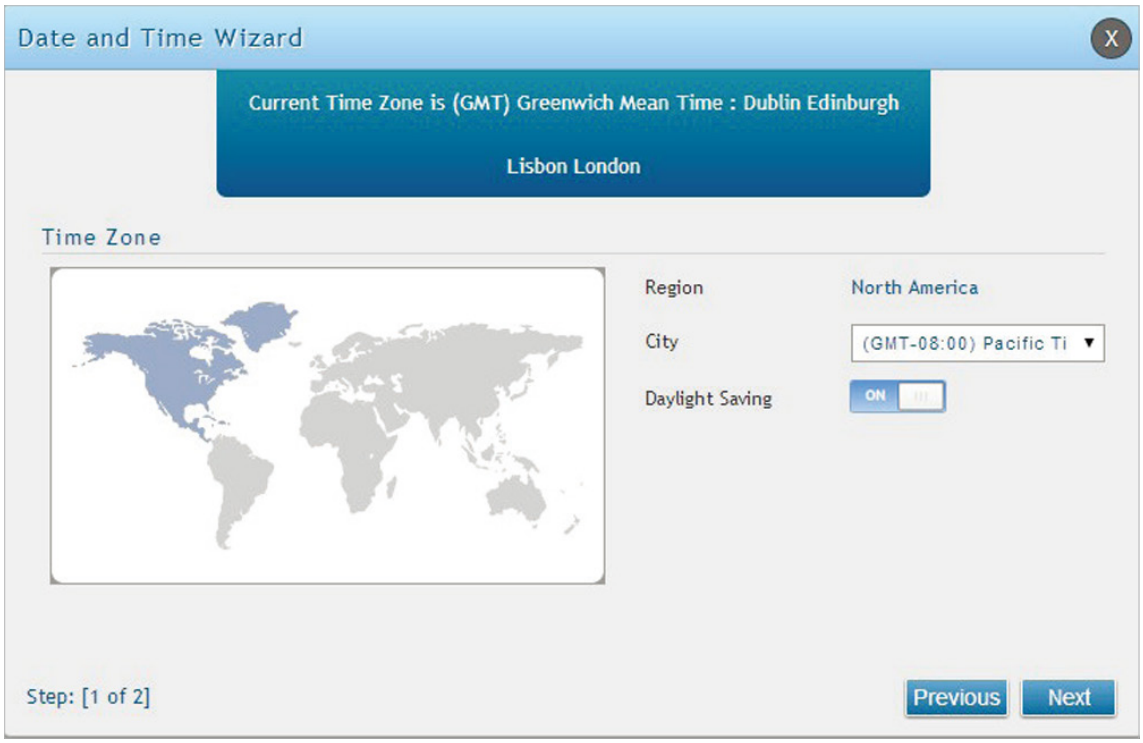

図 3-7　Date and Time Wizard > Time Zone 画面

6. NTP サーバを使用する場合は「NTP Server」を「ON」にします。手動で時間と日付を指定する場合は「OFF」にします。

7. 「ON」を選択した場合、「NTP Server Type」で「Default」または「Custom」を選択します。
「Custom」を選択した場合、プライマリ / セカンダリ NTP サーバアドレスを入力します。

8. 「Time to Synchronize」で NTP サーバとの同期時間を指定します。

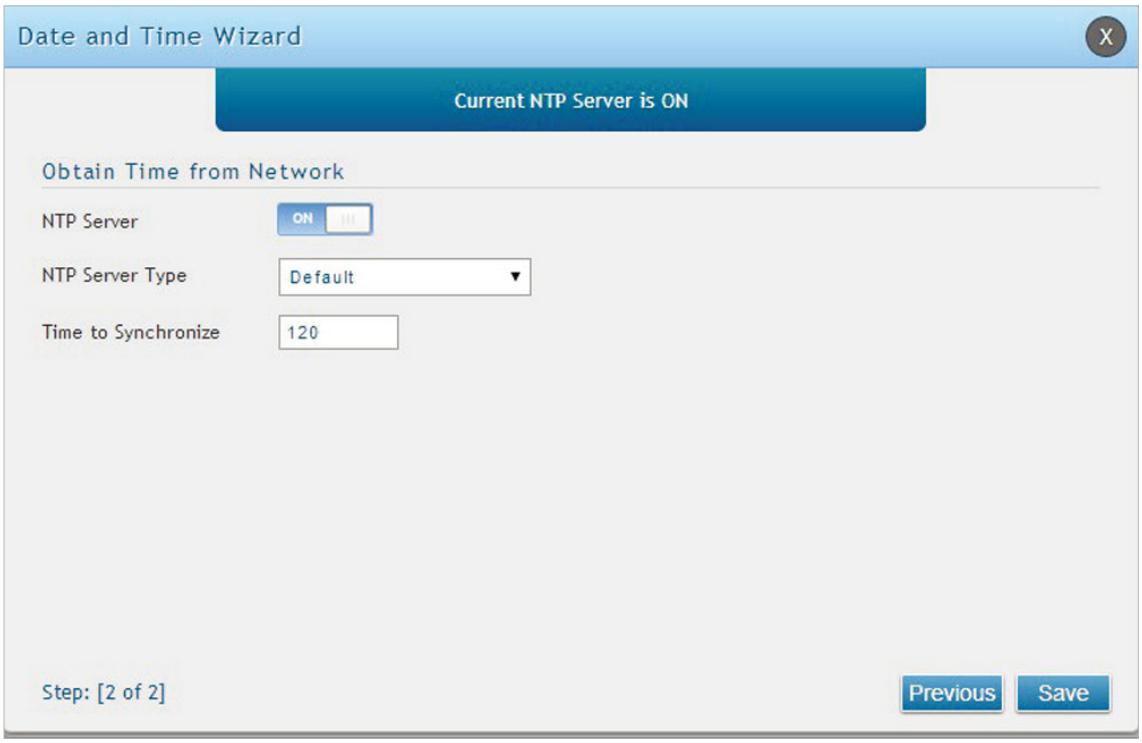

図 3-8　Date and Time Wizard > Obtain Time from Network 画面

9. 「Save」をクリックし、設定を適用します。

10. 確認画面が表示されます。確認後、「Finish」をクリックします。

インターネット接続設定

本製品は二つの WAN ポート保持しており、それらを使用してインターネット接続が利用できます。

ルータのインターネット接続には、現在使用しているインターネットサービスプロバイダ（ISP）からの情報が必要です。設定の際、必要な情報については ISP またはネットワーク管理者にご確認ください。

本製品がサポートしているインターネットの接続タイプは「DHCP」「Static IP Address」「PPPoE」「PPTP」「L2TP」「Japanese multiple PPPoE」「Russian dual PPPoE/PPTP/L2TP」です。本項目では「DHCP」または「Static IP Address」での接続方法を提示します。

1. ルータにログインします。

2. 手動でインターネットの設定を行う場合は「**Wizard**」をクリックします。

図 3-9　Wizard 画面

3. 「Internet Connection Wizard」内の「Run」をクリックします。

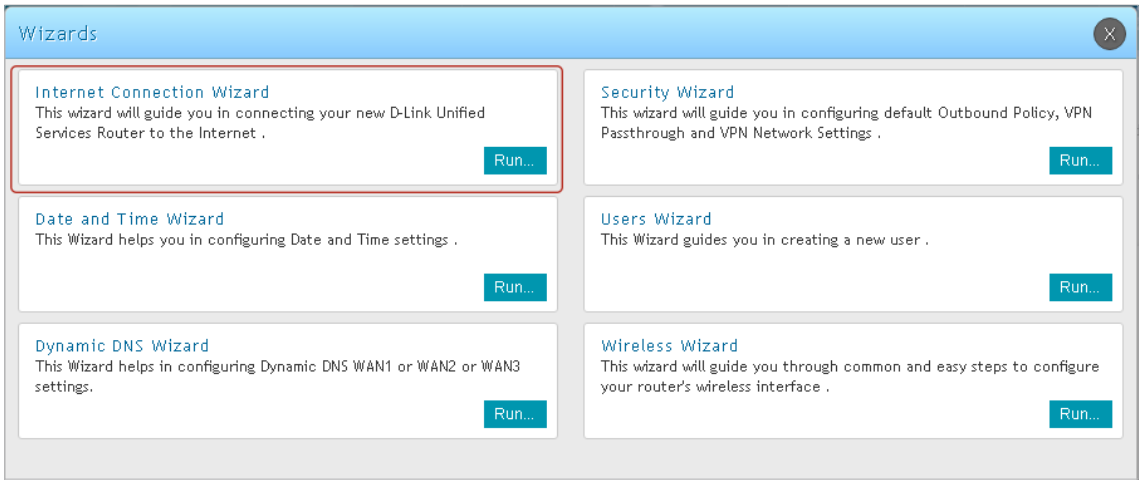

図 3-10　Internet Connection Wizard ボックス 画面

4. 「DHCP」「Static IP Address」のいずれかを「ON」にし、「Next」をクリックします。

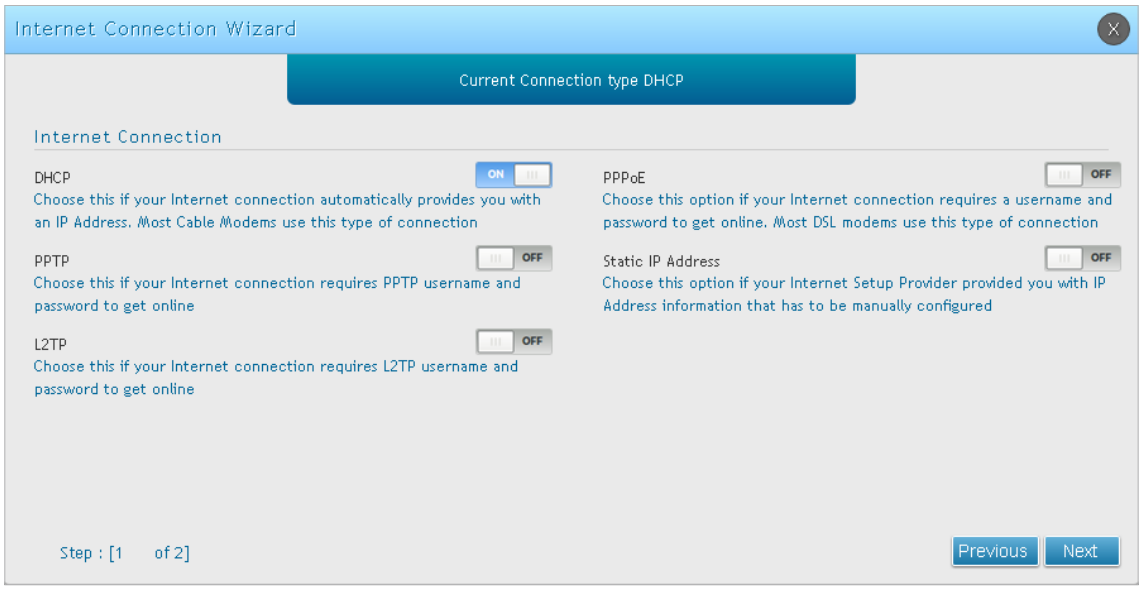

図 3-11　Internet Connection Wizard 画面

5. 「DHCP」を選択した場合、以下の画面で設定を行います。

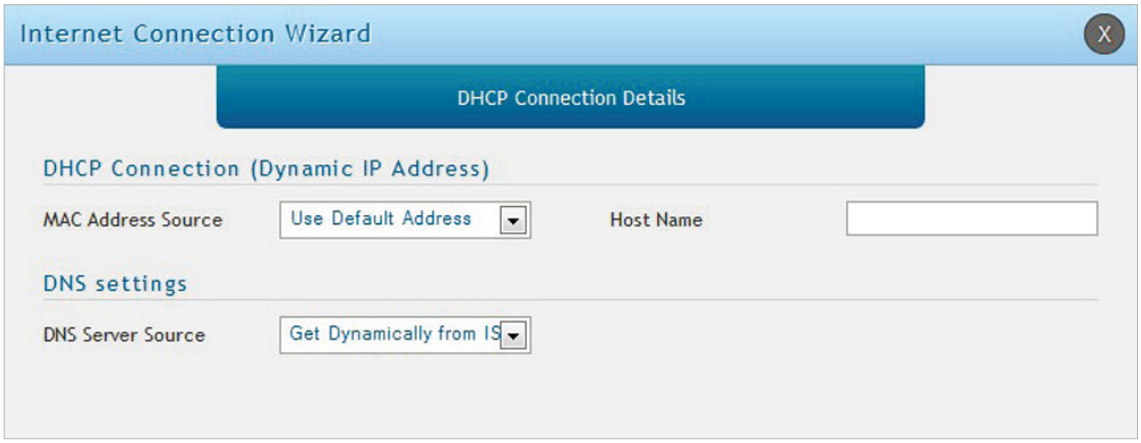

図 3-12　Internet Connection Wizard（DHCP）画面

項目	説明
DHCP Connection (Dynamic IP Address)	
MAC Address Source	ご契約の ISP に認識される MAC アドレスを指定します。 • 「Use Default Address」：本ルータのデフォルト MAC アドレスを使用します。 • 「Clone your PC's MAC Address」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC Address」：手動で MAC アドレスを設定します。
Host Name	ISP に提供する必要がある場合、ホスト名を入力します。
DNS settings	
DNS Server Source	DNS サーバを指定する方式を選択します。 • 「Get Dynamically from ISP」：ISP によって割り当てられた DNS サーバを使用します。 • 「Use These DNS Servers」：手動でプライマリ / セカンダリ DNS サーバの IP アドレスを設定します。

6. 「Static IP Address」を選択した場合、以下の画面で設定を行います。

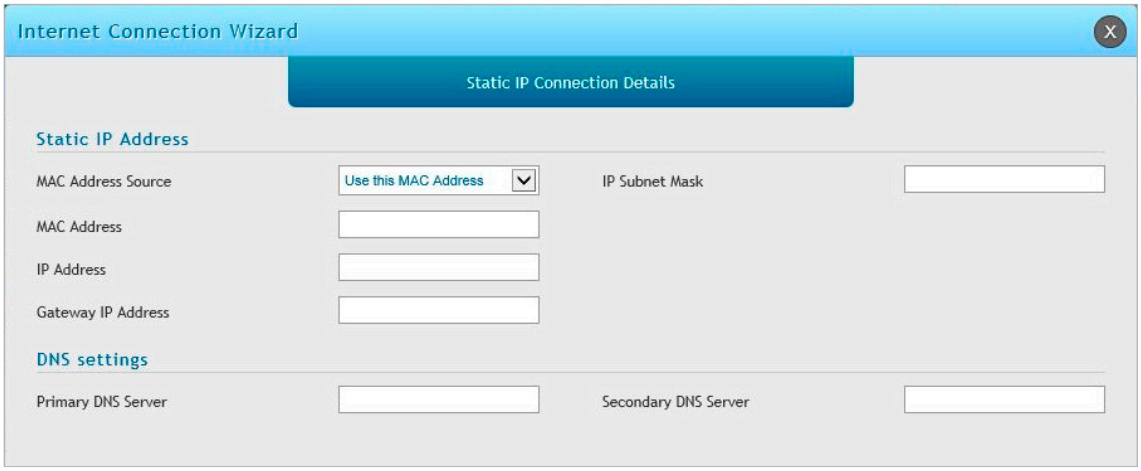

図 3-13　Internet Connection Wizard（Static IP Address）画面

項目	説明
Static IP Address	
MAC Address Source	ご契約の ISP に認識される MAC アドレスを指定します。 • 「Use Default Address」：本ルータのデフォルト MAC アドレスを使用します。 • 「Clone your PC's MAC Address」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC Address」：手動で MAC アドレスを設定します。
IP Address	ISP から割り振られた IP アドレスを指定します。
Gateway IP Address	ISP から割り振られたゲートウェイ IP アドレスを指定します。
IP Subnet Mask	ISP から割り振られたサブネットマスクを指定します。
DNS settings	
Primary DNS Server	ISP から割り振られたプライマリ DNS サーバの IP アドレスを指定します。
Secondary DNS Server	ISP から割り振られたセカンダリ DNS サーバ IP アドレスを指定します。

7. 「Save」をクリックし、設定を適用します。

インターネット接続のためルータが再起動します。接続まで数分お待ちください。

ワイヤレスネットワーク接続（DSR-1000AC のみ）

ワイヤレスネットワークのネットワーク名（SSID）とネットワークキー（事前共有鍵）の設定を行います。
SSID は、クライアントが AP を検出するための識別名です。本製品は、WPA / WPA2 セキュリティに TKIP+AES 暗号を使用します。クライアント側のサポート状況によって、WPA または WPA2 を使用して AP に接続します。事前共有鍵の初期値は「passphrase」です。

1. 「**Wizard**」をクリックします。

図 3-14　Wizard 画面

2. 「Wireless Wizard」内の「Run」をクリックします。

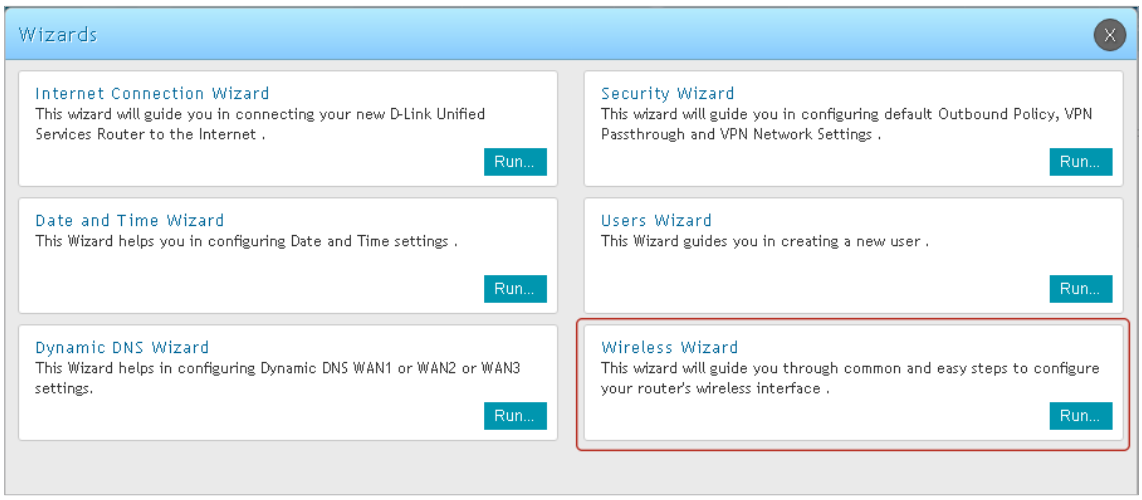

図 3-15　Wireless Wizard ボックス 画面

3. 「Wireless Wizard」画面が表示されます。

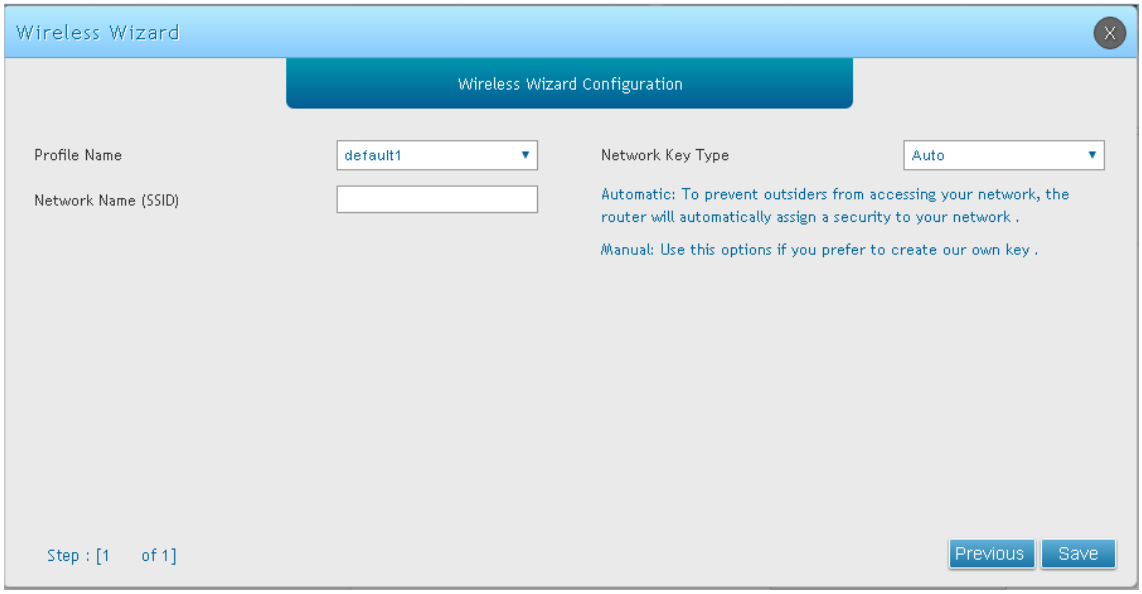

図 3-16　Wireless Wizard 画面

4. 「Profile Name」でプロファイルを「default1」「default2」から指定します。
5. 「Network Name（SSID）」でワイヤレスネットワークの SSID を入力します。
6. 「Network Key Type」で「Manual」を指定します。
7. 「Wireless Security Password」にワイヤレスネットワークのパスワードを入力します。
8. 「Save」をクリックします。
9. 確認画面が表示されます。確認後、「Finish」をクリックします。

ユーザアカウント作成

ユーザアカウントの作成方法について説明します。ユーザアカウントはグループへの参加の際に必要となります。
参加するグループの作成方法については、「Groups（グループの設定）」を参照してください。

注意　参加するグループを事前に作成する必要があります。詳しくは「グループ」をご参照ください。

1. ルータにログインします。
2. 「**Wizard**」をクリックします。

図 3-17　Wizard 画面

3. 「Users Wizard」内の「Run」をクリックします。

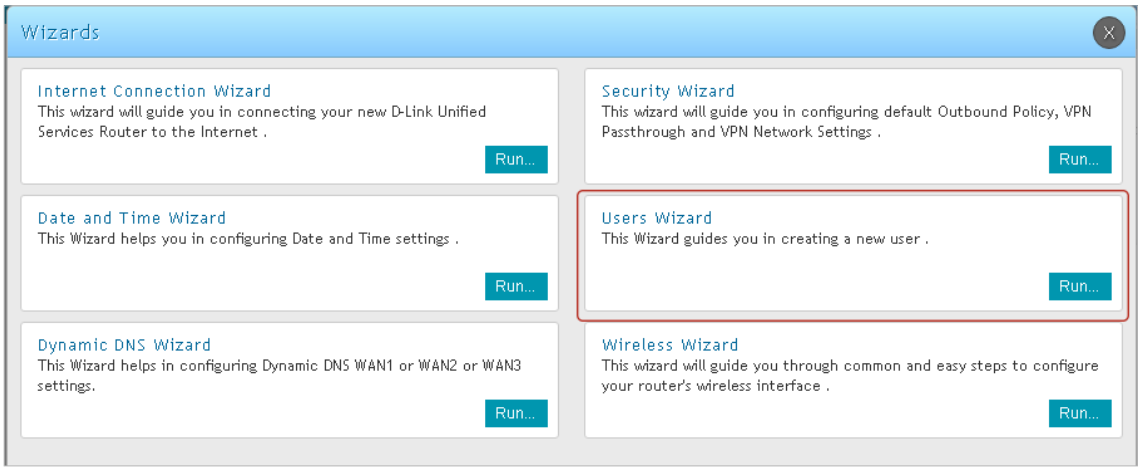

図 3-18　Users Wizard ボックス 画面

4. 「Users Wizard」画面が表示されます。

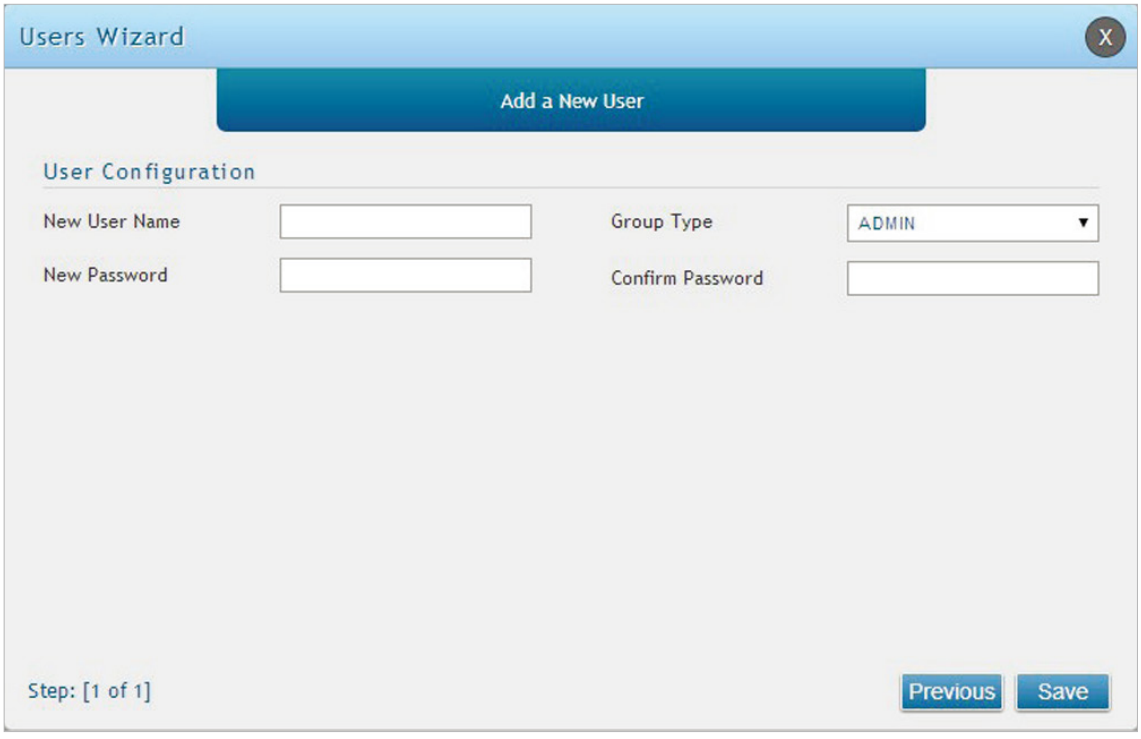

図 3-19　Users Wizard 画面

5. 「New User Name」にユーザ名を入力します。
6. 「Group Type」で参加するグループを指定します。
7. 「New Password」でパスワードを入力　→「Confirm Password」で再度パスワードを入力します。
8. 「Save」をクリックし、設定を適用します。

セキュリティ / VPN ウィザード

VPN パススルーの有効化と VPN の作成について説明します。

1. 「Wizard」をクリックします。

図 3-20　Wizard 画面

2. 「Security Wizard」内の「Run」をクリックします。

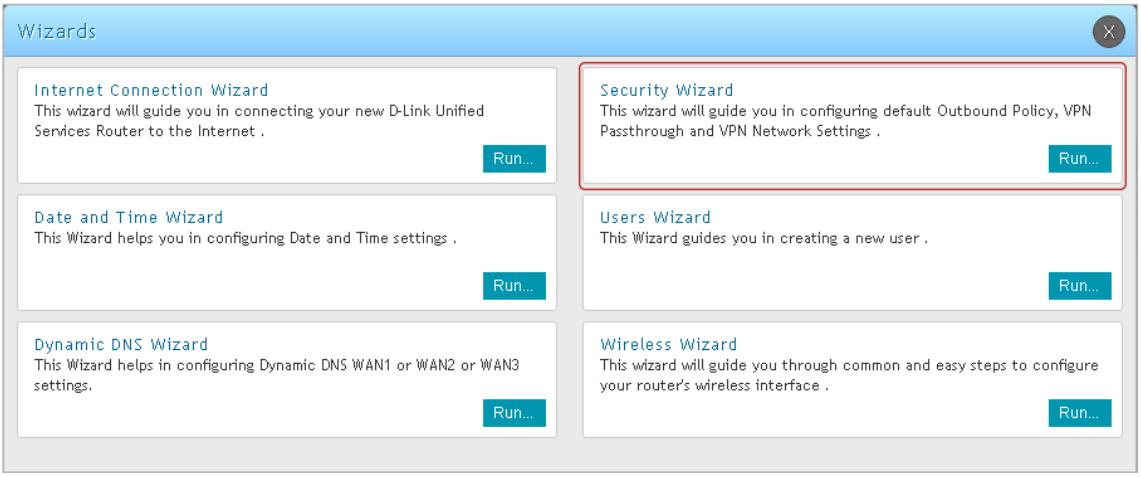

図 3-21　Security Wizard ボックス 画面

3. 「Security Wizard」画面が表示されます。

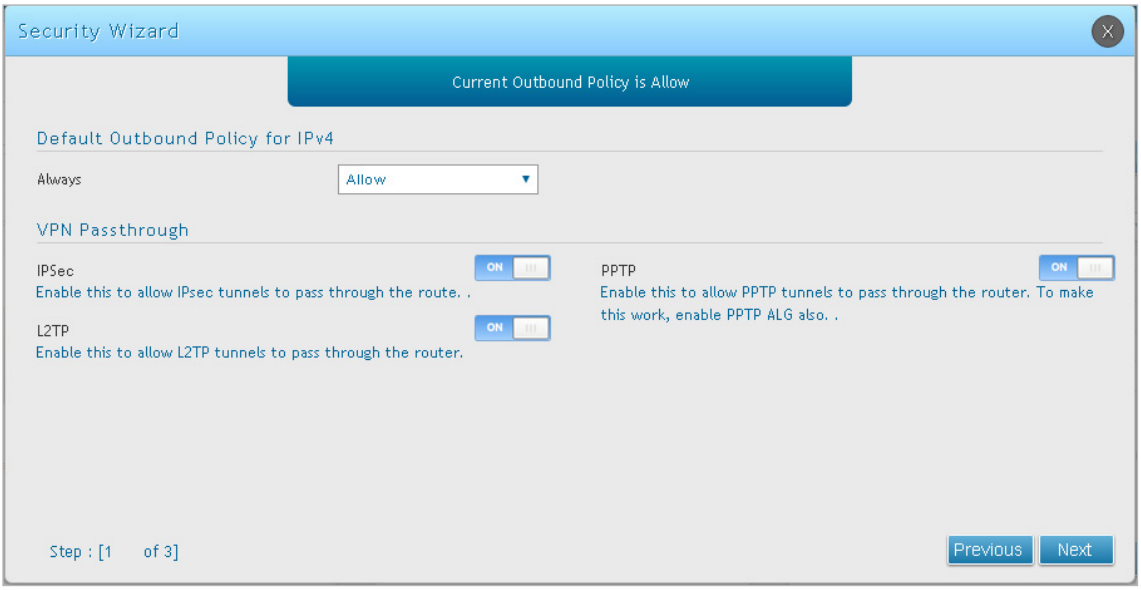

図 3-22　Security Wizard 画面（1/3）

4. 「Default Outbound Policy for IPv4」で「Allow」（許可）または「Block」（拒否）を選択します。
5. パススルーを許可する VPN の種類（「IPSec」「L2TP」「PPTP」）を「ON」にし、「Next」をクリックします。

6. 「IKE」「VPN」のポリシーを作成します。作成したポリシーは必要に応じて編集することが可能です。

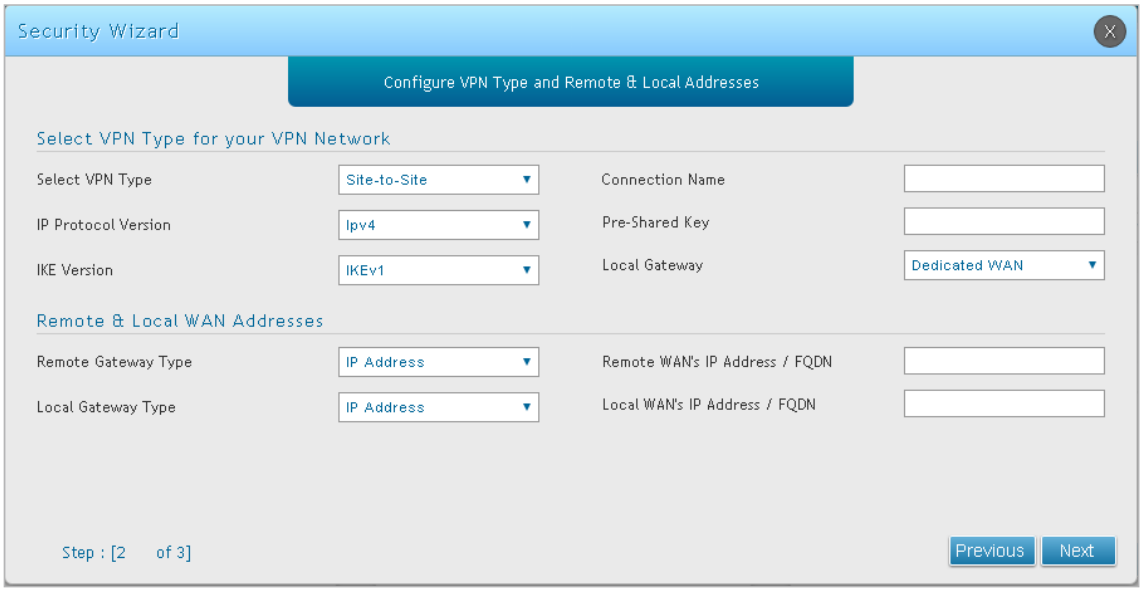

図 3-23　Security Wizard 画面（2/3）

7. 以下の項目を設定後、「Next」をクリックします。

項目	説明
Select VPN Type for your VPN Network	
Select VPN Type	VPN の種類を「Site-to-Site」「Remote Access」から選択します。
Connection Name	VPN 接続名を指定します。
IP Protocol Version	IP プロトコルバージョンを「IPv4」または「IPv6」から選択します。「IPv6」は、IP モードを「IPv4 & IPv6」に設定した場合のみ表示されます。IP モードの設定については「IP Mode（IP モード設定）」を参照してください。
Pre-Shared Key	Pre-Shared Key（事前共有鍵）を指定します。
IKE Version	IKE のバージョンを選択します。
Local Gateway	ローカルゲートウェイに使用する WAN ポートを指定します。
Remote & Local WAN Addresses	
Remote Gateway Type	リモートゲートウェイの種類を「IP Address」「FQDN」から選択します。
Remote WAN's IP Address / FQDN	リモートゲートウェイで選択した「IP Address」または「FQDN」を入力します。
Local Gateway Type	ローカルゲートウェイの種類を「IP Address」「FQDN」から選択します。
Local WAN's IP Address / FQDN	ローカルゲートウェイで選択した「IP Address」または「FQDN」を入力します。

8. 以下の画面で設定を行います。

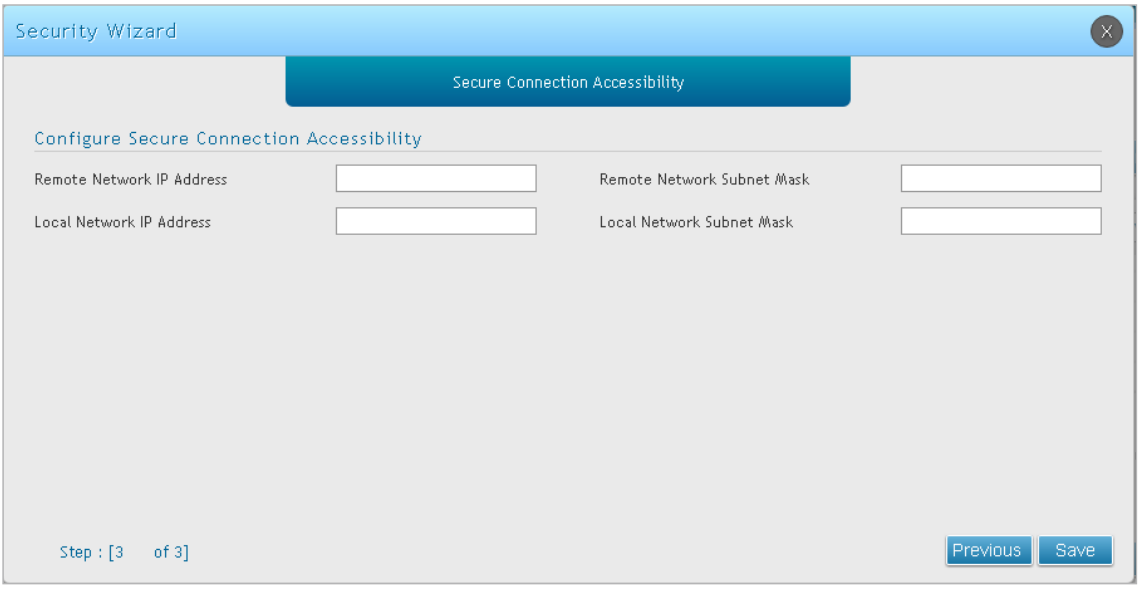

図 3-24　Security Wizard 画面（3/3）

項目	説明
Secure Connection Accessibility	
Remote Network IP Address	リモートネットワークの IP アドレスを入力します。
Remote Network Subnet Mask	リモートネットワークのサブネットマスクを入力します。
Local Network IP Address	ローカルネットワークの IP アドレスを入力します。
Local Network Subnet Mask	ローカルネットワークのサブネットマスクを入力します。

9. 「Save」をクリックし、設定を適用します。

注意 リモート LAN で使用される IP アドレス範囲は、ローカル LAN の IP アドレス範囲と重複できません。

ダイナミック DNS ウィザード（DDNS）

ダイナミック DNS の設定方法について説明します。

ダイナミック DNS（DDNS）は、動的なパブリック IP アドレスを持つルータがインターネットのドメイン名を使用して接続することができるインターネットのサービスです。DDNS を使用するためには、DynDNS.org、DlinkDDNS.com、または Oray.net などの DDNS プロバイダでアカウントをセットアップする必要があります。ダイナミック DNS の詳細については、「Dynamic DNS（ダイナミック DNS 設定）」を参照してください。

1. 「Wizard」をクリックします。

図 3-25　Wizard 画面

2. 「Dynamic DNS Wizard」内の「Run」をクリックします。

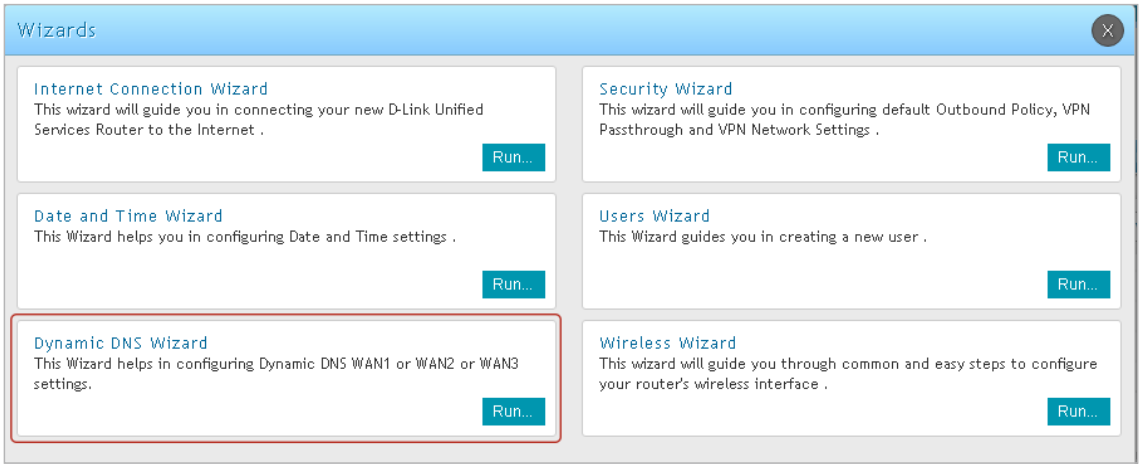

図 3-26　Dynamic DNS Wizard ボックス画面

3. 「Dynamic DNS Wizard」画面が表示されます。

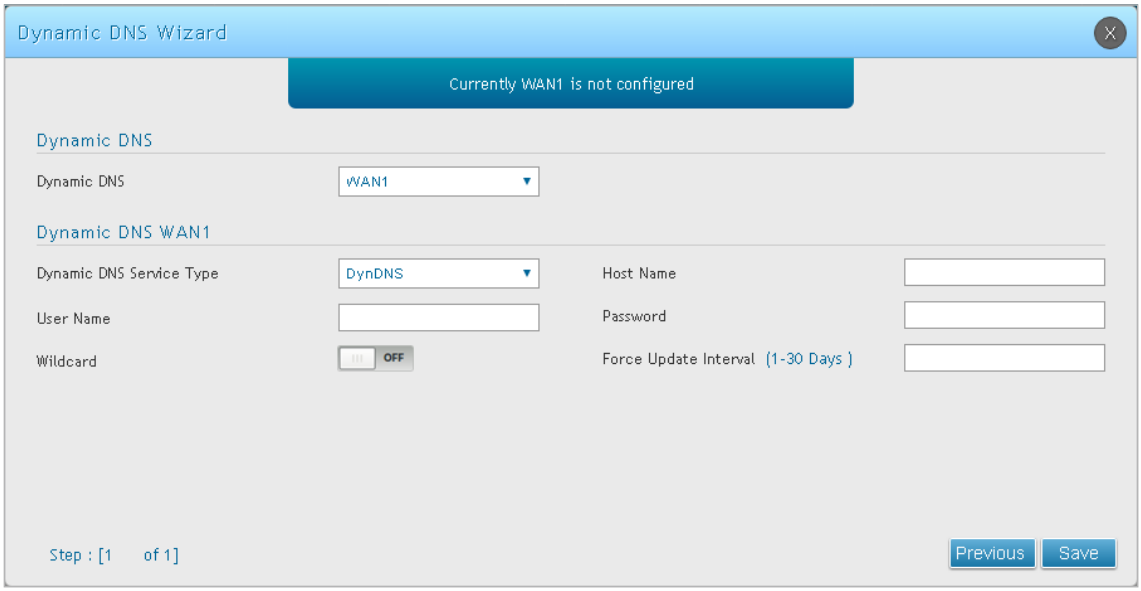

図 3-27　Dynamic DNS Wizard 画面

4. 「Dynamic DNS」で、「WAN1」「WAN2」「WAN3」（DSR-1000AC のみ）を選択します。
5. 「Dynamic DNS Service Type」で DNS サーバタイプを指定します。
6. お使いの DDNS のサービスの内容に従い、「User Name」「Password」「Host Name」を入力します。
7. お使いの DDNS のサービスの内容に従い、「Wildcards」を「ON」にします。
8. 「Force Update Interval」で自動アップデートの間隔（1-30 日）を設定します。
9. 「Save」をクリックし、設定を適用します。

第 4 章　LAN 設定（Network）

本製品の LAN および VLAN の設定方法について説明します。

設定項目	説明
「LAN（LAN 設定）」	IPv4/IPv6 ネットワーク用の LAN 設定、IPv6 通知、DHCP 予約 IP アドレスの設定などを行います。
「VLAN（VLAN 設定）」	ポート VLAN、マルチ VLAN サブネット設定などを行います。

LAN（LAN 設定）

LAN Settings（IPv4 ネットワーク用 LAN 設定）

Network > LAN > LAN Settings
本製品の LAN 設定を行います。

初期値では、ルータは WLAN または LAN ネットワーク上のホストに対して DHCP（Dynamic Host Configuration Protocol）サーバとして機能します。また、DHCP を使用して、DNS サーバ、WINS（Windows Internet Naming Service）サーバ、およびデフォルトゲートウェイに対するアドレスと共に PC とその他の LAN デバイスにも IP アドレスを割り当てることができます。DHCP サーバが有効な場合、ルータの IP アドレスは LAN と WLAN クライアントのためのゲートウェイアドレスとして機能します。LAN 内の PC には、この手順で指定されるアドレスプールから IP アドレスが割り当てられます。各プールアドレスは LAN 上でアドレスの重複を避けるために割り当て前にテストされます。

多くのアプリケーションは、本製品の DHCP および TCP/IP 設定の初期値で動作可能です。ご使用のネットワーク上の PC を DHCP サーバにしたい場合、または手動で全 PC のネットワーク設定を行う場合には、DHCP モードを無効にします。DHCP リレーは、DHCP のリース情報をネットワークの DHCP サーバである別の LAN デバイスから転送するのに使用されます。これは特に無線クライアントに役立ちます。

DNS サーバを使用する代わりに、WINS（Windows Internet Naming Service）サーバを使用できます。WINS サーバは、DNS サーバと同等ですが、ホスト名の解決のために NetBIOS プロトコルを使用します。DHCP クライアントからの DHCP 要求を承諾する場合、ルータの DHCP 設定には WINS サーバの IP アドレスがあります。

また、LAN の DNS プロキシを有効にすることができます。有効にした場合、ルータはすべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します。無効にした場合、すべての DHCP クライアントが ISP の DNS IP アドレスを受信します。

1. **Network > LAN > LAN Settings** の順にメニューをクリックし、以下の画面を表示します。

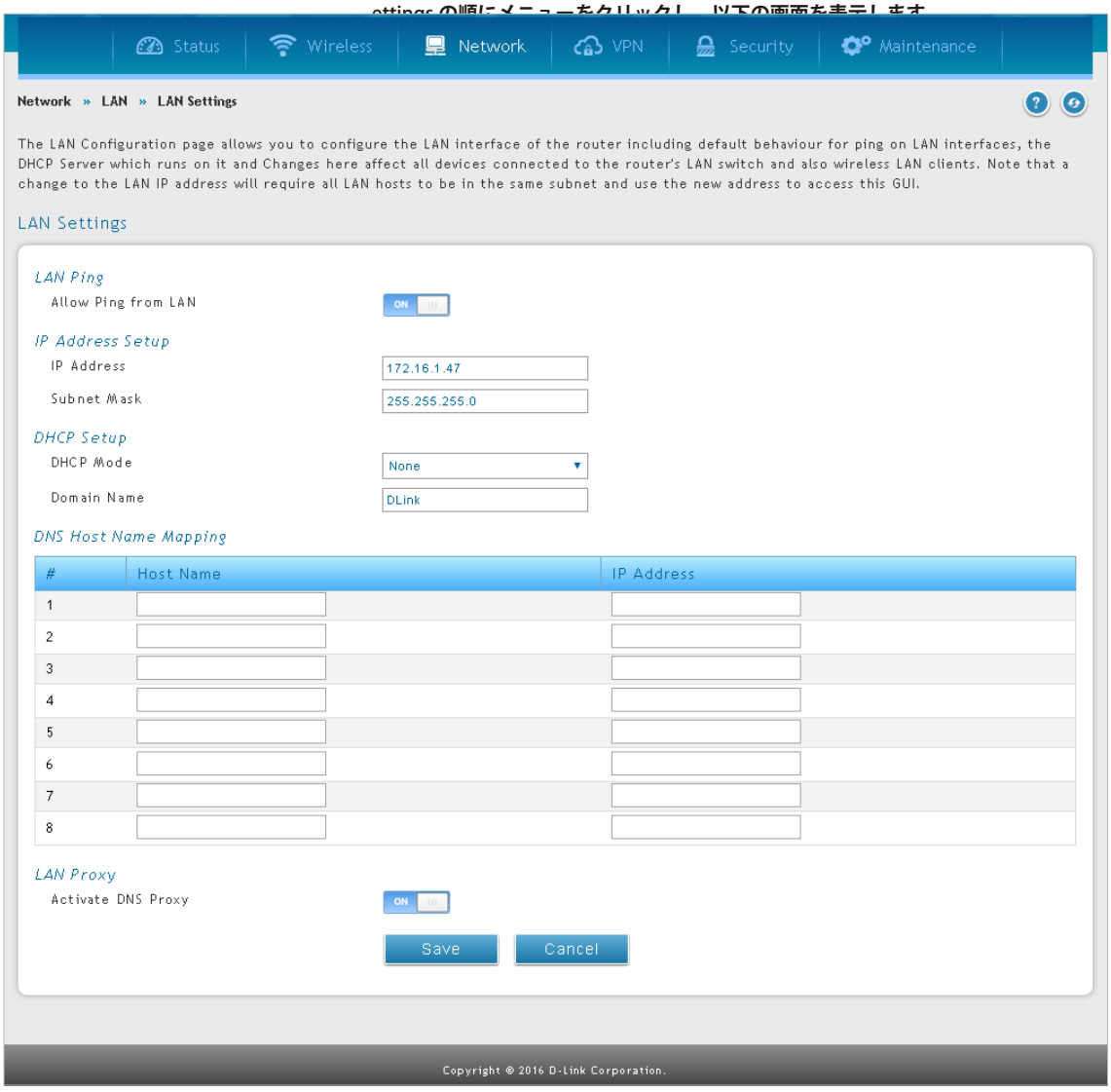

図 4-1　LAN Settings 画面

2. 「LAN Ping」セクションで、「Allow Ping from LAN」の「ON」「OFF」を選択します。「ON」にした場合、LAN 内の Ping が許可されます。

3. 「IP Address Setup」セクションで、以下の項目を設定します。
   - 「IP Address」：IP アドレスを入力します。　初期値：192.168.10.1
   - 「Subnet Mask」：サブネットマスクを入力します。　初期値：255.255.255.0

4. 「DHCP Setup」セクションで、「DHCP Mode」を以下から選択します。
   - 「None」：
     DHCP サーバ機能を無効にします。
   - 「DHCP Server」：
     ルータはネットワーク上で DHCP サーバとして動作します。「DHCP Server」を選択した場合の設定項目については、「DHCP Server（DHCP サーバ設定）」を参照してください。
   - 「DHCP Relay」：
     LAN 上の DHCP クライアントは、異なるサブネットにある DHCP サーバから IP アドレスリースを受け取ることができます。「DHCP Relay」を選択した場合の設定項目については、「DHCP Relay（DHCP リレー設定）」を参照してください。

5. 「DNS Host Name Mapping」セクションで、「Host Name」「IP Address」にそれぞれマッピングするホスト名、IP アドレスを入力します。

6. 「LAN Proxy」セクションで、「Activate DNS Proxy」の「ON」/「OFF」を選択します。
   - 「ON」：DNS プロキシを有効にします。
   - 「OFF」：DNS プロキシを無効にします。

注意　IP アドレスを変更して「Save」をクリックすると、Web GUI が応答しなくなります。
変更後の IP アドレスを使用し、再度 WebGUI にログインしてください。

DHCP Server（DHCP サーバ設定）

1. 「DHCP Mode」で「DHCP Server」を選択します。

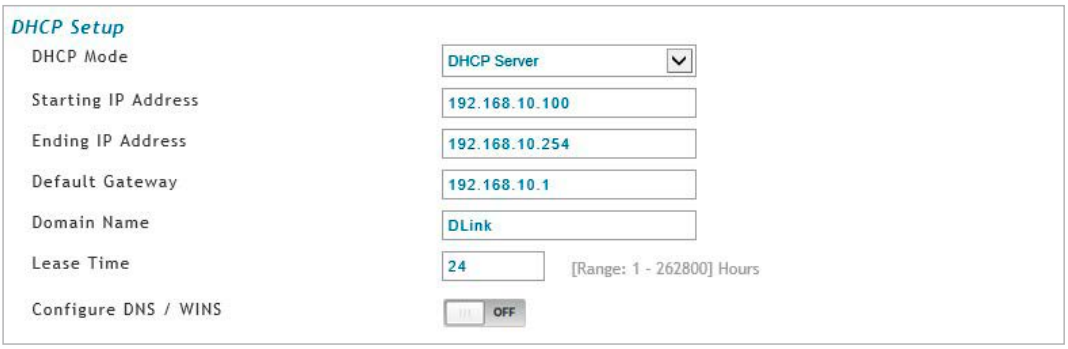

図 4-2　DHCP Server（DHCP Setup）画面

2. 以下の項目を設定します。

項目	説明
Starting IP Address / Ending IP Address	DHCP アドレスプールの開始 IP アドレスと終了アドレスを入力します。 LANに参加する新規のDHCPクライアントには、「Starting IP Address」（開始IPアドレス）と「Ending IP Address」（終了 IP アドレス）で指定した範囲内の IP アドレスが割り当てられます。 開始 IP アドレスと終了 IP アドレスは、ルータの LANIP アドレスと同じサブネット内である必要があります。
Default Gateway	DHCP クライアントに割り当てるデフォルトゲートウェイの IP アドレスを入力します。通常、デフォルトゲートウェイは本製品の LAN IP アドレス（初期値：192.168.10.1）となります。
Domain Name	識別に使用するネットワークのドメイン名を入力します。
Lease Time	IP アドレスがクライアントにリースされる期間を入力します。 • 設定可能範囲：1-262800（時） • 初期値：24（時）
Configure DNS/WINS	「ON」を選択した場合、DNS/WINS サーバの IP アドレスを入力します。「OFF」を選択した場合、本製品の LAN IP アドレスがクライアントに対しての DNS サーバの IP アドレスとしてアサインされ、本製品は ISP から DNS 情報を取得します。

3. 「Save」をクリックし、設定を適用します。

DHCP Relay（DHCP リレー設定）

1. 「DHCP Mode」で「DHCP Relay」を選択します。

図 4-3　DHCP Relay（DHCP Setup）画面

2. 以下の項目を設定します。

項目	説明
Domain Name	ネットワークのドメイン名を入力します。
Gateway	ゲートウェイの IP アドレスを入力します。

3. 「Save」をクリックし、設定を適用します。

LAN DHCP Reserved IPs（LAN DHCP 予約 IP アドレスの設定）

Network > LAN > LAN DHCP Reserved IPs メニュー

本機能では、クライアントのMACアドレス及び予約IPアドレスを追加することで、LAN上のコンピュータにTCP/IP設定を割り当てることができます。

DHCP サーバがクライアントからリクエストを受信するたびに、クライアントの MAC アドレスとデータベース内の MAC アドレスリストが比較されます。データベース内でそのコンピュータまたはデバイスに IP アドレスがすでに割り当てられている場合は、カスタマイズされた IP アドレスが設定されます。それ以外の場合は、DHCP プールから自動的に IP アドレスがクライアントに割り当てられます。

1. **Network > LAN > LAN DHCP Reserved IPs** の順にメニューをクリックし、以下の画面を表示します。

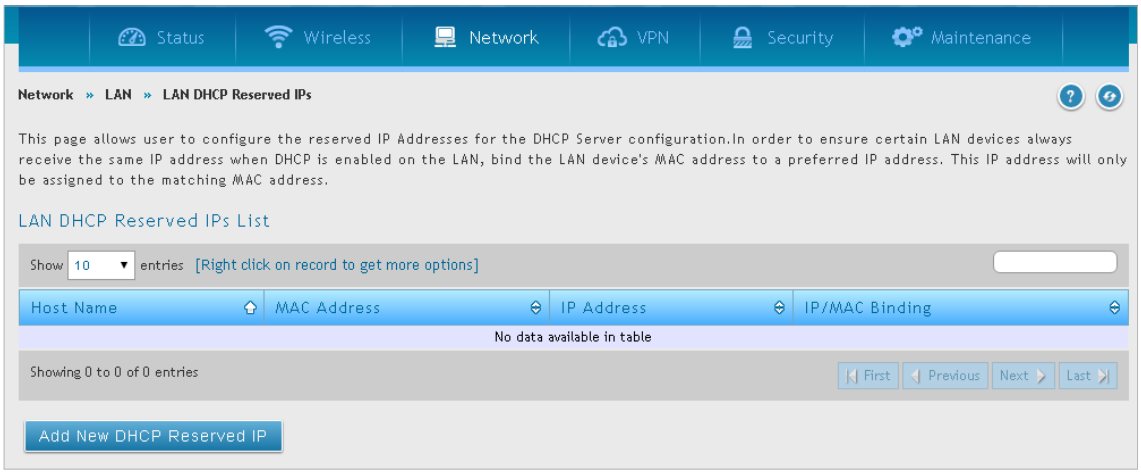

図 4-4　LAN DHCP Reserved IPs 画面

2. 予約 IP アドレスを追加する場合は、「Add New DHCP Reserved IP」をクリックし以下の画面を表示します。

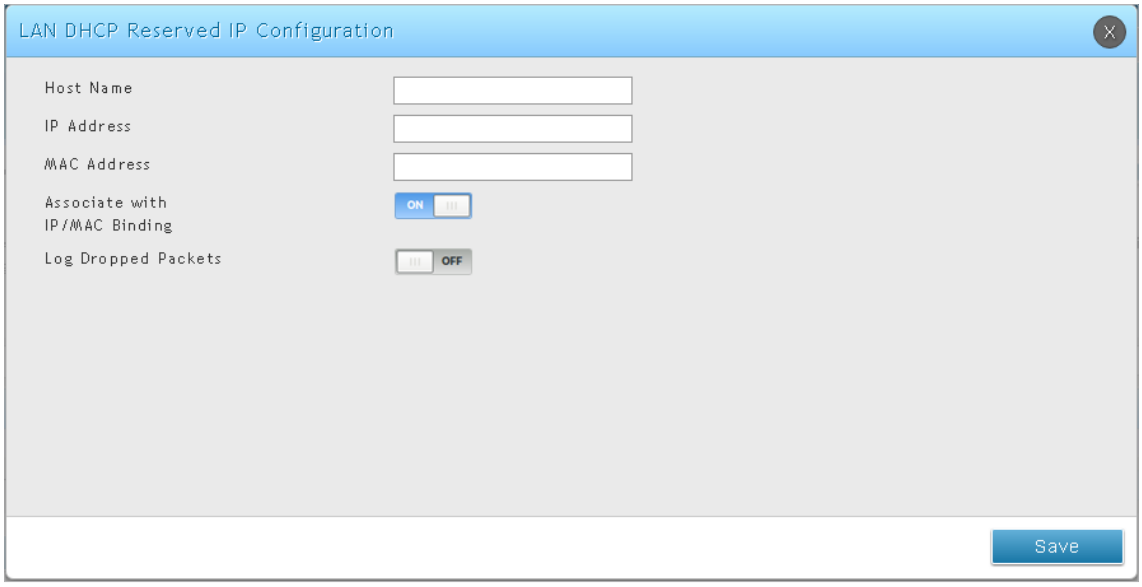

図 4-5　LAN DHCP Reserved IP Configuration 画面

3. 以下の項目を設定します。

項目	説明
Host Name	デバイスのホスト名を入力します。スペースは使用できません。
IP Address	デバイスにわりあてる IP アドレスを入力します。この IP アドレスは、DHCP 設定の開始 IP アドレス／終了 IP アドレスの範囲内で設定する必要があります。
MAC Address	デバイスの MAC アドレスを入力します。大文字と小文字は区別されません。
Associate with IP/MAC Binding	「ON」にした場合、このデバイスの情報を IP/MAC バインディングに関連付けます。
Log Dropped Packets	「ON」にした場合、破棄パケットのログを取得します。

4. 「Save」をクリックし、設定を適用します。

追加した予約 IP アドレスは、LAN DHCP Reserved IPs 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

IP/MAC Binding（IP/MAC バインディング）

Network > LAN > IP/MAC Binding メニュー

IP/MAC バインディングリストの作成について説明します。
IP/MAC バインディングにより、ゲートウェイは送信トラフィックの IP アドレスを構成済み LAN ノード固有の MAC アドレスで検証します。
違反があった場合（トラフィックの送信元 IP アドレスが、同じ IP アドレスを持つ予想される MAC アドレスと一致しない場合）、パケットは破棄され、診断のために記録される場合があります。

1. **Network > LAN >IP/MAC Binding** の順にメニューをクリックし、以下の画面を表示します。

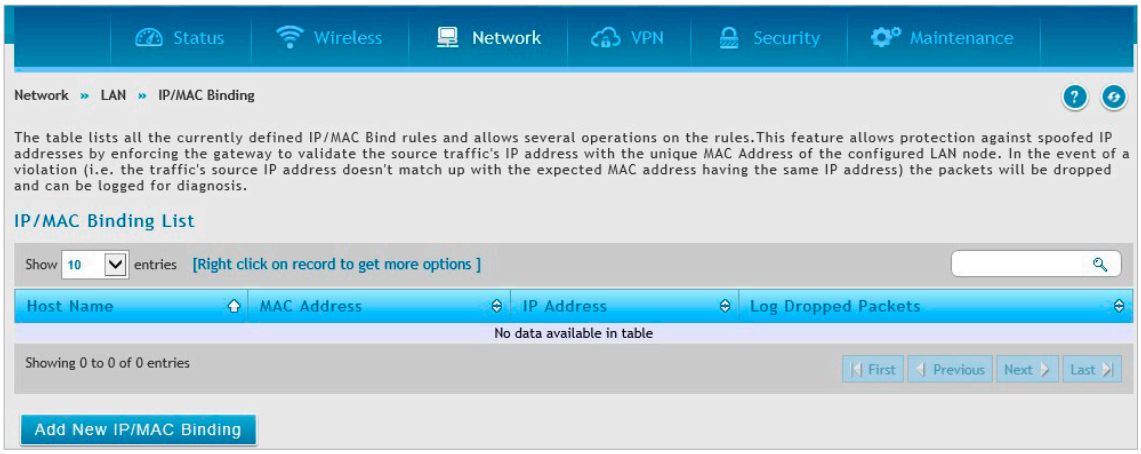

図 4-6　IP/MAC Binding 画面

2. 以下の項目が表示されます。

項目	説明
Host Name	ユーザが定義したルール名が表示されます。
MAC Address	MAC アドレスが表示されます。
IP Address	IP アドレスが表示されます。
Log Dropped Packets	ルールのログオプションが表示されます。

3. バインディングルールを追加する場合は、「Add New IP/MAC Binding」をクリックし以下の画面を表示します。

図 4-7　IP/MAC Binding Configuration 画面

4. 以下の項目を設定します。

項目	説明
Host Name	デバイスのホスト名を入力します。スペースは使用できません。
MAC Address	デバイスの MAC アドレスを入力します。大文字と小文字は区別されません。
IP Address	デバイスにわりあてる IP アドレスを入力します。この IP アドレスは、DHCP 設定の開始 IP アドレス／終了 IP アドレスの範囲内で設定する必要があります。
Log Dropped Packets	「ON」にした場合、破棄パケットのログを取得します。

5. 「Save」をクリックし、設定を適用します。

追加したバインディングルールは、IP/MAC Binding 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

IGMP Setup（IGMP 設定）

Network > LAN > IGMP Setup

IGMP スヌーピングとは、IGMP パケットの中身を確認し、必要なホストにのみマルチキャストパケットを転送する機能です。
本機能は、ネットワーク上に大量のマルチキャストトラフィックが存在しているものの、すべての LAN ホストがこのトラフィックを受信する必要がない場合に有用です。

1. **Network > LAN > IGMP Setup** の順にメニューをクリックし、以下の画面を表示します。

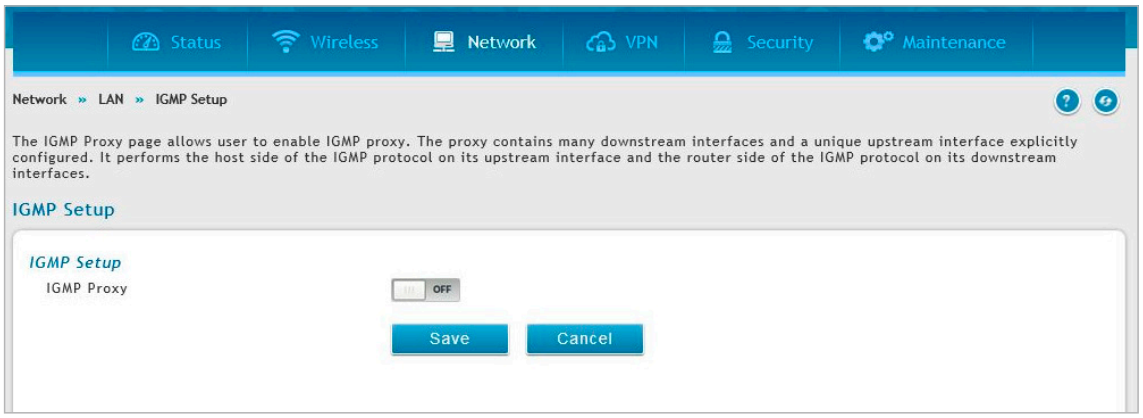

図 4-8　IGMP Setup 画面

2. 以下の項目を設定します。

項目	説明
IGMP Proxy	IGMP プロキシを「ON」または「OFF」に設定します。

3. 「Save」をクリックし、設定を適用します。

UPnP Setup（UPnP 設定）

Network > LAN > UPnP

UPnP の設定方法について説明します。
UPnP（Universal Plug and Play）は、ルータと通信可能なネットワーク上のデバイスを検出し、自動設定を行う機能です。ネットワークデバイスが検出されると、ネットワークデバイスが要求するトラフィックのプロトコル用に内部 / 外部ポートを開放します。
UPnP を無効にした場合はデバイスの自動設定は行われません。アプリケーションを動作させるには、手動でポート開放を行います。

1. **Network > LAN > UPnP** の順にメニューをクリックし、以下の画面を表示します。

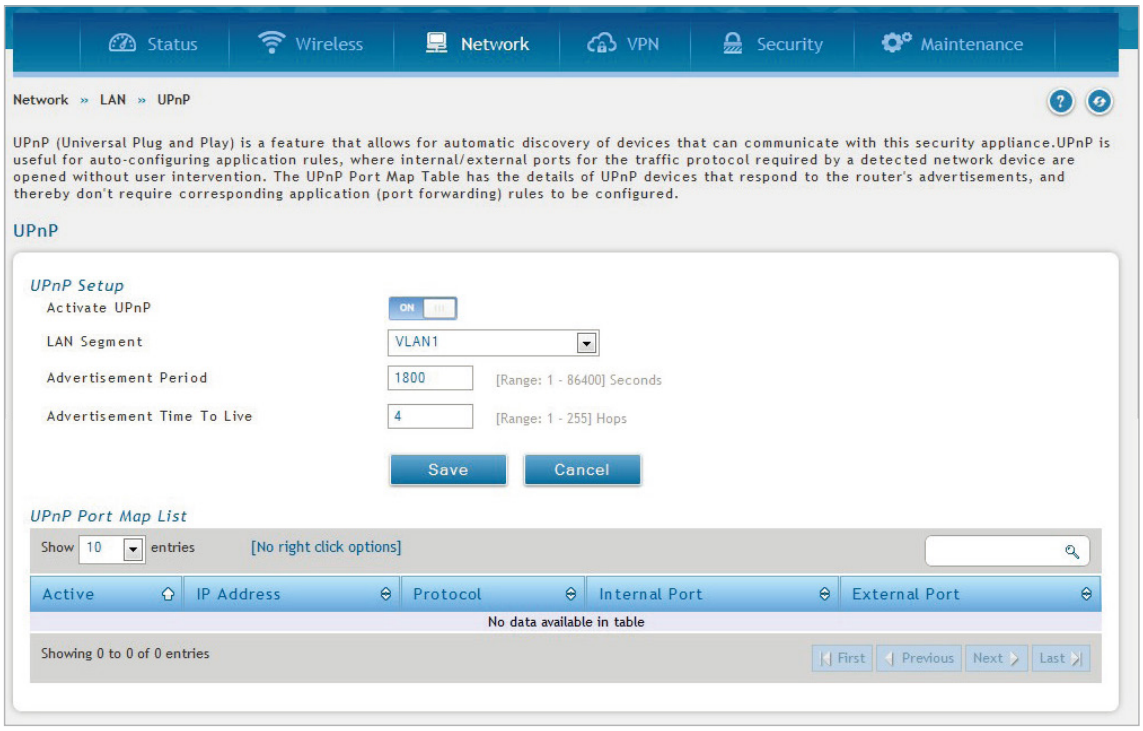

図 4-9　UPnP 画面

2. 以下の項目を設定します。

項目	説明
UPnP Setup	
Activate UPnP	UPnP を「ON」または「OFF」に設定します。
LAN Segment	UPnP を有効にする VLAN を選択します。
Advertisement Period	ルータがネットワーク上に UPnP 情報をブロードキャストする頻度を入力します。 大きい値を設定した場合ネットワークトラフィックが最小限になりますが、新規 UPnP デバイスのネットワークへの識別は遅くなります。 - 設定可能範囲：1-86400（秒） - 初期値：1800（秒）
Advertisement Time to Live	パケットの TTL（生存時間）を設定します。 小さい値に設定した場合、UPnP ブロードキャスト範囲が制限されます。 スイッチの数が少ないネットワークでは、初期値の 4 に設定することが一般的です。 - 設定可能範囲：1-255（Hops） - 初期値：4（Hops）
UPnP Port Map List	
Active	接続を確立した UPnP デバイスのポートが現在アクティブであるかどうかが表示されます。
IP Address	本製品が検出した UPnP デバイスの IP アドレスが表示されます。
Protocol	デバイスが使用しているネットワークプロトコル（HTTP、FTP など）が表示されます。
Internal Port	UPnP によってオープンされた内部ポートが表示されます。
External Port	UPnP によってオープンされた外部ポートが表示されます。

3. 「Save」をクリックし、設定を適用します。

VLAN（VLAN 設定）

Network > VLAN
本製品は、VLAN を使用することで LAN 上に隔離した仮想ネットワークを構築できます。ネットワークデバイスに対し、VLAN 識別子で定義されたサブネットワークと通信するように設定することができます。LAN ポートに固有の VLAN ID を割り当てることで、その物理ポートから送受信されるトラフィックを通常の LAN から隔離することができます。

VLAN フィルタリングは、大規模なネットワークにおけるデバイスのブロードキャストパケットを制限します。ルータの VLAN は初期値では有効になっています。VLAN Settings 画面では、VLAN を有効にし、仮想ネットワークの設定を行います。

VLAN Settings（VLAN 設定）

Network > VLAN > VLAN Settings
VLAN の設定方法について説明します。

「VLAN List」には、設定済みの VLAN のリストが表示されます。リストの下にある「Add New VLAN」をクリックし、VLAN メンバシップを作成します。VLAN メンバーシップエントリは、VLAN ID と、その VLAN メンバシップに割り当てられている数値の VLAN ID で構成されています。

VLAN ID の値は、2 ～ 4093 の任意の数字で設定できます。VLAN ID 1 は、デフォルト VLAN 用に予約されています。VLAN ID 1 は、インタフェースで受信したタグなしフレームに使用されます。

1. **Network > VLAN > VLAN Settings** の順にメニューをクリックし、以下の画面を表示します。

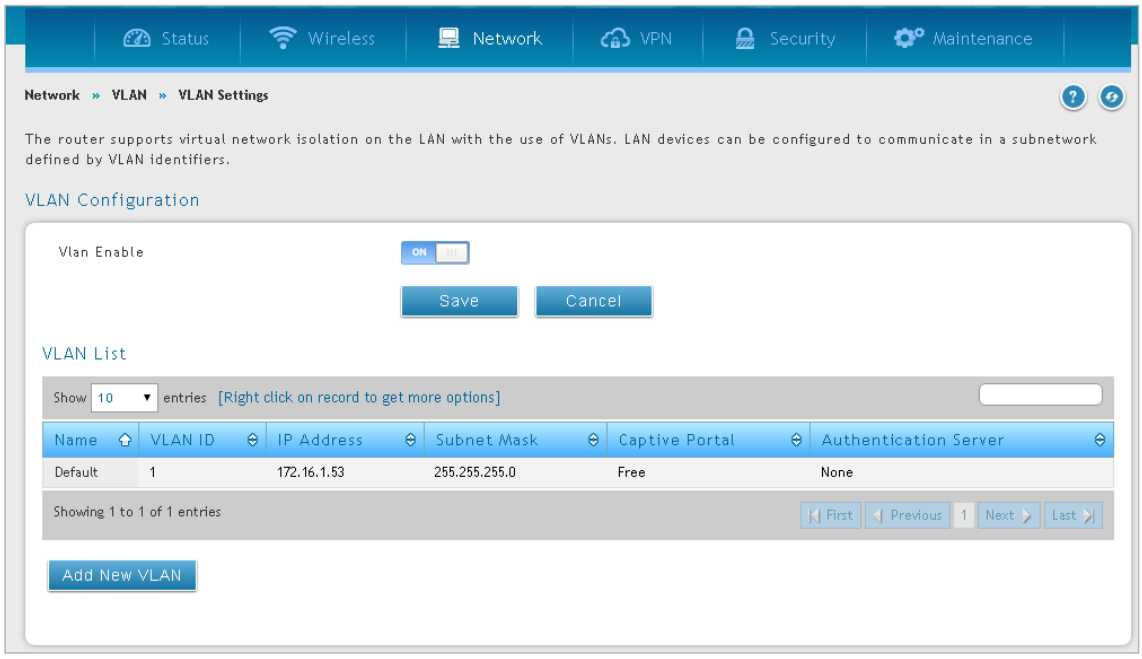

図 4-10　VLAN Settings 画面

2. 「VLAN Enable」を「ON」にし、VLAN を有効にします。
3. 「Save」をクリックし、設定を適用します。

4. VLAN を追加する場合は、「Add New VLAN」をクリックし、以下の画面を表示します。

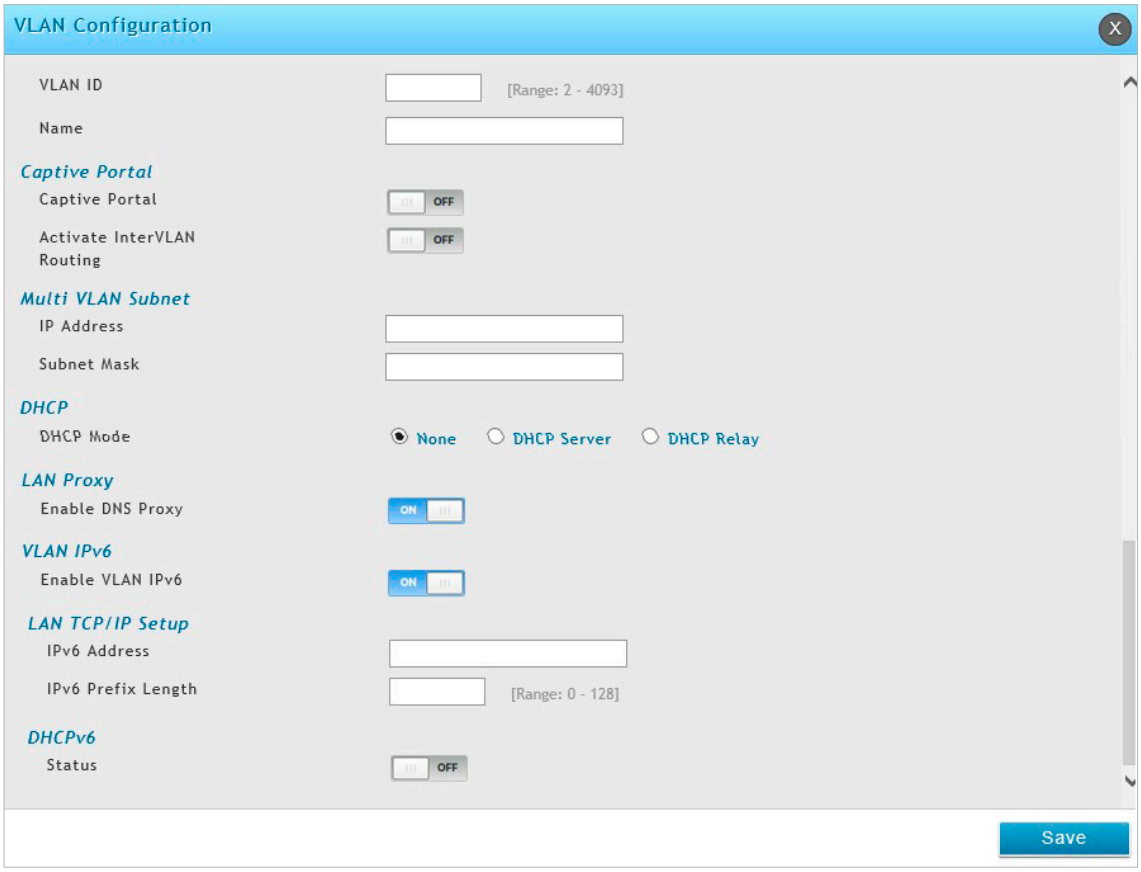

図 4-11　VLAN Configration 画面

5. 以下の項目を設定します。

項目	説明
VLAN ID	VLAN ID（2-4093）を指定します。
Name	VLAN 名を指定します。
Captive Portal	
Captive Portal	VLAN ごとにキャプティブポータルを「Enable」（有効）または「Disable」（無効）にします。 有効にすると、「Captive Portal」セクション内で各項目を設定することができます。
Active InterVLAN Routing	複数の VLAN 間のルーティングを「ON」または「OFF」に設定します。
Multi VLAN Subnet	
IP Address	VLAN の IP アドレスを指定します。
Subnet Mask	VLAN のサブネットマスクを指定します。
DHCP	
DHCP Mode	以下から DHCP モードを指定します。 • 「None 」：DHCP サーバ機能を VLAN に対して無効にします。 • 「DHCP Server」：ルータは DHCP サーバとして動作します。 • 「DHCP Relay」：有効にすると VLAN 上の DHCP クライアントは、異なるサブネットにある DHCP サーバから IP アドレスのリースを受けることができます。
LAN Proxy	
Enable DNS Proxy	「ON」にするとルータがすべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します。
VLAN IPv6	
Enable VLAN IPv6	「ON」にした場合、VLAN の IPv6 アドレスが有効になります。
LAN TCP/IP Setup	
IPv6 Address	VLAN の IPv6 アドレスを入力します。
IPv6 Prefix Length	IPv6 プレフィックス長を入力します。 - 設定可能範囲：0-128

項目	説明
DHCPv6	
Status	DHCPv6 のステータスを「ON」または「OFF」に設定します。有効にした場合、以降に表示される項目を設定してください。
Mode	モードを「Stateless」または「Statefull」から選択します。
Domain Name	DHCPv6 サーバのドメイン名を入力します。
Server Preference	サーバの設定値を 10 進数で入力します。 設定値は、ステートレス DHCP で DHCP サーバの優先レベルを示すために使用されます。DHCPv6 クライアントは最も高い設定値を持つ DHCPv6 サーバを選択します。 - 設定可能範囲：0-255 - 初期値：255
DNS Servers	DNS サーバを以下から選択します。 -「Use DNS Proxy」：DNS プロキシを使用します。 -「Use Below」：以下で設定した「Primary DNS Server」「Secondary DNS Server」を使用します。 -「Use DNS from ISP」：ISP が提供する DNS サーバを使用します。
Primary DNS Server	「Use Below」を選択した場合、プライマリ DNS サーバを入力します。
Secondary DNS Server	「Use Below」を選択した場合、セカンダリ DNS サーバを入力します。
Lease / Rebind Time	アドレスがクライアントにリースされる時間を設定します。 - 設定可能範囲：0-604800（秒） - 初期値：86400（秒）
Prefix Delegation	プレフィックス委任を「ON」または「OFF」に設定します。

6. 「Save」をクリックし、設定を適用します。

Captive Portal（キャプティブポータル）

キャプティブポータルは、各 VLAN ごとに有効にできます。キャプティブポータルを経由して特定の VLAN にあるホストを認証するように指定します。VLAN ごとに、固有の指示やブランド名を持つカスタマイズされたポータルにすることも可能です。本設定における最も重要な点は、認証サーバを選択することです。キャプティブポータル経由でインターネットアクセスを行う全てのユーザ（VLAN ホスト）が、指定のサーバ経由で認証されます。

1. **Network > VLAN > VLAN Settings** の順にメニューをクリックします。

2. 「Add New VLAN」をクリック、または既存の VLAN を右クリックして「Edit」を選択します。

3. 「VLAN Configuration」画面で「Captive Portal」セクションの設定を行います。

「Captive Portal Type」に「Internal CP Web」を選択した場合、以下の項目を設定します。

図 4-12　Captive Portal 画面 -Internal CP Web

項目	説明
Captive Portal	キャプティブポータルを「ON」または「OFF」に設定します。
Captive Portal Type	キャプティブポータルのタイプを「Internal CP Web」に設定します。
Login Profile Name	ログインプロファイル名を指定します。 ドロップダウンメニューから選択、または「Create a Profile」をクリックし新しいプロファイルを指定します。
Authentication Server	この VLAN で利用できる認証サーバを表示します。 このキャプティブポータルにログインするすべてのユーザは、選択したサーバによって認証されます。
Redirect Type	キャプティブポータルログインページのリダイレクションタイプを指定します。HTTP または HTTPS のいずれかを選択します。
Activate InterVLAN Routing	VLAN 間の通信を有効にする場合、「ON」にします。

「Captive Portal Type」に「DUA External CP Web」を選択した場合、以下の項目を設定します。

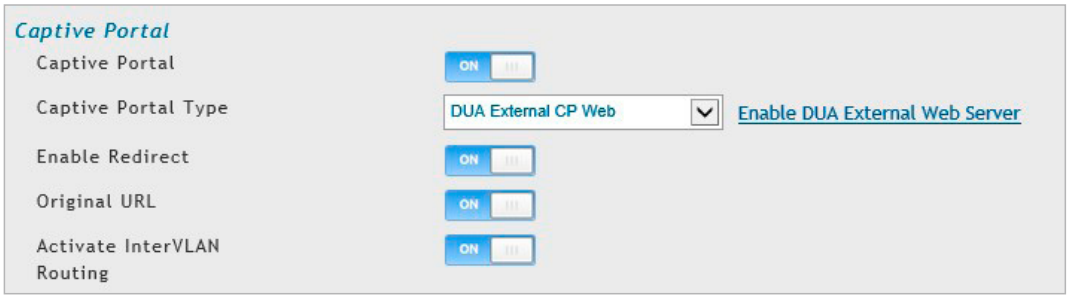

図 4-13　Captive Portal 画面 -DUA External CP Web

項目	説明
Captive Portal	キャプティブポータルを「ON」または「OFF」に設定します。
Captive Portal Type	キャプティブポータルのタイプを「DUA External CP Web」に設定します。 「Enable DUA External Web Server」をクリックして DUA 外部 Web サーバを有効にできます。
Enable Redirect	リダイレクトを「ON」または「OFF」に設定します。
Original URL	「ON」にした場合、ユーザが入力したオリジナル URL へのリダイレクトが有効になります。
Activate InterVLAN Routing	VLAN 間の通信を有効にする場合、「ON」にします。

4.　「Save」をクリックし、設定を適用します。

Port VLAN（ポート VLAN / ワイヤレス VLAN）

Network > VLAN Settings > Port VLAN

VLAN ID が割り当てられた特定の LAN ポートを通過するすべてのトラフィックにタグ付けをするために、物理ポートと無線セグメントに対して VLAN を紐付けることができます。

本画面では、LAN 及び無線 LAN の VLAN メンバシッププロパティ情報の一覧を表示します。

- 「Port VLANs List」：「Port Name」「Mode」「PVID」「VLAN membership」の項目が表示されます。
- 「Wireless VLANs List」：4 つの物理ポートに関連付けられたアクセスポイントが表示されます。

物理ポートまたは構成済みのアクセスポイントを右クリックして「Edit」を選択し、設定画面を開くことができます。

1.　**Network > VLAN Settings > Port VLAN** の順にメニューをクリックし、以下の画面を表示します。

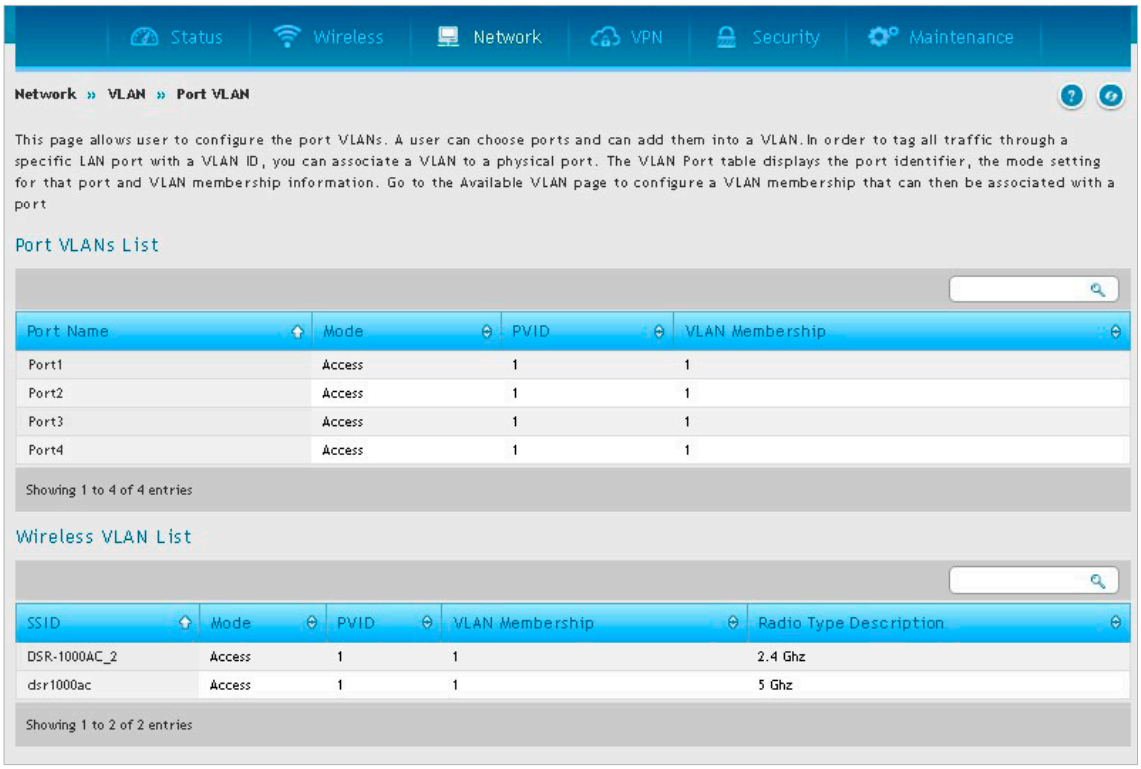

図 4-14　Port VLAN 画面

2. ポートを右クリック→「Edit」を選択し、設定画面を表示します。

選択したモードによって表示される画面が異なります。

図 4-15　Port VLAN - Edit「Access」画面

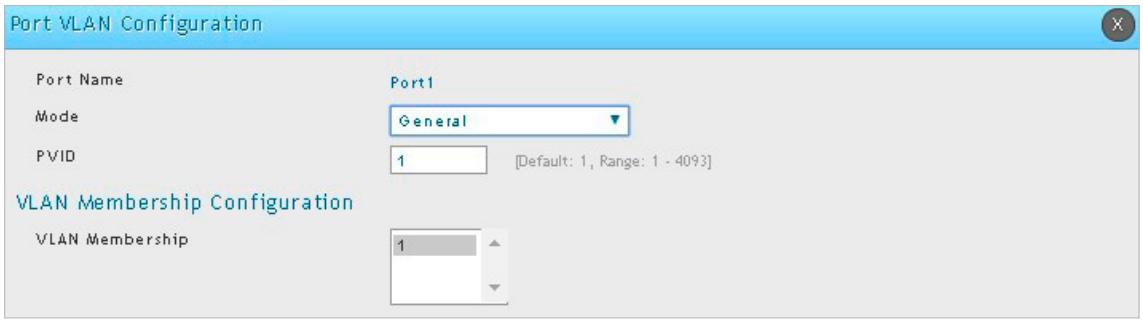

図 4-16　Port VLAN - Edit「General」画面

図 4-17　Port VLAN - Edit「Trunk」画面

3. 以下の項目を設定します。

項目	説明
Mode	VLAN のモードを以下から選択します。 • 「General」 ポートは任意の VLAN セットのメンバになることができます。ポートは VLAN ID を持つタグ付きまたはタグなしデータを送受信します。受信データがアンタグの場合、定義済みの PVID が割り当てられます。 ＜例＞ ポート 3 が PVID 3 を持つ「General」ポートである場合、ポート 3 で受信するデータには PVID 3 が割り当てられます。これと同じ PVID を持つポートから送信されたすべてのタグ付きデータからはタグが取り外されます。これは通常、2 つのイーサネットポートを持つ IP 電話に使用されるモードです。電話からルータのスイッチポートに送信されるデータはタグ付けされます。接続するデバイスから電話を通過するデータはタグが取り外されます。 • 「Access」 ポートは単一の VLAN のメンバです。ポートで送受信する全てのデータはタグなしとなります。アクセスモードのポートを経由するトラフィックは、通常のイーサネットフレームのように扱われます。 • 「Trunk」 ポートは任意の VLAN セットのメンバになることができます。ポートで送受信する全てのデータがタグ付けされます。ポートで受信するタグなしデータは、ポート PVID=1 を持つアンタグのデフォルト VLAN を除き転送されません。トランクポートは、同じ物理リンク上の複数 VLAN に対するトラフィックを多重化します。
PVID	「General」モードを選択した場合、ポートの PVID を入力します。
VLAN Membership	VLAN メンバシップを選択します。

4. 「Save」をクリックし、設定を適用します。

第 5 章　ネットワーク設定（Network）

本製品のネットワーク設定について説明します。

設定項目	説明
「Internet（インターネット接続設定）」	2 つの WAN ポートを使用したインターネット接続の設定を行います。
「Jumbo Frames（ジャンボフレーム設定）」	ジャンボフレーム設定を行います。
「Routing（ルーティング設定）」	スタティック / ダイナミックルーティングの設定を行います。
「IPv6（IPv6 ネットワーク設定）」	IPv6 の関連する LAN 設定を行います。

Internet（インターネット接続設定）

Network > Internet

本ルータにある 2 つの WAN ポートを使用し、インターネット接続を行うことができます。
設定には IP アドレス、アカウント情報などインターネット接続情報が必要です。通常これらの情報は ISP またはご使用のネットワーク管理者によって提供されます。

WAN1 Settings（WAN1 設定）

Network > Internet > WAN1 Settings

「WAN1」インタフェースの設定を行います。以下の画面の「Connection Type」で選択した項目によって、表示される画面が異なります。

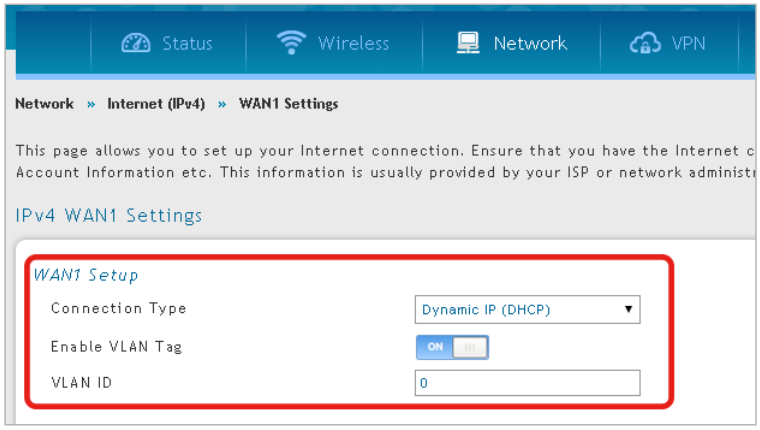

図 5-1　　WAN1 Setup 画面

以下の項目を設定します。

項目	説明
Connection Type	接続タイプを以下から選択します。 • 「Dynamic IP (DHCP)」：ご利用の ISP から自動的に IP アドレス、接続情報を取得します。 • 「Static IP」：手動で IP アドレスを含む接続設定を行います。 • 「PPPoE (Username/Password)」：ISP から提供される PPPoE 情報を元に接続設定を行います。 • 「PPTP (Username/Password)」：ISP から提供される PPTP 情報を元に接続設定を行います。 • 「L2TP (Username/Password)」：ISP から提供される L2TP 情報を元に接続設定を行います。 • 「Japanese multiple PPPoE」：ISP から提供される PPPoE 情報（日本向け）を元に接続設定を行います。 • 「Russian dual access PPPoE」：ISP から提供される PPPoE 情報（ロシア向け）を元に接続設定を行います。 • 「Russian dual access PPTP」：ISP から提供される PPTP 情報（ロシア向け）を元に接続設定を行います。 • 「Russian dual access L2TP」：ISP から提供される L2TP 情報（ロシア向け）を元に接続設定を行います。
Enable VLAN Tag	VLAN タグを「ON」または「OFF」にします。
VLAN ID	VLAN タグを「ON」にした場合、VLAN ID を入力します。

Dynamic IP (DHCP)（自動 IP アドレス設定）

「Connection Type」で「Dynamic IP (DHCP)」を選択した場合の設定です。

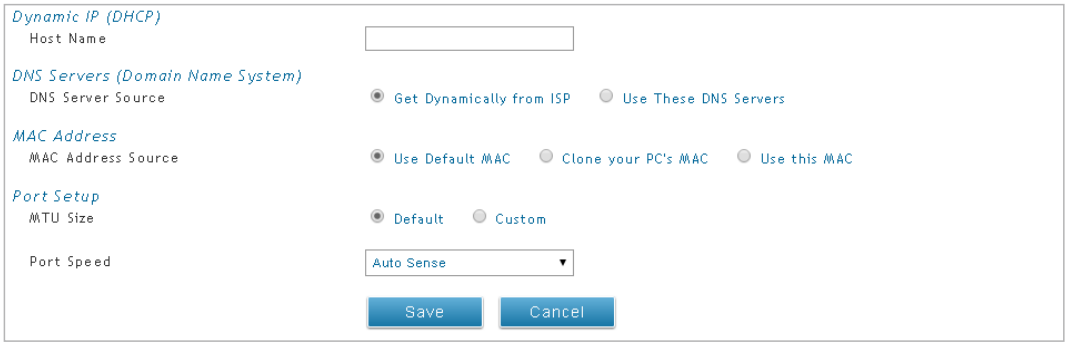

図 5-2　Dynamic IP (DHCP) 画面

以下の設定項目があります。

項目	説明
Dynamic IP (DHCP)	
Host Name	ホスト名を指定します。
DNS Server (Domain Name System)	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」：手動で MAC アドレスを指定します。
MAC Address	ISP と紐付ける MAC アドレスを入力します。（「Use this MAC」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。（「Custom」選択時）
Port Speed	ポート速度を選択します。 • 初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

Static IP（スタティック IP アドレス設定）

「Connection Type」で「Static IP」を選択した場合の設定です。

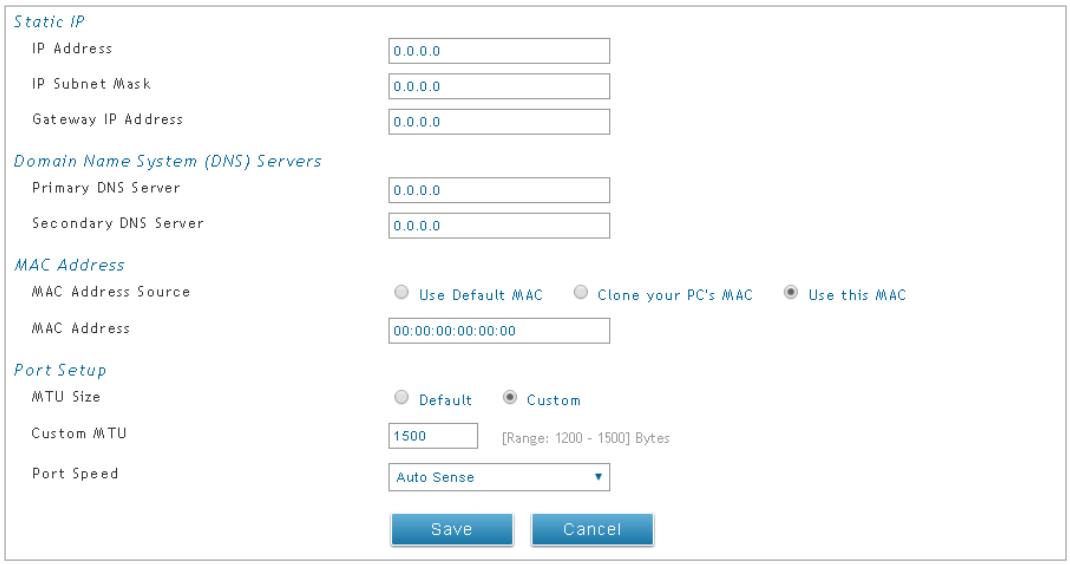

図 5-3　　Static IP 画面

以下の設定項目があります。

項目	説明
Static IP	
IP Address	ISP により提供された IP アドレスを入力します。
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。
Gateway IP Address	ISP により提供されたゲートウェイ IP アドレスを入力します。
Domain Name System(DNS) Servers	
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC 」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC 」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」：手動で MAC アドレスを指定します。
MAC Address	ISP と紐付ける MAC アドレスを入力します。（「Use this MAC」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。（「Custom」選択時）
Port Speed	ポート速度を選択します。 • 初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

PPPoE (Username/Password)（PPPoE 設定）

「Connection Type」で「PPPoE (Username/Password)」を選択した場合の設定です。

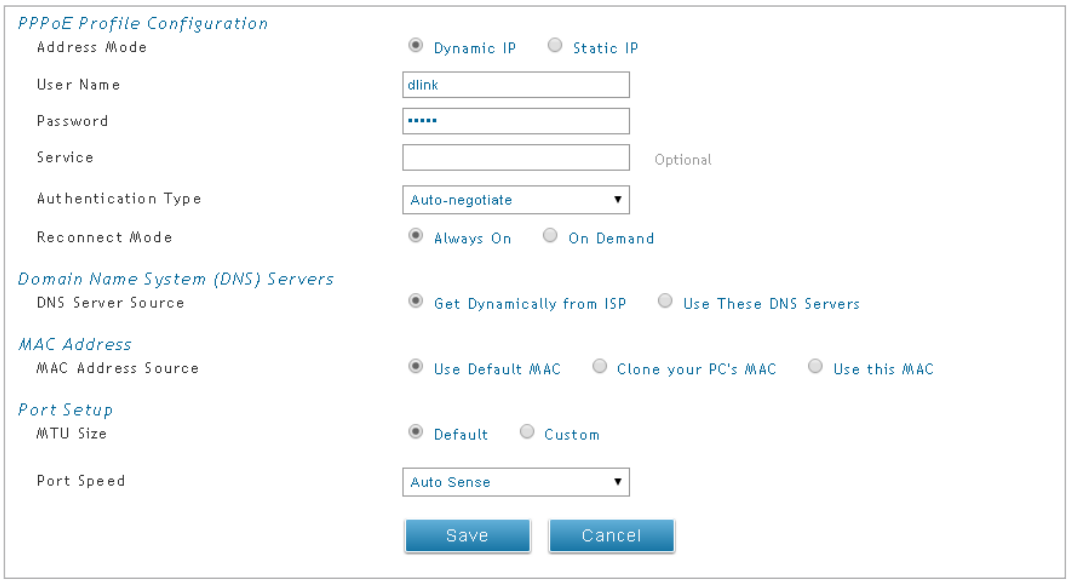

図 5-4　PPPoE (Username/Password) 画面

以下の設定項目があります。

項目	説明
PPPoE Profile Configuration	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP」選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP」選択時）
User Name	PPPoE のユーザ名を入力します。
Password	PPPoE のパスワードを入力します。
Service	ISP により指示があった場合にサービス名を入力します。
Authentication Type	プロファイルが使用する認証タイプを指定します。
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On」：常にインターネットに接続している状態となります。 • 「On Demand」：インターネット接続を開始した場合のみ、ルータがインターネットに接続します。一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers 」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers 」選択時）
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC 」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC 」：手動で MAC アドレスを指定します。
MAC Address	ISP と紐付ける MAC アドレスを入力します。（「Use this MAC」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。（「Custom」選択時）
Port Speed	ポート速度を選択します。 • 初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

PPTP (Username/Password)（PPTP 設定）

「Connection Type」で「PPTP (Username/Password)」を選択した場合の設定です。

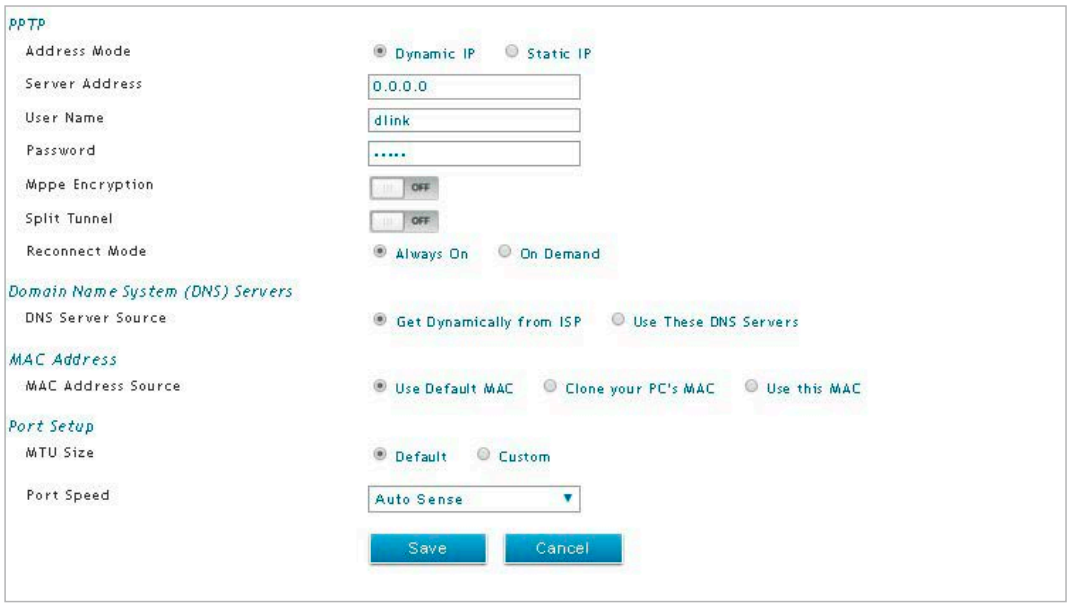

図 5-5　PPTP (Username/Password) 画面

以下の設定項目があります。

項目	説明
PPTP	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP」選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP」選択時）
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。（「Static IP」選択時）
Server Address	PPTP サーバのアドレスを入力します。
User Name	PPTP のユーザ名を入力します。
Password	PPTP のパスワードを入力します。
Mppe Encryption	PPTP サーバが MPPE 暗号化をサポートする場合に「ON」にします。
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。 「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On」：常にインターネットに接続している状態となります。 • 「On Demand」：インターネット接続を開始した場合のみ、ルータがインターネットに接続します。一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers 」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers 」選択時）
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」：手動で MAC アドレスを指定します。
MAC Address	ISP と紐付ける MAC アドレスを入力します。（「Use this MAC」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。（「Custom」選択時）
Port Speed	ポート速度を選択します。 • 初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

L2TP (Username/Password)（L2TP 設定）

「Connection Type」で「L2TP (Username/Password)」を選択した場合の設定です。

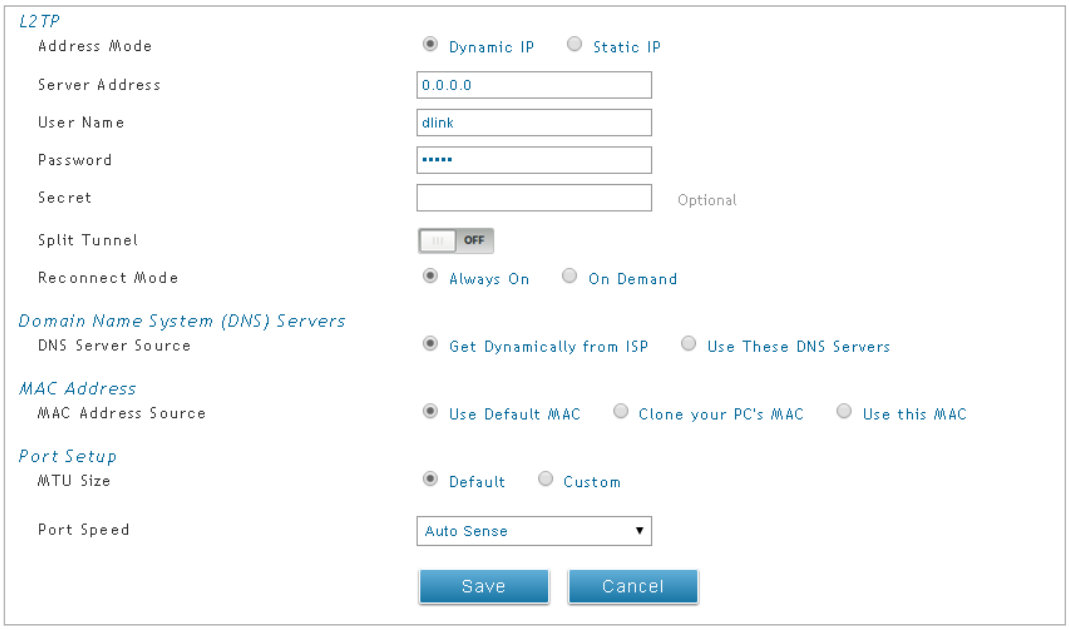

図 5-6　L2TP (Username/Password) 画面

以下の設定項目があります。

項目	説明
L2TP	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP」選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP」選択時）
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。（「Static IP」選択時）
Server Address	L2TP サーバのアドレスを入力します。
User Name	L2TP のユーザ名を入力します。
Password	L2TP のパスワードを入力します。
Secret	シークレットを入力します。
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。 「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On 」：常にインターネットに接続している状態となります。 • 「On Demand」：インターネット接続を開始した場合のみ、ルータがインターネットに接続します。一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers 」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers 」選択時）
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」：手動で MAC アドレスを指定します。
MAC Address	ISP と紐付ける MAC アドレスを入力します。（「Use this MAC」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。（「Custom」選択時）
Port Speed	ポート速度を選択します。 • 初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

Japanese multiple PPPoE（Japanese PPPoE 設定）

「Connection Type」で「Japanese multiple PPPoE」を選択した場合の設定です。

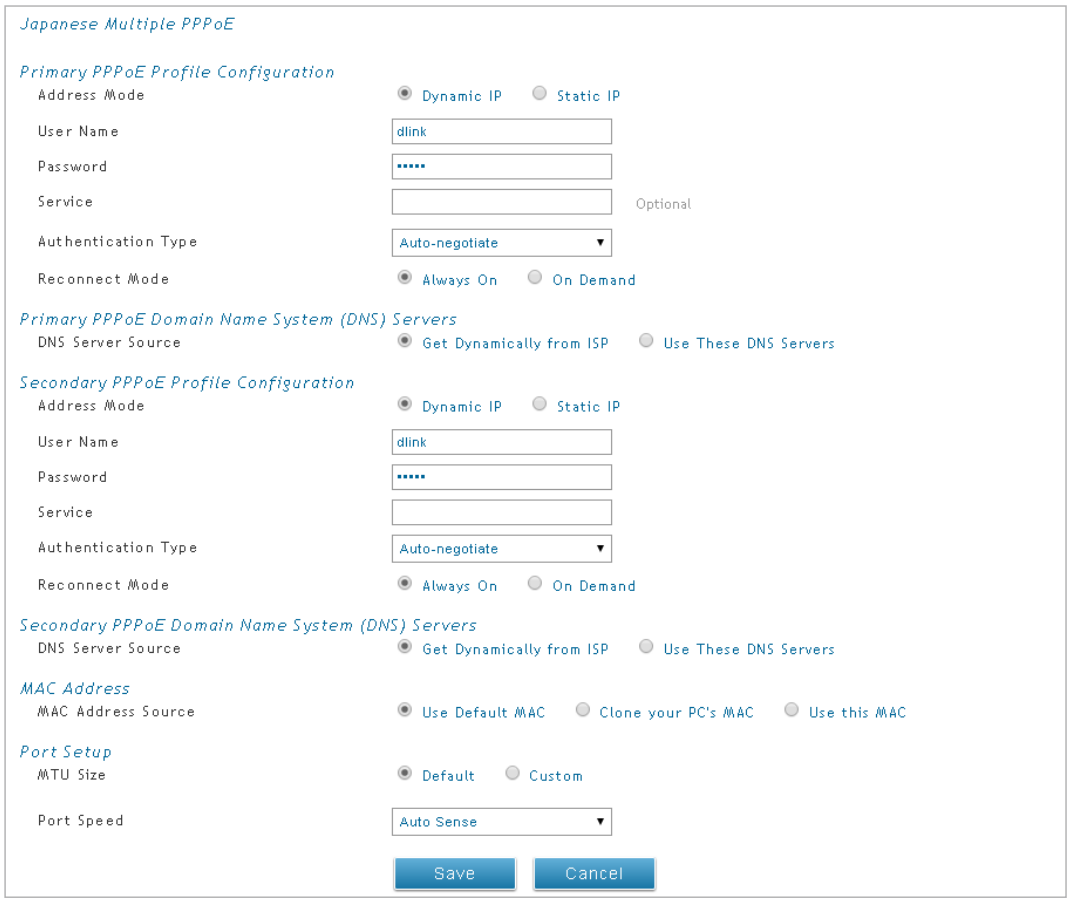

図 5-7　Japanese Multiple PPPoE 画面

以下の設定項目があります。

項目	説明
Primary PPPoE Profile Configuration	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP」選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP」選択時）
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。（「Static IP」選択時）
User Name	PPPoE のユーザ名を入力します。
Password	PPPoE のパスワードを入力します。
Service	ISP により指示があった場合にサービス名を入力します。
Authentication Type	プロファイルが使用する認証タイプを指定します。
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On 」：常にインターネットに接続している状態となります。 • 「On Demand 」：一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Primary PPPoE Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers 」選択時）
Secondary PPPoE Profile Configuration	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP」選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP」選択時）
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。（「Static IP」選択時）
User Name	PPPoE のユーザ名を入力します。

項目	説明
Password	PPPoE のパスワードを入力します。
Service	ISP により指示があった場合にサービス名を入力します。
Authentication Type	プロファイルが使用する認証タイプを指定します。
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On」： 常にインターネットに接続している状態となります。 • 「On Demand 」：一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Secondary PPPoE Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC 」：WAN1 ポートの IP アドレスを使用します。 • 「Clone your PC's MAC 」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC 」：手動で MAC アドレスを指定します。
MAC Address	MAC アドレスを入力します。（「Use this MAC」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。（「Custom」選択時）
Port Speed	ポート速度を選択します。 • 初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

Russian dual access PPPoE（Russian PPPoE 設定）

「Connection Type」で「Russian dual access PPPoE」を選択した場合の設定です。

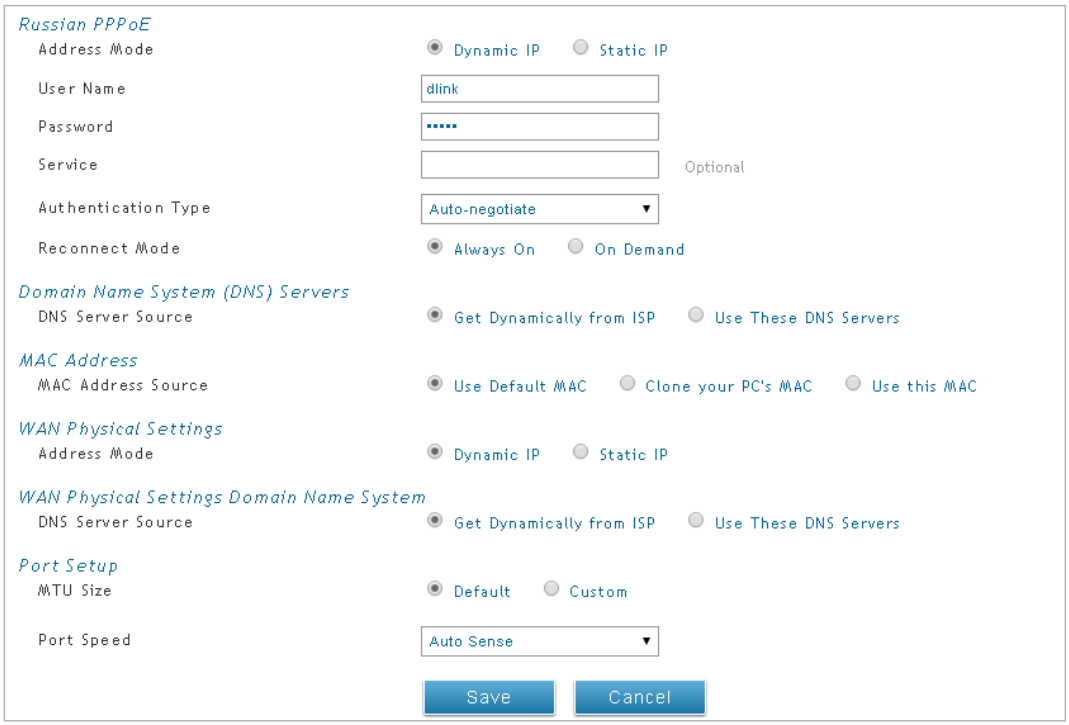

図 5-8　Russian dual access PPPoE 画面

以下の設定項目があります。

項目	説明
Russian PPPoE	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP 選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP 選択時）
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。（「Static IP 選択時）
User Name	PPPoE のユーザ名を入力します。
Password	PPPoE のパスワードを入力します。
Service	ISP により指示があった場合にサービス名を入力します。
Authentication Type	プロファイルが使用する認証タイプを指定します。
Domain Name System (DNS) Servers	
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On 」：常にインターネットに接続している状態となります。 • 「On Demand 」：一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」）選択時
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」）選択時
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC 」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」：手動で MAC アドレスを指定します。
MAC Address	MAC アドレスを入力します。（「Use this MAC」選択時）
WAN Physical Setting	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
WAN Physical Setting Domain Name System	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。
Port Speed	ポート速度を選択します。 • 初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

Russian dual access PPTP（PPTP 設定）

「Connection Type」で「Russian dual access PPTP」を選択した場合の設定です。

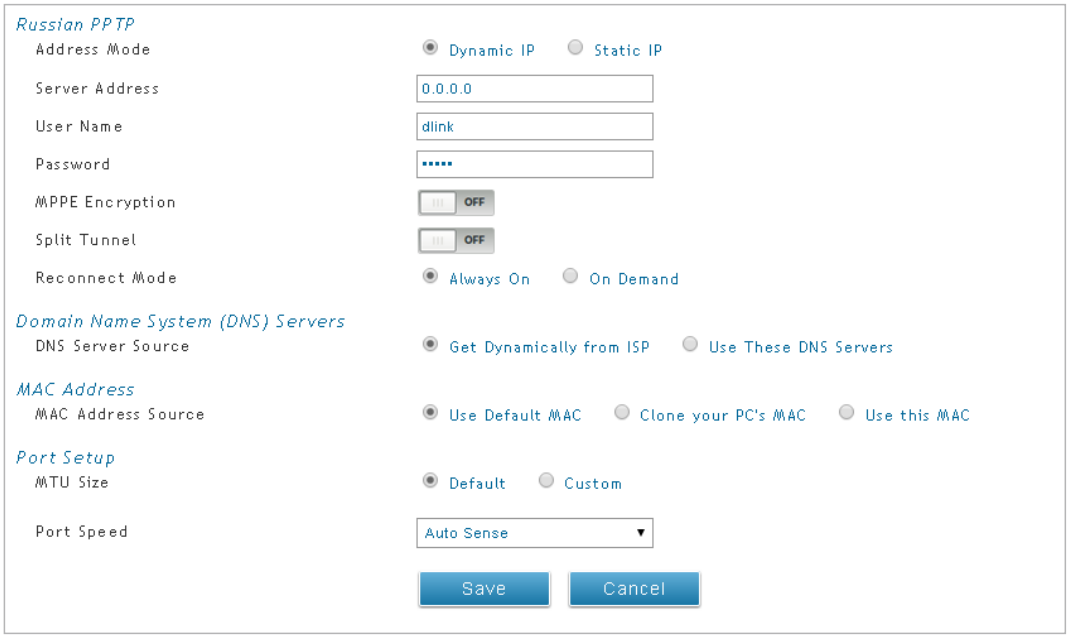

図 5-9　Russian dual access PPTP 画面

以下の設定項目があります。

項目	説明
Russian PPTP	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP」選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP」選択時）
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。（「Static IP」選択時）
Server Address	PPTP サーバの IP アドレスまたはドメイン名を入力します。
User Name	PPTP のユーザ名を入力します。
Password	PPTP のパスワードを入力します。
MPPE Encryption	PPTP サーバが MPPE 暗号化をサポートする場合に「ON」にします。
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。 「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On 」：常にインターネットに接続している状態となります。 • 「On Demand 」：一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC 」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC 」：手動で MAC アドレスを指定します。
MAC Address	MAC アドレスを入力します。
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。（「Custom」選択時）
Port Speed	ポート速度を選択します。初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

Russian dual access L2TP（Russian L2TP 設定）

「Connection Type」で「Russian dual access L2TP」を選択した場合の設定です。

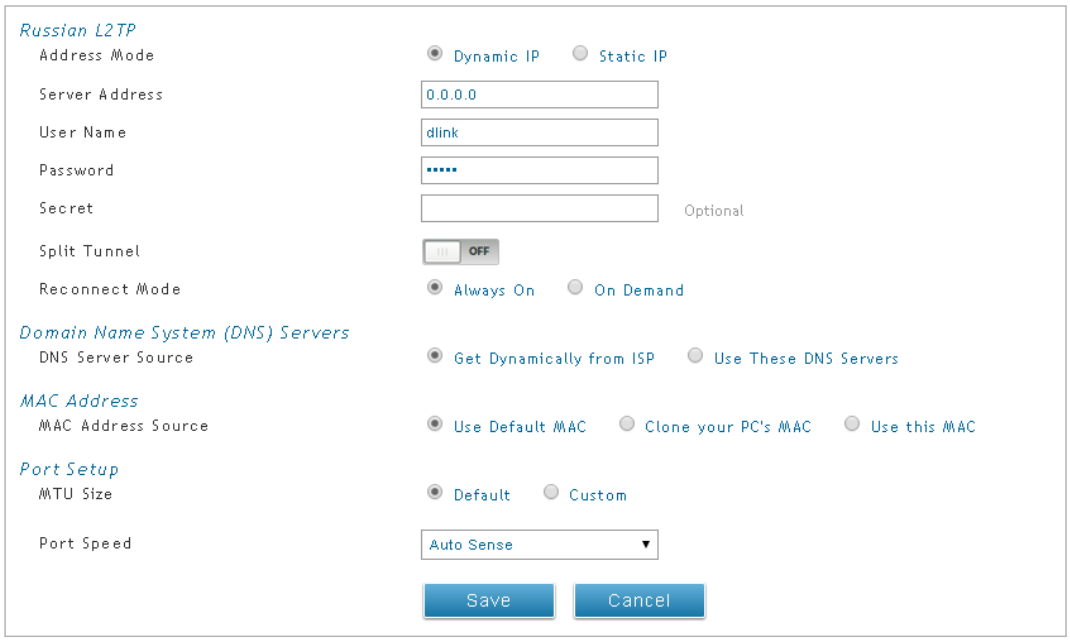

図 5-10　Russian dual access L2TP 画面

以下の設定項目があります。

項目	説明
Russian L2TP	
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。（「Static IP 」選択時）
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。（「Static IP 」選択時）
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。（「Static IP 」選択時）
Server Address	L2TP サーバの IP アドレスまたはドメイン名を入力します。
User Name	L2TP のユーザ名を入力します。
Password	L2TP のパスワードを入力します。
Secret	シークレットを入力します。
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。 「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。
Reconnect Mode	インターネットの再接続モードを以下から選択します。 • 「Always On」：常にインターネットに接続している状態となります。 • 「On Demand」：一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。 • 「Get Dynamically from ISP」：ご契約の ISP から自動的に DNS サーバアドレスを取得します。 • 「Use These DNS Servers」：ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」）選択時
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」：WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」：現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC 」：手動で MAC アドレスを指定します。
MAC Address	MAC アドレスを入力します。（「Use this MAC」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。
Port Speed	ポート速度を選択します。初期値：「Auto Sense」

「Save」をクリックし、設定を適用します。

WAN2 / DMZ Setting（WAN2 / DMZ 設定）

Network > Internet > WAN2 / DMZ Setting

WAN2 ポートに対して、WAN2 または DMZ の設定を行います。

WAN2 に設定する場合、設定内容は WAN1 の設定項目と同等です。DMZ（DeMilitarized Zone）は、外部ネットワークと社内ネットワークの中間につくられるネットワーク上のセグメントです。外部ネットワークからも内部ネットワークからもファイアウォールなどによって隔離されるため、DMZ 内にサーバを設置するなどしてセキュリティの強化を図ることができます。

1. **Network > Internet > IPv4 WAN2/ DMZ Setting** の順にメニューをクリックし、以下の画面を表示します。

図 5-11　IPv4 WAN2 / DMZ Setting「Configurable Port Setup」画面

2. 「WAN」または「DMZ」を選択します。
   「WAN」：WAN2 ポートに対して WAN の設定を行います。WAN の設定内容については「WAN1」での設定項目と同等になります。
   「DMZ」：WAN2 ポートに対して DMZ の設定を行います。

3. 選択後、表示される各項目の設定を行います。

WAN（WAN 設定 /WAN2）

「Configurable Port」で「WAN」を選択した場合、以下の画面が表示されます。

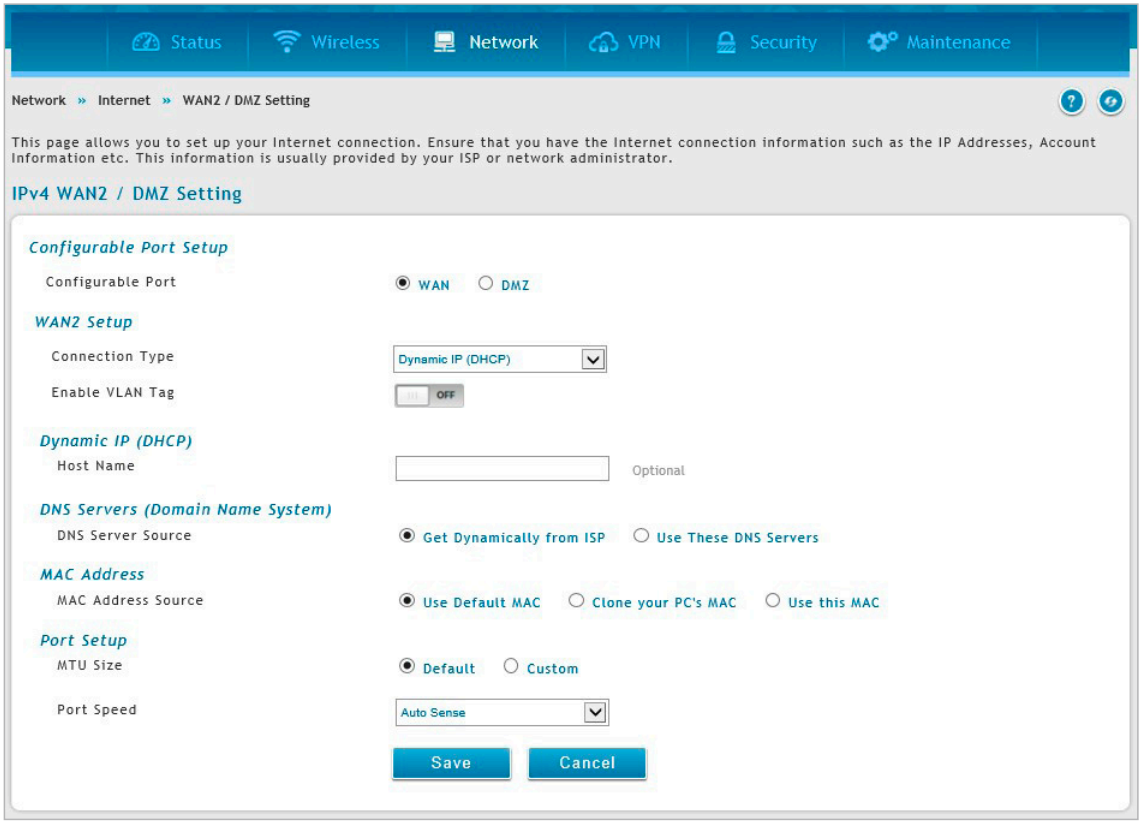

図 5-12　IPv4 WAN2 / DMZ Setting 画面

注意　「WAN2 / DMZ Setting」での「WAN」の設定項目については「WAN1 Settings（WAN1 設定）」と同等となります。WAN2 ポートにおける WAN の設定を行うには「WAN1 Settings（WAN1 設定）」を参照してください。

DMZ（DMZ 設定 /WAN2）

本製品の WAN2 ポートは、セカンダリ WAN イーサネットポート、または DMZ ポートとして設定できます。

DMZ（DeMilitarized Zone）は、パブリックにオープンでありながらファイアウォールに保護されたサブネットワークです。
DMZ により、「特定のポート／サービスによるインターネットへのアクセスは許可しても、ネットワーク（LAN）にはアクセスさせない」というセキュリティレイヤを提供できます。
Web サーバやメールサーバなど、インターネットへのアクセスを必要とするホストを DMZ ネットワークに配置することが推奨されます。

ファイアウォールのルールでは、LAN 及び WAN 両方からの DMZ 上の指定サービス / ポートへのアクセスを許可することができます。DMZ ノードへの攻撃イベントが発生した場合、必ずしも LAN が脆弱になるという訳ではありません。

DMZ 設定は LAN 設定と同等です。DMZ ポートに対しては、ゲートウェイの IP アドレスと同等の IP アドレスを付与すること以外、IP アドレス / サブネットマスクの設定に関する制限はありません。

1. 「IPv4 WAN2 / DMZ Setting」画面の「Configurable Port」で「DMZ」を選択します。

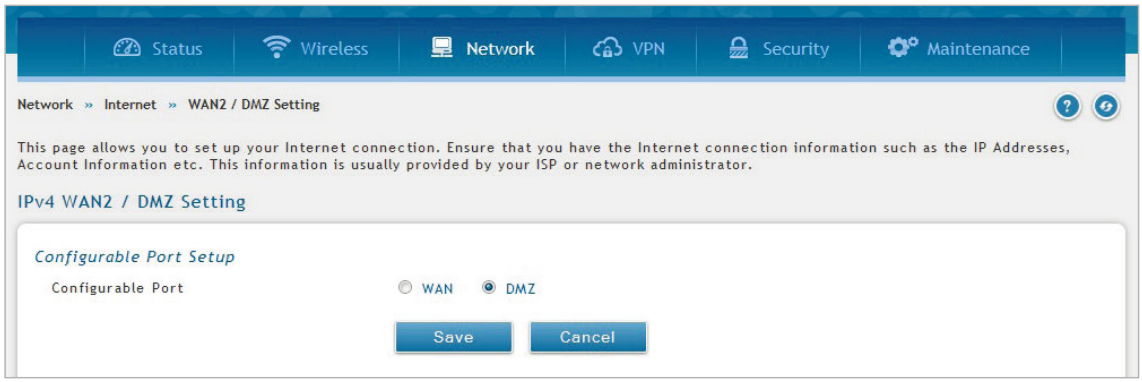

図 5-13　IPv4 WAN2 / DMZ Setting 画面

2. 「Save」をクリックし、設定を適用します。

注意　「WAN2 / DMZ Setting」で DMZ を有効にした場合、DMZ の設定を行う必要があります。WAN2 ポートにおける DMZ の設定を行うには「DMZ Settings（DMZ 設定）」を参照してください。

WAN3 Setting（WAN3 / 3G インターネット設定（未サポート））

Network > Internet > WAN3 Settings

注意　本項目（WAN3 Settings）は未サポートです。

本ルータは 3G インターネットアクセスをサポートしています。DSR シリーズ用 3G USB モデムを使用して、携帯電話用 3G インターネットアクセスが利用できます。実際の接続を行うには通信会社から提供される 3G データプランからの認証要件を満たす必要があります。通信会社から提供される電話番号と APN が固有に存在します。接続種類を設定・保存した後、WAN ステータスのページ（**Status > System Information > Device > WAN3**）から、WAN3 リンクを有効にして 3G 接続を確立することが可能です。

1. **Network > Internet > WAN Mode** の順にメニューをクリックし、以下の画面を表示します。

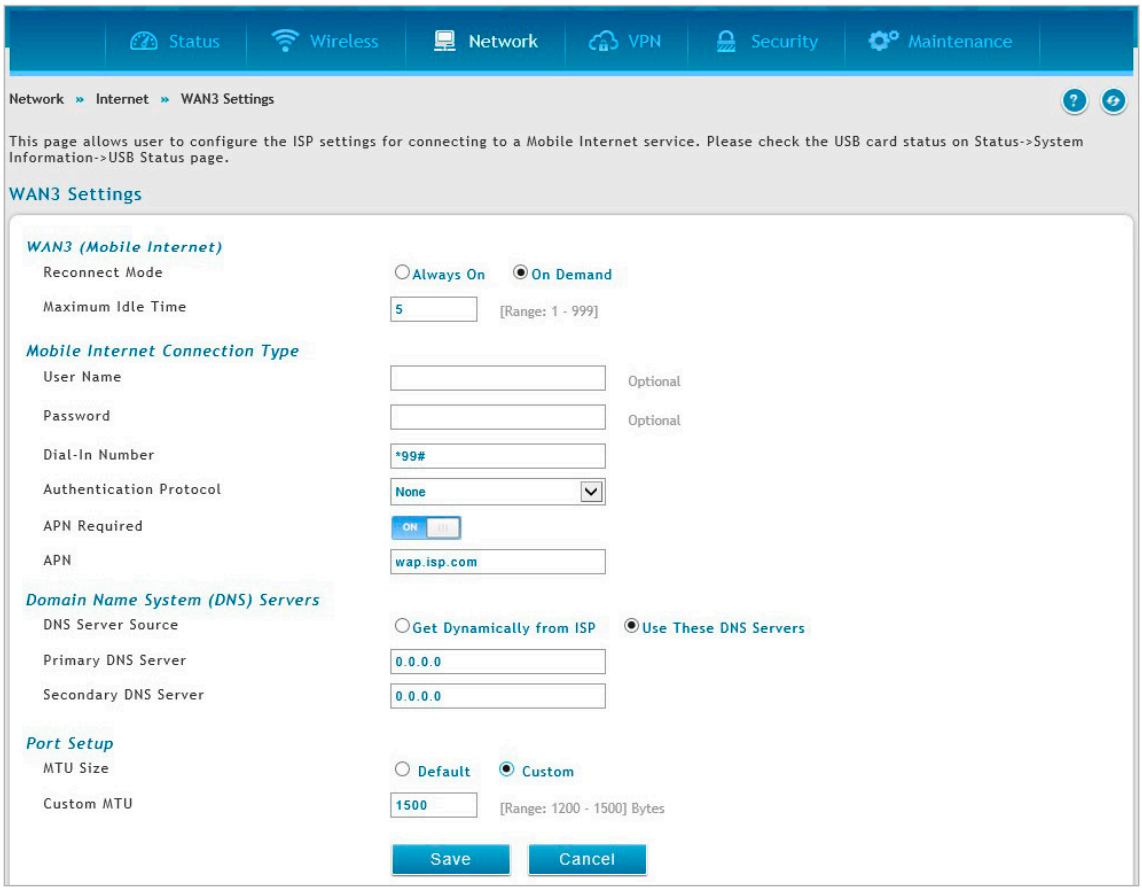

図 5-14　WAN3 Settings 画面

2. 以下の項目を設定します。

項目	説明
WAN3 (Mobile Internet)	
Reconnect Mode	以下のオプションの 1 つを選択します。 ・「Always On」：常にインターネットに接続している状態となります。 ・「On Demand」：一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。（「On Demand」選択時）
Mobile Internet Connection Type	
User Name	3G アカウントのユーザ名を入力します。
Password	3G アカウントのパスワードを入力します。
Dial-In Number	インターネットへのアクセスに使用するダイヤル番号を入力します。
Authentication Protocol	認証プロトコルを指定します。「None」「PAP」「CHAP」から指定できます。
APN Required	お使いの ISP 接続に APN を要件としている場合「ON」にします。
APN	ISP から提供される APN（アクセスポイント名）を入力します。
Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバ情報の設定方法を「Get Dynamically from ISP」「Use These DNS Servers」から指定します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。（「Use These DNS Servers」選択時）
Port Setup	
MTU Size	MTU 値を「Default」（初期値：1500）または「Custom」に設定します。
Custom MTU	ISP とのパフォーマンスを最適にする MTU 値を指定します。（「Custom」選択時）

3. 「Save」をクリックし、設定を適用します。

WAN Mode（WAN モード設定）

Network > Internet > WAN Mode

本製品は、複数の WAN リンクをサポートしています。一つのポートで WAN 接続が不安定になった場合でも、フェイルオーバ機能およびロードバランシング機能により、インターネットを利用する特定のサービスを優先的に処理することができます。

オートフェイルオーバまたはロードバランシングを使用するためには、WAN リンク障害検知を設定する必要があります。これにはインターネット上の DNS サーバへのアクセス、またはインターネットアドレス（ユーザ定義）への ping といった検知設定が含まれています。必要に応じて、リンクが切断していることが疑われる場合のリトライ回数や、WAN ポートがダウンしているかどうかを判断する障害のしきい値を設定することができます。

1. **Network > Internet > WAN Mode** の順にメニューをクリックし、以下の画面を表示します。

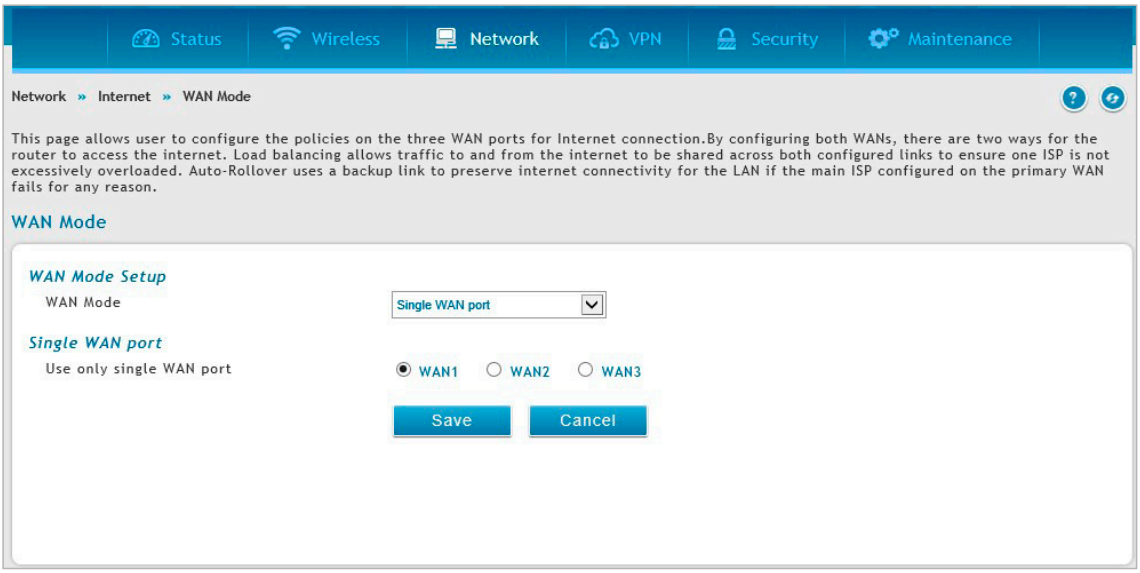

図 5-15　WAN Mode 画面

2. 「WAN Mode Setup」の「WAN Mode」で WAN リンクの種類を選択します。

Single WAN Port（シングル WAN ポート）

オートフェイルオーバまたはロードバランシングを使用しない場合、「Single WAN Port」を選択します。

1. 「WAN Mode」で「Single WAN Port」を選択します。

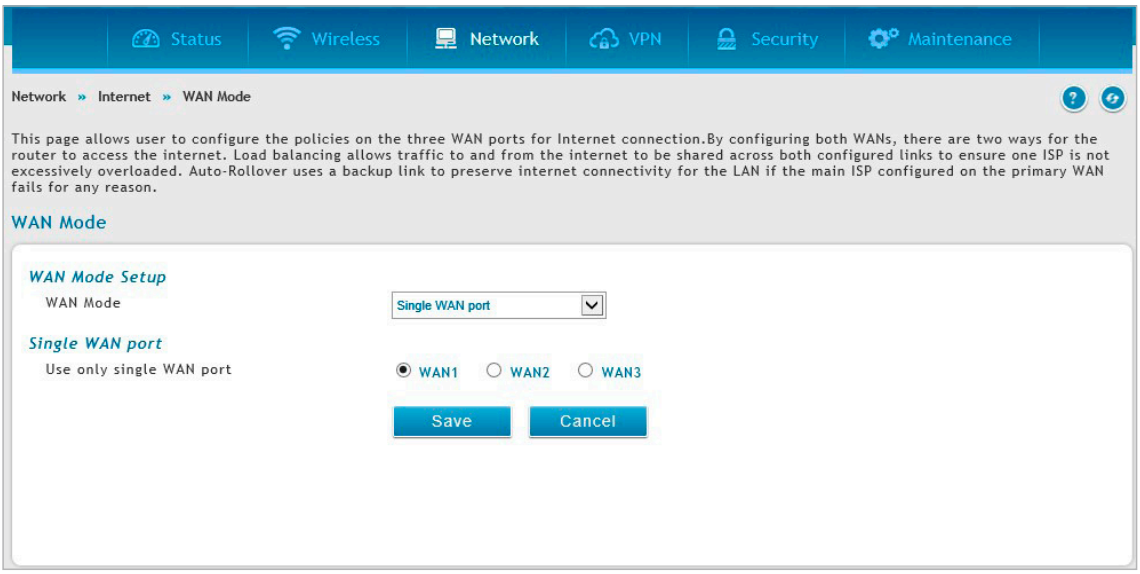

図 5-16　WAN Mode（Single WAN Port）画面

2. 対象の WAN ポートを「WAN1」「WAN2」「WAN3」から選択します。
3. 「Save」をクリックし、設定を適用します。

Auto-Rollover using WAN port（WAN ポートを使用したオートロールオーバ）

本項目では、1 つの WAN ポートをインターネットトラフィック用のプライマリインターネットリンクとして設定し、もう 1 つの WAN ポートをセカンダリインターネットリンクとして設定します。セカンダリインターネットリンクは、なんらかの理由でプライマリリンクがダウンした場合の冗長用として使用されます。本機能を有効にする前に、プライマリ WAN ポート / セカンダリ WAN ポートともに接続用の ISP 情報を設定しておく必要があります。セカンダリ WAN ポートは、プライマリ WAN ポートがダウンした場合のみ接続されます。いずれのポートもプライマリとして使用することができます。オートフェイルオーバモードで設定を行った場合、プライマリ WAN ポートはリンクダウン検知で設定した期間に従いリンクステータスをチェックされます。

1. 「WAN Mode」で「Auto-Rollover Using WAN IP」を選択します。

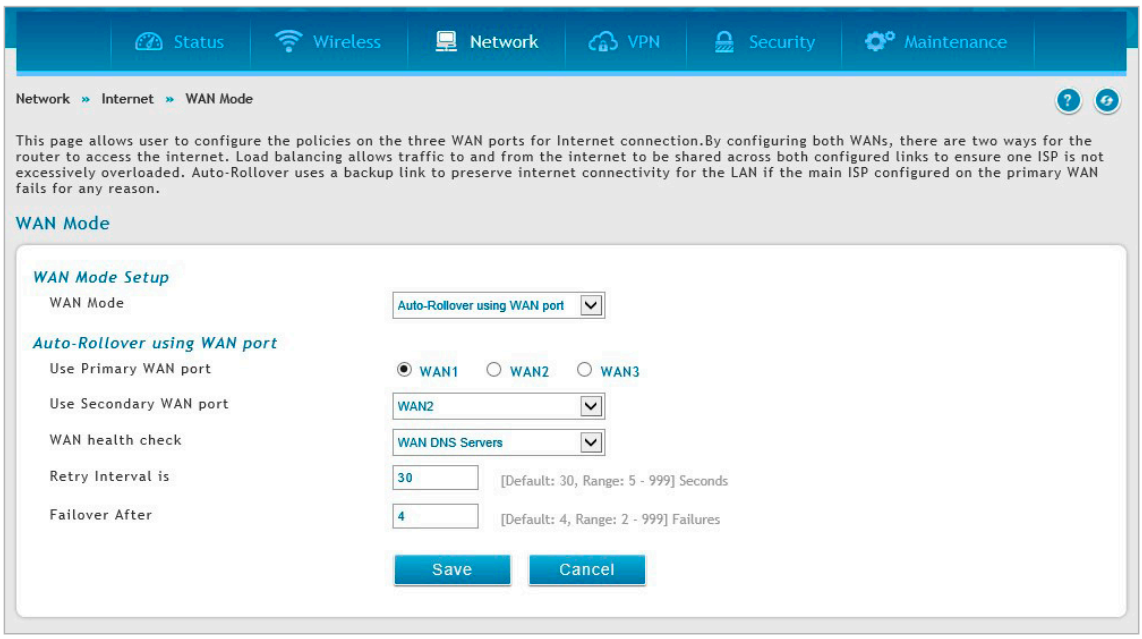

図 5-17　WAN Mode（Auto-Rollover Using WAN port）画面

2. 以下の項目を設定します。

項目	説明
Use Primary WAN Port	プライマリリンクとしての WAN ポートを指定します。
Use Secondary WAN Port	プライマ WAN ポートがダウンした場合に使用されるセカンダリリンクとしての WAN ポートを指定します。
WAN health check	WAN ポートに対するステータスチェックの種類を以下から選択します。 • 「WAN DNS Servers 」： DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 • 「DNS Servers」： カスタム DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 • 「Ping These IP Addresses」： 定期的な Ping を実行してプライマリ WAN の接続性をチェックします。
WAN1/WAN2/WAN3	「DNS Servers」または「Ping These IP Addresses」を選択した場合、Ping を実行する DNS サーバまたは IP アドレスを指定します。WAN3 は未サポートです。
Retry Interval is	「WAN health check」をルータが実行する頻度を指定します。 • 設定可能範囲：5-999（秒） • 初期値：30（秒）
Failover After	フェイルオーバが有効になるまでのリンク不具合の回数を設定します。 • 設定可能範囲：2-999（回） • 初期値：4（回）

3. 「Save」をクリックし、設定を適用します。

Load Balancing（ロードバランシング）

本機能により、同時に複数の WAN リンク（および、複数の ISP）を使用することができます。WAN ポートを複数設定した後、ロードバランシングオプションにより、2 つ以上のリンクにトラフィックを送信するように設定することができます。また、インターネットフロー管理において、各プロトコルサービスを各 WAN ポートに振り分けるために、プロトコルバインディングが使用されます。ロードバランシングモードが設定されている場合、定義した障害検出方式が、すべての設定済み WAN ポート上で定期的に実行されます。

本ルータは、以下のアルゴリズムをサポートしています。

- **Round Robin**
  1 つの WAN ポートの接続速度が他の速度と大きく異なる場合に特に役に立ちます。この場合、遅延の少ないサービス（VoIP など）をより高速なリンクに送信し、低容量のバックグラウンドトラフィック（SMTP など）は低速のリンクに転送するようにプロトコルバインディングを定義できます。
- **Spill Over**
  定義したしきい値に達するまで、プライマリ WAN が専用リンクとして機能します。しきい値に達した後、セカンダリ WAN が新しい接続に使用されます。スピルオーバロジックにより、プライマリからセカンダリ WAN に移動するアウトバウンド通信が管理されるため、セカンダリ WAN におけるインバウンド接続は、本モードで許可されます。スピルオーバモードでは次のオプションを設定することができます。
  - Load Tolerance : この最大帯域幅（%）を超えた場合、プライマリ WAN からセカンダリ WAN に切り替わります。
  - Max Bandwidth : アウトバウンドトラフィックに対してプライマリ WAN で許可される最大の帯域幅を設定します 。

  アウトバウンドトラフィックのリンク帯域がロードトレランス最大帯域を上回ると、ルータは次の接続をセカンダリ WAN に切り替えます。

  例 : プライマリ WAN の最大帯域幅 :1Kbps、ロードトレランス :70 の場合
  ある接続数で帯域幅が 1Kbps の 70% に到達すると、新規のアウトバウンド接続はセカンダリ WAN に切り替えられます。

ロードバランシングは、1 つの WAN ポートの接続速度が他と大きく異なる場合に特に役に立ちます。この場合、低遅延のサービス（VoIP など）をより高速なリンクに送信し、低容量のバックグラウンドトラフィック（SMTP など）は低速のリンクに転送するようにプロトコルバインディングを定義できます。

Round Robin（ラウンドロビン）

1. 「WAN Mode」で「Load Balancing」を選択 →「Round Robin」を選択し以下の画面を表示します。

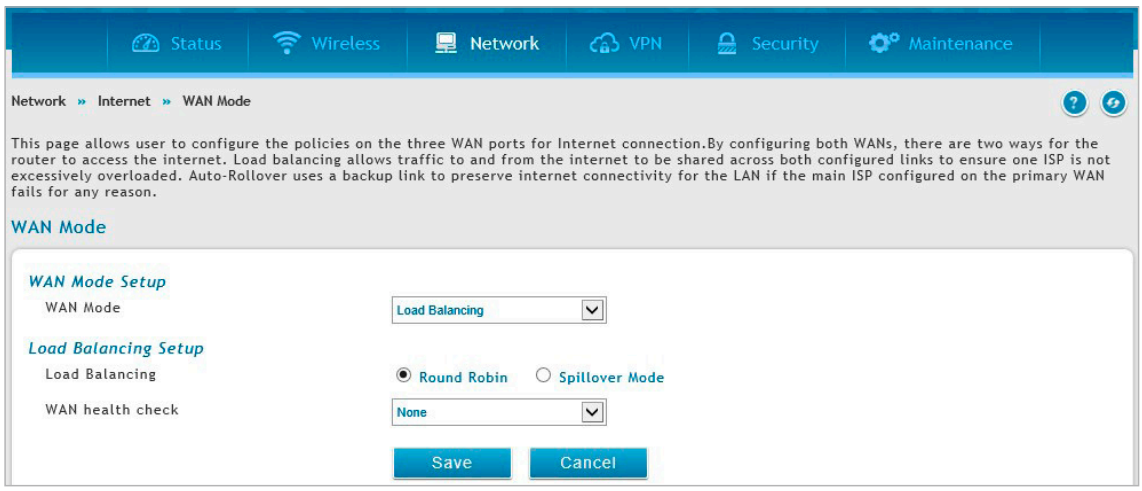

図 5-18　Load Balancing（Round Robin）画面

2. 以下の項目を設定します。

項目	説明
Load Balancing	「Round Robin」を選択します。
WAN health check	WAN ポートに対するステータスチェックの種類を以下から選択します。 • 「WAN DNS Servers 」: DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 • 「DNS Servers」: カスタム DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 • 「Ping these IP addresses」: 定期的な Ping を実行してプライマリ WAN の接続性をチェックします。
WAN1/WAN2/WAN3	「DNS Servers」または「Ping These IP Addresses」を選択した場合、Ping を実行する DNS サーバまたは IP アドレスを指定します。WAN3 は未サポートです。
Retry Interval is	「WAN health check」をルータが実行する頻度を指定します。 • 設定可能範囲：5-999（秒） / 初期値：30（秒）
Failover After	フェイルオーバが有効になるまでのリンク不具合の回数を設定します。 • 設定可能範囲：2-999（回） / 初期値：4（回）

3. 「Save」をクリックし、設定を適用します。

Spillover Mode（スピルオーバモード）

1. 「WAN Mode」で「Load Balancing」を選択 →「Spillover Mode」を選択し、以下の画面を表示します。

注意 スピルオーバモードを使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

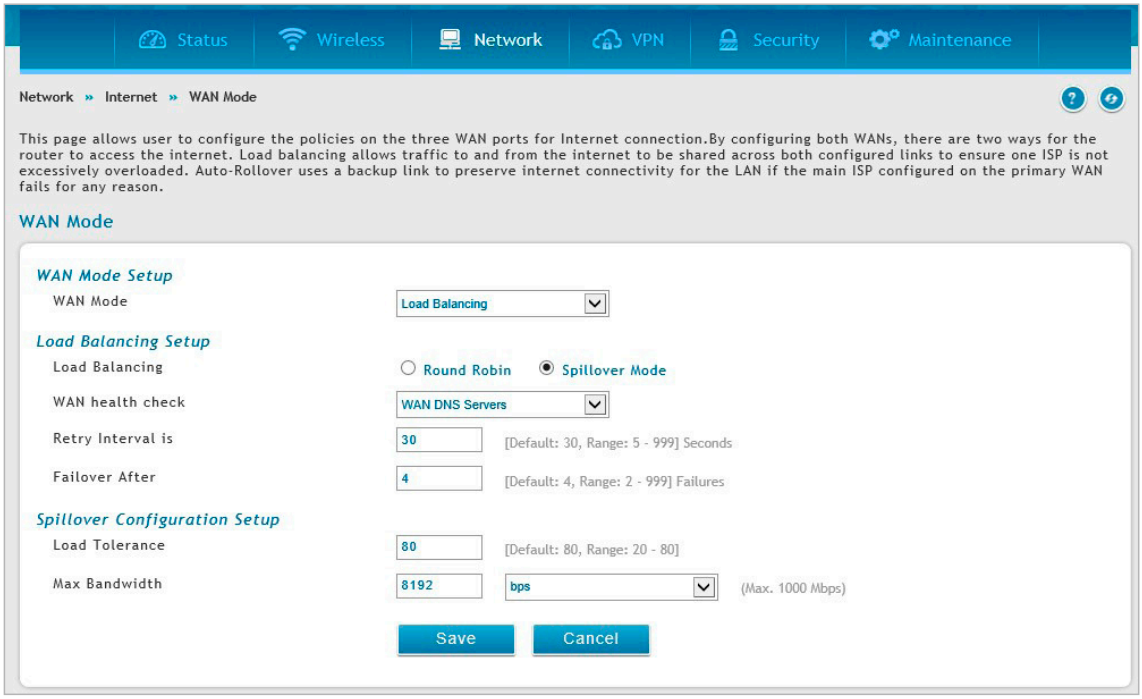

図 5-19　Load Balancing（Spillover Mode）画面

2. 以下の項目を設定します。

項目	説明
Load Balancing Setup	
Load Balancing	「Spillover Mode」を選択します。
WAN health check	WAN ポートに対するステータスチェックの種類を以下から選択します。 • 「WAN DNS Servers」： DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 • 「DNS Servers」： カスタム DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 • 「Ping These IP Addresses」： 定期的な Ping を実行してプライマリ WAN の接続性をチェックします。
WAN1/WAN2/WAN3	「DNS Servers」または「Ping These IP Addresses」を選択した場合、Ping を実行する DNS サーバまたは IP アドレスを指定します。WAN3 は未サポートです。
Retry Interval is	「WAN health check」をルータが実行する頻度を指定します。 • 設定可能範囲：5-999（秒） • 初期値：30（秒）
Failover After	フェイルオーバが有効になるまでのリンク不具合の回数を設定します。 • 設定可能範囲：2-999（回） • 初期値：4（回）
Spillover Configuration Setup	
Load Tolerance	ルータがセカンダリ WAN に切り替わる最大帯域幅（%）を指定します。
Max Bandwidth	プライマリ WAN で許可される最大の帯域幅を設定します。 帯域幅の単位は「bps」「Mbps」「Kbps」から指定します。

3. 「Save」をクリックし、設定を適用します。

SIM Card Authentication（SIM カード認証（未サポート））

Network > Internet > SIM Card Authentication

本ルータは SIM カードをサポートしています。SIM カードのスロットにより携帯電話のモジュールと統合されます。SIM カードの種類によって、3G と 4G がサポートされます。インターネットの利用を開始するには、スロットに SIM カードを挿入し、PIN コードを入力して SIM を解除します。

注意　本項目は未サポートです。

1. **Network > Internet > SIM Card Authentication** の順にメニューをクリックし、以下の画面を表示します。

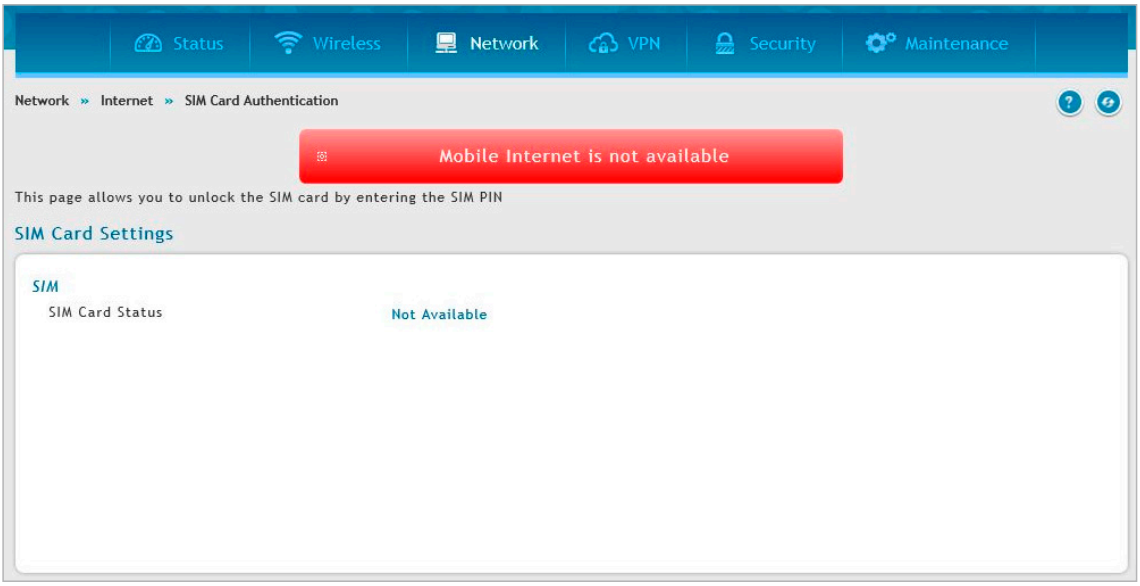

図 5-20　SIM Card Authentication 画面

2. 以下の項目を設定します。

項目	説明
SIM Card Status	SIM カードのステータス（ロック / ロック解除 / ブロック）が表示されます。
Enter SIM PIN	SIM カードがロックされている場合に表示されます。PIN コード（4-8 桁の数字）を入力して SIM カードを解除します。SIM カードがロックされている場合、全てのネットワークサービスがブロックされます。モバイルインターネット及び SMS サービスを利用するには SIM カードのロックを解除する必要があります。

3. 「Save」をクリックし、設定を適用します。

Routing Mode（ルーティングモード設定）

Network > Internet > Routing Mode

LAN と WAN 間のルーティングは、本ルータが物理インタフェースで受信するトラフィックを処理する方法に影響を与えます。
ゲートウェイのルーティングモードは、安全な LAN とインターネット間のトラフィックフローの動作におけるコアとなります。

ルーティングモードの設定

以下のルーティングモードについて説明します。

「NAT or Classical」
「Transparent」
「Bridge」

■ NAT or Classical（NAT/ クラシカルモード）の設定

Classical ルーティングでは、適切なファイアウォールの設定がなされている場合、LAN 上のデバイスはパブリック IP アドレスでインターネット上から直接アクセスする事が可能です。ご利用の ISP からコンピュータ／デバイス用に IP アドレスが割り当てられている場合は、「Classical」を選択します。NAT は LAN の複数のコンピュータがインターネット接続を共有できる技術です。LAN 上のコンピュータは「プライベート」の IP アドレス範囲を使用し、一方、ルータの WAN ポートは 1 つの「パブリック」IP アドレスに設定されます。NAT によって接続の共有が可能になるほか、内部の IP アドレスをインターネット上のコンピュータから隠すことができます。ISP により割り当てられた IP アドレスが 1 個だけの場合、NAT が必要になります。ルータ経由で接続するコンピュータは、プライベートサブネットから IP アドレスを割り当てられる必要があります。

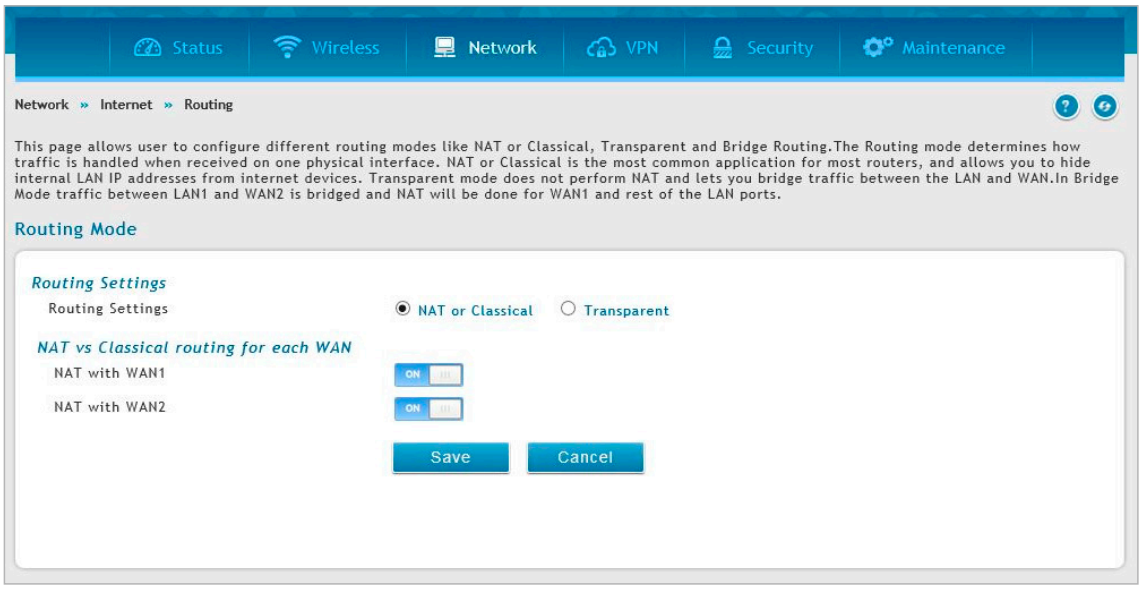

図 5-21　Routing Mode - NAT or Classical 画面

以下の項目を設定します。

項目	説明
Routing Settings	MAT/ クラシカルモードを有効にするには、「NAT or Classical」を選択します。
NAT with WAN1/ NAT with WAN2	WAN1/WAN2 の NAT を「ON」または「OFF」（Classical）にします。

「Save」をクリックし、設定を適用します。

■ Transparent（透過モード）の設定

透過ルーティングモードが有効である場合、LAN と WAN の間のトラフィックに NAT は実行されません。ファイアウォールまたは VPN ポリシーによってフィルタされない場合、LAN インタフェースに到着するブロードキャスト / マルチキャストパケットは WAN にスイッチされます。逆の場合も同様です。LAN と WAN が同じブロードキャストドメインにある場合は、透過モードを選択します。これにより、ルータで終了するトラフィックおよび他の管理トラフィックを除き、LAN から WAN のトラフィック、および WAN から LAN のトラフィックをブリッジすることができます。LAN と WAN が同じブロードキャストドメインにある場合、本製品のすべての機能が透過モードでサポートされます。

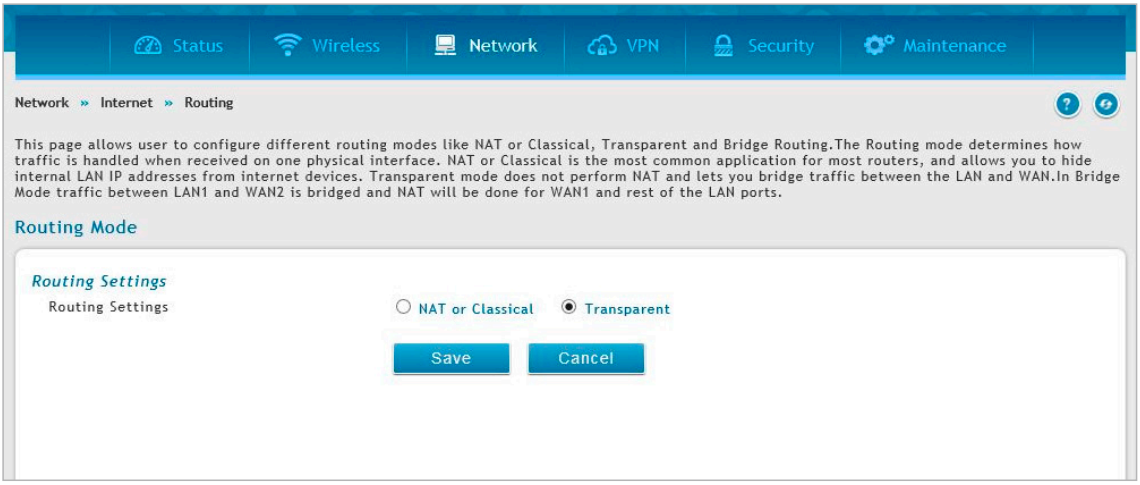

図 5-22　Routing Mode - Transparent 画面

以下の項目を設定します。

項目	説明
Routing Settings	透過モードを有効にするには、「Transparent」を選択します。

「Save」をクリックし、設定を適用します。

■ Bridge（ブリッジモード）の設定

ブリッジモードルーティングが有効になると、最初の物理 LAN ポートとセカンダリ WAN / DMZ（ポート 2）インタフェースがレイヤ 2 でブリッジされ、集約ネットワークが作成されます。他の LAN ポートとプライマリ WAN（WAN1）はこのブリッジの一部ではないため、ルータはこれらの他のポートに対する NAT デバイスとして要求します。LAN ポート 1 および WAN2 / DMZ インタフェースのブリッジモードでは、L2 / L3 ブロードキャストトラフィックと ARP / RARP パケットが通過します。WAN 2 がタグ付きトラフィックを受信すると、パケットが LAN ポート 1 インタフェースに転送される前にタグ情報が削除されます。

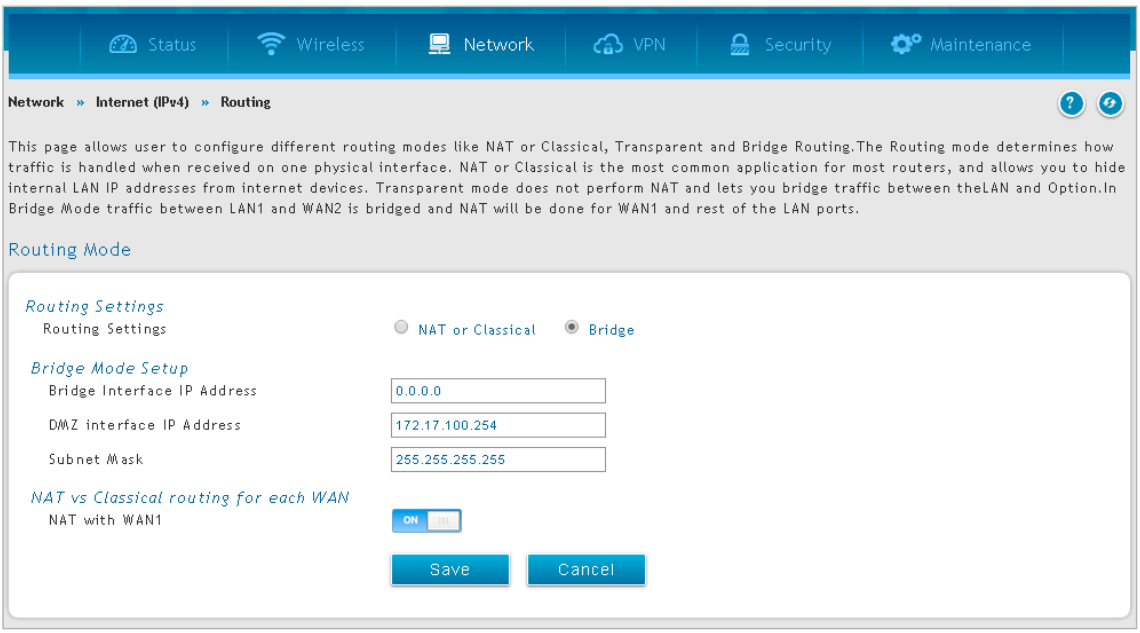

図 5-23　Routing Mode - Bridge 画面

注意　**Network > Internet > WAN2 / DMZ Setting** 画面で DMZ を選択した場合のみ、「Bridge」の項目が表示されます。

以下の項目を設定します。

項目	説明
Routing Settings	
Routing Settings	ブリッジモードを有効にするには、「Bridge」を選択します。ブリッジモードルーティングが有効である場合、物理 LAN ポート 1 とセカンダリ WAN/DMZ インタフェースにおいてトラフィックがブリッジされ、WAN1 と他の LAN ポートに対しては NAT が実行されます。 注意 ルーティングモード（NAT or Classical、Transparent、Bridge）を変更した場合、すべてのインバウンドファイアウォールルールが削除されます。
Bridge Mode Setup	
Bridge Interface IP Address	ブリッジインタフェースの IP アドレスを入力します。
DMZ Interface IP Address	DMZ インタフェースの IP アドレスを入力します。
Subnet Mask	サブネットマスクを入力します。
NAT vs Classical routing for each VLAN	
NAT with WAN1	WAN1 の NAT を「ON」または「OFF」（Classical）にします。

「Save」をクリックし、設定を適用します。

IP Aliasing（IP エイリアス設定）

Network > Internet > IP Aliasing

IP エイリアスアドレスを設定します。
ポートにエイリアスを追加することで、単一の WAN イーサネットポートに複数の IP アドレスでアクセスできます。

1. **Network > Internet > IP Aliasing** の順にメニューをクリックし、以下の画面を表示します。

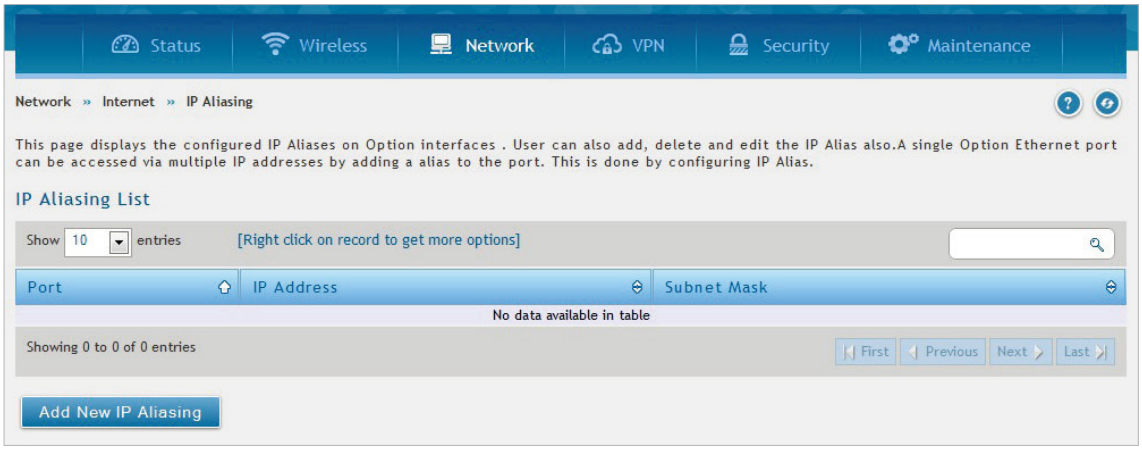

図 5-24　IP Aliasing 画面

2. IP エイリアスを追加する場合は、「Add New IP Aliasing」をクリックし以下の画面を表示します。

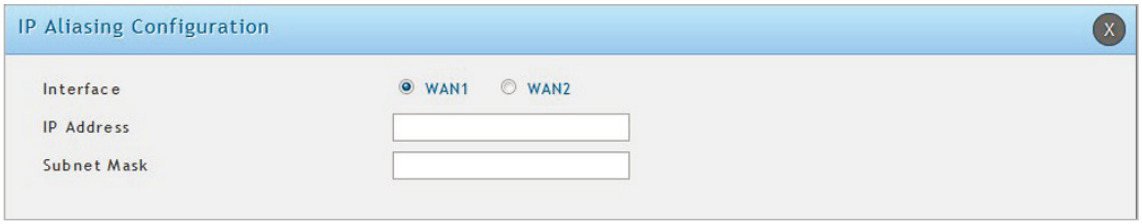

図 5-25　IP Aliasing Configuration 画面

3. 以下の項目を設定します。

項目	説明
Interface	IP エイリアスを設定するインタフェースを「WAN1」「WAN2」から選択します。
IP Address	IP エイリアスの IP アドレスを設定します。
Subnet Mask	IP エイリアスのサブネットマスクを設定します。

4. 「Save」をクリックし、設定を適用します。

追加した予約 IP エイリアスは、IP Aliasing 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

DMZ Settings（DMZ 設定）

Network > Internet > DMZ Settings

WAN2 ポートを DMZ に設定している場合、本項目で DMZ の設定を行う必要があります。

注意 DMZ ポートを設定するためには、**Network > Internet > WAN2 Settings / DMZ Setting** で WAN2 ポートに対して「DMZ」を有効にする必要があります。「IPv4 WAN2 / DMZ Setting」画面の「Configurable Port Setup」で、WAN2 ポートの設定に「DMZ」を選択します。

1. **Network > Internet > DMZ Settings** の順にメニューをクリックし、以下の画面を表示します。

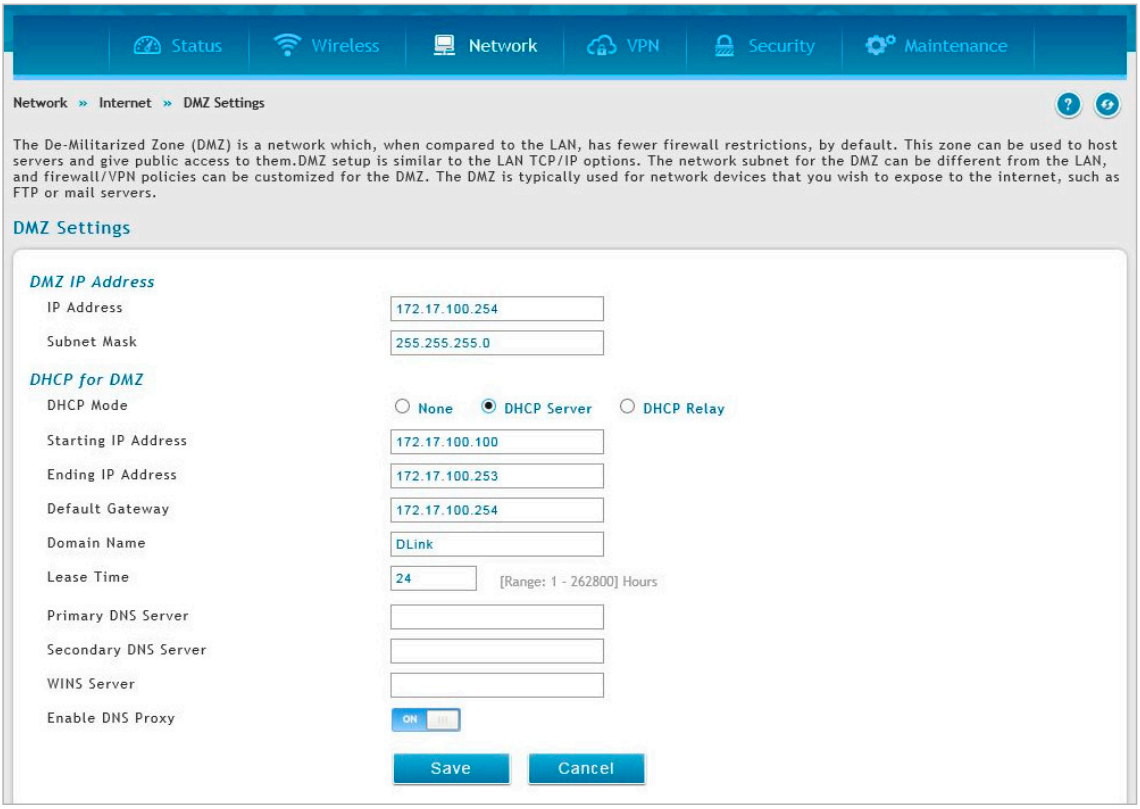

図 5-26　DMZ Settings 画面

2. 以下の項目を設定します。

項目	説明
DMZ IP Address	
IP Address	DMZ LAN IP アドレスを入力します。
Subnet Mask	上記の IP アドレスのサブネットマスクを入力します。
DHCP for DMZ	
DHCP Mode	• 「None」：DHCP 機能を無効化します。 • 「DHCP Server」：ネットワーク上で本ルータを DHCP サーバとして使用します。DHCP サーバ情報を設定します。 • 「DHCP Relay」：ネットワーク上の DHCP クライアントは、異なるサブネットの DHCP サーバから IP アドレスを取得することができます。DHCP Relay を選択した場合は、リレーゲートウェイ情報を入力します。
Starting IP Address	アドレス範囲の開始 IP アドレスを入力します。 DMZ に参加する新しい DHCP クライアントは、このアドレス範囲内で IP アドレスが付与されます。
Ending IP Address	アドレス範囲の終了 IP アドレスを入力します。 DMZ に参加する新しい DHCP クライアントは、このアドレス範囲内で IP アドレスが付与されます。
Default Gateway	デフォルトゲートウェイのアドレスを指定します。 DMZ に参加する新しい DHCP クライアントには、デフォルトゲートウェイとしてこのアドレスが付与されます。
Domain Name	ドメイン名を入力します。
Lease Time	IP アドレスがクライアントにリースされる期間（単位：時間）を指定します。
Gateway	「DHCP Relay」選択時に表示されます。「DHCP Relay」のゲートウェイを指定します。
Primary DNS Server	DNS プロキシが有効化されている場合は、プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	DNS プロキシが有効化されている場合は、セカンダリ DNS サーバ IP アドレスを入力します。
WINS Server	DNS プロキシが有効化されている場合は、WINS サーバの IP アドレス を入力します。
Enable DNS Proxy	「ON」にして、DNS 及び（または）WINS サーバ IP アドレスを手動で設定します。 無効化した場合、本ルータの LAN IP アドレスがクライアントの DNS サーバとして割り当てられ、ルータは ISP から DNS 情報を取得します。

3. 「Save」をクリックし、設定を適用します。

DMZ DHCP Reserved IPs（DMZ DHCP の予約 IP 設定）

Network > Internet > DMZ DHCP Reserved IPs

DHCP サーバでは、ネットワーク上の DMZ クライアントに対し、クライアントの MAC アドレス及び割り当て IP アドレスを設定して予約 IP 設定を行うことができます。クライアントからのリクエストを受けたルータは、データベースの MAC アドレスリストとクライアントの MAC アドレスを確認します。データベース内でそのコンピュータまたはデバイスに IP アドレスがすでに割り当てられている場合は、カスタマイズされた IP アドレスが設定されます。それ以外の場合は、DMZ DHCP プールから自動的に IP アドレスがクライアントに割り当てられます

1. **Network > Internet > DMZ DHCP Reserved IPs** の順にメニューをクリックし、以下の画面を表示します。

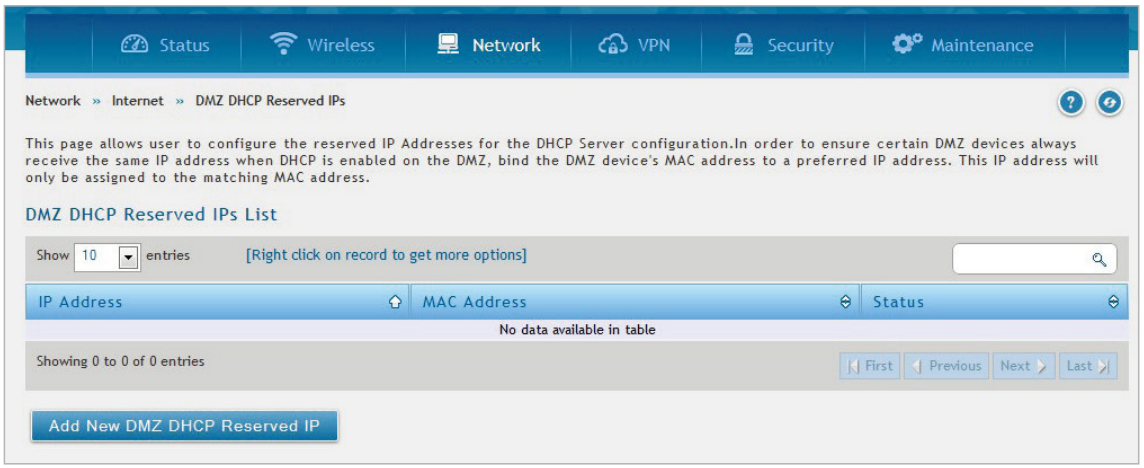

図 5-27　DMZ DHCP Reserved IPs 画面

2. 「Add New DMZ DHCP Reserved IP」をクリックして以下の画面を表示します。

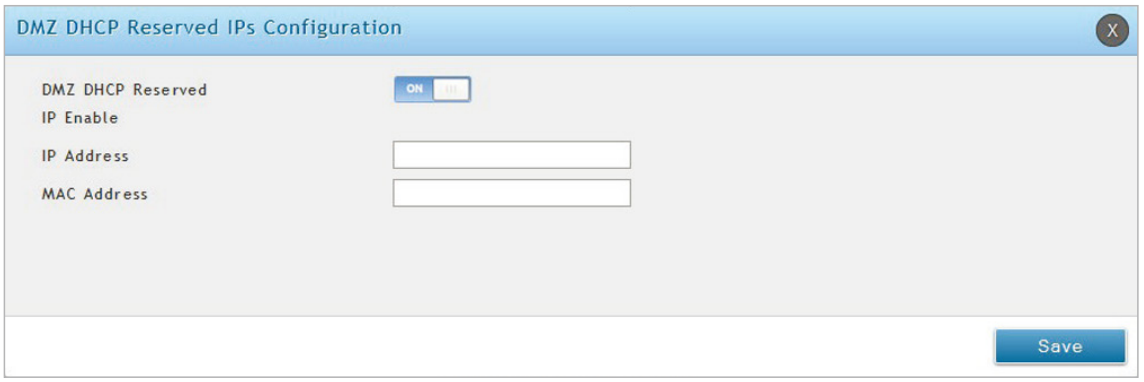

図 5-28　DMZ DHCP Reserved IP Configuration 画面

3. 以下の項目を設定します。

項目	説明
DMZ DHCP Reserved IP Enable	「ON」にして DMZ DHCP 予約 IP アドレスの登録を有効にします。
IP Address	デバイスにわりあてる IP アドレスを入力します。この IP アドレスは、DHCP 設定の開始 IP アドレス／終了 IP アドレスの範囲内で設定する必要があります。
MAC Address	デバイスの MAC アドレスを入力します。（xx:xx:xx:xx:xx:xx 形式）

4. 「Save」をクリックし、設定を適用します。

追加した予約 IP アドレスは、DMZ DHCP Reserved IPs 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Dynamic DNS（ダイナミック DNS 設定）

Network > Internet > Dynamic DNS

ダイナミック DNS の設定について説明します。

ダイナミック DNS（DDNS）は、動的なパブリック IP アドレスを持つルータが、インターネットのドメイン名を使用して接続することができるインターネットのサービスです。DDNS を使用するためには、DynDNS.org、DlinkDDNS.com または Oray.net などの DDNS プロバイダでアカウントをセットアップする必要があります。

必要に応じて、各 WAN に異なる DDNS サービスを設定できます。設定が完了すると、WAN IP アドレスにおける DDNS サービスの変更が更新されます。これにより、FQDN 経由でルータの WAN に接続する機能が正しい IP アドレスを向くように設定されます。DDNS サービス、ホスト、およびドメイン名でアカウントをセットアップする場合、ユーザ名、パスワード、およびワイルドカードのサポートがアカウントプロバイダによって提供されます。

1. **Network > Internet > Dynamic DNS** の順にメニューをクリックし、以下の画面を表示します。

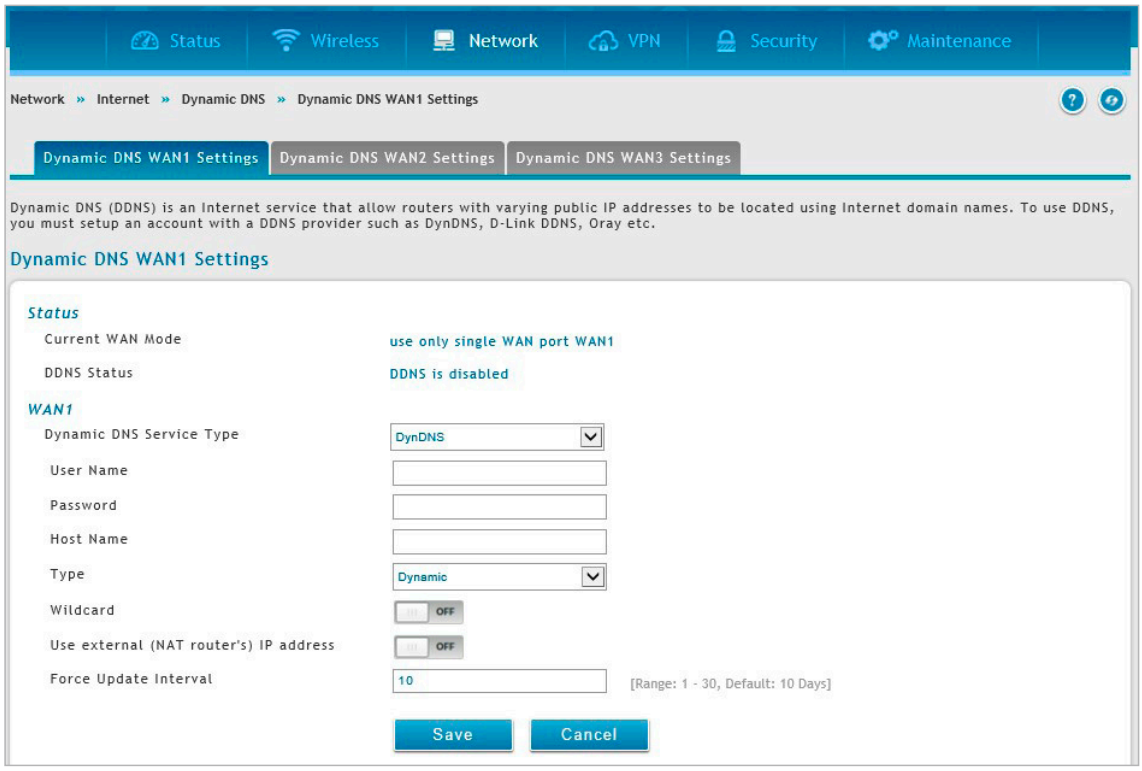

図 5-29　Dynamic DNS > Dynamic DNS WAN1 Settings タブ画面

2. DDNS を設定する WAN のタブを「Dynamic DNS WAN1 Settings」「Dynamic DNS WAN2 Settings」「Dynamic DNS WAN3 Settings」から選択します。
3. 「Dynamic DNS Service Type」から DDNS の種類を選択します。「Dynamic DNS Service Type」以下に表示される項目は、選択した DDNS により異なります。
4. 以下の項目を設定します。

項目	説明
Status	
Current WAN Mode	現在の WAN モードについて表示します。
DDNS Status	現在の接続状況を表示します。
WAN1	
Dynamic DNS Service Type	ダイナミック DNS サービスのタイプを以下から選択します。 「DynDNS」「D-Link DDNS」「FreeDNS」「NO-IP」「3322.org」「Custom」「Oray」
User Name	DDNS のユーザ名を入力します。
Password	DDNS のパスワードを入力します。
Host Name	DDNS のホスト名を入力します。
Type	ホストの種類を指定します。
Wildcards	ワイルドカードを許可します。
Use external (NAT router's) IP address	外部（NAT ルータ）の IP アドレスを指定します。
Force Update Interval	定期的な自動アップデート間隔（単位：日）を指定します。
URL	DDNS のカスタム URL を指定します。
Additional DDNS Options	追加の DDNS オプションを指定します。
Oray UserType	Oray のユーザ名が表示されます。
Oray Domain	Oray のドメインが表示されます。

5. 「Save」をクリックし、設定を適用します。

Traffic Management（トラフィック管理）

Network > Internet > Traffic Management
トラフィック管理の設定を行います。

Bandwidth Profiles（帯域幅プロファイル）

帯域幅プロファイルにより、LAN から WAN1 または WAN2 へのトラフィックフローを規制できます。本機能は、コスト節減または帯域幅優先度の割り当てを目的として、低優先度の LAN ユーザ（ゲストまたは HTTP サービスなど）が WAN の帯域幅を占有しないことを保証するために役に立ちます。

帯域幅プロファイル設定では、GUI による帯域幅制御機能の有効化と制御パラメータを定義するプロファイルの追加を行います。その後、プロファイルをトラフィックセレクタに関連付けることができます。これにより、セレクタと一致するトラフィックに対して帯域幅プロファイルが適用されます。「セレクタ」とは、定義済みの帯域規則をトリガする、IP アドレスやサービスといった要素を意味します。

1. **Network > Internet > Traffic Management > Bandwidth Profiles タブ**の順にメニューをクリックし、以下の画面を表示します。

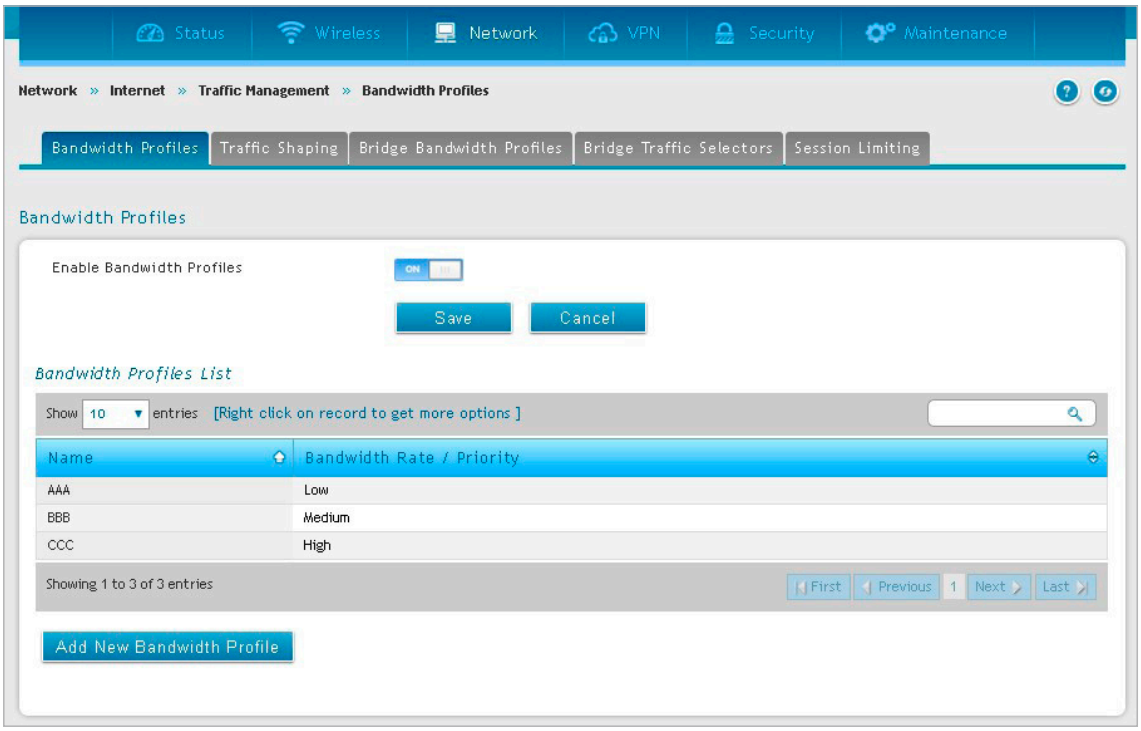

図 5-30　Bandwidth Profiles > Bandwidth Profiles タブ画面

2. 帯域幅プロファイルを有効にする場合は、「Enable Bandwidth Profiles」を「ON」にします。
3. 「Save」をクリックし、設定を適用します。

Add New Bandwidth Profile（新しい帯域幅プロファイルの作成）

1. 「Add New Bandwidth Profile」をクリックして以下の画面を表示します。

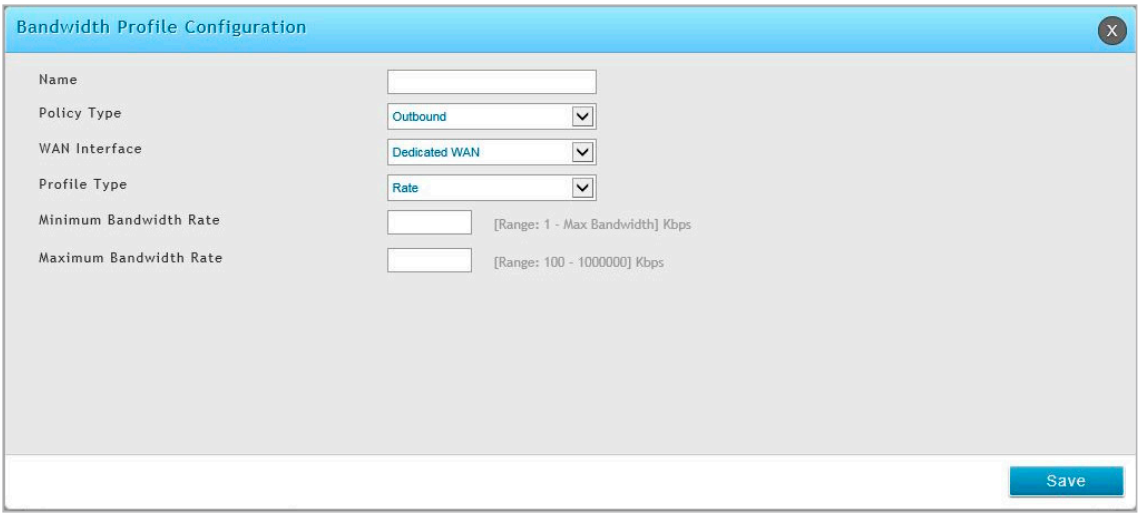

図 5-31　Bandwidth Profile Configuration 画面

2. 以下の項目を設定します。

項目	説明
Name	プロファイル名を入力します。 この識別子は、設定したプロファイルをトラフィックセレクタに関連付けるために使用されます。
Policy Type	「Outbound」（アウトバウンド）または「Inbound」（インバウンド）を選択します。
WAN Interface	「Policy Type」が「Outbound」の場合にプロファイルを関連付ける WAN インタフェースを選択します。
LAN Interface	「Policy Type」が「Inbound」の場合にプロファイルを関連付ける LAN インタフェースを選択します。
Profile Type	「Priority」（優先度）または「Rate」（レート）を選択します。
Priority	「Profile Type」で「Priority」（優先度）を選択した場合、「Low」（低）、「Medium」（中）、「High」（高）から選択します。
Minimum / Maximum Bandwidth Rate	「Profile Type」で「Rate」（レート）を選択した場合、このプロファイルが許可する最小および最大の帯域幅を指定します。

3. 「Save」をクリックし、設定を適用します。

追加した帯域幅プロファイルは、**Bandwidth Profiles > Bandwidth Profiles タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Traffic Shaping（トラフィックシェーピング）

作成したプロファイルは、LAN から WAN へのトラフィックフローに関連付けることができます。
トラフィックセレクタの設定により、帯域幅プロファイルに対して LAN トラフィックのタイプやソースの紐付けを行います。

1. **Network > Internet > Traffic Management > Traffic Shaping タブ**の順にメニューをクリックし、以下の画面を表示します。

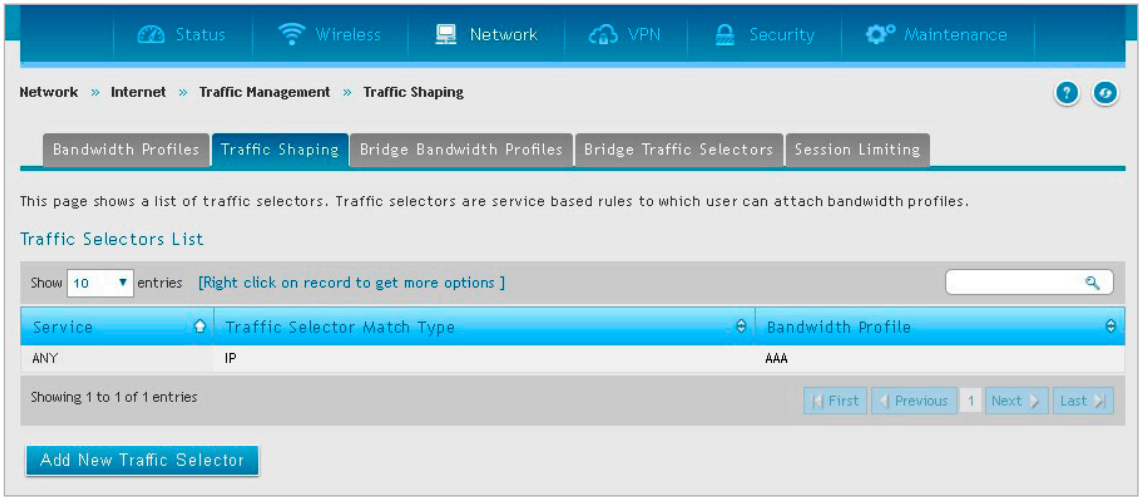

図 5-32　Traffic Management > Traffic Shaping タブ画面

Add New Traffic Selector（トラフィックセレクタの作成）

1. 「Add New Traffic Selector」をクリックし、以下の画面を表示します。

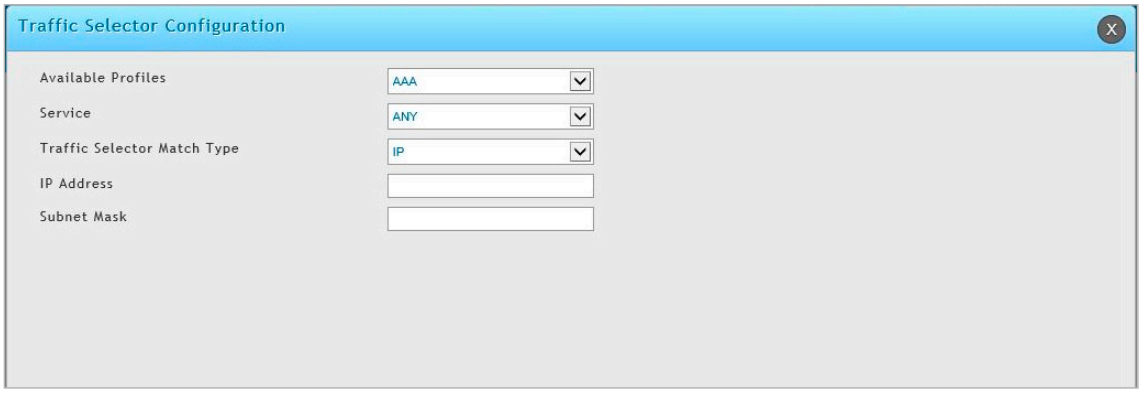

図 5-33　Traffic Selector Configuration 画面

2. 以下の項目を設定します。

項目	説明
Available Profiles	定義済みの帯域幅プロファイルを選択します。
Service	適用するサービスを選択します。
Traffic Selector Match Type	プロファイルを適用する場合にフィルタするパラメータ（IP、MAC Address、Port Name、VLAN）を定義します。
IP Address	「Traffic Selector Match Type」に「IP」を選択した場合、プロファイルに紐付けるソース IP アドレスを入力します。
Subnet Mask	「Traffic Selector Match Type」に「IP」を選択した場合、サブネットマスクを入力します。
MAC Address	「Traffic Selector Match Type」に「MAC Address」を選択した場合、プロファイルに紐付けるソース MAC アドレスを入力します。
Port Name	「Traffic Selector Match Type」に「Port Name」を選択した場合、プロファイルに紐付けるポートを選択します。
VLAN	「Traffic Selector Match Type」に「VLAN」を選択した場合、プロファイルに紐付ける VLAN を選択します。

3. 「Save」をクリックし、設定を適用します。

Bridge Bandwidth Profiles（ブリッジ帯域幅プロファイル）

本項目ではブリッジ帯域幅プロファイルの設定を行います。これらのプロファイルは「Bridge Traffic Selectors」の設定時に使用されます。
ブリッジトラフィックを制御することで、低優先値のユーザがブリッジ帯域幅を独占しないようにします。

注意　ブリッジ帯域幅プロファイル機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

1. **Network > Internet > Traffic Management > Bridge Bandwidth Profiles タブ**の順にメニューをクリックし、以下の画面を表示します。

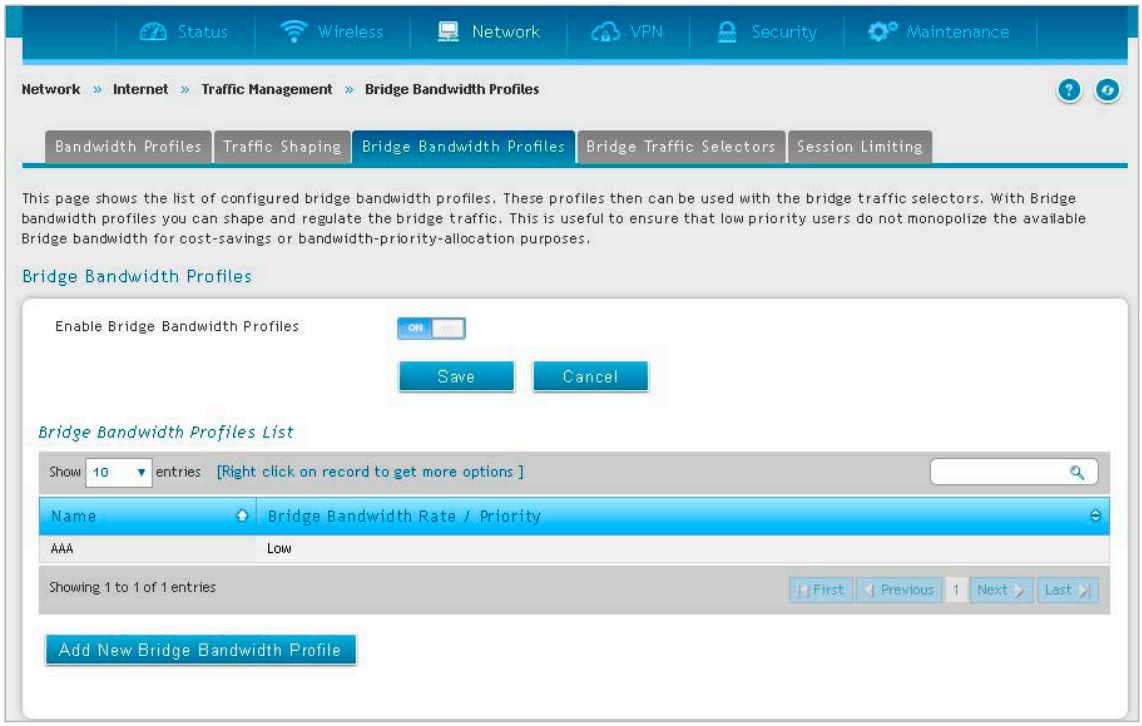

図 5-34　Traffic Management > Bridge Bandwidth Profiles タブ画面

2. 帯域幅プロファイルを有効にする場合は、「Enable Bandwidth Profiles」を「ON」にします。
3. 「Save」をクリックし、設定を適用します。

Add New Bridge Bandwidth Profile（ブリッジ帯域幅プロファイルの追加）

1. 「Add New Bridge Bandwidth Profile」をクリックし、以下の画面を表示します。

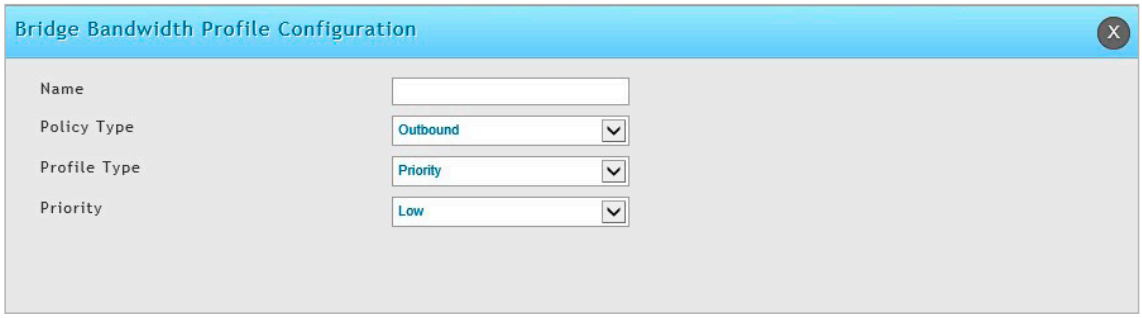

図 5-35　Bridge Bandwidth Profile Configuration 画面

2. 以下の項目を設定します。

項目	説明
Name	プロファイル名を入力します。
Policy Type	「Outbound」（アウトバウンド）または「Inbound」（インバウンド）を選択します。
Profile Type	「Priority」（優先度）または「Rate」（レート）を選択します。
Priority	「Profile Type」に「Priority」（優先度）を選択した場合、「Low」（低）、「Medium」（中）、「High」（高）から選択できます。
Minimum / Maximum Bandwidth Rate	「Profile Type」に「Rate」（レート）を選択した場合、このプロファイルが許可する最小および最大の帯域幅を指定します。

3. 「Save」をクリックし、設定を適用します。

Bridge Traffic Selectors（ブリッジトラフィックセレクタ）

作成したブリッジ帯域幅プロファイルは、「LANPort-1」から「DMZ」へのトラフィックフローと関連づけることができます。
トラフィックセレクタの設定により、帯域幅プロファイルに対してブリッジトラフィックのタイプやソースの紐付けを行います。

1. **Network > Internet > Traffic Management > Bridge Traffic Selectors タブ**の順にメニューをクリックし、以下の画面を表示します。

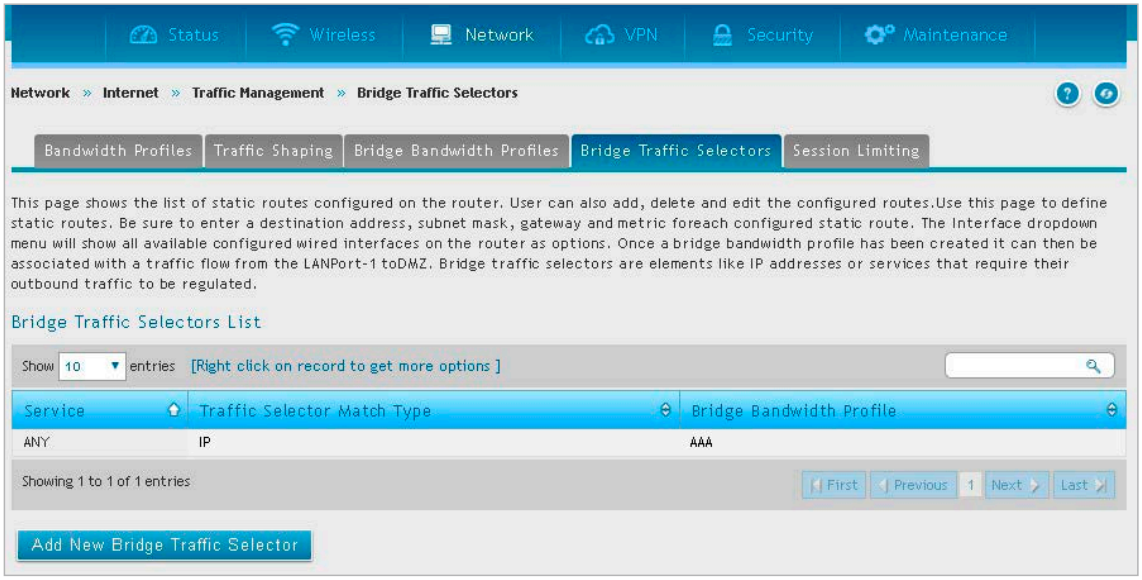

図 5-36　Traffic Management > Bridge Traffic Selectors タブ画面

Add New Bridge Traffic Selector（ブリッジトラフィックセレクタの作成）

1. 「Add New Bridge Traffic Selector」をクリックし、以下の画面を表示します。

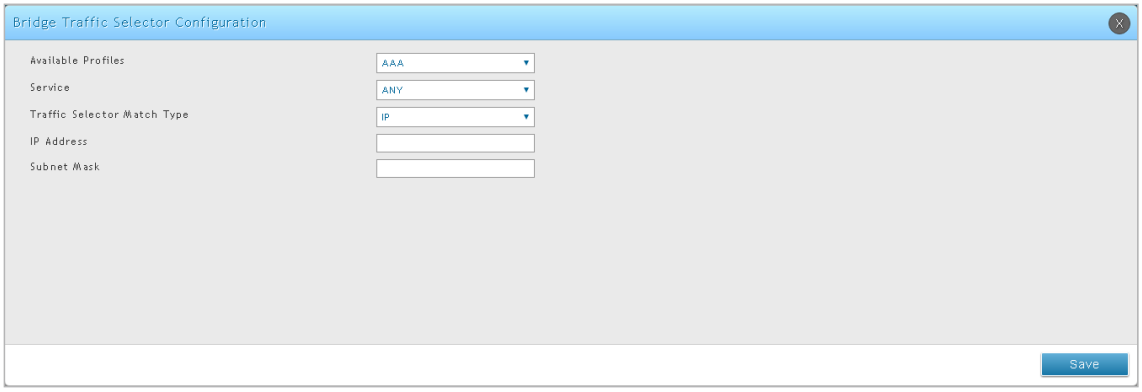

図 5-37　Bridge Traffic Selector Configuration 画面

2. トラフィックセレクタ設定は、以下の設定を使用して LAN トラフィックのタイプまたは送信元に帯域幅プロファイルを割り当てます。

項目	説明
Available profiles	定義済みの帯域幅プロファイルを選択します。
Service	適用するサービスを選択します。
Traffic Selector Match Type	帯域幅プロファイルを適用する場合にフィルタするパラメータ（「IP」または「MAC」）を定義します。LAN 上の指定マシンは、IP アドレスまたは MAC アドレス経由で識別されます。
IP Address	「Traffic Selector Match Type」に「IP」を選択した場合、プロファイルに紐付けるソース IP アドレスを入力します。
	「Traffic Selector Match Type」に「IP」を選択した場合、サブネットマスクを入力します。
MAC Address	「Traffic Selector Match Type」に「MAC Address」を選択した場合、プロファイルに紐付けるソース MAC アドレスを入力します。

3. 「Save」をクリックし、設定を適用します。

Session Limiting（セッション制限）

セッション制限画面では、設定したセッション制限プロファイルの一覧を表示します。セッションの制限は、IP アドレス、IP アドレス範囲、インタフェースごとに行うことができます。また、セッションが上限に達した際の警告メッセージも設定可能です。本設定にはプロファイル名、ソースタイプ、IP アドレス、最大セッション数などが含まれます。

1. **Network > Internet > Traffic Management > Session Limiting タブ**の順にメニューをクリックし、以下の画面を表示します。

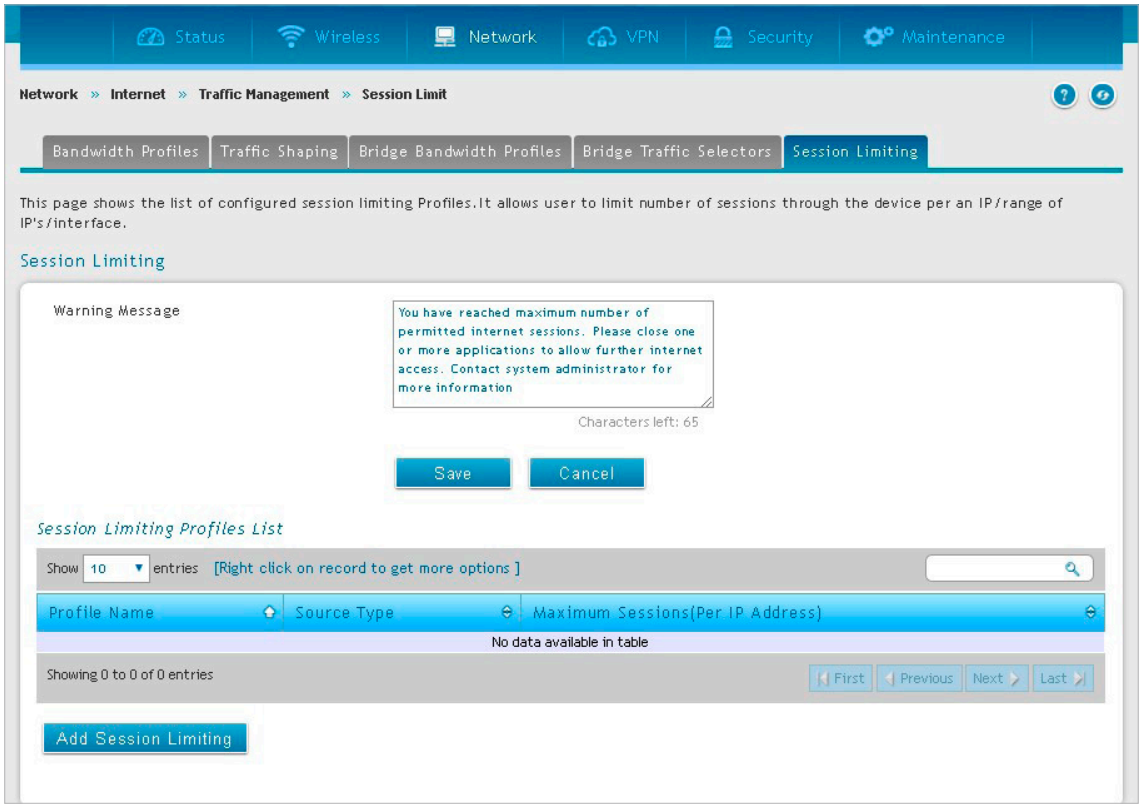

図 5-38　Traffic Management > Session Limiting タブ画面

Warning Message（警告メッセージ）の設定

1. 「Warning Message」を入力します。

図 5-39　Warning Message 画面

2. 「Save」をクリックし、設定を適用します。

Add Session Limiting（セッション制限の追加）

1. 「Add Session Limiting」をクリックし、以下の画面を表示します。

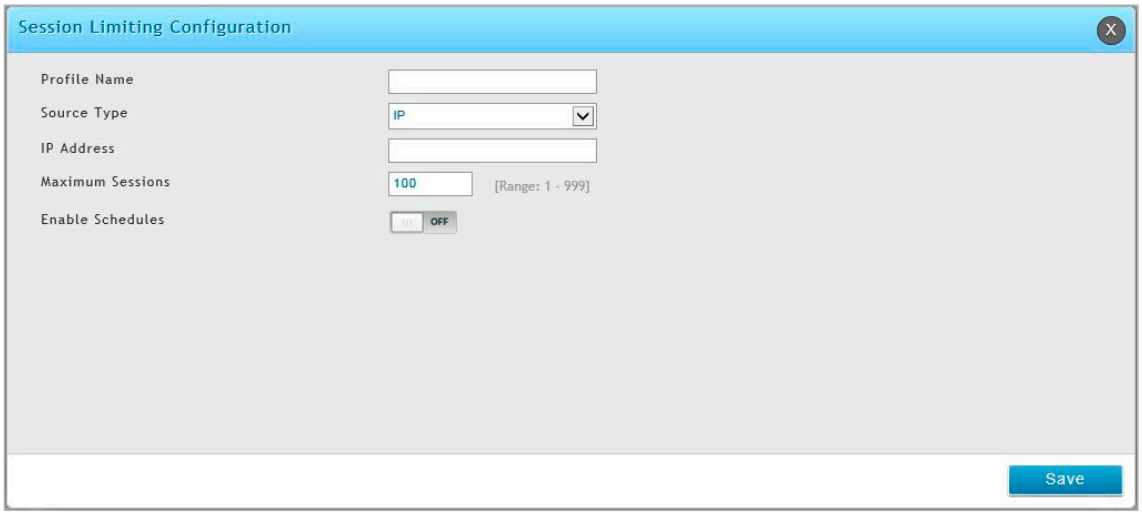

図 5-40　Session Limiting Configuration 画面

2. 以下の項目を設定します。

項目	説明
Profile Name	特定のソースタイプに適用するプロファイル名を入力します。
Source Type	プロファイルのソースタイプを「IP」「Range」「Interface」から指定します。
IP Address	「Source Type」に「IP」を選択した場合、セッション制限プロファイルで制御されるクライアント / ホストの IP アドレスを入力します。
Start IP Address	「Source Type」に「Range」を選択した場合、セッション制限プロファイルで制御されるクライアントの IP アドレス範囲の開始 IP アドレスを入力します。
End IP Address	「Source Type」に「Range」を選択した場合、セッション制限プロファイルで制御されるクライアントの IP アドレス範囲の終了 IP アドレスを入力します。
Interface	「Source Type」に「Interface」を選択した場合、セッション制限プロファイルで制御されるネットワークのインタフェースを選択します。
Maximum Sessions	「Souce Type」に対し許可される最大セッション数を指定します。セッション数の上限に達すると、セッション制限プロファイルにおけるいかなる種類のセッション / トラフィックも受け付けません。 • 設定可能範囲：1-999
Enable Schedules	スケジュールを有効化して、セッション制限プロファイルを特定の曜日や時間帯などに適用するように設定します。
Schedule Profile	セッション制限プロファイルに紐付けるスケジュールプロファイルを選択します。

3. 「Save」をクリックし、設定を適用します。

Jumbo Frames（ジャンボフレーム設定）

Network > Internet > Jumbo Frames

ジャンボフレームは 1500 バイト以上のペイロードを持つイーサネットフレームです。このオプションが有効な場合、LAN デバイスはジャンボフレームレートで情報を交換することができます。

注意　ジャンボフレームを使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

1. **Network > Internet > Jumbo Frames** の順にメニューをクリックし、以下の画面を表示します。

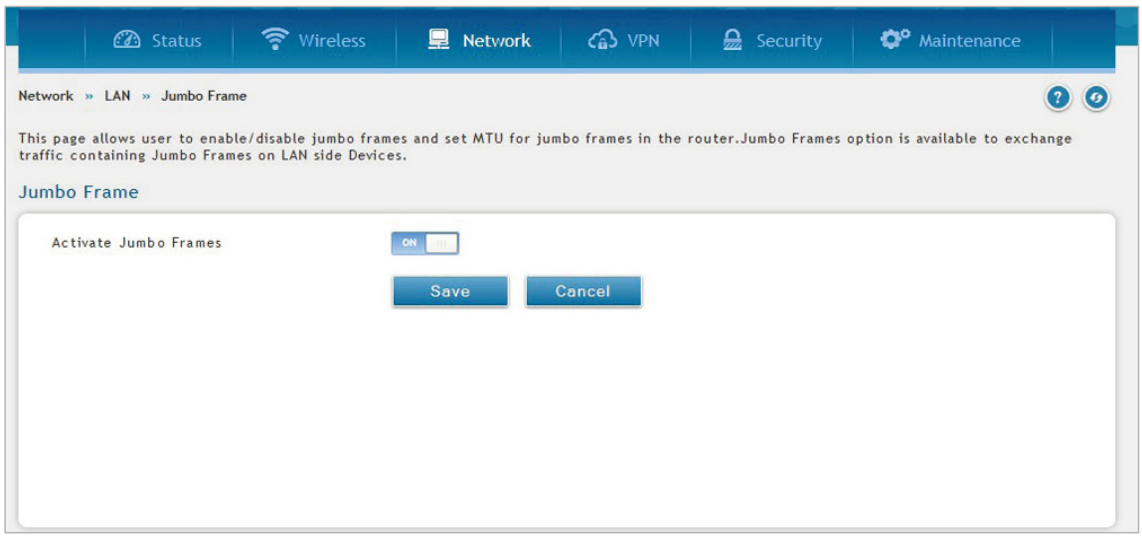

図 5-41　Jumbo Frame 画面

2. 以下の項目を設定します。

項目	説明
Activate Jumbo Frames	「ON」にしてジャンボフレームを有効にします。

3. 「Save」をクリックし、設定を適用します。

Routing（ルーティング設定）

Network > Routing
ルーティングの設定を行います。

Static Routes（スタティックルート）

Network > Routing > Static Routes
ここではルータに設定済みのスタティックルートのリストを表示します。さらに、設定済みのルートの追加、削除および編集ができます。
本ルータに手動でスタティックルートを追加することにより、異なるインタフェース間のトラフィック経路の選択を定義できます。本ルータと他のデバイス間で、経路の変更を説明するための通信はありません。ルートが設定されると、ネットワークの変更があるまでスタティックルートはアクティブで有効となります。

1. **Network > Routing > Static Routes** の順にメニューをクリックし、以下の画面を表示します。

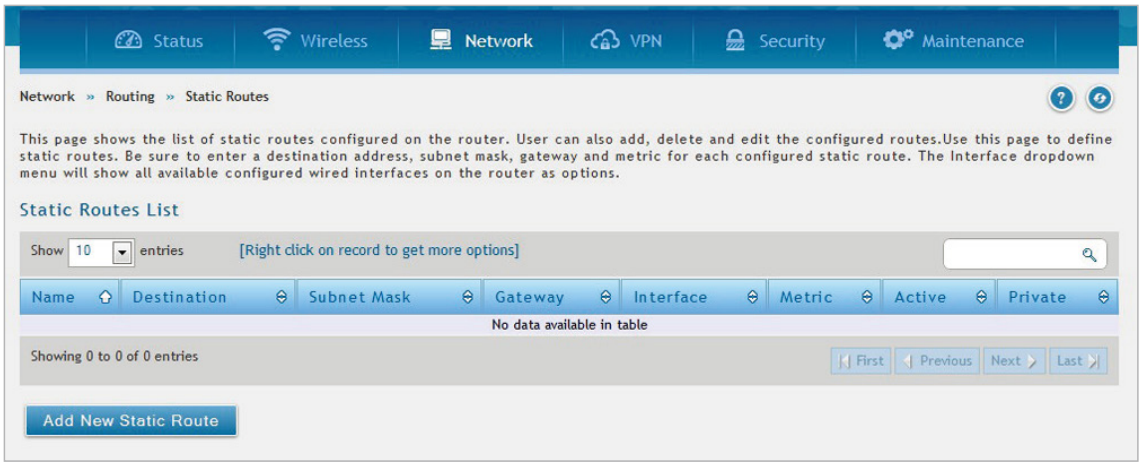

図 5-42　Static Routes 画面

Add New Static Route（スタティックルートの追加）

1. 「Add New Static Route」をクリックして以下の画面を表示します。

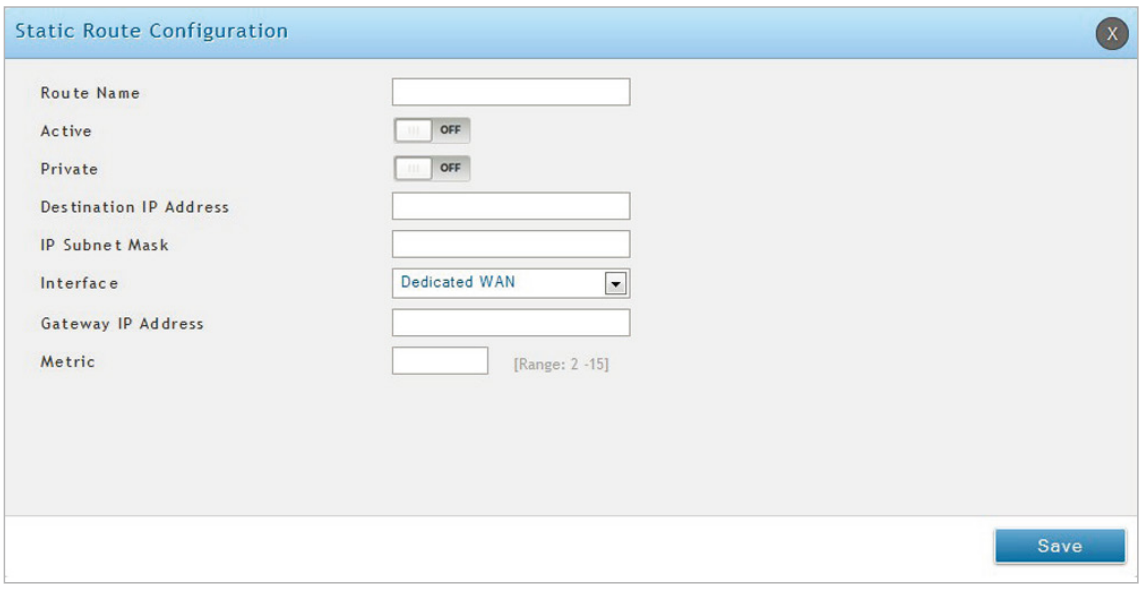

図 5-43　Static Route Configuration 画面

2. 以下の項目を設定します。

項目	説明
Route Name	ルート名を入力します。
Active	「ON」にしてルートを有効、または「OFF」にして無効にします。
Private	「ON」にしてルートを「プライベート」に設定します。「プライベート」に設定した場合、ルートは RIP ブロードキャストまたはマルチキャストで共有されません。
Destination IP Address	ルートの宛先 IP アドレスを指定します。
IP Subnet Mask	ルートのサブネットマスクを指定します。
Interface	物理ネットワークインタフェースを指定します。このインタフェースを介して本ルートがアクセス可能になります。
Gateway IP Address	ゲートウェイの IP アドレスを指定します。このゲートウェイを介して宛先ホストまたはネットワークに到達することができます。
Metric	ルートの優先度を決定します。同じ宛先に対して複数のルートが存在している場合、最も低いメトリックを持つルートが選択されます。

3. 「Save」をクリックし、設定を適用します。

RIP（RIP 設定）

Network > Routing > RIP

RIP（Routing Information Protocol）を使用したダイナミックルーティングは、LAN に一般的に使用される IGP（Interior Gateway Protocol）です。RIP を使用すると、LAN 内の他のルータとルーティング情報を交換できます。
また、動的なルーティングテーブルの更新を行い、トラフィックフローを中断せずに LAN 内の変更を適用することができます。

1. **Network > Routing > RIP** の順にメニューをクリックし、以下の画面を表示します。

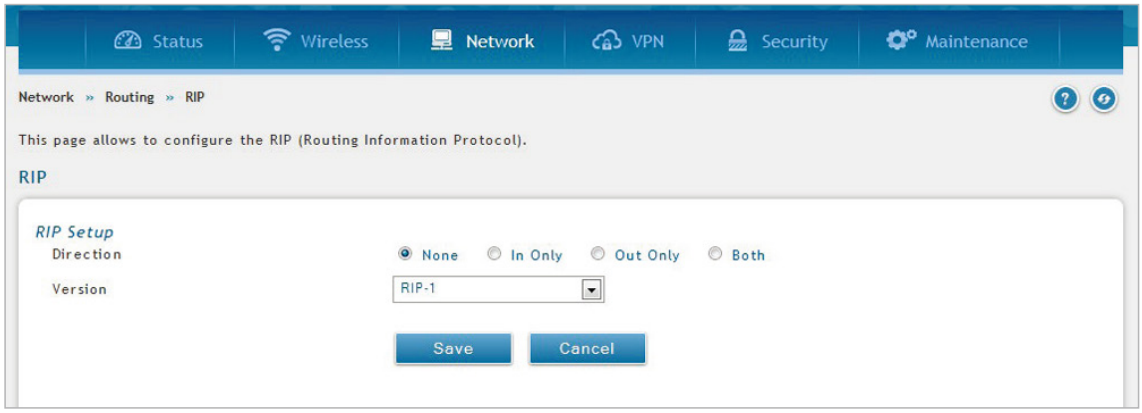

図 5-44　RIP 画面

2. 以下の項目を設定します。

項目	説明
Direction	ルータが RIP パケットを送受信する方法を定義します。 • 「Both」：ルータは自身のルーティングテーブルをブロードキャストし、また、他のルータから受信した RIP 情報を処理します。RIP 機能をフルに活用するためには、この設定をお勧めします。 • 「Out Only」：ルータは定期的にルーティングテーブルをブロードキャストしますが、他のルータから RIP 情報を受信しません。 • 「In Only」：ルータは他のルータから RIP 情報を受信しますが、ルーティングテーブルをブロードキャストしません。 • 「None」：ルータはルーティングテーブルのブロードキャスト、および他のルータからの RIP 情報の受信のいずれもしません。RIP は実質的に無効になります。
Version	RIP バージョンは LAN 内の他のルーティングデバイスの RIP サポートに依存します。 • 「Disabled」：RIP が無効化されている場合に設定します。 • 「RIP-1」：サブネット情報を含んでいないクラスベースのルーティングバージョンです。これは最も一般的にサポートされるバージョンです。 • 「RIP-2」：RIPv1 のすべての機能に加え、サブネット情報をサポートします。データは RIP-2B と RIP-2M の両方に RIP-2 形式で送信されますが、パケットが送信されるモードは異なります。 - RIP-2B - サブネット全体にデータをブロードキャストします。 - RIP-2M - マルチキャストアドレスにデータを送信します。 **3.** RIP-2B または RIP-2M を選択した場合、このルータと他のルータ（同じ RIP バージョンで設定済み）間には認証が必要となります。MD5 認証は第 1 / 第 2 キーの交換処理で使用されます。LAN 上で検出されたルータとのルーティング情報交換が確実に行われるように、認証キーの有効期間を設定できます。

4. 「Save」をクリックし、設定を適用します。

OSPF（OSPF 設定）

Network > Routing > OSPF

OSPF は、単一のルーティングドメインにインターネットプロトコル（IP）パケットを送る IGP（Interior Gateway Protocols）です 。利用可能なルータからリンク状態情報を収集して、ネットワークのトポロジマップを構成します。OSPFv2 は、RFC2328-OSPF バージョン 2 に記述されているルーティングプロトコルです。ISP バックボーンやエンタープライズネットワークなどの大規模ネットワークに広く使用されています。

1. **Network > Routing > OSPF** の順にメニューをクリックし、以下の画面を表示します。

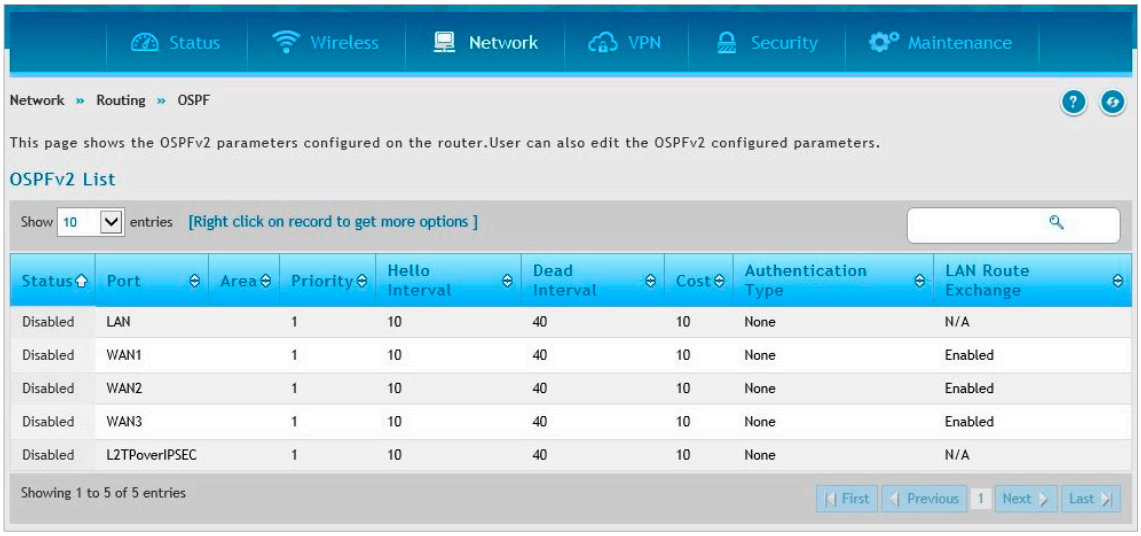

図 5-45　OSPFv2 Configuration 画面

2. 変更するインタフェース（LAN/WAN1/WAN2/WAN3/L2TPoverIPSEC）で右クリック　→　「Edit」を選択し、以下の画面を表示します。

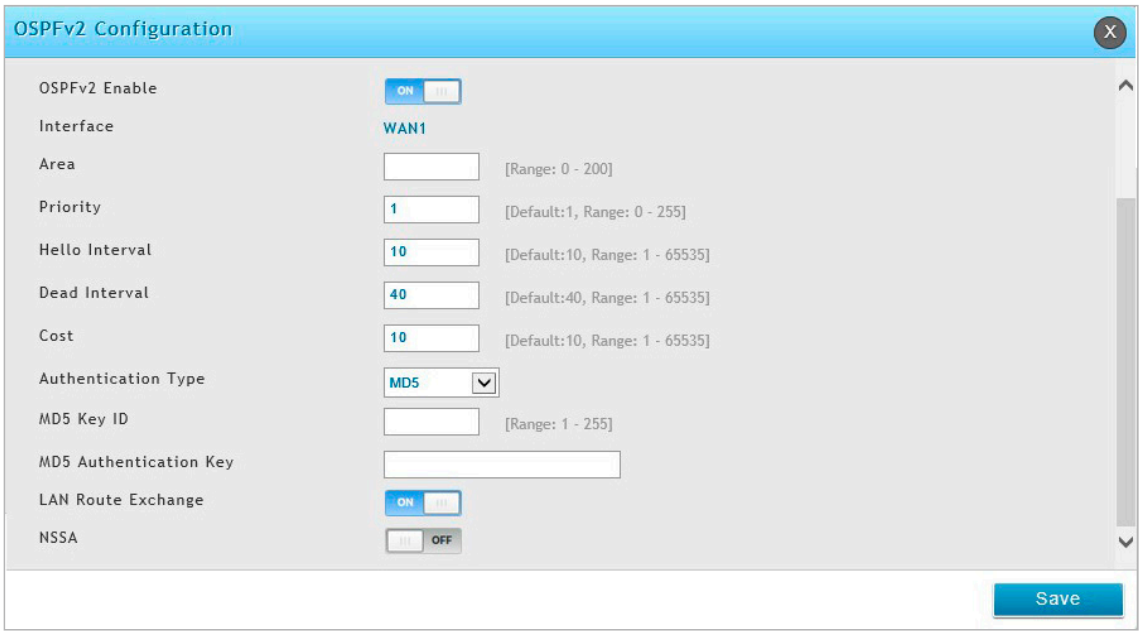

図 5-46　OSPFv2 Configuration 画面

3. 以下の項目を設定します。

項目	説明
OSPFv2 Enable	OSPF を有効にします。
Interface	OSPFv2 を有効 / 無効にする物理ネットワークインタフェースを表示します。
Area	インタフェースが所属するエリアを入力します。2 つのルータが共通のセグメントを持っている場合、インタフェースはセグメント同じエリアに属する必要があります。インタフェースは同じサブネットに属し、同一のサブネットマスクを持ちます。
Priority	ネットワークにおける OSPFv2 代表ルータの選出に使用されます。高い優先度を持つルータが、代表ルータとして、より適格であるとみなされます。値を 0 に設定すると、ルータは代表ルータとして不適格となります。低い番号ほど高い優先度を意味します。 • 初期値：1
Hello Interval	Hello インターバルタイマの値（秒）を入力します。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。 • 初期値：10（秒）
Dead Interval	デバイスの Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF ルータがダウンしていると判断するまでの時間（秒）を入力します。本値は共通ネットワークに接続する全ルータで同じである必要があります。OSPF では、2 つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません。 • 初期値：40（秒）
Cost	OSPFv2 インタフェースでパケットを送信するコストを入力します。
Authentication Type	OSPFv2 に使用する認証タイプを選択します。 •「None」：インタフェースは OSPF パケットを認証しません。 •「Simple」：インタフェースはシンプルテキストキーを使用して OSPF パケットを認証します。 •「MD5」：インタフェースは MD5 認証を使用して OSPF パケットを認証します。
Authentication Key	認証タイプに「Simple」を選択した場合、認証キーを入力します。
MD5 Key ID	認証タイプに「MD5」を選択した場合、MD5 キー ID を入力します。
MD5 Authentication Key	認証タイプに「MD5」を選択した場合、MD5 認証キーを入力します。
LAN Route Exchange	WAN/LAN インタフェース上で LAN/WAN 経路情報の交換を行います。
NSSA	NSSA を ON または OFF に設定します。

4. 「Save」をクリックし、設定を適用します。

L2TP over IPsec でサポートされる OSPF

LAN/WAN1/WAN2 の他に、L2TP over OSPF を使用してルートの変更を行うことができます。OSPF では L2TP over IPsec チャンネルで作成された仮想インタフェースがサポートされています。追加されたスタティックルートはそれらのインタフェースで交換される必要があります。

L2TP over IPsec では IPsec におけるデータリンク層をカプセル化します。プレーンな IPsec では単にネットワークレイヤの暗号化のみ行います。

L2TP over IPsec の設定が保存された後、トンネルイニシエーションが自動的に開始されますが、トンネルの確立はクライアント側とサーバ側の設定及びサーバの応答に依存します。OSPF を有効化する前に、IPsec 上の L2TP トンネルが確立されていることを確認してください。

Protocol Binding（プロトコルバインディング）

Network > Routing > Protocol Binding
IP/MAC バインドルールの表示とルールの設定を行います。

プロトコルバインディングは、ロードバランス機能を使用する場合に有益です。設定済みサービスまたはユーザ定義サービスのリストから選択して、利用可能な WAN ポートの 1 つだけを通過するように、トラフィックの種類を割り当てることができます。柔軟性を高めるため、送信元のネットワーク／端末と送信先のネットワーク／端末を指定できます。たとえば、ある LAN IP アドレスへの VoIP トラフィックを 1 つの WAN に割り当て、残りの IP アドレスからの VoIP トラフィックをもう 1 つの WAN リンクに割り当てることができます。

プロトコルバインディングは、ロードバランシングモードが有効で、複数の WAN が設定されている場合にのみ適用できます。

1. **Network > Routing > Protocol Binding** の順にメニューをクリックし、以下の画面を表示します。

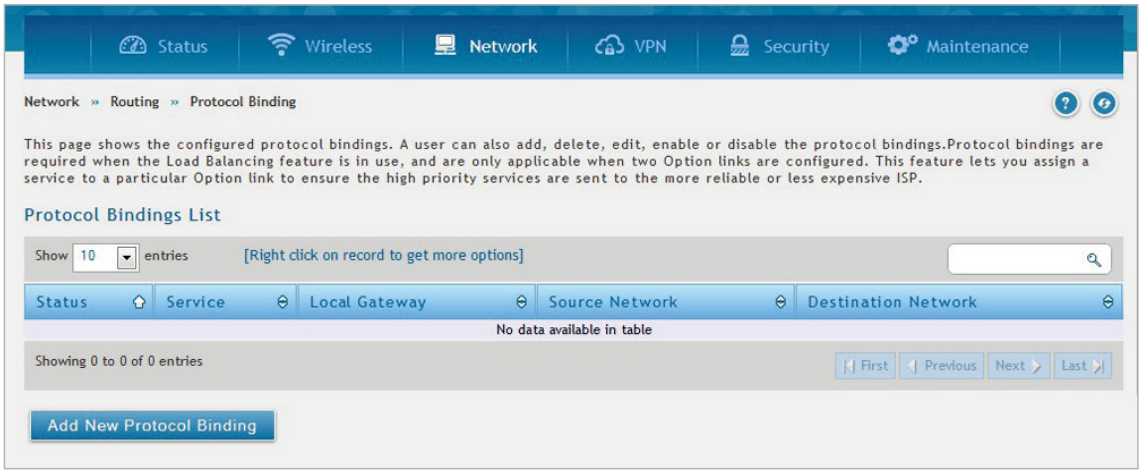

図 5-47　Protocol Binding 画面

2. プロトコルバインディングを追加する場合は、「Add New Protocol Binding」をクリックし以下の画面を表示します。

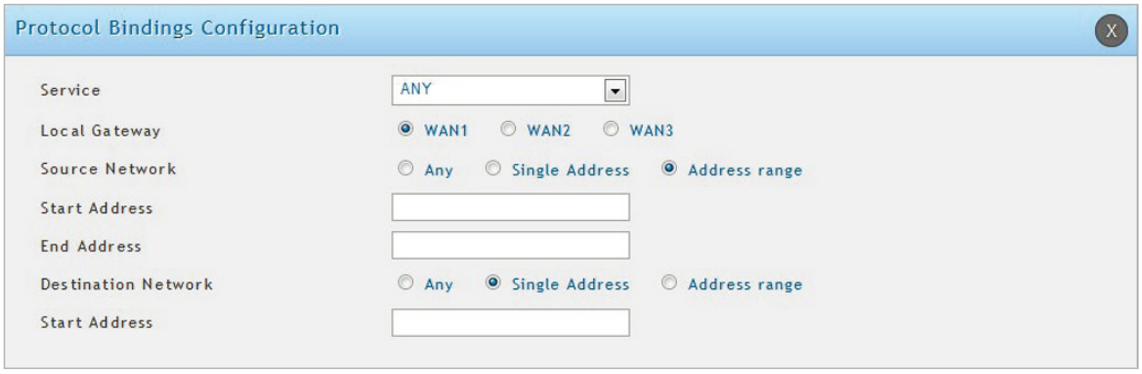

図 5-48　Protocol Bindings Configuration 画面

3. 以下の項目を設定します。

項目	説明
Service	プロトコルバインディングを設定するサービスを選択します。
Local Gateway	WAN インタフェースを選択します。
Source Network	送信元ネットワークとして以下のいずれかを選択します。 • 「Any」：ネットワークの指定は不要です。 • 「Single Address」：1 台のコンピュータを指定します。 • 「Address range」：IP アドレス範囲を指定します。
Destination Network	送信先ネットワークとして以下のいずれかを選択します。「Single Address」「Addres Range」を選択した場合は IP アドレス /IP アドレス範囲を指定します。 • 「Any」：ネットワークの指定は不要です。 • 「Single Address」：1 台のコンピュータに制限します。 • 「Address range」：IP アドレス範囲を指定します。

4. 「Save」をクリックし、設定を適用します。

追加したプロトコルバインディングは、Protocol Bindings 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

IPv6（IPv6 ネットワーク設定）

Network > IPv6
ここでは IPv6 の関連する LAN 設定を行います。

IP Mode（IP モード設定）

Network > IPv6 > IP Mode
本項目では使用する IP プロトコルのバージョンを設定します。お使いのネットワークで IPv6 を使用する場合、「IPv4 & IPv6」モードに指定する必要があります。このモードに設定すると、本ルータを通して IPv4 ノードと IPv6 デバイスの通信が可能になります。

1. **Network > IPv6 > IP Mode** の順にメニューをクリックし、以下の画面を表示します。

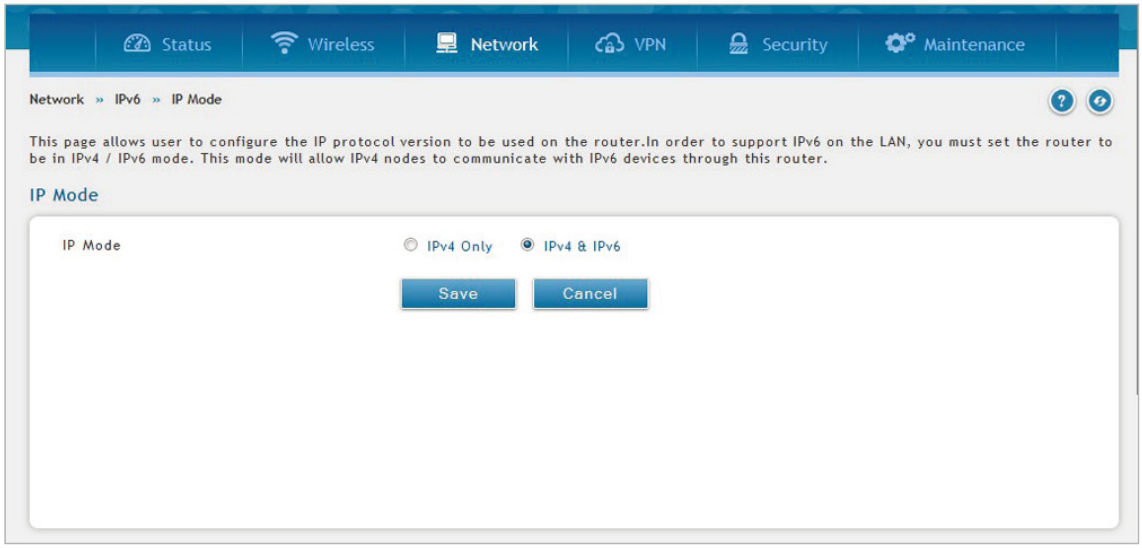

図 5-49　IP Mode 画面

2. 「IPv4」または「IPv4 & IPv6」をチェックします。
3. 「Save」をクリックし、設定を適用します。

注意 IP モードの設定変更を行うと本製品は再起動します。電源を切らずそのままお待ちください。IP モードの設定変更は、VLAN 設定画面（**Network > VLAN > VLAN Settings**）の設定項目に影響します。

IPv6 Wan1 Settings（IPv6 ネットワークにおける WAN1 設定）

Network > IPv6 > IPv6 Wan1 Settings

本ルータは、スタティック IPv6 アドレスを設定する、または DHCPv6 クライアントとして接続情報を受信することによって、IPv6 WAN に接続できます。インターネット接続用に ISP から固定のアドレスを付与されている場合、スタティック IP アドレスの設定を完了させる必要があります。ご使用のルータに割り当てられた IPv6 アドレスに加えて、ISP で定義された IPv6 プレフィックス長が必要となります。デフォルト IPv6 ゲートウェイアドレスは、このルータがインターネットにアクセスするために接続する ISP のサーバです。インターネットアドレスの解決のために ISP の IPv6 ネットワークにおけるプライマリおよびセカンダリ DNS サーバが使用され、これらはスタティック IP アドレスとプレフィックス長と共に ISP から提供されます。

DHCP を介した WAN IP 設定の取得が ISP から許可されている場合、ご使用の DHCPv6 クライアント構成の詳細を提供する必要があります。ゲートウェイ上の DHCPv6 クライアントはステートレスまたはステートフルとすることができます。ステートフルクライアントが選択されている場合、ゲートウェイはアドレスのリースのために ISP の DHCPv6 サーバに接続します。ステートレスの DHCP では、ISP 側の DHCPv6 サーバは不要であり、このゲートウェイから ICMPv6 検出メッセージが生成されて自動設定に使用されます。

また、優先される DHCPv6 サーバの IP アドレスとプレフィックス長を指定することも可能です。

1. **Network > IPv6 > IPv6 Wan1 Settings** の順にメニューをクリックします。「Connection Type」で選択する接続タイプにより表示される画面が異なります。

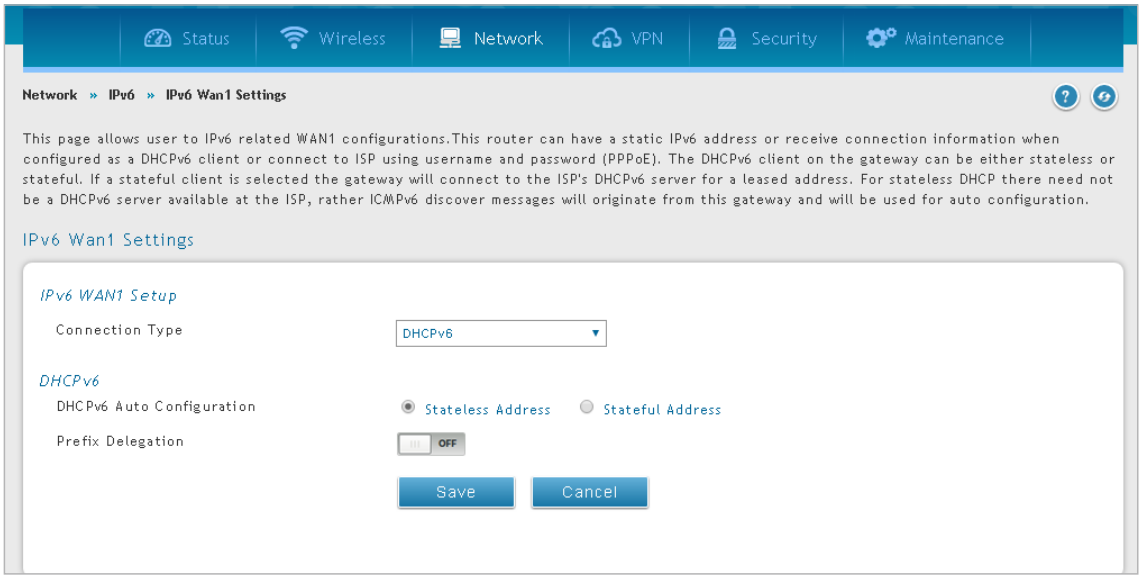

図 5-50　IPv6 Wan1 Settings（DHCPv6）画面

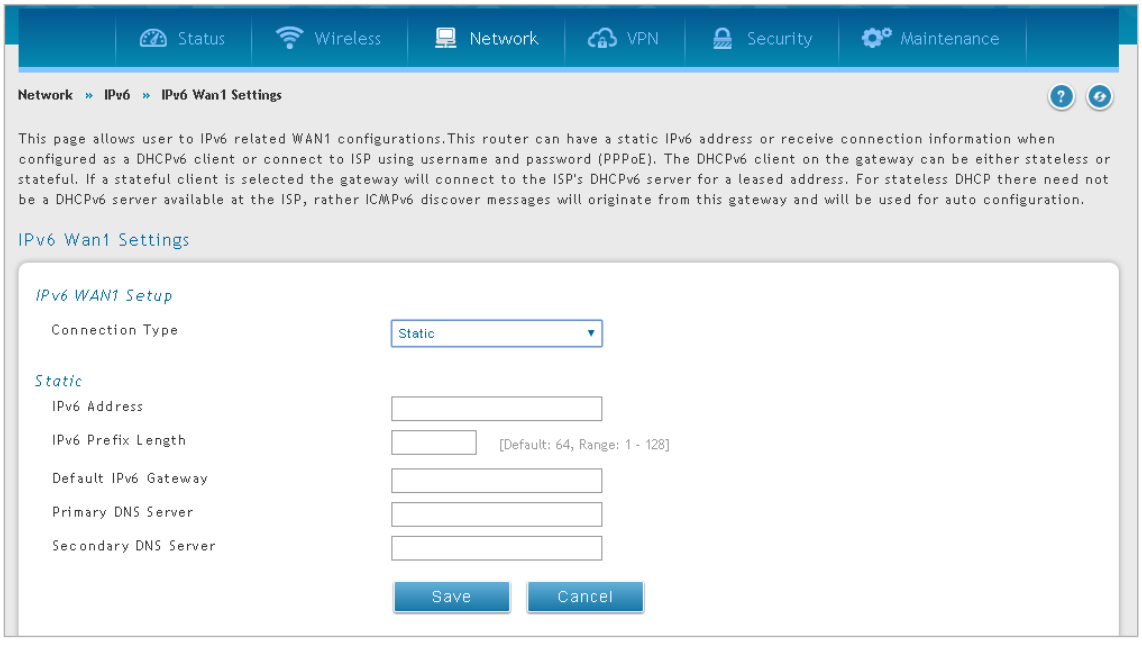

図 5-51　IPv6 Wan1 Settings（Static）画面

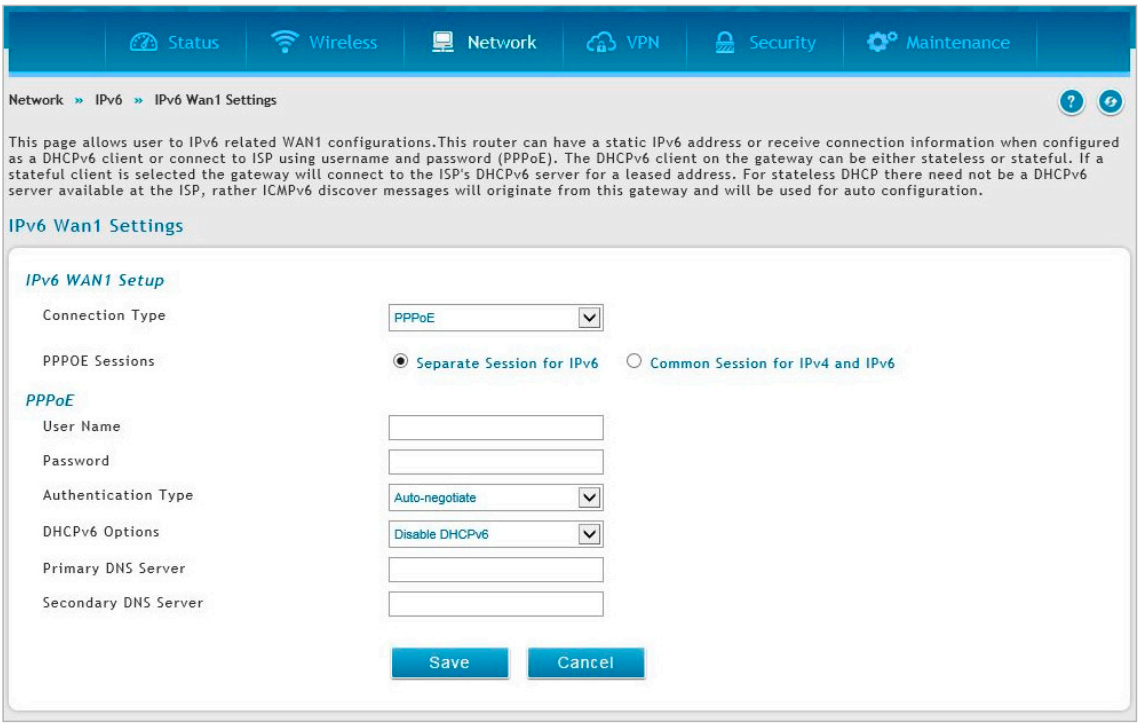

図 5-52　IPv6 Wan1 Settings（PPPoE）画面

2. 以下の項目を設定します。

項目	説明
IPv6 WAN 1 Setup	
Connection Type	接続タイプを以下から選択します。 • 「DHCPv6」 • 「Static」 • 「PPPoE」
DHCPv6	
DHCPv6 Auto Configuration	「Stateless Address 」または「Stateful Address」を選択します。
Prefix Delegation	ルーター広告プレフィックスを要求するには、このオプションを選択します。取得されたプレフィックスは、LAN 側で広告されたプレフィックスに更新されます。 このオプションは、DHCPv6 クライアントのステートレスアドレス自動設定モードでのみ選択できます。
Static	
IPv6 Address	ISP から提供された IP アドレスを指定します。
IPv6 Prefix Length	ISP から提供された IPv6 プレフィックス長を指定します。
Default IPv6 Gateway	ISP から提供された IPv6 ゲートウェイのアドレスを指定します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを指定します。
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを指定します。
PPPoE	
PPPoE Sessions	「Separate sessions for IPv6」または「Common sessions for IPv4 and IPv6」を選択します。 • 「Separate Session for IPv6」：IPv4/IPV6 の個別 PPPoE セッションを処理します。 • 「Common Session for IPV4 and IPv6」：IPv4/IPV6 の共有 PPPoE セッションを処理します。
User Name	PPPoE ユーザ名を入力します。
Password	PPPoE パスワードを入力します。
Authentication Type	プロファイルが使用する認証タイプを以下から選択します。 「Auto-negotiate」「PAP」「CHAP」「MS-CHAP」「MS-CHAPv2」
DHCPv6 Options	DHCPv6 クライアントが開始されるモードを以下から選択します。 「Disable DHCPv6」「Stateless DHCPv6」「Stateful DHCPv6」「Stateless dhcpv6 with Prefix delegation」 「Statelfull dhcpv6 with Prefix delegation」
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。

3. 「Save」をクリックし、設定を適用します。

IPv6 Wan2 Settings（IPv6 ネットワークにおける WAN2 設定）

Network > IPv6 > IPv6 Wan2 Settings

本項目では IPv6 に関する WAN2 設定を行うことができます。

注意 「IPv6 Wan2 Settings」の設定項目は、「IPv6 Wan1 Settings」と同等です。
設定項目については「WAN1 Settings（WAN1 設定）」を参照してください。

Static Routing（IPv6 スタティックルーティング設定）

Network > IPv6 > Static Routing

ルータに設定済みのスタティックルートのリストが表示されます。また、ルートの追加、削除および編集ができます。
このデバイスに手動でスタティックルートを追加すると、特定のインタフェースから別のインタフェースまでのトラフィック経路の選択を定義できます。本ルータと他のデバイス間で、経路の変更を構成するための通信はありません。一度設定されると、ネットワークの変更があるまでスタティックルートは有効となります。
スタティックルートの一覧には、管理者によって手動で追加されたすべてのルートが表示されます。

1. **Network > IPv6 > Static Routing** の順にメニューをクリックし、以下の画面を表示します。

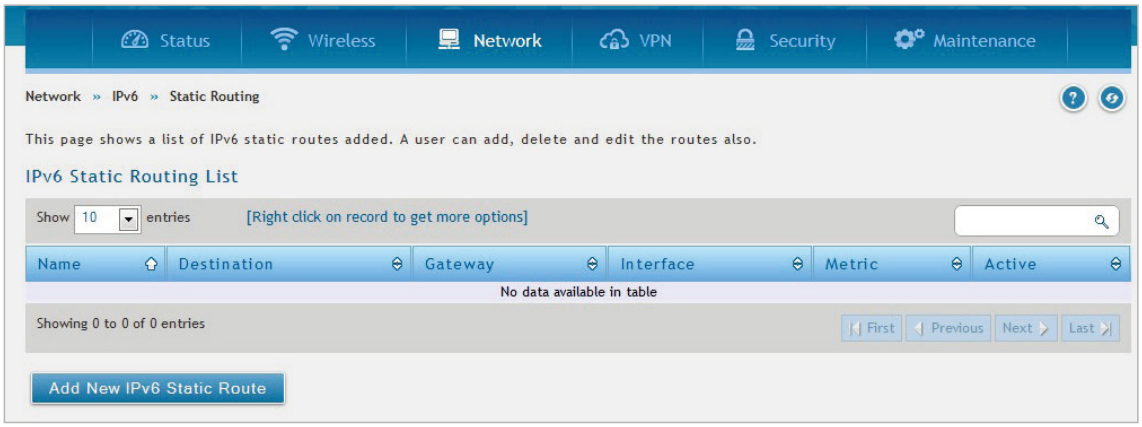

図 5-53　Static Routing 画面

2. IPv6 スタティックルートを追加する場合、「Add New IPv6 Static Route」をクリックし以下の画面を表示します。

図 5-54　IPv6 Static Routing Configuration 画面

3. 以下の項目を設定します。

項目	説明
Route Name	ルート名を入力します。
Active	「ON」：スタティックルートを有効にします。 「OFF」：スタティックルートを無効にします。
IPv6 Destination	スタティックルートの宛先 IPv6 アドレスを指定します。
IPv6 Prefix Length	スタティックルートの IPv6 のプレフィックス長を指定します。
Interface	本ルートがアクセス可能である物理的なネットワークインタフェース を以下から選択します。 「WAN1」「sit0 Tunnel-WAN1」「LAN」「WAN2」「sit0 Tunnel-WAN2」
IPv6 Gateway	宛先ホストまたはネットワークに到達できるゲートウェイの IPv6 アドレスを指定します。
Metric	ルートの優先度を決定します。同じ宛先に対して複数のルートが存在している場合、最も低いメトリックを持つルートが選択されます。

4. 「Save」をクリックし、設定を適用します。

追加したスタティックルートは、Static Routing 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

OSPFv3（OSPFv3 設定）

Network > IPv6 > OSPFv3

OSPF は、単一のルーティングドメインにインターネットプロトコル（IP）パケットを送る内部のゲートウェイプロトコルです。利用可能なルータからリンク状態情報を収集して、ネットワークのトポロジマップを構成します。

OSPFv3（Open Shortest Path First version 3）は IPv6 をサポートしています。ルータの OSPFv3 プロセスを有効にするためには、OSPFv3 プロセスをグローバルに有効とし、ルータ ID を OSPFv3 プロセスに割り当て、このプロセスを関連するインタフェースで有効にする必要があります。

1. **Network > IPv6 > OSPFv3** の順にメニューをクリックし、以下の画面を表示します。

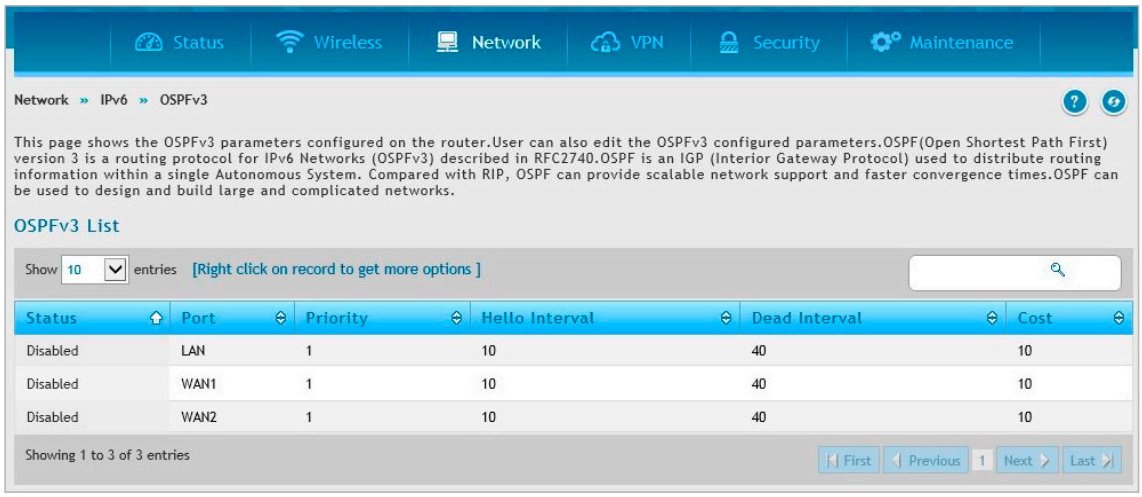

図 5-55　OSPFv3 画面

2. 変更するインタフェース（LAN/WAN1/WAN2）で右クリックし、「Edit」をクリックします。以下の画面が表示されます。

図 5-56　OSPFv3 Configuration 画面

3. 以下の項目を設定します。

項目	説明
OSPFv3 Enable	OSPFv3 を「ON」または「OFF」にします。
Interface	OSPFv3 を有効 / 無効にする物理ネットワークインタフェースが表示されます。
Priority	ネットワークの OSPFv3 代表ルータの決定に使用されます。高い優先度を持つルータが、より代表ルータとして適格であるとみなされます。値を 0 に設定すると、ルータは代表ルータとして不適格となります。低い番号ほど高い優先度を意味します。 • 初期値：1
Hello Interval	Hello インターバルタイマの値（秒）を入力します。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。 • 初期値：10（秒）
Dead Interval	デバイスの Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF ルータがダウンしていると判断するまでの時間（秒）を指定します。本値は共通ネットワークに接続する全ルータで同じである必要があります。OSPF では、2 つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません。 • 初期値：40（秒）
Cost	OSPFv3 インタフェースでパケットを送信するコストを指定します。

4. 「Save」をクリックし、設定を適用します。

6 to 4 Tunneling（6 to 4 トンネル設定）

Network > IPv6 > 6 to 4 Tunneling
6 to 4 トンネリング機能を有効または無効にします。

6 to 4 トンネリング機能は、IPv4 を IPv6 に移行するためのインターネット移行メカニズムです。IPv6 パケットの IPv4 ネットワークへの転送を可能にします。本画面では「Activate Auto Tunneling」を有効にし、IPv6 LAN からのトラフィックを IPv4 オプションでリモート IPv6 ネットワークに到達するように設定できます。

1. **Network > IPv6 > 6 to 4 Tunneling** の順にメニューをクリックし、以下の画面を表示します。

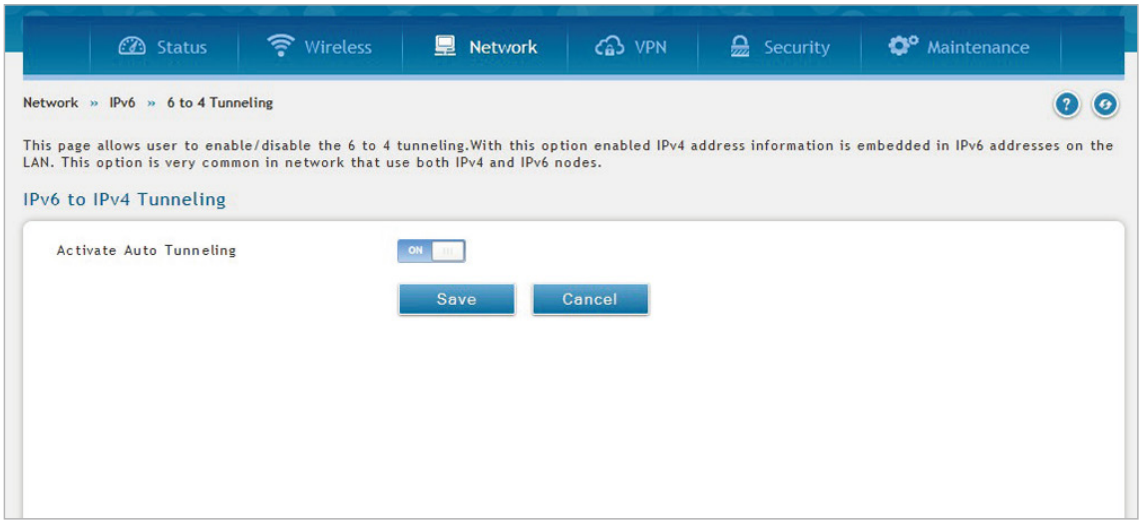

図 5-57　6 to 4 Tunneling 画面

2. 6 to 4 トンネルを有効にする場合は、「Activate Auto Tunneling」を「ON」にします。
3. 「Save」をクリックし、設定を適用します。

ISATAP Tunnels（ISATAP トンネル設定）

Network > IPv6 > ISATAP Tunnels

ISATAP（Intra-Site Automatic Tunnel Addressing Protocol）は、IPv4 ネットワーク上のデュアルスタックノード間で IPv6 パケットを送信する IPv6 移行メカニズムです。ISATAP はサイトの境界ルータ検出方法と同様に IPv6-IPv4 互換性アドレス形式を指定します。また、ISATAP は、特定のリンクレイヤ（IPv6 のリンクレイヤとして使用される IPv4）における IPv6 の操作を決定します。

利用可能な ISATAP トンネルのリストを表示します。また、ISATAP トンネルの追加、削除および編集ができます。

1. **Network > IPv6 > ISATAP Tunnels** の順にメニューをクリックし、以下の画面を表示します。

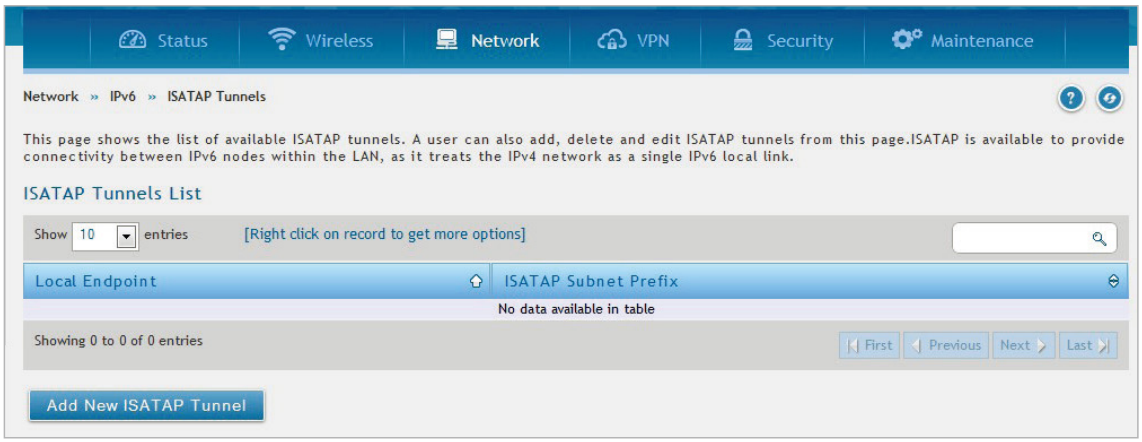

図 5-58　ISATAP Tunnels 画面

2. ISATAP トンネルを追加する場合は、「Add New ISATAP Tunnel」をクリックして以下の画面を表示します。

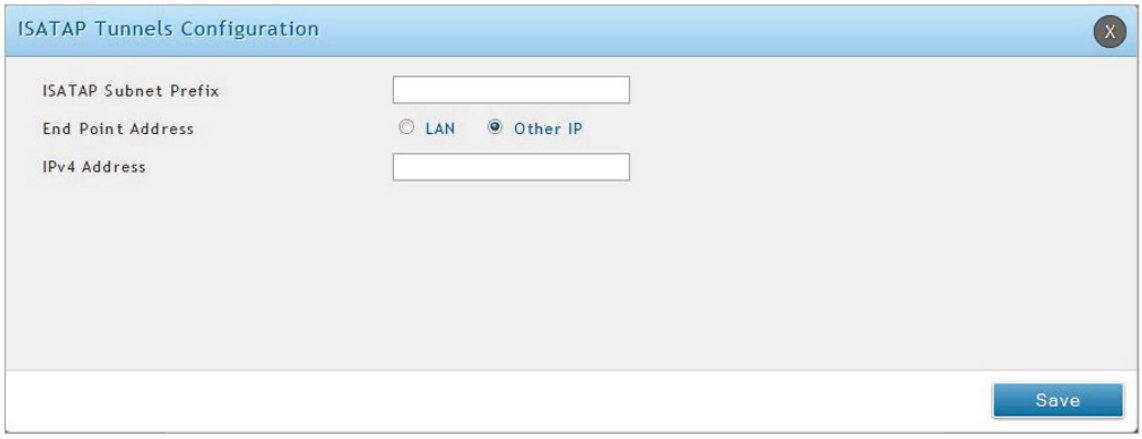

図 5-59　ISATAP Tunnels Configuration 画面

3. 以下の項目を設定します。

項目	説明
ISATAP Subnet Prefix	このイントラネット用に ISATAP 論理サブネットに割り当てられる 64 ビットのサブネットプレフィックスを指定します。ご契約の ISP またはインターネット登録から取得するか、または RFC 4193 を元に設定します。
End Point Address	このルータから開始するトンネルのエンドポイントアドレスを選択します。 ・「LAN」：エンドポイントは、LAN インタフェース です（LAN が IPv4 ネットワークであると想定）。 ・「Other IP」：特定の LAN IPv4 アドレスを指定します。
IPv4 Address	エンドポイントアドレスで「Other IP」を指定した場合、ローカルのエンドポイントアドレスを指定します。

4. 「Save」をクリックし、設定を適用します。

追加した ISATAP トンネルは ISATAP Tunnels 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Teredo Tunnel（Teredo トンネル設定）

Network > IPv6 > Teredo Tunnel
Teredo トンネルの設定をします。
「Teredo Tunnelling」を有効にすると、所属するネットワークにおいて IPv6 接続のない IPv6 が有効なホストに対して IPv6 接続を提供します。

1. **Network > IPv6 > Teredo Tunnel** の順にメニューをクリックし、以下の画面を表示します。

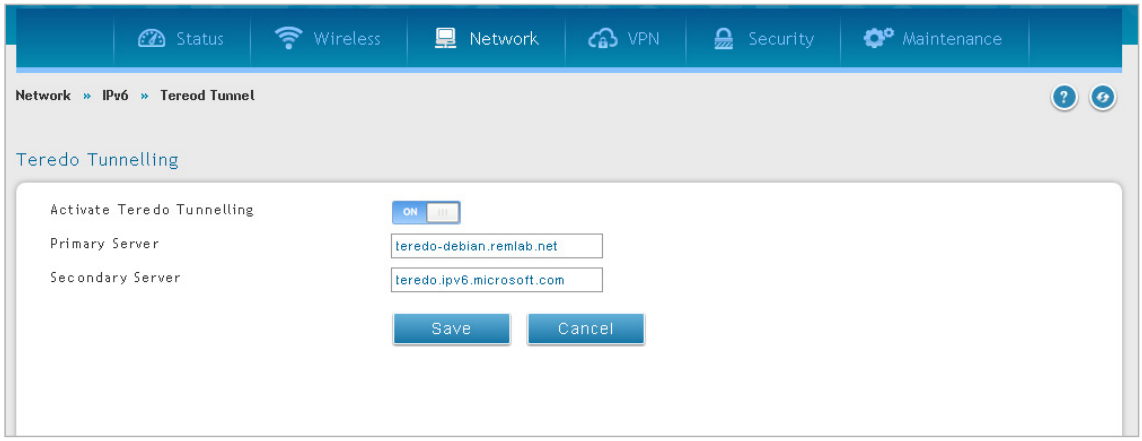

図 5-60　Teredo Tunnelling 画面

2. 「Activate Teredo Tunnelling」を「ON」に指定します。

3. 以下の項目を設定します。

項目	説明
Primary Server / Secondary Server	Teredo サーバのプライマリ / セカンダリサーバを指定します。

4. 「Save」をクリックし、設定を適用します。

IPv6 LAN Settings（IPv6 LAN 設定）

Network > IPv6 > IPv6 LAN Settings

本項目では IPv6 に関する LAN 設定を行います。

IPv6 LAN Settings（IPv6 LAN 設定）

IPv6 モードでは、（IPv4 モードと同様に）LAN DHCP サーバは初期値で無効です。本機能を有効にすると、DHCPv6 サーバによって、LAN に割り当てられたプレフィックス長とともに設定済みアドレスプールから IPv6 アドレスが提供されます。

ルータの IPv6 LAN アドレスの初期値は「fec0::1」です。ご使用のネットワークの要件に基づいてこの 128 ビットの IPv6 アドレスを変更できます。ルータの LAN 設定を定義するために必要なフィールドにはプレフィックス長があります。IPv6 ネットワーク（サブネット）はプレフィックスと呼ばれるアドレスの開始ビットにより特定されます。初期値では、これは 64 ビットの長さです。ネットワーク内のすべてのホストは、IPv6 アドレスに共通の開始ビットがあります。ネットワークアドレスに共通な開始ビット番号はプレフィックス長フィールドによって設定されます。

1. **Network > IPv6 > IPv6 LAN Settings > IPv6 LAN Settings タブ**の順にメニューをクリックし、以下の画面を表示します。

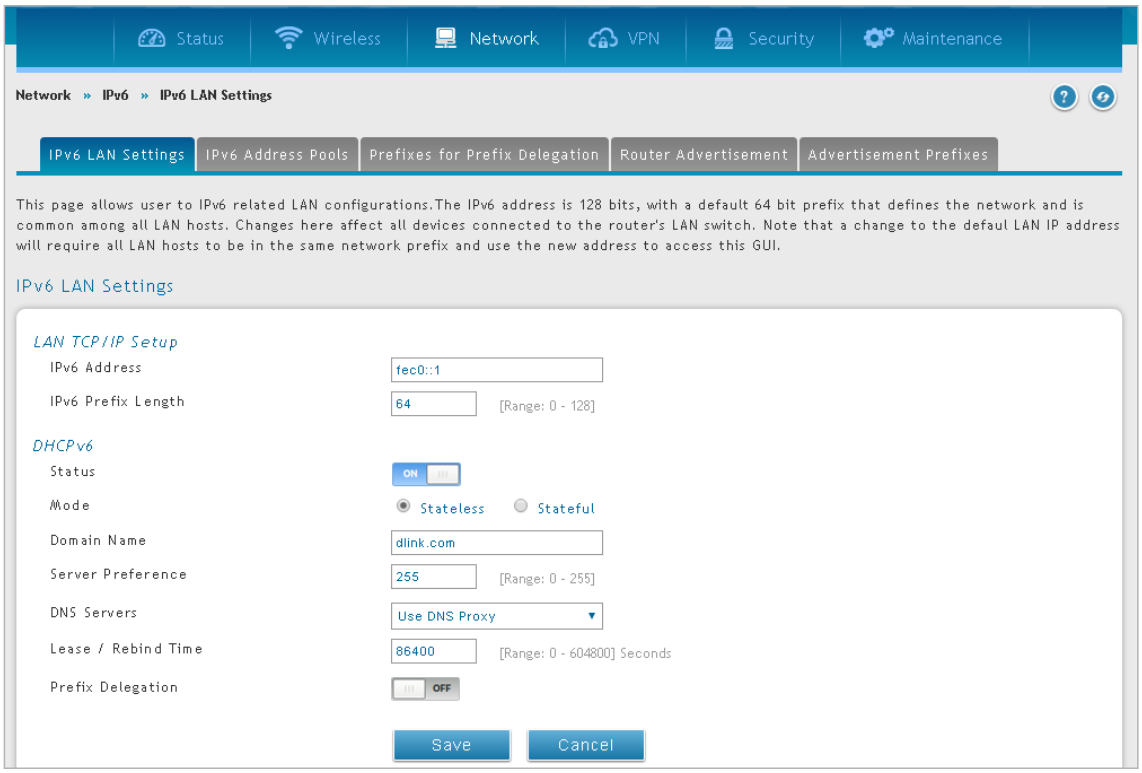

図 5-61　IPv6 LAN Settings > IPv6 LAN Settings タブ画面

2. 以下の項目を設定します。

項目	説明
LAN TCP/IP Setup	
IPv6 Address	ルータの IPv6 アドレスを入力します。
IPv6 Prefix Length	IPv6 プリフィクス長を入力します。
DHCPv6	
Status	DHCPv6 機能を有効にします。有効にすると以下の項目が指定できます。
Mode	IPv6 DHCP サーバに「Stateless」または「Stateful」を指定します。 • 「Stateless」：IPv6 LAN ホストが本ルータによって自動設定されるため、外部の IPv6 DHCP サーバを必要としません。この場合、ルータ通知デーモン（RADVD）をこのデバイスに設定する必要があります。また、ホストは自動設定のために ICMPv6 ルータディスカバリメッセージを使用します。LAN ノードに供給する管理アドレスはありません。 • 「Stateful」：IPv6 LAN ホストは、必要な構成設定を提供するために外部の DHCPv6 サーバに依存します。
Domain Name	DHCPv6 サーバのドメイン名を設定します。（オプション）
Server Preference	サーバ優先度は、この DHCP サーバの優先度レベルを示すために使用されます。LAN ホストに対して最も高いサーバ優先度値を持つ DHCP サーバ通知メッセージは、他の DHCP サーバの通知メッセージより優先されます。 • 初期値：255
DNS Servers	• 「Use Below」：DNS サーバの詳細を手動で設定します。（Primary/Secondary DNS Server オプション） • 「Use DNS from ISP」：LAN DHCP クライアントは、ISP から直接 DNS サーバの詳細を受信します。 • 「Use DNS Proxy」：ルータは、すべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します。（WAN 設定パラメータ）
Lease/Rebind Time	LAN クライアントに対する本ルータからの DHCPv6 リースの期間（秒）を設定します。
Prefix Delegation	DHCPv6 サーバでプレフィックス 委任を有効にします。 本項目は、DHCPv6 の「Mode」を「Stateless」に設定した場合のみ表示されます。

3. 「Save」をクリックし、設定を適用します。

IPv6 Address Pools（IPv6 アドレスプール）

この機能により、ゲートウェイの DHCPv6 サーバが供給する IP アドレスの範囲に IPv6 委任プレフィックスを定義できます。委任プレフィックスを使用すると、LAN 内の他のネットワーク装置に対して、割り当てられたプレフィックス固有の DHCP 情報を通知する処理を自動化できます。

1. **Network > IPv6 > IPv6 LAN Settings > IPv6 Address Pools タブ**の順にメニューをクリックし、以下の画面を表示します。

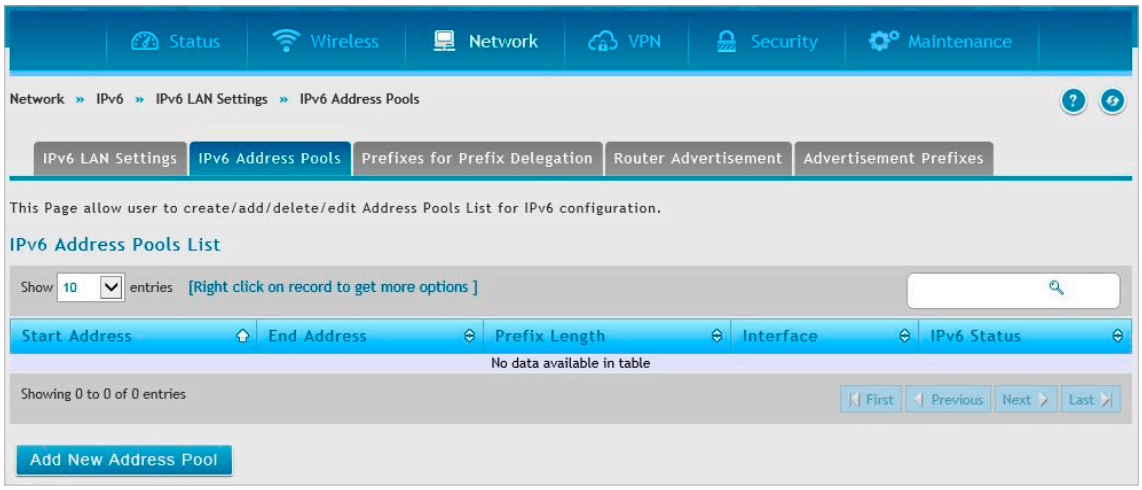

図 5-62　IPv6 LAN Settings > IPv6 Address Pools タブ画面

2. アドレスプールを追加する場合は、「Add New Address Pool」をクリックし以下の画面を表示します。

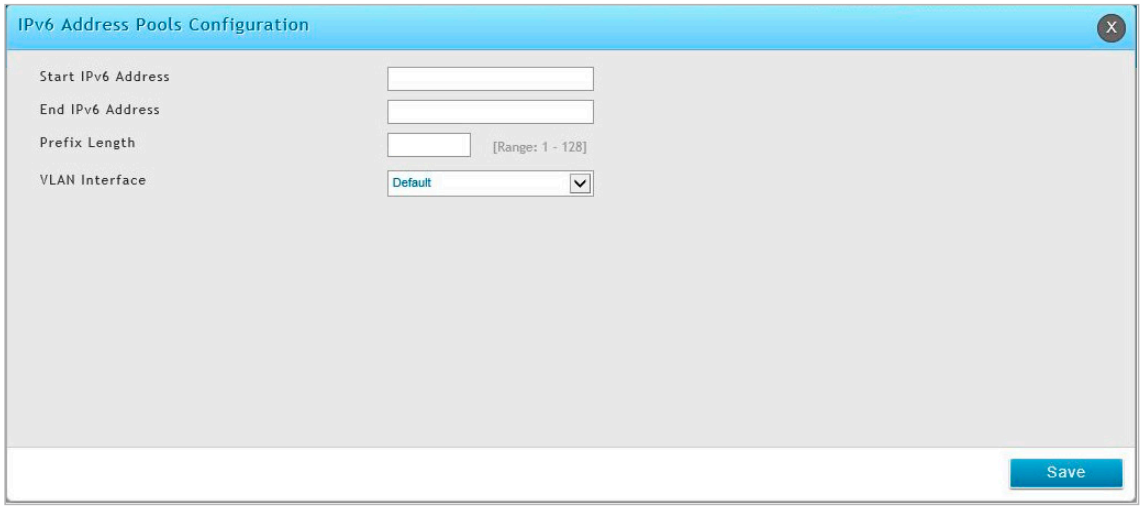

図 5-63　IPv6 Address Pools Configuration 画面

3. 以下の項目を設定します。

項目	説明
Start IPv6 Address	開始 IPv6 LAN アドレスを入力します。
End IPv6 Address	終了 IPv6 LAN アドレスを入力します。
Prefix Length	プレフィックス長を入力します。
VLAN Interface	VLAN インタフェースを指定します。

4. 「Save」をクリックし、設定を適用します。

追加した IPv6 プールは、**IPv6 LAN Settings > IPv6 Address Pools タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Prefixes for Prefix Delegation（IPv6 プレフィックス委任）

IPv6 プレフィックス長の追加 / 編集 / 削除を行います。

1. **Network > IPv6 > LAN Settings > Prefixes for Prefix Delegation タブ**の順にメニューをクリックし、以下の画面を表示します。

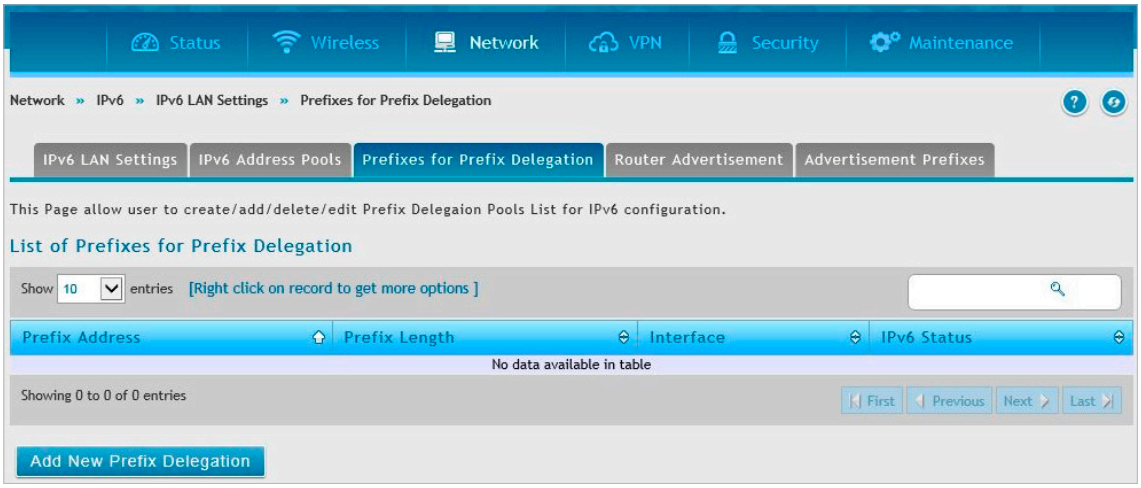

図 5-64　IPv6 LAN Settings>Prefixes for Prefix Delegation タブ 画面

2. プレフィックスを追加する場合は、「Add New Prefix Delegation」をクリックし以下の画面を表示します。

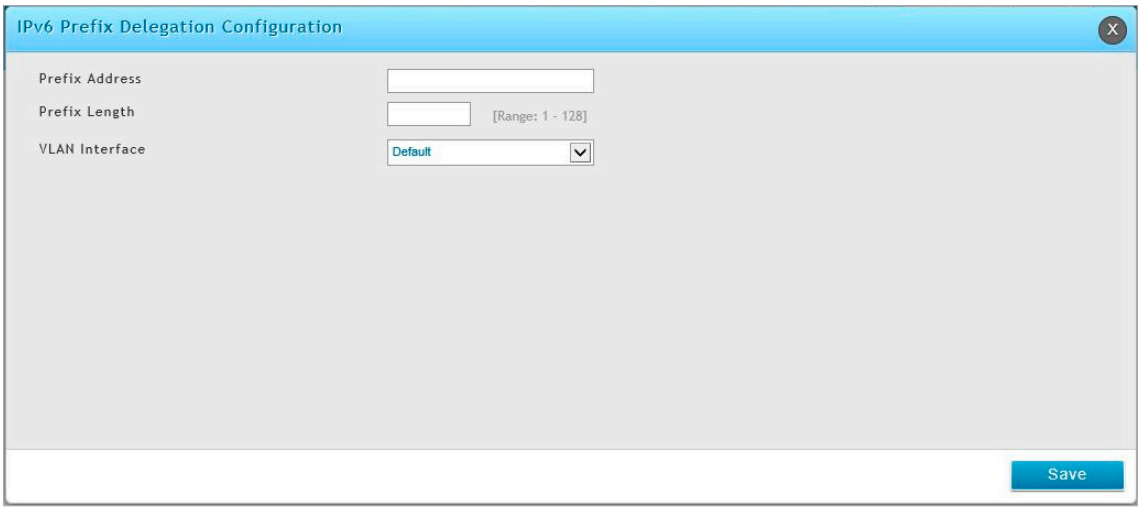

図 5-65　IPv6 Prefix Delegation Configuration 画面

3. 以下の項目を設定します。

項目	説明
Prefix Address	プレフィックスアドレスを入力します。
Prefix Length	プレフィックス長を入力します。
VLAN Interface	VLAN インタフェースを指定します。

4. 「Save」をクリックし、設定を適用します。

追加したプレフィックスは、**IPv6 LAN Settings > Prefixes for Prefix Delegation タブ** 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Router Advertisement（IPv6 ルータ通知）

RA（ルータ通知）は LAN クライアントに対する IPv4 DHCP 割り当てと類似する機能です。IP アドレスやサポートするネットワーク情報といった情報を受け付けるように設定されたデバイスに対してそれらの情報を通知します。
ルータ通知は、IPv6 LAN のステートレスな自動設定のために IPv6 ネットワークで必要とされます。ルータ通知デーモンを設定することにより、本製品は、LAN 上の RS を受信すると LAN 上のホストに対するレスポンスとしてルータ通知を送信します。

1. **Network > IPv6 > IPv6 LAN Settings > Router Advertisement タブ**の順にメニューをクリックし、以下の画面を表示します。

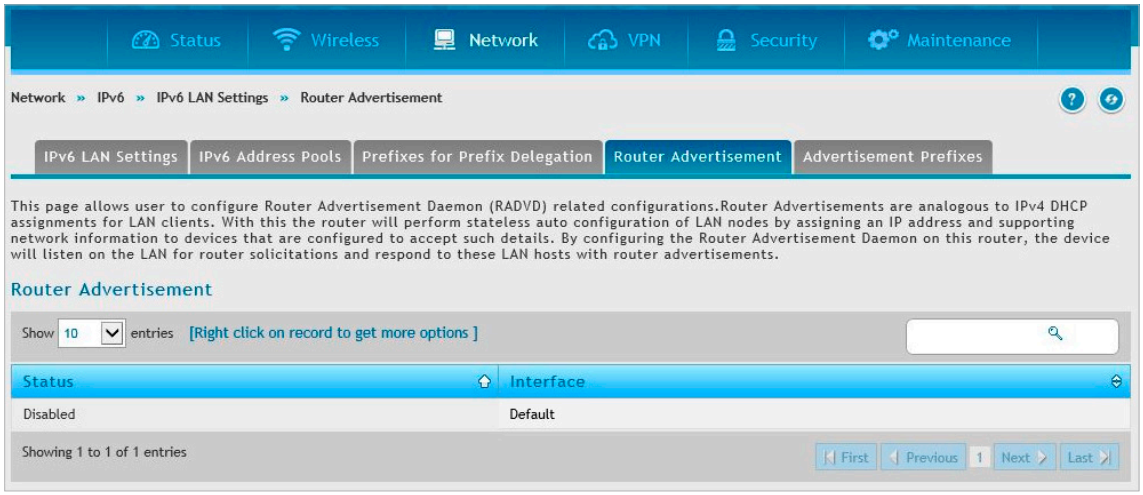

図 5-66　IPv6 LAN Settings > Router Advertisement タブ 画面

2. ルータ通知を編集する場合、エントリ上で右クリック →「Edit」を選択し、以下の画面を表示します。

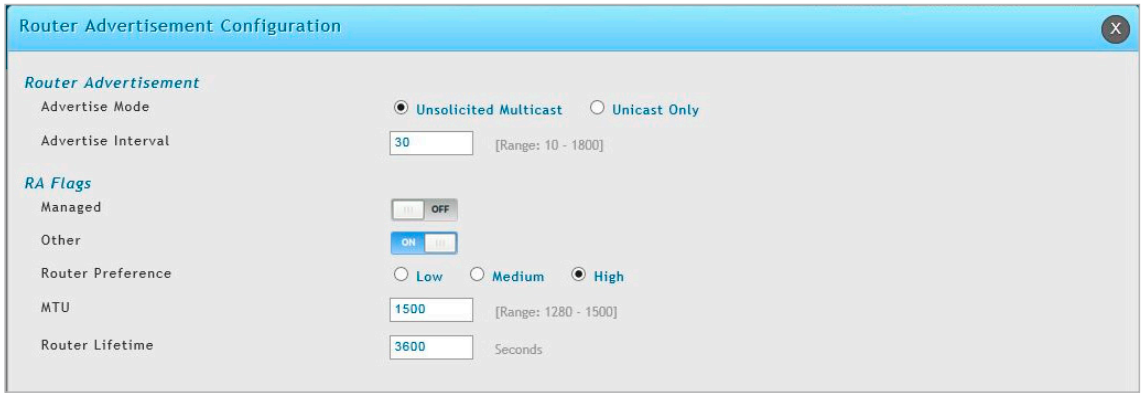

図 5-67　Router Advertisement Configuration 画面

3. 以下の項目を設定します。

項目	説明
Router Advertisement	
Advertise Mode	• 「Unsolicited Multicast」：ルータ通知（RA）をマルチキャストグループに所属する全インタフェースに送信します。 • 「Unicast only」：RA を LAN 上の既知の IPv6 アドレスに制限し、全体的なネットワークトラフィックを軽減させます。
Advertise Interval	「Advertise Mode」で「Unsolicited Multicast」を選択した場合、この間隔にはインタフェースからの通知間隔の最大時間を設定します。通知間の実際の時間は、本値のその 1/3 の値の間のランダムな値となります。 • 初期値：30（秒）
RA Flags	
Managed	「ON」にすると、アドレス自動設定に管理 / ステートフルプロトコルを使用します。
Other	「ON」にすると（アドレス以外の）他の情報の自動設定に管理 / ステートフルプロトコルを使用します。
Router Preference	ルータの RADVD 処理に関連付けられる優先度を「Low/Medium/High」から選択します。LAN 上に RADVD が有効な他のデバイスがある場合、IPv6 クライアントに対して重複を回避するために本機能を使用します。
MTU	ルータによって自動構成される LAN 内のすべてのノードに対して、ルータ通知はこの MTU（Maximum Transmission Unit）値を設定します。 • 設定可能範囲：1280-1500 • 初期値：1500
Router Lifetime	この値は RA に含まれ、インタフェースのデフォルトルータとしてこのルータの有用性を示します。 この期限に到達した際は、新しい RADVD 交換がホストとこのルータ間で行われる必要があります。 • 初期値：3600（秒）

4. 「Save」をクリックし、設定を適用します。

Advertisement Prefixes（通知のプレフィックス）

通知の時に使用される IPv6 プレフィックスを設定します。
ルータ通知と共に通知プレフィックスを設定することで、本ルータはステートレスアドレス自動設定の実行方法をホストに知らせることができます。ルータ通知にはサブネットプレフィックスのリストが含まれています。これによりネイバを決定し、そのホストがルータと同じリンク上に存在するかどうかを識別できます。

1. **Network > IPv6 > IPv6 LAN Settings > Advertisement Prefixes タブ**の順にメニューをクリックし、以下の画面を表示します。

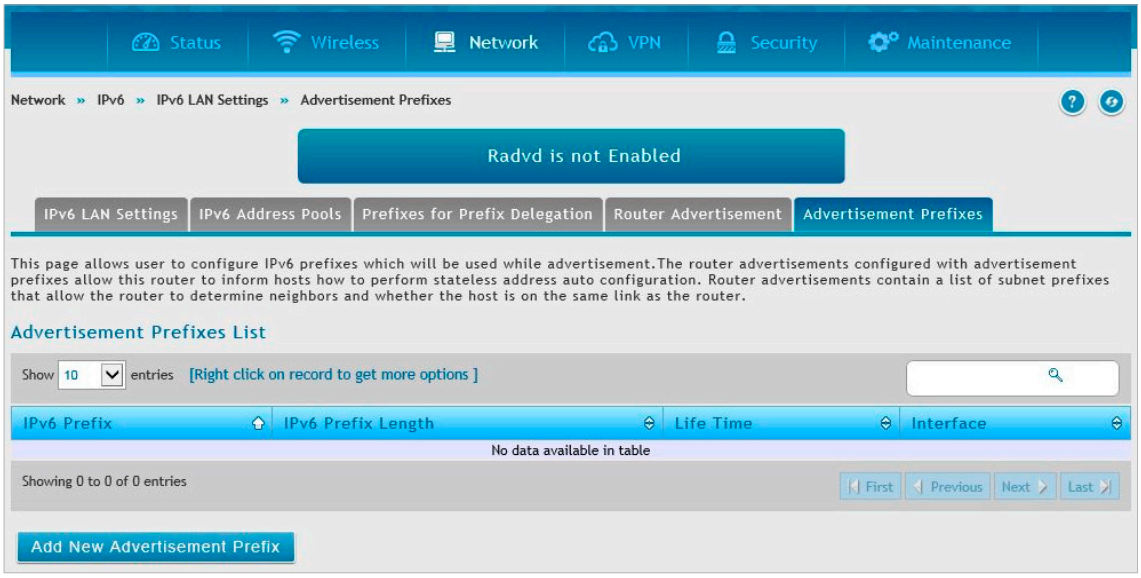

図 5-68　IPv6 LAN Settings >Advertisement Prefixes タブ 画面

2. プレフィックスを追加する場合、「Add New Advertisement Prefix」をクリックし以下の画面を表示します。

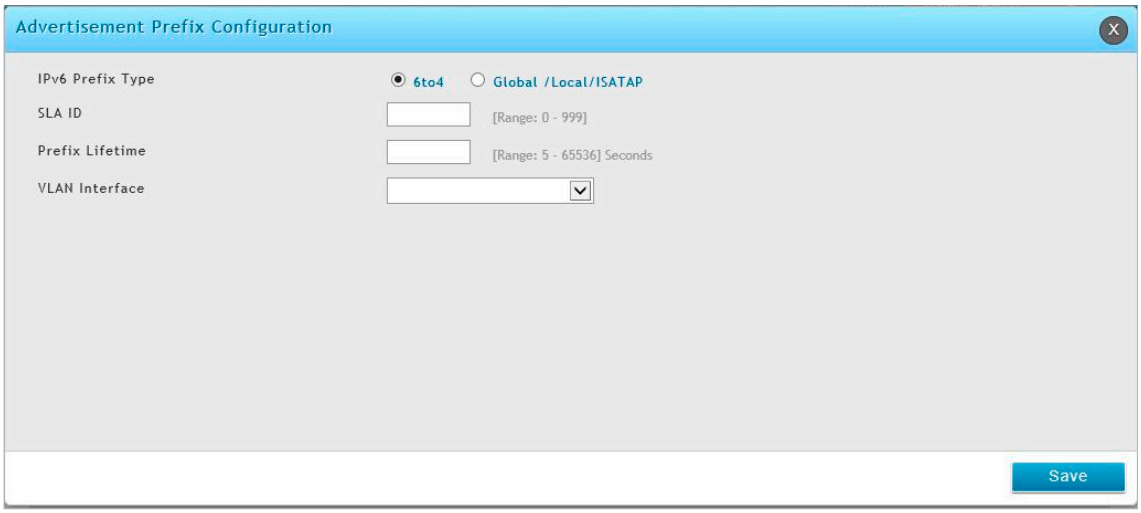

図 5-69　Advertisement Prefix Configuration 画面

3. 以下の項目を設定します。

項目	説明
IPv6 Prefix Type	ホストが IPv6 to IPv4 トンネルを確実にサポートするためには、「6to4」プレフィックスタイプを選択します。「Global/Local/ISATAP」を選択すると、ノードは他のすべての IPv6 ルーティングオプションをサポートすることができます。
SLA ID	SLA ID（Site-Level Aggregation Identifier）は、「6to4」プレフィックスタイプが選択された場合に利用することができます。これはルータ通知に使用されるルータの LAN インタフェースのインタフェース ID とする必要があります。
IPv6 Prefix	「Global/Local/ISATAP」プレフィックスを使用する場合、本ルータが通知する IPv6 ネットワークを定義します。
IPv6 Prefix Length	「Global/Local/ISATAP」プレフィックスを使用する場合、アドレスのネットワーク部分を定義する連続した IPv6 アドレスの高位のビット数を示す数値を指定します。通常は 64 を指定します。
Prefix Lifetime	要求するノードが通知されたプレフィックスを使用できる期間（秒）を定義します。IPv4 ネットワークにおける DHCP リースタイムと類似の機能です。
VLAN Interface	VLAN インタフェースを指定します。

4. 「Save」をクリックし、設定を適用します。

追加したプレフィックスは、**IPv6 LAN Settings > Advertisement Prefixes タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

IPv6 Tunnels Status（IPv6 トンネルステータス）

Network > IPv6 > IPv6 Tunnels Status
IPv6 トンネルのステータスを表示します。

1. **Network > IPv6 > IPv6 Tunnels Status** の順にメニューをクリックし、以下の画面を表示します。

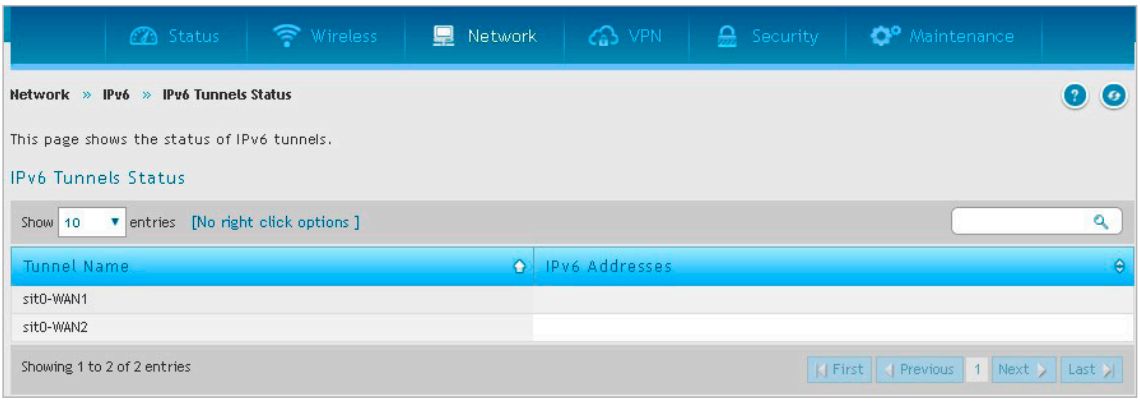

図 5-70　IPv6 Tunnels Status 画面

第 6 章　無線設定（Wireless）（DSR-1000AC のみ）

本製品の無線設定について説明します。
無線設定はウィザードを使用して行うこともできます。
ウィザードを開始するには、「ワイヤレスネットワーク接続（DSR-1000AC のみ）」を参照してください。

項目	説明
「General（一般設定）」	DSR-1000AC の無線ネットワークおける一般的な設定（AP 追加、プロファイル、帯域設定など）をします。
「Advanced（高度な設定）」	DSR-1000AC の無線ネットワークおける高度な設定（WMM、WDS、WPS など）をします。

General（一般設定）

Wireless > General

DSR-1000AC は無線 LAN クライアント用のアクセスポイント機能を設定可能な統合された 802.11n/ac 無線帯域を搭載しています。セキュリティ / 暗号化 / 認証オプションは無線のプロファイルにまとめられ、各設定プロファイルは AP 設定メニューで設定することができます。プロファイルは、無線クライアントと AP 間のセキュリティを含む AP 用の様々なパラメータを定義しており、必要に応じて、同じデバイスの複数の AP インスタンス間で共有できます。

複数の「仮想」の AP を設定することによって、最大 4 つのユニークな無線ネットワークを作成することができます。各仮想 AP はその環境でサポートされるクライアントに対しては独立している AP（ユニークな SSID）として表示されますが、実際にはこのルータに統合される同じ物理周波数帯域で動作しています。

注意 プロファイルは 1 つではなく複数の AP インスタンス（SSID）に適用される AP パラメータをグループ化したものとして考えることができます。そのため、同じパラメータが複数の AP インスタンスまたは SSID に使用される場合に重複を避けることができます。

Access Points（アクセスポイント）

Wireless > General > Access Points

無線 LAN アクセスポイントを設定、表示します。

1. **Wireless > General > Access Points** の順にメニューをクリックし、以下の画面を表示します。

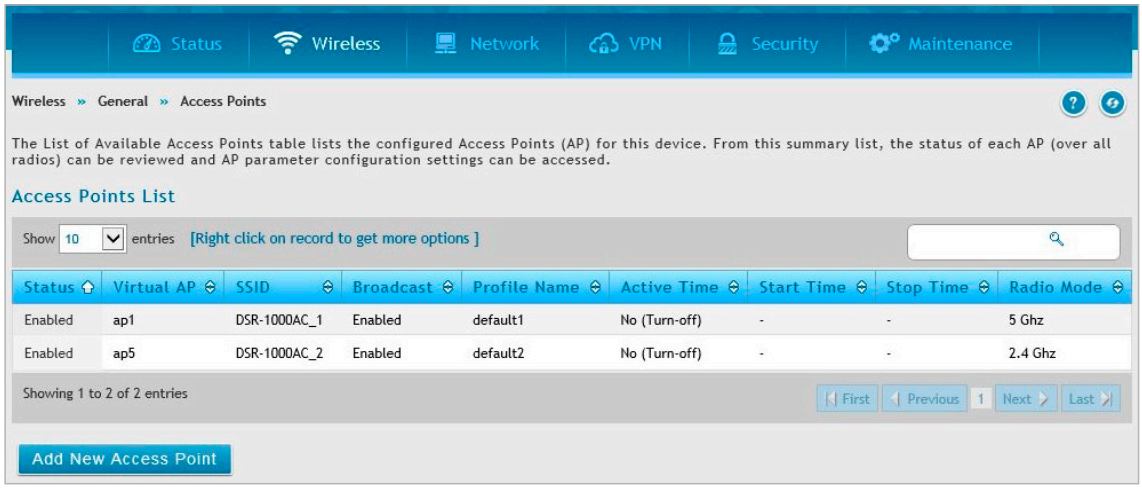

図 6-1　Access Points 画面

2. エントリで右クリックすると、以下のメニューが表示されます。
- 「Edit」：アクセスポイントの追加、編集を行います。
- 「Disable」：アクセスポイントを無効にします。
- 「MAC Filter」：MAC フィルタリングを行います。
- 「Status」：ステータスを表示します。
- 「Delete」：アクセスポイントを削除します。

Add New Access Point（アクセスポイントの追加 / 編集）

1. 「Add New Access Point」をクリック、または既存のエントリ上で右クリック→「Edit」を選択し、以下の画面を表示します。

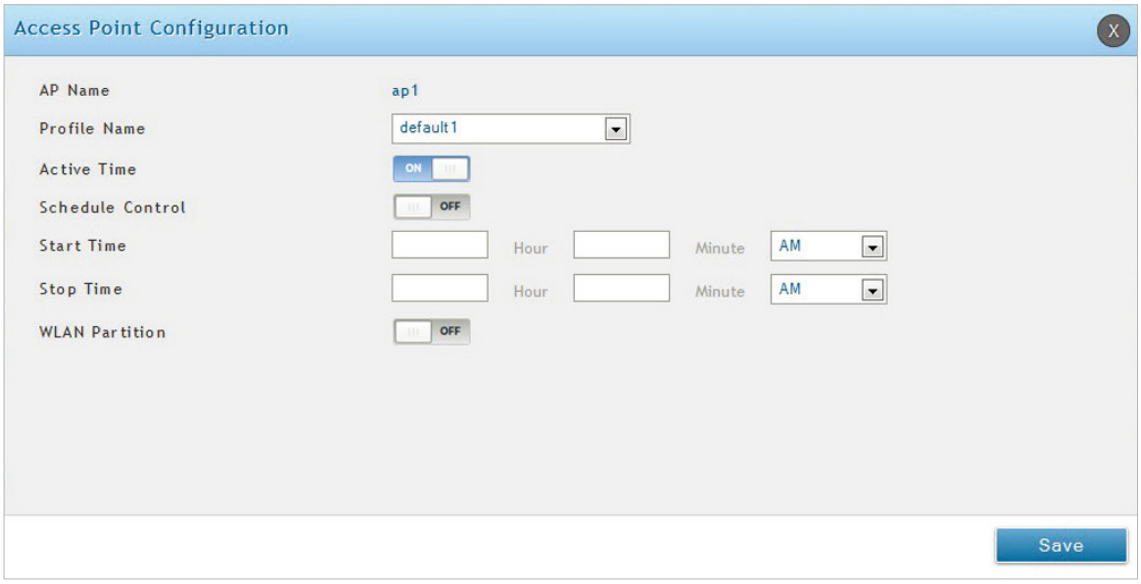

図 6-2　Access Point Configuration 画面

2. 以下の項目を設定します。

項目	説明
AP Name	仮想アクセスポイント名を入力します。
Profile Name	プルダウンメニューからこのアクセスポイントに紐付けるプロファイルを選択します。**Wireless > General > Profiles** 画面で追加したプロファイルが選択肢として表示されます。
Active Time	アクセスポイントとしての機能を有効にします。 以下「Schedule Control」および「Start Time」/「Stop Time」欄を指定することができます。
Schedule Control	アクセスポイントのスケジュール制御を有効にします。 「Start Time」と「Stop Time」欄で指定された期間、クライアント AP を「Turn-on」（有効）/「Turn-off」（無効）にします。 初期値は無効です。
Start Time	スケジュールを開始する時間（時、分、AM/PM）を設定します。
Stop Time	スケジュールを終了する時間（時、分、AM/PM）を設定します。
WLAN Partition	「ON」に設定すると、各無線クライアントは他のクライアントと通信することができなくなります。

3. 「Save」をクリックし、設定を適用します。

MAC Filter（アクセスポイントの MAC フィルタリング）

1. 既存のエントリ上で右クリック→「MAC Filter」を選択し、以下の画面を表示します。

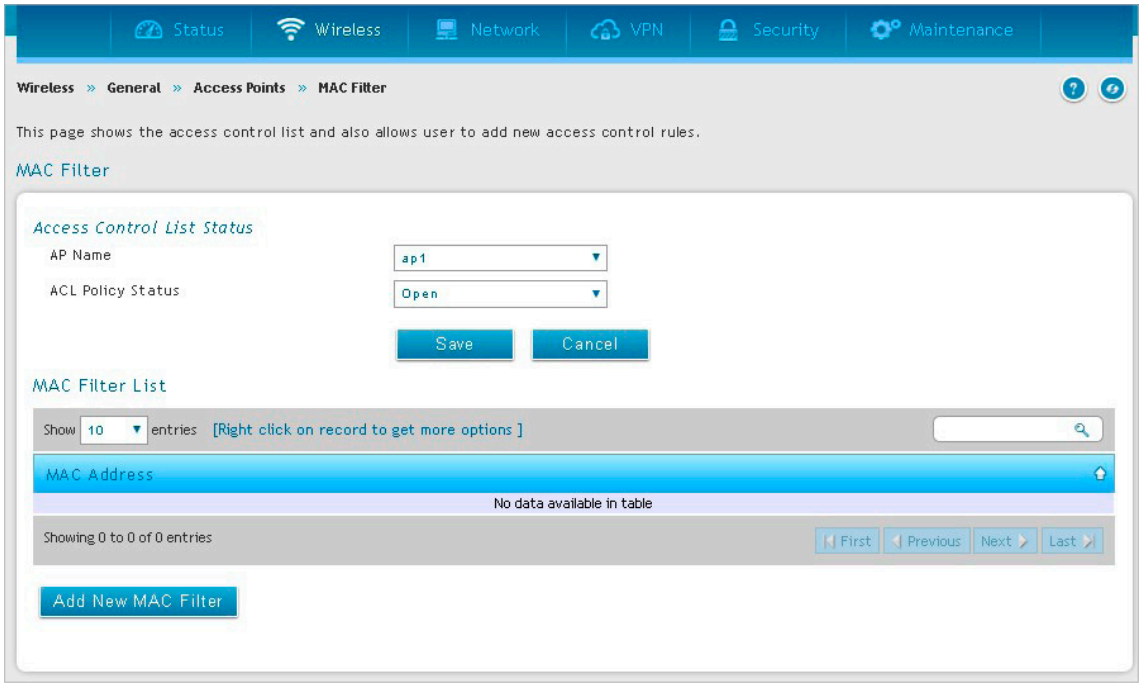

図 6-3　MAC Filter 画面

2. 以下の項目を設定します。

項目	説明
Access Control List Status	
AP Name	アクセスポイントを選択します。
ACL Policy Status	アクセスコントロールリストのステータスを選択します。
MAC Filter List	
MAC Address	アクセスポイントへの接続が許可または拒否されている MAC アドレスのリストが表示されます。

3. MAC アドレスを追加する場合は、「Add New MAC Filter」をクリックし、MAC アドレスを入力します。
4. 「Save」をクリックし、設定を適用します。

Status（アクセスポイントのステータス確認）

1. 既存のエントリ上で右クリック→「Status」を選択し、以下の画面を表示します。

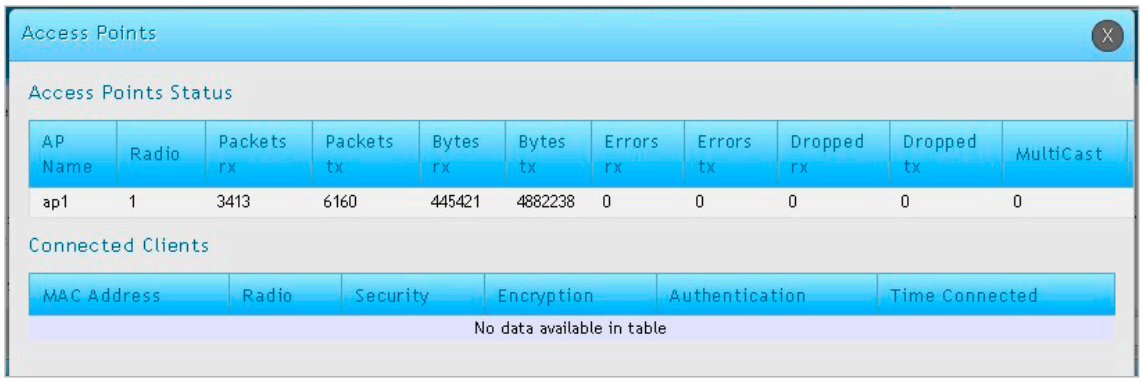

図 6-4　MAC Filter 画面

2. アクセスポイントのステータスと接続しているクライアントの情報を確認します。

Profiles（無線プロファイル）

Wireless > General > Profiles
無線アクセスポイントのためのプロファイルを設定します。

プロファイルを作成することにより、AP と無線クライアントの通信で使用するセキュリティタイプ、暗号化、および認証を割り当てることができます。初期モードは「OPEN」（セキュリティなし）です。このモードでは、すべての互換性のある無線クライアントが AP に接続できるため安全ではありません。

新しいプロファイルの作成
設定の組合せを識別する固有のプロファイル名を使用します。このプロファイルを使用して AP と通信を行うために、クライアントが使用する識別子となる固有の SSID を設定します。SSID のブロードキャストを有効化した場合、AP の範囲内にある互換性を持つ無線クライアントはこのプロファイルを検出できます。

APはWEP、WPA、WPA2、およびWPA+WPA2オプションを含むすべての802.11の高度なセキュリティモードを提供します。アクセスポイントのセキュリティは以下の「Profile Configuration」セクションの「Security」の選択によって設定することができます。

1. **Wireless > General > Profiles** の順にメニューをクリックし、以下の画面を表示します。

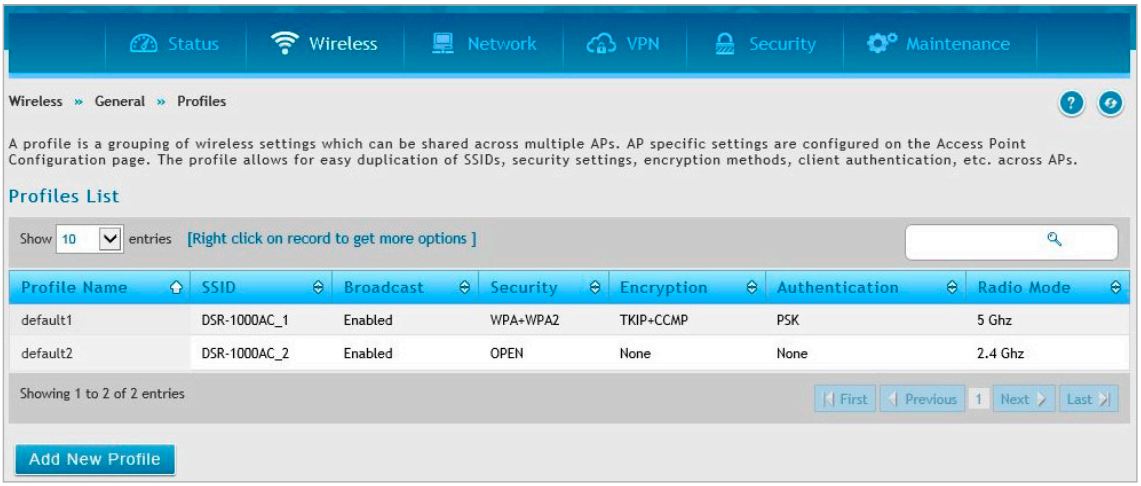

図 6-5　Profiles 画面

注意 DSR-1000AC は 2.4GHz と 5GHz の両方の帯域をサポートしています。デフォルトプロファイルについても編集することができます。

2. プロファイルを追加する場合、「Add New Profile」をクリックし以下の画面を表示します。

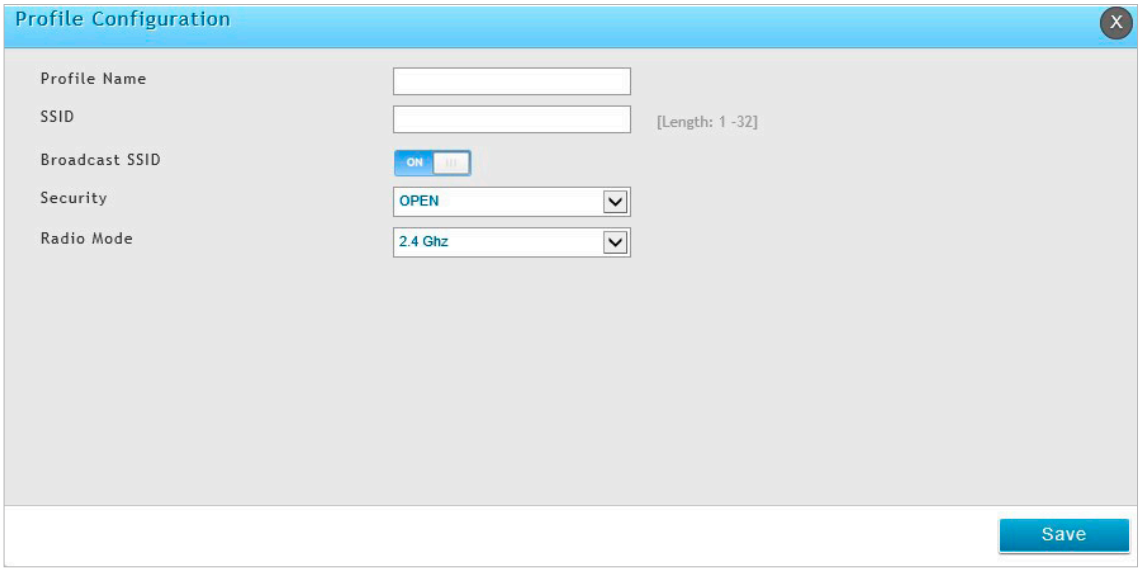

図 6-6　Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
Profile Name	プロファイル名を入力します。
SSID	SSID を入力します。
Broadcast SSID	SSID をブロードキャストにオープンする場合「ON」にします。「OFF」にすると非表示になります。
Security	セキュリティ方式を以下から選択します。 • 「OPEN」：パブリックに「オープン」なネットワークを作成し、この無線ゲートウェイに未認証デバイスがアクセスすることを許可します。 • 「WEP（Wired Equivalent Privacy）」：スタティックな（事前共有）鍵を AP と無線クライアント間で共有することを必要とします。WEP は 802.11n データ速度をサポートしないことに注意してください。これは、旧式の 802.11 接続に適しています。 • 「WPA2」：このセキュリティタイプは PSK（事前共有鍵）またはエンタープライズ（RADIUS サーバ）認証のいずれかの場合に CCMP 暗号化を使用します。 • 「WPA + WPA2」：これは暗号化アルゴリズムの TKIP および CCMP の両方を使用します。WPA クライアントは TKIP を使用し、WPA2 クライアントは CCMP 暗号化アルゴリズムを使用します。
Authentication	暗号の種類を指定したセキュリティ方式に従い、以下から選択します。 • 「WEP」：「Open System」または「Shared Key」を選択します。 • 「WPA2/WPA+WPA2」：「PSK」（パスフレーズ）、「RADIUS」（RADIUS サーバ）、「PSK+RADIUS」から指定します。
Encryption	認証方式を指定したセキュリティ方式に従い、以下から選択します。 • 「WEP」：暗号キーのサイズ（「64 bit WEP」または「128 bit WEP」）を選択します。大きいサイズのキーほど強い暗号化を提供するため、キーの解読が難しくなります。 • 「WPA2」：「CCMP」のみ選択可能です。 • 「WPA+WPA2」：「TKIP+CCMP」のみ選択可能です。
WEP Passphrase/ WEP Key1-4	WEP を選択した場合、パスフレーズまたは 16 進数方式のキーを指定します。 「WEP Passphrase」を入力し、「Generate Key」をクリックすると自動的に「WEP Key」が生成されます。
WPA Password	「WPA2」、「WPA+WPA2」を選択した場合、WPA パスワードを指定します。
Protect Management Frame	「PSK」「PSK+RADIUS」を選択した場合に表示されます。「ON」にすると管理フレームの保護を有効にします。
Enable Pre-Authentication	「WPA2」で「RADIUS」を選択した場合に表示されます。「ON」にすると事前認証を有効にします。
Radio Mode	適用する無線帯域を指定します。「2.4GHz」「5GHz」「Both」（両方）から選択します。

4. 「Save」をクリックし、設定を適用します。

追加したプロファイルは、Profiles 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Wireless > General > Access Points 画面では、新しいアクセスポイントの作成とプロファイルの紐付けを行います。
本製品は複数のアクセスポイントをサポートしており、これは仮想アクセスポイント（VAP）と呼ばれます。固有の SSID を持つ各仮想 AP は、クライアント側から見てそれぞれ独立した 1 台のアクセスポイントのように見えます。こうした仕組みにより、ユーザ要件に沿ってユーザグループに対してセキュリティとスループットの最適化を行うことで、ルータの無線設定を行うことが可能です。VAP の作成手順は、「Access Points（アクセスポイント）」を参照してください。

Radio Settings（無線帯域の詳細設定）

Wireless > General > Radio Settings
DSR-1000AC の無線設定について説明します。

DSR-1000AC では、2.4 GHz または 5 GHz のいずれかの周波数帯を選択できます。
選択した周波数帯に基づき、モードの種類とチャネル幅を設定します。

2.4 GHz（2.4 GHz 設定）

2.4GHz 帯域での無線機能について説明します。

1. **Wireless > General > Radio Settings > 2.4GHz タブ**の順にメニューをクリックし、以下の画面を表示します。

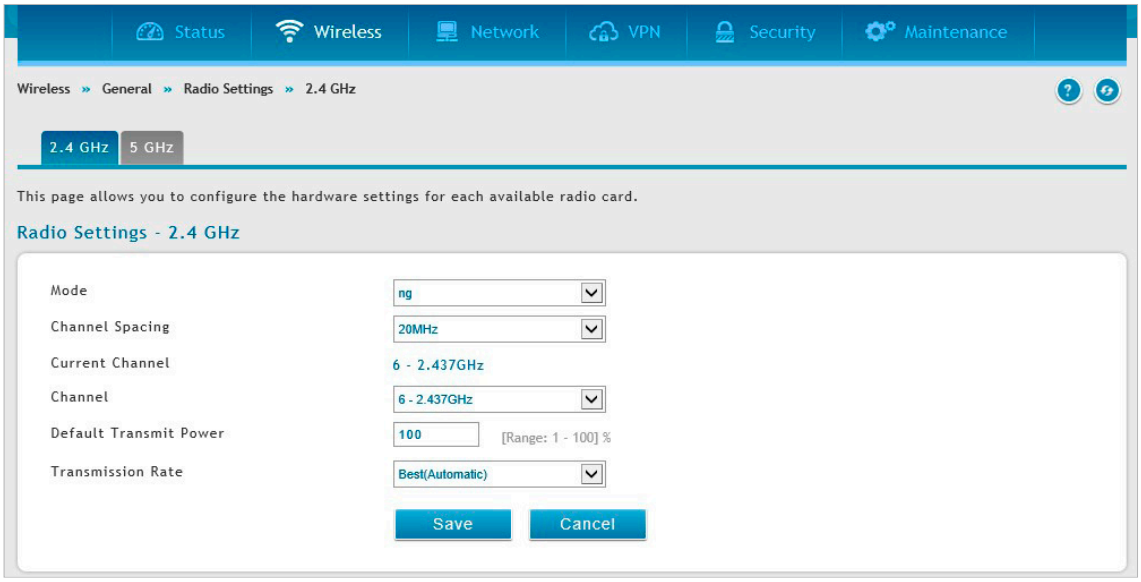

図 6-7　Radio Settings（2.4GHz）画面

2. 以下の項目を設定します。

項目	説明
Mode	802.11 モードを「g and b」「g only」「b only」「ng」「n only」から選択します。
Channel Spacing	チャネル幅を選択します。 • 「20/40 MHz」（初期値） 802.11n 対応の無線機器と 802.11n 非対応の無線機器がネットワークに混在する場合に選択します。「Mode」が「ng」「n only」の場合に選択できます。 • 「20MHz」 802.11n 対応の無線機器を使用しない場合、選択します。「Mode」が「g and b」「g only」「b only」の場合に選択できます。
Control Side Band	「Upper」または「Lower」を選択します。チャネル幅が「20/40 MHz」の場合のみ選択できます。
Current Channel	現在のチャネルを表示します。
Channel	使用するチャネルを選択します。
Default Transmit Power	初期設定の発信強度（単位：%）を指定します。
Transmission Rate	ドロップダウンメニューより送信レートを選択します。 これにより無線接続の送信レートは固定されます。 • 推奨設定：「Best (Automatic)」

3. 「Save」をクリックし、設定を適用します。

5 GHz（5 GHz 設定）

本項目では 5GHz 帯域での無線機能について説明します。

5GHz 帯のみで使用可能な「802.11AC」を使用すると、最大 80MHz までチャンネル帯域を指定することが可能となり、データスループットは「802.11n」に比べて大きく向上します。使用できるチャネルや帯域は DSR-1000AC が使用される国によって制限がある場合があります。「802.11AC」では、5GHz 無線の新しいデザインによる拡張機能を使用し、無線フレームアグリゲーション経由でより多くのデータを単一パケットに乗せて送信することが可能です。

1. **Wireless > General >Radio Settings > 5 GHz タブ**の順にメニューをクリックし、以下の画面を表示します。

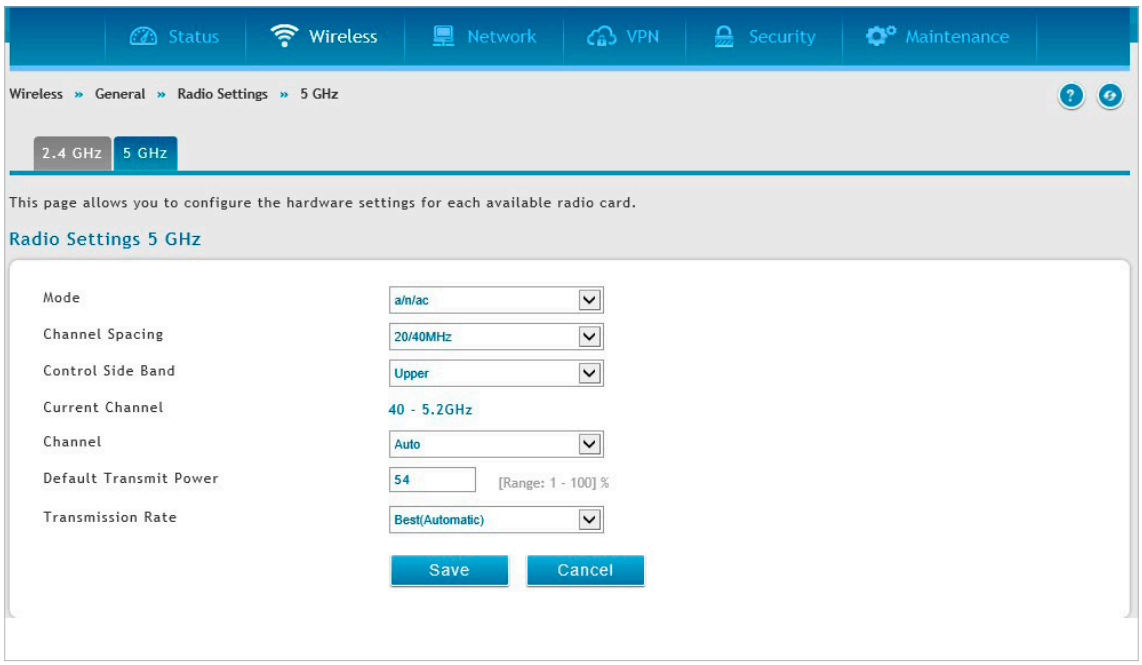

図 6-8　　Radio Settings > 5GHz タブ画面

2. 以下の項目を設定します。

項目	説明
Mode	「a only」「n only」「ac only」「na」「a/n/ac」から選択します。
Channel Spacing	チャンネル幅を選択します。 • 「20/40 MHz」：Mode が「n only」「ac only」「na」「a/n/ac」の場合、選択可能です。 • 「20MHz」：全モードで選択可能です。 • 「80MHz」：Mode が「ac only」「a/n/ac」の場合、選択可能です。
Control Side Band	「Upper」または「Lower」を選択します。「20/40 MHz」選択時のみ有効です。
Current Channel	現在のチャネルを表示します。
Channel	使用するチャネルを選択します。
Default Transmit Power	初期設定の発信強度（単位：%）を指定します。
Transmission Rate	ドロップダウンメニューより送信レートを選択します。 これにより無線接続の送信レートは固定されます。推奨設定：「Best (Automatic)」

3. 「Save」をクリックし、設定を適用します。

Advanced（高度な設定）

Wireless > Advanced
無線設定における高度な設定を行います。

WMM（WMM 設定）

Wireless > Advanced > WMM
WMM（Wi-Fi Multimedia）は、IEEE 802.11 ネットワークに基本的な QoS（Quality of Service）機能を提供します。WMM は、音声、ビデオ、ベストエフォート、およびバックグラウンドの 4 つの AC（Access Categories: アクセスカテゴリ）に従ってトラフィックを優先させます。

1. **Wireless > Advanced > WMM** の順にメニューをクリックし、以下の画面を表示します。

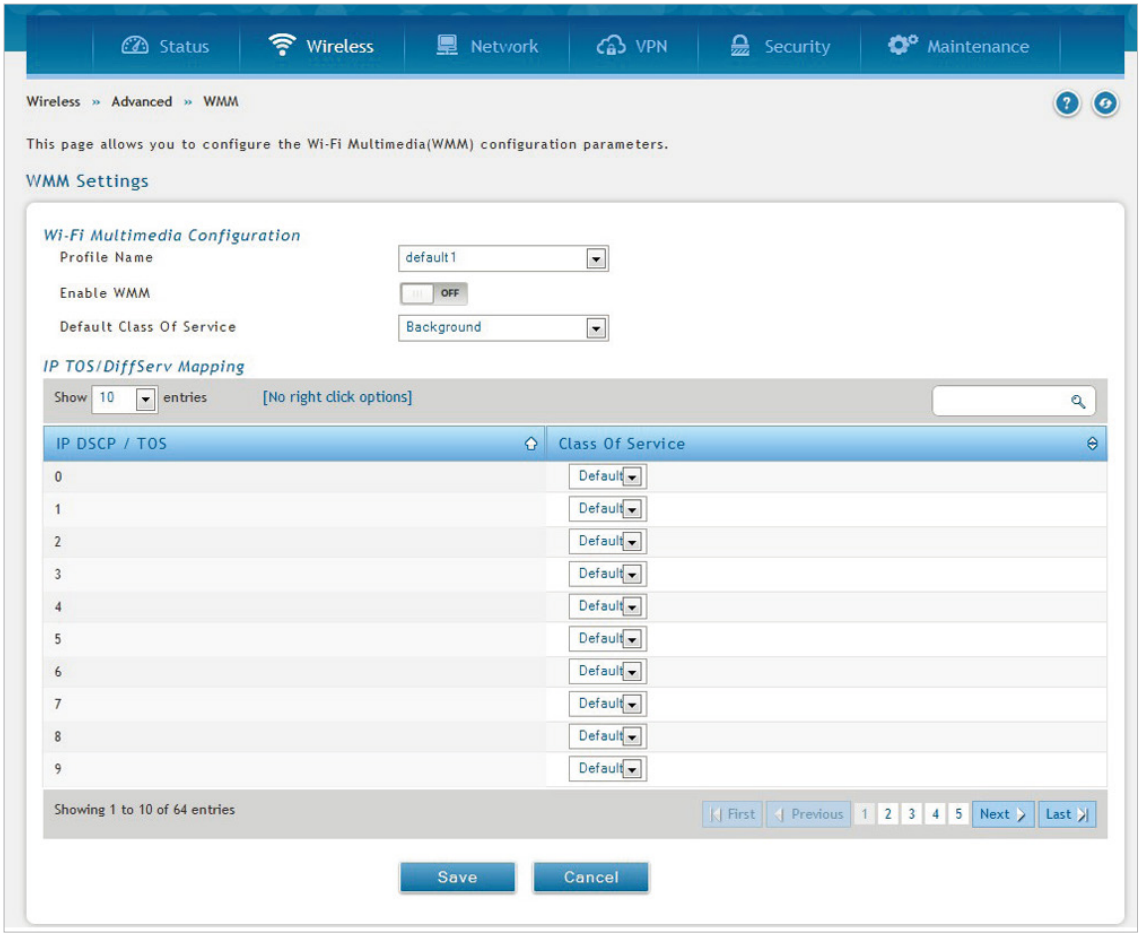

図 6-9　WMM 画面

2. 以下の項目を設定します。

項目	説明
Profile Name	本設定に関連付けるプロファイルを選択します。
Enable WMM	「ON」にすると WMM 機能が有効になります。
Default Class Of Service	利用可能なアクセスカテゴリ（Voice、Video、Best Effort および Background）を選択します。
IP DSCP / TOS	「Class Of Service」毎にサービスを選択し、「IP DSCP / TOS」とのマッピングを設定します。

3. 「Save」をクリックし、設定を適用します。

WDS（WDS 設定）

Wireless > Advanced > WDS

WDS（Wireless Distribution System）は、ネットワーク上のアクセスポイント同士での無線相互接続を有効にするシステムです。本機能は、同じタイプのデバイス間（同じチップセット / ドライバを使用している場合など）でのみ正常な動作が保証されます。

WDS リンクが有効である場合には、デフォルトアクセスポイントと同じセキュリティ設定を使用します。WDS リンクが適切な WPA/WPA2 をサポートしないと、WPA キーのハンドシェイクが実行されません。代わりに、WDS Peer と共に使用されるセッションキーは、（WPA PMK を計算するのに使用するものと同じ）ハッシュ関数を使用して計算されます。本関数には、（WDS 設定ページで管理者による設定が可能な）PSK と（設定不可の）内部の「magic」文字列が、入力値として使用されます。

実際には、WDS リンクは、デフォルト AP に設定された暗号化に従って TKIP/AES 暗号化を使用します。Default AP で TKIP ＋ AES が選択されている場合、WDS リンクでは AES 暗号化方式が使用されます。

WDS 設定は各帯域（5GHz/2.4GHz）でタブで切り替えて設定を行います。表示される項目は同一です。

1. **Wireless > Advanced > WDS > 2.4 GHz タブ / 5GHz タブ**の順にメニューをクリックし、以下の画面を表示します。

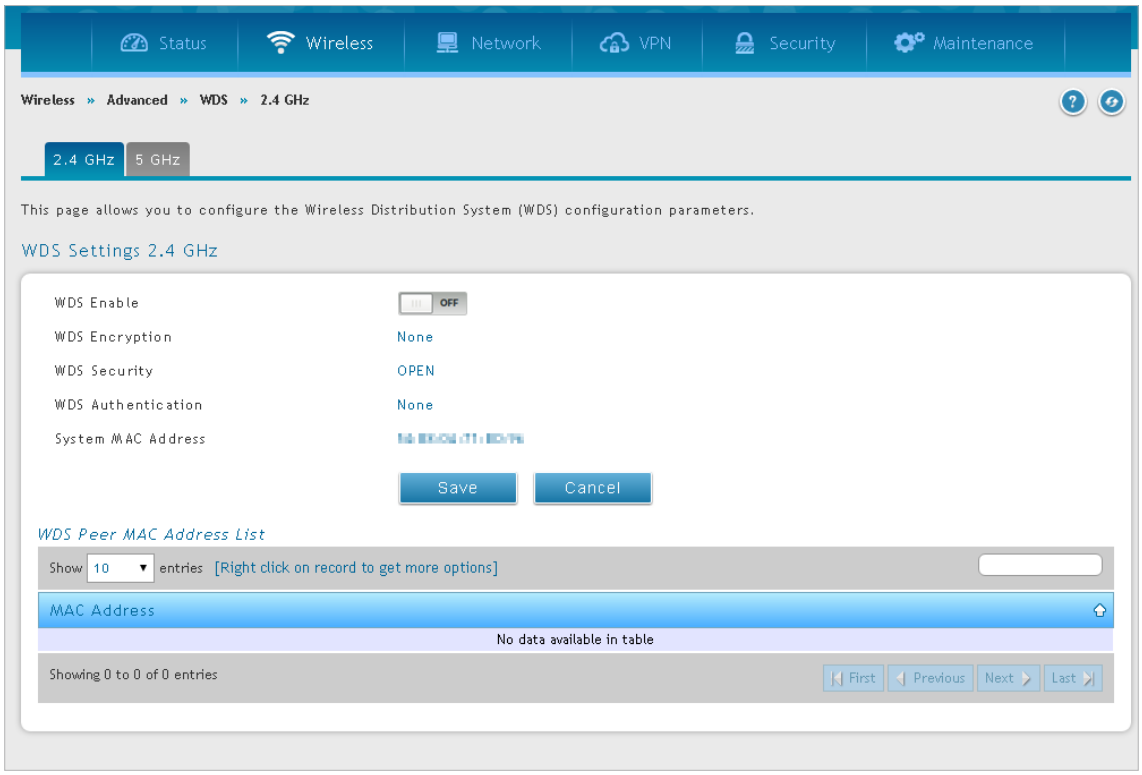

図 6-10　WDS > 2.4 GHz タブ画面

注意　WDS リンクが適切に機能するためには、WDS ピアにおける無線帯域設定を同一にする必要があります。

2. 以下の項目を設定します。

項目	説明
WDS Enable	「ON」にして WDS を有効にします。
WDS Encryption	現在 WDS リンクで使用されている暗号化のタイプを表示します。
WDS Security	現在 WDS リンクで使用されているセキュリティを表示します。
WDS Authentication	現在 WDS リンクで使用されている認証方法を表示します。
WDS Passphrase	WDS のパスフレーズを入力します。本項目は、WEP、WPA、WPA2、WPA+WPA2 が有効で、「WDS Enable」を「ON」にした場合のみ表示されます。
System MAC Address	システム MAC アドレスを表示します。

3. 「Save」をクリックし、設定を適用します。

Advanced Settings（詳細設定）

Wireless > Advanced > Advanced Settings
ここでは無線の詳細な設定を行います。

802.11 の通信パラメータを変更することができます。通常、多くのネットワークでは初期設定が適しています。
Advanced Settings（詳細設定）は各帯域（5GHz/2.4GHz）でタブで切り替えて設定を行います。表示される項目は一部を除き同じです。

1. **Wireless > Advanced > Advanced Settings > 2.4 GHz タブ / 5GHz タブ**の順にメニューをクリックし、以下の画面を表示します。

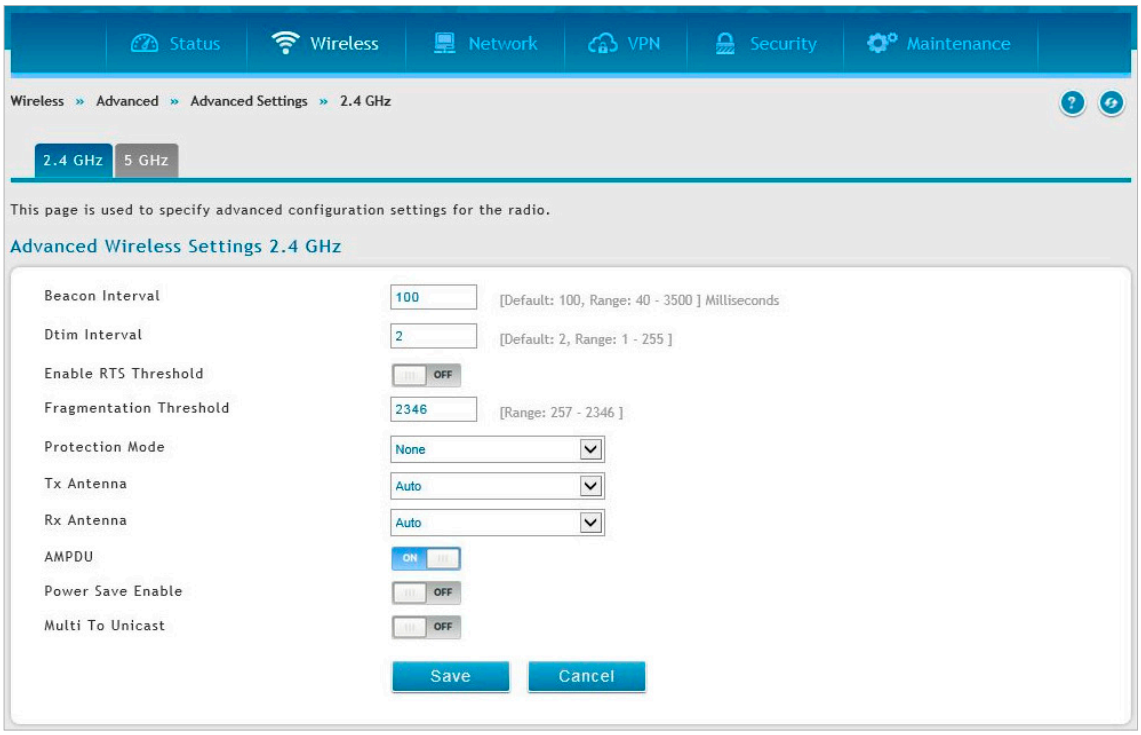

図 6-11　Advanced Settings 画面（2.4GHz）画面

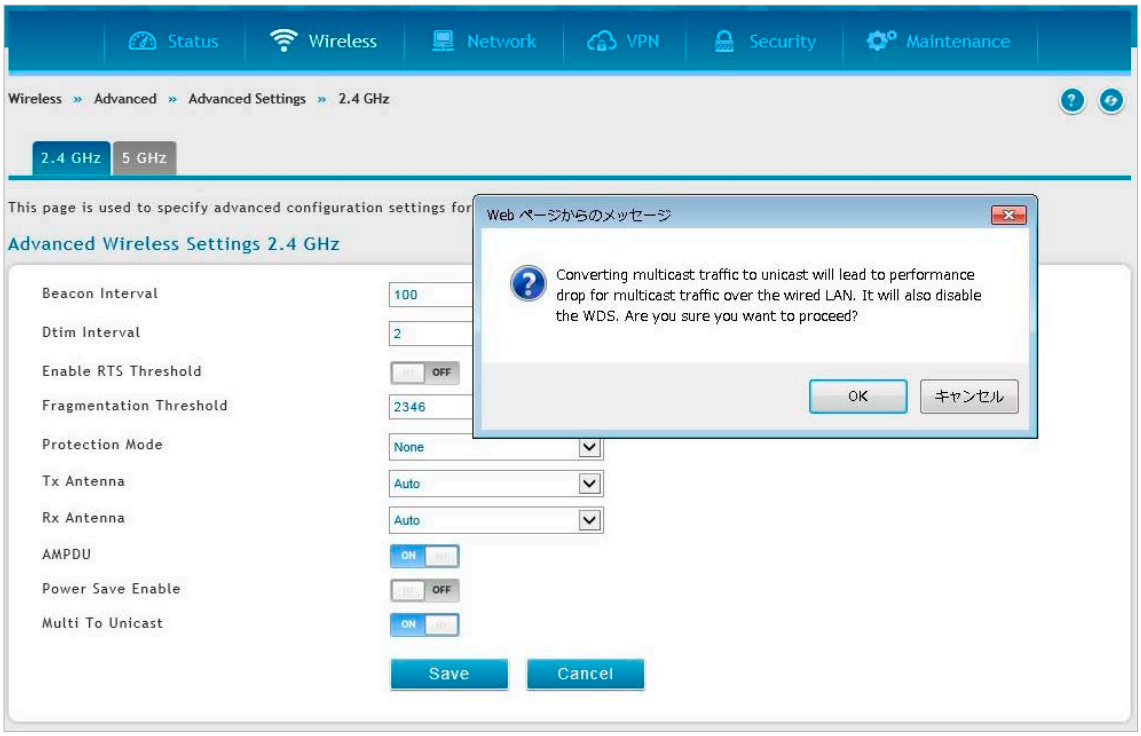

図 6-12　Advanced Settings 画面（2.4GHz）（Multi To Unicast 有効化時）画面

2. 以下の項目を設定します。

項目	説明
Beacon Interval	「ビーコン」は無線ネットワークに同期するためにアクセスポイントから送信されるパケットです。初期値は 100 です。
Dtim Interval	ビーコンに含まれる DTIM（Delivery Traffic Information Message）の周期を設定します。 省電力モードの無線クライアントに対して、送信待ちのデータがあることを伝えます。 • 初期値：2
Enable RTS Threshold	RTS しきい値を指定します。送信データがこのパケットサイズ（Byte）よりも大きい場合、無線クライアントへ RTS（Request To Send：送信要求）信号を送信します。値を小さくすると RTS パケットの送信頻度が高くなり、ネットワーク帯域を消費してスループットの低下を招く可能性があります。初期値の 2432 のままとしておくことを推奨します。
Fragmentation Threshold （2.4GHz のみ）	フラグメンテーションしきい値を設定します。設定のしきい値を超えたパケットを送信前にフラグ化します。 • 初期値：2346
Preamble Mode （5GHz のみ）	プリアンブルモードを「Long」「Short」から選択します。アクセスポイントとローミング無線アダプタ間の通信において、CRC（Cyclic Redundancy Check）ブロックの長さを定義します。ネットワークのトラフィックが多い場所では「Short」を選択します。
Protection Mode （2.4GHz のみ）	プロテクションモードを「None」「CTS-to-Self Protection」から選択します。 「CTS-to-Self Protection」を選択すると 802.11b と g が混在した環境下でのステーション同士のコリジョン（衝突）を軽減する「CTS-to-Self」防御メカニズムが有効になります。 • 初期値：「None」
Tx/Rx Antenna	送信（Tx）、受信（Rx）におけるアンテナへの割り当てを指定します。
AMPDU	AMPDU（aggregation MAC protocol data unit）を有効にします。MAC ヘッダを含んだフレーム集約を行います。
Power Save Enable	省電力機能を有効にします。「ON」にすると U-APSD（WMM Power Save）によって無線の電力消費が抑制されます。
Multi To Unicast	外部から受信したコンテンツプロバイダのマルチキャスト宛先アドレスを有効にし、ユニキャスト宛先アドレスに変換します。

3. 「Save」をクリックし、設定を適用します。

WPS（WPS 設定）

Wireless > Advanced > WPS

ここでは Wi-Fi Protected Setup（WPS）設定パラメータの定義と変更を行うことができます。

WPS はサポートされる無線クライアントをネットワークに追加するシンプルな方法であり、WPA または WPA2 セキュリティが設定された AP で使用することができます。WPS を使用するには、これらのセキュリティが設定されている AP をドロップダウンメニューから選択し、この AP の WPS ステータスを有効にします。

「WPS Current Status」セクションでは選択した AP のセキュリティ、認証、および暗号化設定についての概要が表示されます。これらは AP のプロファイルと一致しています。WPS には利用可能な 2 つの設定オプションがあります。

• PIN（Personal Identification Number）：

4. WPS をサポートする無線デバイスが、英数字の PIN を持っている場合、この欄に PIN を入力します。ルータは「PIN」フィールドの下にある「Configure via PIN」をクリックした後、60 秒以内に接続します。クライアントが接続したことを示す LED 表示はありません。

• PBC（Push Button Configuration）：

5. PBC をサポートする無線デバイスに対しては、2 秒間「Configure via PBC」を押し続けます。AP は、無線デバイスを検出して、クライアントとのリンクを確立します。

1. **Wireless > Advanced > WPS** の順にメニューをクリックし、以下の画面を表示します。

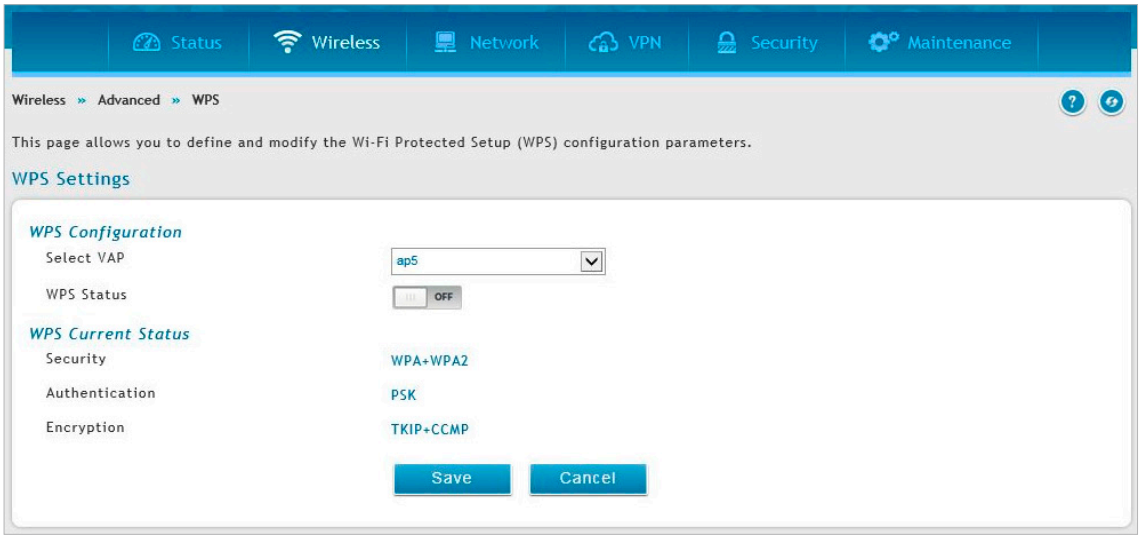

図 6-13　WPS 画面

2. 「Select VAP」で WPS を使用する VAP をドロップダウンメニューから選択します。
3. 「WPS Status」を「ON」にして、設定を適用します。
4. WPS が有効になると以下の画面が表示されます。

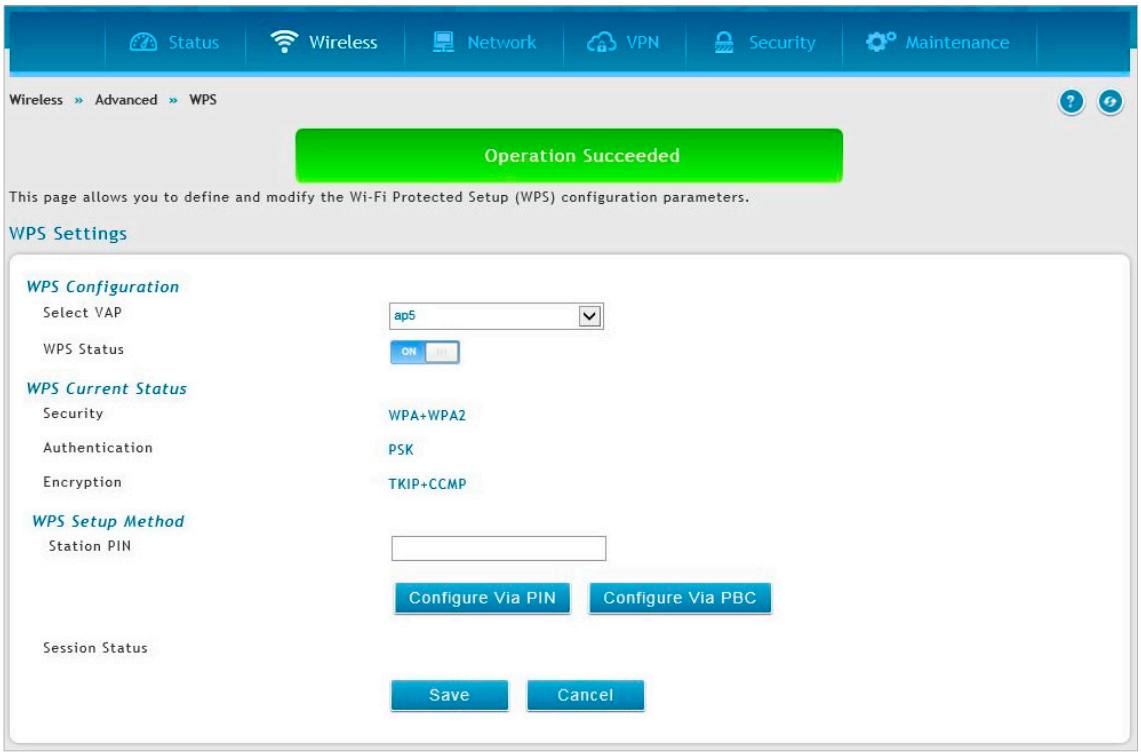

図 6-14　WPS(ON) 画面

5. 「WPS Setup Method」で WPS の方法として、「Configure Via PIN」（PIN 入力）または「Configure Via PIN」（WPS ボタン押下）を選択します。
6. 「PIN」を使用する場合、「Station PIN」に無線クライアントのピンコードを入力し、「Configure Via PIN」（PIN 入力）をクリックします。
7. プッシュボタン方式を使用する場合、「Configure Via PBC」をクリックします。これにより WPS セッションが起動され、無線クライアントの WPS ボタンを 1 分以内に押す（またはインタフェース上で開始する）必要があります。
8. 接続には約 2 分程度かかります。「Session Status」で正常に接続されたことを確認します。

第 7 章　VPN 設定（VPN）

VPN（Virtual Private Network）の設定について説明します。

設定項目	説明
「IPSec VPN（IPSec VPN の設定）」	IPSec VPN の設定を行います。
「PPTP VPN（PPTP VPN 設定）」	PPTP VPN の設定を行います。
「L2TP VPN（L2TP VPN 設定）」	L2TP VPN の設定を行います。
「SSL VPN（SSL VPN 設定）」	SSL VPN の設定を行います。
「OpenVPN（OpenVPN 設定）」	OpenVPN の設定を行います。
「GRE（GRE 設定）」	GRE の設定を行います。

VPN は 2 つのゲートウェイルータ間またはリモート PC クライアント間に安全な通信チャネル（トンネル）を提供します。
以下のタイプのトンネルを作成することができます。

- Gateway-to-gateway VPN
  リモートサイト間のトラフィックを保証するために 2 つ以上のルータを接続します。

- リモートクライアント（client-to-gateway VPN トンネル）
  リモート PC クライアントの IP アドレスが事前に知られていない場合に、リモートクライアントが VPN トンネルを開始します。この場合、ゲートウェイは応答者として動作します。

- NAT ルータの後方のリモートクライアント
  クライアントはダイナミック IP アドレスを持ち、NAT ルータの後方にあります。リモート NAT ルータの IP アドレスが事前に知られていない場合に、NAT ルータにあるリモート PC が VPN トンネルを開始します。ゲートウェイの WAN ポートが応答者として動作します。

- LAN/WAN PPTP クライアント接続のための PPTP サーバ

- LAN/WAN L2TP クライアント接続のための L2TP サーバ

IPSec VPN（IPSec VPN の設定）

VPN > IPSec VPN

Policies（IPSec VPN ポリシーの設定）

VPN > IPSec VPN > Policies

ここではルータに設定済みの IPSec VPN ポリシーのリストを表示します。さらに、IPsec VPN ポリシーの追加、削除、編集、および有効化 / 無効化ができます。

IPSec ポリシーは、本ルータと他のゲートウェイ間、または本ルータとリモートホストの IPSec クライアント間の通信に適用されます。IPSec モードは、ポリシーの 2 つのエンドポイント間を横切るネットワークに応じて「Tunnel Mode」または「Transport Mode」のどちらかになります。

- Transport（転送モード）：
  このモードは、本ルータとトンネルのエンドポイント（別の IPsec ゲートウェイまたはホスト上の IPSec VPN クライアントのいずれか）間の end-to-end 通信のために使用されます。データペイロードのみが暗号化され、IP ヘッダは、変更または暗号化されません。

- Tunnel（トンネルモード）：
  このモードは network-to-network IPSec トンネルに使用されます。このゲートウェイがトンネルの一方のエンドポイントとなります。このモードでは、ヘッダを含むすべての IP パケットは、暗号化と認証の両方、またはどちらかが行われています。

  トンネルモードを選択した場合、NetBIOS および DHCP over IPSec を有効にすることができます。DHCP over IPSec によりこのルータはリモート LAN のホストに IP リースを提供することができます。また、このモードでは、ローカル及びリモートのプライベートネットワークの両方に対し、IP アドレスや IP アドレス範囲、サブネットを定義してトンネル経由の通信を許可することも可能です。

1. **VPN > IPSec VPN > Policies** の順にメニューをクリックし、以下の画面を表示します。

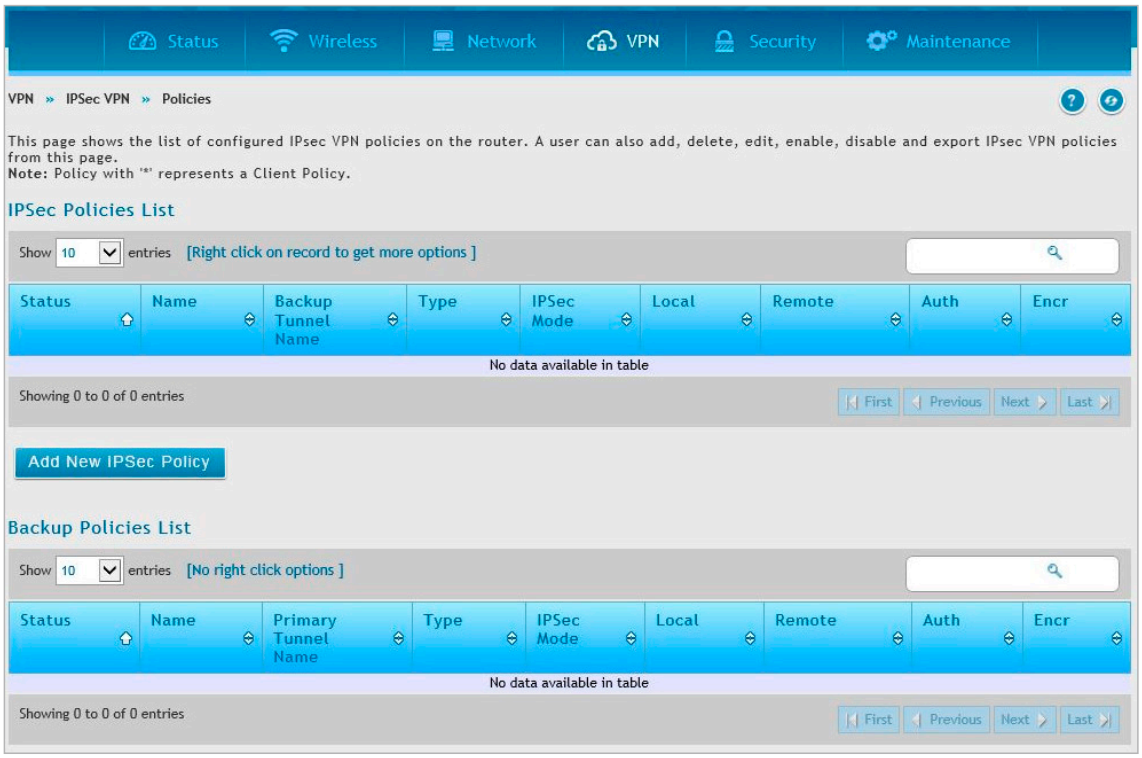

図 7-1　Policies 画面

Add New IPSec Policy（IPSec VPN ポリシーの追加）

1. 「Add New IPSec Policy」をクリックし、以下の画面を表示します。

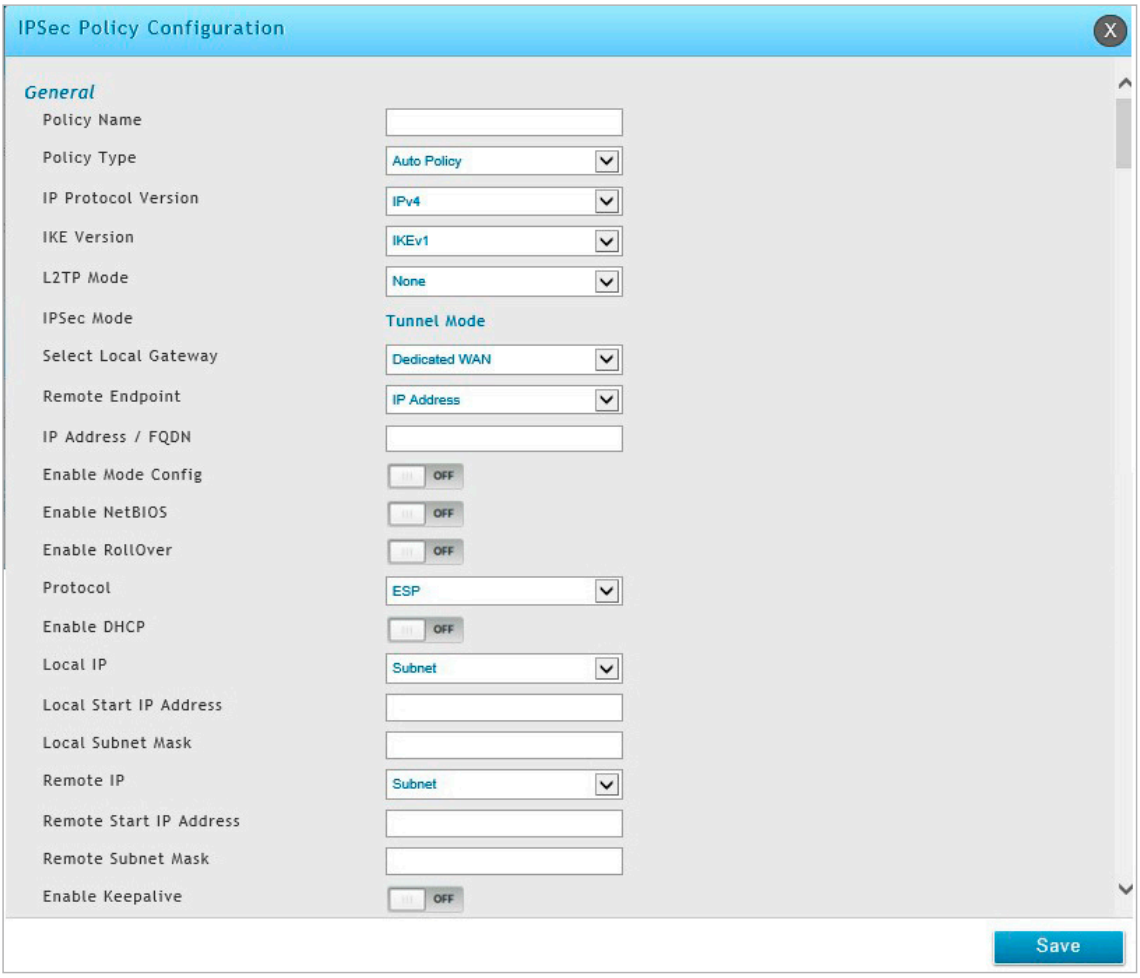

図 7-2　IPSec Policy Configuration 画面

2. 以下の項目を設定します。

項目	説明
Policy Name	VPN ポリシー名を入力します。これはリモート WAN/ クライアントの識別名とはなりません。
Policy Type	VPN ポリシーの種類を「Manual Policy」「Auto Policy」から指定します。 • 「Manual Policy」：各エンドポイントに対し、キーなども含め VPN トンネルのすべての設定を手動で行います。第三者機関サーバや組織などは含まれません。 • 「Auto Policy」：VPN トンネルのいくつかのパラメータは自動的に生成されます。これには二つの VPN エンドポイント間での IKE プロトコルを使用したネゴシエーションが必要になります。
IP Protocol Version	IP バージョン を「IPv4」または「IPv6」から選択します。
IKE Version	IKE バージョン を「IKEv1」または「IKEv2」から選択します。
L2TP Mode	L2TP モードを「None」「Client」「Gateway」から指定します。
IPSec Mode	IPSec モードの状態を「Tunnel Mode」「Transport Mode」で表示します。 IPsec トンネルモードは信頼性の低いネットワークを通過するトラフィックを保護する際に有効です。相互運用性を目的として、主に「L2TP/IPsec」「PPTP」接続などをサポートしていないゲートウェイやエンドシステムなどにおいて、トンネルモードが使用されます。「トランスポートモード」は IPSec の初期モードであり、end-to-end 通信に使用されます。（例：クライアント / サーバ間など）
Select Local Gateway	IPSec トンネルのためのローカルゲートウェイを指定します。1 つ以上の設定済み WAN がある場合、トンネルはゲートウェイのいずれかに対して設定されます。
Remote Endpoint	FQDN または IP アドレスによってトンネルのリモートエンドポイントを識別します。L2TP モードに「Client」を選択した場合は表示されません。
IP Address / FQDN	ルータの識別子を入力します。
Enable Mode Config	「ON」で「Mode Config」を有効にします。 「Mode Config」は、DHCP 機能のようにリモートの VPN クライアントに IP アドレスをアサインする機能です。
Enable NetBIOS	「ON」で VPN トンネルにおける「NetBIOS」ブロードキャストの通過を許可します。
Enable RollOver	「ON」で VPN ロールオーバを有効にします。WAN モードを「Rollover」に指定する必要があります。

項目	説明
Protocol	プロトコルを選択します。
Enable DHCP	「ON」にすると、IPsec 経由でルータに接続している VPN クライアントが、DHCP による割り当て IP アドレスを取得できるようになります。
Remote IP / Local IP	「Enable DHCP」を「OFF」にした場合、エンドポイント用の識別の種類を指定します。 ・「Any」：ポリシーは、ローカル / リモートのエンドポイントからのトラフィックに適用されます。 ・「Single」：ポリシーの適用を 1 台のホストのみに限定します。入力したホストの IP アドレスが VPN の一部になります。 ・「Range」：VPN への接続を許可する IP アドレスの範囲を指定します。開始 IP アドレスと終了 IP アドレスを入力します。 ・「Subnet」：VPN への接続を許可するサブネットを指定します。ネットワークアドレスとサブネットマスクを入力します。
Enable Keepalive	「ON」にした場合、以下の項目を入力します。 ・Source IP Address ・Destination IP Address ・Detection Period [Range: 10 - 999] ・Reconnect After Failure

トンネルのトンネルタイプとエンドポイントが定義されたら、トンネルに使用するフェーズ 1 / フェーズ 2 ネゴシエーションを決定できます。
ポリシーは手動または自動で設定することができます。自動ポリシーの場合、インターネットキー交換（IKE）プロトコルは 2 つの IPsec ホスト間でキーを動的に交換します。

3. 「Phase1(IKE SA Parameters)」「Phase2(Auto Policy Parameters)」の設定を行います。

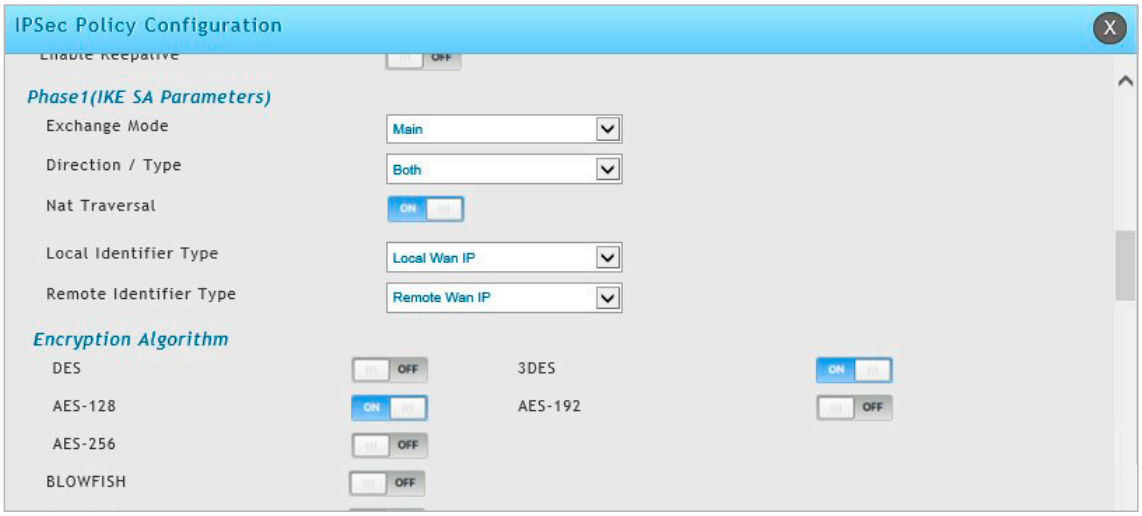

図 7-3　IPSec Policy Configuration 画面 -Phase1/Phase2 画面

フェーズ 1 の「IKE SA Parameter」セクションでは、トンネルのセキュリティアソシエーションの詳細を定義します。
フェーズ 2 の「Auto Policy Parameter」セクションでは、フェーズ 2 キーネゴシエーションのセキュリティアソシエーションの有効期間と暗号化 / 認証の詳細を設定します。

VPN ポリシーは、自動 IPSec VPN トンネルを確立するのに必要とされる IKE/VPN ポリシーのペアの片方です。
2 つの VPN エンドポイントにあるマシンの IP アドレスは、トンネルをセキュアにするために必要とされるポリシーパラメータと共にここで設定されます。

「Manual Policy」では、IKE を使用せず、2 つの IPsec ホスト間での認証パラメータ交換を手動で行います。
送受信される SPI（Security Parameter Index）値は、リモートのトンネルエンドポイントに反映される必要があります。

また、トンネルを確立するためには、暗号化、整合性アルゴリズム、およびキーがリモート IPSec ホストに一致する必要があります。
一部の IPsec では、SPI（Security Parameter Index）値が各エンドポイントで変換を必要とするため、「Auto Policy」で IKE を使用することが推奨されます。

DSR は VPN ロールオーバ機能をサポートしています。これは、プライマリ WAN におけるリンク障害の場合にプライマリ WAN に設定されたポリシーがプセカンダリ WAN にロールオーバすることを意味します。
WAN が「Auto-Rollover」モードに設定されている場合にのみ本機能を使用することができます。

4. 項目を設定後、「Save 」をクリックして設定内容を適用します。

注意 IPsec ポリシー作成後、ポリシーを右クリックして「Export」を選択し、保存することができます。エクスポートファイルは別の DSR にアップロードしたりバックアップファイルとして保存したりすることが可能です。
ポリシーをアップロードする手順については「Easy VPN Setup（VPN セットアップ）」を参照してください。

注意 L2TP over IPSec 設定を適用後、両端（サーバとエンドポイント）が正しく設定されサーバが応答中である場合は、トンネルイニシエーションが自動的に開始されます。

Tunnel Mode（トンネルモード）

VPN > IPSec VPN > Tunnel Mode

トンネルモードを選択した場合、NetBIOS および DHCP over IPSec を有効にすることができます。DHCP over IPSec によりこのルータはリモート LAN のホストに IP リースをサービスすることができます。また、このモードでは、1 つの IP アドレス、IP アドレス範囲、またはトンネル上で通信できるローカルおよびリモート両方のプライベートネットワークにおけるサブネットを定義できます。

本ルータは「Full Tunnel」（フルトンネル）と「Split Tunnel」（スプリットトンネル）をサポートしています。
「Full Tunnel」モードは VPN トンネル中のクライアントからルータにすべてのトラフィックを送信します。「Split Tunnel」モードは事前に指定したクライアントのルートに基づいてプライベート LAN にトラフィックを送信します。

Tunnel Mode（トンネルモード）

1. **VPN > IPSec VPN > Tunnel Mode > Tunnel Mode タブ**の順にメニューをクリックし、以下の画面を表示します。

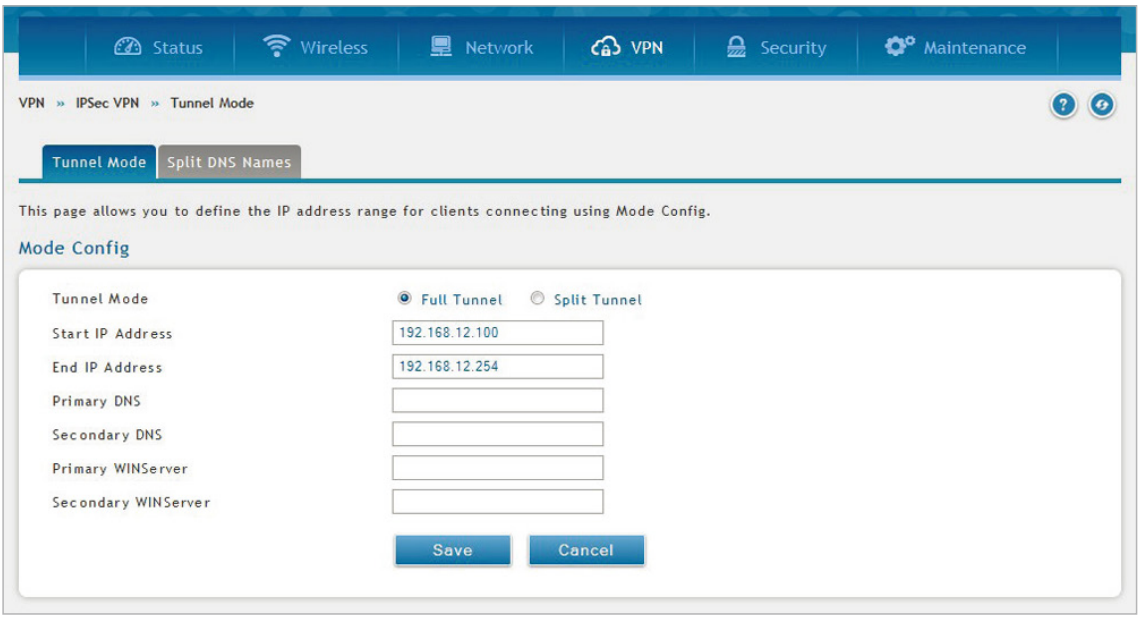

図 7-4　Tunnel Mode > Tunnel Mode タブ画面

2. 以下の項目を設定します。

項目	説明
Tunnel Mode	「Full Tunnel」（フルトンネル）または「Split Tunnel」（スプリットトンネル）を選択します。フルトンネルでは（インターネットまたはリモートサーバに向かう）すべてのパケットがトンネルを通過しますが、スプリットトンネルではインターネットに向かうトラフィックはトンネルを通過しません。
Start IP Address	このプールに割り当てられる最初のアドレスを入力します。
End IP Address	このプールに割り当てられる最後のアドレスを入力します。
Primary DNS	プライマリ DNS サーバは、このルータに接続するクライアントがドメイン名を解決するために使用します。トンネルモードがスプリットトンネルである場合、DNS サーバを内部のドメイン名サーバとする必要があります。
Secondary DNS	セカンダリ DNS サーバは、このルータに接続するクライアントがドメイン名を解決するために使用します。トンネルモードがスプリットトンネルである場合、DNS サーバを内部のドメイン名サーバとする必要があります。
Primary WIN Server	プライマリ WIN サーバを設定します。
Secondary WIN Server	セカンダリ WIN サーバを設定します。

3. 「Save」をクリックし、設定を適用します。

Split DNS Names（スプリット DNS 名）

スプリット DNS では同一のドメインに 2 つのゾーンを作成できます。1 つは内部ネットワークに使用し、もう 1 つは外部ネットワークに使用します。スプリット DNS では、名前解決の際に内部ホストは内部ドメインネームサーバに、外部ホストは外部ドメインネームサーバに向かうように処理されます。

1. **VPN > IPSec VPN > Tunnel Mode > Split DNS Names タブ**の順にメニューをクリックし、以下の画面を表示します。

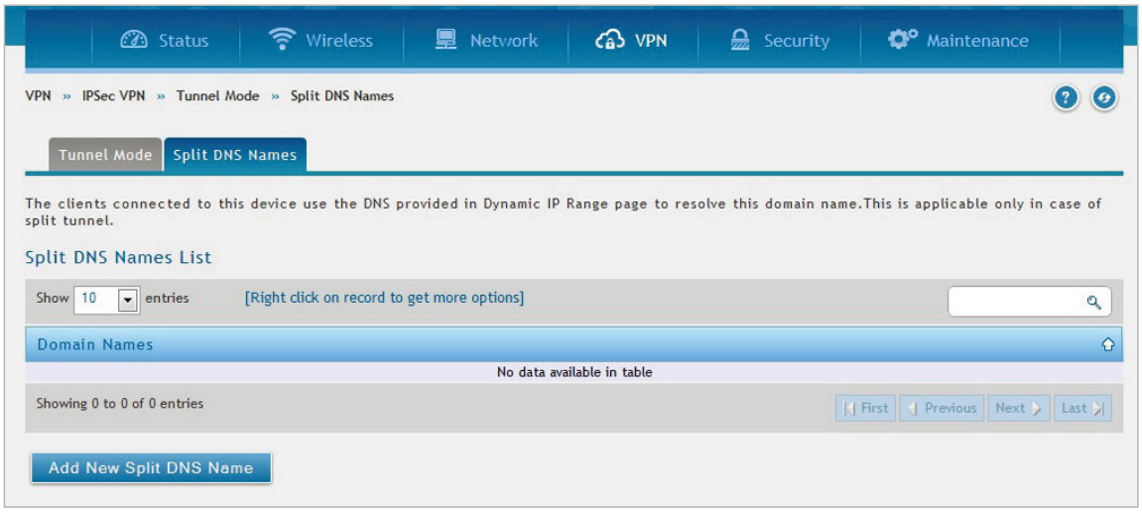

図 7-5　Tunnel Mode > Split DNS Names タブ 画面

2. 「Add New Split DNS Name」をクリックして以下の画面を表示します。

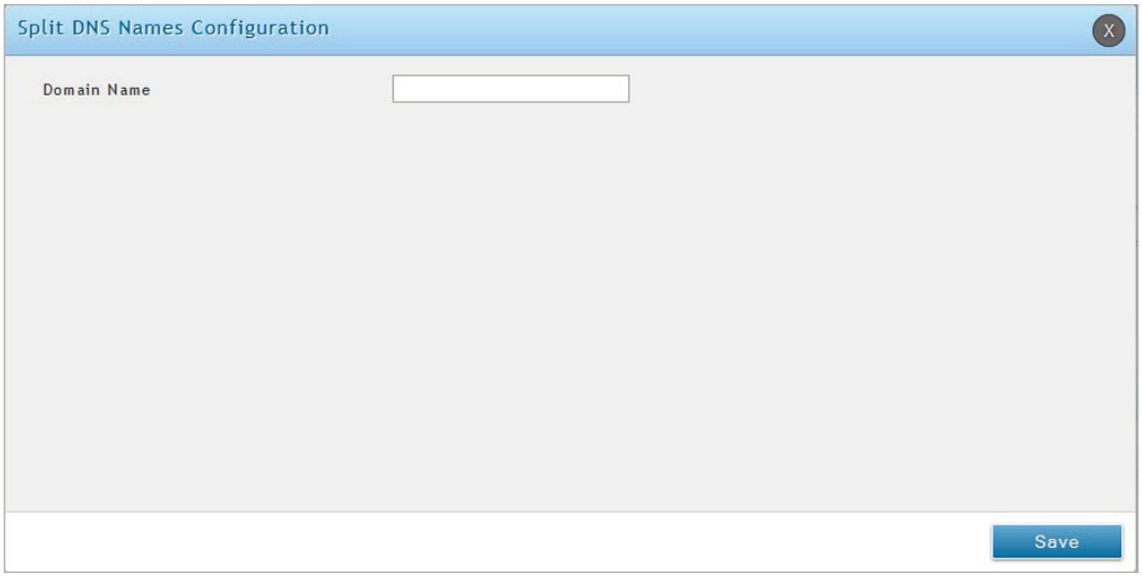

図 7-6　Split DNS Names Configuration 画面

3. 「Domain Name」にドメイン名を入力します。

4. 「Save」をクリックし、設定を適用します。

DHCP Range（IP アドレス範囲の設定）

VPN > IPSec VPN > DHCP Range

DHCP over IPSec を使用して接続するクライアント用の IP アドレス範囲を定義します。
初期値は 192.168.12.0 サブネットの範囲です。

1. **VPN > IPSec VPN > DHCP Range** の順にメニューをクリックし、以下の画面を表示します。

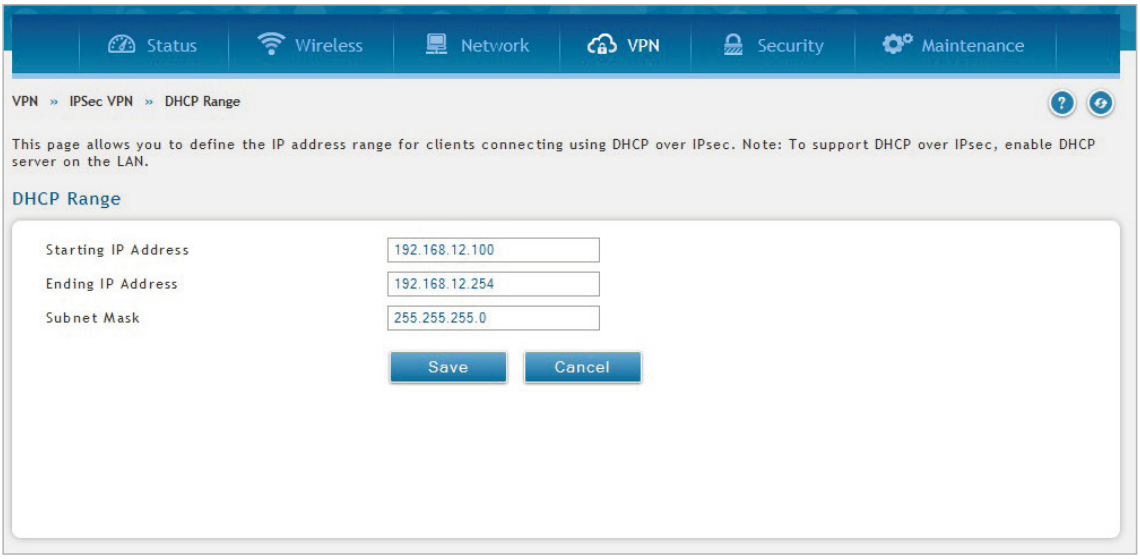

図 7-7　　DHCP Range 画面

2. 「Starting IP Address」「Ending IP Address」に IP アドレスを入力し、IP アドレス範囲を指定します。

3. 「Subnet Mask」でサブネットマスクを指定します。

4. 「Save」をクリックし、設定を適用します。

Certificate（認証証明書）

VPN > IPSec VPN > Certificate

本ルータは IPSec VPN 認証にデジタル証明書を使用します。VeriSign（ベリサイン）などの認証局（CA）からデジタル証明書を入手するか、または、本ゲートウェイで利用可能な機能を使用して自己署名証明書を生成することができます。

本ルータには自己署名証明書が存在し、ご使用のネットワーク要件に応じて認証局によって署名されたものと置き換えることができます。CA 証明書はサーバのアイデンティティに関する強力な保証を提供しており、多くの企業ネットワーク VPN ソリューションにおいて必要条件となっています。

Trusted Certificates（トラスト証明書）

現在ルータにロードされている証明書（CA および自己署名の両方）のリストを参照することができます。トラスト（CA）証明書のリストには以下の証明書データが表示されます。

項目	説明
CA Identity (Subject Name)	証明書発行先の人物または組織です。
Issuer Name	この証明書を発行した CA 名です。
Expiry Date & Time	このトラスト証明書が無効になる日付です。

1. **VPN > IPSec VPN > Certificate > Trusted Certificates タブ**の順にメニューをクリックし、以下の画面を表示します。

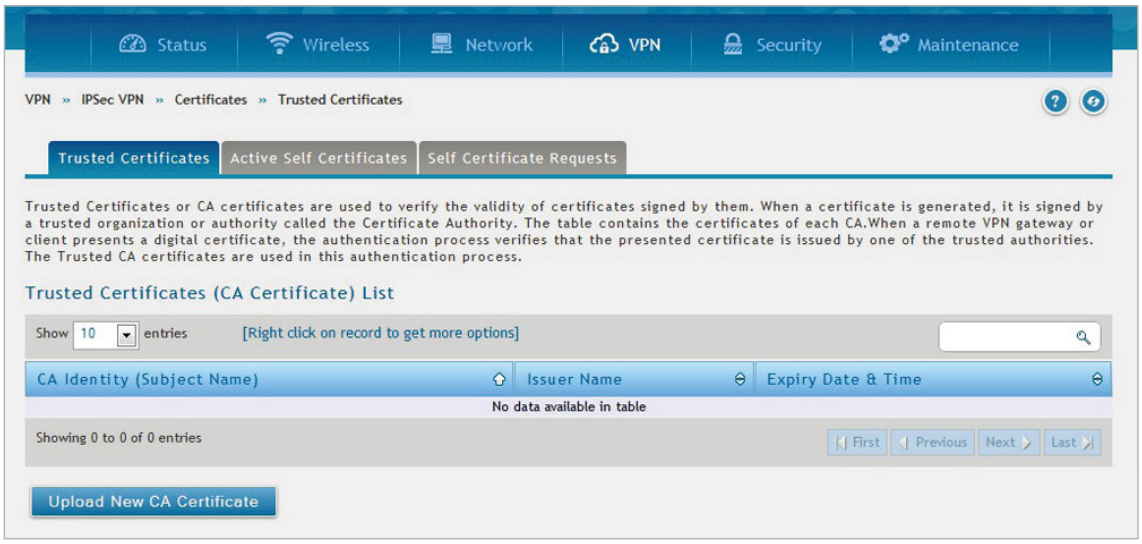

図 7-8　Certificate > Trusted Certificates タブ画面

2. 「Upload New CA Certificate」をクリックします。
3. 以下の画面で「参照 /Browse」をクリック → 証明書の場所を指定し「Save」をクリックします。

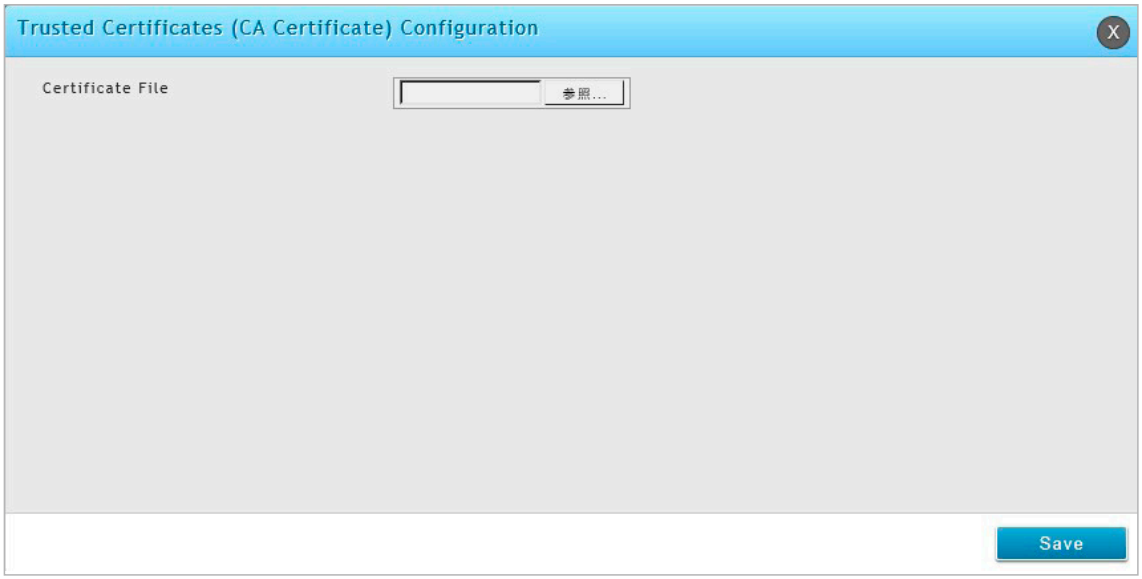

図 7-9　Trusted Certificates (CA Certificate) Configuration 画面

Active Self Certificates（自己証明書）

自己証明書は、CA によって発行された、ご使用のデバイスを保障する証明書です。CA のアイデンティティ保護が必要ない場合には、自己署名証明書を使用します。Active Self Certificate タブでは、現在ルータにロードされている自己証明書を表示します。

アップロードされている各自己証明書に対して、以下の情報が表示されます。

項目	説明
Name	この証明書の名前（識別名）です。
Subject Name	この証明書の所有者として表示される名前です。通常、公式に登録されたビジネスまたは会社名です。
Serial Number	シリアル番号は CA によって証明書を識別するために使用されます。
Issuer Name	この証明書を発行した（署名した）CA 名です。
Expiry Time	署名証明書が無効になる日付です。期限が切れる前に証明書を更新する必要があります。

1. **VPN > IPSec VPN > Certificate > Active Self Certificates タブ**の順にメニューをクリックし、以下の画面を表示します。

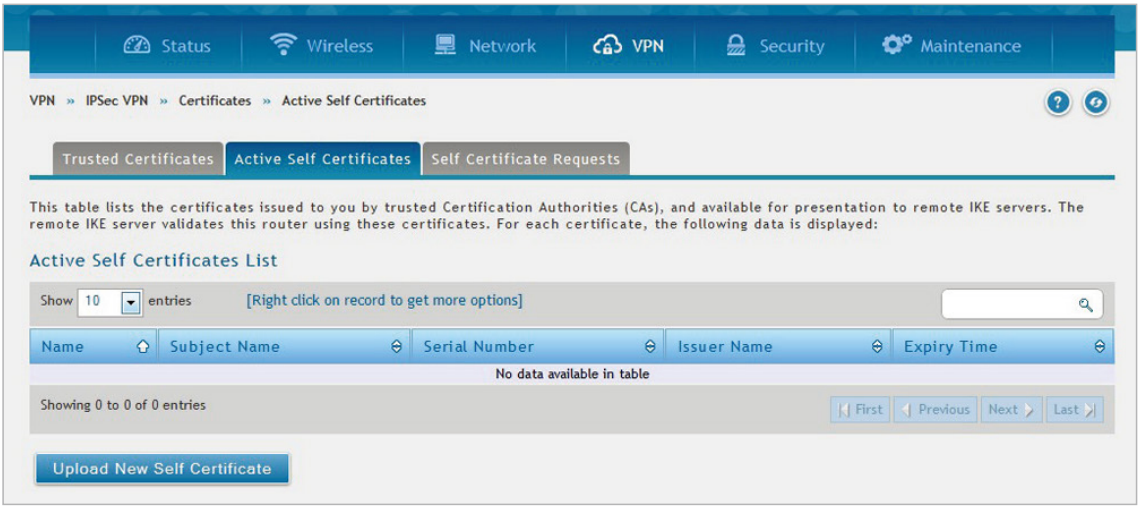

図 7-10　Certificate > Active Self Certificates タブ画面

2. 「Upload New Self Certificate」をクリックします。
3. 以下の画面で「参照 /Browse」をクリック → 自己証明書の場所を指定し「Upload」をクリックします。

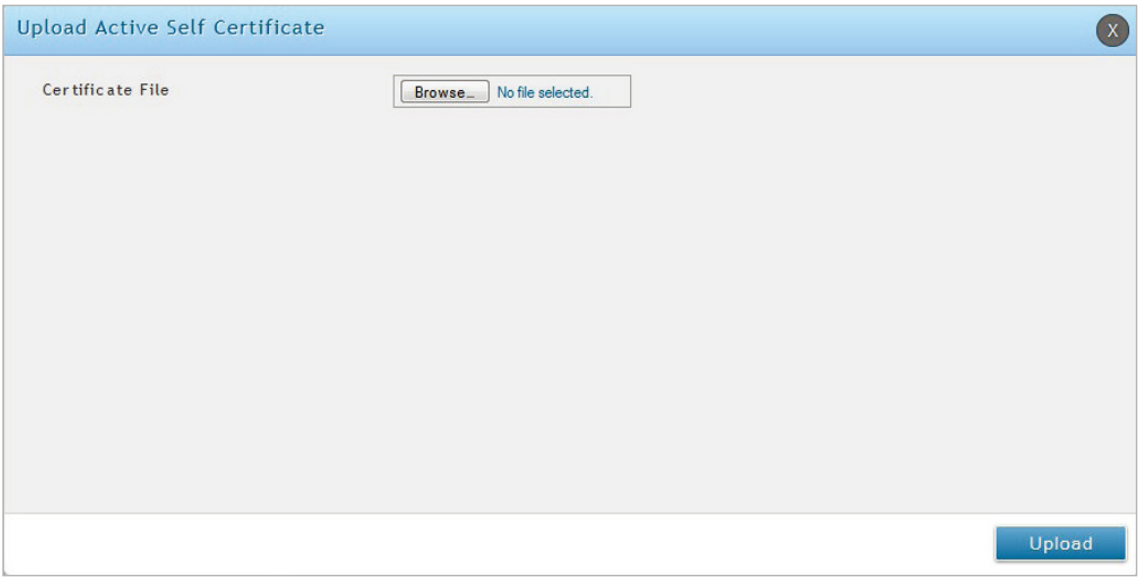

図 7-11　Upload Active Self Certificate 画面

Self Certificate Requests（自己証明書リクエスト）

自己証明書を CA で署名してもらうには、ルータで識別子パラメータを入力して証明書署名要求（CSR）を生成し、生成したファイルを CA に提出します。CA のトラスト証明書及び CA によって署名されたサーバ証明書をアップロードし、ゲートウェイの正当性を証明する自己証明書をアクティブにすることができます。自己証明書は、ピアとの IPsec および SSL 接続でゲートウェイの信頼性を検証するために使用されます。

1. **VPN > IPSec VPN > Certificate > Self Certificate Requests タブ**の順にメニューをクリックし、以下の画面を表示します。

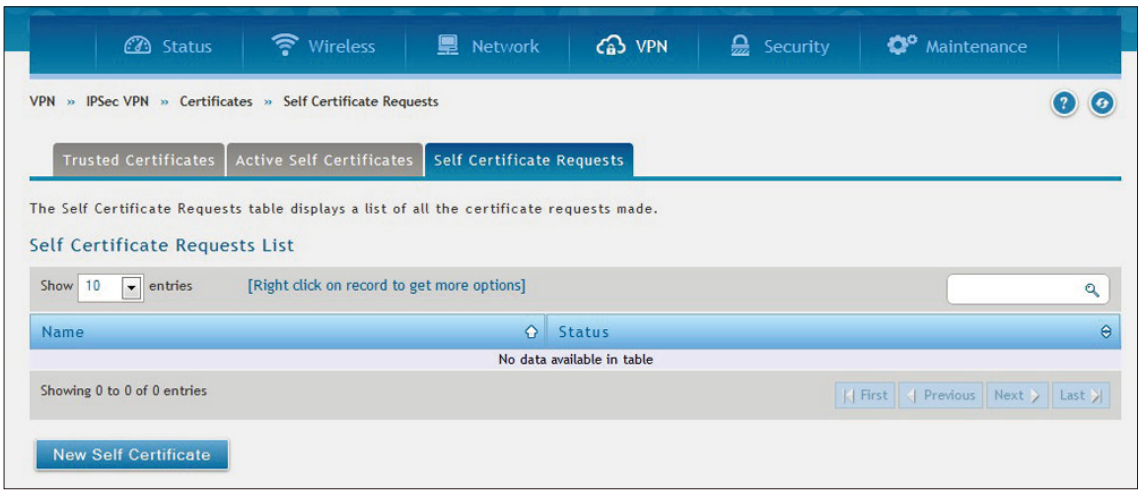

図 7-12　Certificate > Self Certificate Requests タブ画面

2. 自己証明書を追加する場合、「New Self Certificate」をクリックし以下の画面を表示します。

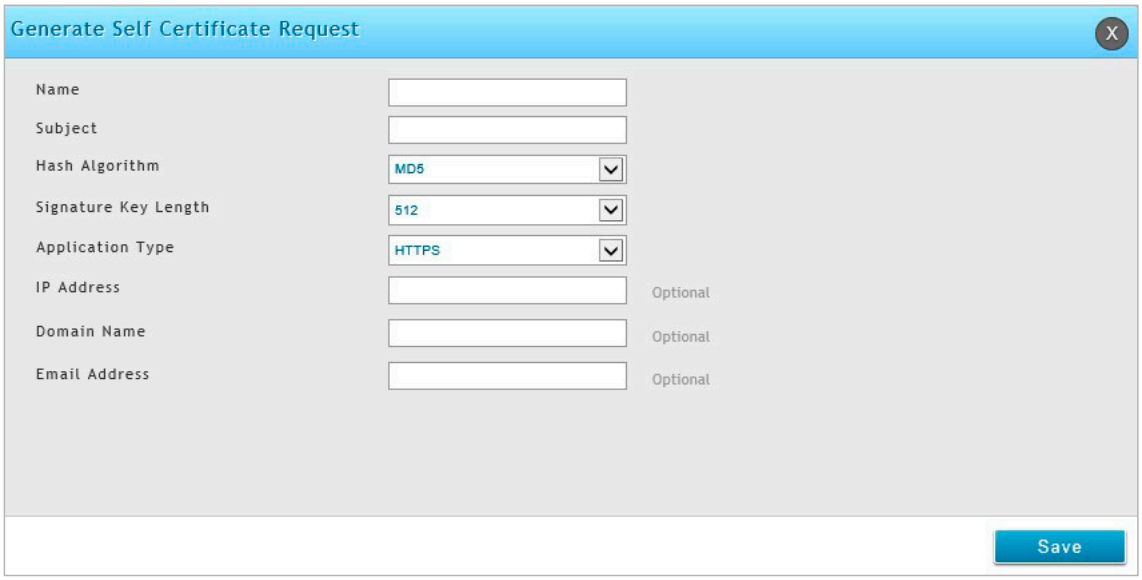

図 7-13　Generate Self Certificate Request 画面

3. 以下の項目を設定します。

項目	説明
Name	証明書の名前（識別子）を入力します。
Subject	生成される証明書の CN（Common Name）エントリが含まれます。サブジェクト名は通常次のフォーマットによって定義されます。 CN=<device name/ デバイス名 >, OU=<department/ 部署 >, O=<organization/ 組織 >, L=<city/ 市町 >, ST=<state/ 県、州 >, C=<country/ 国 > （例 : CN=router1, OU=my_company, O=mydept, L=SFO, C=US.）
Hash Algorithm	アルゴリズムを以下から指定します。 「MD5」「SHA1」「SHA256」「SHA384」「SHA512」
Signature Key Length	シグニチャキーの長さを「512」「1024」「2048」から指定します。
Application Type	アプリケーションの種類を「HTTPS」「IPSec」から指定します。
IP Address	IP アドレスを入力します。本項目はオプションです。
Domain Name	ドメイン名を入力します。本項目はオプションです。
Email Address	メールアドレスを入力します。本項目はオプションです。

4. 「Save」をクリックし、設定を適用します。

追加した自己証明書は **Certificate > Self Certificate Requests タブ**画面に表示されます。

右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Easy VPN Setup（VPN セットアップ）

VPN > IPSec VPN > Easy VPN Setup
エクスポートされた IPSec VPN ポリシーをアップロードします。

1. **VPN > IPSec VPN > Easy VPN Setup** の順にメニューをクリックします。
2. 以下の画面で「参照 /Browse」をクリック　→　ポリシーの場所を指定し「Upload」をクリックします。

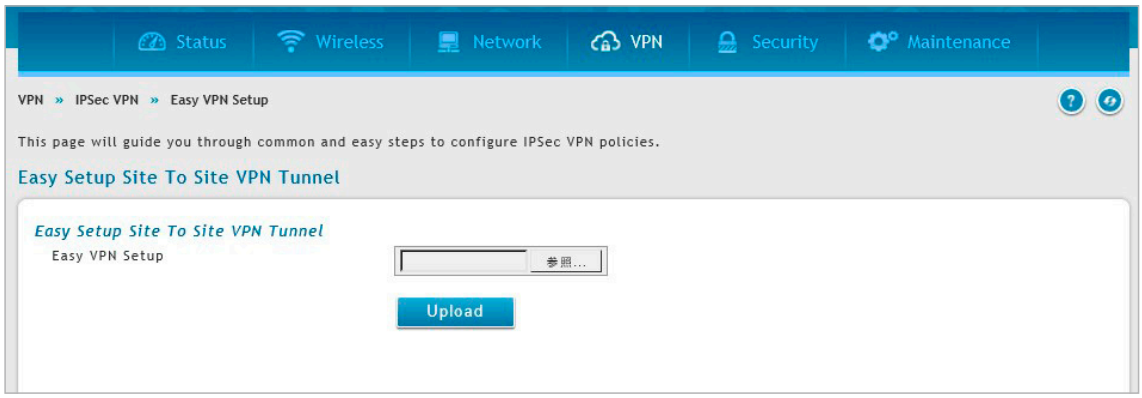

図 7-14　Easy VPN Setup 画面

アップロード後、**VPN > IPSec VPN > Policies** 画面に読み込まれた VPN が表示されます。
右クリックし「Edit」（編集）、「Delete」（削除）を実行できます。

One To One Mapping（One To One マッピング）

VPN > IPSec VPN > Certificate > One To One Mapping
設定済みの「IPsec One To One マッピング」のリストを表示します。また、「One To One マッピング」の追加、編集、削除を行うことができます。

1. **VPN > IPSec VPN > One To One Mapping** の順にメニューをクリックし、以下の画面を表示します。

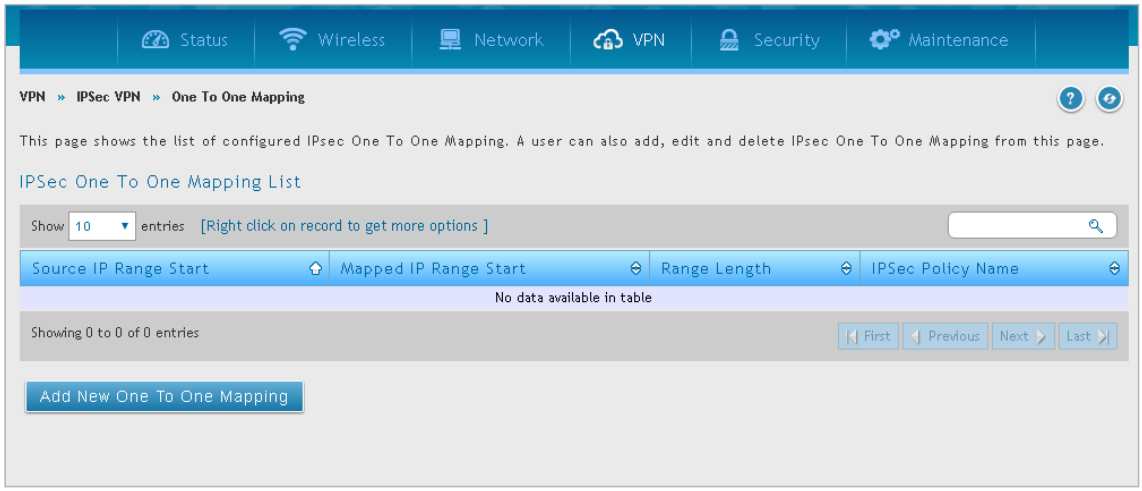

図 7-15　One To One Mapping 画面

2. マッピングリストを追加する場合、「Add New One To One Mapping」をクリックし以下の画面を表示します。

図 7-16　IPSec One To One Mapping Configuration 画面

3. 以下の項目を設定します。

項目	説明
Source IP Range Start	One to One マッピングルールの開始 IP アドレスになる、プライベート（LAN）IP サブネットの IP アドレスを入力します。
Mapped IP Range Start	プライベート LAN IP サブネットへの One to One マッピングサブネットの、マッピング範囲開始 IP として機能する IP アドレスを入力します。 この IP は、リモートホストからのトラフィックをローカル LAN ホスト / LAN ホストのサブネットにマッピングするために使用されます。ローカルデバイスの IPSec ポリシーの「ローカル開始 IP アドレス」およびリモートデバイスの IPSec ポリシーの「リモート開始 IP アドレス」と同じである必要があります。
Range Length	プライベート / パブリックアドレスの One to One マッピング範囲を入力します。 設定可能範囲：1-254
IPSec Policy Name	One To One マッピングルールに紐付ける IPSec ポリシーを選択します。

4. 「Save」をクリックし、設定を適用します。

PPTP VPN（PPTP VPN 設定）

VPN > PPTP VPN

PPTP Server（PPTP VPN サーバ設定）

VPN > PPTP VPN > PPTP Server

本ルータを介して PPTP VPN 接続を確立することができます。PPTP を有効にし、LAN/WAN PPTP クライアントユーザが接続するためのサーバの設定を行います。PPTP サーバが有効化されると、許可された IP 範囲に存在する PPTP クライアントは、ルータの PPTP サーバに到達できるようになります。その後、PPTP サーバ（トンネルのエンドポイント）によって認証されると、PPTP クライアントはルータによって管理されたネットワークに接続可能となります。PPTP クライアントに割り当てる IP アドレス範囲は LAN サブネットと同じにすることができます。また、PPTP サーバはローカルな PPTP ユーザ認証をデフォルトとしますが、外部認証サーバを使用することも可能です。

1. **VPN > PPTP VPN > PPTP Server** の順にメニューをクリックし、以下の画面を表示します。

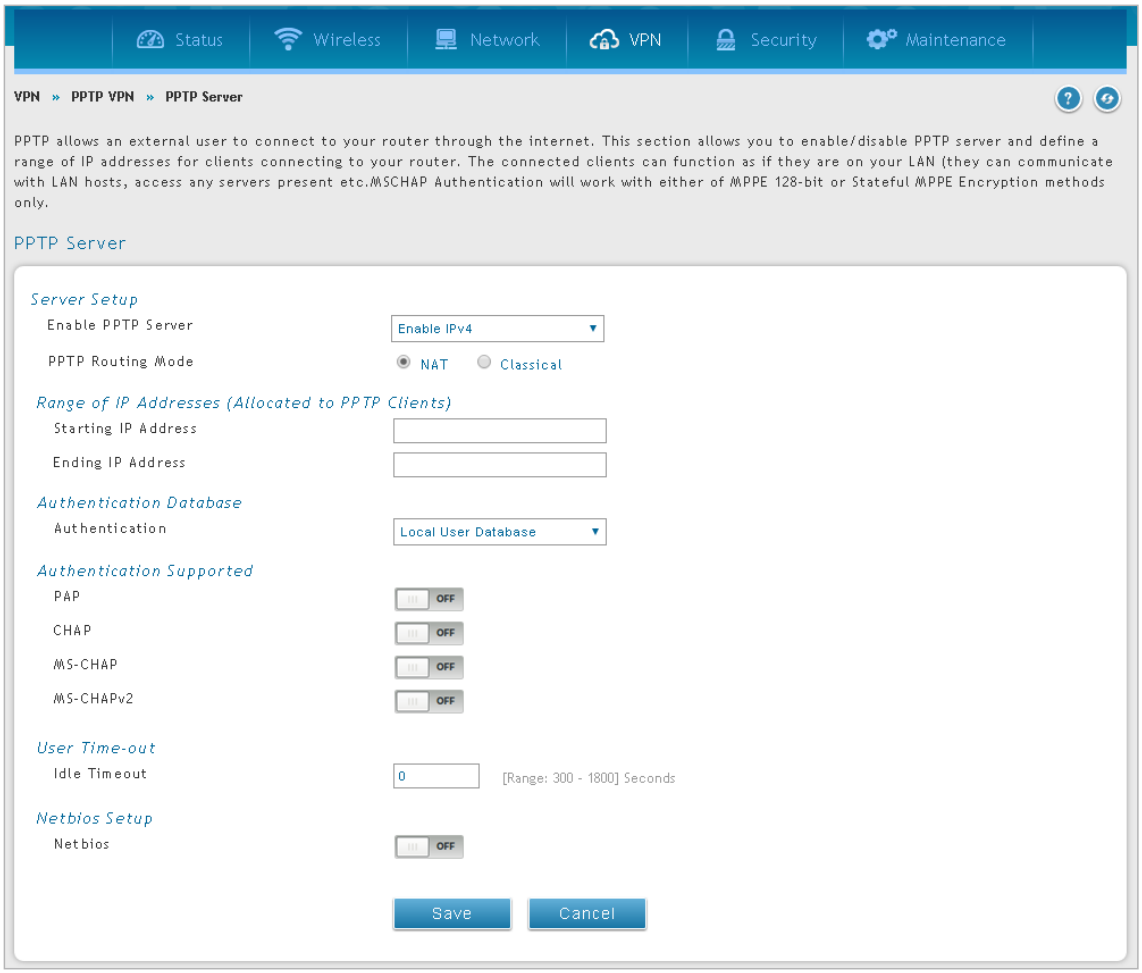

図 7-17　PPTP Server 画面

2. 以下の項目を設定します。

項目	説明
Server Setup	
Enable PPTP Server	PPTP サーバを有効にするモードを選択します。: Enable IPv4 (IPv4)、Enable IPv6 (IPv6)、Disable (無効)
PPTP Routing Mode	PPTP ルーティングモード を「NAT」または「Classical」から選択します。
Range of IP Addresses (Allocated to PPTP Client)	
Starting IP Address	PPTP クライアントに割り当てる IP アドレス範囲の開始 IP アドレスを入力します。
Ending IP Address	PPTP クライアントに割り当てる IP アドレス範囲の終了 IP アドレスを入力します。
IPv6 Prefix	IPv6 モードを選択した場合、IPv6 プレフィックスを入力します。
IPv6 Prefix Length	IPv6 モードを選択した場合、IPv6 プレフィックス長を入力します。
Authentication Database	
Authentication	認証タイプを選択します。
Authentication Supported	
PAP	PAP 認証方式のサポートを有効にします。
CHAP	CHAP 認証方式のサポートを有効にします。
MS-CHAP	MS-CHAP 認証方式のサポートを有効にします。
MS-CHAPv2	MS-CHAPv2 認証方式のサポートを有効にします。
User Time-Out	
Idle Timeout	指定したタイムアウトを経過してもユーザからのトラフィックがない場合、接続は切断されます。
Netbios Setup	
Netbios	「ON」にすると、VPN トンネルにおける NetBIOS ブロードキャストの通過を許可します。

3. 「Save」をクリックし、設定を適用します。

PPTP Client（PPTP クライアント）

VPN > PPTP VPN > PPTP Client

本ルータに PPTP VPN クライアントを設定します。PPTP クライアントを使用し、PPTP サーバの存在するリモートネットワークに接続します。クライアント有効化後、**Status > Active VPNs** 画面で PPTP VPN トンネルの接続を確立します。

1. **VPN > PPTP VPN > PPTP Client** の順にメニューをクリックし、以下の画面を表示します。

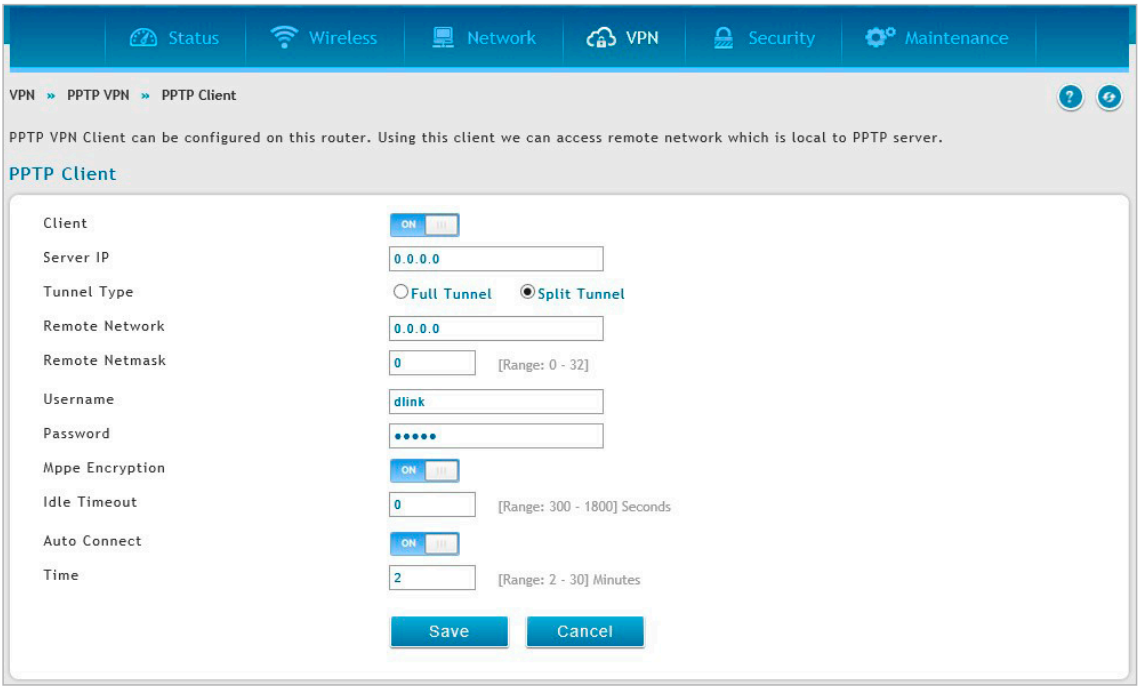

図 7-18　PPTP Client 画面

2. 以下の項目を設定します。

項目	説明
Client	PPTP クライアントを有効にします。
Server IP	接続する PPTP サーバの IP アドレスを指定します。
Tunnel Type	トンネルタイプを「Full Tunnel」（フルトンネル）または「Split Tunnel」（スプリットトンネル）から選択します。
Remote Network	PPTP サーバにとってローカルとなるリモートネットワークアドレスを指定します。トンネルタイプに「Split Tunnel」を選択した場合のみ表示されます。
Remote Netmask	リモートネットワークのサブネットマスクを指定します。トンネルタイプに「Split Tunnel」を選択した場合のみ表示されます。
Username	PPTP ユーザ名を指定します。
Password	PPTP パスワードを指定します。
Mppe Encryption	「ON」にして Microsoft Point-to-Point Encryption (MPPE) を有効にします。
Idle Timeout	アイドル状態時に PPTP サーバから切断するまでの時間を指定します。 • 設定可能範囲：300-1800（秒） • 初期値：0（秒）
Auto Connect	自動接続機能を有効または無効にします。 クライアントが切断された後、「Time」で指定した時間を過ぎると再度サーバへの接続を自動的に試します。
Time	再接続までの時間を入力します。 クライアントが切断された後、「Time」で指定した時間を過ぎると再度サーバへの接続を自動的に試行します。 • 設定可能範囲：2-30（分） • 初期値：2（分）

3. 「Save」をクリックし、設定を適用します。

PPTP Active Users（PPTP アクティブユーザリスト）

VPN > PPTP VPN > PPTP Active Users

PPTP の接続状況について表示します。

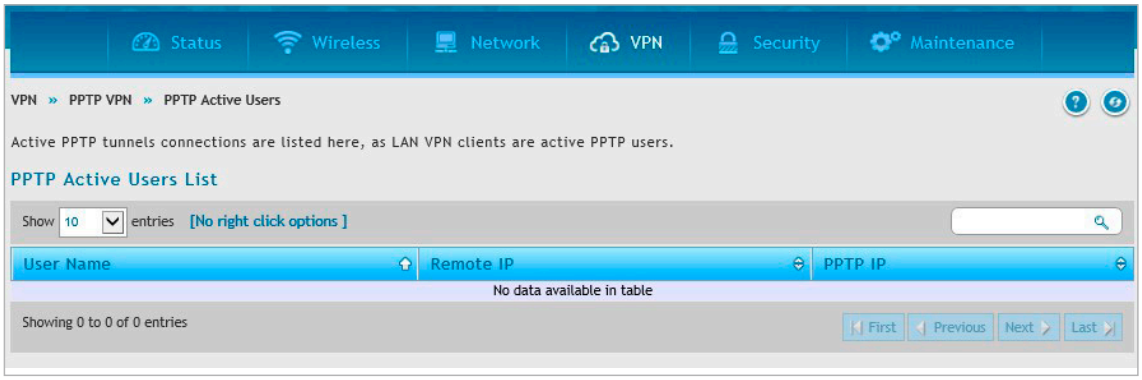

図 7-19　PPTP Active Users List 画面

項目	説明
User Name	現在接続中のユーザ名が表示されます。'*' が表示されている場合は、認証なしで接続中のユーザを意味します。
Remote IP	PPTP サーバによってユーザに割り当てられている IP アドレスが表示されます。
PPTP IP	サーバのローカル IP が表示されます。

PPTP サーバと L2TP サーバのトンネル数の上限値は以下のとおりです。

	DSR-1000/1000AC	DSR-500
PPTP トンネル数	25	15
L2TP トンネル数	25	15
合計	50	30

L2TP VPN（L2TP VPN 設定）

VPN > L2TP VPN

L2TP Server（L2TP VPN サーバ設定）

VPN > L2TP VPN > L2TP Server
本ルータを介して L2TP VPN 接続を確立することができます。
L2TP を有効にし、LAN/WAN L2TP クライアントユーザが接続するためのサーバの設定を行います。
L2TP サーバが有効化されると、許可された IP 範囲に存在する L2TP クライアントは、ルータの L2TP サーバに到達できるようになります。
その後、L2TP サーバ（トンネルのエンドポイント）によって認証されると、L2TP クライアントはルータによって管理されたネットワークに接続可能となります。

L2TP クライアントに割り当てる IP アドレス範囲は LAN サブネットと同じにすることはできません。
また、L2TP サーバはローカルな L2TP ユーザ認証をデフォルトとしますが、外部認証サーバを使用することも可能です。

1. **VPN > L2TP VPN > L2TP Server** の順にメニューをクリックし、以下の画面を表示します。

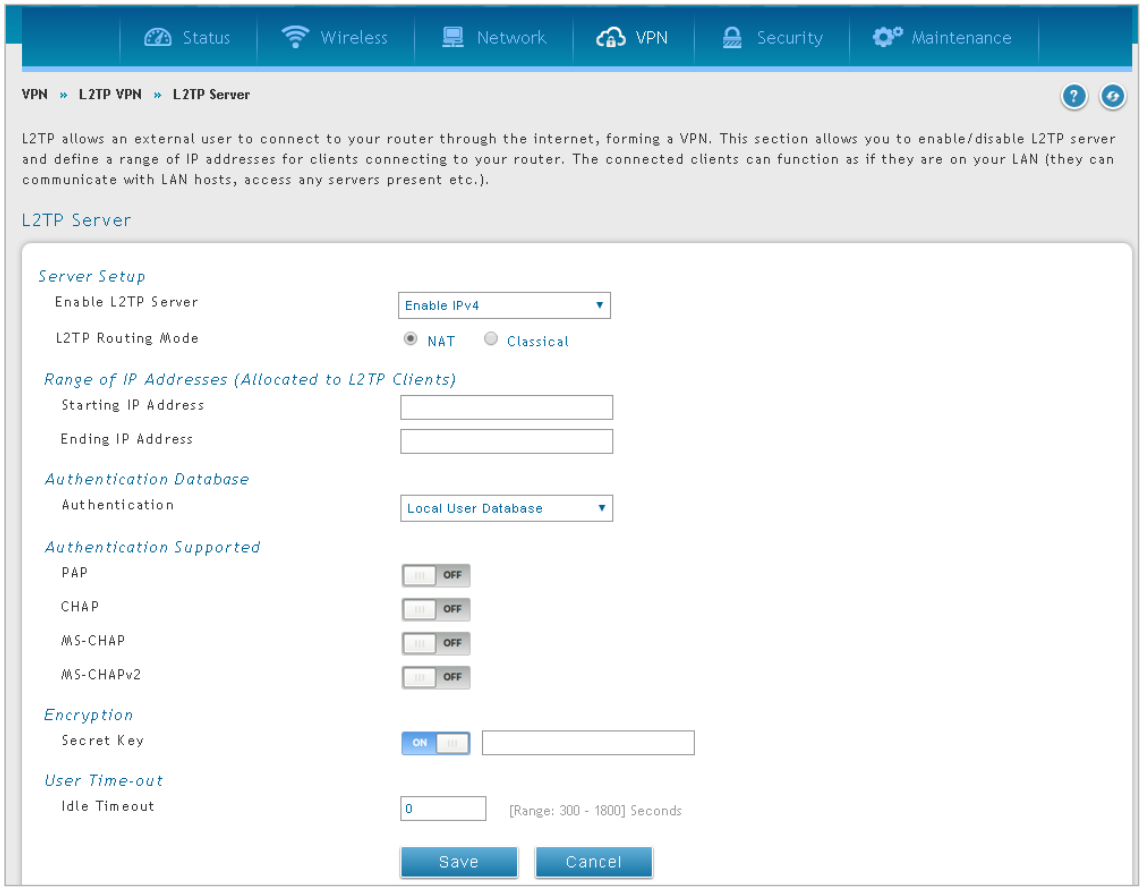

図 7-20　L2TP Server 画面

2. 以下の項目を設定します。

項目	説明
Server Setup	
Enable L2TP Server	L2TP サーバを IPv4 または IPv6 で有効、または無効にします。 -「Enable IPv4」（IPv4 で有効） -「Enable IPv6」（IPv6 で有効） -「Disable」（無効）
L2TP Routing Mode	L2TP ルーティングモードを「NAT または「Classical」から選択します。
Range of IP Addresses (Allocated to PPTP Client)	
Starting IP Address	L2TP クライアントに割り当てる IP アドレス範囲の開始 IP アドレスを入力します。
Ending IP Address	L2TP クライアントに割り当てる IP アドレス範囲の終了 IP アドレスを入力します。
IPv6 Prefix	IPv6 モードを選択した場合、IPv6 プレフィックスを入力します。
IPv6 Prefix Length	IPv6 モードを選択した場合、IPv6 プレフィックス長を入力します。
Authentication Database	
Authentication	認証タイプを選択します。
Authentication Supported	

項目	説明
PAP	PAP 認証方式のサポートを有効にします。
CHAP	CHAP 認証方式のサポートを有効にします。
MS-CHAP	MS-CHAP 認証方式のサポートを有効にします。
MS-CHAPv2	MS-CHAPv2 認証方式のサポートを有効にします。
Encryption	
Secret Key	暗号鍵（暗号キー）を指定します。
User Time-Out	
Idle Timeout	指定したタイムアウトを経過してもユーザからのトラフィックがない場合、接続は切断されます。

3. 「Save」をクリックし、設定を適用します。

L2TP Client（L2TP VPN クライアント）

VPN > L2TP VPN > L2TP Client

L2TP VPN クライアントを設定します。このクライアントを使用して、L2TP サーバに対してローカルであるリモートネットワークにアクセスできます。クライアント有効化後、Status > Active VPNs 画面で L2TP VPN トンネルの接続を確率します。

1. **VPN > L2TP VPN > L2TP Client** の順にメニューをクリックし、以下の画面を表示します。

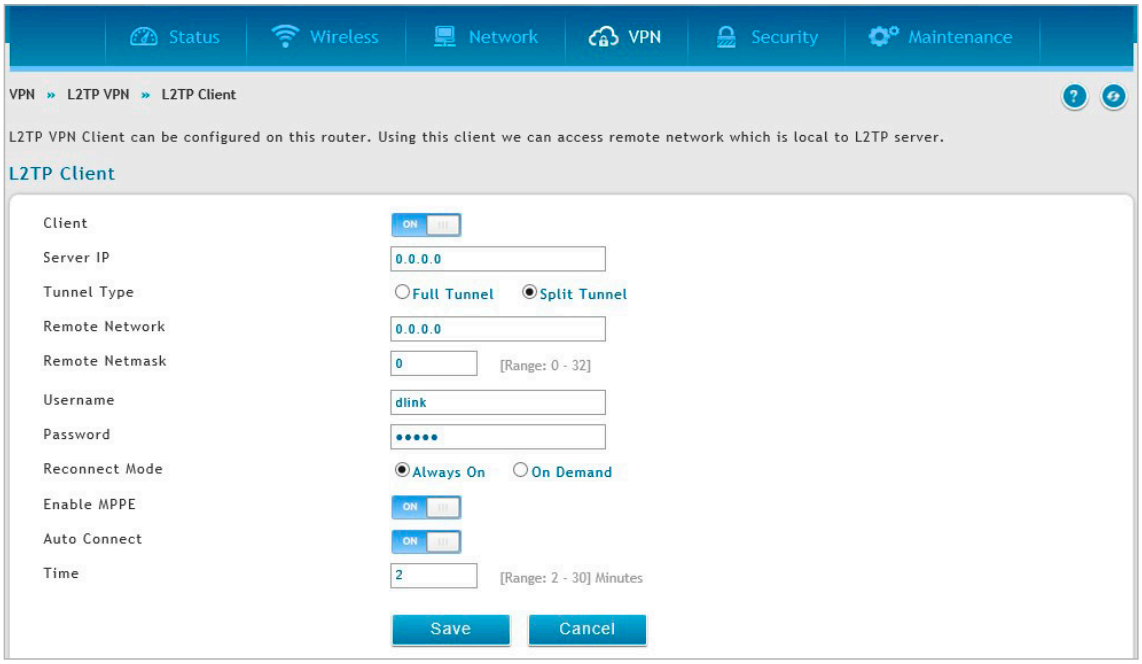

図 7-21　L2TP Client 画面

2. 以下の項目を設定します。

項目	説明
Client	L2TP クライアントを有効にします。
Server IP	接続する L2TP サーバの IP アドレスを指定します。
Tunnel Type	トンネルタイプを「Full Tunnel」（フルトンネル）または「Split Tunnel」（スプリットトンネル）から選択します。
Remote Network	L2TP サーバにとってローカルとなるリモートネットワークアドレスを指定します。トンネルタイプに「Split Tunnel」を選択した場合のみ表示されます。
Remote Netmask	リモートネットワークのサブネットマスクを指定します。トンネルタイプに「Split Tunnel」を選択した場合のみ表示されます。
Username	L2TP ユーザ名を指定します。
Password	L2TP パスワードを指定します。
Reconnect Mode	再接続モードを指定します。「Always On」「On Demand」から選択できます。
Maximum Idle Time	「On Demand」を選択した場合、アイドル状態時に L2TP サーバから切断するまでの時間を指定します。（単位：秒）
Enable MPPE	「ON」にして Microsoft Point-to-Point Encryption (MPPE) を有効にします。
Auto Connect	自動接続機能を有効または無効にします。 クライアントが切断された後、「Time」で指定した時間を過ぎると再度サーバへの接続を自動的に試します。
Time	「Auto Connect」を有効にした場合、自動接続を行うまでの時間（単位：分）を指定します。

3. 「Save」をクリックし、設定を適用します。

注意　L2TP クライアントが適切に設定・保存され L2TP サーバが起動すると、トンネルイニシエーションが自動的に開始されます。

L2TP Active Users（L2TP アクティブユーザリスト）

L2TP の接続状況について表示します。

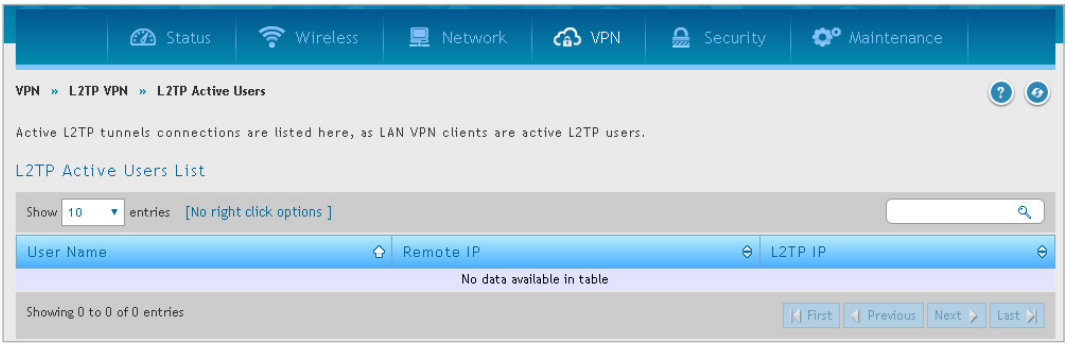

図 7-22　L2TP Active Users 画面

項目	説明
User Name	現在接続中のユーザ名が表示されます。'*' が表示されている場合は、認証なしで接続中のユーザを意味します。
Remote IP	PPTP サーバによってユーザに割り当てられている IP アドレスが表示されます。
L2TP IP	サーバのローカル IP が表示されます。

PPTP サーバと L2TP サーバのトンネル数の上限値は以下のとおりです。

	DSR-1000/1000AC	DSR-500
PPTP トンネル数	25	15
L2TP トンネル数	25	15
合計	50	30

SSL VPN（SSL VPN 設定）

VPN > SSL VPN
SSL VPN ポリシーはグローバル、グループまたはユーザレベルで作成できます。
各ポリシーの優先度は、高いほうからユーザレベルポリシー > グループレベルポリシー > グローバルポリシーの順です。

これらのポリシーは、LAN の特定のネットワークリソースや IP アドレス /IP 範囲、ルータによってサポートされる様々な SSL VPN サービスに適用できます。
利用可能なポリシーのリストは、ポリシータイプ（ユーザ、グループ、すべてのユーザ（グローバル））によってフィルタ可能です。

設定は以下の流れで行います。

（1）
SSL VPN ポリシーを追加するにあたり、ポリシーの適用先をユーザ、グループ、またはグローバル（すべての SSL VPN ユーザに適用）から指定します。
グループに適用する場合は、プルダウンメニューで利用可能な定義済みグループを選択します。
ユーザに適用する場合は、利用可能な定義済みユーザのリストから SSL VPN ユーザを選択します。

（2）
ポリシーの詳細を定義します。ポリシー名はこのルールに固有の識別子となります。
ルータの LAN における特定のネットワークリソース、IP アドレス、IP ネットワーク、またはすべてのデバイスにポリシーを割り当てることができます。
これら 4 つオプションごとに異なる設定フィールドが表示されます。
（例：定義済みリソースのリストからのネットワークリソースの選択、または IP アドレスの定義など）。
ポリシーをアドレスに適用する場合、ポート範囲 / ポート番号を定義できます。

（3）
選択したアドレスまたはネットワークリソースへのアクセスを許可 / 拒否する Permission 設定を行います。サポートしている SSL VPN サービス（VPN トンネル）のうち 1 つまたはすべてにポリシーを指定できます。

ポリシーは定義後にすぐに有効となります。
ポリシー名、適用する SSL サービス、送信先（ネットワークリソースまたは IP アドレス）、Permission 設定は、ルータの定義済みポリシー一覧の概要で確認することができます

注意　本機能を設定するには、**Maintenance > Management > Remote Management** 画面でリモート管理を有効にする必要があります。

SSL VPN 対応 OS/ ブラウザ一覧

SSL VPN 接続が可能な Windows OS、ブラウザ一覧は以下の通りです。

OS	ブラウザ
Windows 7（32bit）	IE9.0/11、Firefox 47.0.1
Windows 7（64bit）	IE9.0
Windows 8（32bit）	IE10.0、Firefox 47.0.1
Windows 8（64bit）	IE10.0
Windows 8.1（32bit）※	IE11、Firefox 47.0.1
Windows 8.1（64bit）※	IE11

※ Windows 8.1 上での IE11 ブラウザ経由の SSL VPN スプリットトンネル接続には対応していません。

SSL VPN Server Policy（SSL VPN ポリシー設定）

VPN > SSL VPN > SSL VPN Server Policy メニュー

SSL VPN ポリシーを設定します。

1. **VPN > SSL VPN > SSL VPN Server Policy** の順にメニューをクリックし、以下の画面を表示します。

図 7-23　SSL VPN Server Policy 画面

SSL VPN ポリシーの追加

1. 「Add New SSL VPN Server Policy」をクリックして、以下の画面を表示します。

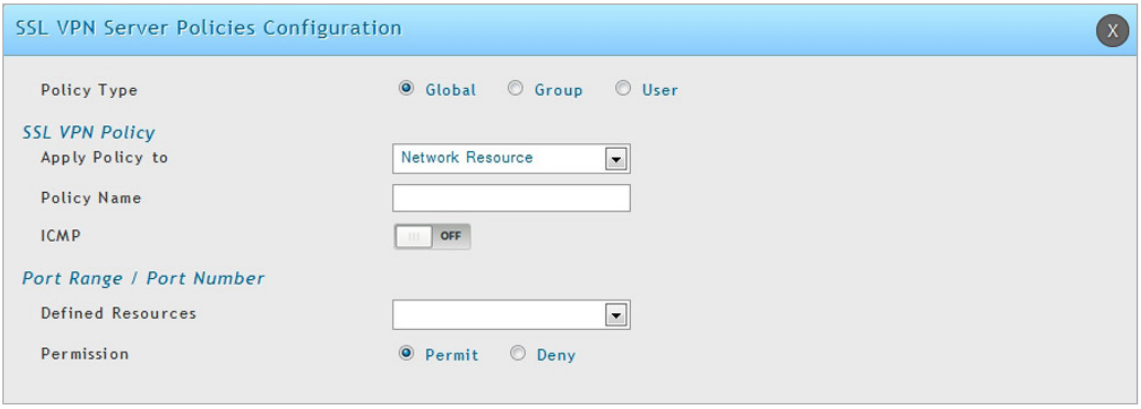

図 7-24　SSL VPN Server Policies Configuration（Network Resource）画面

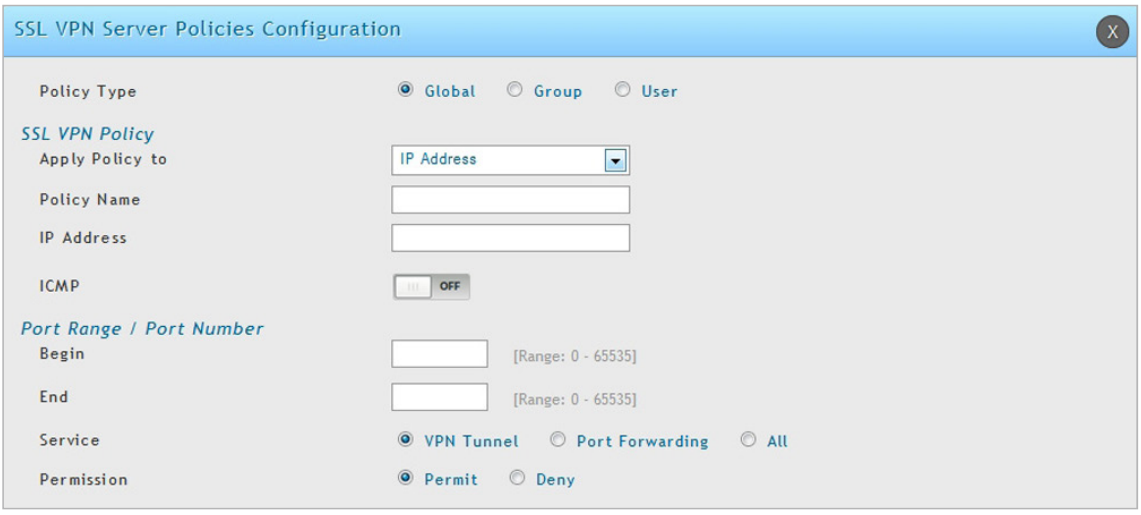

図 7-25　SSL VPN Server Policies Configuration（IP Address）画面

2. 以下の項目を設定します。

項目	説明
Policy Type	ポリシータイプを以下から選択します。 • 「Global」: ポリシーをすべての SSL VPN ユーザに適用します。 • 「Group」: ポリシーを選択したグループに適用します。 • 「User」: ポリシーを選択したユーザに適用します。
SSL VPN Policy	
Apply Policy to	ポリシーの適用先を以下から選択します。
Policy Name	ポリシーの識別名を指定します。
IP Address	ポリシーを「IPAddress」（IP アドレス）または「IP Netrwork」（IP ネットワーク）に適用する場合、IP アドレスを入力します。
Mask Length	ポリシーを「IP Netrwork」（IP ネットワーク）に適用する場合、マスク長（0-32）を入力します。
ICMP	ICMP トラフィックを含める場合は、「ON」に設定します。
Port Range / Port Number	
Begin / End	ポート範囲を入力します。すべての TCP/UDP ポートを含める場合は空欄にします。「Network Resource」を選択した場合は本設定は不要です。
Service	「VPN Tunnel」（VPN トンネル）、「Port Forwarding」（ポートフォワーディング）、または「All」（両方）を選択します。ネットワークリソースを選択した場合は本設定は不要です。
Defined Resources	「Network Resource」を選択した場合、プルダウンメニューから定義済みリソースを選択します。リソースが作成されていない場合は、「Resources（ネットワークリソース）」の手順を参照し、定義済みリソースを作成してください。
Permission	本ポリシーによって定義したリソースを「Permit」（許可）または「Deny」（拒否）に設定します。

3. 「Save」をクリックし、設定を適用します。

Portal Layouts（ポータルレイアウトの作成）

VPN > SSL VPN > Portal Layouts メニュー

リモート VPN ユーザの認証時に表示される、カスタムページを作成することができます。
カスタムページには、ログイン手順やサービス等の情報を記載することが可能です。

1. **VPN > SSL VPN > Portal Layouts** の順にメニューをクリックして、以下の画面を表示します。

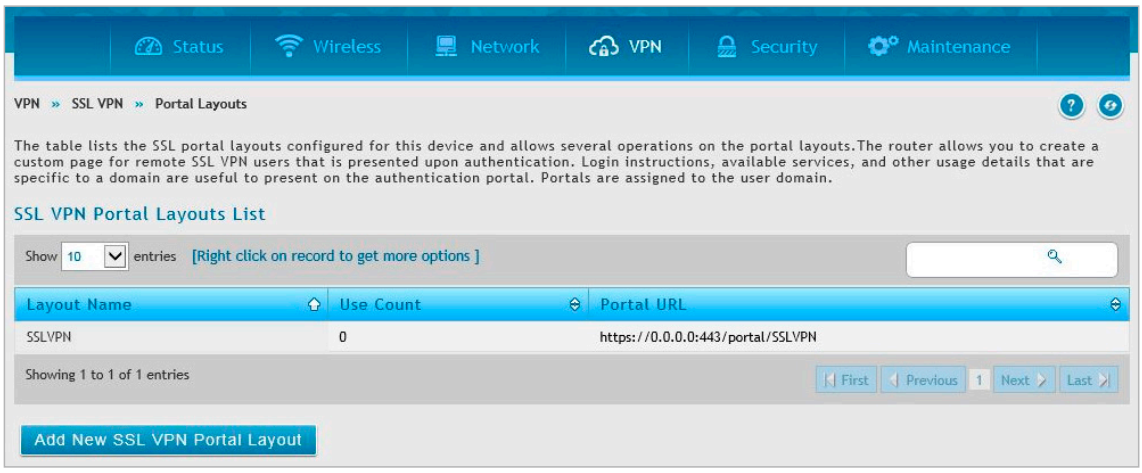

図 7-26　Portal Layouts 画面

2. レイアウトを追加する場合は、「Add New SSL VPN Portal Layout」をクリックし以下の画面を表示します。

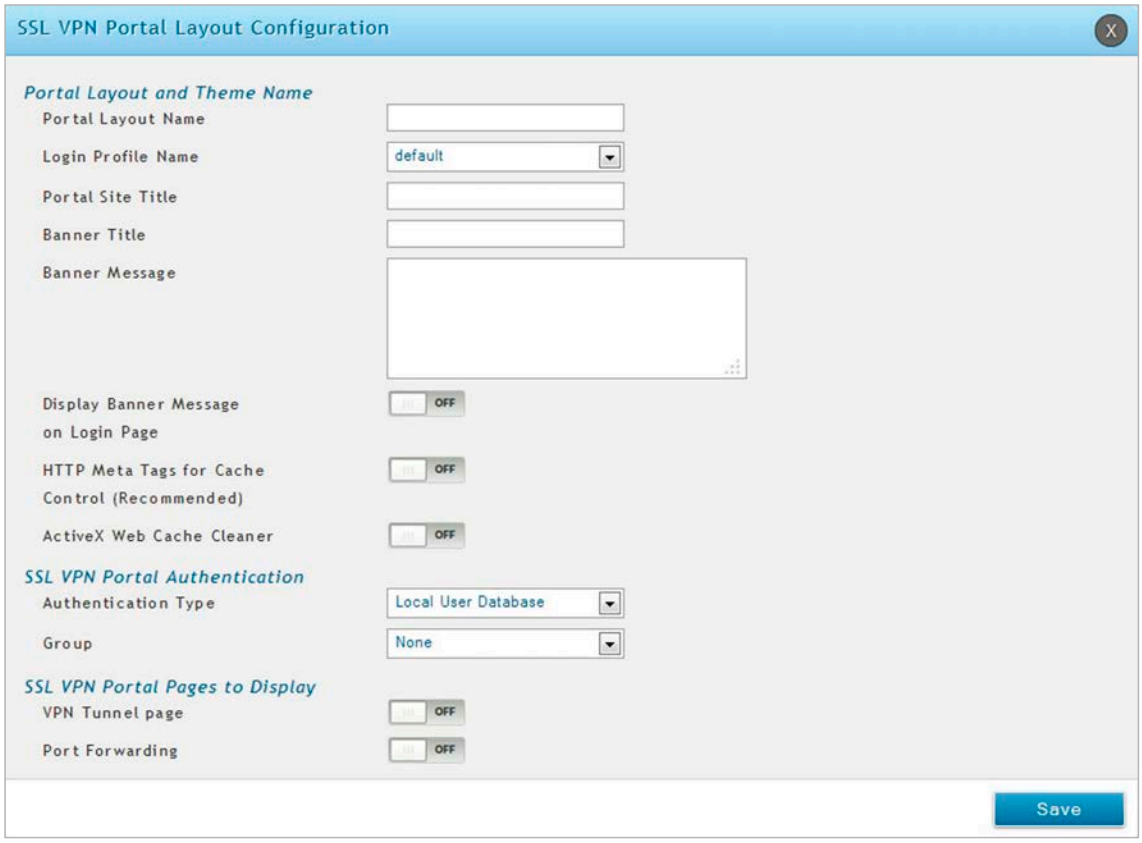

図 7-27　SSL VPN Portal Layout Configuration 画面

注意 ポータル LAN の IP アドレスの初期値は https://192.168.10.1/scgibin/userPortal/portal です。これは、ルータの Web GUI の SSL VPN メニューで「Portal URL」リンクをクリックしたときに開くページと同じです。

3. 以下の項目を設定します。

項目	説明
Portal Layout Name	ポータル名を英数字で入力します。ポータル名は、SSL ポータル URL パスの一部として使用されます。
Login Profile Name	ログインプロファイル名を指定します。
Portal Site Title	クライアントがこのポータルにアクセスする場合に表示されるポータル Web ブラウザ画面のタイトルです。 この項目はオプションです。この項目はオプションです。
Banner Title	ログイン前に SSL VPN クライアントに表示されるバナータイトルです。この項目はオプションです。
Banner Message	ログイン前に SSL VPN クライアントに表示されるバナーメッセージです。この項目はオプションです。
Display Banner Message on Login Page	ログインページのバナータイトル及びメッセージの表示を「ON」（表示）または「OFF」（非表示）に設定します。
HTTP Meta Tags for Cache Control (Recommended)	期限切れの Web ページとデータがクライアントの Web ブラウザキャッシュに保存されるのを防ぎます。 推奨される設定：「ON」
ActiveX Web Cache Cleaner	SSL VPN ポータルにユーザがログインする毎に、ActiveX キャッシュ制御 Web クリーナ機能がゲートウェイからクライアントのブラウザに対して実行されます。
Authentication Type	ドロップダウンメニューで認証の種類を選択します。
Group	ドロップダウンメニューで所属するグループを選択します。
VPN Tunnel Page	リモートユーザによる VPN トンネルページの閲覧を許可します。
Port Forwarding	リモートユーザによるポートフォワーディングページの閲覧を許可します。

4. 「Save」をクリックし、設定を適用します。

追加したレイアウトは Portal Layouts 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Resources（ネットワークリソース）

VPN > SSL VPN > Resources メニュー

ネットワークリソースは、LAN IP アドレスのサービスまたはグループです。
SSL VPN ポリシーを簡単に作成、設定するために使用します。
複数のリモート SSL VPN ユーザを対象に同様のポリシーを作成する場合、本機能によって設定時間を短縮できます。

ネットワークリソースを追加する場合、リソースを識別する固有名を作成し、サポートする SSL サービスのうちの 1 つまたはすべてを割り当てます。
作成したネットワークリソースを編集し、サービスに紐づくオブジェクトタイプ（IP アドレスまたは IP 範囲）を設定することも可能です。
必要に応じて、このリソースにネットワークアドレス、マスク長、ポート範囲 / ポート番号を定義できます。

ネットワークリソースの追加

1. **VPN > SSL VPN > Resources** の順にメニューをクリックして、以下の画面を表示します。

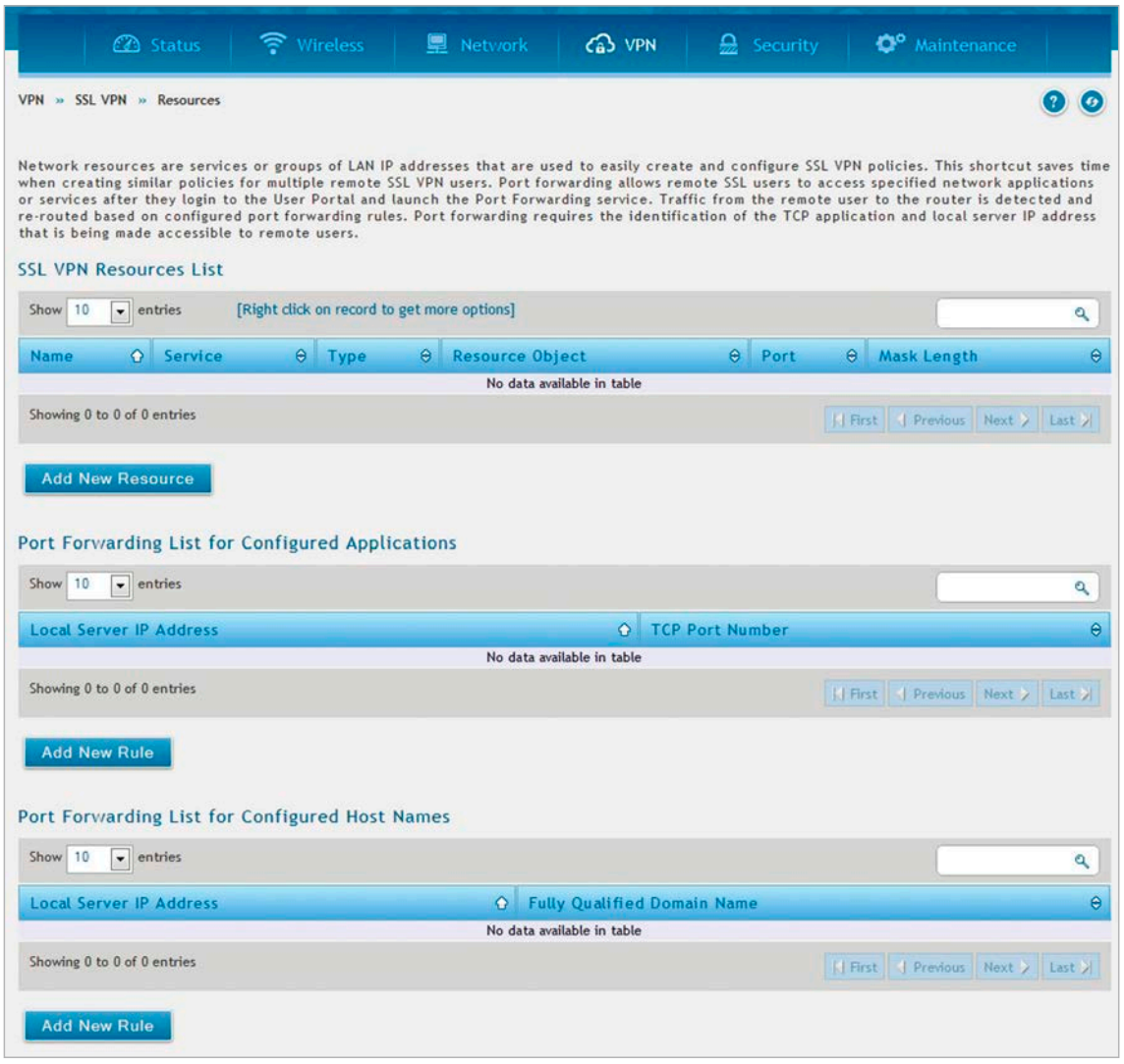

図 7-28　Resources 画面

2. 「Add New Resource」をクリックして、以下の画面を表示します。

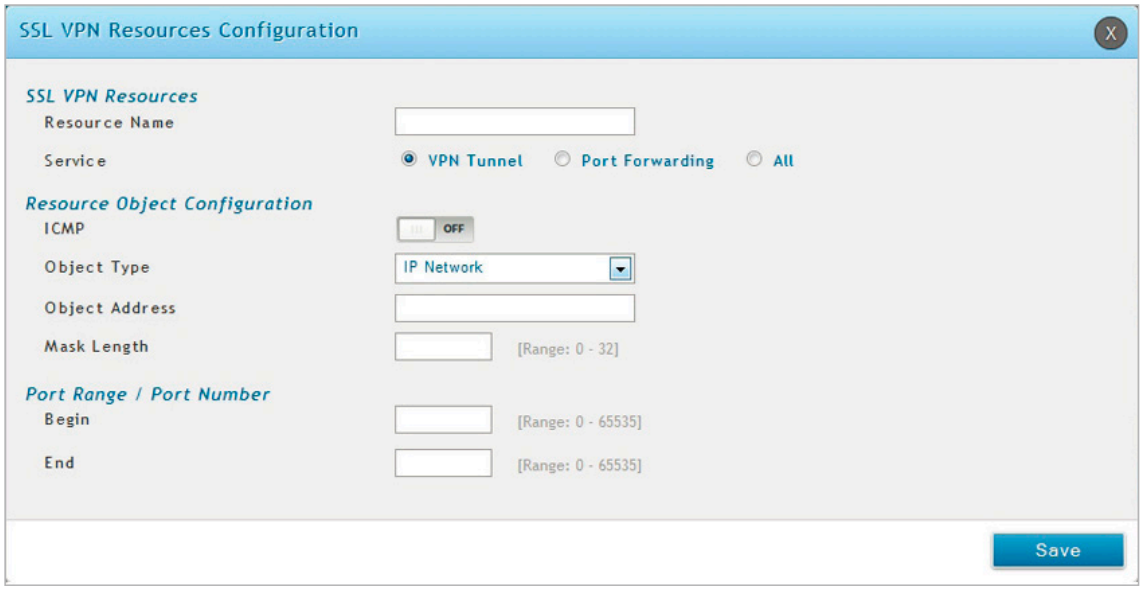

図 7-29　SSL VPN Resources Configuration 画面

3. 以下の項目を設定します。

項目	説明
SSL VPN Resource	
Resource Name	リソースに固有の名称を設定します。
Service	リソースの SSL VPN サービスを「VPN Tunnel」「Port Forwarding」「All」からを選択します。
Resource Object Configurarion	
ICMP	「ON」にして ICMP トラフィックを有効にします。
Object Type	オブジェクトのタイプを「IP Address」「IP Network」から選択します。
Object Address	IP アドレスを入力します。
Mask Length	オブジェクトのタイプを「IP Network」に設定した場合、マスク長を指定します。 • 設定可能範囲：0 - 32
Port Range / Port Number	
Begin / End	オブジェクトのポート範囲（開始 / 終了）を指定します。

4. 「Save」をクリックし、設定を適用します。

追加したネットワークリソースは、Resources 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

ポートフォワーディングルールの追加

ユーザポータルにログインしてポートフォワーディングサービスを起動すると、リモート SSL ユーザは特定のネットワークアプリケーションまたはサービスにアクセスできます。
リモートユーザからルータへのトラフィックは、設定済みのポートフォワーディングルールに基づいて検出され、再ルーティングされます。

内部ホストサーバまたは TCP アプリケーションは、リモートユーザがアクセスできるように指定する必要があります。
LAN サーバへのアクセスを許可するには、トンネリングするアプリケーションのローカルサーバの IP アドレスと TCP ポート番号を入力します。

1. **VPN > SSL VPN > Resources** の順にメニューをクリックして、以下の画面を表示します。

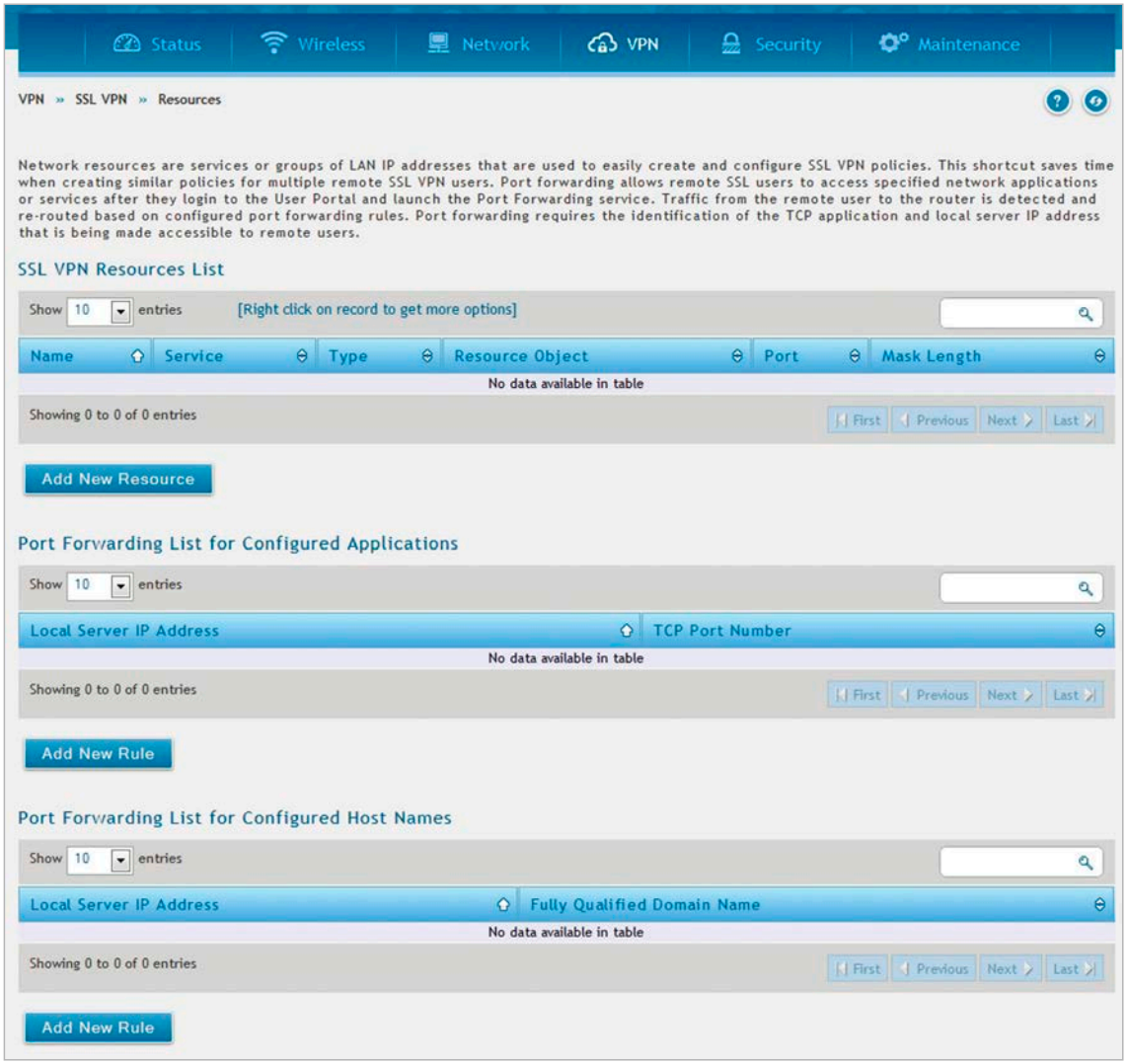

図 7-30　Resources 画面

2. 「**Port Forwarding List for Configured Applications**」または「**Port Forwarding List for Configured Host Names**」内にある「**Add New Rule**」をクリックします。

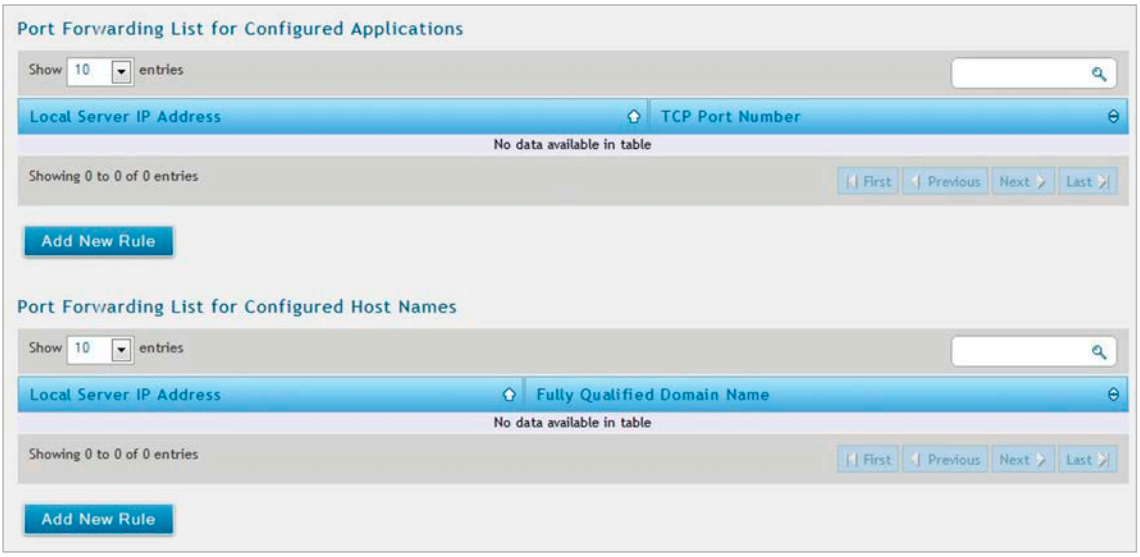

図 7-31　Port Forwarding List for Configured Applications/Host Names 画面

3. 以下の画面で設定を行います。

図 7-32　Port Forwarding List for Configured Applications 画面
「Local Server IP Address」：ローカルサーバの IP アドレスを入力します。
「TCP Port Number TCP」：ポート番号を入力します。

図 7-33　Port Forwarding List for Host Configuration 画面
「Local Server IP Address」：ローカルサーバの IP アドレスを入力します。
「Fully Qualified Domain Name」：ドメイン名（FQDN）を入力します。

4. 「Save」をクリックし、設定を適用します。

SSL VPN Client（SSL VPN クライアント設定）

VPN > SSL VPN > SSL VPN Client メニュー

SSL VPN トンネルクライアントにより、本ルータとブラウザ側マシンとのポイントツーポイント接続が可能となります。
SSL VPN クライアントがユーザポータルから起動されると、企業サブネット内の IP アドレス、DNS および WINS 設定を持つ「ネットワークアダプタ」が自動的に作成されます。
これにより、リモート SSLVPN クライアントのマシン上で特別なネットワーク設定をせずに、ローカルアプリケーションをプライベートネットワーク上のサービスにアクセスさせることができます。

VPN トンネルクライアントの仮想（PPP）インタフェースアドレスは、LAN 上の物理デバイスと重複しないようにしてください。
SSL VPN 仮想ネットワークアダプタ用の IP アドレス範囲は、コーポレート LAN と異なるサブネット、または重複しない範囲に設定します。

本ルータは「Full Tunnel」（フルトンネル）と「Split Tunnel」（スプリットトンネル）をサポートしています。
フルトンネルモードでは、VPN トンネル経由でクライアントからルータにすべてのトラフィックを送信します。
スプリットトンネルモードでは、事前に指定したクライアントルートに基づいて、プライベート LAN へトラフィックを送信します。
これらのクライアントルートは、SSL クライアントに特定のプライベートネットワークへのアクセスを許可し、特定の LAN サービスに対するアクセス制御を可能にします。

1. **VPN > SSL VPN > SSL VPN Client** の順にメニューをクリックして、以下の画面を表示します。

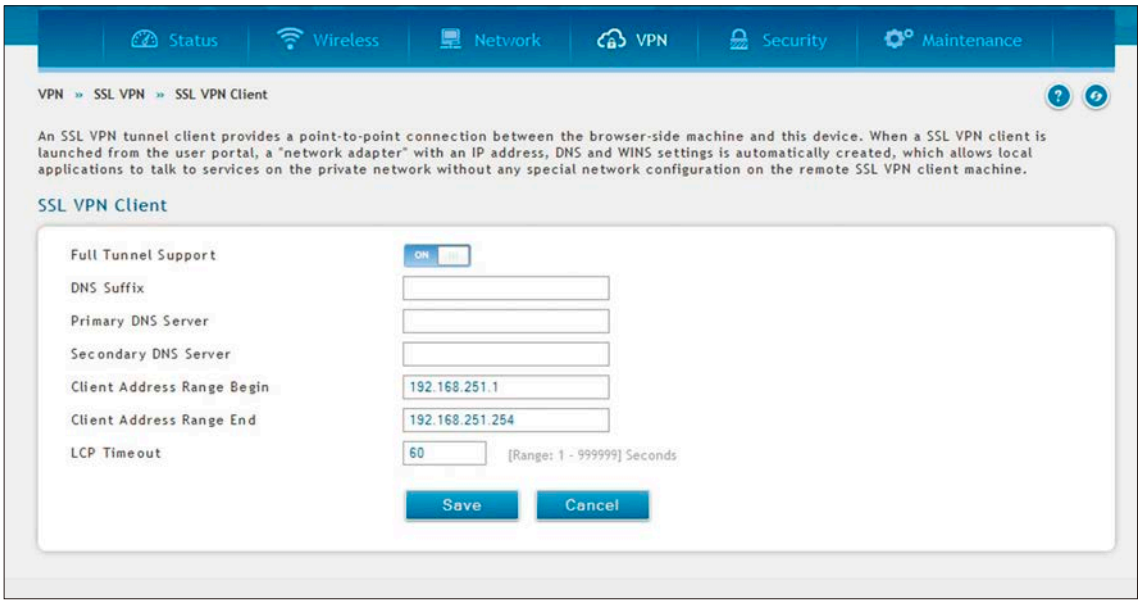

図 7-34　SSL VPN Client 画面

2. 以下の項目を設定します。

項目	説明
Full Tunnel Support	フルトンネルを「ON」または「OFF」にします。
DNS Suffix	SSL VPN クライアントに付与される DNS サフィックス名を入力します。本項目はオプションです。
Primary DNS Server	クライアントホストに作成したネットワークアダプタに設定する DNS サーバの IP アドレスを入力します。本項目はオプションです。
Secondary DNS Server	クライアントホストに作成したネットワークアダプタに設定するセカンダリ DNS サーバの IP アドレスを入力します。本項目はオプションです。
Client Address Range Begin	クライアントに割り当てる IP アドレス範囲の開始 IP アドレスを入力します。
Client Address Range End	クライアントに割り当てる IP アドレス範囲の終了 IP アドレスを入力します。
LCP Timeout	LCP ECHO の送信間隔を入力します。（単位：秒）

3. 「Save」をクリックし、設定を適用します。

Client Routes（SSL VPN クライアントルート設定）

VPN > SSL VPN > Client Routes

SSL VPN クライアントルートの設定を行います。
SSL VPN クライアントが企業ネットワークと異なるサブネット内の IP アドレスをアサインされた場合、VPN トンネルを通じてプライベート LAN にアクセスできるようにクライアントルートを追加します。同様に、VPN ファイアウォールを通じてリモート SSL VPN クライアントにプライベートトラフィックを送信できるように、プライベート LAN のファイアウォール（通常はこのルータ）上にスタティックルートを設定する必要があります。

スプリットトンネルモードが有効である場合、VPN トンネルクライアントにルートを設定する必要があります。
• 宛先ネットワーク：VPN トンネルクライアントから見た LAN のネットワークアドレスまたは宛先ネットワークのサブネット情報を設定します。
• サブネットマスク：宛先ネットワークのサブネット情報を指定します。

1. **VPN > SSL VPN > Client Routes** の順にメニューをクリックして、以下の画面を表示します。

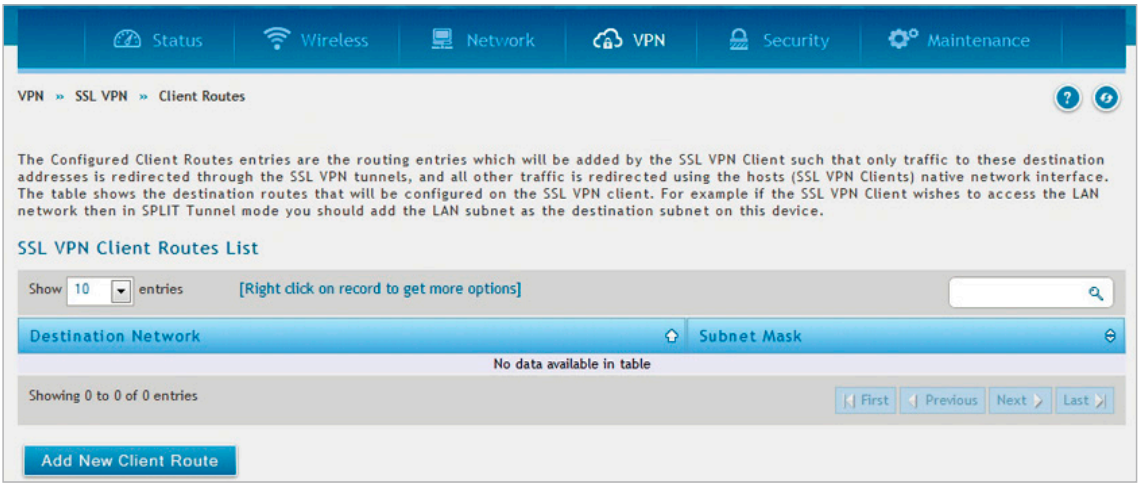

図 7-35　Client Routes 画面

クライアントルートの追加

1. 「Add New Client Route」をクリックして、以下の画面を表示します。

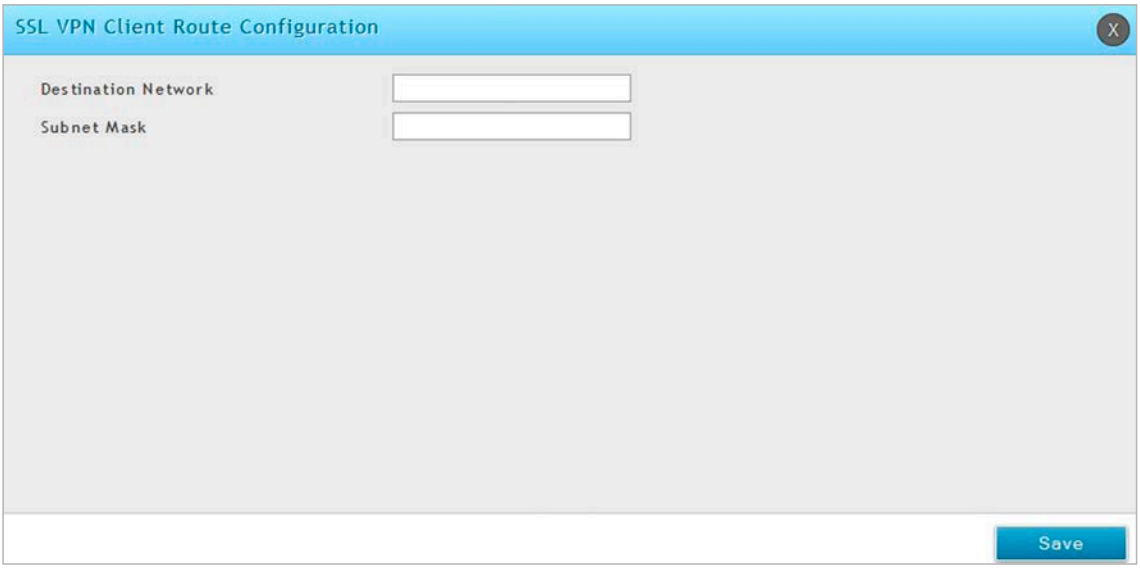

図 7-36　SSL VPN Client Route Configuration 画面

2. 以下の項目を設定します。

項目	説明
Destination Network	VPN トンネルクライアントから見た LAN のネットワークアドレスまたは宛先ネットワークのサブネット情報を設定します。
Subnet Mask	宛先ネットワークのサブネット情報を指定します。

3. 「Save」をクリックし、設定を適用します。

OpenVPN（OpenVPN 設定）

VPN > OpenVPN メニュー

Open VPN の設定を行います。

OpenVPN は、VPN を構築するためのアプリケーションです。VPN を利用することにより、インターネット上に仮想的にネットワークを構築し、場所の離れた拠点間、またモバイル環境とオフィス内 LAN の間などを安全に接続することができます。

また、SSL VPN 機能の代替となる OmniSSL 機能の設定方法についても説明します。

OpenVPN 設定

VPN > OpenVPN > OpenVPN Settings メニュー

OpenVPN では、証明書やユーザ名 / パスワードを使用したピアの相互認証が可能です。マルチクライアント - サーバ設定で利用した場合、サーバは署名と CA（認証局）を使用して、すべてのクライアントに対して認証証明書をリリースすることができます。OpenVPN は、本ルータを介して確立することができます。

OpenVPN のモードを「Server」モード、「Client」モード、「Access Server Client」モードから選択します。アクセスサーバクライアントモードで接続するには、「OpenVPN Access Server」から自動ログインプロファイルをダウンロードし、本ルータにアップロードする必要があります。

1. **VPN > OpenVPN > OpenVPN Settings** の順にメニューをクリックし、以下の画面を表示します。

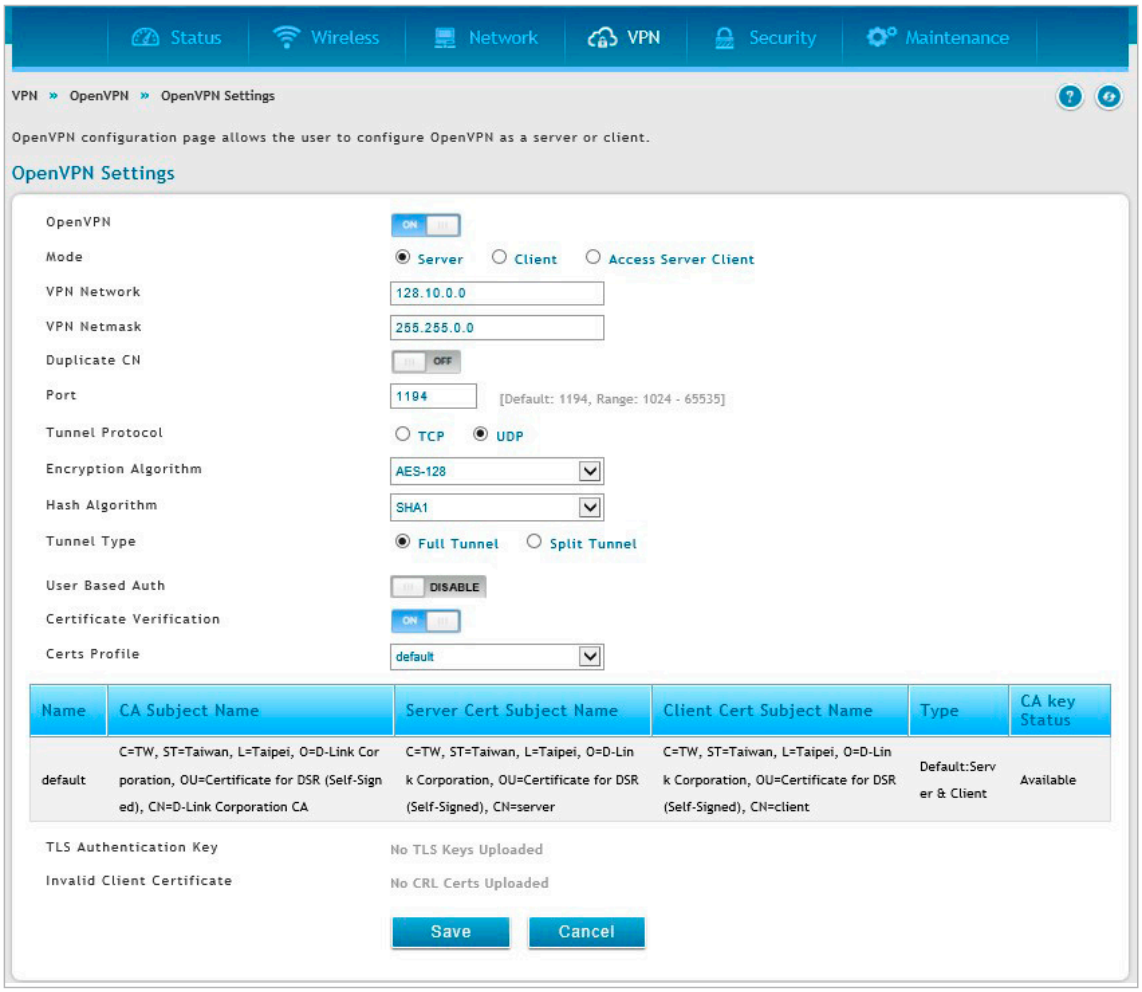

図 7-37　OpenVPN Settings（Server）画面

2. 以下の項目を設定します。

項目	説明
Open VPN	Open VPN を「ON」または「OFF」にします。
Mode	モードを以下から選択します。 • 「Server」：サーバモード • 「Client」：クライアントモード • 「Access Server Client」：アクセスサーバクライアントモード 選択したモードによって、画面に表示される項目が異なります。
Server	
VPN Network	VPN の IP ネットワークを入力します。
VPN Netmask	ネットマスクを入力します。
Duplicate CN	有効にすると、複数のクライアントに同じ認証を使用することが可能になります。

項目	説明
Port	使用するポート番号を入力します。初期値：1194
Tunnel Protocol	「TCP」または「UDP」を選択します。初期値：UDP
Encryption Algorithm	暗号化方式を選択します。
Hash Algorithm	ハッシュアルゴリズムを選択します。
Tunnel Type	トンネルタイプを以下から選択します。 • 「Full Tunnel」：トンネルを通じてすべてのトラフィックをリダイレクトします。（初期値） • 「Split Tunnel」：トンネルを通じて、事前定義されたクライアントルートに基づくプライベート LAN のみにトラフィックをリダイレクトします。
Client to Client Communication	有効にした場合、スプリットトンネルにおいて Open VPN クライアント同士の相互通信が可能になります。トンネルタイプに「Split Tunnel」を選択した場合のみ表示されます。 • 初期値：無効
User Based Auth	ユーザ名 / パスワードを使用した追加の認証方式を有効化 / 無効化します。
Certificate Verification	本機能を有効化した場合、クライアント証明書が必要になります。無効化した場合、クライアントはユーザ名 / パスワードのみを使用して認証を行います。 • 初期値：有効
Certs Profile	設定されたサーバ / クライアント用に証明書がアップロードされているプロファイルを選択します。 初期値では、サーバ証明書とクライアント証明書の両方を持つデフォルトプロファイルが選択されています。
TLS Authentication Key	TLS 認証を有効化し、追加の認証レイヤを追加します。TLS キーがアップロードされた場合にだけチェックされます • 初期値：無効
Invalid Client Certificate	不正なクライアント証明書をブロックするファシリティを追加します。ブロックされるクライアント証明書のリストを含む CRL 形式の証明書が必要です。 • 初期値：無効
Client	
Server IP	クライアントが接続する OpenVPN サーバ IP アドレスを入力します。
Failover Server IP	フェイルオーバ IP アドレスを入力します。
Port	使用するポート番号を入力します。初期値 : 1194
Tunnel Protocol	「TCP」または「UDP」を選択します。初期値 : UDP
Encryption Algorithm	暗号化方式を選択します。
Hash algorithm	ハッシュアルゴリズムを選択します。
Auto Connect	自動接続を有効または無効にします。 有効にした場合、自動的に再接続を試行するまでの間隔を設定します。 **Status > Network Information > Active VPNs > OpenVPN Connections** 画面でもサーバへの接続または切断を設定できます。
Interval	自動的に再接続を試行するまでの間隔を設定します。（単位：分）
User Based Auth	ユーザ名 / パスワードを使用した追加の認証方式を有効化 / 無効化します。
Certificate Verification	本機能を有効化した場合、クライアント証明書が必要になります。無効化した場合、クライアントはユーザ名 / パスワードのみを使用して認証を行います。 • 初期値：有効
Certs Profile	設定されたサーバ / クライアント用に証明書がアップロードされているプロファイルを選択します。 初期値では、サーバ証明書とクライアント証明書の両方を持つデフォルトプロファイルが選択されています。
TLS Authentication Key	TLS 認証を有効化し、追加の認証レイヤを追加します。TLS キーがアップロードされた場合にだけチェックされます • 初期値：無効
Access Server Client	
Port	使用するポート番号を入力します。初期値：1194
Enable Private Tunnel	「ON」にした場合、安全なアクセス接続を提供する www.privatetunnel.com に接続します。 初期値：「OFF」 以下の項目は「Enanle Private Tunnel」を「ON」にした場合のみ表示されます。 • 「Email Address」：www.privatetunnel.com に登録する Email アドレスを入力します。 • 「Password」：パスワードを入力します。パスワードには英数字を使用可能です。 • 「VPN Cluster」：VPN クラスタのタイプを選択します。
Auto Connect	自動接続を有効または無効にします。有効にした場合、自動的に再接続を試行するまでの間隔を設定します。 **Status > Network Information > Active VPNs > OpenVPN Connections** 画面でもサーバへの接続または切断を設定できます。
Interval	自動的に再接続を試行するまでの間隔を設定します。（単位：分）
Upload Status	設定ファイルのアップロード状況について表示します。
File	「Browse/ 参照」をクリックし、設定ファイルをアップロードします。

3. 「Save」をクリックし、設定を適用します。

OpenVPN Certificates（Open VPN 証明書）

VPN > OpenVPN > OpenVPN Certificates メニュー

Open VPN では、証明書を使用した認証を行うことができます。
pem 形式の証明書とキーのアップロード方法について説明します

OpenVPN Certificates（Open VPN 証明書）

1. **VPN > Open VPN > OpenVPN Certificates > OpenVPN Certificates タブ**の順にメニューをクリックし、以下の画面を表示します。

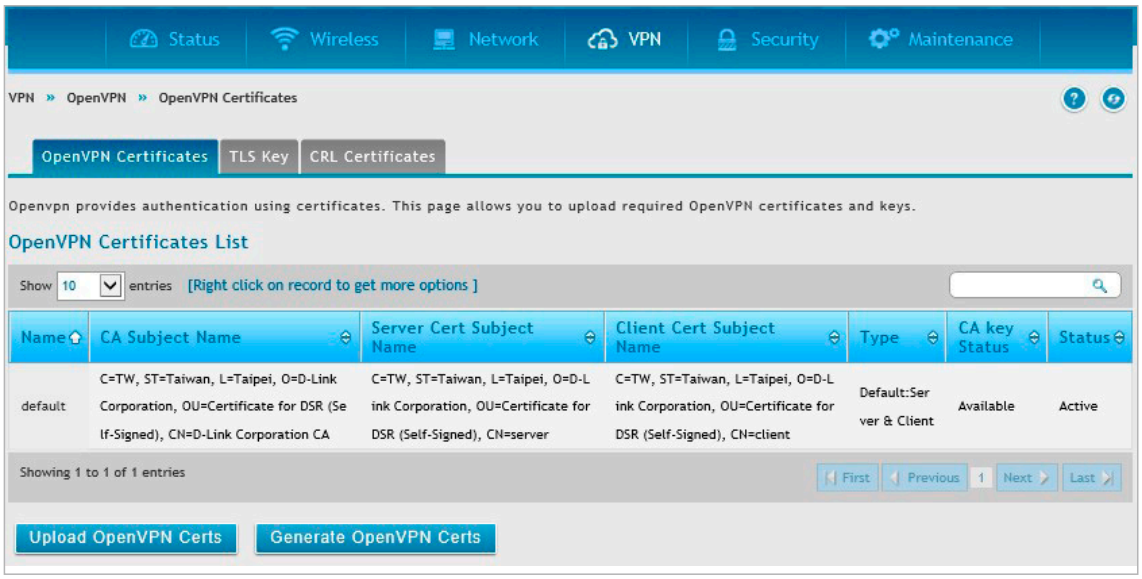

図 7-38　OpenVPN Certificates > OpenVPN Certificates タブ 画面

項目	説明
Name	プロファイル名が表示されます。
CA Subject Name	CA 証明書のサブジェクト名が表示されます。 名前には、C、ST、L、O、OU、CN、E などのコンテンツが含まれます。CN は CA 証明書のコモンネームです。
Server Cert Subject Name	サーバ証明書のサブジェクト名が表示されます。 名前には、C、ST、L、O、OU、CN、E などのコンテンツが含まれます。CN は CA 証明書のコモンネームです。 サーバ証明書が存在しない場合、「N/A」と表示されます。
Client Cert Subject Name	クライアント証明書のサブジェクト名が表示されます。 名前には、C、ST、L、O、OU、CN、E などのコンテンツが含まれます。CN は CA 証明書のコモンネームです。 クライアント証明書が存在しない場合、「N/A」と表示されます。
Type	プロファイルのタイプが表示されます。 タイプは、証明書（Generated/Uploaded/Default）と設定したモード（Server/Client/Server & Client）の組み合わせです。
CA Key Status	CA キーのステータスが表示されます。 • 「N/A」：CA キーが存在しません。 • 「Available」：CA キーが使用可能です。
Status	プロファイルのステータスが表示されます。
Upload OpenVPN Certs	クリックすると、Server/Client Certificate Configuration 画面が表示されます。
Generate OpenVPN Certs	クリックすると、OpenVPN Certificate Configuration 画面が表示されます。

■ Open VPN 証明書のアップロード

1. 「Upload OpenVPN Certs」をクリックし、以下の画面を表示します。

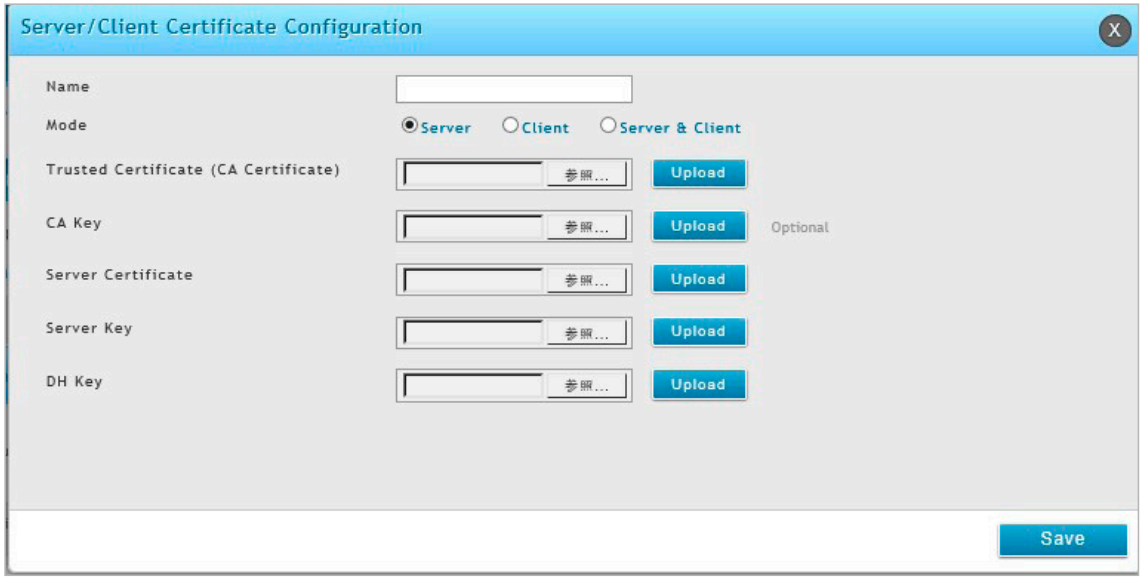

図 7-39　Server/Client Certificate Configuration 画面

2. 以下の項目を設定します。

項目	説明
Name	プロファイル名が表示されます。
Mode	モードを以下から選択します。 ・「Server」「Client」「Server & Client」 選択したモードによって、以降に表示される項目が異なります。
Trusted Certificate (CA Certificate)	「Browse」をクリックし、pem 形式の CA 証明書をアップロードします。
CA Key	「Browse」をクリックし、pem 形式の CA キーをアップロードします。
Server Certificate	「Browse」をクリックし、pem 形式のサーバ証明書をアップロードします。
Server Key	「Browse」をクリックし、pem 形式のサーバキーをアップロードします。
Client Certificate	「Browse」をクリックし、pem 形式のクライアント証明書をアップロードします。
Client Key	「Browse」をクリックし、pem 形式のクライアントキーをアップロードします。
DH Key	「Browse」をクリックし、pem 形式の Diffie Hellman キーをアップロードします。

3. 「Save」をクリックし、設定を適用します。

■ Open VPN 証明書の生成

1. 「Generate OpenVPN Certs」をクリックし、以下の画面を表示します。

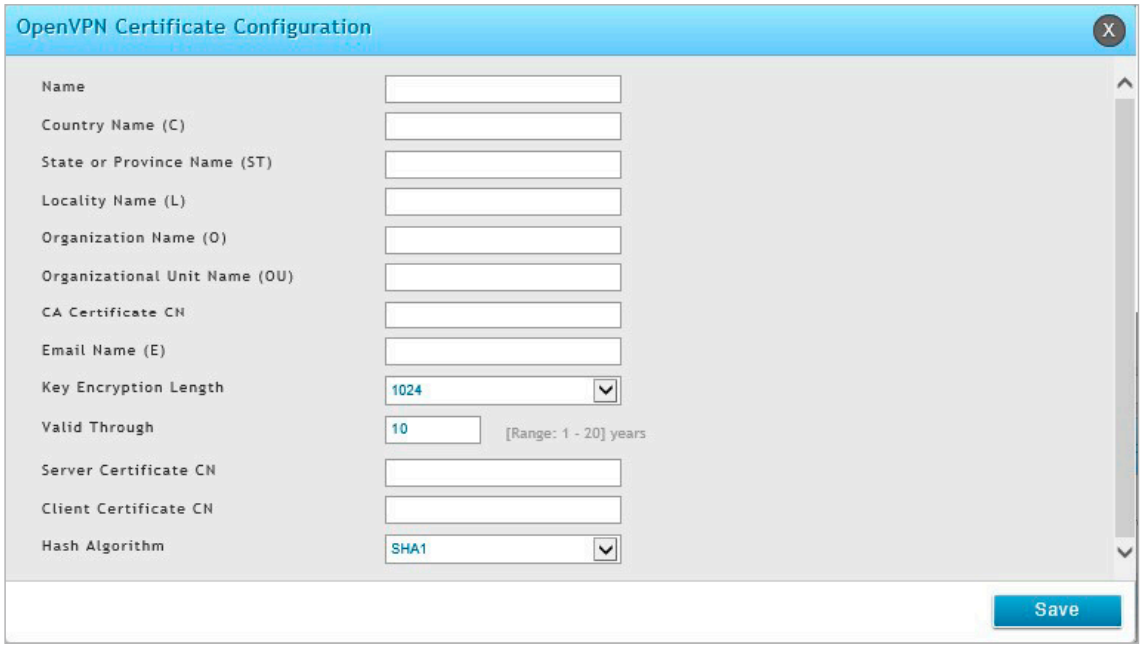

図 7-40　OpenVPN Certificate Configuration 画面

2. 以下の項目を設定します。

項目	説明
Name	プロファイル名が表示されます。
Country Name (C)	ISO 形式の 2 文字の国名コードを入力します。日本の場合は「JP」です。
State or Province Name (ST)	都道府県名を入力します。
Locality Name (L)	市区町村名を入力します。
Organizational Name (O)	企業名などの組織名を入力します。組織名は、公的機関に登録されている正式名称を入力してください。
Organizational Unit Name (OU)	組織内の部門を区別するため、証明書を取り扱う組織のユニット名を入力します。
CA Certificate CN	CA 証明書の CN（コモンネーム）を入力します。 コモンネームは、サーバの DNS ルックアップに使用されるドメイン名です。（例：www.mydomain.com） ブラウザは、ウェブサイトを識別するためにこの情報を使用します。お使いのホスト名を変更した場合、別のデジタル ID を要求する必要があります。 ホストに接続しているクライアントブラウザは、デジタル ID のコモンネームと URL が一致しているか確認します。
Email Name (E)	組織への連絡に使用する E メールアドレスを入力します
Key Encryption Length	接続の暗号化に使用される暗号化キーの長さを選択します。
Valid Through	証明書の有効期間を入力します。（単位：年）
Server Certificate CN	使用するサーバ証明書のコモンネームを入力します。
Client Certificate CN	使用するクライアント証明書のコモンネームを入力します。
Hash Algorithm	証明書で使用するハッシュアルゴリズムを、「SHA1」または「SHA256」から選択します。

3. 「Save」をクリックし、設定を適用します。

TLS Key（TLS キー）

pem 形式の TLS キーをアップロードします。

1. **VPN > Open VPN > OpenVPN Certificates > TLS Key タブ**の順にメニューをクリックし、以下の画面を表示します。

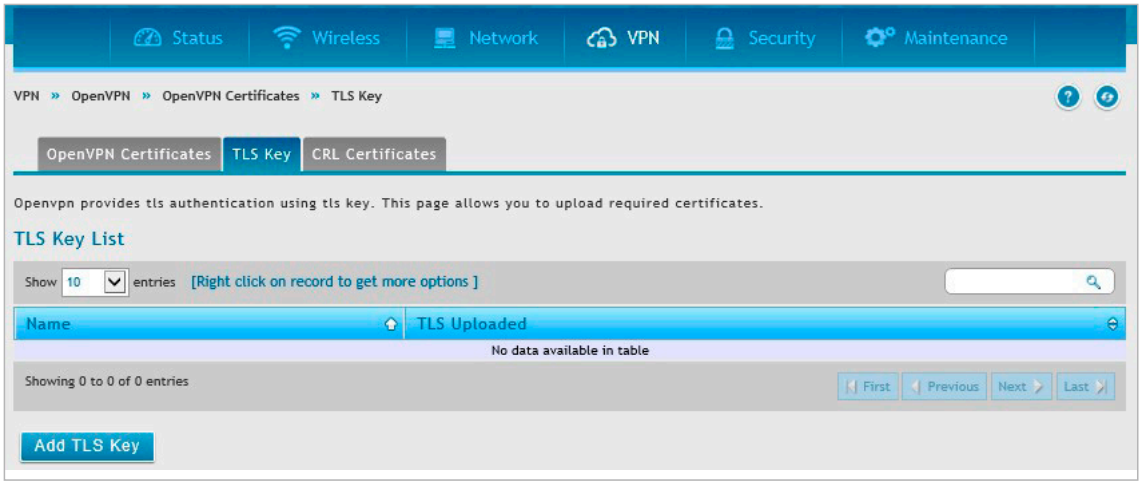

図 7-41　OpenVPN Certificates > TLSKey タブ 画面

2. 「Add TLS Key」をクリックします。

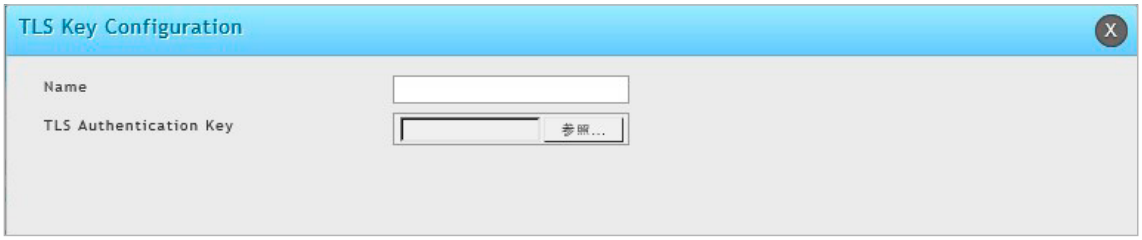

図 7-42　TLS Key Configuration 画面

3. TLS キーの名前を入力します。OpenVPN Setting 画面で識別可能とするためです。
4. 「Browse/ 参照」をクリックし、pem 形式の TLS キーをアップロードします。
5. 「Save」をクリックし、設定を適用します。

CRL Certificate（CRL 証明書）

Open VPN では、CRL 証明書を使用した CRL 認証が可能です。
必要な証明書のアップロード方法について説明します。

1. **VPN > Open VPN > OpenVPN Certificates > CRL Certificate タブ**の順にメニューをクリックし、以下の画面を表示します。

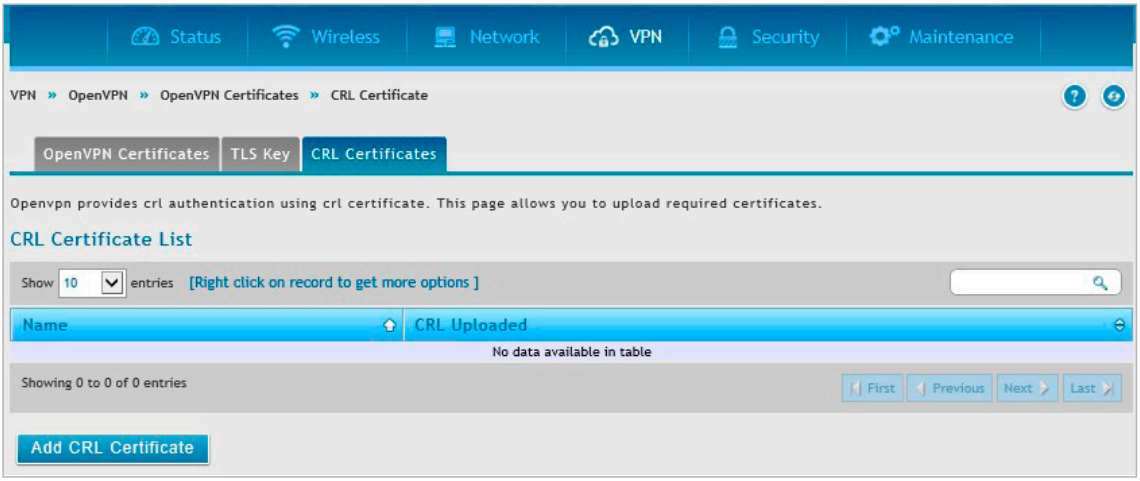

図 7-43　OpenVPN Certificates > CRL Certificate タブ画面

2. 「Add CRL Certificate」をクリックします。

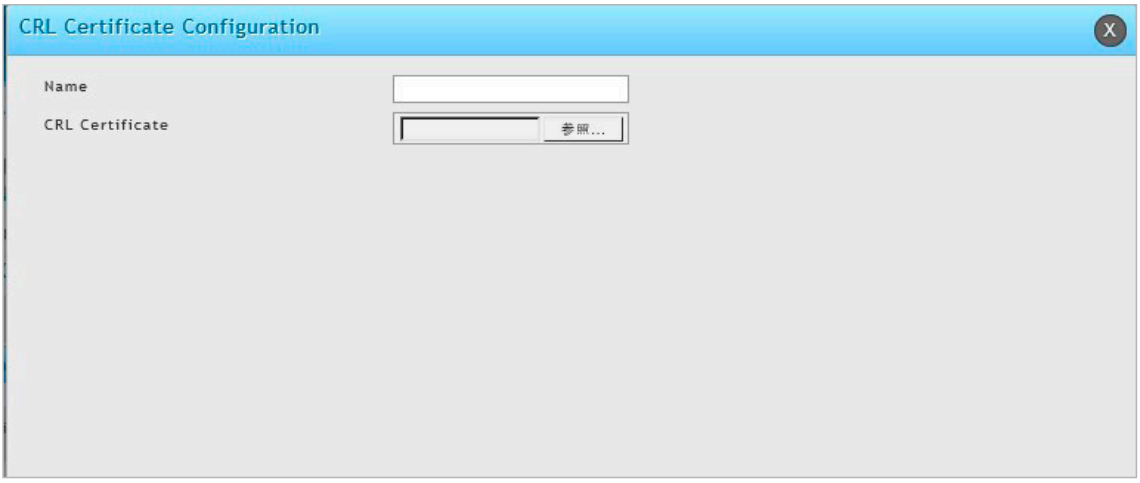

図 7-44　CRL Certificate Configuration 画面

3. CRL 証明書の名前を入力します。OpenVPN Setting 画面で識別可能とするためです。
4. 「Browse/ 参照」をクリックし、pem 形式の CRL 証明書をアップロードします。クライアント証明書は無効になります。
5. 「Save」をクリックし、設定を適用します。

OpenVPN Server Policy（Open VPN サーバポリシー）

VPN > OpenVPN > OpenVPN Server Policy メニュー

Open VPN サーバポリシーの設定方法について説明します。Open VPN サーバポリシーは、SSL VPN サーバポリシーの代替となるものです。

1. **VPN > OpenVPN > OpenVPN Server Policy** の順にメニューをクリックし、以下の画面を表示します。

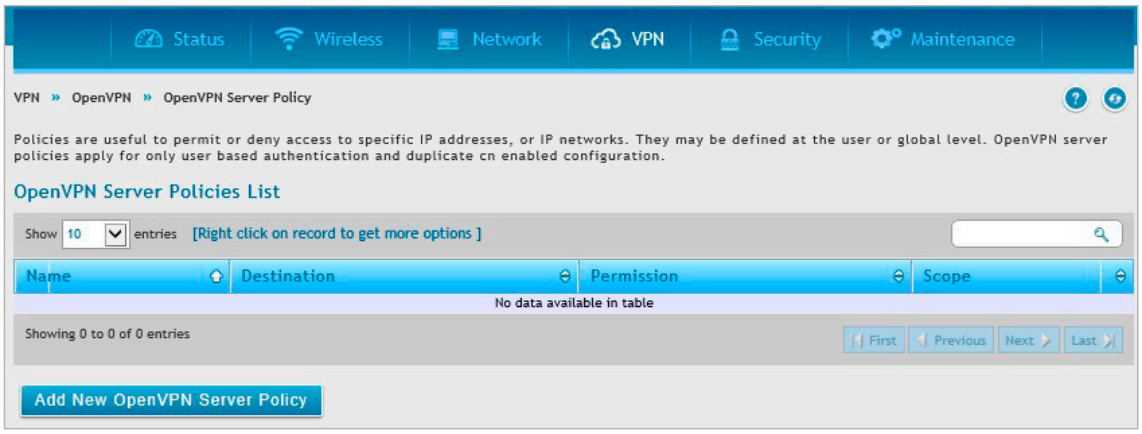

図 7-45　OpenVPN Server Policy 画面

2. Open VPN サーバポリシーを追加する場合、「Add New OpenVPN Server Policy」をクリックし以下の画面を表示します。

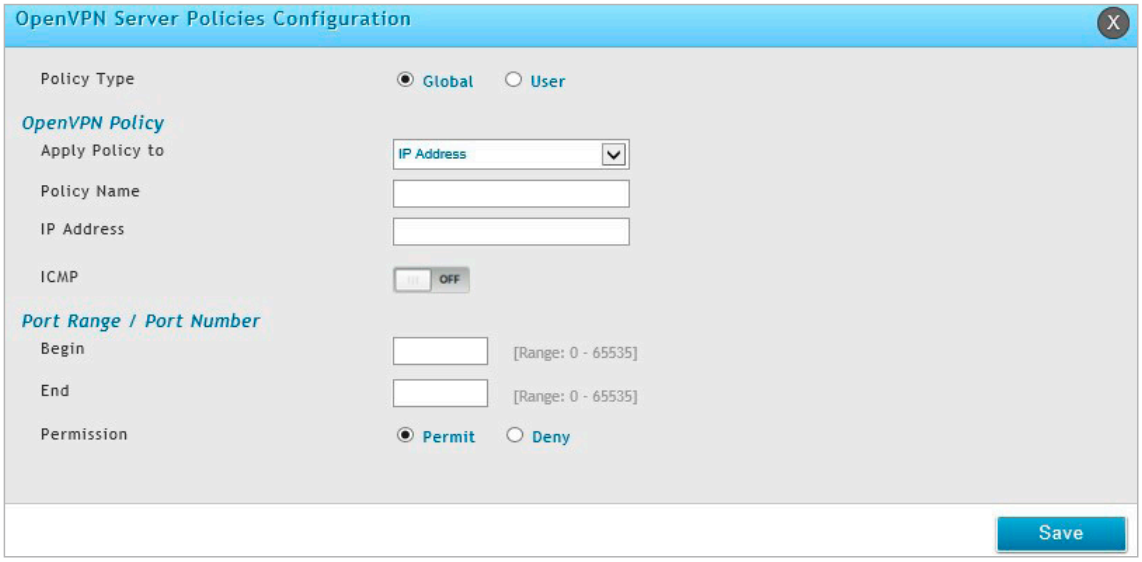

図 7-46　OpenVPN Sever Policies Configuration 画面

3. 以下の項目を設定します。

項目	説明
Policy Type	ポリシータイプを以下から選択します。 • 「Global」: すべてのユーザにポリシーを適用します。 • 「User」: 特定のユーザにポリシーを適用します。「User」を選択した場合は、「Available Users」でユーザを選択します。
OpenVPN Policy	
Apply Policy To	ポリシーの適用先を以下から選択します。 • 「IP Address」: ポリシーを IP アドレスに対して適用します。 • 「IP Network」: ポリシーを IP ネットワークに対して適用します。
Policy Name	ポリシー名を入力します。
ICMP	IPCMP を「ON または「OFF」に設定します。 • 「ON」: ICMP トラフィックをサポートします。 • 「OFF」: ICMP トラフィックをサポートしません。
IP Address	IP アドレスを入力します。
Mask Length	「IP Network」を選択した場合、マスク長を入力します。
Port Range / Port NUmber	
Begin / End	適用するポート番号の範囲を入力します。
Permission	「Permit」: ポリシーを許可します。 「Deny」: ポリシーを拒否します。

4. 「Save」をクリックし、設定を適用します。

Local Networks（ローカルネットワーク設定）

VPN > OpenVPN > Local Networks メニュー

Open VPN のローカルネットワークの作成方法について説明します。

ローカルネットワークの作成は、**VPN > OpenVPN > OpenVPN Settings** 画面でトンネルタイプにスプリットトンネルを選択した場合に行います。

1. **VPN > OpenVPN > Local Networks** の順にメニューをクリックし、以下の画面を表示します。

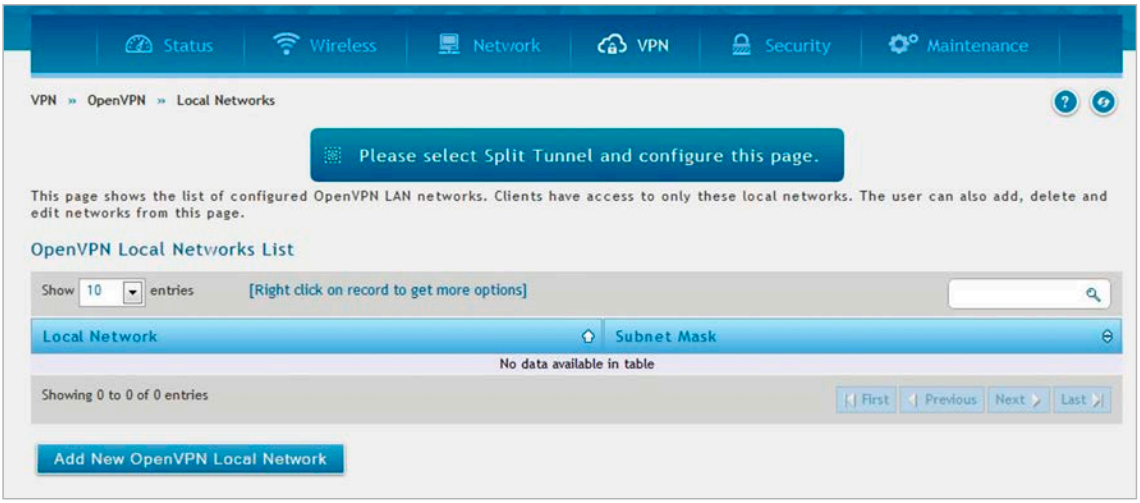

図 7-47　Local Networks 画面

2. 「Add New OpenVPN Local Network」をクリックし以下の画面を表示します。

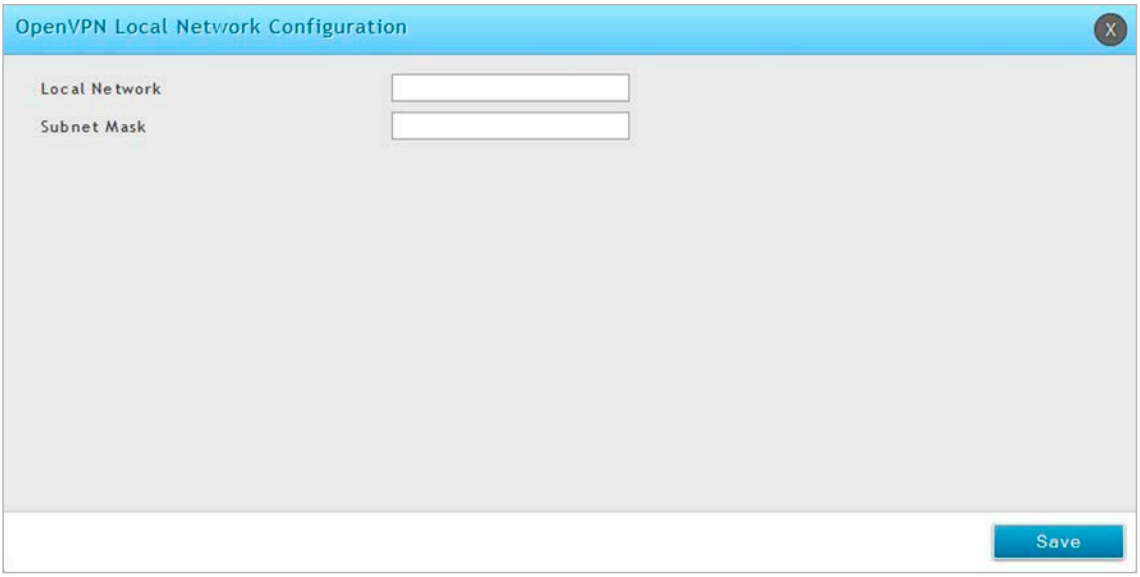

図 7-48　OpenVPN Local Network Configuration 画面

3. 以下の項目を設定します。

項目	説明
Local Network	ローカル IP ネットワークを入力します。
Subnet Mask	サブネットマスクを入力します。

4. 「Save」をクリックし、設定を適用します。

Remote Networks（リモートネットワーク設定）

VPN > OpenVPN > Remote Networks メニュー

Open VPN のリモートネットワークの作成方法について説明します。

1. **VPN > OpenVPN > Remote Networks** の順にメニューをクリックし、以下の画面を表示します。

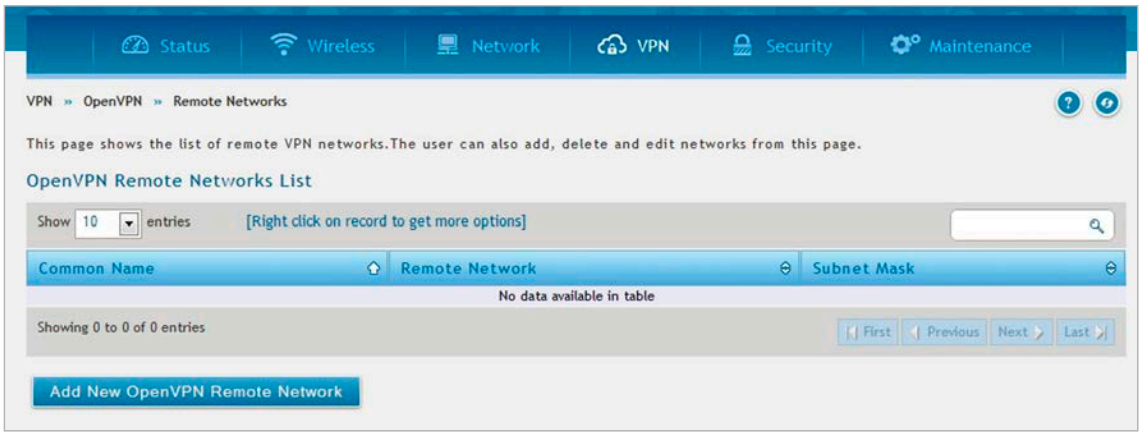

図 7-49　Remote Networks 画面

2. 「Add New OpenVPN Local Network」をクリックし以下の画面を表示します。

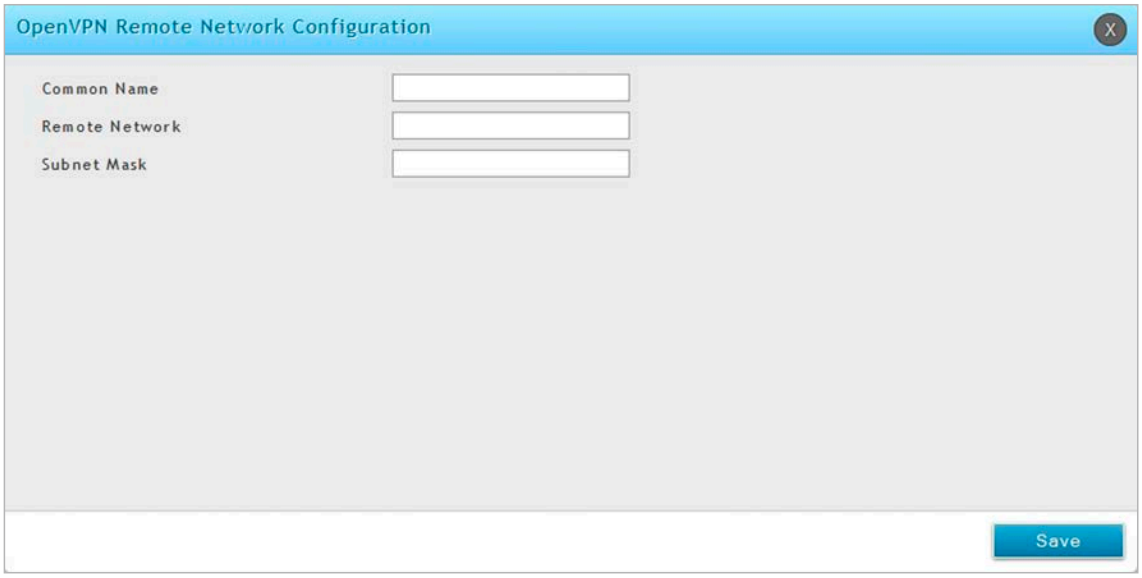

図 7-50　OpenVPN Remote Network Configuration 画面

3. 以下の項目を設定します。

項目	説明
Common Name	リモートネットワークの名前を指定します。
Remote Network	リモート IP ネットワークを入力します。
Subnet Mask	サブネットマスクを入力します。

4. 「Save」をクリックし、設定を適用します。

作成したネットワークは Remote Networks 画面に表示されます。
右クリックで「Edit」（編集）、「Delete」（削除）を実行できます。

OmniSSL Client Configuration（OmniSSL クライアント設定）

VPN > OpenVPN > OmniSSL Client Configuration メニュー

本ルータは多くの SSL VPN 機能をサポートする一方で、SSL VPN 機能の代替となる OmniSSL 機能も提供しています。
OmniSSL により、ポータル画面を通じたデバイスからのクライアントインストールが容易になり、既存の OpenVPN 機能を強化することができます。
さらに、この VPN ツールはモバイルデバイス経由で使用することが可能であるため、SSL VPN ソリューションで発生するブラウザ・Java 依存の問題を解決します。
OmniSSL は、様々な OS でインストールが可能です。本画面では、クライアント設定を生成できます。

1. **VPN > OpenVPN > OmniSSL Client Configuration** の順にメニューをクリックし、以下の画面を表示します。

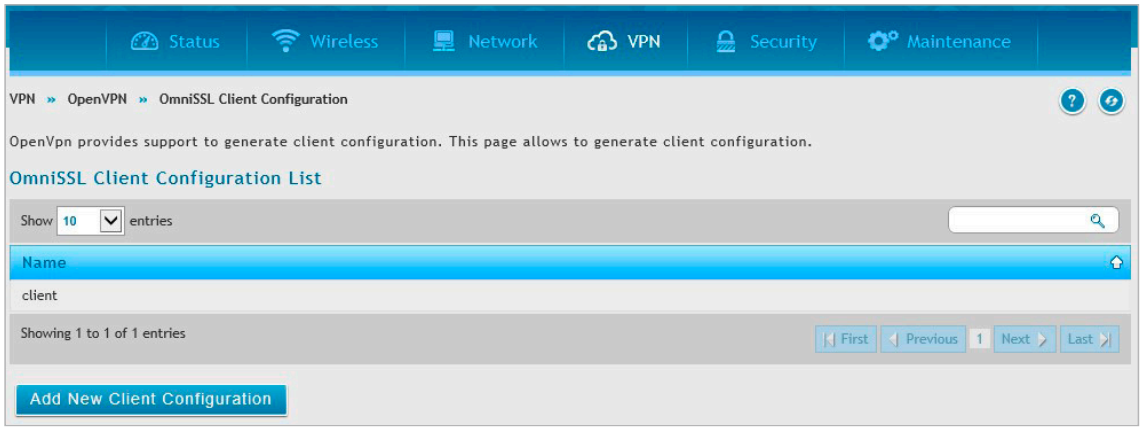

図 7-51　OmniSSL Client Configuration 画面

2. クライアントを右クリックすると、以下のメニューが表示されます。

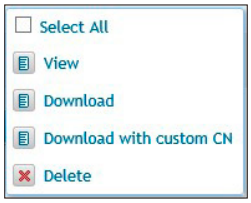

図 7-52　OmniSSL Client Configuration Menu 画面

項目	説明
Select All	リストに表示されたすべてのクライアント設定を選択します。
View	クライアント名と、クライアント設定ファイルの詳細を表示します。
Download	選択した設定をダウンロードします。ポータル以外のユーザおよび OS 固有のものであり、IP/FQDN 固有のオプションは維持されません（例：dev、設定内のリモートオプション）。
Download with custom CN	テキストボックスに表示されたカスタムクライアント名で設定をダウンロードします。
Delete	選択したクライアントを削除します。デフォルトのクライアントは削除できません。

注意　CA 証明書をアップロードした後は、クライアント設定を再生成してください。

3. 新しいクライアント設定を追加する場合は、「Add New Client Configuration」をクリックし以下の画面を表示します。

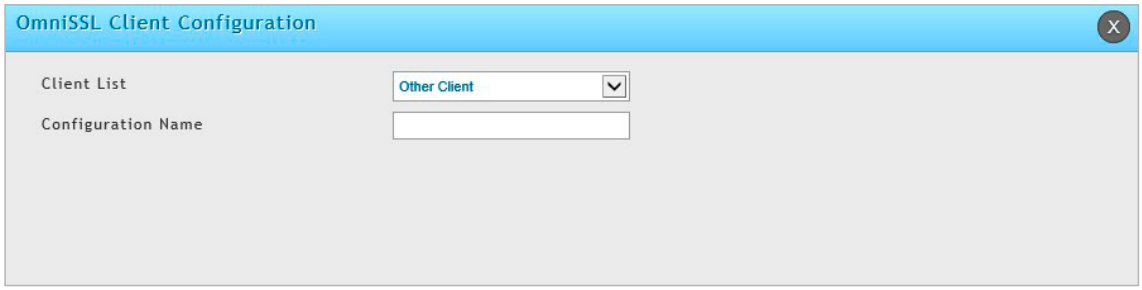

図 7-53　OmniSSL Client Configuration 画面

4. 以下の項目を設定します。

項目	説明
Client List	設定した OpenVPN ユーザ、または「Other Client」（その他のクライアント）を選択してください。
Configuration Name	設定名を入力します。

5. 「Save」をクリックし、設定を適用します。

OmniSSL Portal Layouts（OmniSSL ポータルレイアウト）

VPN > OpenVPN > OmniSSL Portal Layouts メニュー
リモート OmniSSL ユーザの認証時に表示される、カスタムページを作成します。

1. **VPN > OpenVPN > OmniSSL Portal Layouts** の順にメニューをクリックし、以下の画面を表示します。

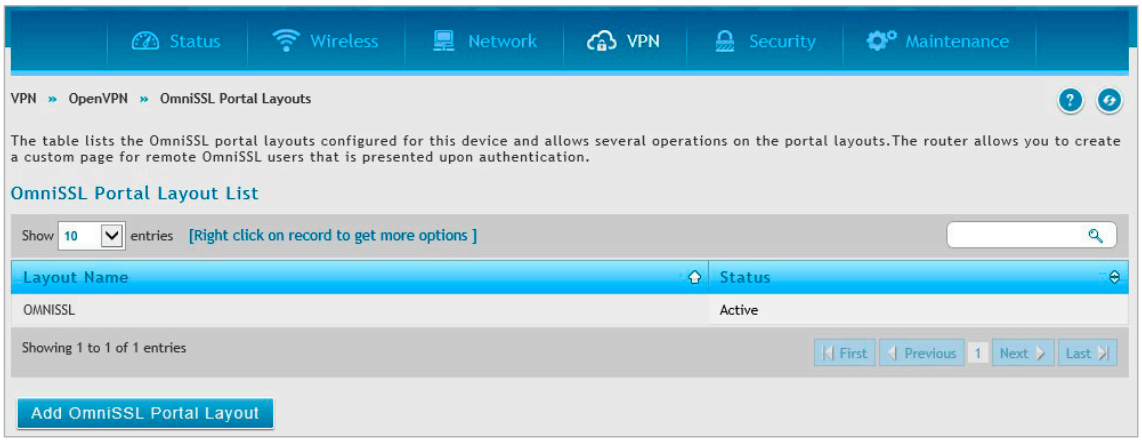

図 7-54　OmniSSL Portal Layouts 画面

2. 「Add OmniSSL Portal Layout」をクリックし以下の画面を表示します。

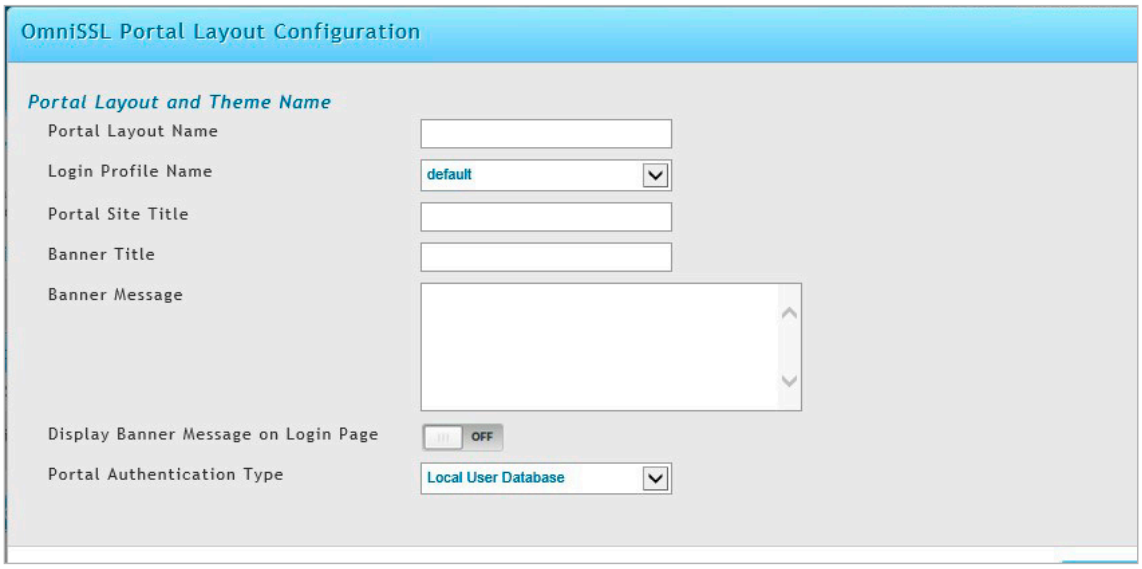

図 7-55　OmniSSL Portal Layout Configuration 画面

3. 以下の項目を設定します。

項目	説明
Portal Layout Name	ポータルレイアウトの名称を英字で入力します。
Login Profile Name	ログインプロファイルを選択します。
Portal Site Title	ポータルサイトのタイトルを入力します。本項目はポータルの Web ブラウザウィンドウのタイトルとして表示されます。
Banner Title	ポータルにログインする前に表示されるバナータイトルを入力します。
Banner Message	バナーメッセージを入力します。 バナーメッセージはバナータイトルと共に表示されます。
Display Banner Message on Login Page	「ON」：バナータイトルとバナーメッセージをログイン画面に表示します。 「OFF」：バナータイトルとバナーメッセージをログイン画面に表示しません。
Portal Authentication Type	OmniSSL ポータルユーザの認証方法を以下から選択します。 「Local User Database」「Radius-PAP, Radius-CHAP」「Radius-MSCHAP」「Radius-MSCHAPv2」「NT Domain」「Active Directory」「 LDAP」「POP3」

4. 「Save」をクリックし、設定を適用します。

追加したポータルレイアウトは OmniSSL Portal Layouts 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

GRE（GRE 設定）

VPN > GRE メニュー

GRE Tunnels（Gre トンネル設定）

VPN > GRE > GRE Tunnels メニュー

GRE（Generic Routing Encapsulation）は、トンネルプロトコルの 1 つです。パケットを別のプロトコルでカプセル化して伝送を行います。GRE トンネルを作成すると、トンネルを介してマルチキャストパケットの送受信が可能となります。
GRE トンネルは、D-Link Discovery Protocol（DDP）のブロードキャストトラフィックをリモート LAN サブネット間で送受信する場合に使用できます。

注意　設定できる GRE トンネル数は製品によって異なります。

- DSR-500：15
- DSR-1000/1000AC : 25

以下の手順で GRE トンネルを確立します。

1. GUI から GRE トンネルを作成します。
2. GRE トンネルを使用して、リモートローカルネットワーク用のスタティックルートを設定します。

GRE トンネルを作成する場合、GRE トンネルのエンドポイントに固有の IP アドレスを設定します。
この IP アドレスは、もう一方ルータのスタティックルートでゲートウェイ IP アドレスとして参照されます。
GRE Tunnels Configuration 画面の「Remote End Address」には、エンドポイントルータの WAN IP アドレスを入力します。

トンネル確立後、GRE トンネル名に対して設定されたインタフェースを使用し、ルータ上にスタティックルートを作成します。
スタティックルートの宛先 IP アドレスはリモート LAN のサブネットです。
スタティックルートのゲートウェイ IP アドレスは、終端ルータ（リモート LAN サブネットを管理しているルータ）の GRE トンネル IP になります。
これらの手順が完了すると、すべての DDP ブロードキャストトラフィックが GRE トンネルを通じてリモート LAN サブネット間に流れます。

1. **VPN > GRE > GRE Tunnels** の順にメニューをクリックし、以下の画面を表示します。

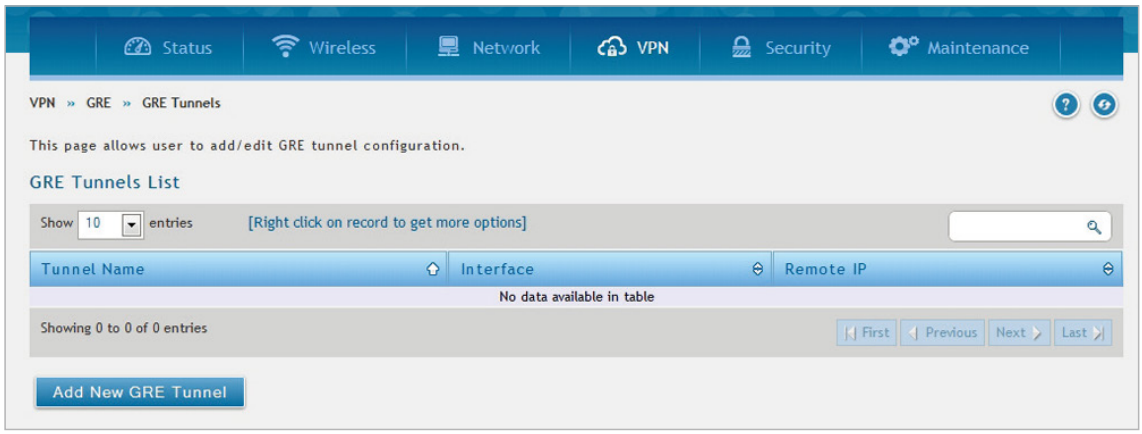

図 7-56　GRE Tunnels 画面

2. GRE トンネルを追加する場合、「Add New GRE Tunnel」をクリックし以下の画面を表示します。

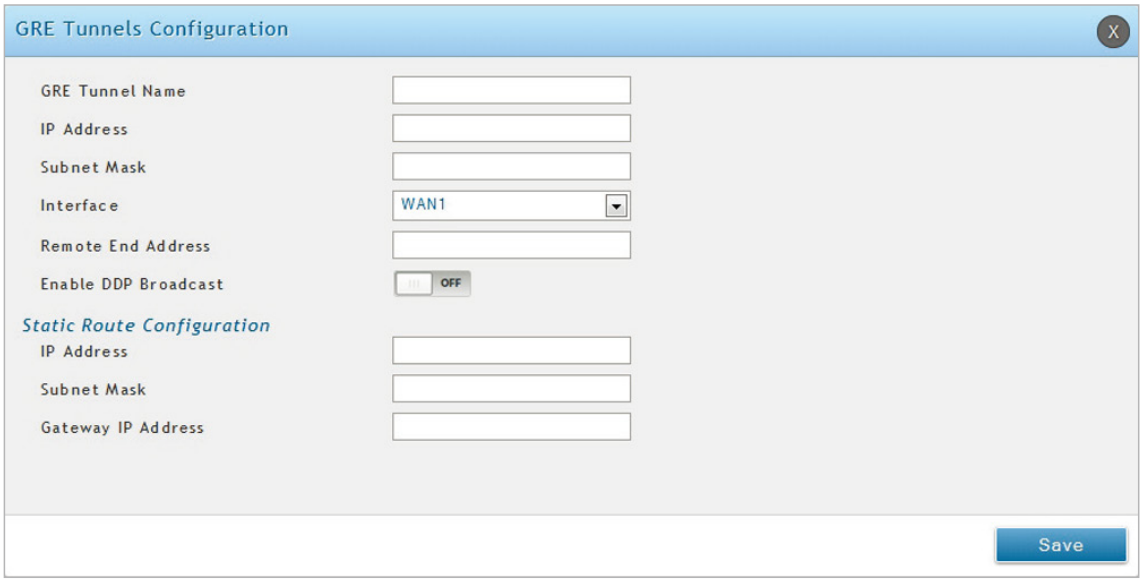

図 7-57　GRE Tunnels Configuration 画面

3. 以下の項目を設定します。

項目	説明
GRE Tunnel Name	トンネル名を入力します。
IP Address	本エンドポイントの IP アドレスを入力します。ゲートウェイ IP アドレスとして他のルータのスタティックルートで参照されます。
Subnet Mask	サブネットマスクを入力します。
Interface	GRE トンネル設定に使用する IP インタフェースを選択します。
Remote End Address	エンドポイントルータの WAN IP アドレスを入力します。
Enable DDP Broadcast	DDP ブロードキャストを有効にします。
Static Route Configuration	
IP Address	スタティックルートにおけるリモート LAN サブネットの宛先 IP アドレスを入力します。
Subnet Mask	宛先 IP アドレスのサブネットマスクを入力します。
Gateway IP Address	終端ルータの IP アドレスを入力します。

4. 「Save」をクリックし、設定を適用します。

追加した GRE トンネルは GRE Tunnels 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

第 8 章　セキュリティ設定（Security）

ご使用のネットワークの安全を確保する、セキュリティ機能の設定について説明します。

設定項目	説明
「Authentication（認証設定）」	本ルータの認証に関する設定を行います。
「Web Content Filter（Web コンテンツフィルタリング）」	Web のコンテンツを対象としたアクセスポリシーを作成、適用する、Web フィルタリング機能の設定を行います。
「Firewall（ファイアウォール設定）」	本ルータのファイアウォールの設定を行います。
「App Control Policy（アプリケーションコントロールポリシー）」	アプリケーションのトラフィックのコントロールを行います。

注意　ネットワークの概念と専門用語を理解している熟練したユーザのみ本章の手順を実行してください。

Authentication（認証設定）

Security > Authentication メニュー

Internal User Database（内部ユーザデータベース）

Security > Authentication > Internal User Database メニュー
内部ユーザデータベースの管理方法について説明します。
ユーザグループを作成後、グループに適用するポリシーを設定し、ユーザをグループに追加します。

Groups（グループの設定）

ユーザグループは同じ特権を共有するユーザの集まりです。作成したユーザグループについて、ログインポリシー、ブラウザポリシー、IP ポリシーを設定することができます。
作成したグループ及びポリシーは **Internal User Database > Groups タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

■ ユーザグループの追加

1. **Security > Authentication > Internal User Database > Groups タブ**の順にメニューをクリックし、以下の画面を表示します。

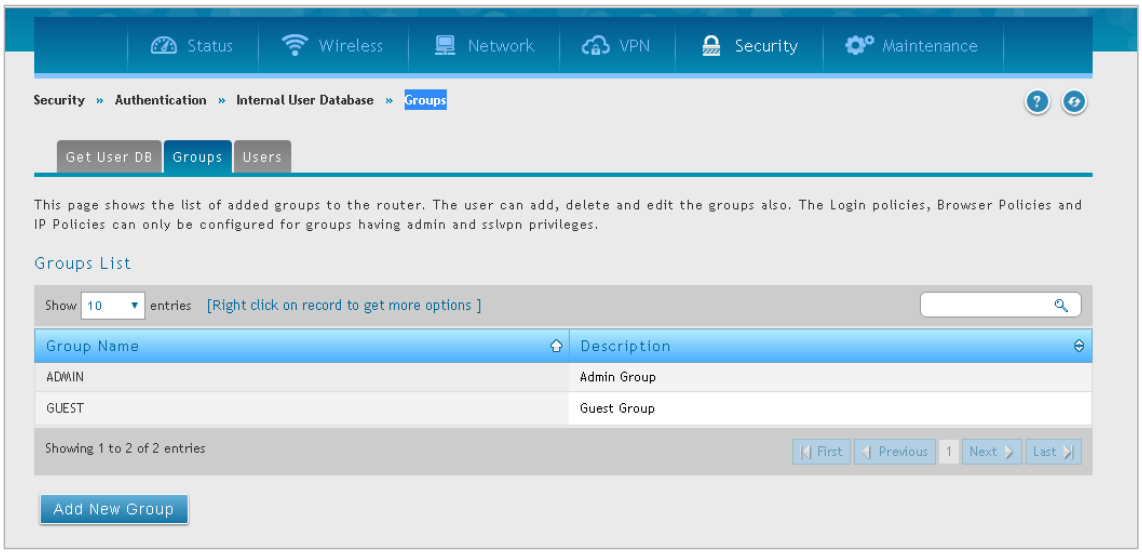

図 8-1　Internal User Database > Groups タブ画面

2. 「Add New Group」をクリックし、以下の画面を表示します。

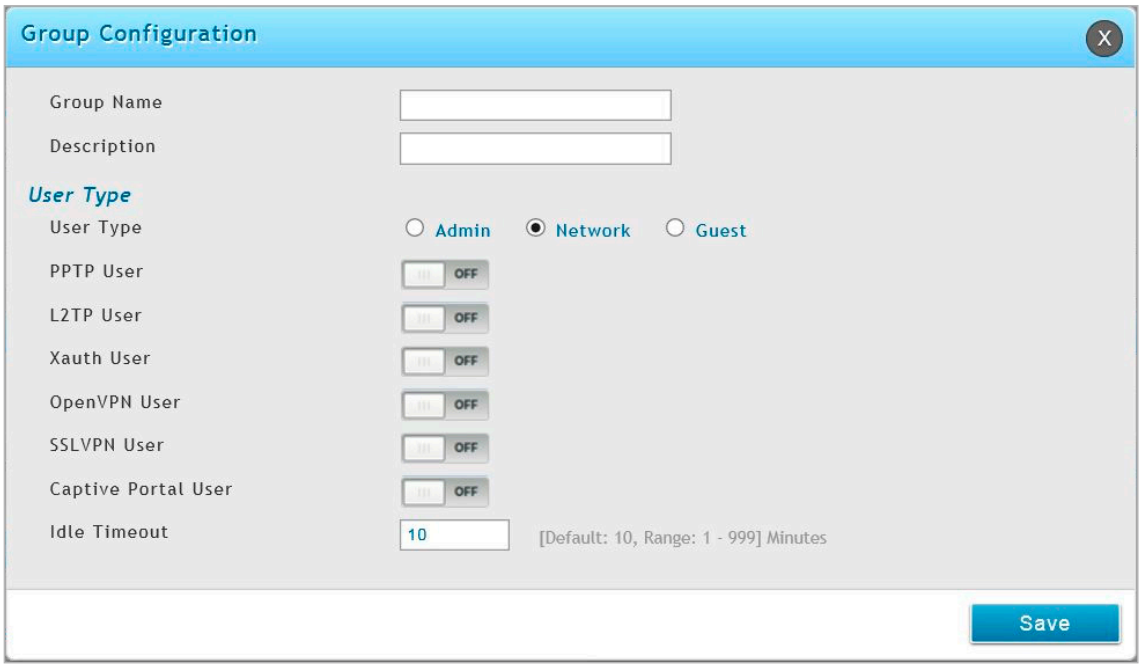

図 8-2　Group Configuration 画面

3. 以下の項目を設定します。

項目	説明
Group Name	グループ名を入力します。
Description	本ユーザグループの説明文を入力します。
User Type	
User Type	ユーザの種類を選択します。 • 「Admin」：このグループのすべてのユーザには、スーパーユーザ権限が付与されます。初期値では、Admin ユーザが 1 つ登録されています。 • 「Network 」：Admin の次に高いレベルの権限を付与されます。 • 「Guest 」：このグループのユーザには、閲覧権限のみが付与されます。 「Network」または「Admin」ユーザを選択した場合、「PPTP」「L2TP」「Xauth（Network グループのみ）」「SSLVPN」「Captive Portal」を有効にすることができます。
PPTP User	PPTP User を有効 / 無効にします。
L2TP User	L2TP User を有効 / 無効にします。
Xauth User	Xauth User を有効 / 無効にします。
OpenVPN User	OpenVPN User を有効 / 無効にします。
SSL VPN User	SSL VPN User を有効 / 無効にします。
Captive Portal User	Captive Portal User を有効 / 無効にします。
Idle Timeout	ユーザグループ内のユーザが Web 管理セッションを自動的にログアウトするまでの無通信の時間を入力します。「0」を設定した場合、ログアウトしません。

4. 「Save」をクリックし、設定を適用します。

■ ログインポリシーの設定

ユーザグループに対して、Web GUI へのログインアクセスを許可または拒否することができます。

1. **Security > Authentication > Internal User Database > Groups** の順にメニューをクリックし、以下の画面を表示します。

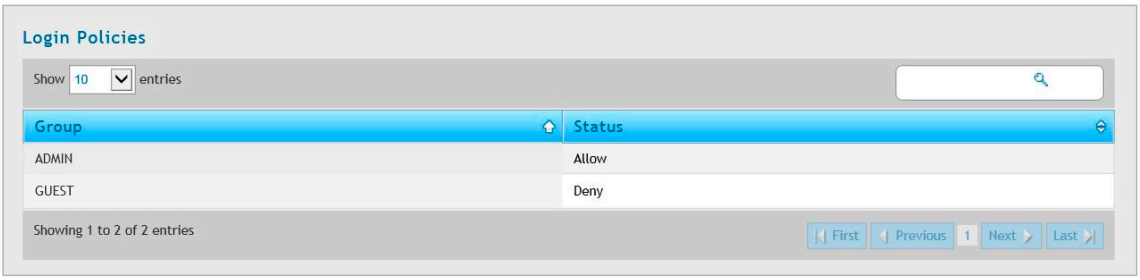

図 8-3　Login Policies 画面

2. エントリを右クリックして「Edit」を選択すると、以下の画面が表示されます。

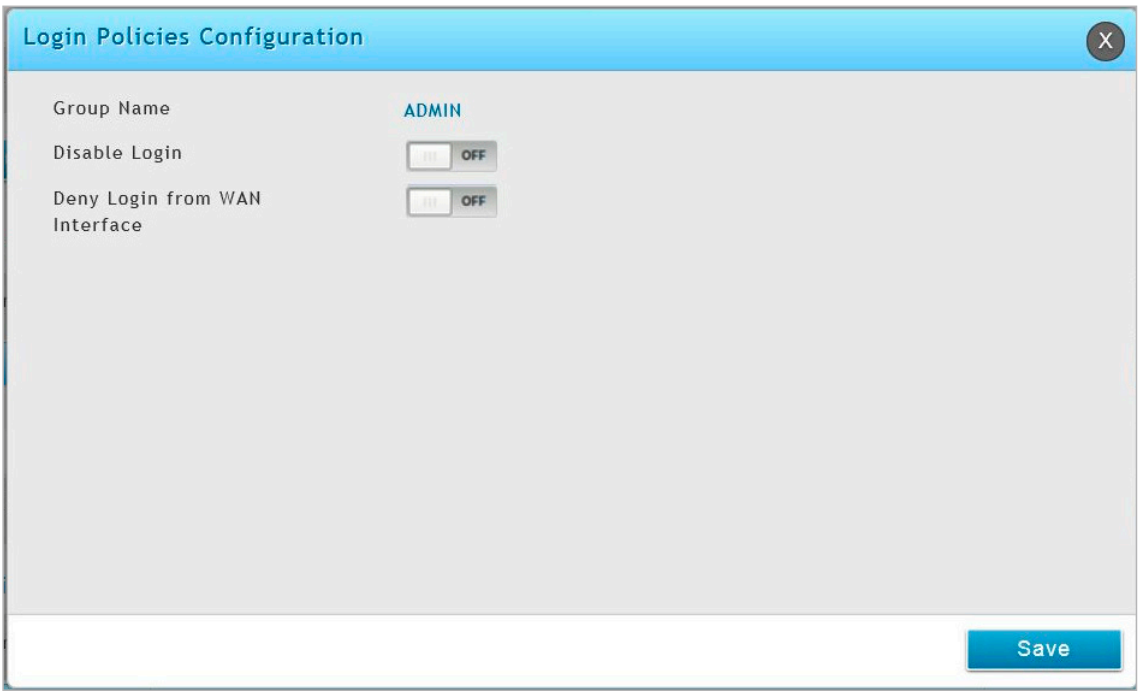

図 8-4　Login Policies Configuration 画面

3. 以下の項目を設定します。

項目	説明
Group Name	グループ名が表示されます。
Disable Login	選択したグループ内の全ユーザに対して Web GUI へのログインアクセスを許可または拒否します。 • 「ON」：ログインアクセスを無効にします。 • 「OFF」：ログインアクセスを有効にします。
Deny Login from WAN Interface	選択したグループ内の全ユーザに対して WAN2/DMZ ポートからの Web GUI へのログインアクセスを許可または拒否します。 • 「ON」：ログインアクセスを無効にします。 • 「OFF」：ログインアクセスを有効にします。

4. 「Save」をクリックし、設定を適用します。

■ ブラウザポリシーの設定

Web ブラウザから本製品の Web GUI にログインすることを許可または拒否することができます。

1. **Security > Authentication > Internal User Database > Groups** の順にメニューをクリックし、以下の画面を表示します。

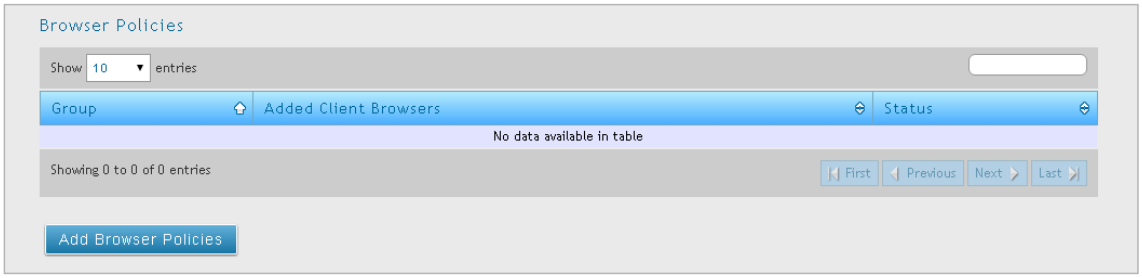

図 8-5　Browser Policies 画面

2. 「Add Browser Policies」をクリックし、以下の画面を表示します。

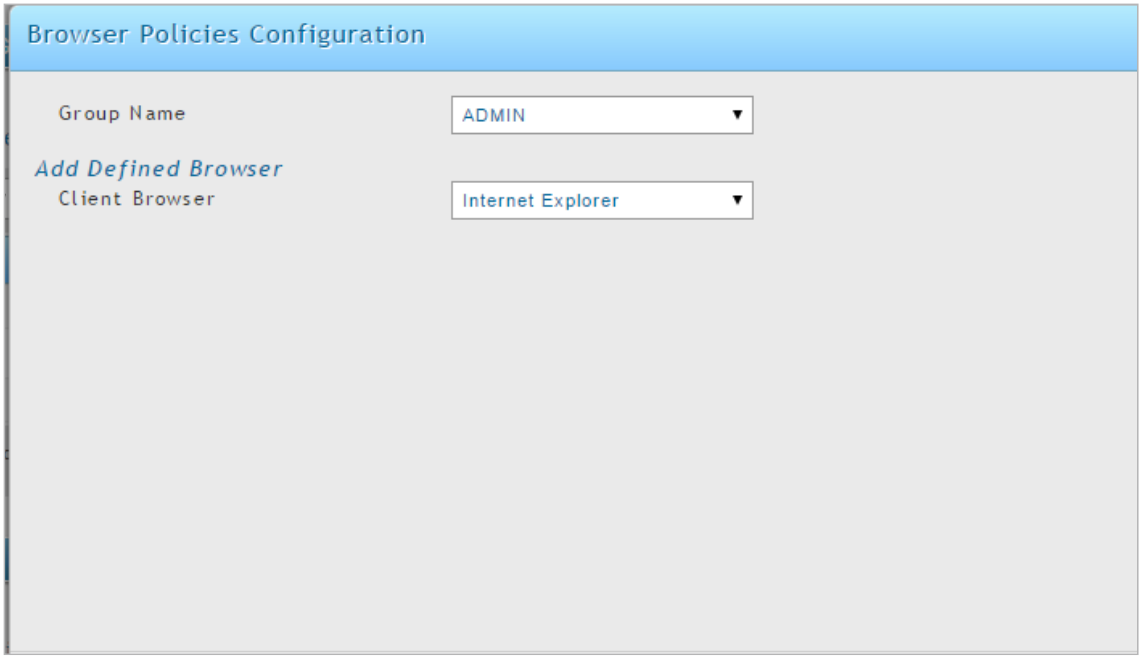

図 8-6　Browser Policies Configuration 画面

3. 以下の項目を設定します。

項目	説明
Group Name	プルダウンメニューからグループ名を選択します。
Client Browser	プルダウンメニューから Web ブラウザを選択します。

4. 「Save」をクリックし、設定を適用します。

IP ポリシーの設定

ユーザグループに IP の詳細なポリシーを設定します。
ユーザグループ内のユーザが、特定のネットワークまたは IP アドレスから本製品の Web GUI にログインすることを許可または拒否することができます。

1. **Security > Authentication > Internal User Database > Groups** の順にメニューをクリックし、以下の画面を表示します。

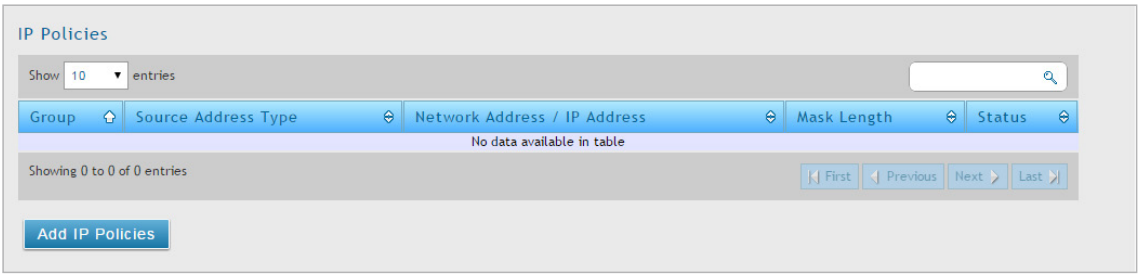

図 8-7　IP Policies 画面

2. 「Add IP Policies」をクリックし、以下の画面を表示します。

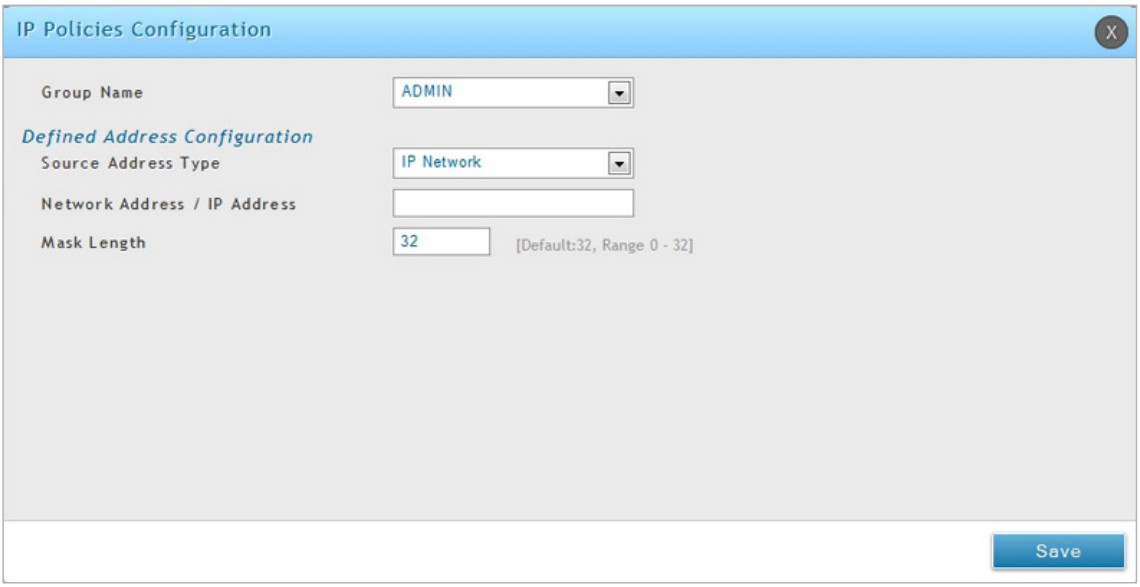

図 8-8　IP Policies Configuration 画面

3. 以下の項目を設定します。

項目	説明
Group Name	プルダウンメニューからグループ名を選択します。
Source Address Type	ソースアドレスのタイプを選択します。 • 「IP Address」：特定の IP アドレスを指定します。 • 「IP Network」：特定の IP ネットワークを指定します。
Network Address / IP Address	ネットワークまたは IP アドレスを入力します。
Mask Length	サブネットマスク長を入力します。（「IP Network」選択時）

4. 「Save」をクリックし、設定を適用します。

Users（ユーザの追加）

ユーザグループの作成後、グループにユーザを追加します。ユーザは個別または CSV 形式のファイルで一括インポートすることが可能です。

1. **Security > Authentication > Internal User Database > Users タブ**の順にメニューをクリックし、以下の画面を表示します。

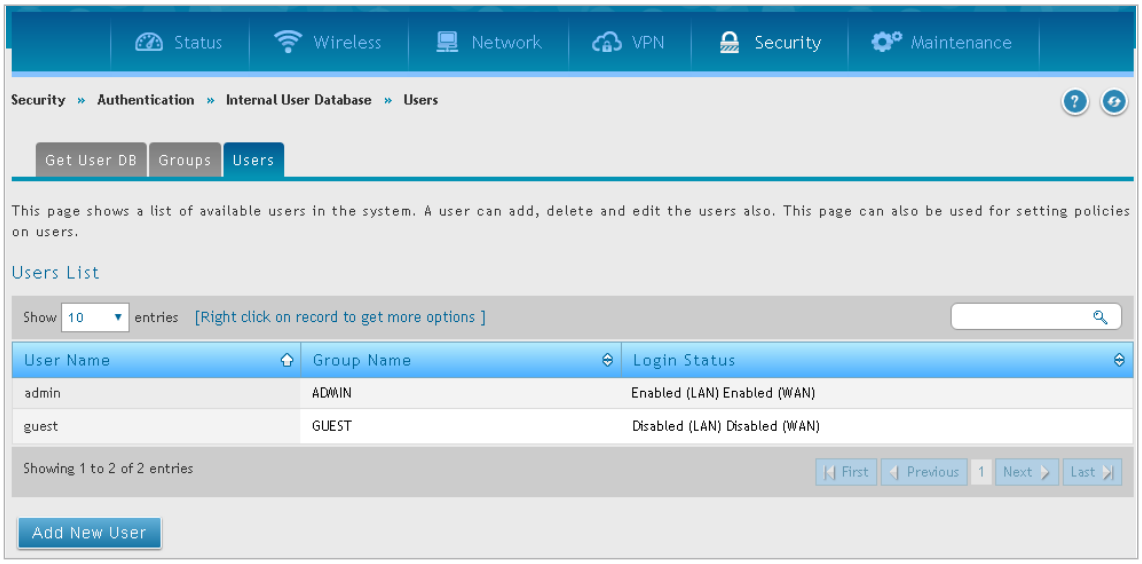

図 8-9　Internal User Database > Users タブ画面

2. 「Add New User」をクリックし、以下の画面を表示します。

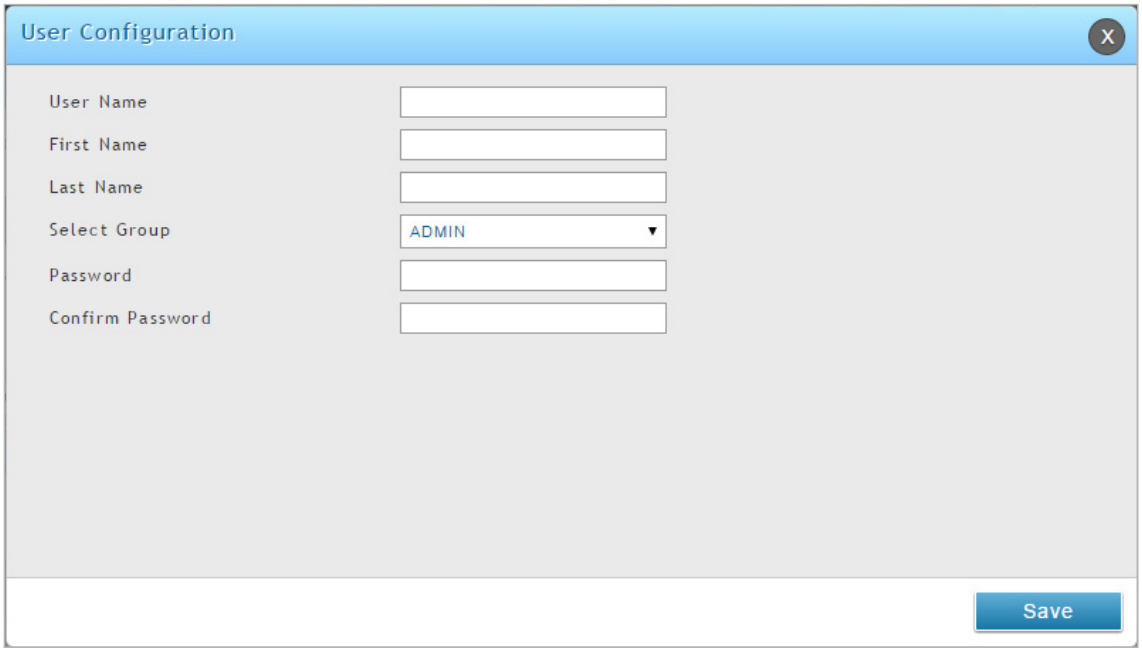

図 8-10　User Configuration 画面

3. 以下の項目を設定します。

項目	説明
User Name	固有の識別名となるユーザ名を入力します。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Select Group	ユーザが所属するグループを選択します。
Password	ユーザが Web GUI にアクセスする際に指定するログインパスワード（大文字と小文字を区別）を入力します。セキュリティのために、入力したパスワード文字は、「・」で表示されます。
Confirm Password	確認のため、再度パスワードを入力します。

4. 「Save」をクリックし、設定を適用します。

追加したユーザは **Internal User Database > Users タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

■ ユーザ情報の編集

管理者およびユーザのグループ、Web GUI のログインパスワードを変更することができます。

1. **Security > Authentication > Internal User Database > Users タブ**の順にメニューをクリック → 編集したいユーザ上で右クリックし、「Edit」（編集）を選択します。

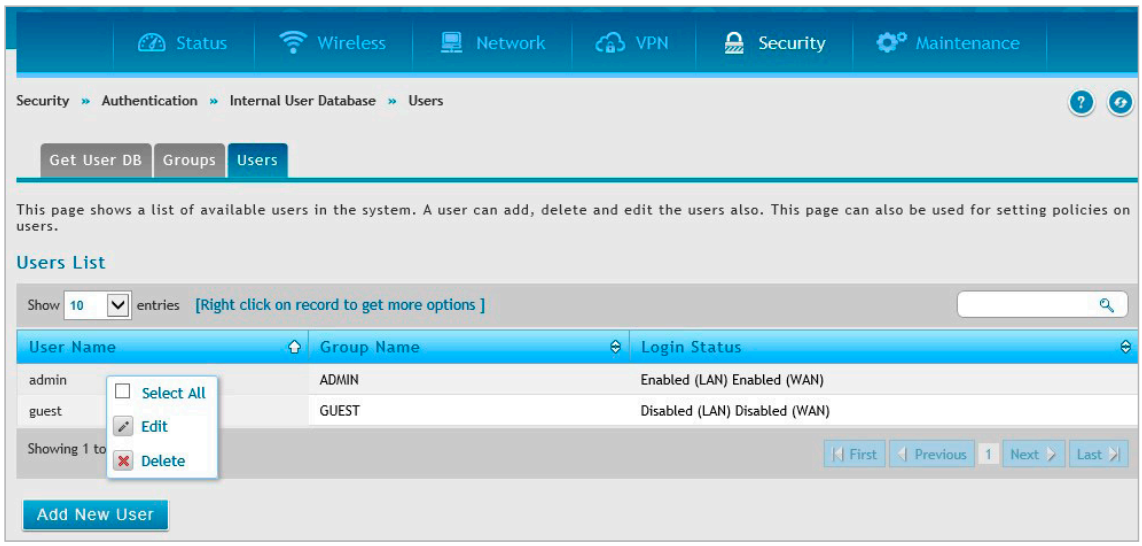

図 8-11　Internal User Database > Users タブ画面

2. 以下の画面が表示されます。ログインパスワードを変更する場合は、「Edit Password」を「ON」にします。

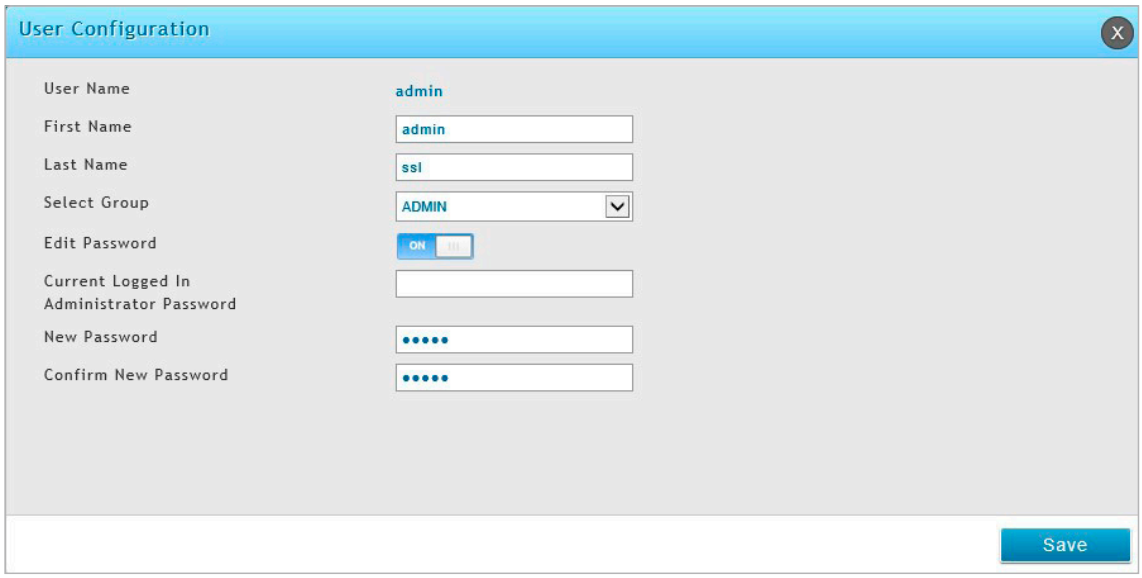

図 8-12　User Configuration 画面

3. 以下の項目を設定します。

項目	説明
User Name	固有の識別名となるユーザ名を入力します。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Select Group	ユーザが所属するグループを選択します。
Edit Password	Web GUI のログインパスワードを変更する場合は「ON」にします。
Current Logged In Administrator Password	現在設定されている Web GUI のログインパスワードを入力します。
New Password	Web GUI の新しいログインパスワード（大文字と小文字を区別）を入力します。セキュリティのために、入力したパスワード文字は、「・」で表示されます。
Confirm New Password	確認のため、再度新しいログインパスワードを入力します。

4. 「Save」をクリックし、設定を適用します。

注意　Web GUI のログインパスワードを変更した場合、「Save」をクリックすると一旦 Web GUI からログアウトします。
ログイン画面が表示されますので、新しいパスワードを入力して再度ログインしてください。

Get User DB（ユーザデータベースのインポート）

DSR の管理者は、適切な形式の CSV（Comma separated value）ファイルをインポートすることにより、内部ローカルデータベースに直接ユーザを追加することができます。本機能を使用することで、システムに多数のユーザを一括で追加することが可能です。また、必要に応じて同じファイルを別の DSR デバイスにアップロードすることもできます。ローカルユーザデータベースにアップロードされたユーザは、Web GUI で編集することができます。

1. **Security > Authentication > Internal User Database > Get User DB** の順にメニューをクリックし、以下の画面を表示します。

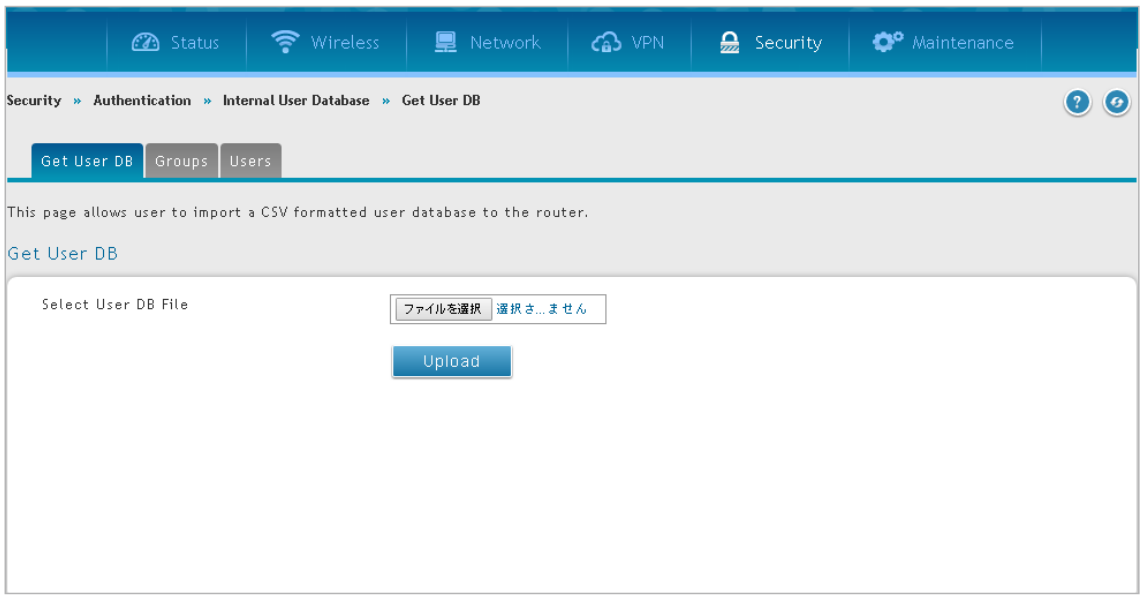

図 8-13　Internal User Database > Get User DB タブ画面

2. 「参照 /Browse」をクリックします。
3. CSV ファイルの場所に移動して、ファイルを選択し、「開く（Open）」をクリックします。
4. 「Upload」をクリックします。

■ ユーザデータベースの作成（CSV ファイル）

ユーザデータベースの CSV ファイルを定義するには、以下のパラメータを使用する必要があります。

1. 拡張子 .csv を持つ空のテキストファイルを作成します。
2. ファイルの各行は 1 つのユーザエントリに対応します。すべての行が CRLF（復帰改行）で終了する必要があります。このファイルにコメントや他のテキストを追加しないでください。
3. 形式のルール :
   a) すべてのフィールドを 2 重引用符で囲む必要があります。
   b) 連続したフィールドは「,」（カンマ）で区切ります。
   c) 行の前後に空白を入れてはいけません。
   d) フィールド間に空白を入れてはいけません。

CSV ユーザデータベースファイルの各行は次の形式に従う必要があります。

"UserName","FirstName","LastName","GroupName","Password","MultiLogin"

以下の値を定義するフィールドがあります。

- Username（文字列フィールド）: DSR のデータベースにおけるユーザ（識別子）で、ローカルユーザデータベースで固有である必要があります。
- FirstName（文字列フィールド）: ユーザの詳細であり、固有である必要はありません。
- LastName（文字列フィールド）: ユーザの詳細であり、固有である必要はありません。
- GroupName（文字列フィールド）: このユーザに関連付けられるグループ。
- MultiLogSup（ブーリアン値）: 本項目を有効（「1」）にすると、複数のユーザで単一のユーザ名とパスワードを共有できます。
- Password（文字列フィールド）: このユーザ名に割り当てるパスワード。

注意　ユーザデータベースの CSV アップロードを行う前に、Web GUI を使用してユーザに対応するグループ（CSV における「GroupName」）を作成する必要があります。

注意　ユーザデータベースの CSV では、上記のフィールドのいずれも空または NULL とすることはできません。

External Auth Server（外部認証）

Security > Authentication > External Auth Server メニュー
外部認証を行うサーバの設定について説明します。設定は以下のタブごとに行います。
「RADIUS Server」「POP3 Server」「POP3 Trusted CA」「LDAP Server」「AD Server」「NT Domain Server」

Radius Server（RADIUS サーバの設定）

クライアント接続の際に、RADIUS サーバによる認証を行います。
RADIUS サーバはユーザアカウントのデータベースを保持しており、ネットワークにアクセスしようとするユーザの認証を行います。プライマリ RADIUS サーバにアクセスできない場合は、セカンダリ / ターシャリ RADIUS サーバが認証を行います。

1. **Security > Authentication > External Auth Server > RADIUS Server タブ**の順にメニューをクリックし、以下の画面を表示します。

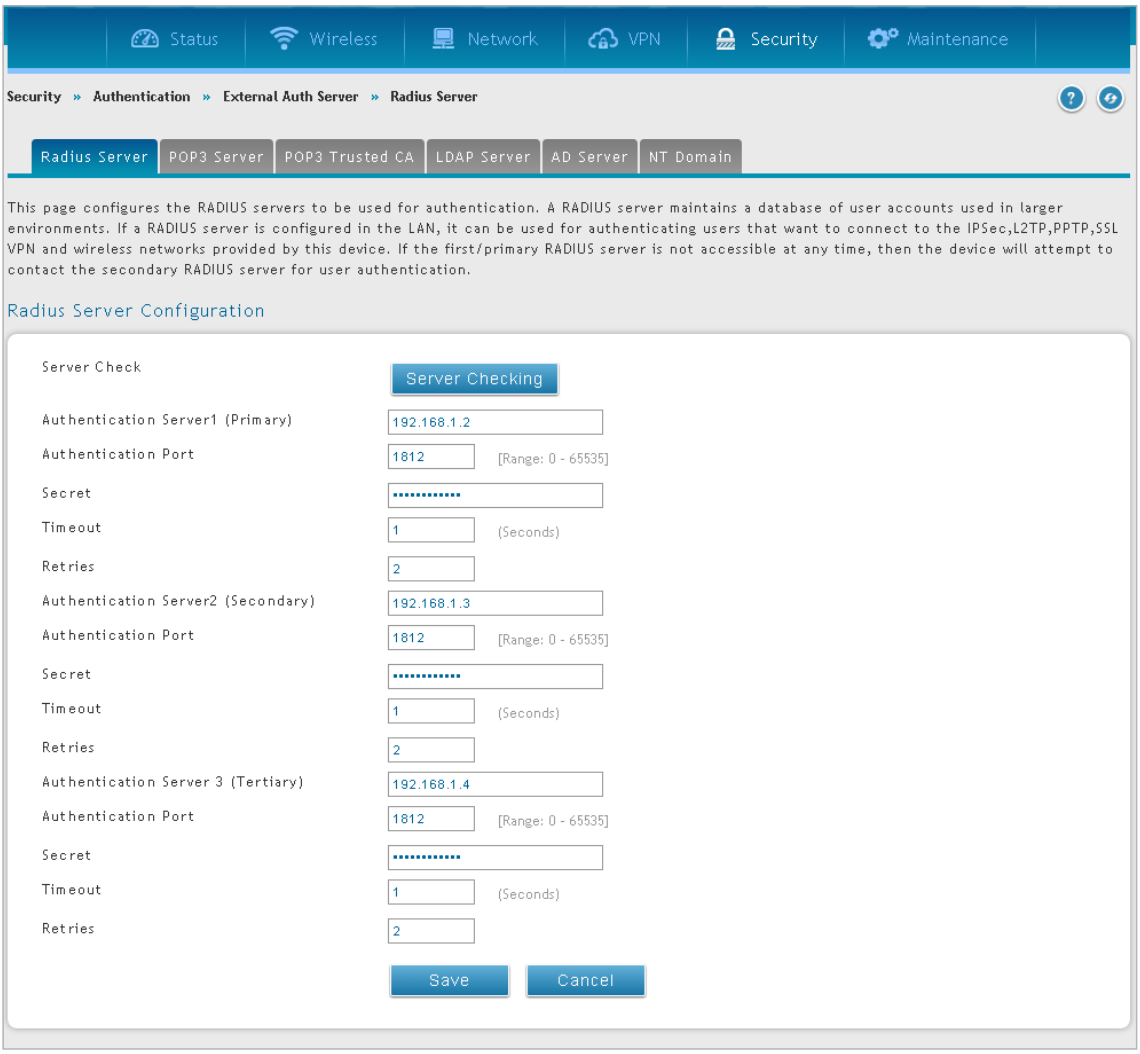

図 8-14　External Auth Server > RADIUS Server タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	RADIUS 認証サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。 「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Authentication Port	RADIUS 認証サーバのポートを指定します。
Secret	デバイスが設定済みの RADIUS サーバにログインするための秘密鍵を指定します。これは RADIUS サーバの秘密鍵に一致する必要があります。
Timeout	RADIUS サーバからの応答に対するルータの待ち時間（秒）を設定します。
Retries	RADIUS サーバへの接続試行回数を指定します。

3. 「Save」をクリックし、設定を適用します。

POP3 Server（POP3 サーバ）

POP3 は、TCP/IP 接続におけるメール通信で最も一般的に使用されるアプリケーション層のプロトコルです。暗号化トラフィックを POP3 サーバに送信する際に、ポート 995 経由の SSL 暗号化と共に認証サーバを使用します。POP3 サーバの証明書は、ユーザがアップロードした CA 証明書によって検証されます。SSL 暗号化が使用されない場合、ポート 110 が POP3 認証トラフィックに使用されます。

1. **Security > Authentication > External Auth Server > POP3 Server タブ**の順にメニューをクリックし、以下の画面を表示します。

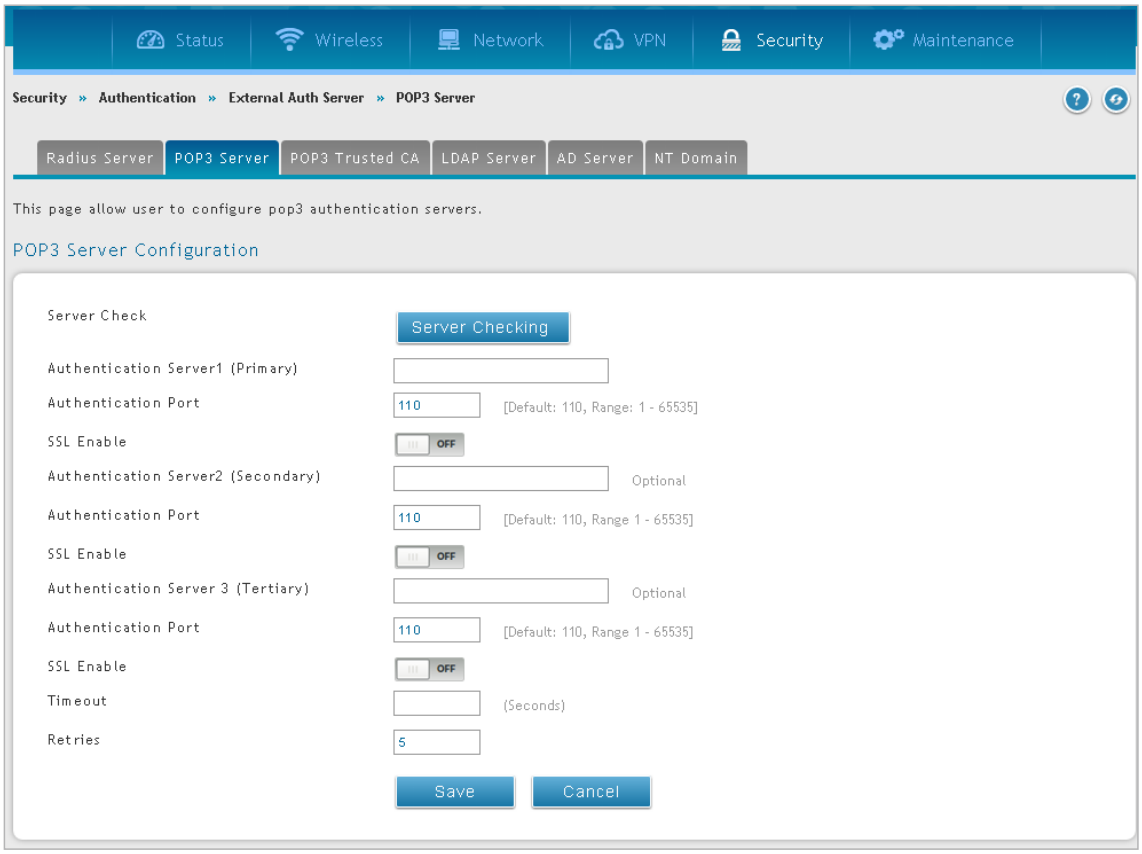

図 8-15　External Auth Server > POP3 Server タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	POP3 認証サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。 「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Authentication Port	RADIUS 認証サーバのポートを指定します。 • 設定可能範囲：1-65535 • 初期値：110
SSL Enable	POP3 の SSL サポートを有効にします。本オプションが有効な場合、CA（認証局）を選択する必要があります。
CA File	POP3 サーバの証明書を検証する CA（認証局）を指定します。
Timeout	POP3 サーバからの応答に対するルータの待ち時間（秒）を設定します。
Retries	POP3 サーバへの接続試行回数を指定します。

3. 「Save」をクリックし、設定を適用します。

POP3 Trusted CA（POP3 トラスト CA）

設定した認証サーバの ID を検証するために、POP3 ネゴシエーションの一部として CA ファイルが使用されます。
3 つの設定サーバごとに、認証に使用する固有の CA を持つことができます。

1. **Security > Authentication > External Auth Server > POP3 Trusted CA タブ**の順にメニューをクリックし、以下の画面を表示します。

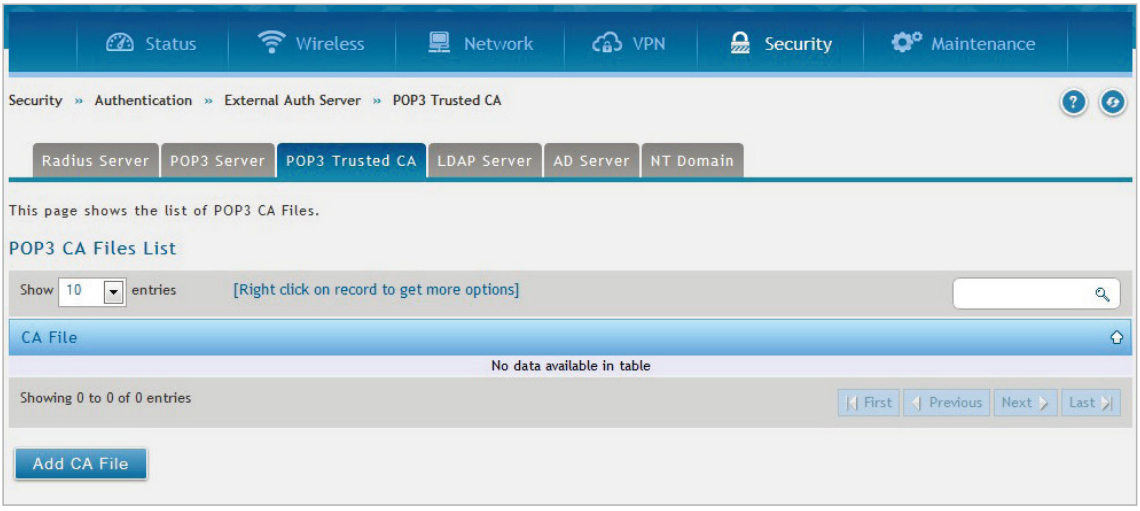

図 8-16　External Auth Server > POP3 Trusted CA タブ

2. 「Add CA File」をクリックして、CA ファイルを追加します。

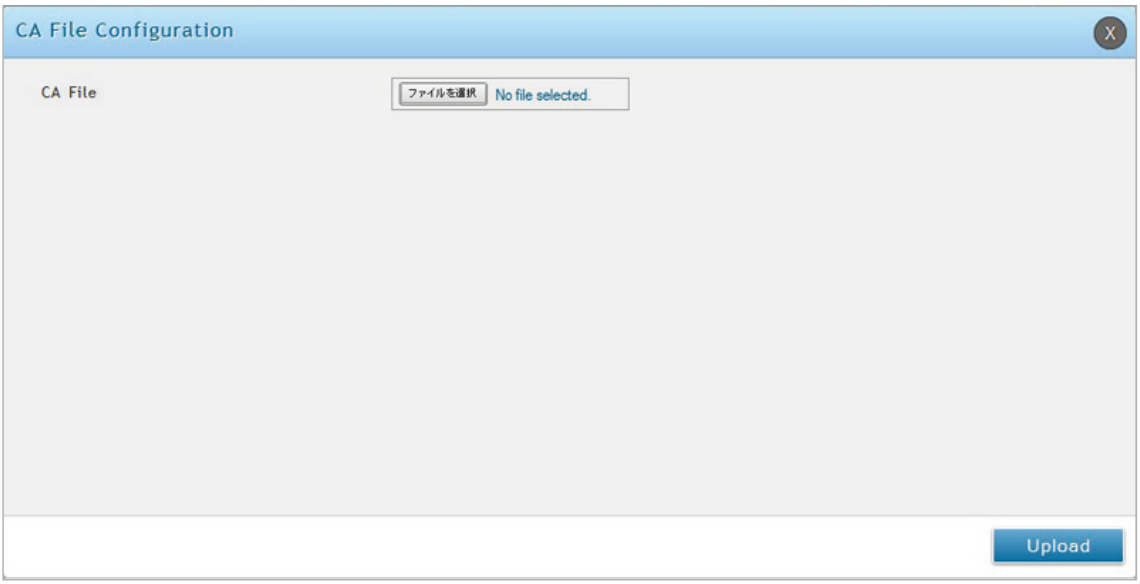

図 8-17　CA File Configuration 画面

3. 「参照 /Browse」をクリックして、CA ファイルを参照します。ファイルを選択後、「Upload」をクリックします。

LDAP Server（LDAP サーバ）

LDAP サーバは、ディレクトリ構造により大容量のユーザデータベースを保持します。ディレクトリ構造ではユーザ情報が階層的に保存されるため、同じユーザ名で異なるグループに所属するユーザを認証することができます。なお、Windows または Linux サーバにおける LDAP サーバの設定は、ユーザ認証用の NT ドメインや Active Directory サーバの設定よりも格段にシンプルになっています。

ルータに設定された詳細情報は、ルータとそのホストの認証のために送信されます。LDAP サーバがルータを認証する上で、LDAP 属性、ドメイン名（DN）、場合によっては管理者アカウントとパスワードがキーフィールドとなります。

1. **Security > Authentication > External Auth Server > LDAP Server タブ**の順にメニューをクリックし、以下の画面を表示します。

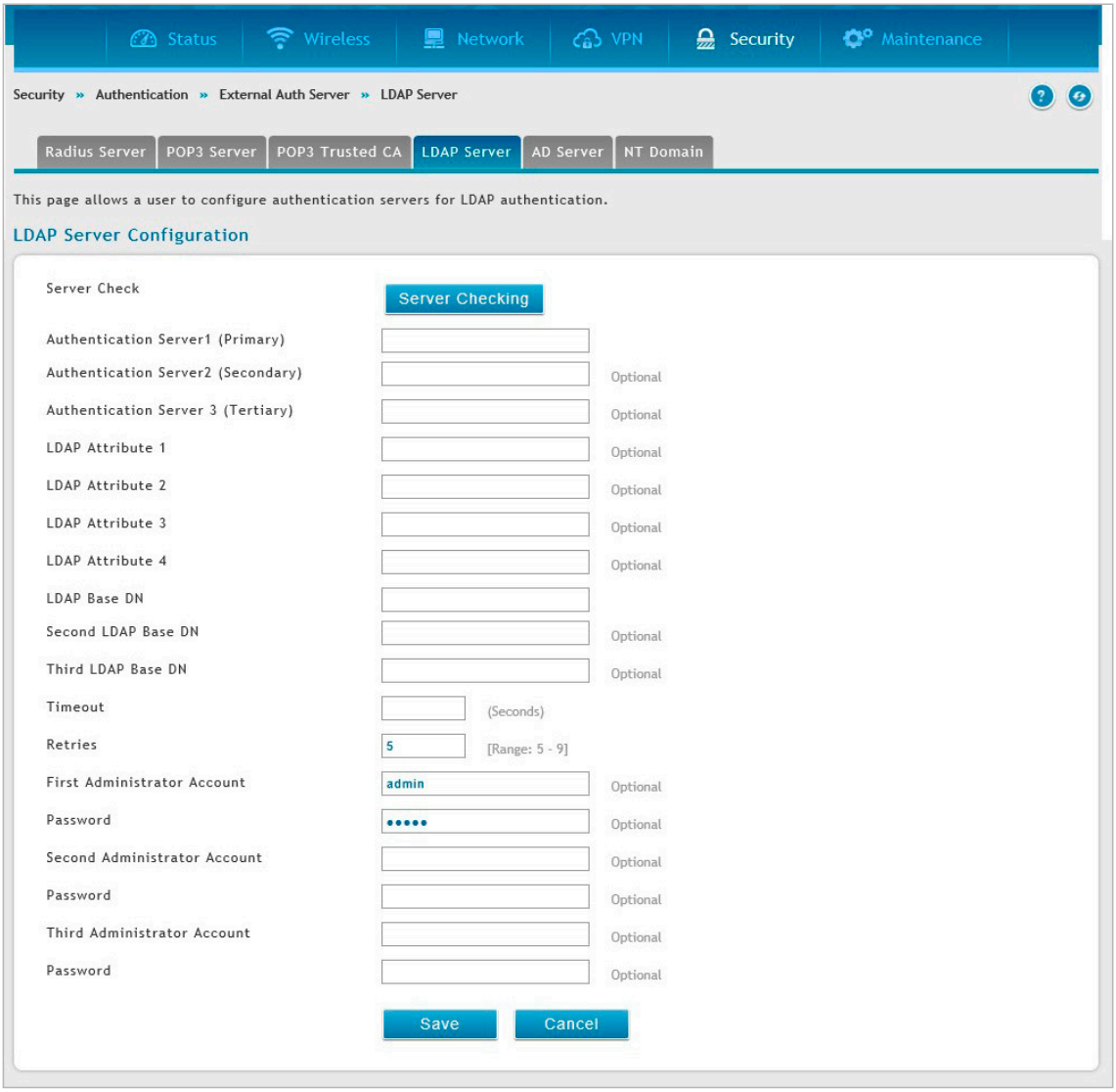

図 8-18　External Auth Server > LDAP Server タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	LDAP 認証サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。 「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
LDAP Attribute	LDAP サーバで設定された LDAP ユーザに関連する属性を指定します。これらは、SAM アカウント名、対応するドメイン名などの属性を含みます。同じユーザ名を持つ異なるユーザを識別するために使用されます。
LDAP Base DN	LDAP 認証におけるベースドメイン名を指定します。
Timeout	ルータが LDAP サーバからの応答を待つ待機時間（秒）を設定します。
Retries	ルータから LDAP サーバへの接続試行回数を決定します。
Administrator Account	PPTP/L2TP 接続で LDAP 認証が必要な場合に使用される管理者アカウント情報を入力します。「First Administrator Account」「Second Administrator Account」「Third Administrator Account」の 3 つを設定可能です。
Password	管理パスワードを入力します。

3. 「Save」をクリックし、設定を適用します。

AD Server（アクティブディレクトリサーバ）

アクティブディレクトリ認証は、NT ドメイン認証の高機能バージョンです。
Organizational Units（OUs）内でグループ化されているユーザの認証に Kerberos プロトコルが使用されます。NT ドメインサーバでサポートされるユーザは数千程度ですが、Active Directory サーバは通常百万単位のユーザをサポートすることができるストラクチャを有しています。
設定された認証サーバと Active Directory ドメインは、外部の Windows ベースサーバのユーザディレクトリを使用して、ユーザを認証します。この認証方法は「SSL VPN」クライアントで一般的であり、「IPSec」「PPTP」「L2TP」クライアント認証などでも有効です。

1. **Security > Authentication > External Auth Server > AD Server タブ**の順にメニューをクリックし、以下の画面を表示します。

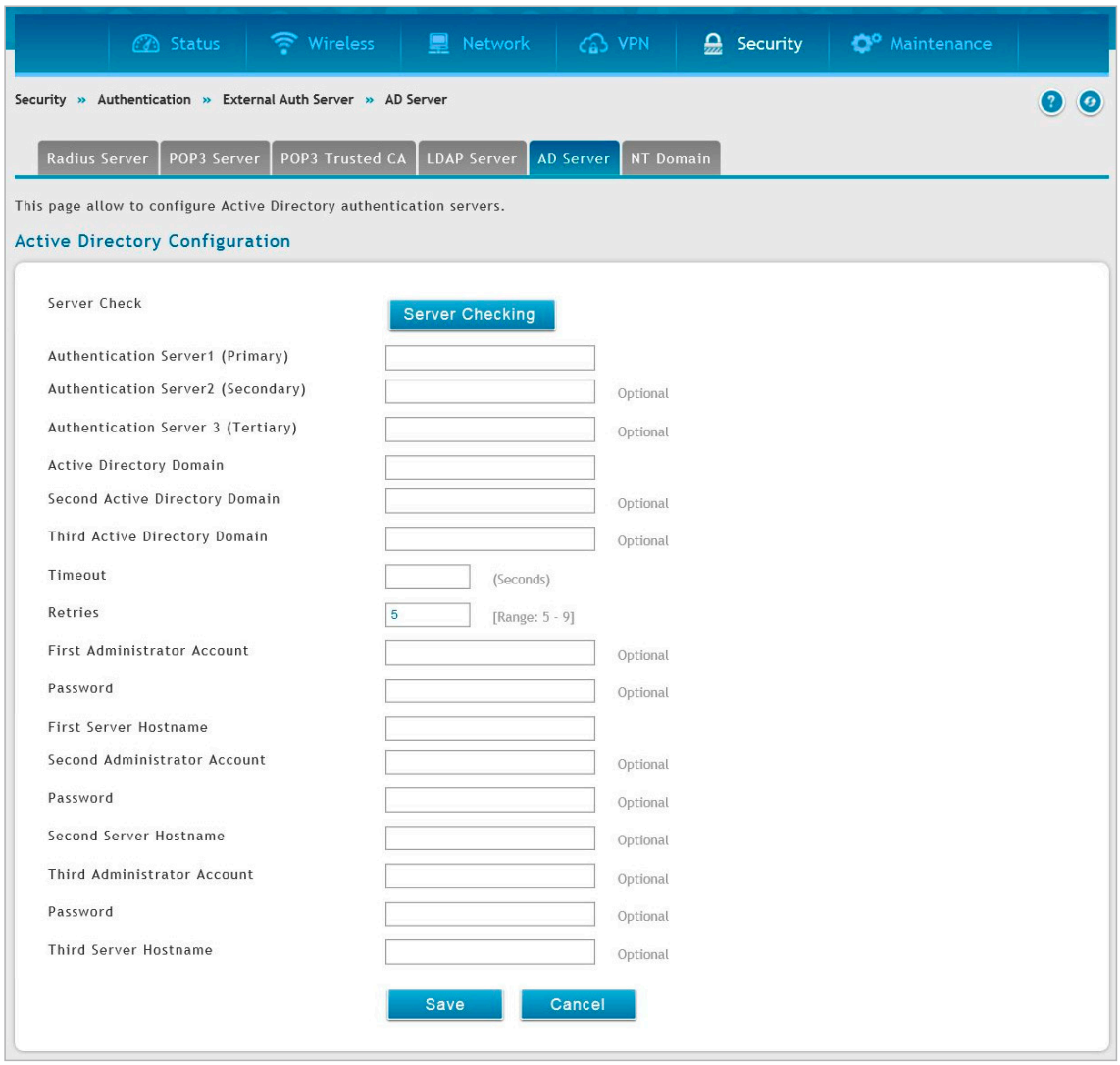

図 8-19　External Auth Server > AD Server タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	AD サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。 「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Active Directory Domain	アクティブディレクトリドメイン名を入力します。オプションとして「Second Active Directory Domain」「Third Active Directory Domain」も設定可能です。
Timeout	AD サーバからの応答を待つ待機時間（秒）を指定します。
Retries	ルータから認証サーバへの認証試行回数を指定します。
Administrator Account	PPTP/L2TP 接続で認証が必要な場合に使用される管理者アカウント情報を入力します。 「First Administrator Account」「Second Administrator Account」「Third Administrator Account」の 3 つを設定可能です。

3. 「Save」をクリックし、設定を適用します。

NT Domain Server（NT ドメインサーバ）

NT ドメインサーバは事前に設定済みのワークグループフィールドを経由したユーザとホストの認証を行います。通常、認証ユーザのディレクトリ集約のため、認証ドメインの管理には Windows サーバまたは Samba サーバが使用されます。

1. **Security > Authentication > External Auth Server > NT Domain タブ**の順にメニューをクリックし、以下の画面を表示します。

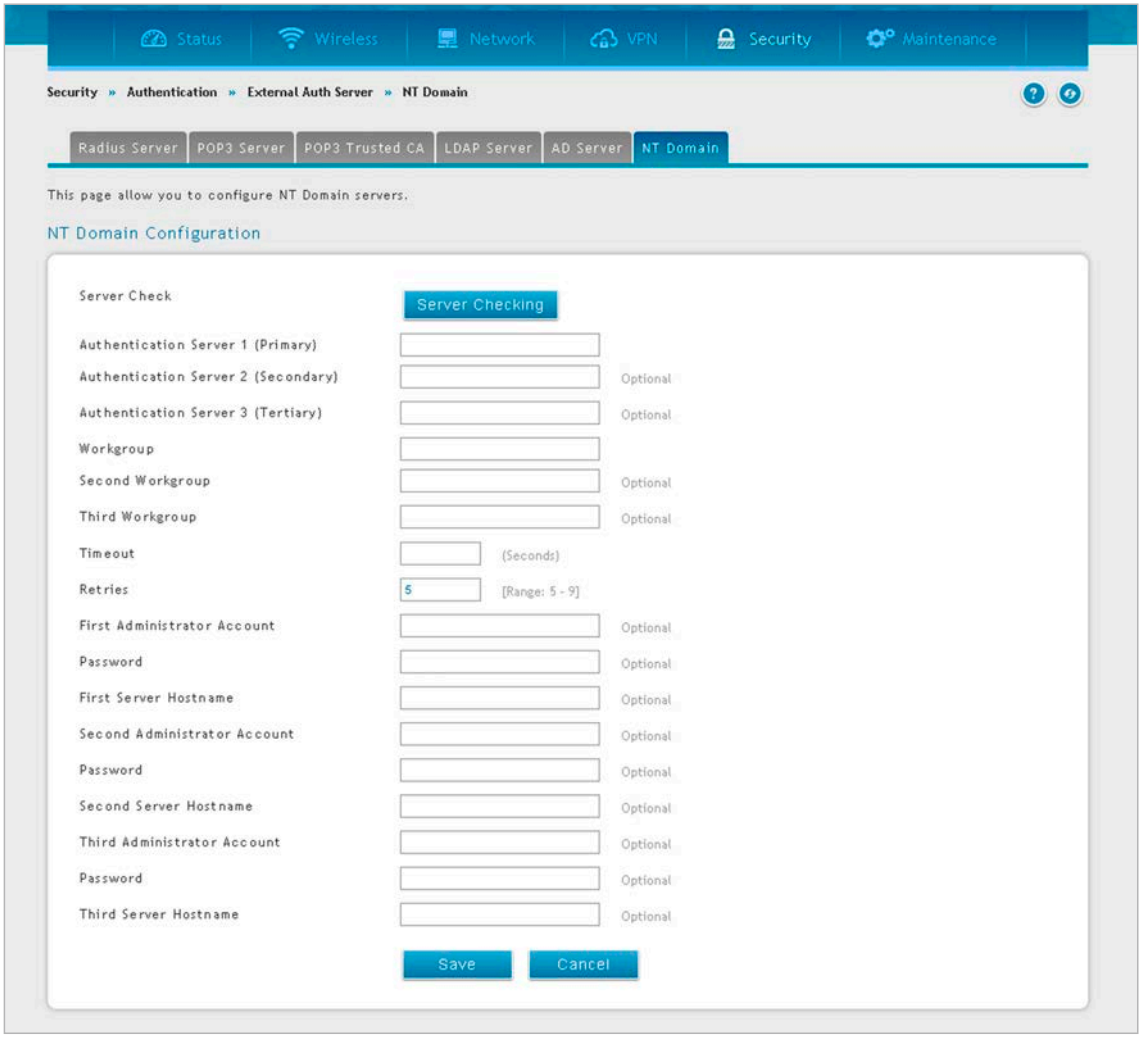

図 8-20　External Auth Server > NT Domain タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	NT ドメインサーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。 「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Workgroup	NT ドメイン認証に必要なワークグループを入力します。 「Second Workgroup」「Third Workgroup」まで設定可能です。
Timeout	NT ドメインサーバからの応答を待つ待機時間（秒）を指定します。
Retries	NT ドメインサーバへの認証試行回数を指定します。
Administrator Account	PTP/L2TP 接続で認証が必要な場合に使用される管理者アカウント情報を入力します。 「First Administrator Account」「Second Administrator Account」「Third Administrator Account」の 3 つを設定可能です。
Password	管理パスワードを入力します。
Server Hostname	サーバのホスト名を入力します。「First Server Hostname」「Second Server Hostname」「Third Server Hostname」の 3 つを設定可能です。

3. 「Save」をクリックし、設定を適用します。

Radius Accounting（Radius アカウンティング設定）

Security > Authentication > Radius Accounting メニュー

本画面では、ユーザの Radius アカウンティング認証の有効化 / 無効化を行います。また、定義済み Radius サーバに対してアカウンティングメッセージ内でセッションのトラフィック統計が送信される間隔（Accounting Interim Interval）の設定が可能です。

Radius Accounting（Radius アカウンティング）

以下の手順に従って Radius サーバへの接続設定を行います。

1. **Security > Authentication > Radius Accounting > Radius Accounting タブ**の順にメニューをクリックし、以下の画面を表示します。

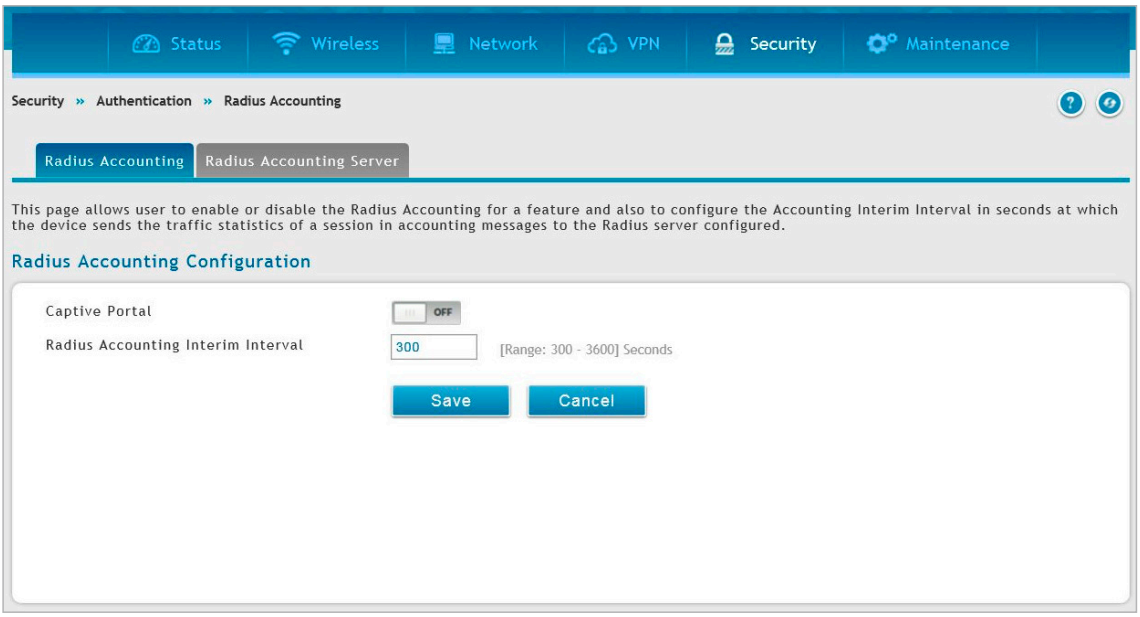

図 8-21　Radius Accounting > Radius Accounting タブ画面

2. 以下の項目を設定します。

項目	説明
Captive Portal	「ON」: キャプティブポータルの Radius アカウンティング機能を有効にします。 「OFF」: キャプティブポータルの Radius アカウンティング機能を無効にします。
Radius Accounting Interim Interval	デバイスから Radius Accounting（Interim-Update）パケットが送信される間隔を設定します。 • 設定可能範囲：300-3600（秒） • 初期値：300（秒）

3. 「Save」をクリックし、設定を適用します。

Radius Accounting Server（Radius アカウンティングサーバ）

RADIUS アカウンティングサーバの設定について説明します。プライマリ RADIUS サーバに接続できない場合、デバイスはセカンダリ RADIUS サーバに対してアカウンティングリクエスト送信のコンタクトを試行します。

1. **Security > Authentication > Radius Accounting > Radius Accounting Server タブ**の順にメニューをクリックし、以下の画面を表示します。

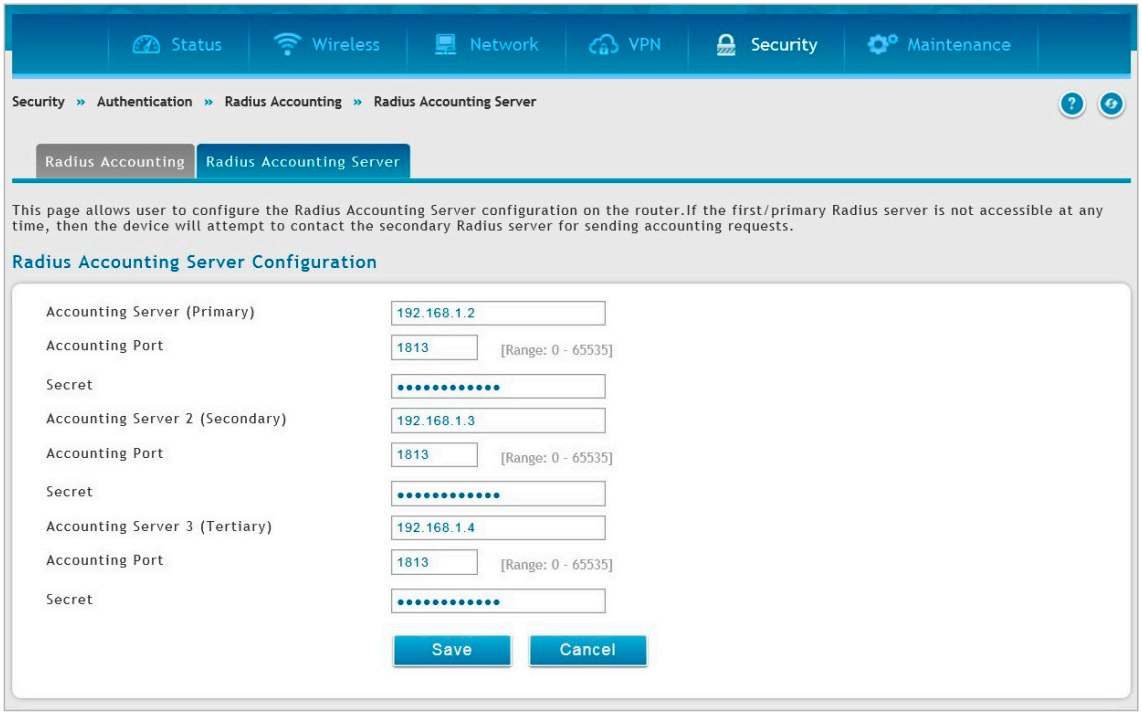

図 8-22　Radius Accounting > Radius Accounting Server タブ画面

2. 以下の項目を設定します。

項目	説明
Accounting Server	RADIUS アカウンティングサーバの IP アドレスを入力します。サーバは以下の 3 つを登録できます。 「Accounting Server (Primary)」「Accounting Server 2 (Secondary)」「Accounting Server 3 (Tertiary)」
Accounting Port	Radius アカウンティングサーバのポート番号を入力します。 • 設定可能範囲：0-65535 • 初期値：1813
Secret	デバイスが設定済みの RADIUS サーバにログインするための秘密鍵を指定します。これは RADIUS サーバの秘密鍵に一致する必要があります。

3. 「Save」をクリックし、設定を適用します。

Login Profiles（ログインプロファイル）

Security> Authentication> Login Profiles メニュー

無線クライアントがアクセスポイントの SSID や VLAN に接続する際、ログイン画面が表示されます。
本項目では、ログイン画面のカスタマイズ方法について説明します。

1. **Security > Authentication > Login Profiles** の順にメニューをクリックし、以下の画面を表示します。

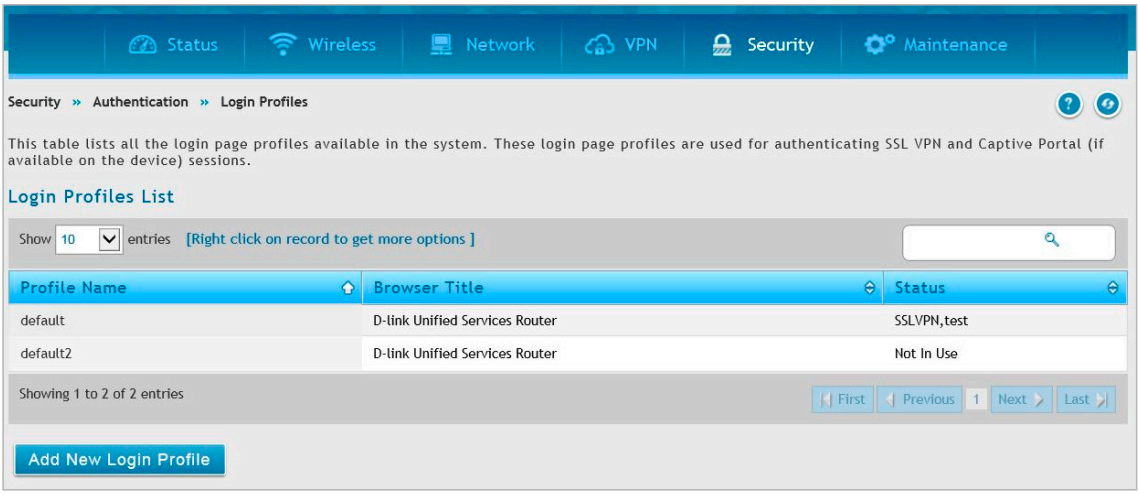

図 8-23　Login Profiles 画面

2. 「Add New Login Profile」をクリックし、以下の画面を表示します。

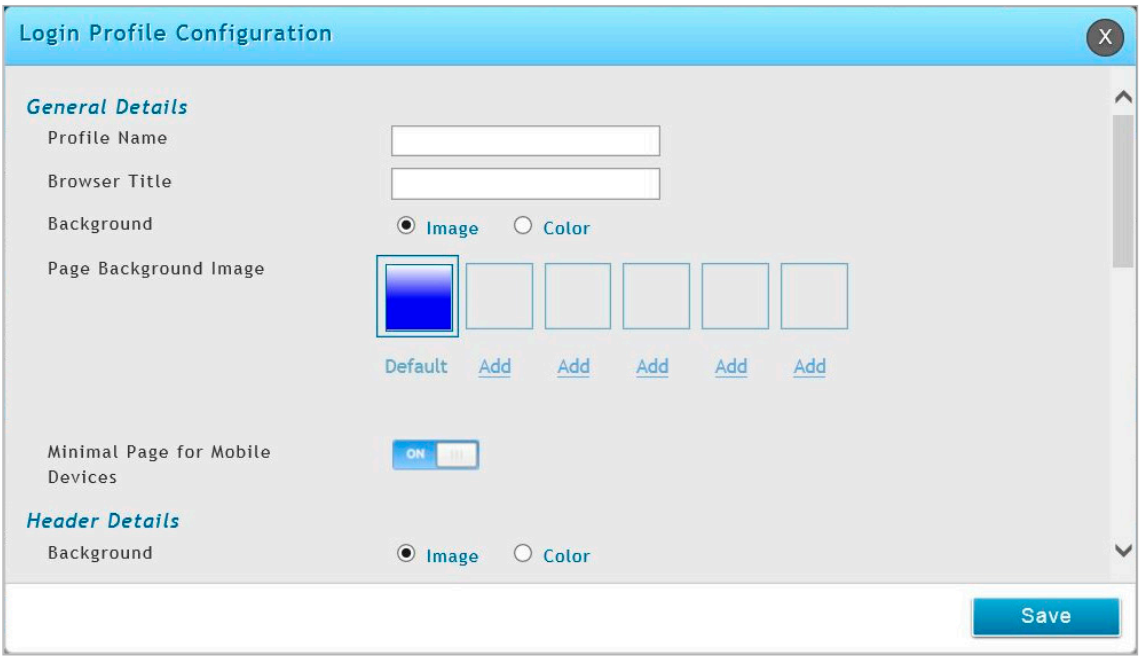

図 8-24　Login Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
General Details	
Profile Name	キャプティブポータルプロファイルの名称を入力します。他のプロファイルと区別できる名前を設定します。
Browser Title	キャプティブポータルセッション中にブラウザのタイトルとして表示される文字列を入力します。
Background	キャプティブポータルセッション中に表示されるログインページの背景として、画像またはカラーを選択します。 • 「Image」：ページの背景として画像を表示します。「Page Background Image」フィールドを使用して、背景画像を選択します。 • 「Color」：ページの背景色を設定します。プルダウンメニューから色を選択します。
Page Background Image	「Background」に「Image」を選択した場合、キャプティブポータルセッション中に表示されるページの背景画像を選択します。新しく画像ファイルをアップロードするには、「Add」をクリックします。
Page Background Upload	画像ファイルをアップロードします。「Page Background Image」で「Add」クリックすると、本項目が表示されます。画像ファイルを指定後、「Upload」をクリックします。アップロードできる画像の最大サイズは 100KByte です。
Page Background Color	「Background」に「Color」を選択した場合、キャプティブポータルセッション中に表示されるページの背景色をプルダウンメニューから選択します。
Custom Color	「Page Background Color」に「Custom」を選択した場合、HTML のカラーコードを入力します。
Minimal Page for Mobile Devices	モバイル端末で Web ページを適切に表示させる機能です。
Header Details	
Background	キャプティブポータルセッション中に表示されるログインページのヘッダーとして、画像またはカラーを選択します。 • 「Image」：ページの背景として画像を表示します。「Header Background Image」フィールドを使用して、背景画像を選択します。 • 「Color」：ページの背景色を設定します。プルダウンメニューから色を選択します。
Header Background Image	「Background」に「Image」を選択した場合、キャプティブポータルセッション中に表示されるページのヘッダー画像を選択します。新しく画像ファイルをアップロードするには、「Add」をクリックします。
Header Background Upload	画像ファイルをアップロードします。「Page Background Image」で「Add」クリックすると、本項目が表示されます。画像ファイルを指定後、「Upload」をクリックします。アップロードできる画像の最大サイズは 100KByte です。
Header Background Color	「Background」に「Color」を選択した場合、キャプティブポータルセッション中に表示されるページのヘッダー色をプルダウンメニューから選択します。
Custom Color	「Header Background Color」に「Custom」を選択した場合、HTML のカラーコードを入力します。
Header Caption	キャプティブポータルセッション中にログインページのヘッダに表示されるテキストを入力します。
Caption Font	ヘッダテキストのフォントを選択します。
Font Size	ヘッダテキストのフォントサイズを選択します。
Font Color	ヘッダテキストのフォント色を選択します。
Login Details	
Login Section Title	キャプティブポータルセッションへのログイン時に表示されるログインボックスのタイトルに表示されるテキストを入力します。 本項目はオプションです。
Welcome Message	キャプティブセッションへのログインに成功した場合に表示されるウェルカムメッセージを入力します。 本項目はオプションです。
Error Message	キャプティブセッションへのログインに失敗した場合に表示されるエラーメッセージを入力します。 本項目はオプションです。
Advertisement Details	
Enable Advertisement	広告の表示の有無を指定します。
Ad Place	広告の表示箇所を指定します。「Top」「Bottom」から指定できます。
Ad Content	広告の内容を指定します。
Font	広告のフォントを指定します。
Font Size	広告のフォントサイズを指定します。
Font Color	広告のフォント色を指定します。
Footer Details	
Change Footer Content	ログインページのフッターコンテンツへの変更を有効または無効にします。
Footer Content	「Change Footer Content」をチェックした場合、フッターに表示されるテキストを入力します。
Footer Font Color	「Change Footer Content」がチェックした場合、フッターに表示される色を入力します。

4. 「Save」をクリックし、設定を適用します。

Services Route Management（サービスルート管理）

Security > Authentication > Services Route Management メニュー

サービスルート管理機能では、認証でサービストラフィックが送信されるインタフェースを設定することができます。また、認証用としてトンネルのリモート LAN ネットワーク上の Radius サーバを利用することも可能です。

1. **Security > Authentication > Services Route Management** の順にメニューをクリックし、以下の画面を表示します。

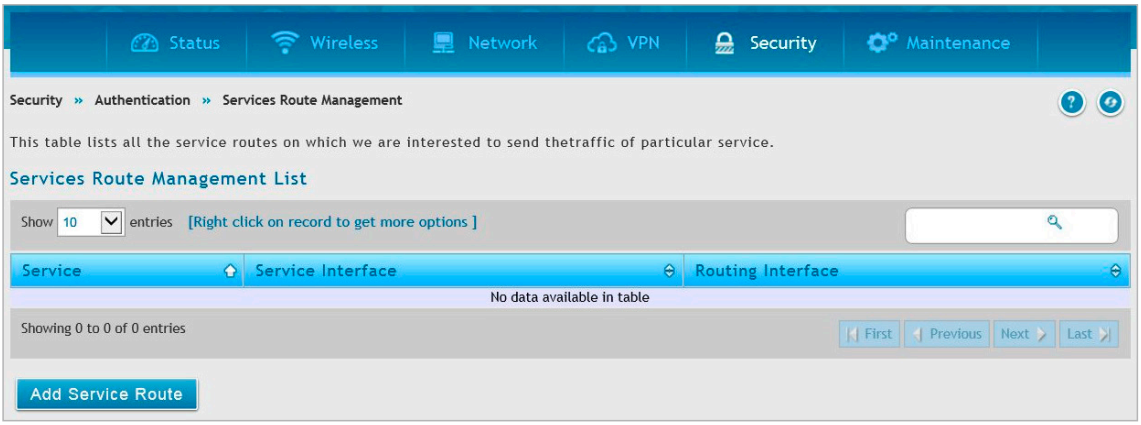

図 8-25　Services Route Management 画面

2. 「Add Service Route」をクリックし、以下の画面を表示します。

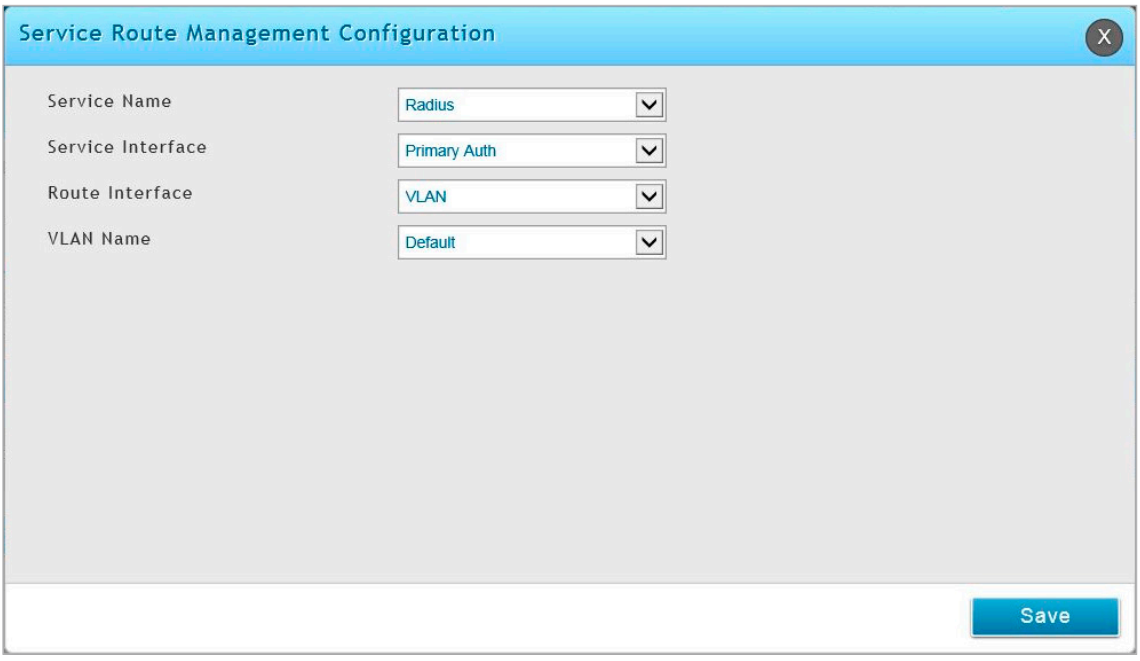

図 8-26　Service Route Management Configuration 画面

3. 以下の項目を設定します。

項目	説明
Service Name	サービスを選択します。
Service Interface	サービスのインタフェースを選択します。
Route Interface	トラフィックが送信されるインタフェースを選択します。「VLAN」または「IPSec」から選択します。
VLAN Name	「Route Interface」で「VLAN」を選択した場合、ルートの VLAN を選択します。この VLAN 上でトラフィックが送信されます。
Policy Name	「Route Interface」で「IPSec」を選択した場合、ルートの IPSec ポリシーを選択します。このポリシー上でトラフィックが送信されます。

4. 「Save」をクリックし、設定を適用します。

DUA External CP Web（DUA 外部キャプティブポータル Web サーバ）

Security > Authentication > DUA External CP Web メニュー

DUA 外部キャプティブポータル Web サーバの設定方法について説明します。

1. **Security > Authentication > DUA External CP Web** の順にメニューをクリックし、以下の画面を表示します。

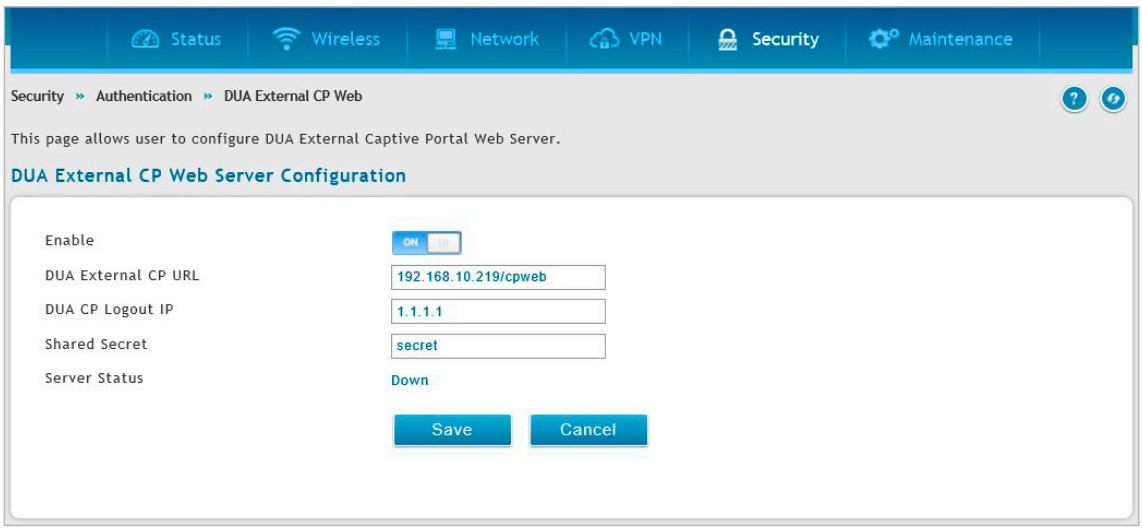

図 8-27　DUA External CP Web 画面

2. 以下の項目を設定します。

項目	説明
Enable	DUA 外部キャプティブポータル Web サーバを有効または無効にします。
DUA External CP URL	DUA 外部サーバの URL を入力します。
DUA CP Logout IP	設定する CP ログアウト IP を入力します。
Shared Secret	DUA 外部サーバに対して設定する共有シークレットを入力します。
Server Status	DUA 外部 Web サーバの現在のステータスが表示されます。

3. 「Save」をクリックし、設定を適用します。

Web Content Filter（Web コンテンツフィルタリング）

Security > Web Content Filter メニュー
Web コンテンツフィルタリングは、特定のインターネットサービスへの接続をブロックする機能です。
スタティックフィルタリング、ダイナミックフィルタリング、URL フィルタリング ACL の設定方法について説明します。

Static Filtering（スタティックフィルタリング）

Security > Web Content Filter > Static Filtering メニュー
スタティックフィルタリングにより、Web プロキシや Java など、特定のインターネットサービスをブロックすることができます。「Static Filtering」タブでブロックするサービスを選択します。
また、「Approved URL」タブと「Blocked URL」タブでは許可または拒否する URL のリストを登録できます。

Static Filtering（スタティックフィルタリング）

1. **Security > Web Content Filter > Static Filtering > Static Filtering タブ**の順にメニューをクリックし、以下の画面を表示します。

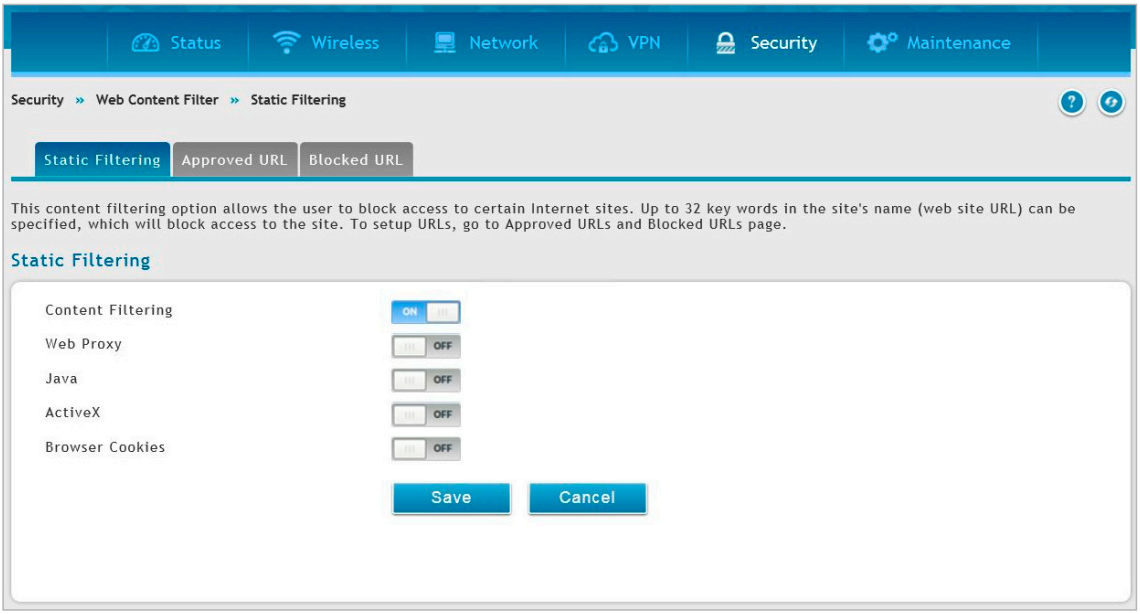

図 8-28　Static Filtering > Static Filtering タブ画面

2. 以下の項目を設定します。

項目	説明
Content Filtering	コンテンツフィルタリングを「ON」または「OFF」にします。
Web Proxy	「ON」にした場合、プロキシサーバがブロックされます。 プロキシサーバを介した通信では、特定のファイアウォールルールを回避した状態で通信が行われます。例えば、ファイアウォールによって特定の IP アドレスへの通信がブロックされている場合であっても、プロキシを経由してリクエストが転送されるという状況が考えられます。
Java	「ON」にした場合、Java アプレットをブロックします。 Java アプレットは Web ページに組み込まれた小さなプログラムであり、ページの動的処理を行います。コンピュータへの不正アクセスや感染を目的として不正なアプレットが使用されることがあります。
ActiveX	「ON」にした場合、ActiveX のダウンロードがブロックされます。 ActiveX コントロールは、Java アプレットと同様に Internet Explorer 実行中に Windows コンピュータにインストールされます。コンピュータへの不正アクセスや感染を目的として不正な ActiveX が使用されることがあります。
Browser Cookies	「ON」にした場合、Web サイトによるクッキーの作成がブロックされます。 クッキーは、Web サイトによって保存されるセッション情報であり、主にログイン時に使用されます。Web サイトによっては情報の追跡と閲覧習慣のために保存することもあります。

3. 「Save」をクリックし、設定を適用します。

Approved URL（承認済み URL）

URL ドメイン名の承認リストを作成します。
承認リストに登録されたドメインは、どの形式でもアクセスを許可されます。
例：ドメイン「dlink」を登録した場合
LAN からのアクセスを許可される URL → www.dlink.com, support.dlink.com など

承認リストはテキストまたは CSV ファイルでインポート／エクスポートできます。

1. **Security > Web Content Filter > Static Filtering > Approved URL** の順にメニューをクリックし、以下の画面を表示します。

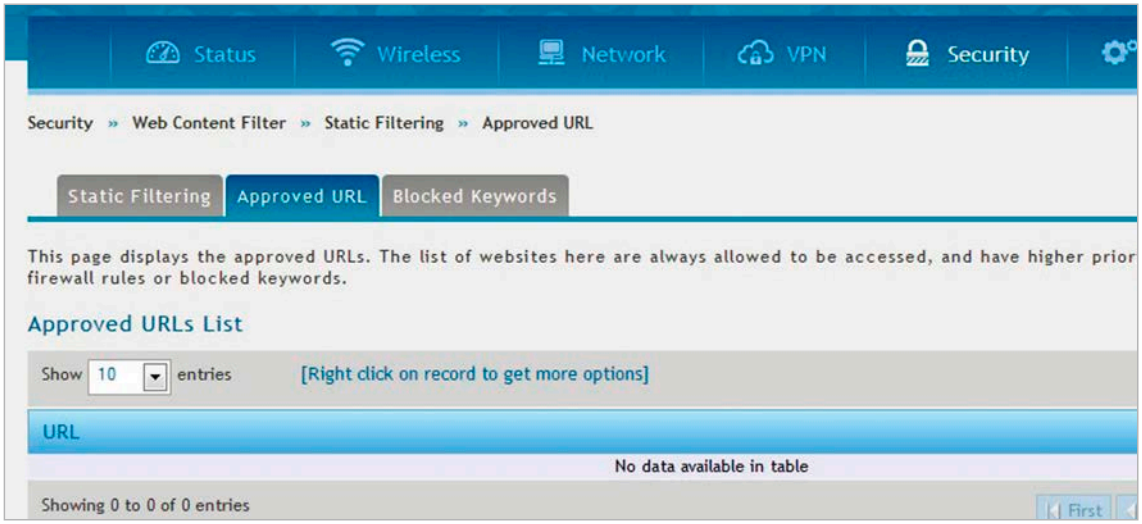

図 8-29　Static Filtering > Approved URL タブ画面

■ URL のインポート / アップロード

1. テキスト /CSV ファイルからインポートする場合は、「Upload URLs List from File」をクリックします。
2. CSV ファイルを参照し、「Upload」をクリックして URL をインポートします。

■ URL のエクスポート

1. 現在のリストをエクスポートする場合は、「Export URLs List to File」をクリックします。

■ URL の追加

1. 「Add New Approved URL」をクリックして、以下の画面を表示します。

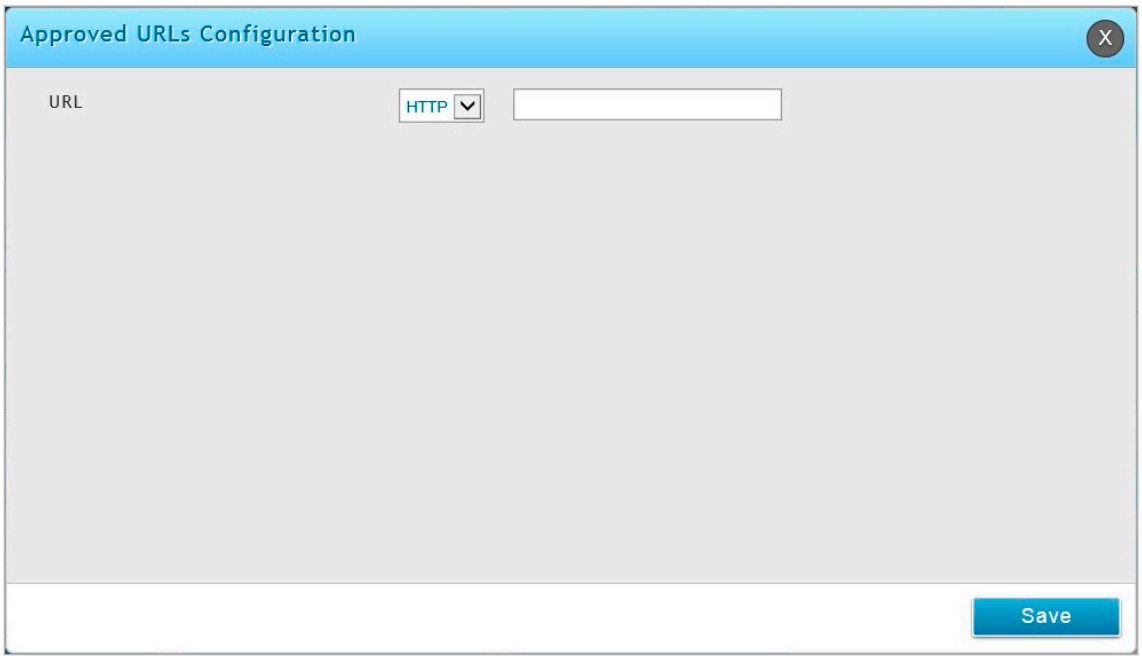

図 8-30　Approved URLs Configuration 画面

2. 「Save」をクリックし、設定を適用します。

Blocked URL（ブロック URL）

指定した URL へのアクセスをブロックします。
ブロック URL では、指定した URL 含むすべての Web サイトの URL をブロックすることができます。これは「Approved URLs List」より低い優先度です。例えば、ブロック URL が「Approved URLs List」の信頼されたドメインによって許可されたサイト内に存在している場合、そのサイトへのアクセスは許可されます。Blocked URL はテキストまたは CSV ファイルでインポート / エクスポートすることができます。

1. **Security > Web Content Filter > Static Filtering > Blocked URL** の順にメニューをクリックし、以下の画面を表示します。

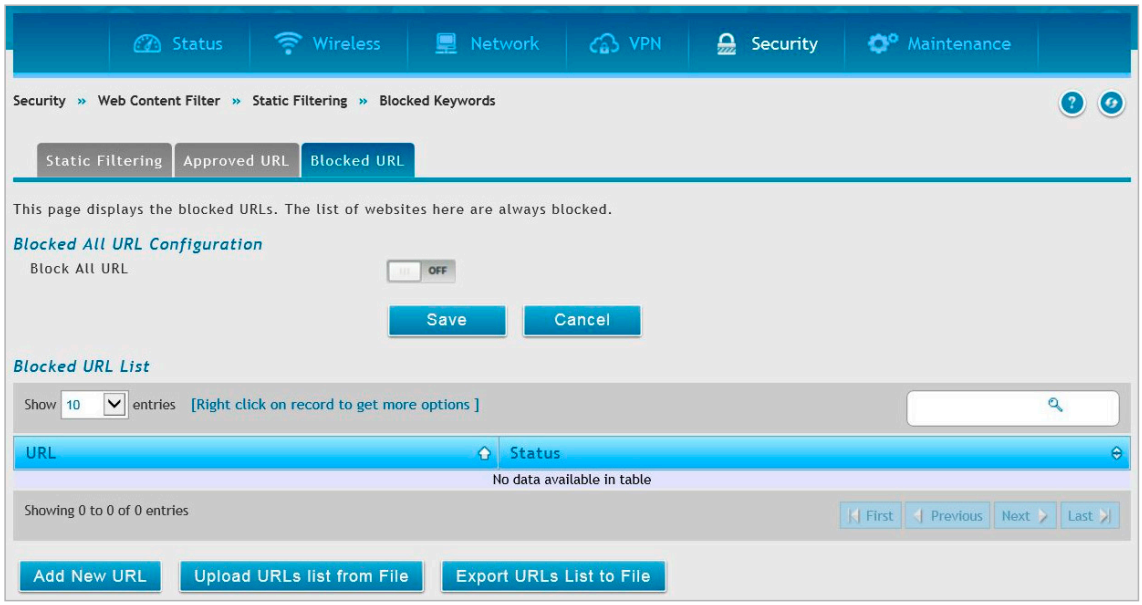

図 8-31　Static Filtering > Blocked URL タブ画面

■ ブロック URL の有効化

1. 「Blocked All URL Configuration」の「Block All URL」を「ON」にします。
2. 「Save」をクリックし、設定を適用します。

■ URL リストのインポート / アップロード

1. テキスト /CSV ファイルからインポートする場合は、「Upload URLs List from File」をクリックします。
2. CSV ファイルを選択 →「Upload」をクリックし URL リストをインポートします。

■ URL リストのエクスポート

1. 現在のリストをエクスポートする場合は、「Export URLs List to File」をクリックします。

■ URL の追加

1. 「Add New URL」をクリックして、以下の画面を表示します。

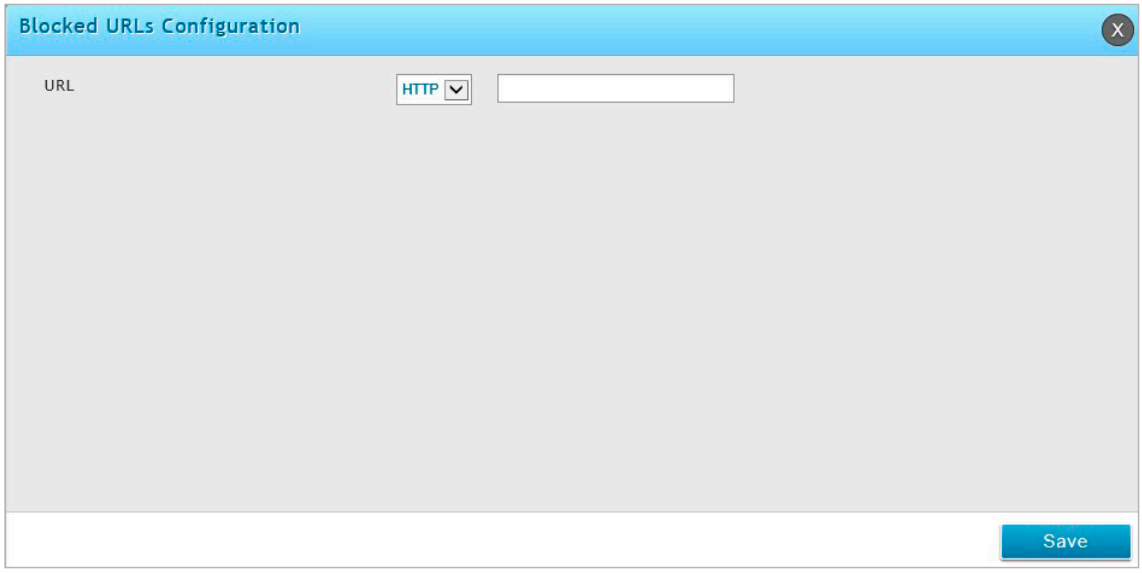

図 8-32　Blocked URLs Configuration 画面

2. URL を入力します。
3. 「Save」をクリックし、設定を適用します。

Dynamic Filtering（ダイナミックフィルタリング）

Security > Web Content Filter > Dynamic Filtering メニュー

注意 本機能を使用するには WCF ライセンスが必要です。

WCF ライセンスのアクティブ化については、「License Update（WCF ライセンスのアップデート）」を参照してください。

ダイナミックフィルタリングは、カテゴリリストに基づきコンテンツのフィルタリングを行う機能です。
ルータを WCF ライセンスでアップグレードしてから、フィルタリングするカテゴリを選択します。ブロック対象のカテゴリに属する Web サイトへアクセスした場合は、エラー画面が表示されます。

1. **Security > Web Content Filter > Dynamic Filtering** の順にメニューをクリックし、以下の画面を表示します。

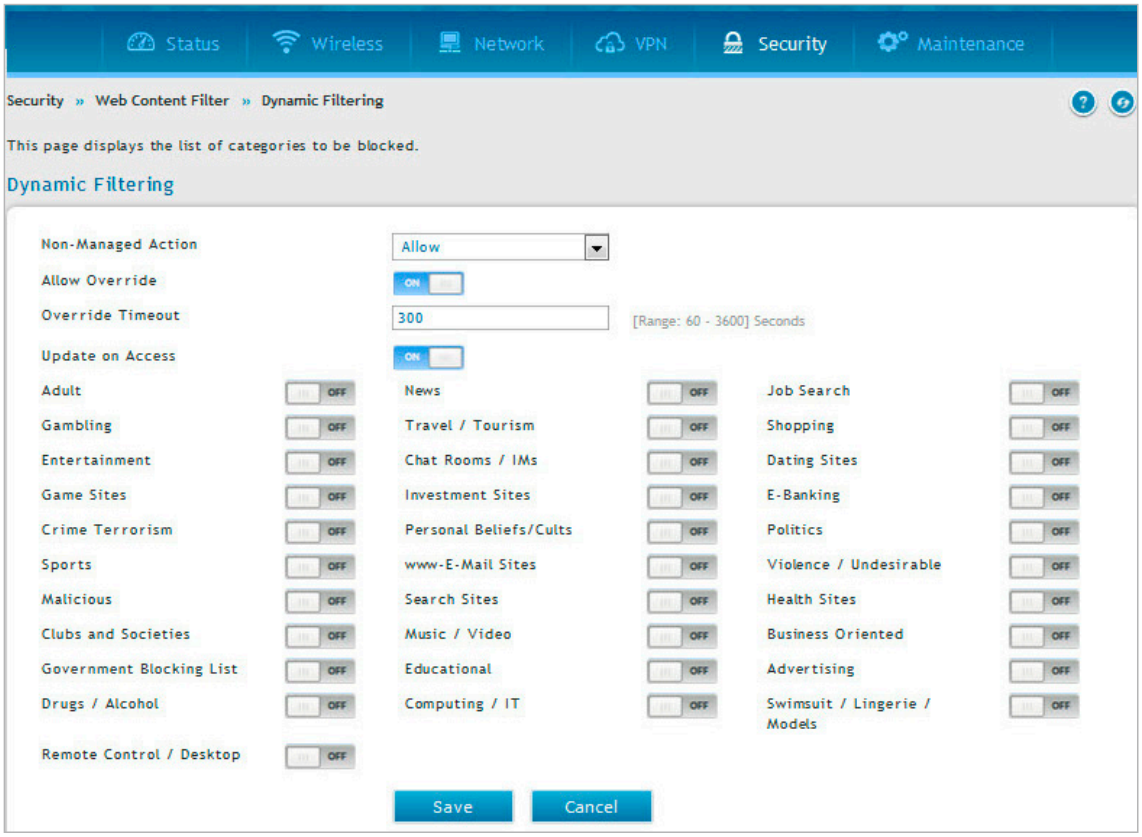

図 8-33　Dynamic Filtering 画面

2. 以下の項目を設定します。

項目	説明
Non-Managed Action	管理対象外サイトに対して実行されるアクションを「Allow」（許可）または「Block」（拒否）から選択します。 • 初期値：「Allow」
Allow Override	「ON」にした場合、ブロックするカテゴリに分類されたサイトを許可します。
Override Timeout	ブロック対象のカテゴリが「Allow Override」によって許可される時間（秒）を指定します。
Update on Access	ブロック対象のカテゴリへの新しいアクセス毎に Override（上書き）タイマを再起動します。タイムアウトするまで接続は許可されます。
Adult	性的なコンテンツ、ヌードを提供するサイトなど。
News	ニュースや最近の時事情報を提供するサイト。新聞、放送局、その他出版社など。
Job Search	仕事の情報、インタビューコーチング、その他雇用に関するサービスを提供するサイト。
Gambling	オンラインギャンブルやギャンブルに関する情報のサイト。
Travel/Tourism	旅や旅行情報のサイト。シティマップや旅程、バス / 電車 / 航空の予約、ホテルの予約など。
Shopping	オンラインショッピング、カタログ、オークションサイトや広告など。
Entertainment	テレビ、映画、エンタメニュースなどのサイト及び映画の映像コンテンツやテレビ配信を提供するサイト。
Chat rooms/IMs	ソーシャルネットワークサイト。チャットルームやインスタントメッセージサイト。
Dating Sites	オンラインデート、結婚の仲介、交際アドバイス、個人広告、結婚に関連する Web サイト。
Game Sites	オンラインゲーム、MORPG、コンピュータゲームの情報やチートコードなどを提供するサイト。
Investment Sites	仲買、信託、保険、その他組織に関連した投資のサイト。

項目	説明
E-banking	金融機関によるオンライン銀行サービスを提供するサイト。
Crime/Terrorism	殺人や破壊活動、爆撃など反社会的行動に関する情報を提供するサイト。
Personal Beliefs/Cults	宗教、礼拝所、宗教グループ、カルトに関するサイト。
Politics	政治、選挙、法律のサイト及び政治家や政党のプロモーションを行うサイト。
Sports	スポーツチームやファンクラブなどスポーツに関するサイト。
www-E-mail Sites	Web アクセス可能な E メールアカウントを使用して送信 / 受信する Web サイト。
Violence/ Undesirable	暴力、闘争、ヘイト、人種差別を促進または残虐な情報を含むサイト。
Malicious	マルウェアに感染またはマルウェアを広めるためにチャンネルとして使用されているサイト。
Search Sites	Web やその他のコンテンツを検索する検索エンジンサイト。
Health Sites	医師の検索や病気の回復などに関する情報を含む、個人の健康や医療サービスに関連したサイト。
Clubs and Societies	コミュニティ、掲示板、クラブのサイト。
Music/Video	インターネットラジオ、配信メディア、ミュージシャン、バンド、MP3 ダウンロードサイト。
Business Oriented	大企業、事業、中小ビジネスのサイト。
Government Blocking List	Australian Broadcasting Authorities（ABA）のブロックリスト。
Educational	教育組織の Web サイト、教育に関するコンテンツや辞書・百科事典を含む参照資料を提供しているサイト。
Advertising	広告を提供するサイト。広告フィルタではなく広告サーバの識別とブロックのためのカテゴリです。
Drugs/Alcohol	アルコール飲料の販売促進や販売を行うサイト、カクテルレシピなどの作成方法を提供するサイト。
Computing/IT	コンピュータ、ソフトウェア、ハードウェア、テクノロジに関するサイト。技術製品を提供する会社のウェブサイト。
Swimsuit/ Lingerie/Models	下着やビキニ等を表示・販売するサイト。
Remote Control/ Desktop	リモートコントロール / リモートデスクトップのサイト。

3. 「Save」をクリックし、設定を適用します。

URL Filtering ACL（URL フィルタリング ACL）

Security > Web Content Filter > URL Filtering ACL メニュー

URL フィルタリング ACL の設定方法について説明します。
アクセスコントロールリスト（ACL）を使用すると、承認されたユーザのみが特定のリソースにアクセスできるため、ネットワークリソースへの不正なアクセスを阻止できます。

1. **Security > Web Content Filter > URL Filtering ACL** の順にメニューをクリックし、以下の画面を表示します。

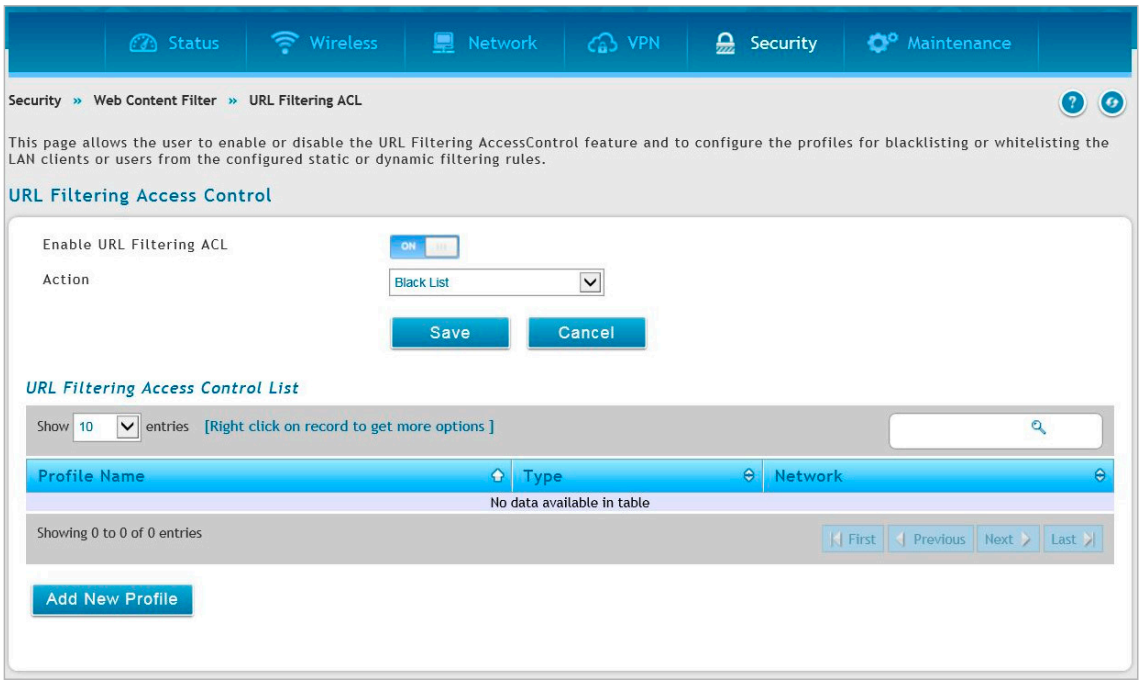

図 8-34　URL Filtering ACL 画面

2. アクセスコントロールリストを有効化する場合は、「Enable URL Filtering ACL」を「ON」にします。
3. 「Action」でポリシーを「White List」（ホワイトリスト）、「Black List」（ブラックリスト）から指定し、「Save」をクリックします。
ブラックリストに指定されたクライアントはスタティック / ダイナミックルールで制御されます。ホワイトリストに指定されたクライアントはスタティック / ダイナミックルールで制御されません。
4. ルールを編集、削除するにはエントリ上で右クリックし、「Edit」または「Delete」を選択します。
5. 新しいルールを追加する場合は、「Add New Profile」をクリックし、以下の画面を表示します。

図 8-35　URL Filtering ACL Configuration 画面画面

6. 以下の項目を設定します。

項目	説明
Profile Name	プロファイル名を入力します。
Type	プロファイルのタイプを「Single IP」「Range」「Interface」から選択します。
IP Address	「Type」で「Single IP」を選択した場合、制御するクライアントの IP アドレスを指定します。
Start Address	「Type」で「Range」を選択した場合、制御するクライアントの IP アドレス範囲の開始アドレスを指定します。
End Address	「Type」で「Range」を選択した場合、制御するクライアントの IP アドレス範囲の終了アドレスを指定します。
Interface	「Type」で「Interface」を選択した場合、制御するネットワークのインタフェースを選択します。

7. 「Save」をクリックし、設定を適用します。

Firewall（ファイアウォール設定）

Security > Firewall メニュー
ファイアウォールの設定方法について説明します。

Firewall Rules（ファイアウォールルールの設定）

Security > Firewall > Firewall Rules メニュー
インバウンド（WAN から LAN/DMZ）ルールでは、ご利用のネットワークに到達するトラフィックに対してアクセス制限を行い、選択的に特定の外部ユーザのみ特定のローカルリソースにアクセスすることを許可することができます。初期値では、LAN または DMZ からの要求に応答する場合を除き、安全でない WAN 側からセキュアな LAN に対するすべてのアクセスをブロックします。外部のデバイスがセキュアな LAN 上のサービスにアクセスすることを許可するために、各サービスにインバウンドのファイアウォールルールを作成する必要があります。

ご利用のネットワークに到達するトラフィックを許可する場合、ルータの WAN ポートの IP アドレスをパブリックに知らせる必要があります。アドレスを知らせる方法は WAN ポートの設定方法によって異なります。
このルータでは、スタティックなアドレスを WAN ポートに割り当てる場合には IP アドレスを使用します。使用の WAN アドレスがダイナミックである場合は、DDNS（Dynamic DNS）名を使用できます。

アウトバウンド（LAN/DMZ から WAN）ルールでは、ご利用のネットワークから送出されるトラフィックに対してアクセス制限を行い、選択的に特定のローカルユーザのみ外部リソースにアクセスすることを許可することができます。アウトバウンドの初期ルールは、安全なゾーン（LAN）からパブリック DMZ または安全でない WAN のいずれかへのアクセスを許可するものです。アウトバウンド初期ルールは、一方で、DMZ から安全でない WAN までのアクセスを拒否するものです。「Default Outbound Policy」画面（**Security > Firewall > Firewall Rules > IPv4/IPv6 Firewall Rules**）で初期ルールの設定を変更することができます。デフォルトのインバウンドポリシーが「Always Allow」である場合、各サービスにインバウンドファイアウォールルールを作成することで、インターネットサービスからの LAN ホストへのアクセスをブロックすることができます。

IPv4/IPv6 Firewall Rules（IPv4/IPv6 ファイアウォールルール）

1. **Security > Firewall > Firewall Rules > IPv4 Firewall Rules タブ**、または **IPv6 Firewall Rules タブ**の順にメニューをクリックし、以下の画面を表示します。

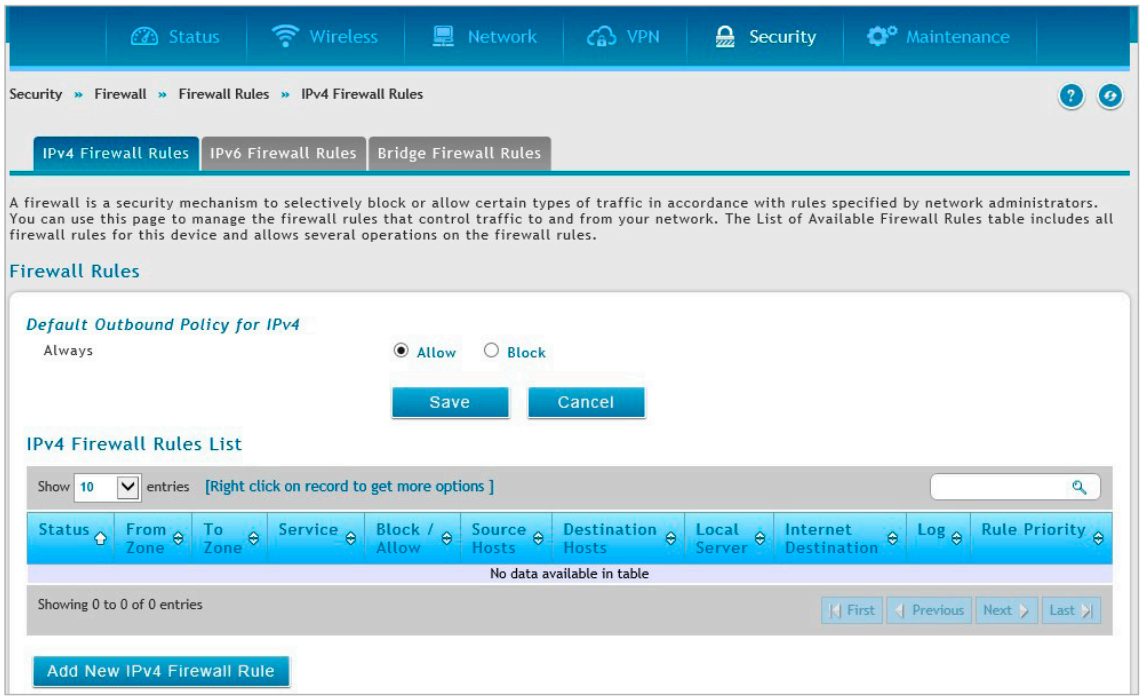

図 8-36　IPv4 Firewall Rules/IPv6 Firewall Rules タブ画面

2. 「Default Outbound Policy for IPv4/IPv6」でポリシーを「Allow」「Block」から指定し、「Save」をクリックします。

3. 新しいルールを追加するには、「Add New IPv4/IPv6 Firewall Rule」をクリックし、以下の画面を表示します。

図 8-37　IPv4 Firewall Rules Configuration 画面

4. 以下の項目を設定します。

項目	説明
From Zone	トラフィックの送信元を以下から選択します。 **IPv4 設定時：**「SECURE(LAN)」「SECURE(VLAN)」「INSECURE (WAN1/WAN2/WAN3 (Mobile Internet))」「DMZ」 **IPv6 設定時：**「SECURE(LAN)」「INSECURE (Dedicated WAN/Optional WAN)」
Available VLANs	「From Zone」で「SECURE(VLAN)」を選択した場合、VLAN を指定します。
To Zone	トラフィックの送信先を選択します。
Service	トラフィックを適用するサービスを選択します。 「ANY」を選択した場合、すべてのトラフィックにこのルールが適用されます。
Action	プルダウンメニューからアクションを選択します。 • 「Always Block」：常にブロック • 「Always Allow」：常に許可 • 「Block by schedule」：スケジュールによりブロック • 「Allow by schedule」：スケジュールにより許可
Select Schedule	スケジュールを選択します。「Action」で「Block by schedule」または「Allow by schedule」を選択した場合のみ表示されます。 スケジュールの設定については「Schedule（ファイアウォールスケジュール設定）」を参照してください。
Source Hosts/Destination Host	送信元 / 宛先ホストを指定します。 • 「Any」：すべてのホスト • 「Single Address」：IP アドレスを入力します。 • 「Address Range」：IP アドレス範囲を入力します。
Log	ファイアウォールトラフィックのログ出力を設定します。
QoS Priority （IPv4 時のみ）	アウトバウンドルールの場合は、QoS のプライオリティを選択します。IPv6 Firewall Rules Configuration 画面では表示されません。 • 「Normal-Service」: ToS=0（最も低い QoS） • 「Minimize-Cost」: ToS=1 • 「Maximize-Reliability」: ToS=2 • 「Maximize-Throughput」: ToS=4 • 「Minimize-Delay」: ToS=16（最も高い QoS）
External IP Address	「From Zone」で「INSECURE (WAN1/WAN2/WAN3 (Mobile Internet))」を選択した場合、宛先 NAT 設定として外部 IP アドレスを指定します。
Source NAT Settings	
アウトバウンドルールを作成する場合に表示される項目です。 SNAT（Source Network Address Translation）は、受け取ったパケットの送信元 IP アドレスを別の IP アドレスに変換します。	
External IP Address	外部 IP アドレスを選択します。
Destination NAT Settings	
インバウンドルールを作成する場合に表示される項目です。 DNAT（Destination Network Address Translation）は、送信するパケットの宛先 IP アドレスを別の IP アドレスに変換します。	
Internal IP Address	サーバを保持しているローカルネットワークのマシンの IP アドレスを指定します。
Enable Port Forwarding	「ON」：ポートフォワーディングを有効にします。有効にした場合、「Translate Port Number」を設定します。 「OFF」：ポートフォワーディングを無効にします。
Translate Port Number	ポートフォワーディングに使用するポート番号を入力します。
External IP Address	外部 IP アドレスを選択します。

5. 「Save」をクリックし、設定を適用します。

追加したルールは **IPv4 Firewall Rules/IPv6 Firewall Rules タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Bridge Firewall Rules（ブリッジファイアウォールルール）

Security > Firewall Rules > Bridge Firewall Rules タブ

ブリッジネットワークにおけるファイアウォールの設定について説明します。

初期設定では、ブリッジネットワークのインタフェース間で、すべてのアクセスがインバウンド／アウトバウンドの双方向に許可されています。

インバウンドルールは DMZ ポートから LAN ポート 1 へのアクセスについて管理します。アウトバウンドは LAN ポート 1 から送信されるトラフィックのアクセスを制御します。

ファイアウォールルールは最も制御の厳しいルールがリストの上部に表示され、リストの順で適用されます。

1. **Security > Firewall > Firewall Rules > Bridge Firewall Rules タブ**の順にメニューをクリックし、以下の画面を表示します。

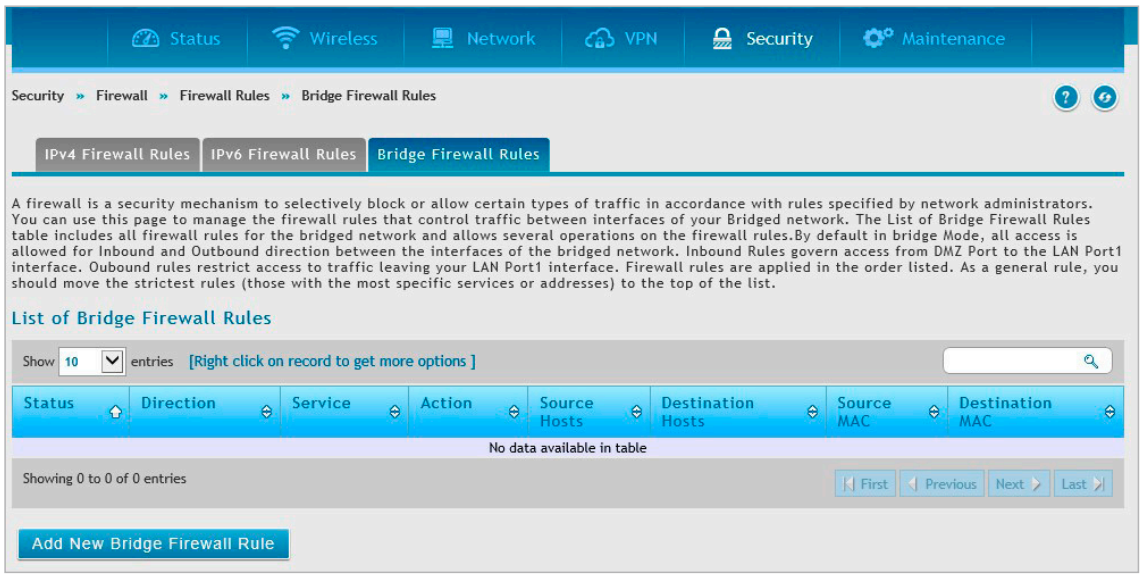

図 8-38　Firewall Rules > Bridge Firewall Rules タブ画面

2. 「Add New Bridge Firewall Rule」をクリックし、ルールを追加します。

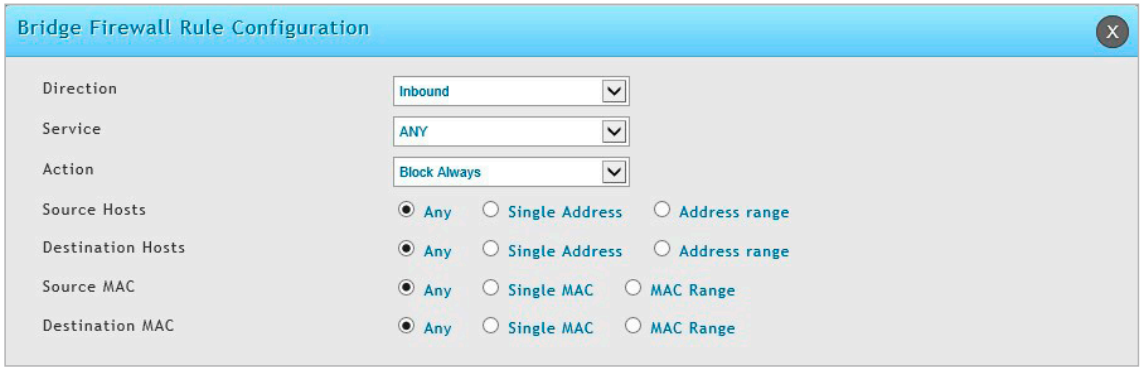

図 8-39　Bridge Firewall Rule Configuration 画面

3. 以下の項目を設定します。

項目	説明
Direction	トラフィックの方向を「Inbound」または「Outbound」から選択します。
Service	トラフィックを適用するサービスを選択します。 「ANY」を選択した場合、すべてのトラフィックにこのルールが適用されます。
Action	プルダウンメニューからアクションを選択します。 • 「Always Block」：常にブロック • 「Always Allow」：常に許可
Source Hosts/Destination Host	送信元 / 宛先ホストを指定します。 • 「Any」：すべてのホスト • 「Single Address」：IP アドレスを入力します。 • 「Address Range」：IP アドレス範囲を入力します。
Source Mac/Destination Mac	送信元 / 宛先 MAC アドレスを指定します。 • 「Any」：すべての MAC • 「Single MAC」：MAC アドレスを入力します。 • 「MAC Range」：MAC アドレス範囲を入力します。

4. 「Save」をクリックし、設定を適用します。

追加したルールは **Firewall Rules > Bridge Firewall Rules タブ**画面に表示されます。

右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Schedule（ファイアウォールスケジュール設定）

Security > Firewall > Schedules メニュー

ファイアウォールのルールは関連付けられたスケジュールに基づき、自動的に有効 / 無効に指定することが可能です。スケジュール設定ページでは曜日 / 時刻の単位で新しくスケジュールを設定することが可能です。設定したスケジュールを **Security > Firewall > Firewall Rules** 画面で選択して適用します。

注意 全てのスケジュールはルータで設定された時刻とタイムゾーンを基準としています。時刻、タイムゾーンの設定については「Data and Time（システムの日時設定）」を参照してください。

1. **Security > Firewall > Schedules** の順にメニューをクリックし、以下の画面を表示します。

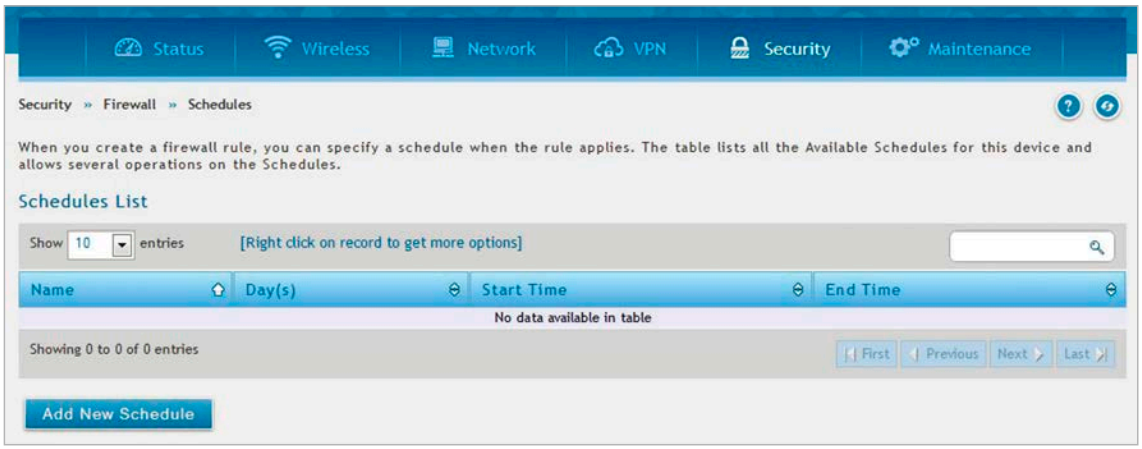

図 8-40　Schedules 画面

2. 「Add New Schedule」をクリックし、スケジュールを追加します。

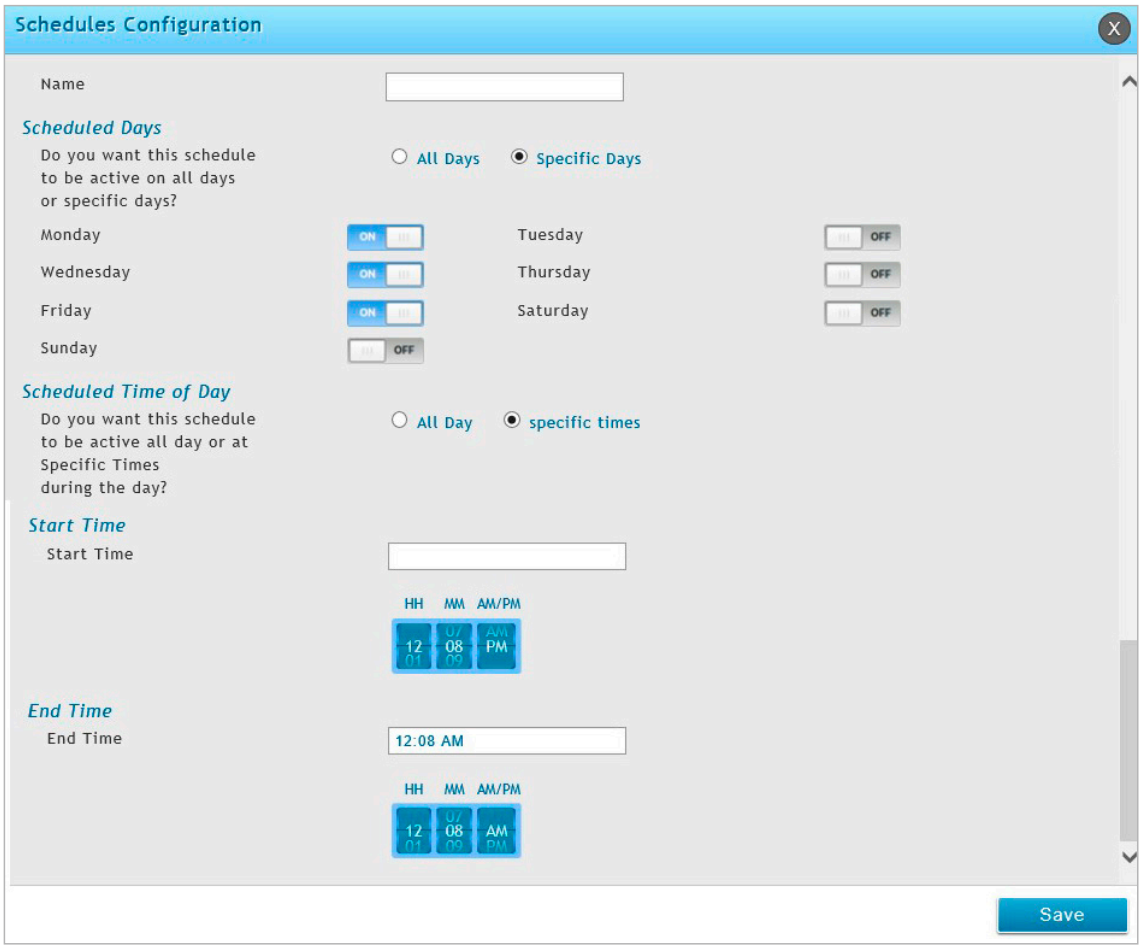

図 8-41　Schedules Configuration 画面

3. 以下の項目を設定します。

項目	説明
Name	スケジュール名を入力します。
Scheduled Days	「All Days」（毎日）または「Specific Days」（指定日）を選択します。
Monday - Sunday	「Specific Days」を選択した場合、有効にする曜日を「ON」にします。
Scheduled Time of Day	「All Day」（終日）または「specific times」（指定時間）を選択します。
Start Time/End Time	「specific times」を選択した場合、開始時刻（Start Time）と終了時刻（End Time）を指定します。

4. 「Save」をクリックし、設定を適用します。

追加したスケジュールは Schedules 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Blocked Clients（クライアントブロック設定）

Security > Firewall > Blocked Clients メニュー

クライアントブロック設定では、指定した MAC アドレスのクライアントをブロックすることができます。
ブロックするクライアントの追加方法について説明します。

1. **Security > Firewall > Blocked Clients** の順にメニューをクリックし、以下の画面を表示します。

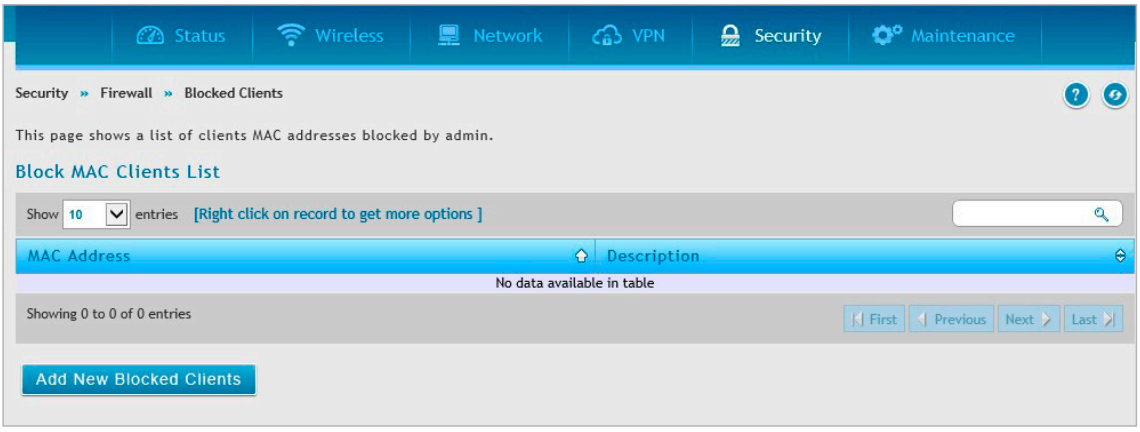

図 8-42　Blocked Clients 画面

2. 「Add New Blocked Clients」をクリックし、クライアントを追加します。

図 8-43　Blocked MAC Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
MAC Address	ブロックするクライアントの MAC アドレスを入力します。
Description	ブロックするクライアントの概要について入力します。

4. 「Save」をクリックし、設定を適用します。

追加したクライアントのリストは Blocked Clients 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Custom Services（カスタムサービスの設定）

Security > Firewall > Custom Services メニュー

ファイアウォールルールを定義するカスタムサービスの設定方法について説明します。
一般的なサービスは TCP/UDP/ICMP ポートを使用しますが、多くのカスタムまたは一般的でないアプリケーションが LAN または WAN に存在します。
カスタムサービス設定では、ポート範囲を定義し、トラフィックタイプ（TCP/UDP/ICMP など）を指定することができます。
本画面で定義したサービスは、**Security > Firewall > Firewall Rules** 画面のサービスリストに表示されます。

1. **Security > Firewall > Custom Services** の順にメニューをクリックし、以下の画面を表示します。

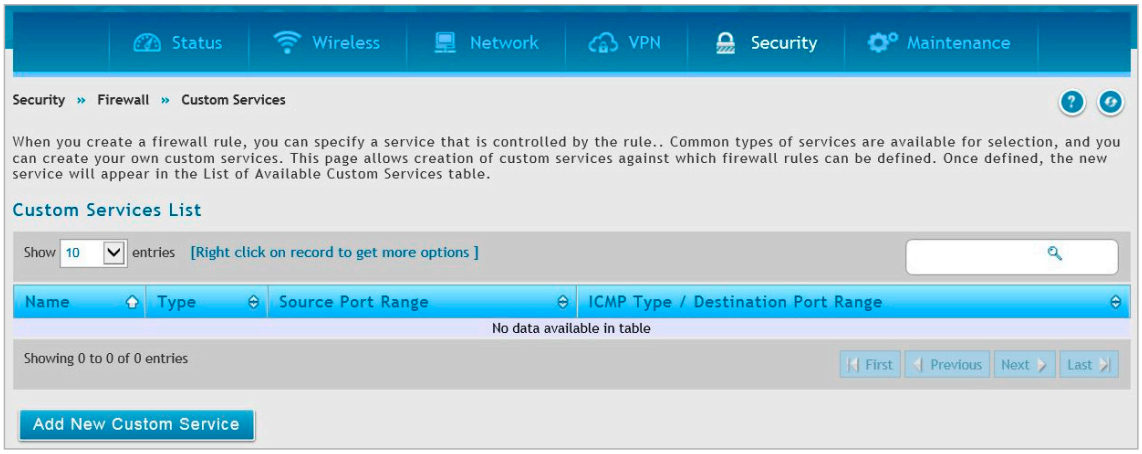

図 8-44　Custom Services 画面

2. 「Add New Custom Service」をクリックし、カスタムサービスを追加します。

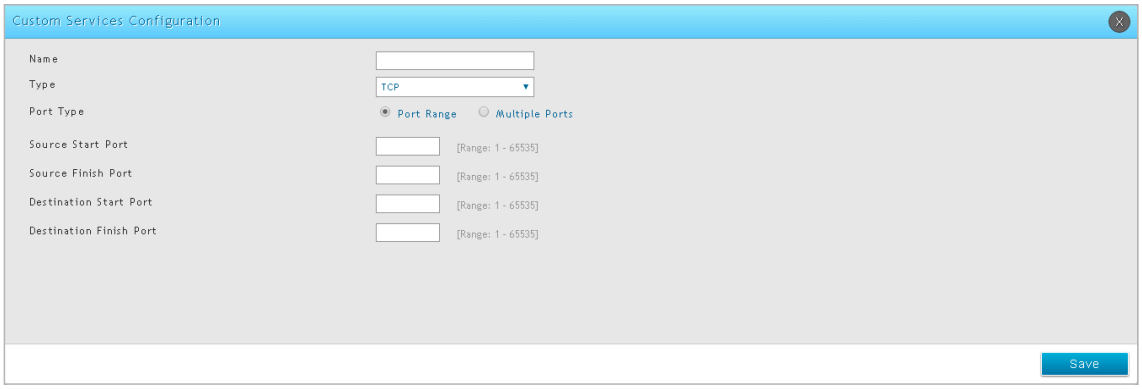

図 8-45　Custom Services Configuration 画面

3. 以下の項目を設定します。

項目	説明
Name	カスタムサービス名を入力します。
Type	サービスが使用する L3 プロトコルを以下から選択します。 「TCP」「UDP」「BOTH」「ICMP」「ICMPv6」
Port Type	ポートタイプを以下から選択します。 「Port Range」「Multiple Ports」
Source / Destination Start Port	「Port Range」を選択した場合、サービスに使用する送信元 / 宛先開始ポートを指定します。
Source / Destination Finish Port	「Port Range」を選択した場合、サービスに使用する送信元 / 宛先終了ポートを指定します。
Source / Destination Ports	「Multiple Port」を選択した場合、サービスに使用する送信元 / 宛先の複数ポートを「,」（コンマ）で区切り指定します。
ICMP/ICMPv6 Type	「ICMP/ICMPv6 Type」を選択した場合、適用する数値を指定します。 ・ICMP の設定可能範囲：0-40 ・ICMPv6 の設定可能範囲：1-255

4. 「Save」をクリックし、設定を適用します。

追加したカスタムサービスは Custom Servce 画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

ALGs（ALG サポート）

Security > Firewall > ALGs メニュー

ALG（Application Level Gateways）は、本ルータのファイアウォールと NAT サポートを強化し、シームレスにアプリケーションレイヤプロトコルをサポートするセキュリティコンポーネントです。

ALG の有効化により、特定のクライアントアプリケーション（H.323、RSTP など）が既知のポートと通信する際、ファイウォールで動的なエフェメラル TCP/UDP ポートを使用することができます。そのため、管理者が多数のポートをオープンする必要がなくなります。

ALG は、サポートされる特定のアプリケーションが使用するプロトコルを認識することができるため、ルータのファイアウォールを通じたクライアントアプリケーションのサポートを導入する非常に安全で効率的な方法となっています。

ALGs

ALG 機能において、ルータへの通過を許可するプロトコルを選択します。

1. **Security > Firewall > ALGs タブ**をクリックして、以下の画面を表示します。

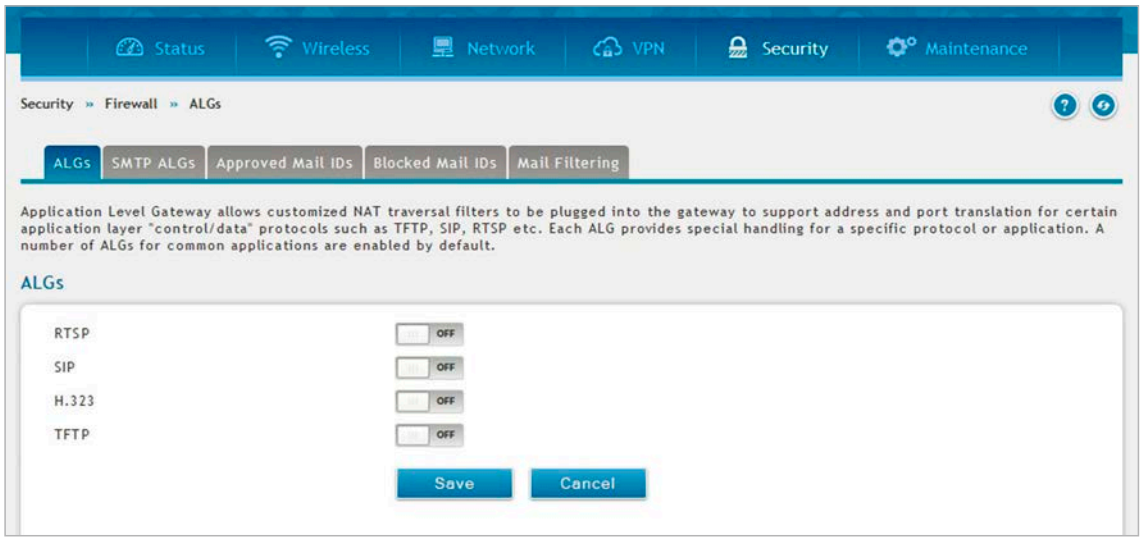

図 8-46　ALG > ALGs タブ画面

2. ルータへの通過を許可するプロトコルを「ON」にします。
3. 「Save」をクリックし、設定を適用します。

SMTP ALGs

Simple Mail Transfer Protocol（SMTP）は、インターネット経由で E-mail を送信するために使用されるテキストベースのプロトコルです。通常、ローカル SMTP サーバは DMZ に置かれ、リモート SMTP サーバから送信されたメールがルータを横断してローカルサーバに届くように構成されます。ローカルユーザは、E-mail のクライアントソフトウェアを使用してローカルの SMTP サーバから E-mail を取得します。また、SMTP はクライアントが E メールを送信する際に使用され、クライアント・サーバ双方からの SMTP トラフィックをモニタするために SMTP ALG を使用することも可能です。

注意　SMTP ALG 機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

1. **Security > Firewall > ALGs > SMTP ALGs タブ**をクリックして、以下の画面を表示します。

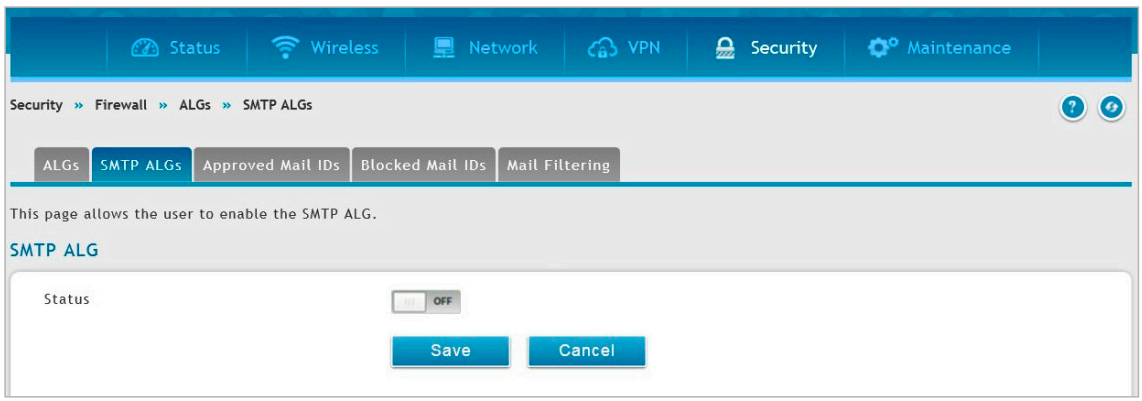

図 8-47　ALGs > SMTP ALGs タブ

2. 「Status」を「ON」にし、SMTP パケットを検査するポートを指定します。
3. 「Save」をクリックし、設定を適用します。

Approved Mail ID（許可メール ID）

メール ID を追加し、該当するメールを許可することができます。

1. **Security > Firewall > ALGs > Approved Mail IDs タブ**をクリックして、以下の画面を表示します。

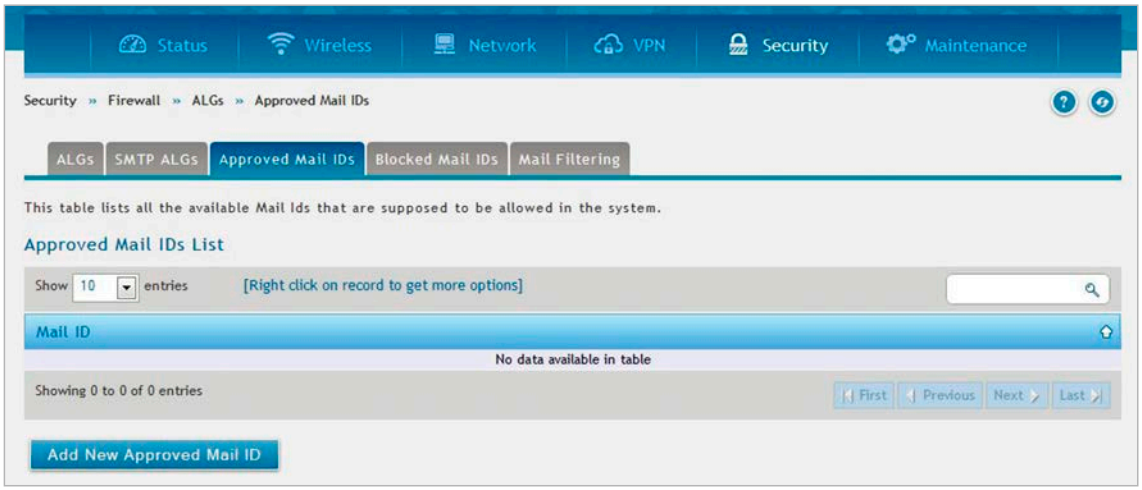

図 8-48　ALGs > Approved Mail IDs タブ画面

2. 「Add New Approved Mail ID」をクリックし、許可するメール ID を追加します。

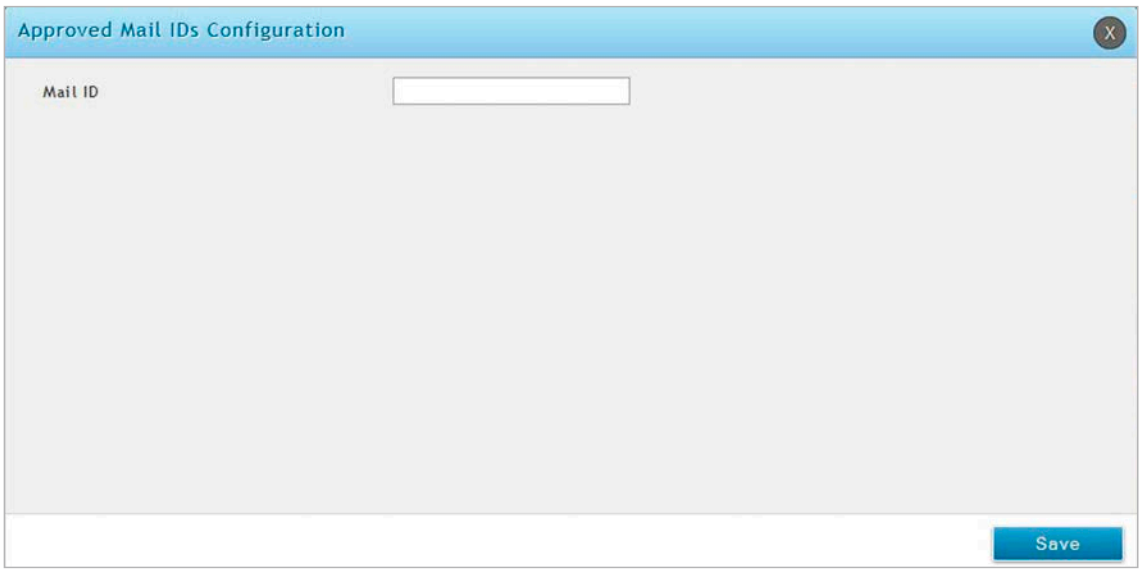

図 8-49　Approved Mail IDs Configuration 画面

3. 「Save」をクリックし、設定を適用します。

追加したメール ID は **ALGs > Approved Mail IDs タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Blocked Mail IDs（拒否メール ID）

メール ID を追加し、該当するメールを拒否することができます。

1. **Security > Firewall > ALGs > Blocked Mail IDs タブ**をクリックして、以下の画面を表示します。

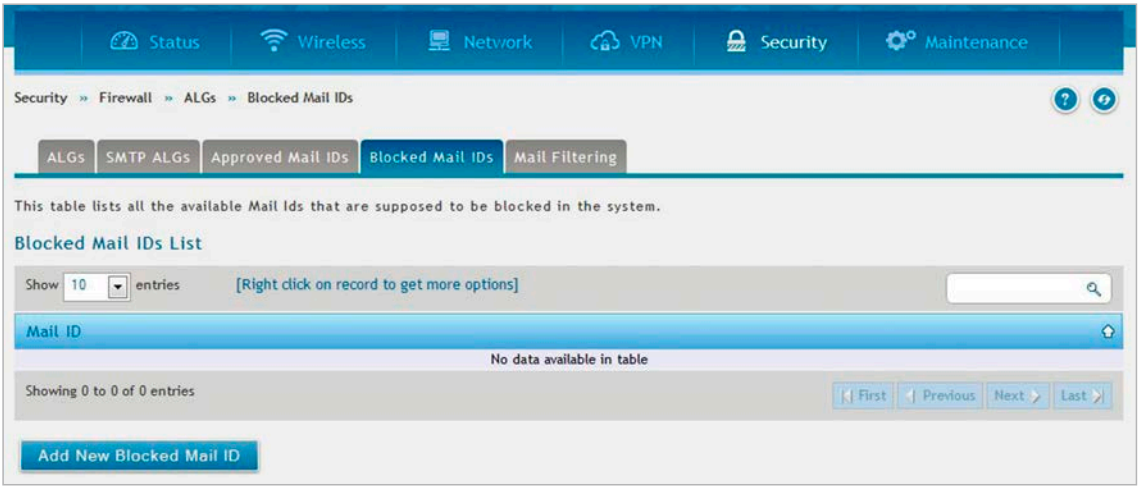

図 8-50　ALGs > Blocked Mail IDs タブ画面

2. 「Add New Blocked Mail ID」をクリックし、拒否するメール ID を追加します。

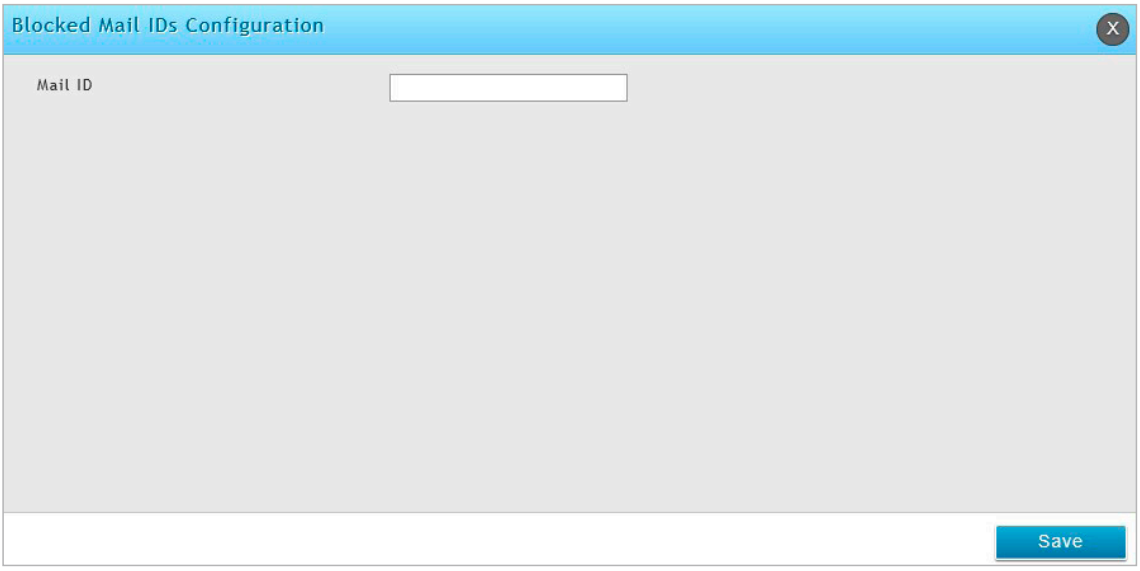

図 8-51　ALGs > Mail Filtering タブ画面

3. 「Save」をクリックし、設定を適用します。

追加したメール ID は **ALGs > Blocked Mail IDs タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Mail Filtering（メールフィルタリング）

Security > Firewall > ALGs > Mail Filtering タブ
メールフィルタリングの設定について説明します。

1. **Security > Firewall > ALGs > Mail Filtering タブ**をクリックして、以下の画面を表示します。

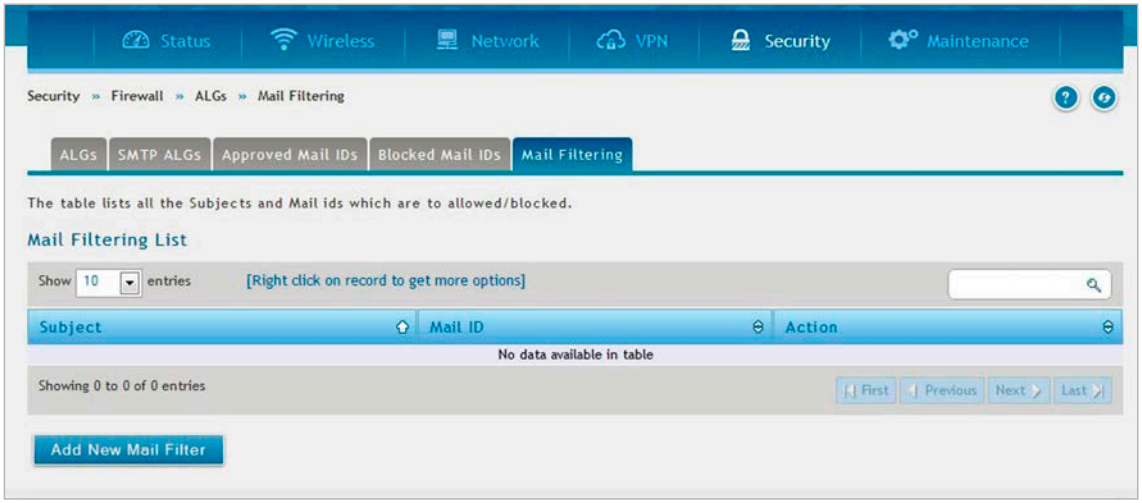

図 8-52　ALGs > Mail Filtering タブ画面

2. 「Add New Mail Filter」をクリックし、メールフィルタを追加します。

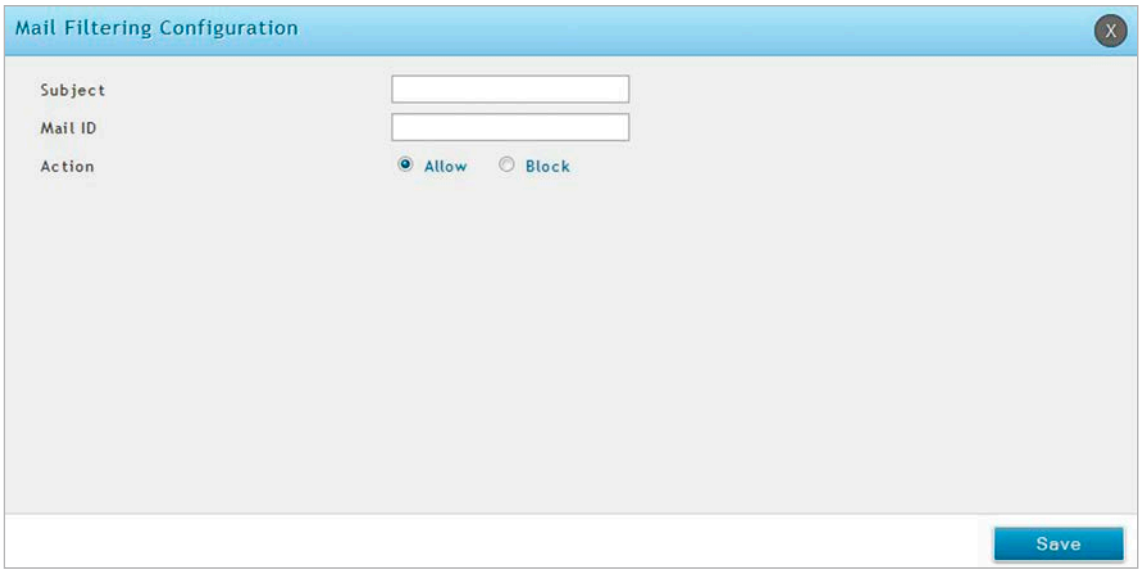

図 8-53　Mail Filtering Configuration 画面

3. 「Subject」と「Mail ID」を指定し、「Action」を「Allow」（許可）または「Deny」（拒否）から選択します。
4. 「Save」をクリックし、設定を適用します。

追加したメールフィルタは **ALGs > Mail Filtering タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

VPN Passthrough（VPN パススルー）

Security > Firewall > VPN Passthrough メニュー
VPN パススルーの設定方法について説明します。
VPN パススルーは、LAN 内のプライベートアドレスを持った VPN クライアントのパケットをインターネット側に通過させる機能です。

1. **Security > Firewall > VPN Passthrough** の順にメニューをクリックし、以下の画面を表示します。

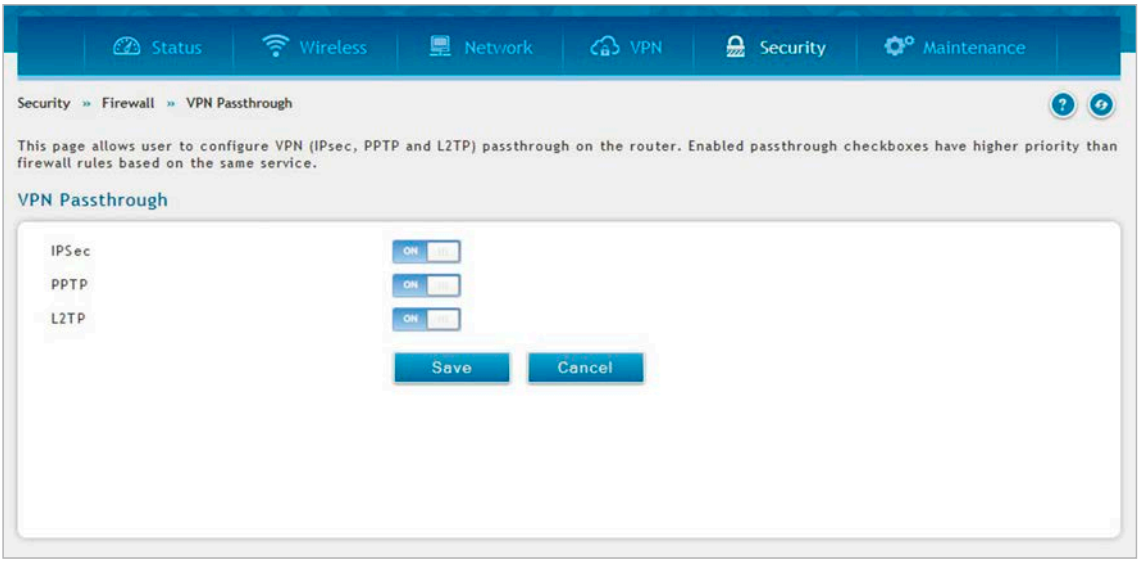

図 8-54　VPN Passthrough 画面

2. 許可する VPN プロトコルを「ON」にします。

3. 「Save」をクリックし、設定を適用します。

Dynamic Port Forwarding（ダイナミックポートフォワーディング）

Security > Firewall > Dynamic Port Forwarding メニュー

ダイナミックポートフォワーディングの設定方法について説明します。

Application Rules タブでアプリケーションルールの設定を行います。設定したルールのステータスは、Application Rules Status タブに表示されます。

Application Rules（アプリケーションルール設定）

アプリケーションルールはポートトリガルールとも呼ばれます。本機能により、LAN または DMZ 上のデバイスに送信されるように 1 つ以上のポートを要求することができます。ポートトリガは、定義済みの出力ポートの 1 つにある LAN/DMZ からのアウトバウンドのリクエストを待ち、その後、その特定のトラフィックタイプ用の入力ポートをオープンします。この動作は、オープンした出力または入力ポートでアプリケーションがデータを送信している間のダイナミックなポートフォワーディングの形式と考えることができます。

ポートトリガを行うアプリケーションルールは、特定の LAN IP または IP 範囲を参照する必要がないため、スタティックポートフォワーディングよりも柔軟性があります。また、使用されていないポートはオープンの状態にされないため、セキュリティのレベルを向上できます。

注意　入力ポートのオープン前に出力用の接続を行う LAN デバイスに依存するため、ポートトリガは LAN 上のサーバには適切ではありません。

アプリケーションによっては、機能が適切に動作するために、外部デバイスから接続される際に特定のポートまたはポート範囲でデータを受信する必要があります。ルータは、必要なポートまたはポート範囲のみでそのアプリケーションの全受信データを送信する必要があります。ルータは一般的なアプリケーションやゲームのアウトバウンド / インバウンドポートの一覧を保持しており、オープンすることができます。また、トラフィックタイプ（TCP や UDP）及びオープンするインバウンド / アウトバウンドポートの範囲を定義して、ポートトリガルールを指定することもできます。

1. **Security > Firewall > Dynamic Port Forwarding > Application Rules タブ**の順にメニューをクリックし、以下の画面を表示します。

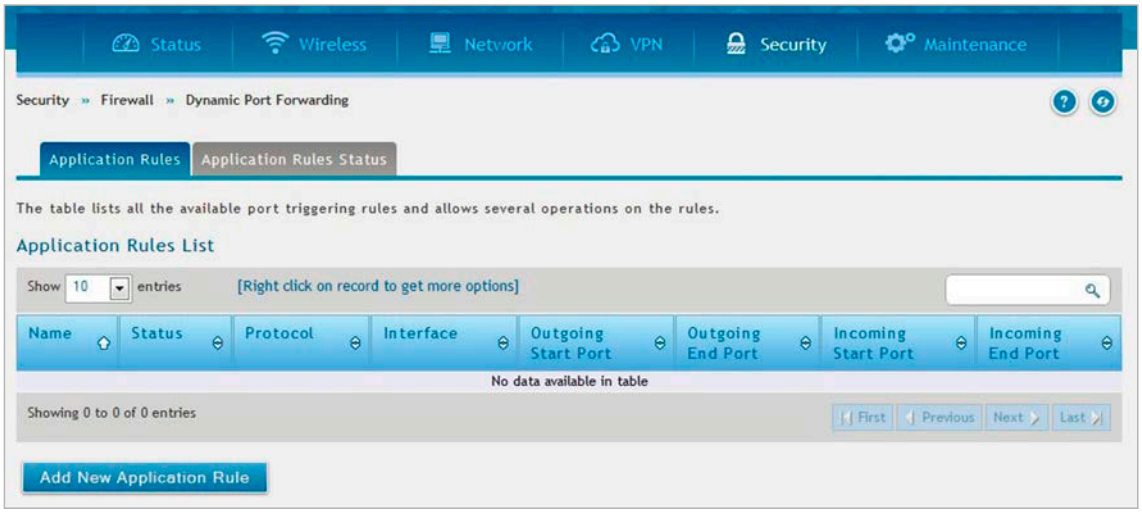

図 8-55　Dynamic Port Forwarding > Application Rules タブ画面

2. アプリケーションルールを追加する場合は、「Add New Application Rule」をクリックし以下の画面を表示します。

図 8-56　Application Rules Configuration 画面

3. 以下の項目を設定します。

項目	説明
Name	ルール名を入力します。
Enable	「ON」にしてルールを有効にします。
Protocol	プロトコルを「TCP」「UDP」から選択します。
Interface	インタフェースを「LAN」「DMZ」から選択します。
Outgoing (Trigger) Port Range	トリガポート範囲の開始 / 終了ポートを指定します。
Incoming (Response) Port Range	受信ポートを範囲の開始 / 終了ポートを指定します。

4. 「Save」をクリックし、設定を適用します。

追加したルールは **Dynamic Port Forwarding > Application Rules タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Application Rules Status（アプリケーションルールステータス）

アプリケーションルールのステータスが表示されます。

1. **Security > Firewall > Dynamic Port Forwarding > Application Rules Status タブ**の順にメニューをクリックし、以下の画面を表示します。

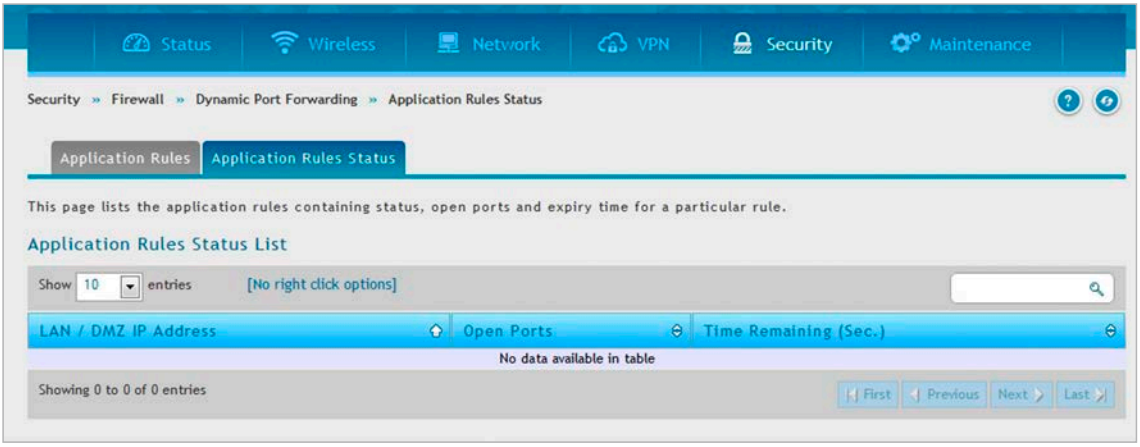

図 8-57　Application Rules > Application Rules タブ画面

2. 以下の項目を確認します。

項目	説明
LAN / DMZ IP Address	アプリケーションルールがアクティブになり、応答ポートが開かれるトリガとなった内部ネットワーク IP アドレスが表示されます。
Open Ports	内部デバイスのリクエストにより、このファイアウォールを通過してオープンになった応答ポートが表示されます。
Time Remaining (Sec.)	開いているポートが外部トラフィックを許可する時間（単位：秒）が表示されます。 この時間は、トラフィックが LAN / DMZ からトリガポートに送信されるたびにリセットされます。

Attack Checks（攻撃のチェック）

Security > Firewall > Attack Checks メニュー

攻撃（アタック）とは、ルータを使用不能にする悪意あるセキュリティ違反、または意図的ではないネットワークの問題を意味します。攻撃を確認することにより、連続する ping リクエストや ARP スキャンを経由するディスカバリなど、WAN におけるセキュリティの脅威を管理できます。
また、TCP フラッド、UDP フラッド、Dos 攻撃など、帯域幅を消費し通常のネットワークサービスの動作を妨げる攻撃をブロックすることが可能です。

1. **Security > Firewall > Attack Checks** の順にメニューをクリックし、以下の画面を表示します。

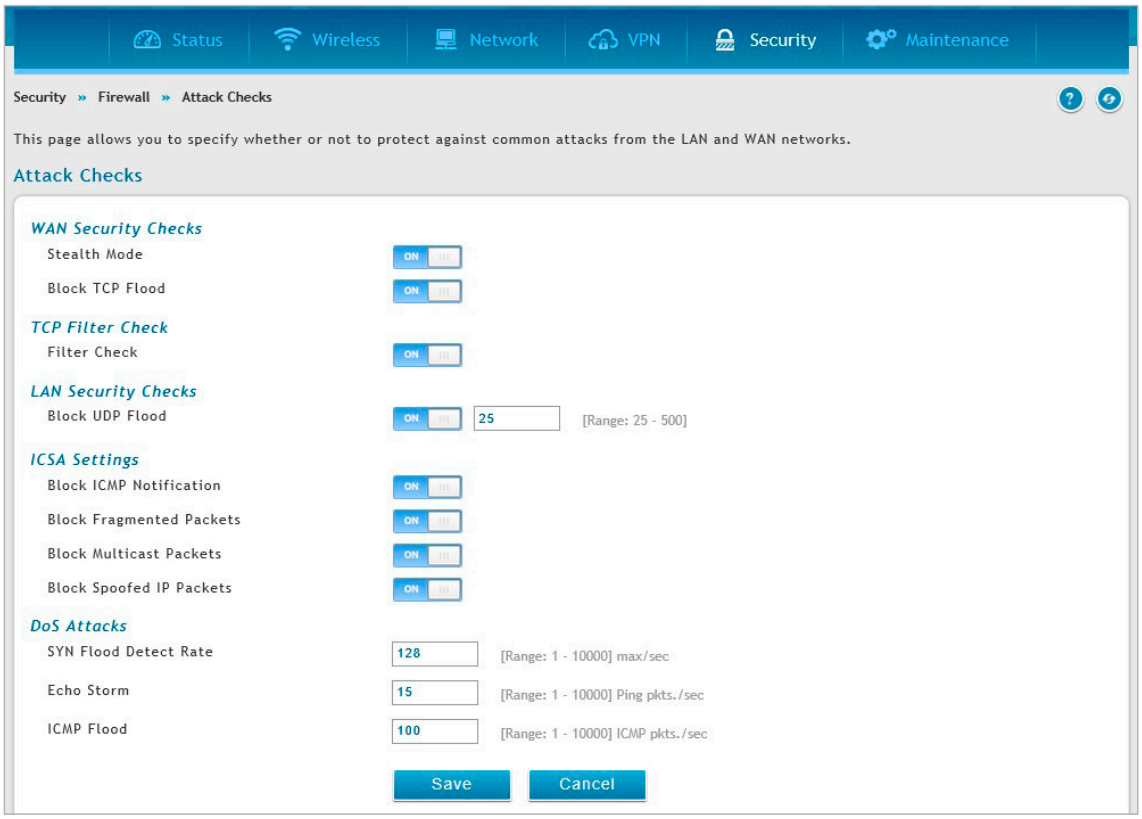

図 8-58　Attack Checks 画面

2. 以下の項目を設定します。

項目	説明
WAN Security Checks	
Stealth Mode	「ON」にした場合、ルータは WAN からのポートスキャンに応答しません。検出と攻撃による影響が低減されます。
Block TCP Flood	本オプションを有効にすると、ルータは不正な TCP パケットをすべて破棄して、SYN フラッド攻撃から保護されます。
TCP Filter Check	
Filter Check	本オプションを有効にすると、不正な TCP パケット（FIN、RST や ACK）は SNAT とともに破棄され、接続は遮断されます。「TCP OUT-OF-WINDOW」のようなパケットは不正として判断されます。
LAN Security Checks	
Block UDP Flood	「ON」にした場合、UDP フラッドをブロックします。 LAN 上の単一コンピュータからの、設定した数を超えたアクティブな UDP 接続を受け付けません。 • 設定可能範囲：25-500 • 初期値：25
ICSA Settings	
Block ICMP Notification	本オプションを有効にすると、ICMP パケットが特定されることを防止します。ICMP パケットは、特定されるとキャプチャされて Ping (ICMP) フラッド DoS 攻撃に使用される可能性があります。
Block Fragmented Packets	本オプションを有効にすると、ゲートウェイを経由する全てのフラグメント化パケットを破棄します。
Block Multicast Packets	本オプションを有効にすると、ゲートウェイを経由するマルチキャストパケットを破棄します。ルータ経由またはルータへのスプーフィング攻撃の可能性があります。
Block Spoofed IP Packets	本オプションを有効にすると、IP スプーフィングパケットを破棄します。
DoS Attacks	
SYN Flood Detect Rate	SYN フラッドを検出できるレートを指定します。
Echo Storm	ルータが WAN からのエコーストーム攻撃を検出して、その外部アドレスからの ping トラフィックを防止する 1 秒あたりの ping パケット数を指定します。
ICMP Flood	ルータが WAN からの ICMP フラッド攻撃を検出して、その外部アドレスからの ICMP トラフィックを防止する 1 秒あたりの ICMP パケット数を指定します。

3. 「Save」をクリックし、設定を適用します。

Intel® AMT（インテル ® アクティブ・マネジメント・テクノロジー）

Security > Firewall > Intel AMT メニュー

インテル ® アクティブ・マネジメント・テクノロジー（AMT）により、IT 管理者はネットワークに接続するコンピュータのシステムにリモートでアクセスし管理できます。PC が電源およびネットワーク接続している限り、電源がオフの場合または OS やハードディスクが動作していない場合でも制御することが可能です。インテル ®AMT は、クライアントマシンで独立して動作する、有線または無線ネットワークを通じて接続できる個別の管理プロセッサを使用しています。

1. **Security > Firewall > Intel AMT** の順にメニューをクリックし、以下の画面を表示します。

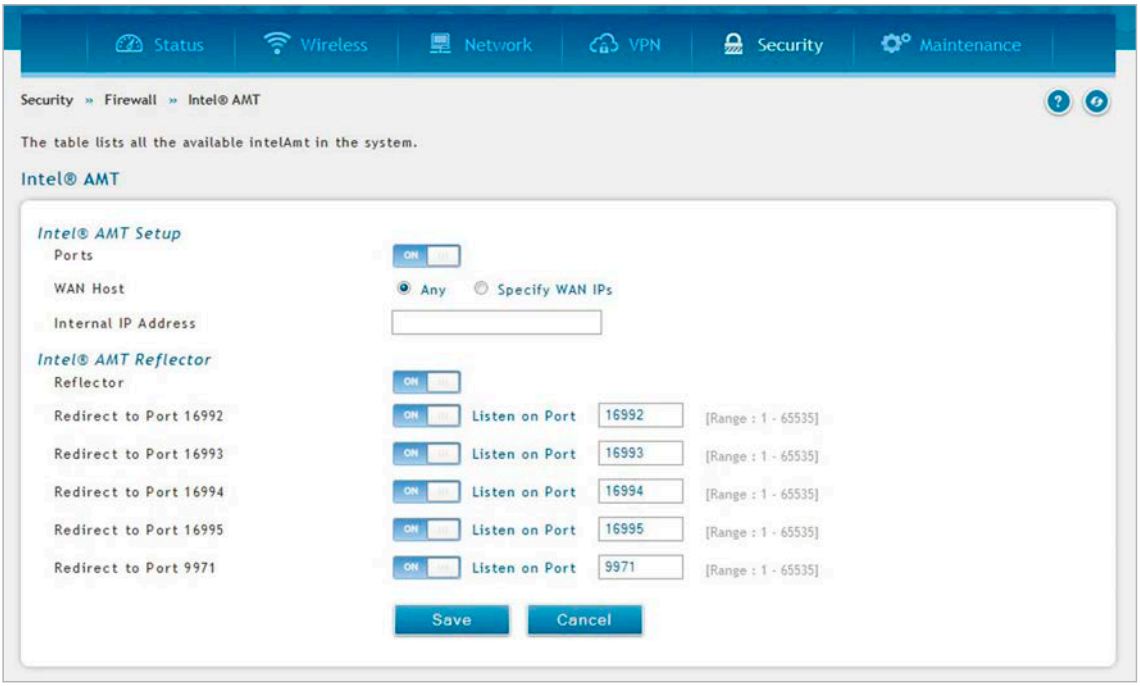

図 8-59　Intel AMT 画面

2. 以下の項目を設定します。

項目	説明
Intel® AMT Setup	
Ports	本項目を有効にすると、特定のポートに対してインバウンド / アウトバウンドファイアウォールルールを追加して、インテル ® AMT サービスを有効にします。
WAN Hosts	「Any」を選択すると、WAN 側の全ホストに対してローカルサーバへのアクセスが許可されます。「Specify WAN IPs」を選択した場合、ローカルサーバ（LAN ホスト）へのアクセスを許可される WAN ホストアドレスリストを指定します。アドレスはカンマ「,」で区切って指定する必要があります。
WAN Host Addresses	「Specify WAN IPs」を選択した場合、ローカルユーザへのアクセス許可が必要な WAN IP アドレスリストをカンマ「,」で区切って指定する必要があります。カンマだけが許可されており、カンマと IP アドレスの間に空白を入れないでください。
Internal IP Address	LAN ホスト（ローカルサーバ）の IP アドレスを指定します。
Intel® AMT Reflector	
Reflector	「ON」にしてリフレクターを有効にします。指定したポートでクライアントに対してデータを送り返します。
Redirect to Port 16992	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port：サーバがインバウンド通信をリッスンするポートを指定します。
Redirect to Port 16993	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port：サーバがインバウンド通信をリッスンするポートを指定します。
Redirect to Port 16994	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port：サーバがインバウンド通信をリッスンするポートを指定します。
Redirect to Port 16995	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port：サーバがインバウンド通信をリッスンするポートを指定します。
Redirect to Port 9971	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port：サーバがインバウンド通信をリッスンするポートを指定します。

3. 「Save」をクリックし、設定を適用します。

IPS（侵入防止システム）

Security > Firewall > IPS メニュー

IPS（Intrusion Prevention System）/ ルーター侵入防止システムは、インターネットからの悪意ある攻撃がプライベートネットワークにアクセスするのを防ぎます。ルータに保存されたスタティックな攻撃シグニチャにより、一般的な攻撃を検出して防止することが可能です。また、管理者はWAN からの悪意のある侵入の試みが防止された回数を確認できます。

注意　IPS 機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

1. **Security > Firewall > IPS** の順にメニューをクリックし、以下の画面を表示します。

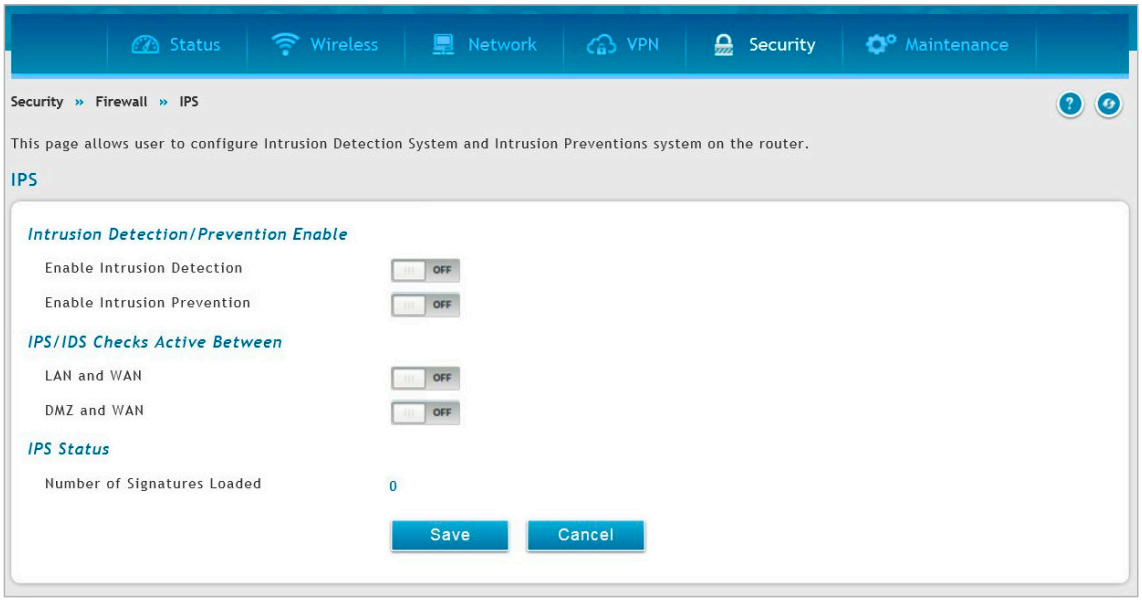

図 8-60　IPS 画面

2. 以下の項目を設定します。

項目	説明
Intrusion Detection/Prevention Enable	
Enable Intrusion Detection	「ON」にして侵入の検出を有効にします。
Enable Intrusion Prevention	「ON」にして侵入の防止を有効にします。
IPS/IDS Checks Active Between	
LAN and WAN	「LAN / WAN」間での IPS を有効にします。
DMZ and WAN	「DMZ / WAN」間での IPS を有効にします。
IPS Status	
Number of Signatures Loaded	シグネチャの読み込み回数が表示されます。

3. 「Save」をクリックし、設定を適用します。

App Control Policy（アプリケーションコントロールポリシー）

Application Control（アプリケーションコントロール）

Security > App Control Policy > Application Control メニュー

処理中のアプリケーションのトラフィックをネットワーク管理者が許可、ブロック、またはコントロールすることができます。

注意　アプリケーションコントロール機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

Policies（ポリシー設定）

グループを作成し、管理するアプリケーションを選択します。また、アプリケーション管理のポリシーを設定することも可能です。

1. **Security > App Control Policy > Application Control > Policies タブ**の順にメニューをクリックし、以下の画面を表示します。

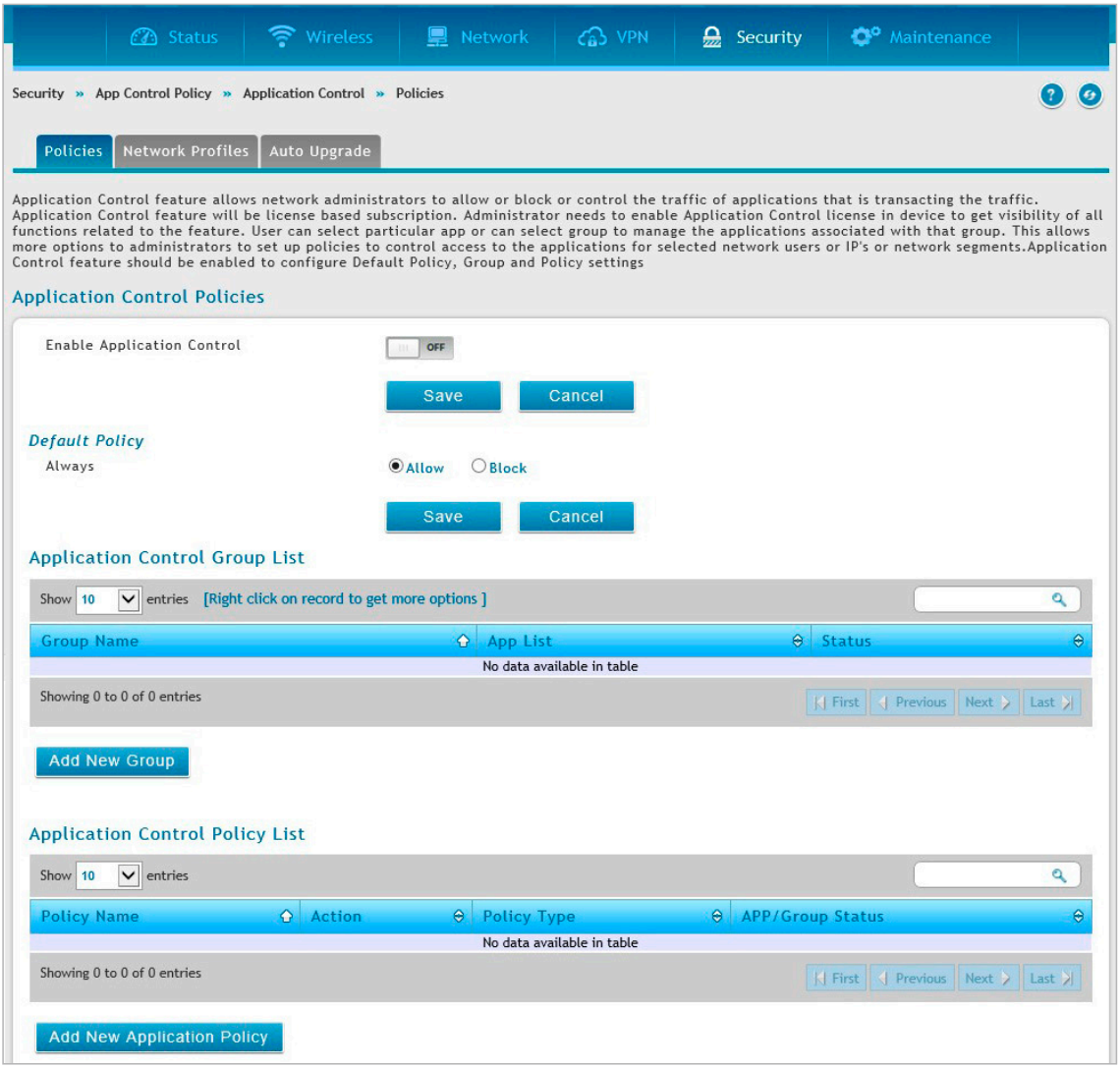

図 8-61　Application Control > Policies タブ画面

2. 「Enable Application Control」を「ON」または「OFF」に設定　→「Save」をクリックします。（初期値：「OFF」）

3. 以下の項目を設定します。

項目	説明
Default Policy	
Always	作成したグループに対するデフォルトポリシーを以下から選択します。 ・「Allow」：グループのアプリケーションを常に許可します。 ・「Deny」：グループのアプリケーションを常にブロックします。
Application Control Group List	
Group Name	グループ名が表示されます。
App List	選択したアプリケーションが表示されます。
Status	選択したアプリケーションのステータスが表示されます。
Application Control Policy List	
Policy Name	ポリシー名が表示されます。
Action	ポリシールールのアクションが表示されます。
Policy Type	ポリシータイプが表示されます。
APP/Group Status	アプリケーションおよびグループのステータスが表示されます。

4. 「Save」をクリックし、設定を適用します。

■ グループの追加

「Enable Application Control」を「ON」にした場合のみグループの追加を行うことができます。

1. 「Add New Group」をクリックし、グループを追加します。

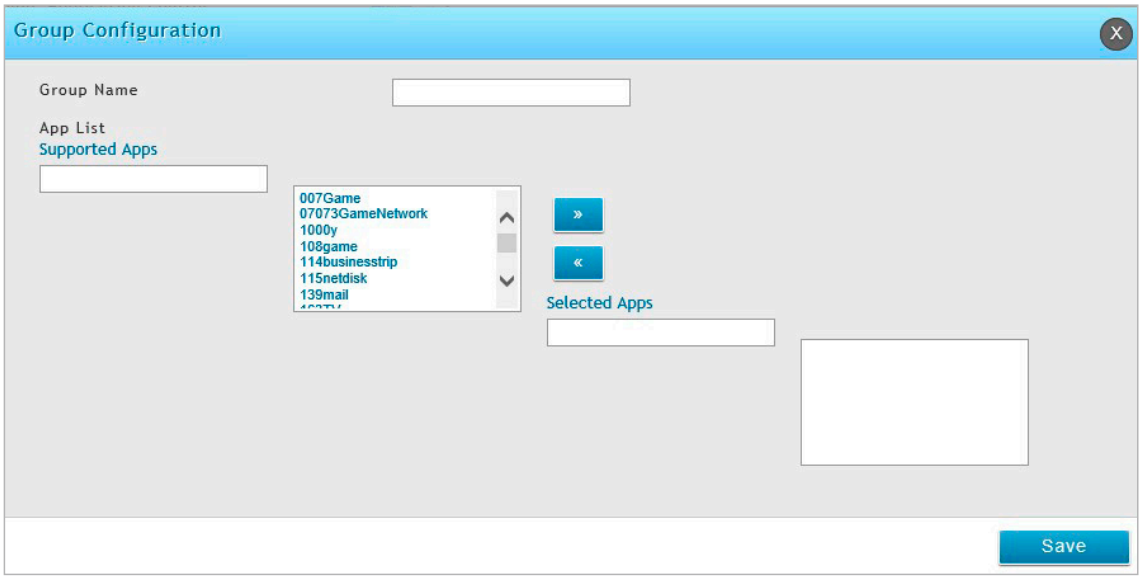

図 8-62　Group Configuration 画面

2. 以下の項目を設定します。

項目	説明
Group Name	グループ名を入力します。
Supported Apps	サポートされているアプリケーションが表示されます。
Selected Apps	「Supported Apps」からアプリケーションを選択します。 選択したアプリケーションが「Selected Apps」のボックスに表示されます。

3. 「Save」をクリックし、設定を適用します。

追加したグループは **Application Control > Policies タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

■ ポリシーの追加

「Enable Application Control」を「ON」にした場合のみポリシーの追加を行うことができます。

1. 「Add New Application Policy」をクリックし、アプリケーションポリシーを追加します。

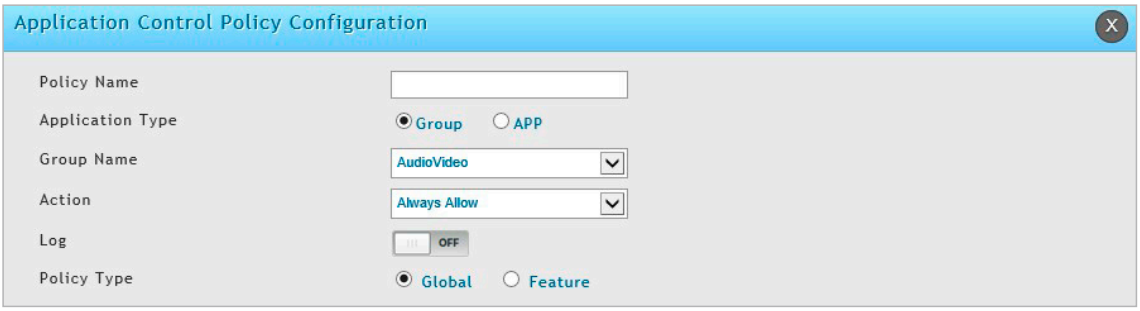

図 8-63　Application Control Policy Configuration 画面

2. 以下の項目を設定します。

項目	説明
Policy Name	ポリシー名を入力します。
Application Type	アプリケーションタイプを「Group」または「APP」から選択します。
Group Name	グループ名を選択します。
APP Name	アプリケーション名を選択します。
Action	ポリシーのアクションを以下から選択します。 • 「Always Allow」：常に許可 • 「Always Block」：常にブロック • 「Allow by schedule」：スケジュールにより許可 • 「Block by schedule」：スケジュールによりブロック
Select Schedule	「Action」で「Allow by schedule」「Block by schedule」を選択した場合、スケジュールを選択します。 スケジュールは、**Security > Firewall > Schedules** 画面で登録します。
Log	「ON」にした場合、統計のログを取得します。
Policy Type	ポリシータイプを以下から選択します。 • 「Global」：選択したアプリケーションに該当するすべてのトラフィックにポリシーを適用します。 • 「Feature」：以降に表示される項目でポリシーを設定します。
Network Profiles	ネットワークプロファイルを選択します。
Captive Portal User	キャプティブポータルを「ON」または「OFF」にします。「ON」にした場合、すべてのキャプティブポータルクライアントがこのポリシーに従います。
User DB	ユーザデータベースを「ON」または「OFF」にします。ユーザデータベースは、選択したアプリケーションを制御するネットワークユーザを選択するために使用します。
Network Type	ネットワークタイプを「Groups」または「Users」から選択します。
Available Groups/ Available Users	アプリケーションを管理するグループまたはユーザを選択します。
QoS	QoS を「ON」または「OFF」にします。 選択したアプリケーションを介してアクセスするトラフィックの帯域幅レートまたは優先順位を選択できます。 「Action」で「Always Allow」「Allow by schedule」を選択した場合のみ表示されます。
Profile Type	プロファイルのタイプを「Rate」または「Priority」から選択します。 QoS を有効にした場合のみ表示されます。
Priority	プロファイルのタイプを「Priority」にした場合、優先度を以下から選択します。 「High」「Medium」「Low」
Minimum Bandwidth Rate	プロファイルのタイプを「Rate」にした場合、最小の帯域幅を入力します。
Maximum Bandwidth Rate	プロファイルのタイプを「Rate」にした場合、最大の帯域幅を入力します。
VPN Traffic	VPN トラフィックを「ON」または「OFF」にします。 「ON」にした場合、以下の項目の「ON」「OFF」を選択します。 • 「PPTP」「L2TP」「OpenVPN」「SSL VPN」「IPSec」

「Network Profiles」以降の項目は、「Policy Type」で「Feature」を選択した場合にのみ表示されます。

3. 「Save」をクリックし、設定を適用します。

追加したポリシーは **Application Control > Policies タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Network Profiles（ネットワークプロファイル設定）

アプリケーションポリシーの設定時に使用する、ネットワークプロファイルの追加方法について説明します。

1. **Security > App Control Policy > Application Control > Network Profiles タブ**の順にメニューをクリックし、以下の画面を表示します。

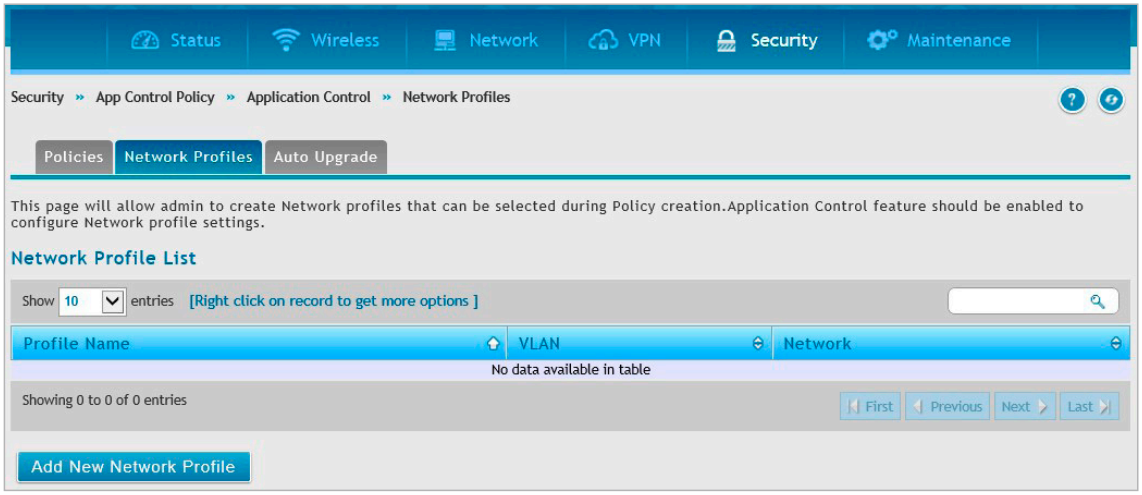

図 8-64　Application Control > Network Profiles タブ画面

2. 「Add New Network Profile」をクリックし、以下の画面を表示します。

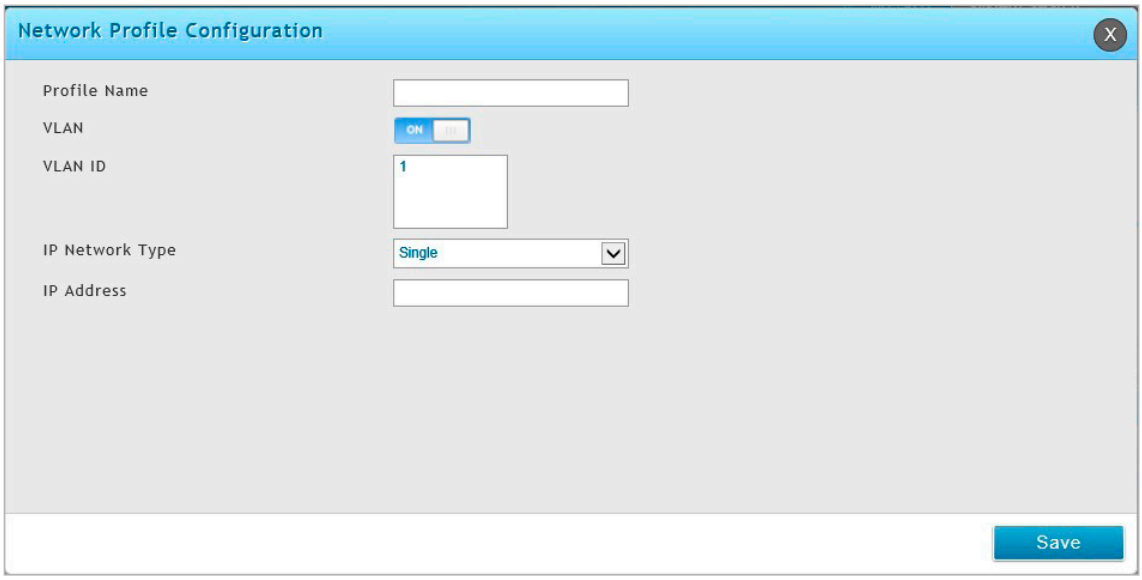

図 8-65　Network Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
Profile Name	プロファイル名を入力します。
VLAN	VLAN を「ON」または「OFF」にします。
VLAN ID	VLAN を「ON」にした場合、VLAN ID を選択します。
IP Network Type	IP ネットワークのタイプを以下から選択します。 「None」「Single」「Network」「Range」 選択したタイプに応じて、以降に表示される項目を設定します。
IP Address	IP アドレスを入力します。
Subnet Mask	サブネットマスクを入力します。
Start IP Address	IP アドレス範囲の開始 IP アドレスを入力します。
End IP Address	IP アドレス範囲の終了 IP アドレスを入力します。

4. 「Save」をクリックし設定を適用します。

追加したプロファイルは、**Application Control > Network Profiles タブ**画面に表示されます。
右クリックし、「Edit」（編集）、「Delete」（削除）を実行できます。

Auto Upgrade（オートアップグレード設定）

パッケージのオートアップグレード設定について説明します。

1. **Security > App Control Policy > Application Control > Auto Upgrade タブ**の順にメニューをクリックし、以下の画面を表示します。

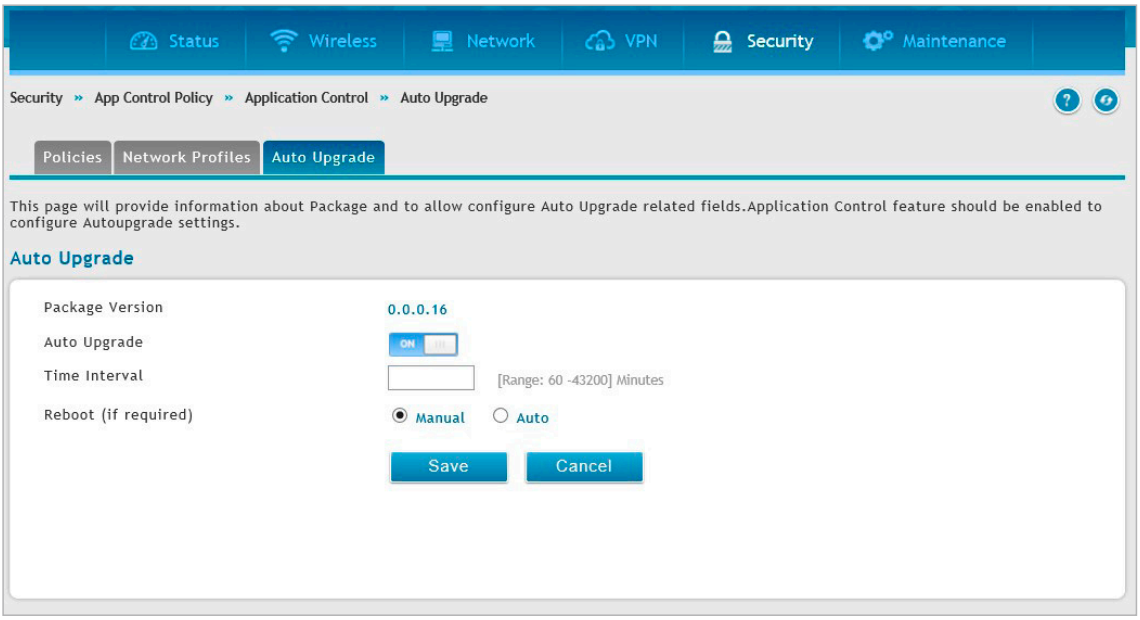

図 8-66　Application Control > Auto Upgrade タブ画面

2. 以下の項目を設定します。

項目	説明
Package Version	現在のパッケージバージョンが表示されます。
Auto Upgrade	オートアップグレードを「ON」または「OFF」にします。 「ON」にした場合、アプリケーションコントロールのパッケージは自動でアップグレードされます。
Time Interval	サーバ上に新しいパッケージが存在するか確認する間隔を設定します。 ・ 設定可能範囲：60-43200（分）

3. 「Save」をクリックし設定を適用します。

第 9 章　メンテナンス（Maintenance）

本章では、ファームウェアアップデートなど、本製品のメンテナンス作業について説明します。

設定項目	説明
「Administration（システム管理設定）」	システム名、日時、言語、Web GUI 設定やライセンス更新などの設定を行います。
「Management（管理設定）」	リモート管理、SNMP、診断ツールなどの設定を行います。
「Firmware & Config（ファームウェアとコンフィグ）」	ファームウェアアップデート、コンフィグレーションのバックアップ / リストアなどの設定を行います。
「Logs Settings（ログ設定）」	トラフィックの追跡 / ルーティングログ、Syslog、リモートログ、イベントログなどの設定を行います。

Administration（システム管理設定）

Maintenance > Administration メニュー

System Setting（システム名の設定）

Maintenance > Administration > System Setting メニュー
ルータのシステム名を変更することができます。

1. **Maintenance > Administration > System Setting** の順にメニューをクリックし、以下の画面を表示します。

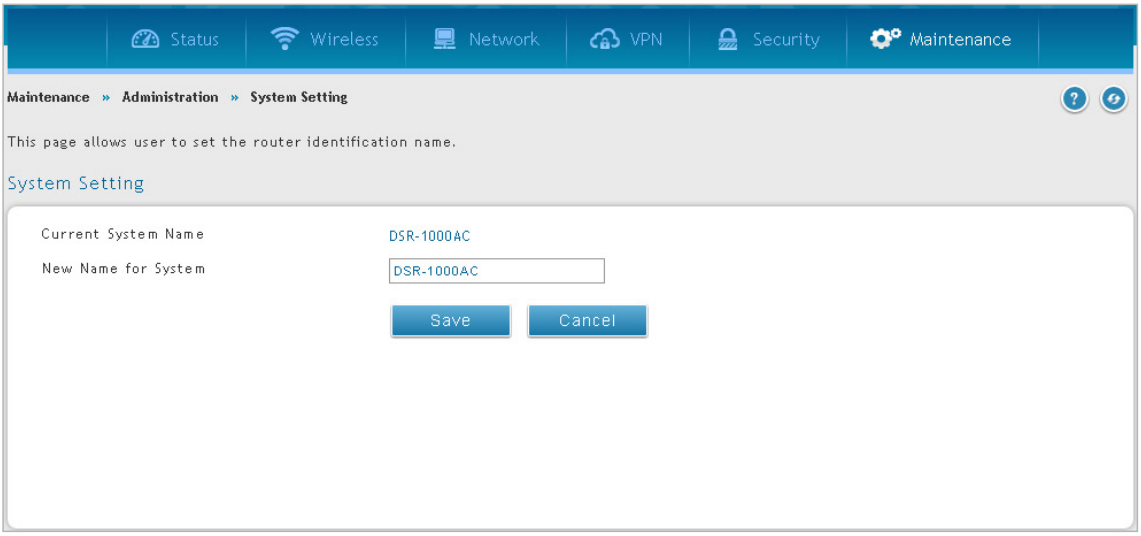

図 9-1　System Setting 画面

2. 「New Name for System」に新しいシステム名を入力します。
3. 「Save」をクリックし、設定を適用します。

Data and Time（システムの日時設定）

Maintenance > Administration > Date and Time メニュー
タイムゾーン、サマータイム（Daylight Savings Time）の調整の有無、日時を同期する NTP（ Network Time Protocol）サーバの使用について設定します。また、手動で日時を入力することも可能です。手動の場合、ルータの RTC（Real Time Clock）に情報を保存します。
ルータがインターネットにアクセス可能な場合、NTP サーバ通信を有効すると最も正確に日時を設定できます。

1. **Maintenance > Administration > Date and Time** の順にメニューをクリックし、以下の画面を表示します。

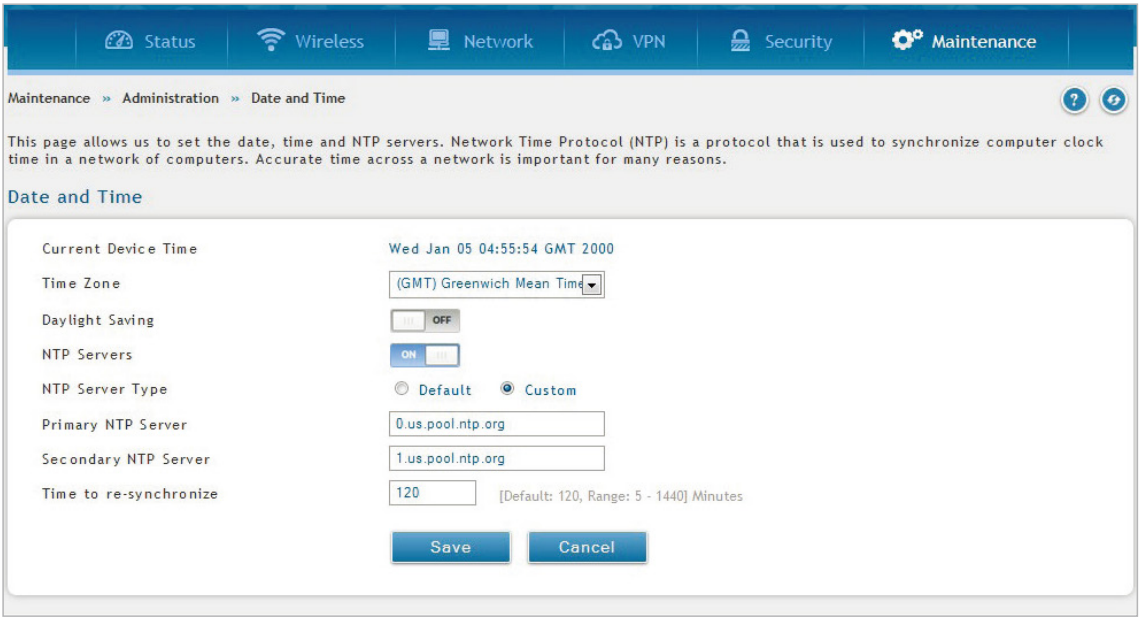

図 9-2　Date and Time 画面

2. 以下の項目を設定します。

項目	説明
Current Device Time	ルータの現在の日時を表示します。
Time Zone	プルダウンメニューからタイムゾーンを選択します。
Daylight Saving	「ON」にしてサマータイムを有効にします。
NTP Servers	「ON」にするとインターネット上の NTP サーバを使用します。
NTP Server Type	「Default」または「Custom」を選択します。 「Custom」を選択した場合は NTP サーバのアドレスを入力します。
Primary NTP Server	NTP サーバの種類で「Custom」を選択した場合、プライマリ NTP サーバのアドレスを入力します。
Secondary NTP Server	NTP サーバの種類で「Custom」を選択した場合、セカンダリ NTP サーバのアドレスを入力します。
Time to re-synchronize	NTP サーバと同期する間隔（分）を指定します。

3. 「Save」をクリックし、設定を適用します。

Session Settings（セッションタイムアウトの設定）

Maintenance > Administration > Session Settings メニュー
管理者およびゲストアカウントに対してタイムアウト設定を行います。

1. **Maintenance > Administration > Session Settings** の順にメニューをクリックし、以下の画面を表示します。

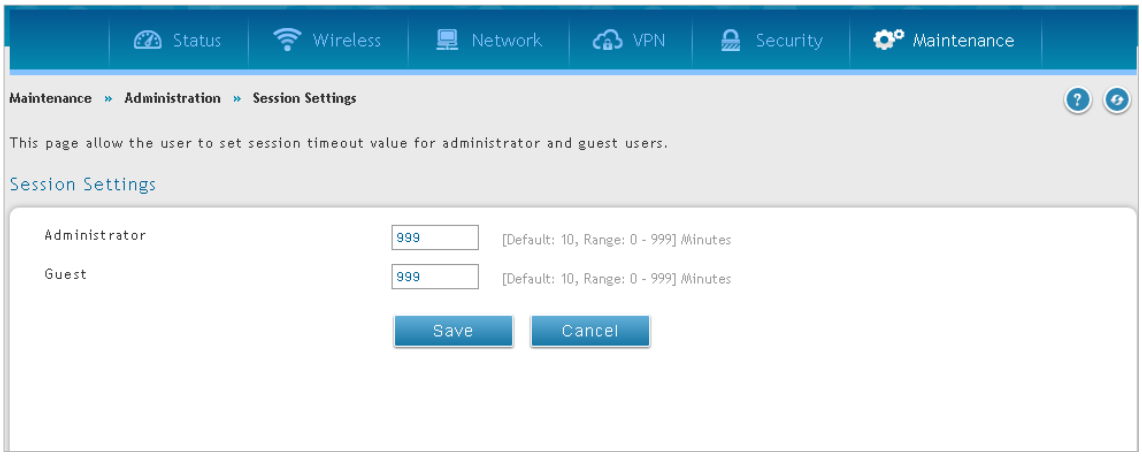

図 9-3　Session Settings 画面

2. 以下の項目を設定します。

項目	説明
Administrator	管理者ユーザのセッションタイムアウト値を入力します。
Guest	ゲストユーザのセッションタイムアウト値を入力します。

3. 「Save」をクリックし、設定を適用します。

License Update（WCF ライセンスのアップデート）

Maintenance > Administration > License Update メニュー

Web Content Filter（Web コンテンツフィルタリング）機能を使用するには、別途購入した WCF ライセンスが必要です。
本項目ではライセンスをアクティブ化する方法について説明します。

1. D-Link からアクティベーションキーを取得します。
   a. デバイスの底面にある本製品のシリアル番号を探します。
   b. ライセンスの購入後に、D-Link からライセンスキーを取得します。
   c. Web ブラウザを開き、https://register.dlink.com アクセスします。
   d. アカウントがない場合、新しいアカウントを登録します。
   e. 登録したユーザ名とパスワードでログインします。
   f. D-Link Global Registration ポータル Web サイトで「ライセンスキーのアクティベーション」をクリックします。
   g. 指示に従って、アクティベーションコードを受信します。

2. アクティベーションキーを取得後、**Maintenance > Administration > License Update** の順にメニューをクリックし、以下の画面を表示します。

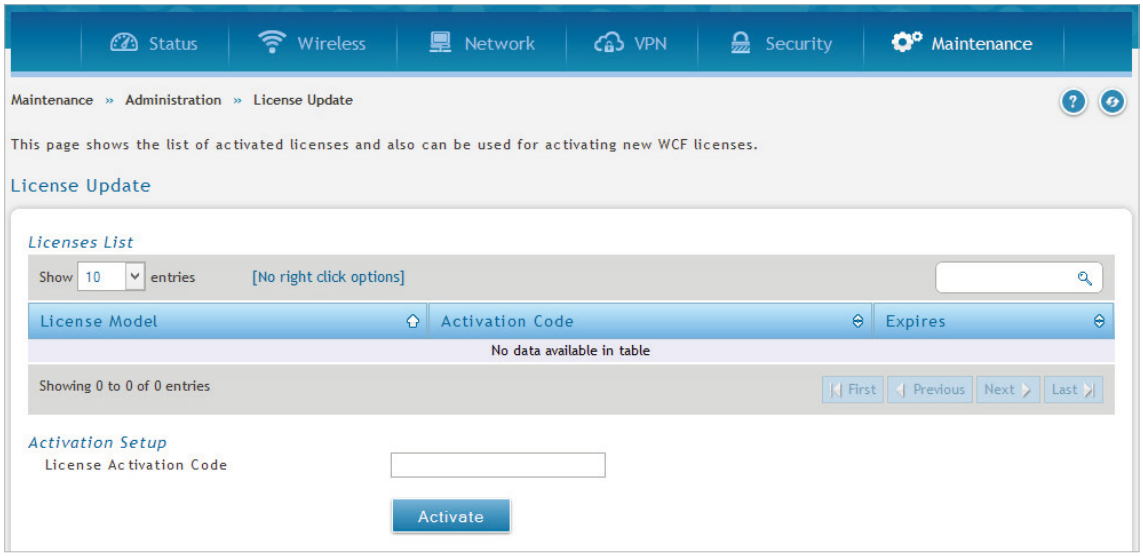

図 9-4　License Update 画面

3. 「Activation Setup」セクション の「License Activation Code」に、アクティブ化したいライセンスに対して D-Link が供給したコードを入力します。
4. 「Activate」をクリックします。アクティベーションコードはリストに表示されます。
5. ライセンスを有効にするには、本製品を再起動します。

USB Share Ports（USB 共有ポートの設定）

Maintenance > Administration > USB Share Ports メニュー

デバイスに USB 共有機能を設定します。

1. **Maintenance > Administration > USB Share Ports** の順にメニューをクリックし、以下の画面を表示します。

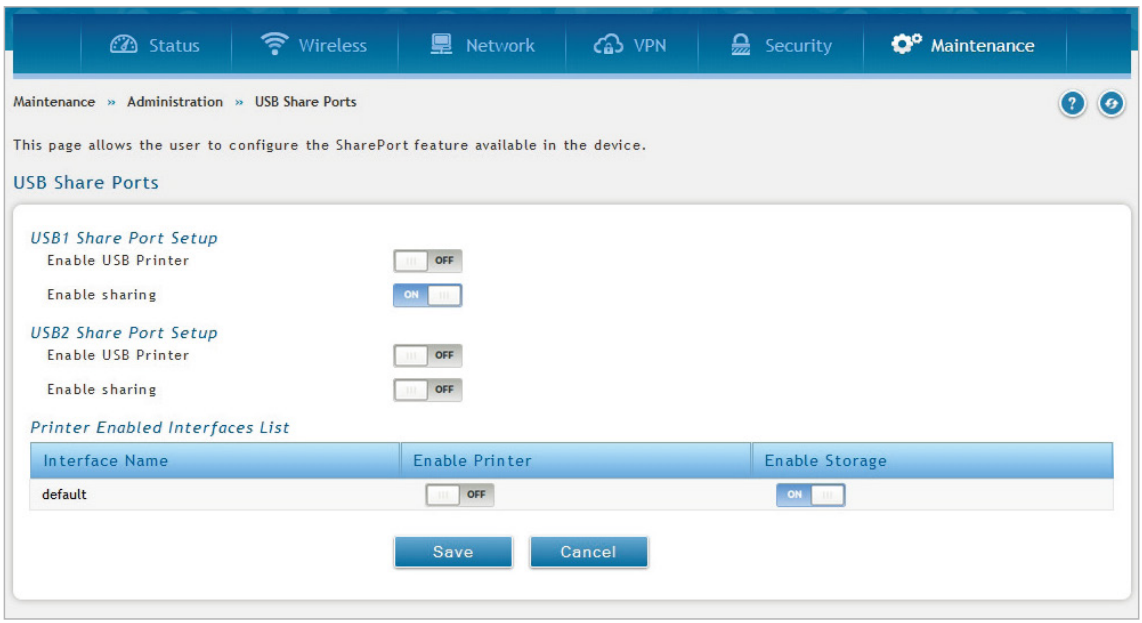

図 9-5　　USB Share Ports 画面

2. 以下の項目を設定します。

項目	説明
USB1/2 Share Port Setup	
Enable USB Printer	「ON」にすると、当該 USB ポートに接続するプリンタをネットワークを経由して共有できるようになります。
Enable Sharing	「ON」にすると、当該 USB ポートに接続する USB デバイスをネットワークを経由して共有できるようになります。
Printer Enabled Interfaces List	
Interface Name	プリンタのインタフェース名が表示されます。
Enable Printer	インタフェースのプリンタを「ON」または「OFF」にします。
Enable Storage	インタフェースのストレージを「ON」または「OFF」にします。

3. 「Save」をクリックし、設定を適用します。

SMS Service（SMS サービス（未サポート））

Maintenance > Administration > SMS Service メニュー
SMS サービス機能を設定します。

注意　本機能は未サポートです。

本ルータでは USB インタフェースに 3G モデムを差し込みショートメールサービス（SMS）の送受信を行うことが可能です。受信したメッセージは「Inbox」に格納され、また新しいショートメッセージ（SMS）を作成、送信することが可能です。「WAN3」が WAN モード、ロードバランシングモードとして使用されている場合、または 3G USB モデムが接続されていない場合は、本項目は表示されません。

Inbox（受信箱）

受信した SMS を表示します。

1. **Maintenance > Administration > SMS Service > Inbox タブ**の順にメニューをクリックし、以下の画面を表示します。

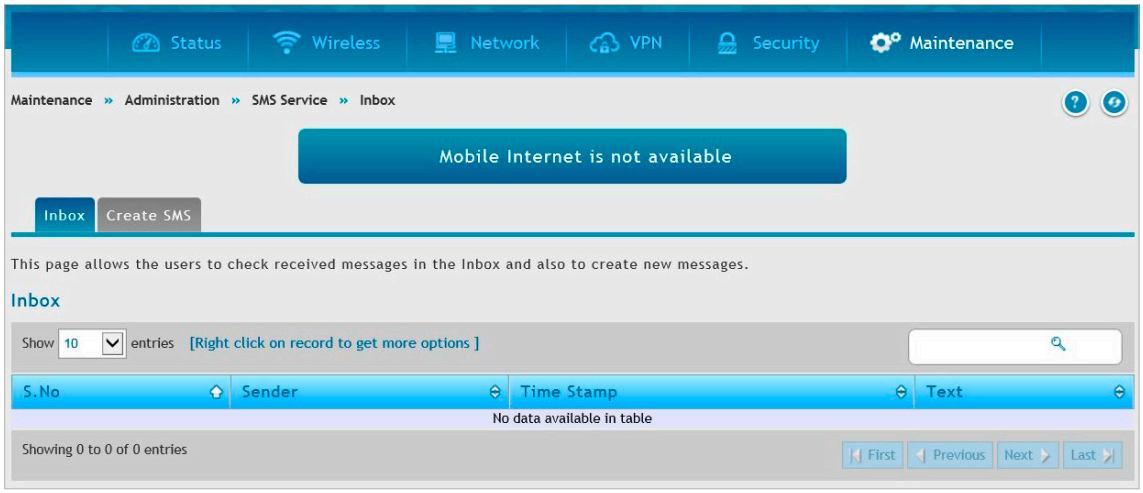

図 9-6　SMS Service > Inbox タブ画面

2. 以下の項目が表示されます。

項目	説明
S. No	SMS のシリアル番号を表示します。
Sender	SMS の送信者を表示します。
Time Stamp	SMS の送信時間を表示します。
Text	SMS の本文を表示します。

エントリを右クリックすると、以下のメニューを選択できます。
- 「Delete」：削除
- 「Refresh」：更新
- 「Reply」：返信
- 「Forward」：転送

3. 「Save」をクリックし、設定を適用します。

Create SMS（SMS 作成）

SMS の作成と送信を行います。

注意　本機能は未サポートです。

1. **Maintenance > Administration > SMS Service > Create SMS タブ**の順にメニューをクリックし、以下の画面を表示します。

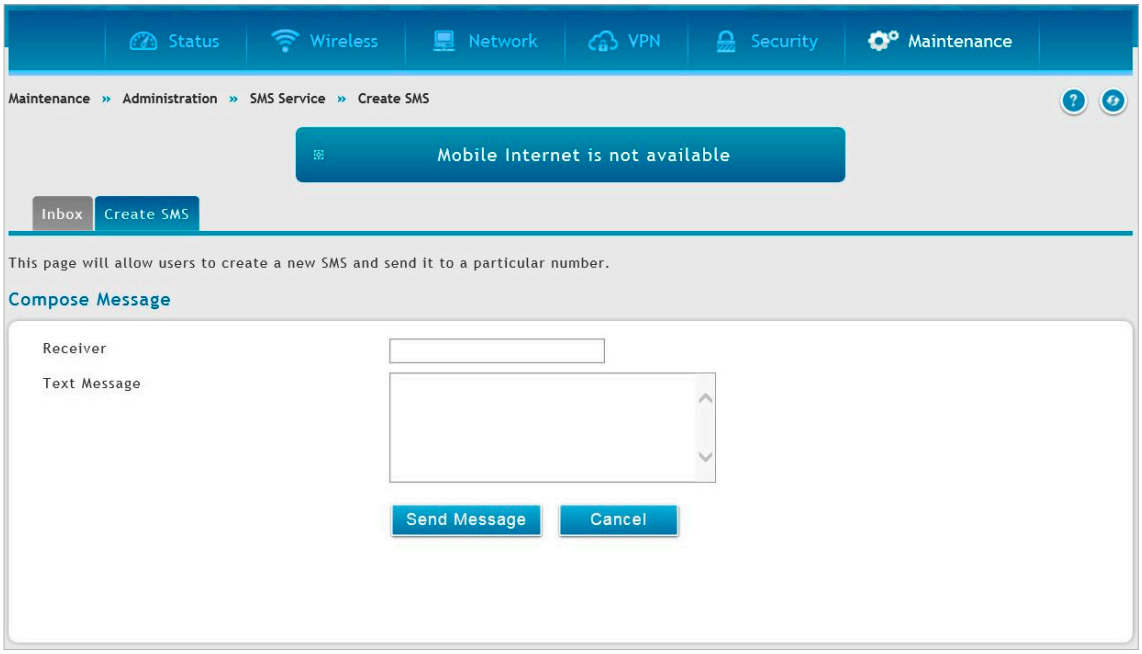

図 9-7　SMS Service > Create SMS タブ画面

2. 以下の項目で設定を行います。

項目	説明
Receiver	受信者の電話番号を指定します。
Text Message	メッセージ本文を作成します。
Send Message	クリックしてメッセージを送信します。
Cancel	メッセージの送信をキャンセルします。

Package Manager（パッケージマネージャ）

Maintenance > Administration > Package Manager メニュー

「Package（パッケージ）」はルータによって D-Link リポジトリからインストールされるファイルの集合体です。本機能では、サポートされる USB デバイス用のドライバや、ルータ管理画面の多言語サポートを有効にする言語パックなどをダウンロードします。

パッケージマネージャによる多言語サポートでは、ルータのユーザインタフェースで使用されている全テキストを選択した言語で表示させます。ドライバと言語の言語パックはそれぞれ 1 種類ずつルータ上に保存することができます。ドライバおよび言語パックは、ルータの再起動後に使用可能となります。

以下 2 種類のインストール方法があります。

1. 手動インストール（Manual Installation）: 手動インストールを行う場合は、まずパッケージをダウンロードする必要があります。ダウンロードしたパッケージは GUI で表示され、選択することができるようになります。

   注意　D-Link からの提供されるドライバのみ選択できます。検証プロセスはインストール中に行われます。

2. 自動インストール（Auto Installation）: 表示されるリンク “click here” をクリックすることで自動インストール対応のパッケージリストが表示されます。有効なドライバ / 言語パックのリストが表示されている画面からオプションを指定し、インストールを行います。このタイプのインストールでは、リポジトリサーバからパッケージをダウンロードするため、ルータは常にインターネットに接続されている必要があります。

1. **Maintenance > Administration > Package Manager** の順にメニューをクリックし、以下の画面を表示します。

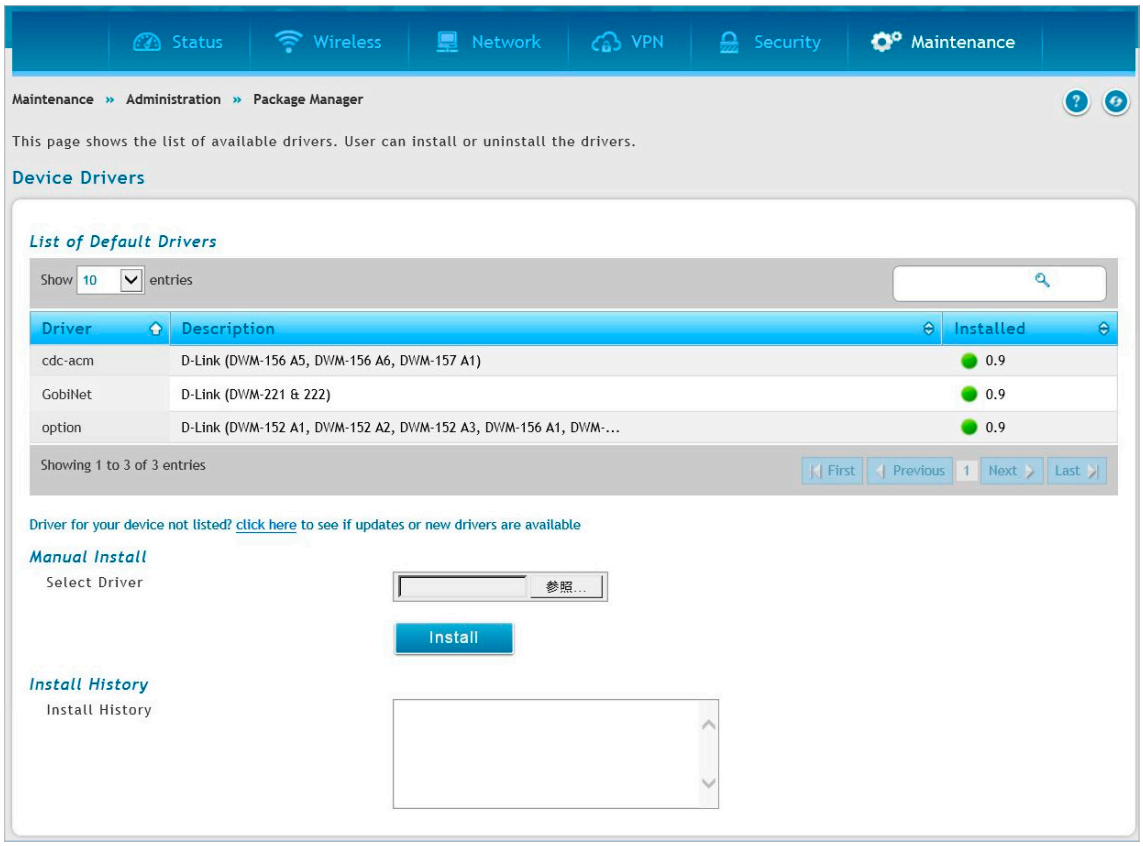

図 9-8　Package Manager 画面

2. 以下の項目を設定します。

項目	説明
List of Default Drivers	インストールされている初期ドライバを表示します。
Click Here	クリックしてダウンロード可能なパッケージ一覧を表示します。インターネットに接続している必要があります。パッケージ一覧からアップデート / インストールするドライバを選択します。
Manual Install	パッケージをダウンロード済みの場合、以下の手順でインストール行います。 （1）「Browse/ 参照」をクリックしパッケージを選択 （2）「Opem/ 開く」をクリックします。 （3）「Install」をクリックします。
Install History	インストール履歴を表示します。

日本語言語パック（Japanese Language Installation Pack）の設定

日本語言語パック（Japanese Language Installation Pack）のダウンロード、インストールについて説明します。

1. **Maintenance > Administration > Package Manager** の順にメニューをクリックし、以下の画面の「click here」をクリックします。

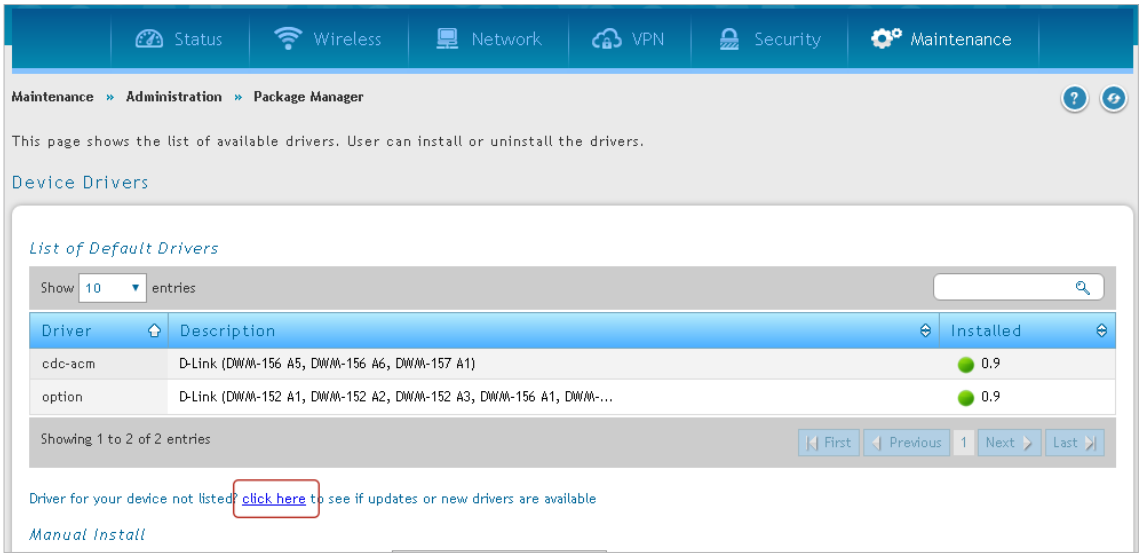

図 9-9　Package Manager 画面（ダウンロード）

項目	説明
Driver for your device not listed? click here to see if updates or new drivers are available	リストに希望のドライバーがない場合、「click here」をクリックし、有効なドライバのアップデートをご確認ください。

2. インストール可能なドライバの一覧が表示されます。
「List of Device Drivers」から「Japanese Language Installation Pack」を選択 → 右クリックし「Install」を選択します。

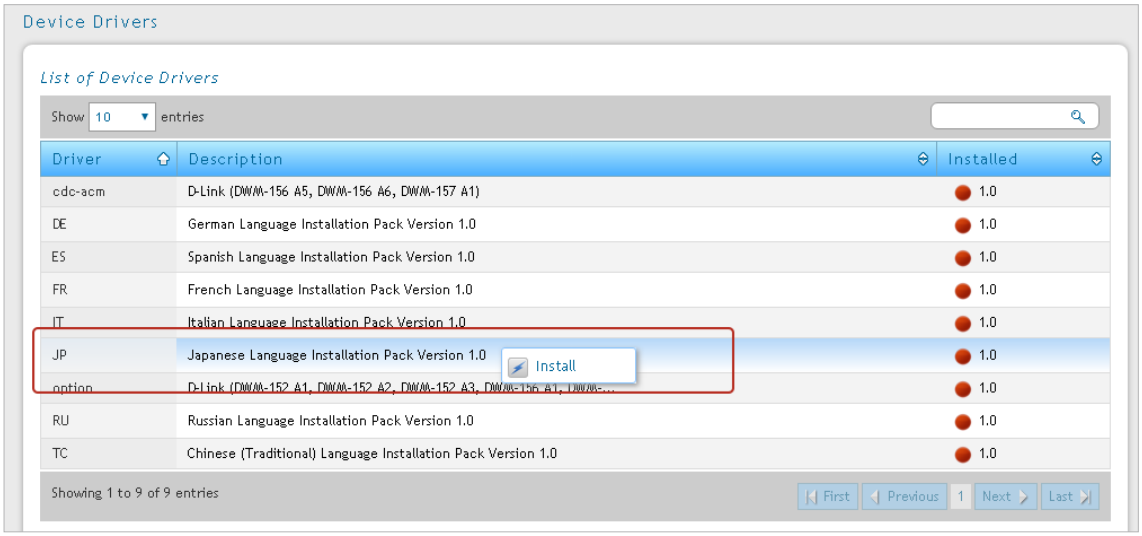

図 9-10　Japanese Language Installation Pack 画面

3. 上部に「Operation Succeeded」と表示され、「Japanese Language Installation Pack」の「Installed」の項目が緑になっていると、言語パックが正しくインストールされたことを意味します。

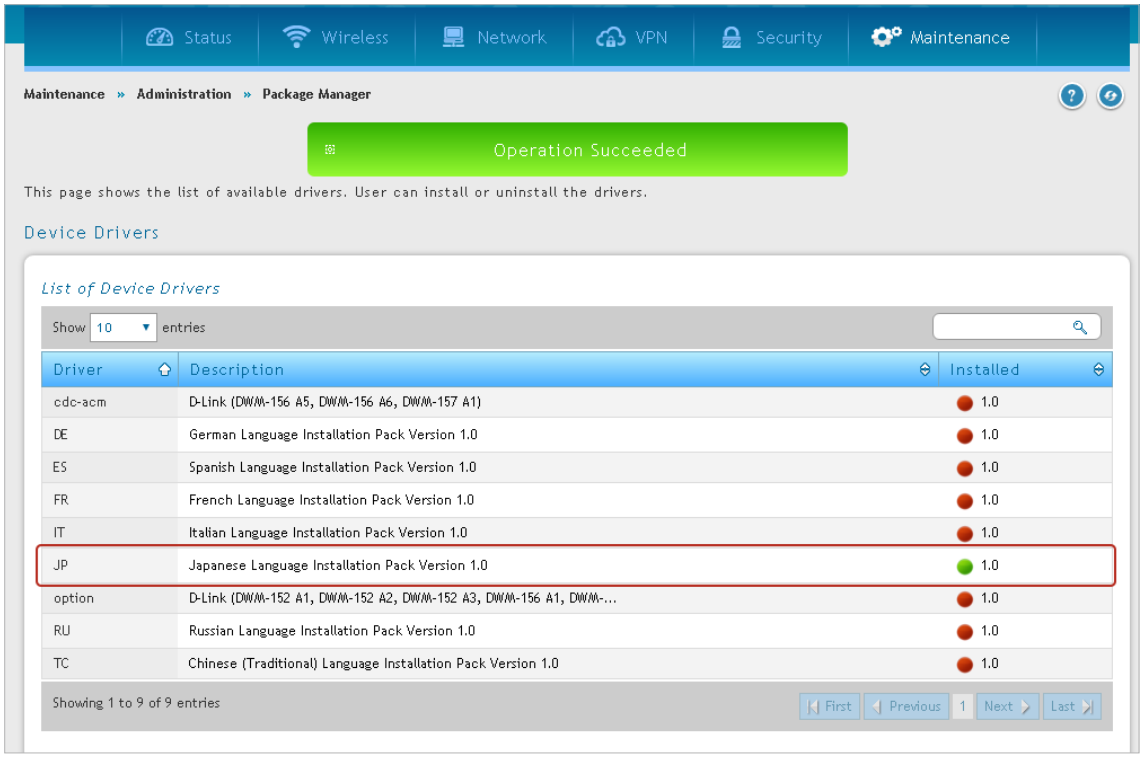

図 9-11　Japanese Language Installation Pack 画面（インストール済み）

4. 次に、**Maintenance > Administration > Set Language** の順にメニューをクリックし、「Set Language」（言語設定）を表示します。「Set Language」のドロップダウンメニューで「Japanese」を選択 →「Save」をクリックし、設定を適用します。

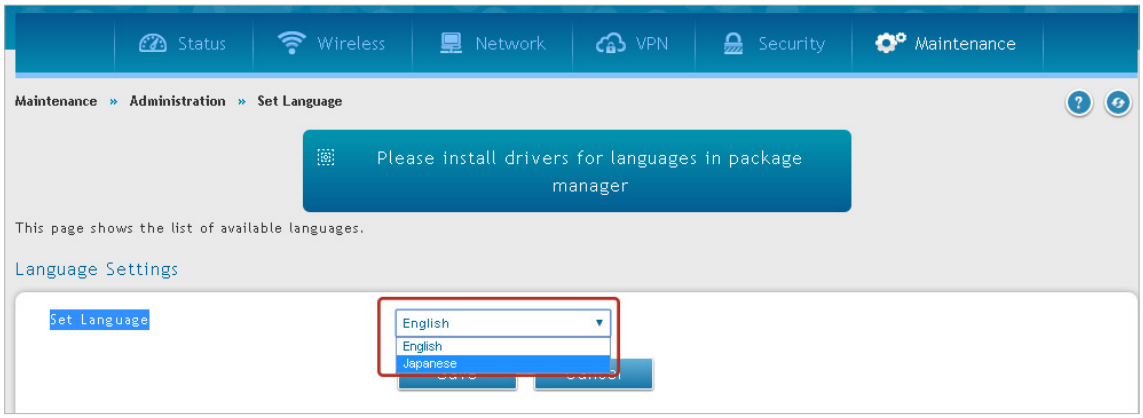

図 9-12　Set Language 画面（選択）

5. 上部に「操作に成功しました」と表示されます。

図 9-13　Set Language 画面（日本語）

Set Language（言語設定）

Maintenance > Administration > Set Language メニュー

「Package Manager」で取得した言語パックの設定を行います。

1. **Maintenance > Administration > Set Language** の順にメニューをクリックし、以下の画面を表示します。

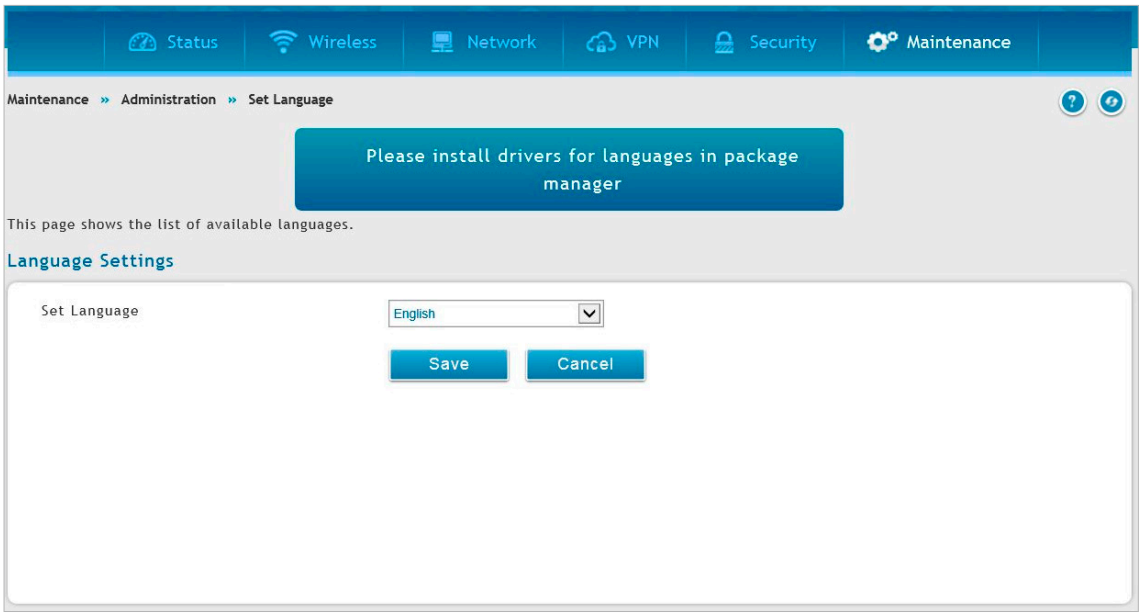

図 9-14　Set Language 画面

2. 以下の項目を設定します。

項目	説明
Set Language	ドロップダウンメニューから言語を選択します。

注意　Web GUI の日本語化を行う場合は、「日本語言語パック（Japanese Language Installation Pack）の設定」を参照してください。

Web GUI Management（Web GUI 管理）

Maintenance > Administration > Web GUI Management メニュー
Web GUI へのアクセスを許可する IP アドレスまたは VLAN を指定します。

1. **Maintenance > Administration > Web GUI Management** の順にメニューをクリックし、以下の画面を表示します。

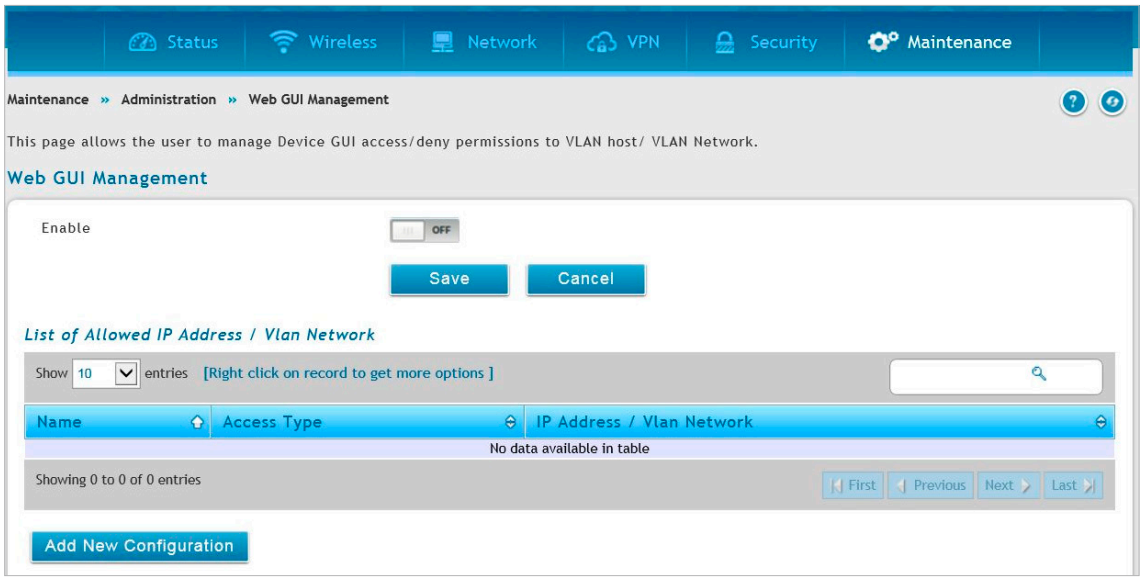

図 9-15　Web GUI Management 画面

2. 「Enable」を「ON」にし、「Save」をクリックします。
3. 「Add New Configuration」をクリックし、新しい設定を追加します。

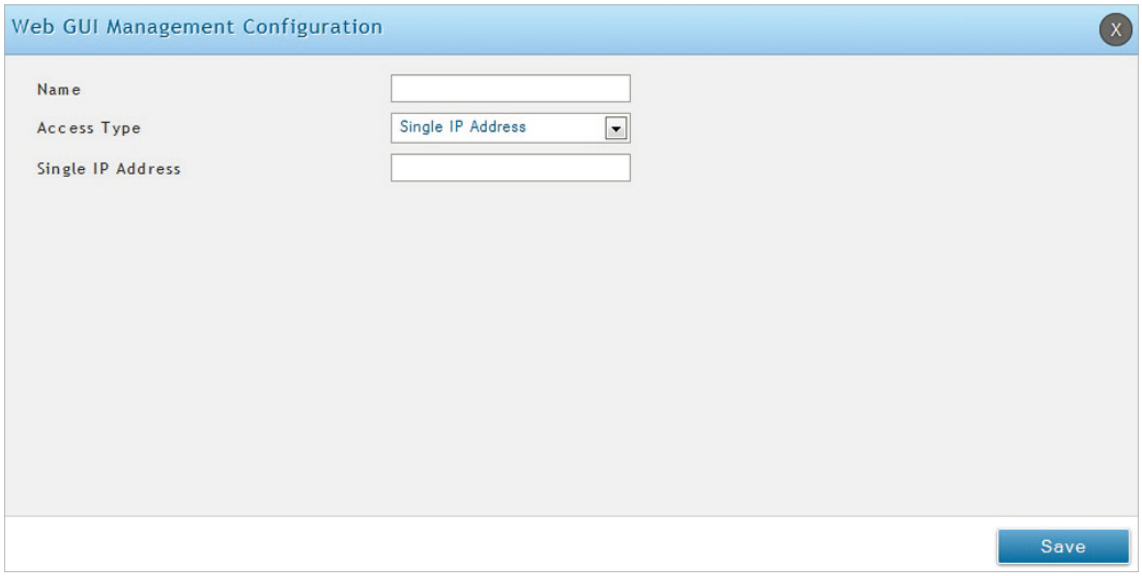

図 9-16　Web GUI Management Configuration 画面

4. 以下の項目を設定します。

項目	説明
Name	設定名を指定します。
Access Type	アクセスタイプを「Single IP Address」または「VLAN Network」から選択します。
Single IP Address	Web GUI へのアクセスを許可するコンピュータ / デバイスの IP アドレスを指定します。
VLAN Network	Web GUI へのアクセスを許可するコンピュータ / デバイスの VLAN ID を指定します。

5. 「Save」をクリックし、設定を適用します。

エントリの編集
編集するエントリを右クリックし、「Edit」を選択します。
設定変更後、「Save」をクリックします。

エントリの削除
削除するエントリを右クリックし、「Delete」を選択します。
すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

Management（管理設定）

Maintenance > Management メニュー

Remote Management（リモート管理）

Maintenance > Management > Remote Management メニュー

HTTPS または Telnet を使用した本製品のリモート管理を有効にできます。IP アドレスのサブネットに対し、HTTPS と Telnet 両方の接続を制限することができます。ルータの管理者は、お使いの PC、IP アドレス /IP アドレス範囲で HTTPS 経由での GUI へアクセスを制限できます。リモート IP アドレス範囲の許可設定と同時に、SSL トラフィックのオープンポートを初期値である 443 から変更することも可能です。

1. **Maintenance > Management > Remote Management** の順にメニューをクリックし、以下の画面を表示します。

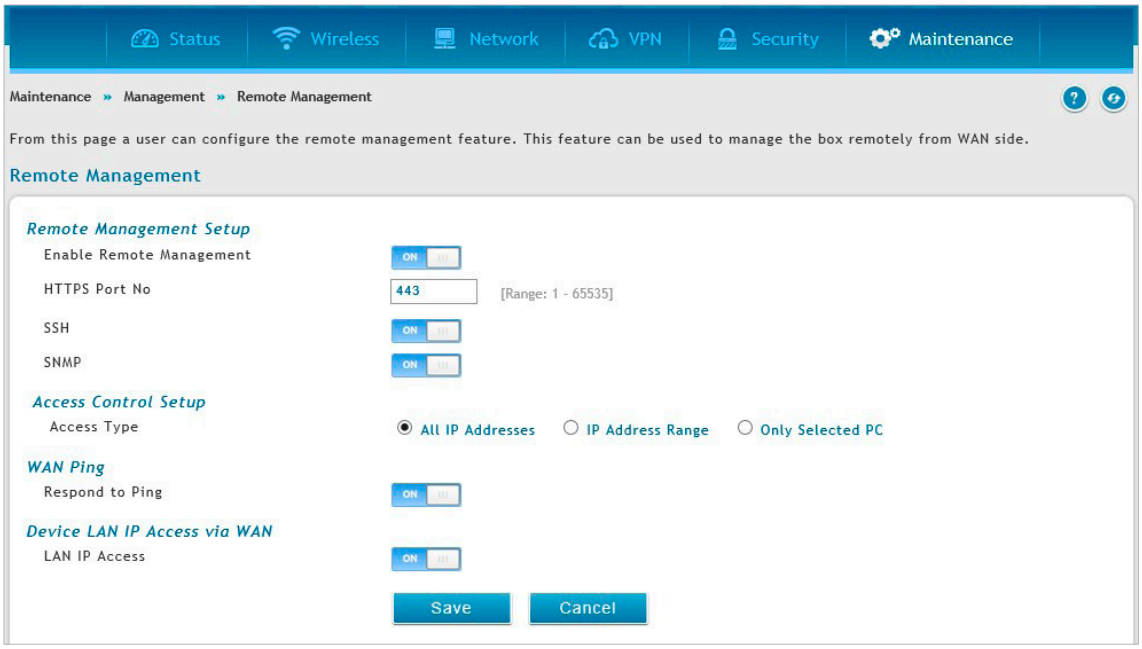

図 9-17　Remote Management 画面

2. 以下の項目を設定します。

項目	説明
Enable Remote Management	「ON」にしてリモート管理を有効にします。
HTTPS Port No	HTTPS 接続のポート番号を指定します。 • 初期値：443
SSH	「ON」にして SSH（Secure Shell）プロトコルを有効にします。SSH は、リモートホストからのネットワークを介した CLI アクセスで使用されます。
SNMP	「ON」にして SNMP でのリモート管理を有効にします。
Access Type	アクセスのタイプを以下から選択します。 「All IP Addresses」（全 IP アドレス）、「IP Address Range」（IP アドレス範囲）、「Only Selected PC」（選択したデバイス） • 「IP Address Range」（IP アドレス範囲）選択時は「From IP Address」と「To IP Address」で IP アドレス範囲を指定します。 • 「Only Selected PC」（選択したデバイス）選択時はデバイスの IP アドレスを指定します。
Respond to Ping	「ON」にして WAN からの Ping リクエストへの応答を許可します。
LAN IP Access	「ON」にして WAN 側からの LAN IP アクセスを有効にします。

3. 「Save」をクリックし、設定を適用します。

SNMP（SNMP の使用）

Maintenance > Management > SNMP メニュー

SNMP は、ネットワーク内の複数のルータが中央のマスタシステムに管理されている場合に便利な追加の管理ツールです。外部の SNMP マネージャにこのルータの MIB（Management Information Base）ファイルを提供する場合、マネージャは、構成パラメータの参照または更新のためにルータの階層変数を更新できます。管理デバイスとしてのルータは、マスタ（SNMP マネージャ）によって MIB 設定変数がアクセスされるのを許可する SNMP エージェントを搭載しています。ルータのアクセスコントロールリストは、Read-Only または Read-Write の SNMP 権限を持つネットワーク内のマネージャを識別します。トラップリストでは、このルータからの通知が SNMP コミュニティ（マネージャ）に提供されるポートと、トラップ用の SNMP バージョン（v1、v2c、v3）について概要が表示されます。

注意　本製品の SNMP 機能は読み取り専用となります。そのため、ユーザに割り当てる本製品へのアクセス権は「読み取り」のみです。

SNMP（SNMPv3 ユーザリストの設定）

SNMP v3 ユーザリストを設定します。

1. **Maintenance > Management > SNMP > SNMP タブ**の順にメニューをクリックし、以下の画面を表示します。

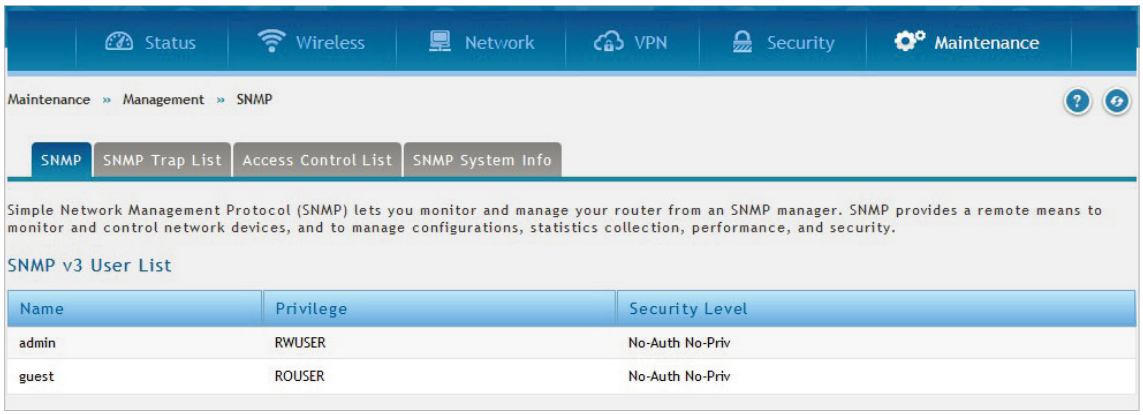

図 9-18　SNMP > SNMP タブ画面

2. 「admin」または「guest」を右クリック →「Edit」を選択し、以下の画面を表示します。

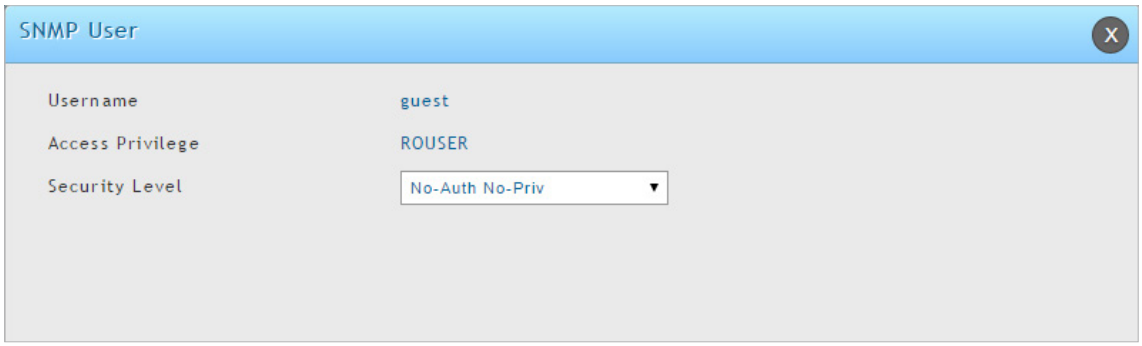

図 9-19　SNMP User 画面（guest）

3. 以下の項目を設定します。

項目	説明
Username	SNMPv3 マネージャのユーザ名を表示します。
Access Privilege	アクセス権限が表示されます。
Security Level	このユーザの認証とプライバシー設定を定義します。 - 「No-Auth No-Priv」：認証にユーザ名の一致のみを必要とします。 - 「Auth No-Priv」：MD5 または SHA アルゴリズムに基づいた認証を提供します。 - 「AuthPriv」：DES-256 ビットを使用した暗号プライバシーと、MD5 または SHA アルゴリズムに基づいた認証を提供します。

4. 「Save」をクリックし、設定を適用します。

SNMP Trap List（SNMP トラップリスト）

ルータがトラップメッセージを送信する SNMP エージェントの IP アドレスを設定および表示します。

1. **Maintenance > Management > SNMP > SNMP Trap List タブ**の順にメニューをクリックし、以下の画面を表示します

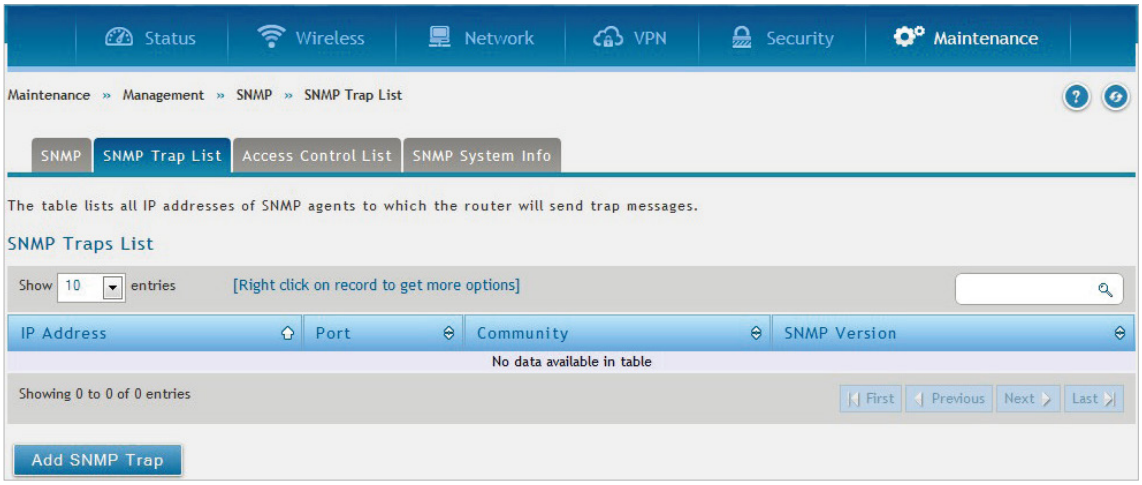

図 9-20　SNMP > SNMP Trap List タブ画面

2. トラップを追加する場合は、「Add SNMP Trap」をクリックし画面を表示します。

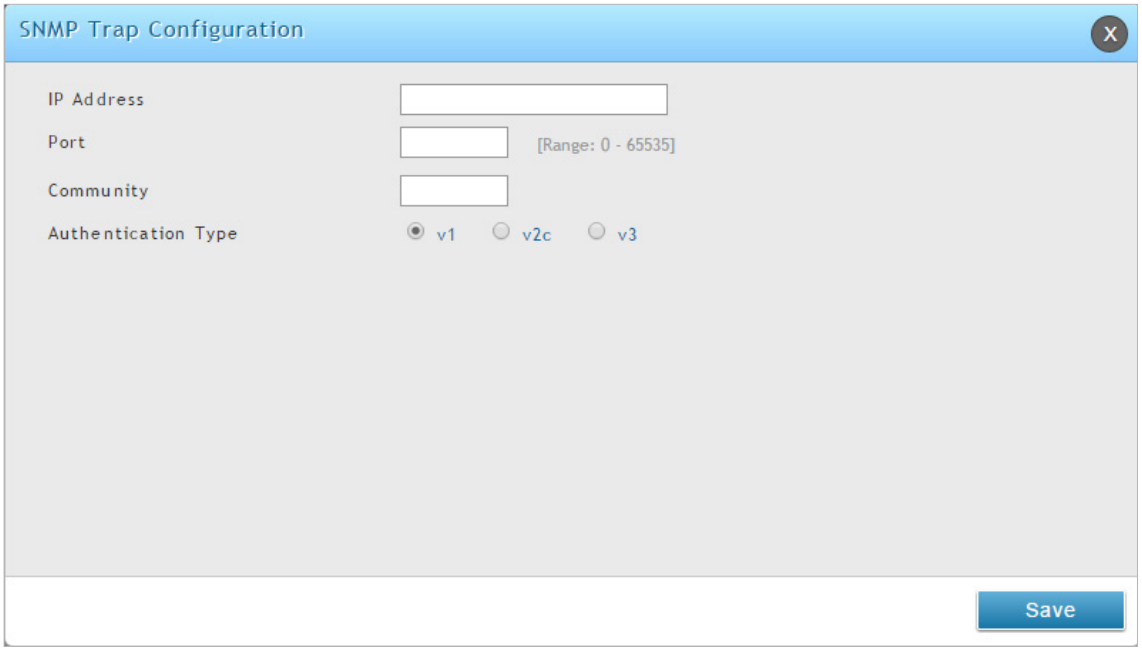

図 9-21　SNMP Trap Configuration 画面

3. 以下の項目を設定します。

項目	説明
IP Address	SNMP トラップエージェントの IP アドレスを入力します。
Port	トラップメッセージが送信される宛先 SNMP トラップポートを指定します。
Community	エージェントが所属するコミュニティストリングを指定します。多くのエージェントは、Public コミュニティでトラップにリッスンするように設定されます。
Authentication Type	トラップエージェントが使用する SNMP バージョン（v1、v2c、または v3）を選択します。

4. 「Save」をクリックし、設定を適用します。

エントリの編集

編集するエントリを右クリックし、「Edit」を選択します。
設定変更後、「Save」をクリックします。

エントリの削除

削除するエントリを右クリックし、「Delete」を選択します。
すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

Access Control List（SNMP アクセスコントロールリストの設定）

SNMP アクセスコントロールリストを設定します。

1. **Maintenance > Management > SNMP > Access Control List タブ**の順にメニューをクリックし、以下の画面を表示します

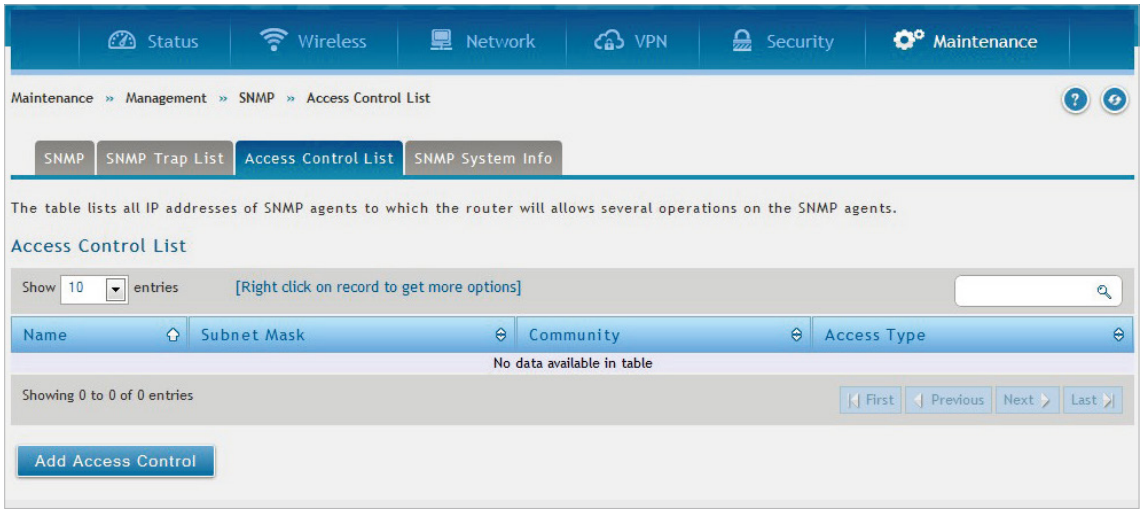

図 9-22　ASNMP > Access Control List タブ画面

2. エントリを右クリックして「Edit」「Delete」を行います。

3. 新しくアクセスコントロールを作成するには、「Add Access Control」をクリックします。

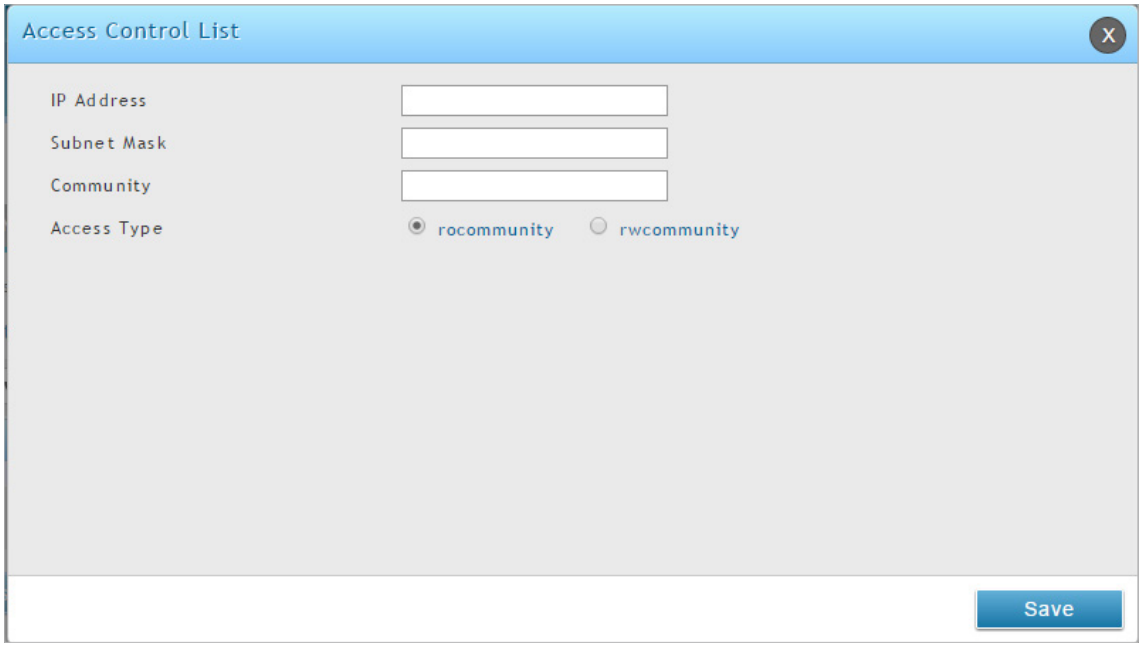

図 9-23　Access Control List 画面

4. 以下の項目を設定します。

項目	説明
IP Address	SNMP トラップエージェントの IP アドレスを入力します。
Subnet Mask	許可される SNMP マネージャリストを決定するために使用されるネットワークマスクを入力します。
Community	エージェントが所属するコミュニティストリングを入力します。多くのエージェントは、Public コミュニティでトラップにリッスンするように設定されます。
Access Type	アクセスの種類として、読取専用（rocommunity）または読み書き（rwcommunity）を選択します。

5. 「Save」をクリックし、設定を適用します。

エントリの編集

編集するエントリを右クリックし、「Edit」を選択します。
設定変更後、「Save」をクリックします。

エントリの削除

削除するエントリを右クリックし、「Delete」を選択します。
すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

SNMP System Info（SNMP システム情報の設定）

ルータの SNMP システム情報を設定します。

1. **Maintenance > Management > SNMP > SNMP System Info タブ**の順にメニューをクリックし、以下の画面を表示します

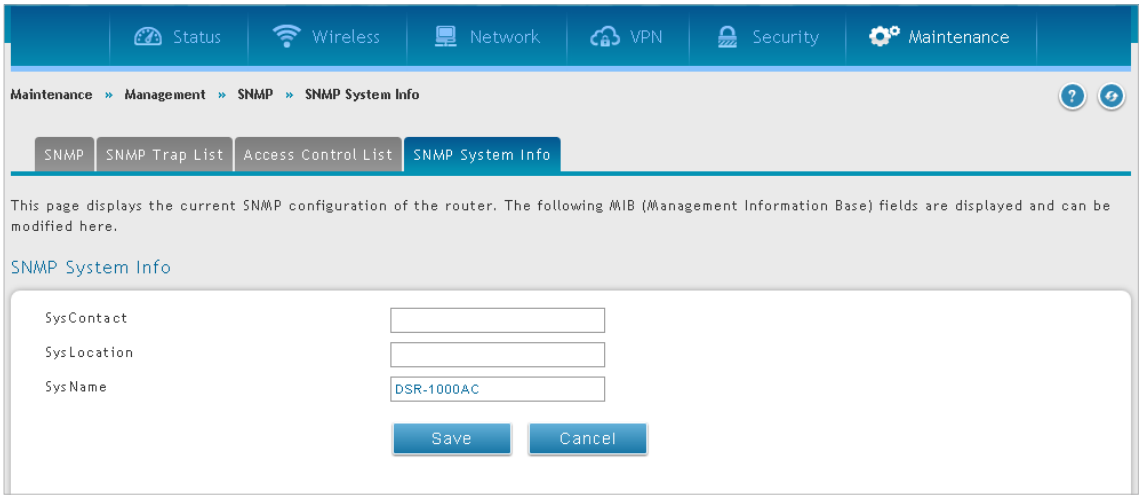

図 9-24　SNMP > SNMP System Info タブ画面

2. 以下の項目を設定します。

項目	説明
SysContact	本ルータの連絡窓口の名前を入力します。例 : admin、John Doe
SysLocation	ルータの物理的な位置を入力します。 例 : Rack#2,4th Floor
SysName	ルータの簡単な識別名を入力します。

3. 「Save」をクリックし、設定を適用します。

Diagnostics（診断ツール）

Maintenance > Management > Diagnostics メニュー
ルータの診断機能を実行します。

Network Tools（ネットワークツール）

Network Tools タブでは、ネットワークやインターネット上で本製品と他のデバイス間の接続性をテストすることができます。

■ Ping の送信

1. **Maintenance > Management > Diagnostics > Network Tools タブ**の順にメニューをクリックし、以下の画面を表示します。

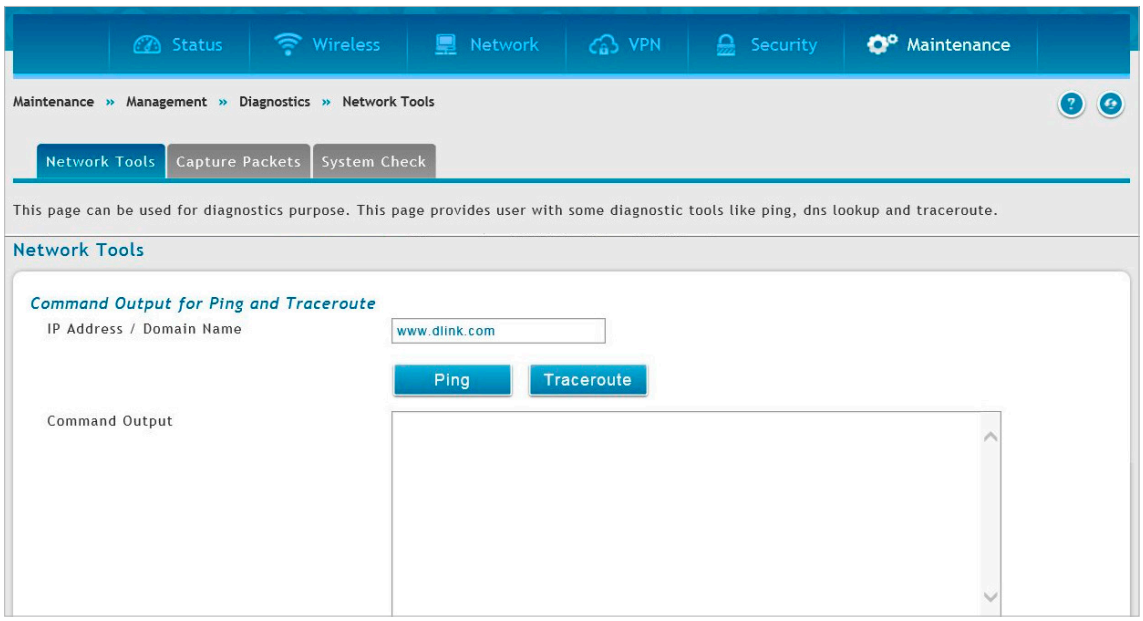

図 9-25　Diagnostics > Network Tools タブ画面

2. 「Command Output for Ping and Traceroute」セクションの「IP Address / Domain Name」に、IP アドレスまたはドメイン名を入力します。
3. 「Ping」をクリックすると、「Command Output」に結果が表示されます。

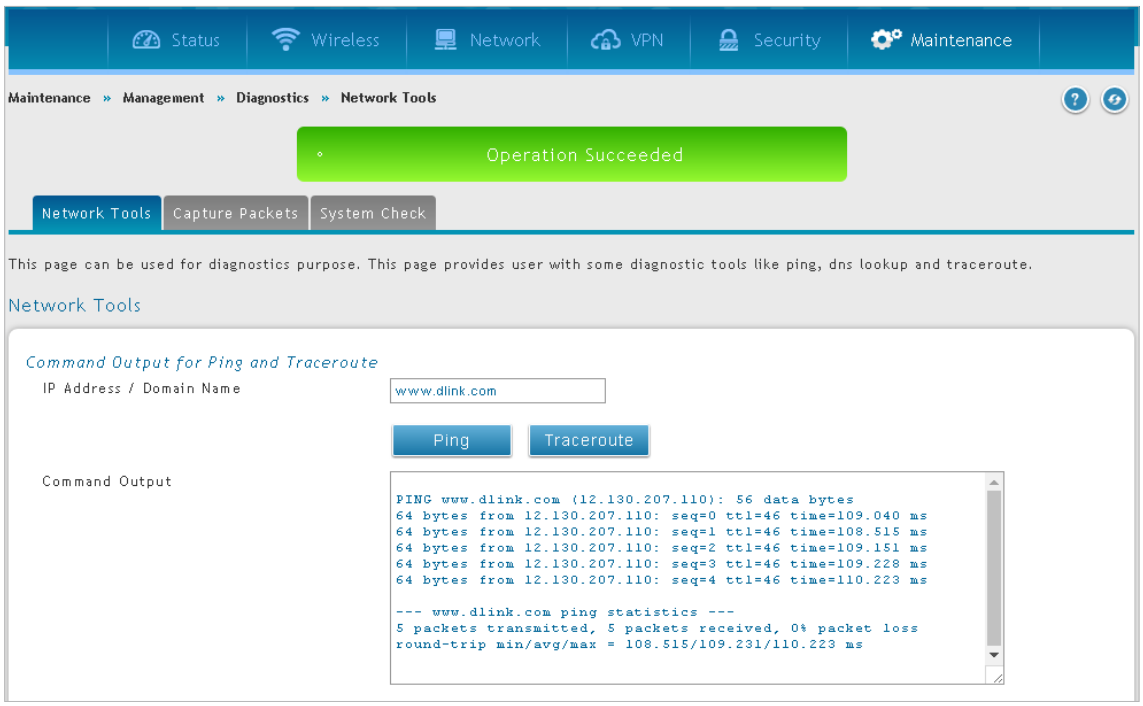

図 9-26　Diagnostics > Network Tools タブ画面

■ **Traceroute の使用**

本ルータは、ネットワークのパスをパブリックホストにマップさせる Traceroute 機能を提供します。
本ルータと宛先の間に位置する最大 30 個までのルータ（または「ホップ」）が表示されます。

1. **Maintenance > Management > Diagnostics > Network Tools タブ**の順にメニューをクリックし、以下の画面を表示します

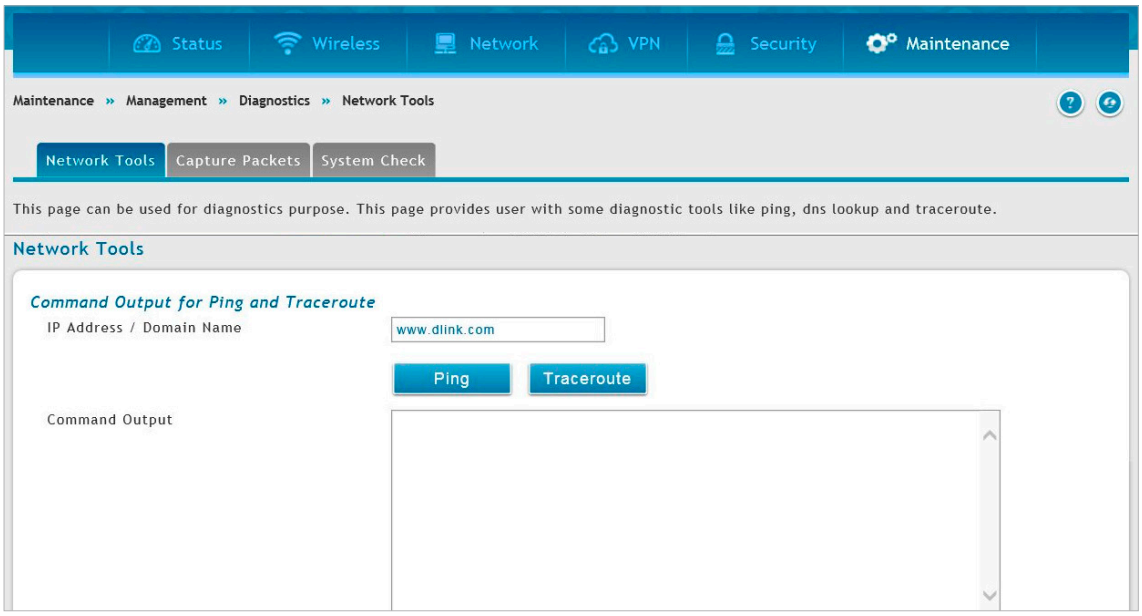

図 9-27　Diagnostics > Network Tools タブ画面

2. 「Command Output for Ping and Traceroute」にある「IP Address/Domain Name」に IP アドレスまたはドメイン名を入力します。
3. 「Traceroute」をクリックすると、「Command Output」に結果が表示されます。

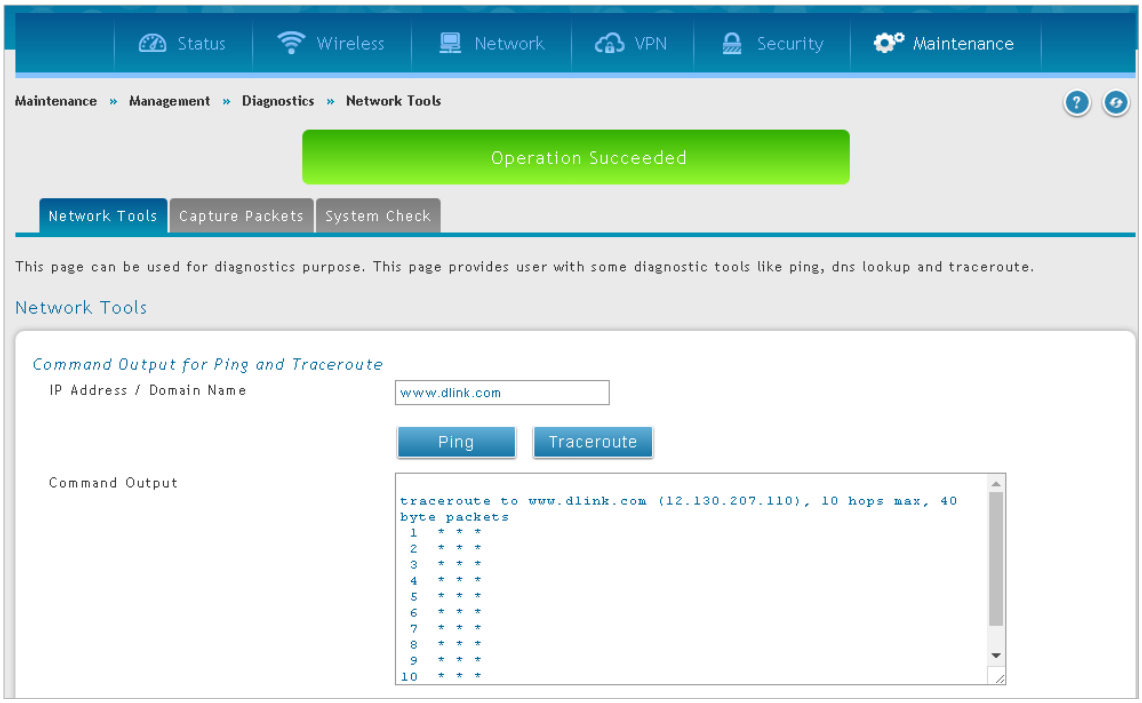

図 9-28　Diagnostics > Network Tools タブ画面

■ DNS 検索の実行

本製品は、インターネット上の Web、FTP、メール、またはその他のサーバの IP アドレスも検索できる DNS 索引機能を提供します。

1. **Maintenance > Management > Diagnostics > Network Tools タブ**の順にメニューをクリックし、以下の画面を表示します。

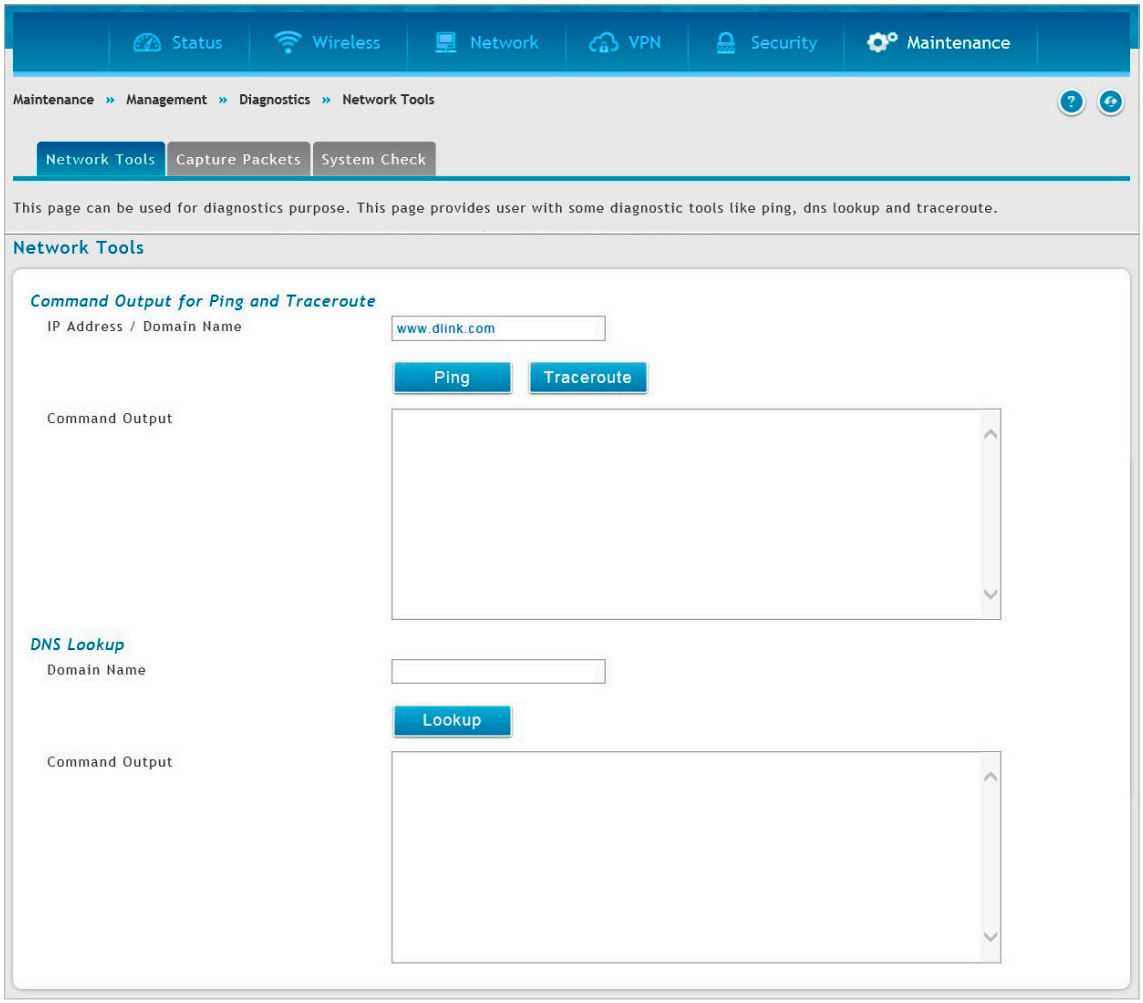

図 9-29　Diagnostics > Network Tools タブ画面

2. 「DNS Lookup」セクションの「Domain Name」に、インターネット名を入力します。

3. 「Lookup」をクリックすると、「Command Output」に結果が表示されます。ホストまたはドメインエントリが存在する場合、IP アドレスと共に応答を表示します。「Host Unknown」メッセージ表示された場合、そのインターネット名は存在しません。

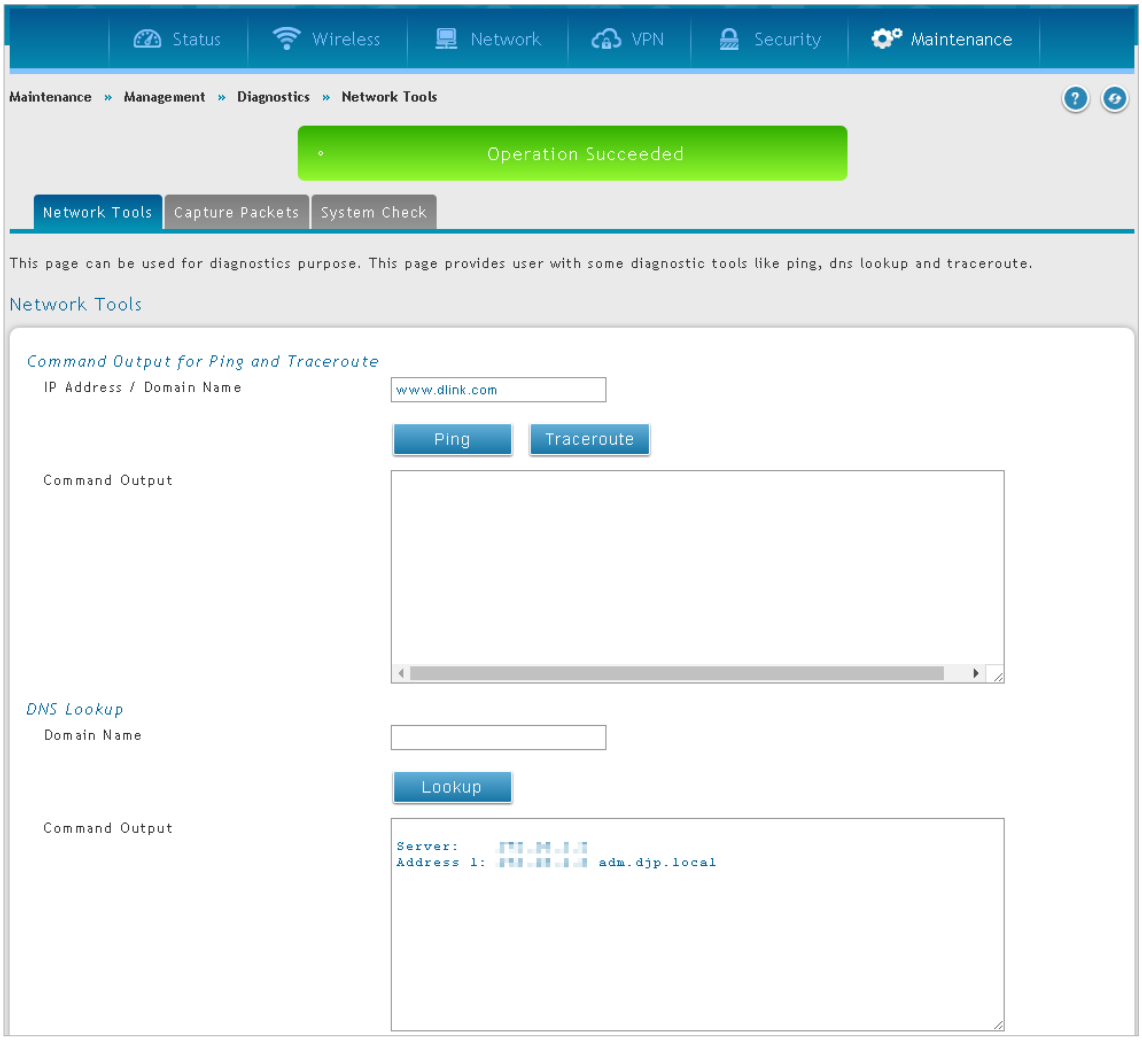

図 9-30　Diagnostics > Network Tools タブ画面

Capture Packets（パケットのキャプチャ）

本ルータでは LAN インタフェースを通過するすべてのパケットをキャプチャすることができます。パケットのトレースはキャプチャセッションあたり 1MB のデータに制限されます。キャプチャファイルサイズが 1MB を超えると、自動的に削除されて新しいキャプチャファイルが作成されます。

1. **Maintenance > Management > Diagnostics > Capture Packets タブ**の順にメニューをクリックし、以下の画面を表示します

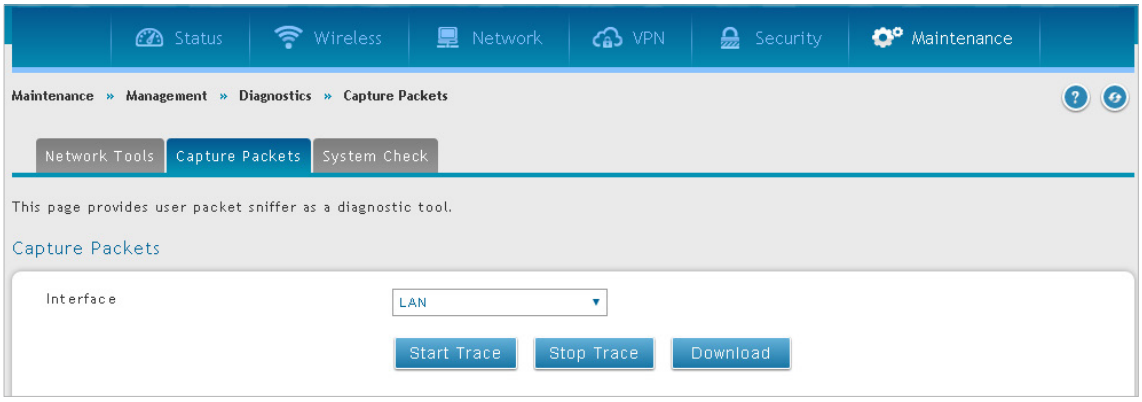

図 9-31　Diagnostics > Capture Packets タブ画面

2. 「Interface」のプルダウンメニューからインタフェースを選択します。

3. 「Start Trace」をクリックすると、パケットのキャプチャが開始されます。

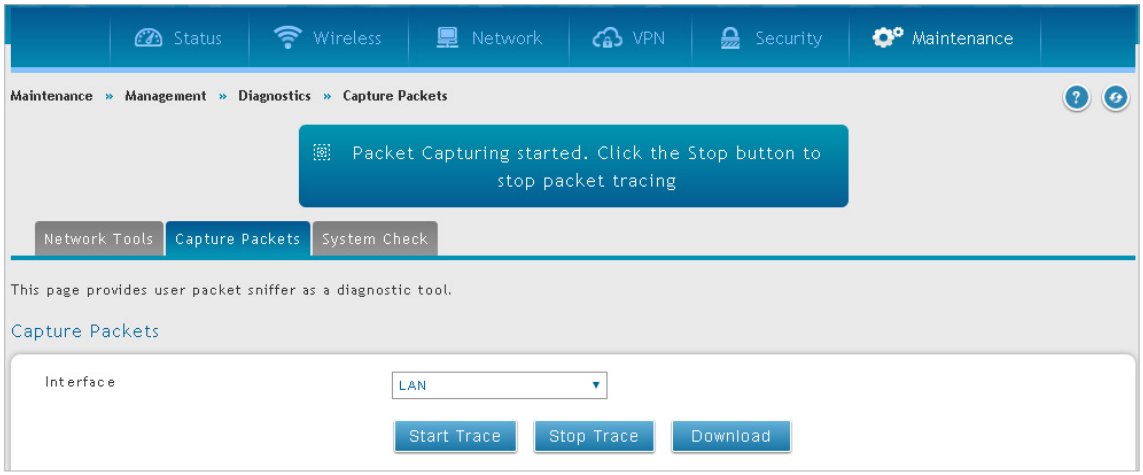

図 9-32　Diagnostics > Capture Packets タブ画面

4. パケットのキャプチャを停止するには「Stop Trace」をクリックします。

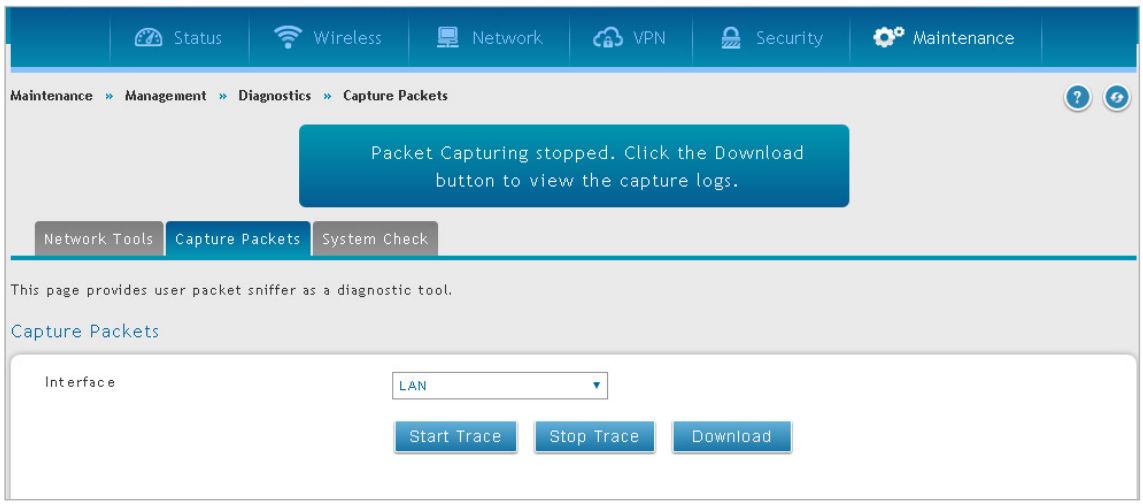

図 9-33　Diagnostics > Capture Packets タブ画面

5. 「Download」をクリックすると、トレース結果がブラウザのデフォルトのダウンロードフォルダに保存されます。

System Check（システムチェック）

ルータの診断機能の一部として、IPv4/IPv6 の両方についてスタティック / ダイナミックルートを表示することができます。

1. **Maintenance > Management > Diagnostics > System Check タブ**の順にメニューをクリックし、以下の画面を表示します

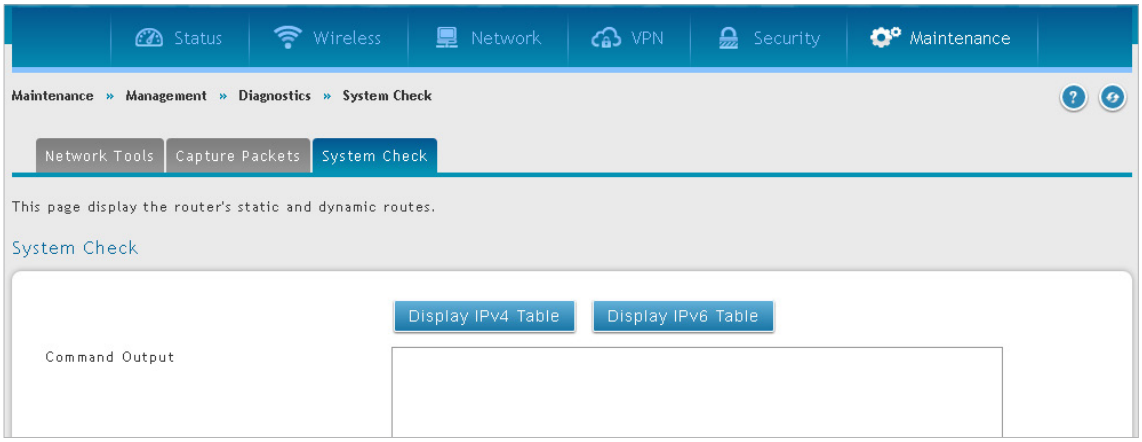

図 9-34　Diagnostics > System Check タブ画面

注意　IPv4 & IPv6 モードに設定されている場合、「Display IPv6 Table」が表示されます。

2. 「Display IPv4 Table」または「Display IPv6 Table」をクリックすると、「Command Output」に結果が表示されます。

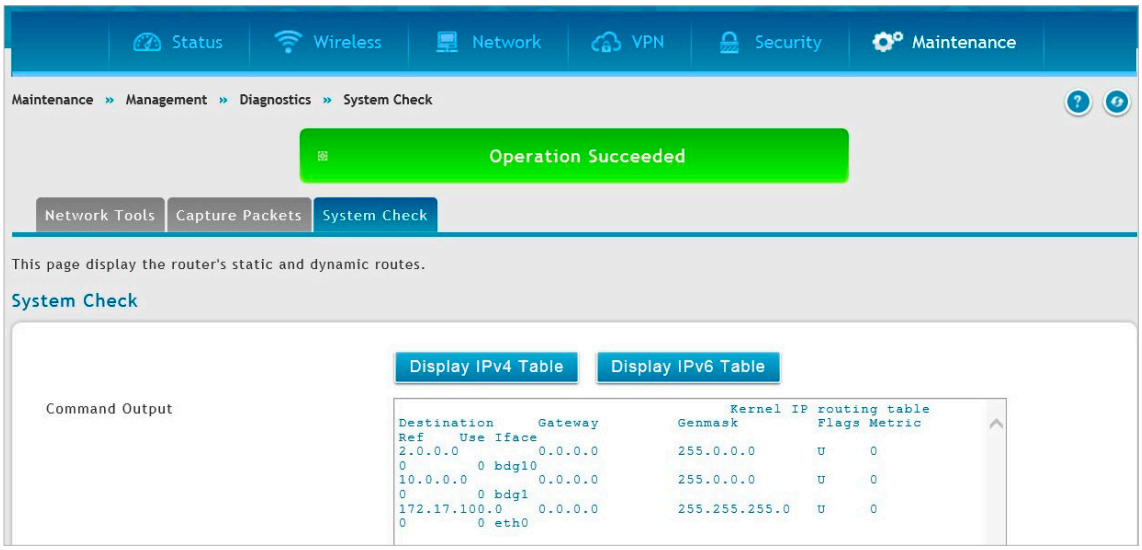

図 9-35　Diagnostics > System Check タブ画面（IPv4）

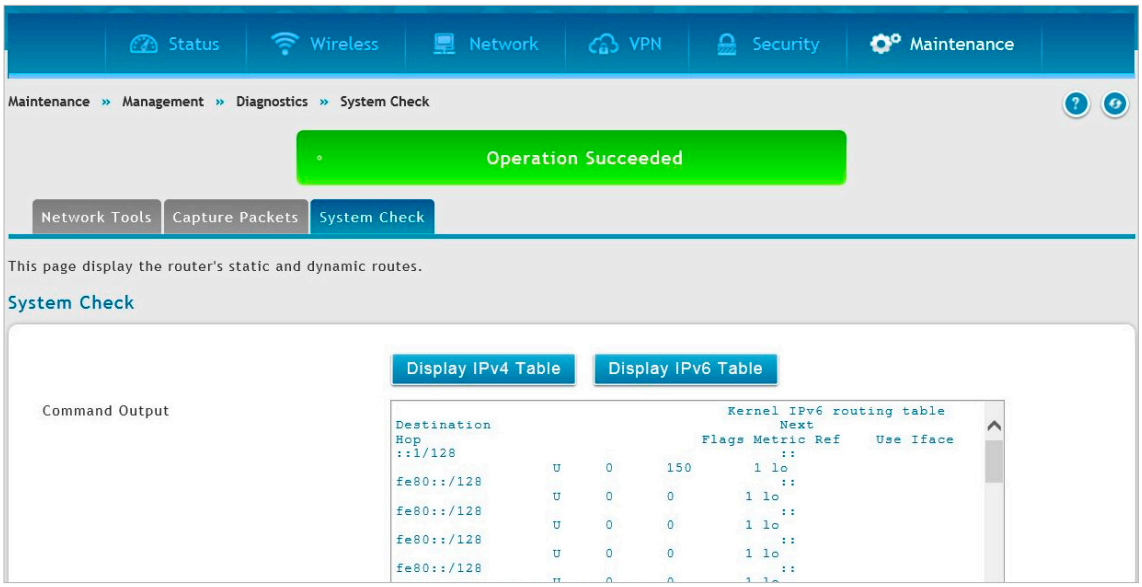

図 9-36　Diagnostics > System Check タブ画面（IPv6）

3. **Network > Routing > Static Routes > Static Route Configuration** 画面でルートが private に設定されている場合、「Display IPv4 Table」をクリックすると”Private ルートテーブル”が表示されます。

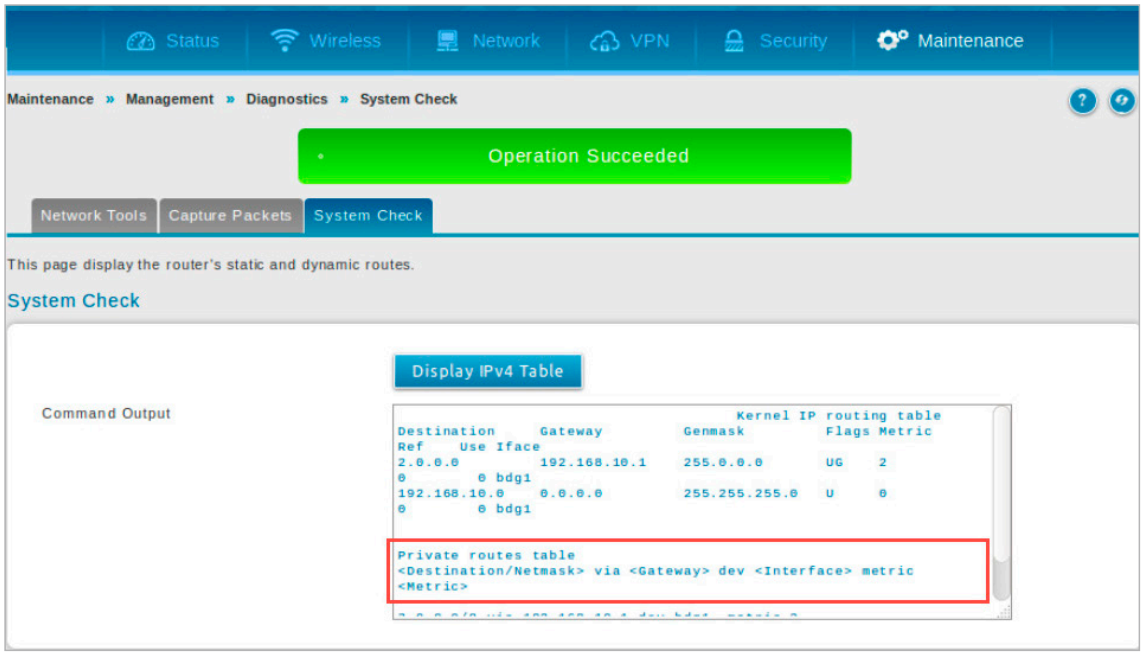

図 9-37　Diagnostics > System Check タブ画面（IPv4 - Private）

Power Saving（省エネ設定）

Maintenance > Management > Power Saving メニュー

本製品は、実際のハードウェアの状況に基づいて電力を調整することができます。
リンクステータスまたはケーブルの長さに応じて、消費電力を調整します。

1. **Maintenance > Management > Power Saving** の順にメニューをクリックし、以下の画面を表示します。

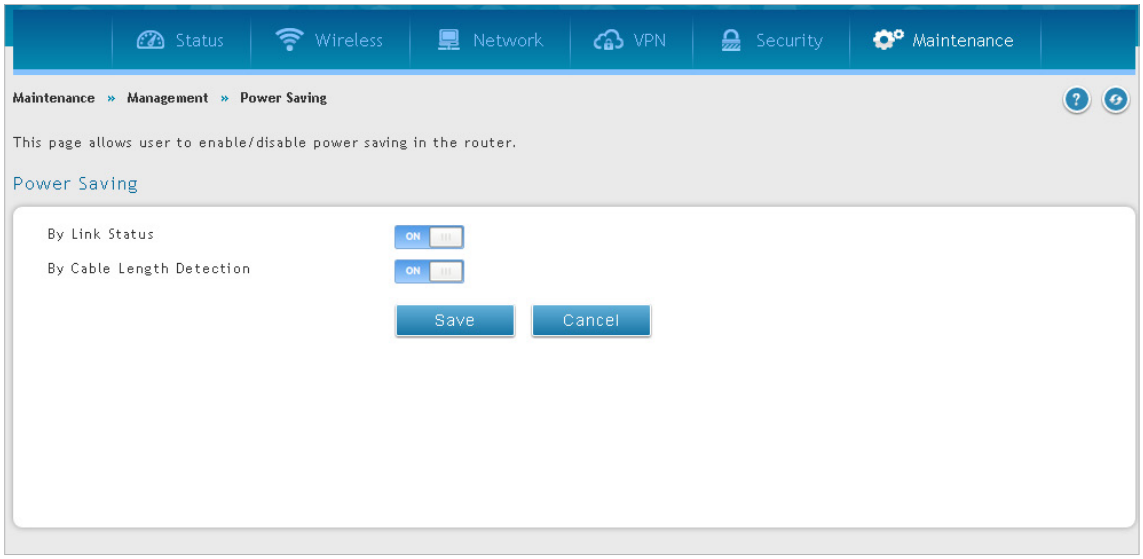

図 9-38　Power Saving 画面

2. 有効にする機能を「ON」に指定します。

項目	説明
By Link Status	本オプションを有効にすると、消費電力は接続ポート数に依存するようになります。すべての有効な LAN ポートがアクティブなイーサネット接続を行っている状態よりも、単一ポートのみ接続状態にある方が、電力消費を抑えられます。
By Cable Length Detection	本オプションを有効にすると、短いケーブルに接続した LAN ポートの消費電力を抑えることができます。

3. 「Save」をクリックし、設定を適用します。

DDP Client（DDP クライアント設定）

Maintenance > Management > DDP Client メニュー
DDP クライアントを有効または無効に設定します。

1. **Maintenance > Management > DDP Client** の順にメニューをクリックし、以下の画面を表示します。

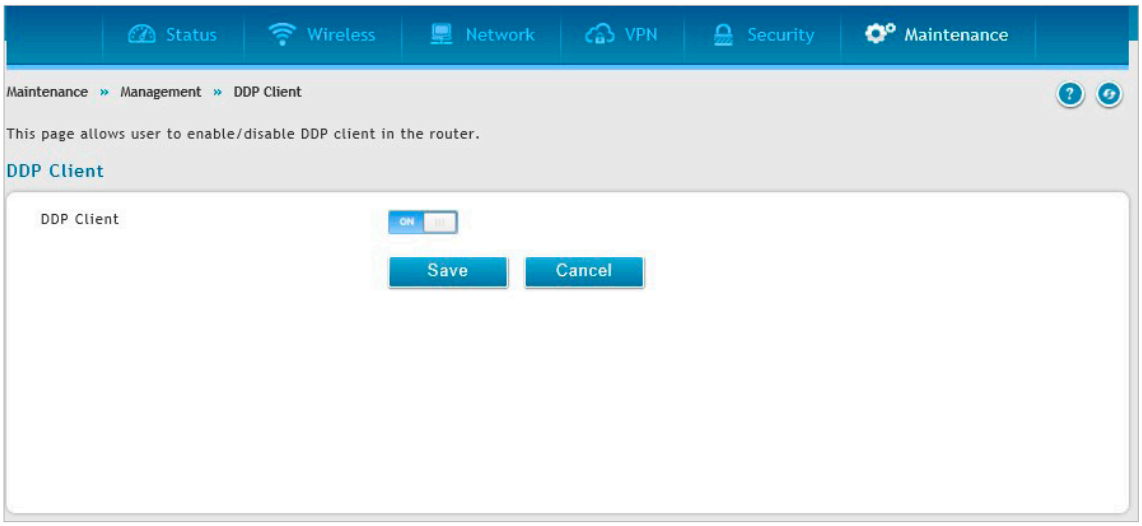

図 9-39　DDP Client 画面

2. DDP クライアントを「ON」または「OFF」に設定します。
3. 「Save」をクリックし、設定を適用します。

Firmware & Config（ファームウェアとコンフィグ）

Maintenance > Firmware & Config メニュー
ファームウェアのアップグレード方法と、コンフィグレーションのバックアップ / リストア方法について説明します。

Firmware Upgrade（ファームウェアアップグレード）

Maintenance > Firmware & Config > Firmware Upgrade メニュー

本画面では新しいファームウェアにアップグレードすることができます。「Firmware Upgrade」セクションでファイルを選択し、「Upgrade」をクリックしてアップグレードを実施します。新しいファームウェアファイルが検証された後、新しいイメージがフラッシュに書き込まれ、ルータは新しいファームウェアで自動的に再起動します。

■ ユニバーサルファームウェアの命名規則

新しいファームウェアの命名規則は「DSR_<Modelname>_<Hardware>x_FW <Version number>_<WW>」となります。各ハードウェア（A、B、Cなど）のすべてのバージョン（1、2、3など）に使用されるファームウェアファイルは 1 種類のみです。例えば、新しいファームウェアファイル名が「DSR_500_Ax_FW3.12_WW」である場合、このファームウェアは A2/A3/A4 などのハードウェアバージョンにおけるアップグレードで使用することができます。

注意 ファームウェアのアップグレード中は、オンライン接続・DSR の電源切断・PC のシャットダウンなど、処理を中断するアクションは行わないでください。アップグレードは再起動まで含めて数分程度で完了します。フラッシュ書き込み中にアップグレード処理が中断されると、フラッシュメモリが破損し、Web GUI を経由せずにフラッシュファームウェアをリストアしなければ使用することができなくなります。

Check Update（アップデートチェック）

新しいバージョンの利用可能なファームウェアがあるかチェックを行います。

注意 日本で使用する場合は、ディーリンクジャパンのサイト（https://www.dlink-jp.com/）からダウンロードしたファームウェアのみをご利用ください。

1. **Maintenance > Firmware & Config > Firmware Upgrade > Check Update タブ**の順にメニューをクリックし、以下の画面を表示します。

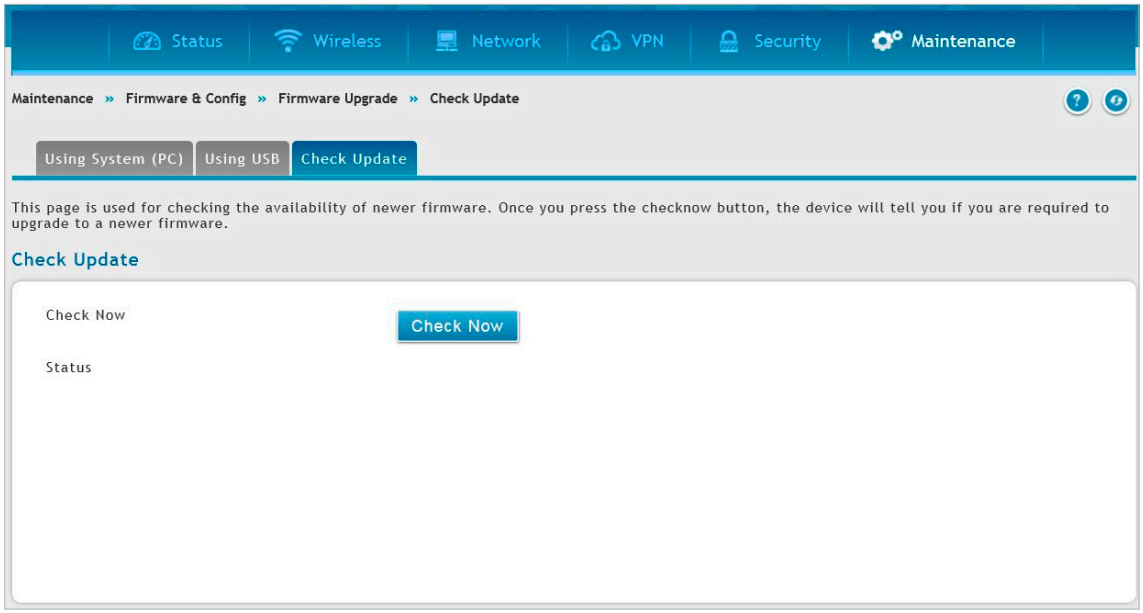

図 9-40　Firmware Upgrade > Check Update タブ画面

2. 「Check Now」をクリックすると、「Status」欄に新しいファームウェアの有無が表示されます。

Using System (PC)（PC を使用したファームウェアアップグレード）

1. D-Link Web サイトから新しいファームウェアをダウンロードします。
2. 本製品の Web GUI で、**Maintenance > Firmware & Config > Firmware Upgrade > Using System (PC) タブ**の順にメニューをクリックし、以下の画面を表示します。

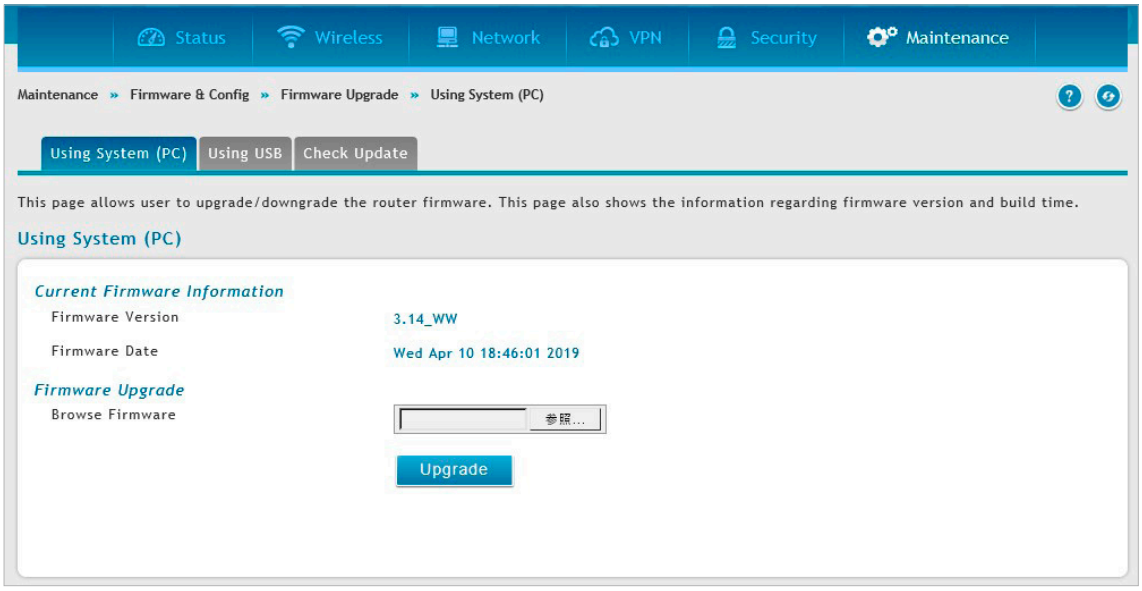

図 9-41　Firmware Upgrade > Using System (PC) タブ画面

3. 「Browse Firmware」の「参照 /Browse」をクリックします。
4. ファームウェアを選択後、「開く（Open）」をクリックします。
5. 「Upgrade」をクリックします。

注意 アップグレードのプロセスには数分かかります。アップグレードを中止したり、システムをオフにしたりしないでください。アップグレードが中断された場合、ファームウェアが破損する場合があります。ブラウザで他のサイトを参照せずに、アップグレードが完了するまでお待ちください。

Using USB（USB ドライブを使用したファームウェアアップグレード）

1. D-Link Web サイトから新しいファームウェアをダウンロードし、USB ドライブにコピーします。
2. USB ドライブを本ルータの USB ポートに接続します。
3. 本製品の Web GUI で、**Maintenance > Firmware & Config > Firmware Upgrade > Using USB タブ**の順にメニューをクリックし、以下の画面を表示します。

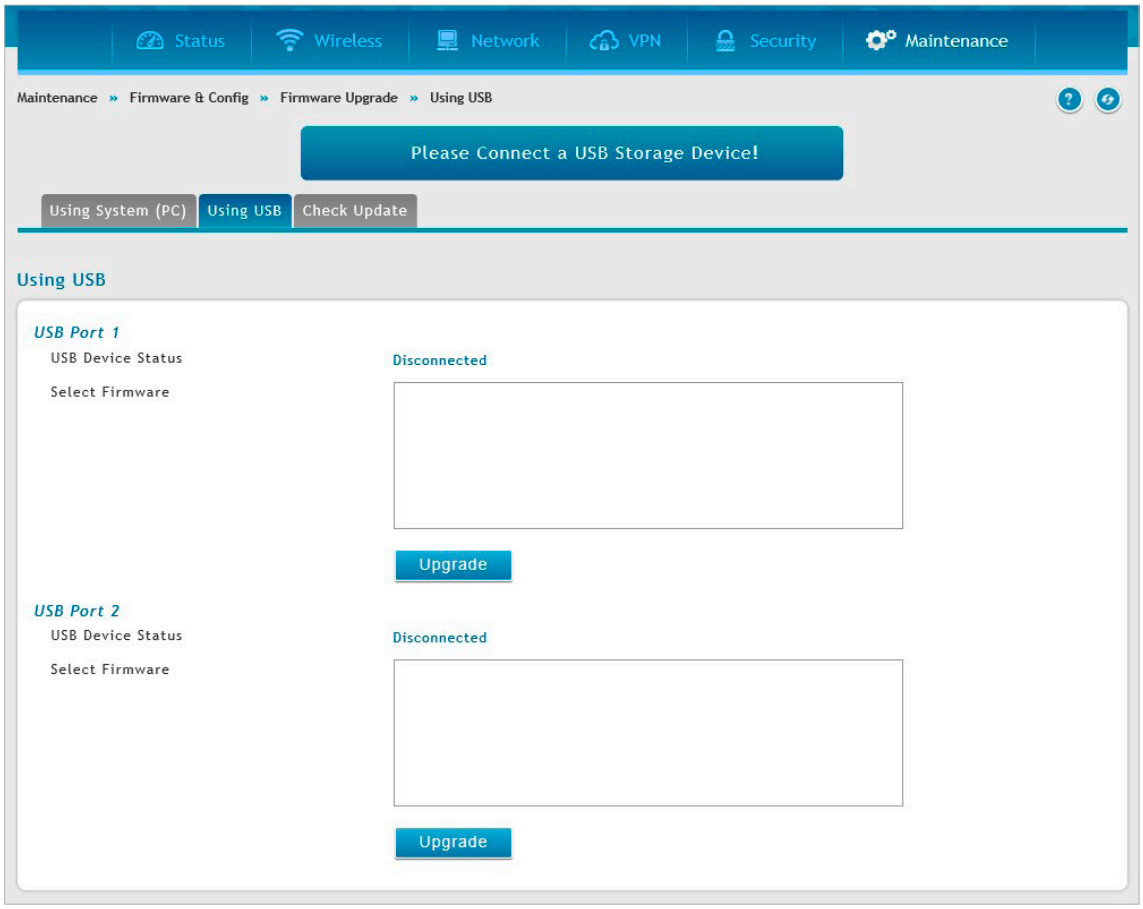

図 9-42　Firmware Upgrade > Using USB タブ画面

4. 一覧からファイルを選択し、「Upgrade」をクリックします。

注意 アップグレードのプロセスには数分かかります。アップグレードを中止したり、システムをオフにしたりしないでください。アップグレードが中断された場合、ファームウェアが破損する場合があります。ブラウザで他のサイトを参照せずに、アップグレードが完了するまでお待ちください。

Backup/Restore（コンフィグレーションのバックアップとリストア）

Maintenance > Firmware & Config > Backup/Restore メニュー
本製品の設定後、設定内容をコンフィグレーションファイルとしてバックアップする方法について説明します。何らかの理由で不具合が生じた場合、バックアップしたファイルを使用して設定を復元することができます。
また、同じモデルの別のルータにコンフィグレーションファイルをアップロードすることも可能です。

Backup（コンフィグレーションのバックアップ）

コンフィグレーションのバックアップ方法について説明します。

1. **Maintenance > Firmware & Config > Backup/Restore > Backup/Restore タブ**の順にメニューをクリックし、以下の画面を表示します。

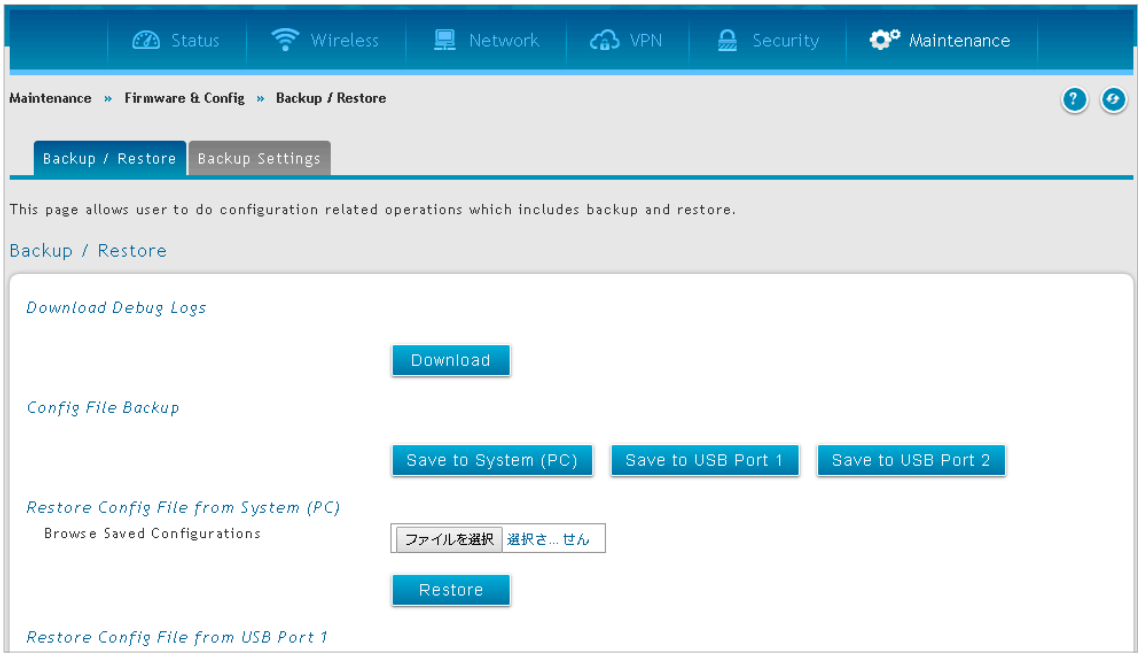

図 9-43　Backup/Restore > Backup/Restore タブ画面

2. 「Download Debug Logs」で「Download」をクリックすることにより、デバッグログをダウンロードします。
3. バックアップを保存する場所によって、「Save to System (PC)」、「Save to USB Port 1」、または「Save to USB Port 2」をクリックします。ファイル名には「.cfg」という拡張子が付加されます。

Restore（コンフィグレーションのリストア）

保存したコンフィグレーションファイルのリストア方法について説明します。リストアすることにより、設定が復元されます。

1. **Maintenance > Firmware & Config > Backup/Restore > Backup/Restore タブ**の順にメニューをクリックし、以下の画面を表示します。

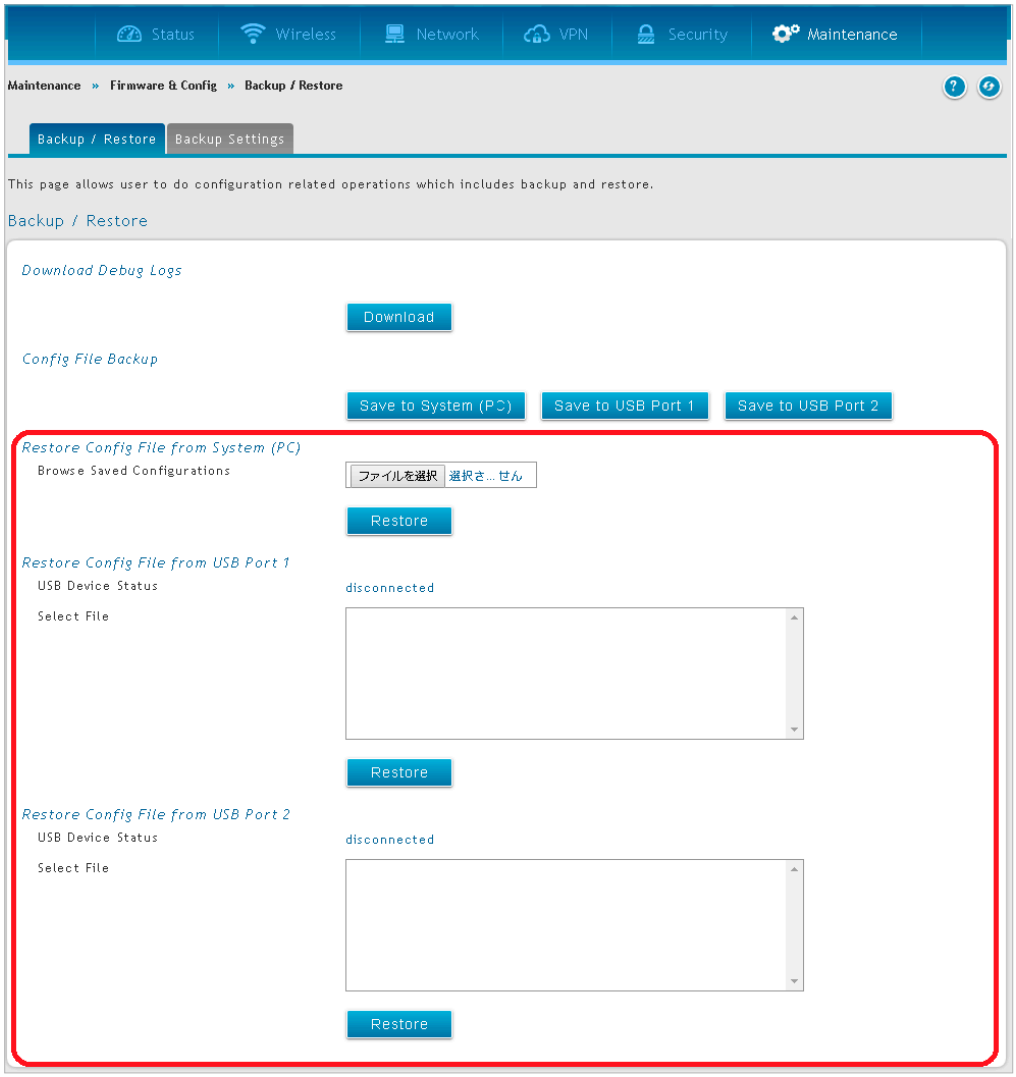

図 9-44　Backup/Restore > Backup/Restore タブ画面

2. 「Restore Config File from System (PC)」セクションで、「参照 /Browse」をクリックします。バックアップファイルを選択して、「開く（Open）」をクリック、次に「Restore」をクリックします。

3. 「Restore Config File from USB Port 1」「Restore Config File from USB Port 2」に表示される、各 USB ポートに接続した USB デバイスにあるコンフィグレーションファイルを選択、復元することも可能です。

4. 「Restore」をクリックすると、選択したファイルからコンフィグレーションを復元します。

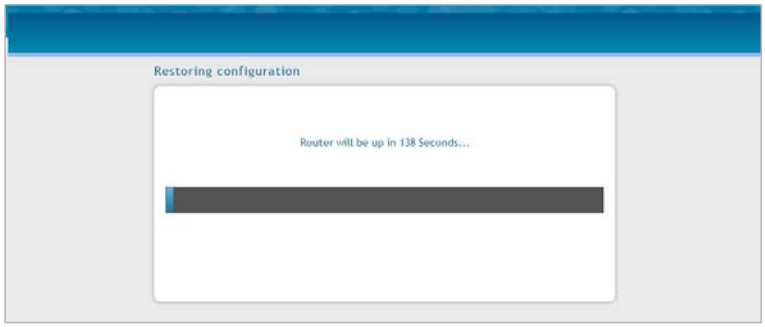

図 9-45　Restoring Configuration 画面

5. 完了するまでしばらくお待ちください。リストアが完了すると、ログイン画面が表示されます。

注意　コンフィグレーションのリストア後に「電源を切る」もしくは「再起動する」場合は、復元完了後のログイン画面が表示されてから 3 分以上経過してから実行してください。

Backup Settings（バックアップ設定）

コンフィグレーションのバックアップ方法について説明します。ルータに USB ストレージデバイスが接続されている場合、自動バックアップ（Auto-Backup）機能を使用することが可能です。現在のコンフィグレーションが USB ストレージデバイスに保存され、同様のファイル名が存在する場合は上書きされます。（以前にバックアップファイルを保存したことがある場合など）。また、コンフィグレーションファイルの暗号化も可能です。

1. **Maintenance > Firmware & Config > Backup / Restore > Backup Settings タブ**の順にメニューをクリックし、以下の画面を表示します

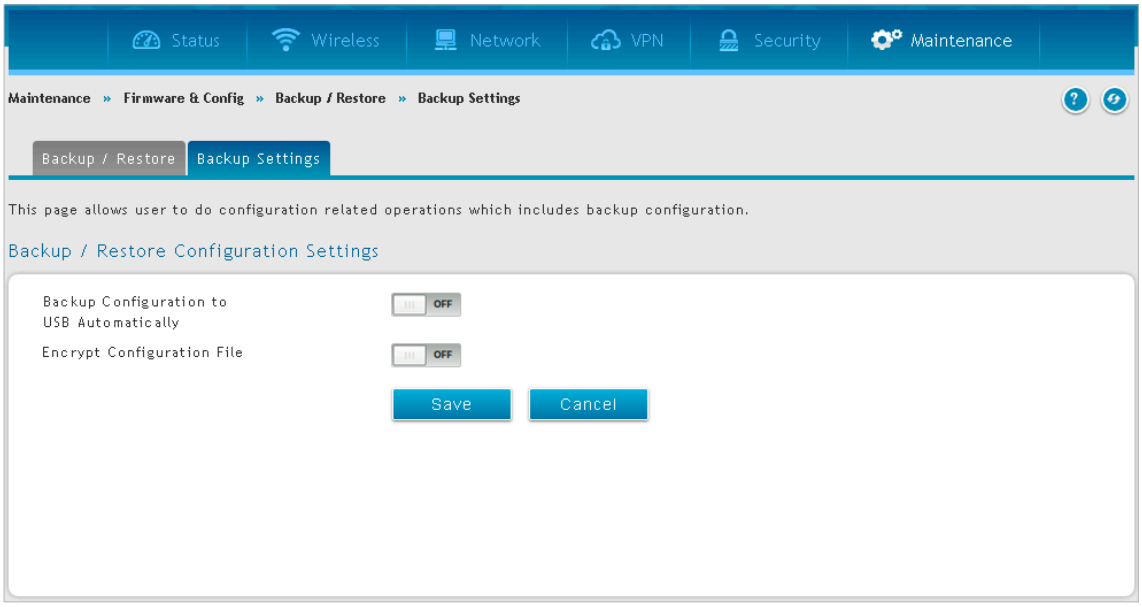

図 9-46　Backup/Restore > Backup Settings タブ

2. 「Backup Configuration to USB Automatically」を「ON」にすると自動的にコンフィグレーションが USB ストレージにファイルとして保存されます。
3. 「Encrypt Configuration File」を「ON」にするとコンフィグレーションファイルが暗号化されます。これによりシステムユーザ名 / パスワードなどの機密情報が未認証のソースなどから閲覧されることはありません。USB ドライブ及びホスト上のコンフィグバックアップファイルに適用されます。

Soft Reboot（再起動／工場出荷時設定の復元）

Maintenance > Firmware & Config > Soft Reboot メニュー

Soft Reboot（再起動）

本製品を再起動します。再起動は、電源の切断と投入を実行しますが、初期状態から変更した設定については保持します。

1. **Maintenance > Firmware & Config > Soft Reboot** の順にメニューをクリックし、以下の画面を表示します。

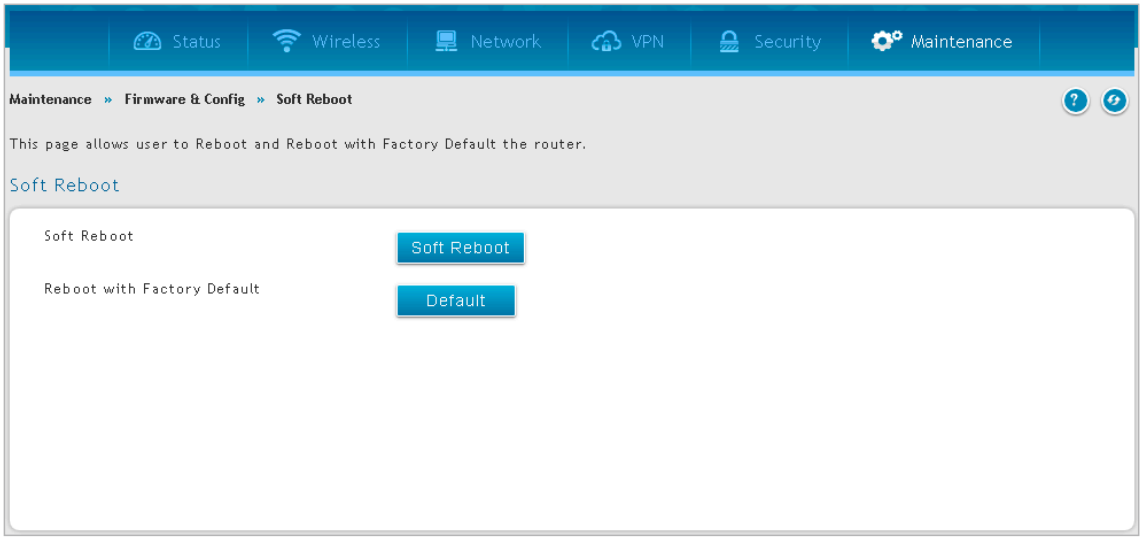

図 9-47　Soft Reboot 画面

2. 「Soft Reboot」の「Soft Reboot」をクリックして、ルータを再起動します。「Cancel」をクリックすると、再起動はキャンセルされます。

Reset to Factory Default Settings（工場出荷時設定へのリセット）

本製品を工場出荷時設定にリセットする方法について説明します。
工場出荷時設定にリセットすると、すべての設定が購入時の状態に戻ります。ログインパスワード、SSID、IP アドレスや無線セキュリティキーなど、インターネット接続を行うために必要とされる重要な項目もすべてリセットされます。

1. **Maintenance > Firmware & Config > Soft Reboot** の順にメニューをクリックし、以下の画面を表示します。

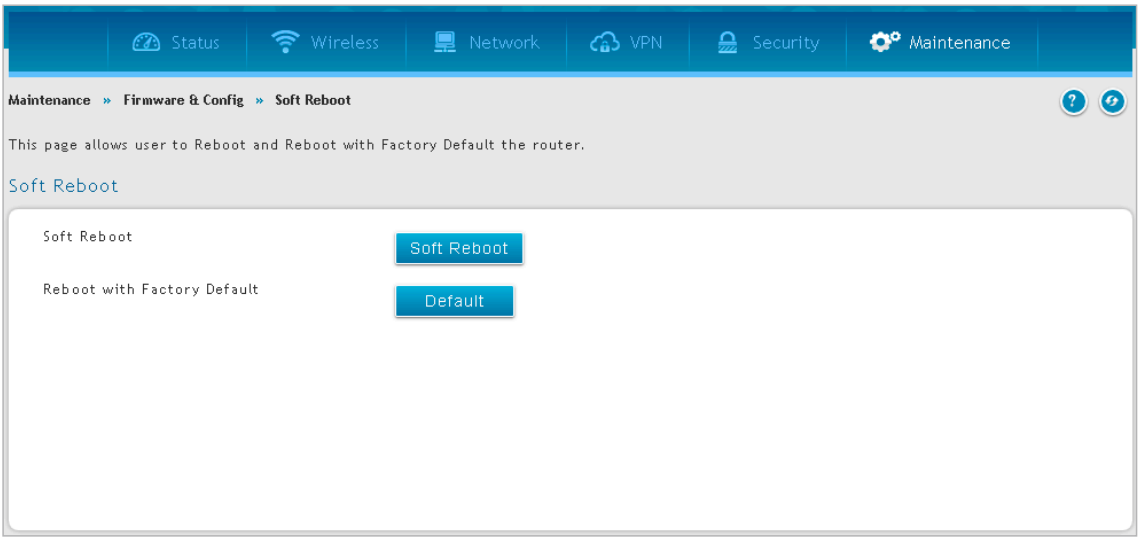

図 9-48　Soft Reboot 画面

2. 「Reboot with Factory Default」の「Default」をクリックすると、工場出荷時の設定で再起動します。

本製品の工場出荷時の IP アドレス、ログインユーザ名、パスワードは以下の通りです。
　IP アドレス：192.168.10.1　／　ログインユーザ名：admin　／　パスワード：admin

Logs Settings（ログ設定）

Maintenance > Logs Settings メニュー
本ルータでは、ログメッセージを取得することができます。ルータを追加するトラフィックの種類をモニタして、潜在的な攻撃やエラーの検出時に通知を受け取ることができます。以下のセクションはログ構成設定とこれらのログにアクセスする方法を説明しています。

Log Facilities（ログファシリティ）

Maintenance > Logs Settings > Log Facilities メニュー
ファシリティは、ログの種類を意味します。
「Facilities」でログの種類を選択し、「Configuration Options」でログを取得するイベントのセベリティを選択します。

1. **Maintenance > Logs Settings > Log Facilities** の順にメニューをクリックし、以下の画面を表示します。

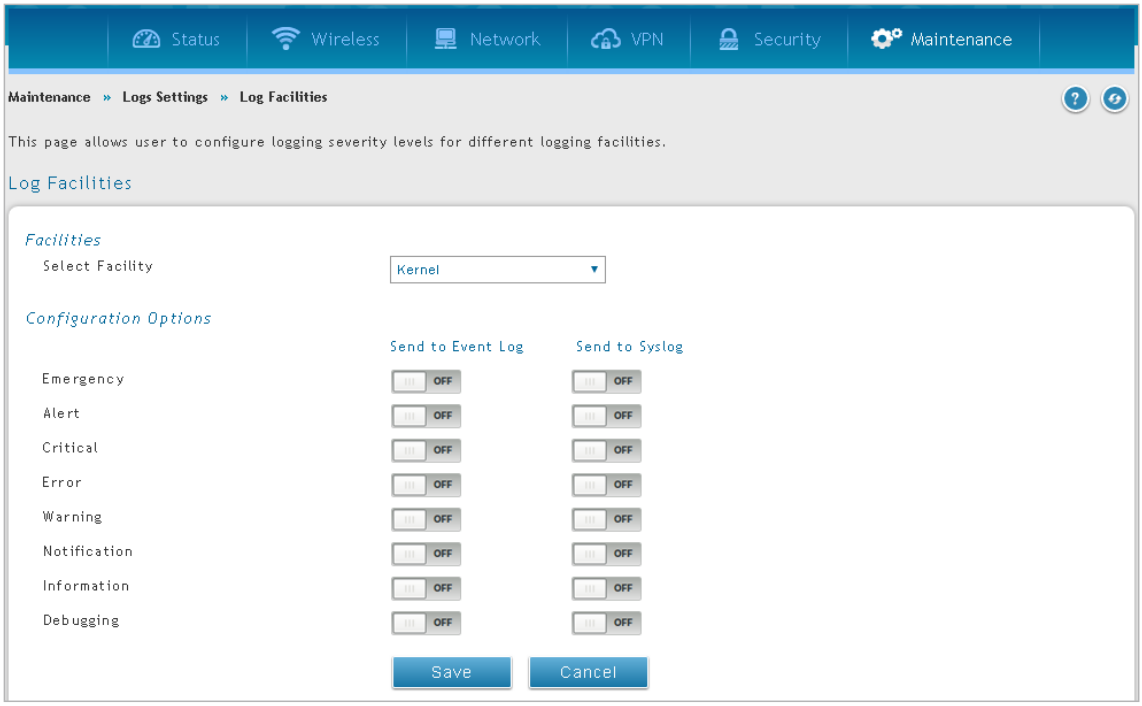

図 9-49　Log Facilities 画面

2. 「Facility」セクションでログの種類を選択→「Configuration Options」セクションでログを取得するイベントのセベリティを選択します。

項目	説明
Facilities	
Select Facility	ログの種類を以下から選択します。 • 「Kernel」：カーネル関連のログです。 • 「System 」：アプリケーションまたは管理レベルの機能、またはユニット管理に関する管理者による変更に対応するログです。 • 「Wireless」：無線（AP）関連の設定と動作に関するログです。 • 「Network 」：ネットワーク関連のログです。 • 「VPN」：「sslvpn」「openvpn」「ipsec」など VPN 関連のログです。 • 「Firewall」：ファイアウォール関連のログです。
Configuration Options	
ログの送信方法を以下から選択します。 • 「Send to Event Log」：設定した以上のセベリティのイベントが発生した場合、イベントがキャプチャされデバイスに保存されます。 • 「Send to Syslog」：設定した以上のセベリティのイベントが発生した場合、イベントがキャプチャされ Syslog サーバに転送されます。	
Emergency	システムは使用不能
Alert	すぐになんらかの対処が必要
Critical	クリティカルな状態
Error	エラー状態
Warning	警告状態
Notification	正常だが注意を要する状態
Information	情報メッセージ
Debugging	デバッグッセージ

3. 「Save」をクリックし、設定を適用します。

特定のセベリティレベルが選択された場合、それと同等以上のセベリティを持つすべてのイベントがキャプチャされます。例えば、「Wireless」ファシリティに対し「CRITICAL」レベルのログを設定した場合、CRITICAL、ALERT、EMERGENCY レベルの 802.11 のログが出力されます。

Web 内のイベントログビューア（**Status > System Information > All Logs > Current Logs** 画面）、またはリモート Syslog サーバのどちらでログを閲覧するかによって、ログ表示をカスタマイズすることができます。以降のセクションで説明するメールログは、Syslog サーバに設定されたログと同じ設定が適用されます。

Routing Logs（ルーティングログ）

Maintenance > Logs Settings > Routing Logs メニュー

ファイアウォールがパケットを受け付けたか、または破棄したかによってトラフィックを追跡することができます。
DoS（Denial of Service）攻撃、一般的な攻撃情報、ログインの試み、破棄されたパケットなどのイベントを、閲覧・確認することができます。

注意　ログオプションを有効にすると、大量のログメッセージを生成する可能性があるため、デバッグ目的だけに使用することをお勧めします。

各ネットワークセグメント（LAN、WAN、DMZ）を通過するトラフィックは、ファイアウォールによるパケットの許可 / 破棄の処理に基づいて追跡することができます。Accepted Packets（許可パケット）は各ネットワークセグメントにおいて送信成功を意味します。本オプションは特に「Default Outbound Policy」が「Always Block」（常にブロック）の時に有効で、ファイアウォールを通過するトラフィックをモニタすることができます。
Dropped Packet（破棄パケット) は、各ネットワークセグメントにおいて送信がブロックされたことを意味します。本オプションは特に「Default Outbound Policy」が「Always Allow」（常に許可）の時に有効で、ファイアウォールを通過するトラフィックをモニタすることができます。

IPv4

1. **Maintenance > Logs Settings > Routing Logs > IPv4 タブ**の順にメニューをクリックし、以下の画面を表示します。

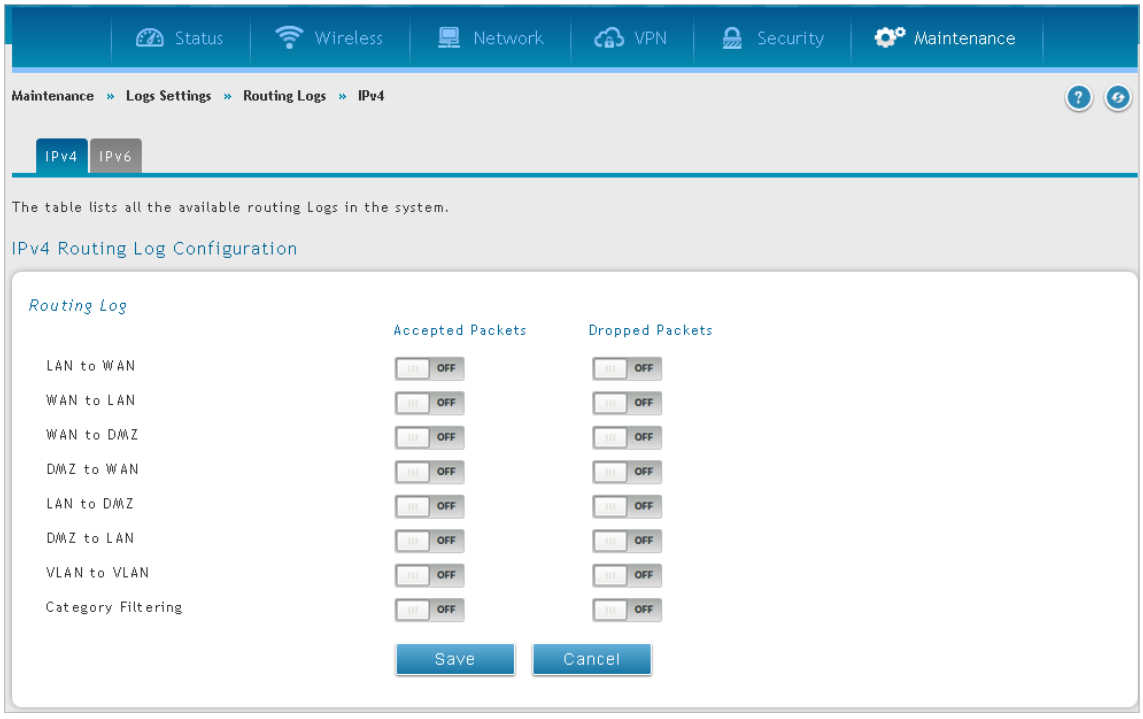

図 9-50　Routing Logs > IPv4 タブ画面

2. 「Accepted Packets 」または「Dropped Packets 」について、以下のイベントの「ON」「OFF」を選択します。
「LAN to WAN」　「DMZ to WAN」　「VLAN to VLAN」
「WAN to LAN」　「LAN to DMZ」　「Category Filtering」
「WAN to DMZ」　「DMZ to LAN」

- **Accepted Packets**
セグメント間で正常に転送されたパケットをログ出力します。
「Default Outbound Policy」が「Always Block」（常にブロック）の時に役に立ちます。
- **Dropped Packets**
セグメント間でブロックされたパケットをログ出力します。
「Default Outbound Policy」が「Always Allow」（常に許可）の時に役に立ちます。

3. 「Save」をクリックし、設定を適用します。

「Cancel」をクリックした場合は、変更前の設定に戻ります。

IPv6

1. **Maintenance > Logs Settings > Routing Logs > IPv6 タブ**の順にメニューをクリックし、以下の画面を表示します。

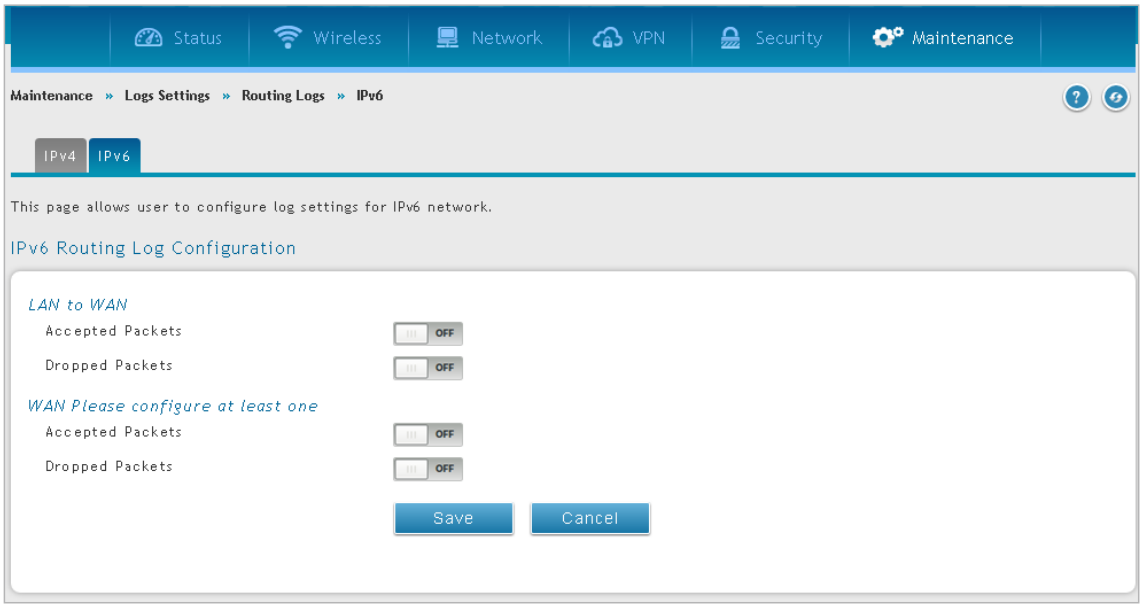

図 9-51　Routing Logs > IPv6 タブ画面

2. 「LAN to WAN」セクションで、「Accepted Packets 」「Dropped Packets 」を「ON」または「OFF」にします。
3. 「WAN（Please configure at least one）」セクションで、「Accepted Packets 」「Dropped Packets 」を「ON」または「OFF」にします。
   - **Accepted Packets**
     セグメント間で正常に転送されたパケットをログ出力します。
     「Default Outbound Policy」が「Always Block」（常にブロック）の時に役に立ちます。
   - **Dropped Packets**
     セグメント間でブロックされたパケットをログ出力します。
     「Default Outbound Policy」が「Always Allow」（常に許可）の時に役に立ちます。
4. 「Save」をクリックし、設定を適用します。

「Cancel」をクリックした場合は、変更前の設定に戻ります。

Sytem Log（System ログ）

Maintenance > Logs Settings > System Logs メニュー

ネットワークセグメントのログの他に、ユニキャストとマルチキャストトラフィックのログを出力することができます。
ユニキャストパケットはネットワーク上に単一の宛先を持っており、一方で、ブロードキャスト（またはマルチキャスト）パケットは、到達可能なすべての宛先に同時に送信されます。もう 1 つの有用なログの設定として、設定済みの帯域プロファイルによって特定のインタフェース上で破棄されたパケットをログ出力することもできます。これらのデータを元に、LAN ユーザにとって望ましいインターネットトラフィックになるように、帯域プロファイルの変更する必要があるかどうか検討することができます。

1. **Maintenance > Logs Settings > System Logs** の順にメニューをクリックし、以下の画面を表示します。

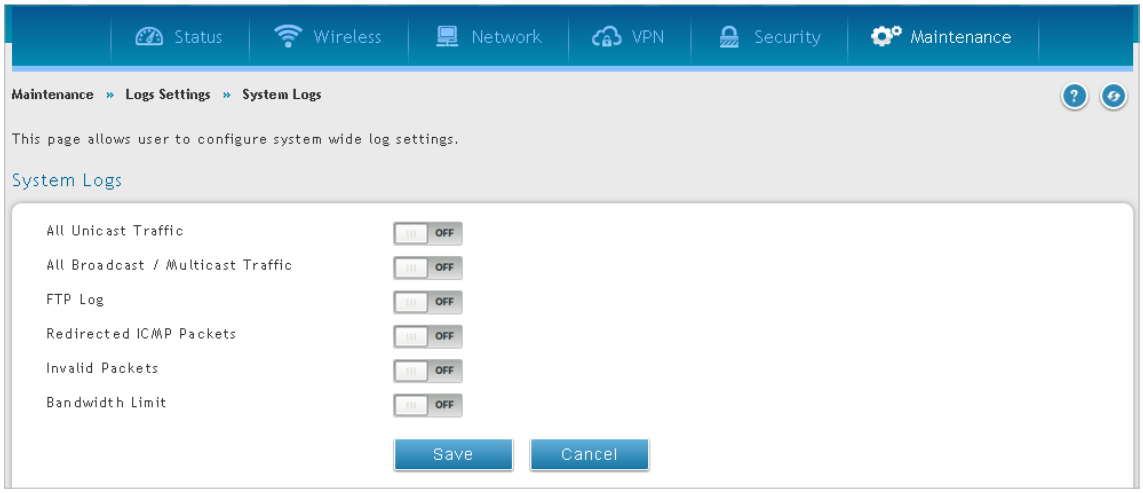

図 9-52　System Logs 画面

2. 以下の項目を設定します。

項目	説明
All Unicast Traffic	有効にするとルータに向けたパケットを追跡します。
All Broadcast / Multicast Traffic	有効にするとルータに向けたすべてのブロードキャストまたはマルチキャストパケットを追跡します。
FTP Log	有効にするとログ情報を FTP ログに送信します。
Redirected ICMP Packets	有効にするとリダイレクトされた ICMP（Internet Control Message Protocol）パケット数を追跡します。
Invalid Packets	有効にすると受信した無効なパケット数を追跡します。
Bandwidth Limit	有効にすると帯域制限に関連した無線クライアントの情報をログに出力します。

3. 「Save」をクリックし、設定を適用します。

Remote Logging（リモートログ）

Maintenance > Logs Settings > Remote Logging メニュー

ルータが収集するログの種類を設定後、Syslog または E-Mail アドレスにログを送信するように設定できます。
リモートログにおけるキーコンフィグレーションフィールドは、Remote Log Identifier です。各ログメッセージには設定された Remote Log Identifier のプレフィックスが含まれているため、1 台以上のルータからログを受信したシスログサーバやメールサーバは関連デバイスのログをソートすることが可能です。

メールログに対してオプションを有効にした後、SMTP サーバの E メールアドレス（IP アドレスまたは FQDN）を入力します。メールを設定したアドレスに送信する場合、ルータはこのサーバに接続します。ルータがログをパッケージ化して “send-to” アドレスの 1 つで受信される E メールを送信するために、SMTP ポートと返信メールアドレスが必要となります。ログ受信者として最大 3 つのメールアドレスを設定できます。

設定された SMTP ポートとサーバで通信を確立するために、サーバの認証要求を定義します。ルータは、SMTP サーバに送信されるユーザ名とパスワードデータに使用される「LoginPlain」（暗号化しない）または「CRAM-MD5」（暗号化）をサポートしています。サーバ側で認証が不要な場合、認証を「None」（無効）にすることもできます。SMTP サーバは IDENT 要求を送信することがありますが、本ルータでは、必要に応じてこの応答オプションを有効にすることができます。

メールサーバと受信者の詳細が定義されると、ルータによるログの送信タイミングを決定することができます。ログを送信する際のユニット（頻度など）を選択し、そこで指定した定義済みスケジュールに従って E メールログが送信されます。「Never」を選択した場合、E メールログが無効化されますが、メールサーバの設定は保存されます。

Email

1. **Maintenance > Logs Settings > Remote Logging > Email タブ**の順にメニューをクリックし、以下の画面を表示します。

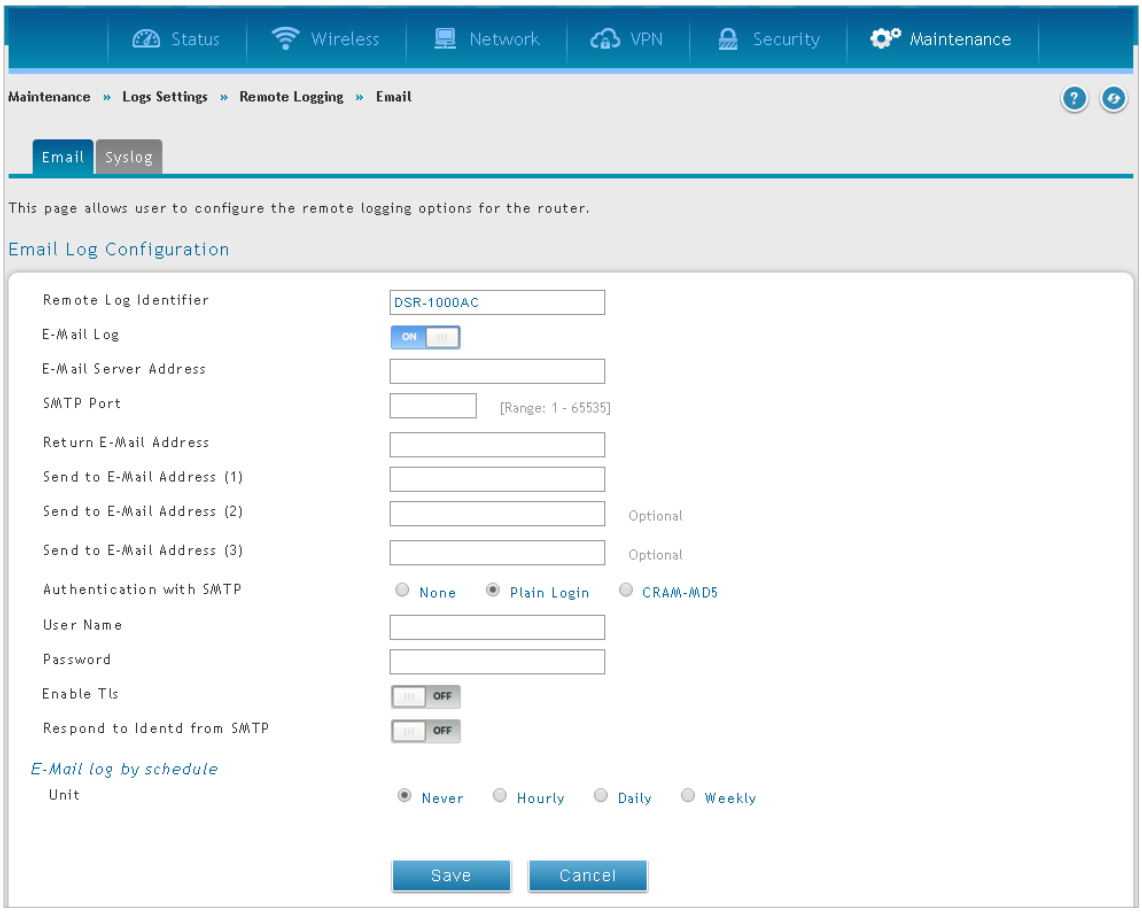

図 9-53　Remote Logging > Email タブ画面

2. 以下の項目を設定します。

項目	説明
Remote Log Identifier	メッセージの送信元を識別するのに使用されるプレフィックスを入力します。この識別子はメールと Syslog メッセージ両方の先頭に付けられています。
E-Mail Log	メールログを有効、または無効にします。 • 「ON 」：E メールログを有効にします。有効にした場合、以降の項目を設定します。 • 「OFF 」：E メールログを無効にします。
E-Mail Server Address	「E-Mail Log」を「ON」にした場合、SMTP（Simple Mail Transfer Protocol）サーバの IP アドレスまたはネットワークアドレスを入力します。要求があった場合に、ルータはこのサーバに接続してメールログを送信します。SNMP サーバで E メール通知が受信可能に設定されている必要があります。
SMTP Port	「E-Mail Log」を「ON」にした場合、メールサーバの SMTP ポートを入力します。
Return E-Mail Address	「E-Mail Log」を「ON」にした場合、SMTP サーバからの応答が送信されるメールアドレスを入力します。（失敗メッセージ送信時に必要）
Send to E-mail Address (1-3)	「E-Mail Log」を「ON」にした場合、ログ、警告が送信されるメールアドレスを最大 3 つまで入力します。
Authentication with SMTP	「E-Mail Log」を「ON」にした場合、接続を受け入れる前に SMTP サーバ側で認証を必要とする場合、認証の種類を選択します。 • 「None」：認証は使用されません。「User Name」および「Password」フィールドは利用できません。 • 「Login Plain」：非暗号化の通信セッション上で Base64 によりコード化されたパスワードを使用してログインするのに使用される認証。Base64 でコード化されたパスワードでは暗号の保護を提供しないため、攻撃の被害を受けやすくなります。 • 「CRAM-MD5」：HMAC-MD5 MAC アルゴリズムに基づき RFC 2195 で定義されたチャレンジレスポンス認証メカニズム。「CRAM-MD5」は、「Login Plain」よりも高いレベルの認証を提供します。
User Name	「Authentication with SMTP」で「Login Plain」または「CRAM-MD5」を設定した場合、認証に使用するユーザ名を入力します。
Password	「Authentication with SMTP」で「Login Plain」または「CRAM-MD5」を設定した場合、認証に使用するパスワード（大文字、小文字の区別あり）を入力します。
Enable Tls	「Authentication with SMTP」で「Plain Login」または「CRAM-MD5」を選択した場合、TLS を有効にすることが可能です。
Respond to Identd from SMTP	「E-Mail Log」を有効にした場合、ルータが SMTP サーバからの IDENT 要求に応答するかどうかを指定します。 • 「ON 」：ルータは SMTP サーバからの IDENT 要求に応答します。 • 「OFF 」：ルータは SMTP サーバからの IDENT 要求を無視します。
E-Mail log by schedule	
スケジュールに基づいてメールログを受信するためには、スケジュール設定を行います。	
Unit	ログを送信する間隔を選択します。ログの定期送信を無効化した場合でも、**Status > System Information > All Logs > Current Logs** 画面で「Send Log」をクリックし、ログを送信することができます。 • 「Never」：ログの送信を無効にします。 • 「Hourly」：1 時間ごとにログを送信します。 • 「Daily」：毎日指定した時間にログを送信します。 • 「Weekly」：毎週指定した曜日と時間にログを送信します。
Day	「Unit」を「Weekly」に設定した場合、ログを送信する曜日を選択します。
Time	「Unit」を「Daily」または「Weekly」に設定した場合、ログを送信する時間を選択します。

3. 「Save」をクリックし、設定を適用します。

Syslog

ルータからログを収集して保存する場合、一般的に Syslog サーバが使用されます。そのようなリモートデバイスでは、通常、ルータのローカルメモリよりも容量制限の影響が少なくなっています。多くのログを収集することができるため、長期間に渡ってネットワーク問題のデバッグを実施したり、ルータトラフィックをモニターする際に役に立ちます。

本画面の設定を使用して、各サーバに対してセベリティの異なる様々なログファシリティメッセージを受信するように設定することができます。ログの定義については、「Log Facilities（ログファシリティ）」を参照してください。

1. **Maintenance > Logs Settings > Remote Logging > Syslog タブ**の順にメニューをクリックし、以下の画面を表示します。

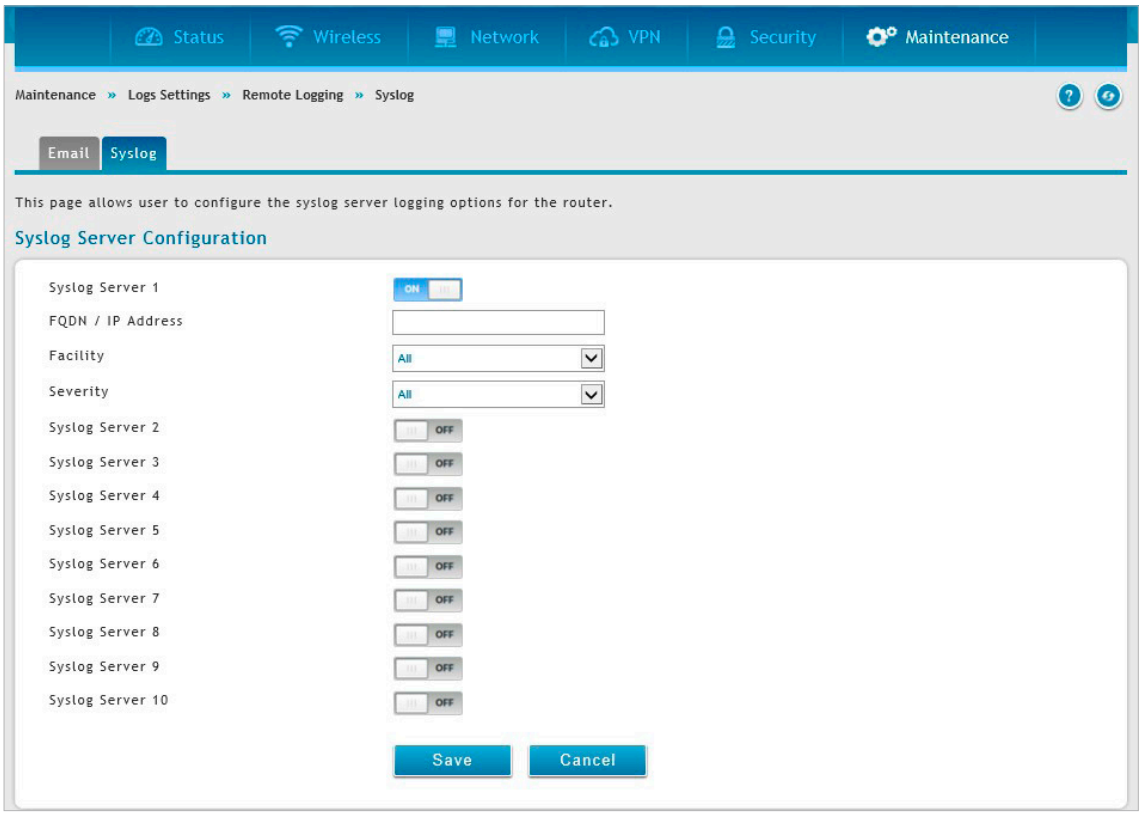

図 9-54　Remote Logging > Syslog タブ画面

2. 以下の項目を設定します。

項目	説明
Syslog Server	Syslog サーバを「ON」または「OFF」に設定します。 サポートしている Syslog サーバの数は製品によって異なります。 • DSR-1000/1000AC：10 • DSR-500：7
FQDN/IP Address	Syslog サーバのインターネット名 /IP アドレスを指定します。
Facility	ログ出力のファシリティ（「All」「Kernel」「System」「Network」「VPN」「Firewall」）を選択します。
Severity	ログ出力のセベリティを選択します。 • 「Log Debug」 • 「Log Info」 • 「Log Notice」 • 「Log Warning」 • 「Log Error」 • 「Log Critical」 • 「Log Alert」 • 「Log Emerg」

3. 「Save」をクリックし、設定を適用します。

SMS Logging（SMS ログ（未サポート））

Maintenance > Logs Settings > SMS Logging メニュー

「WAN」「VPN」「CPU/Memory」に関するログ情報を指定の携帯端末番号へ SMS で送信します。

注意　本機能は未サポートです。

1. **Maintenance > Logs Settings > SMS Logging** の順にメニューをクリックし、以下の画面を表示します。

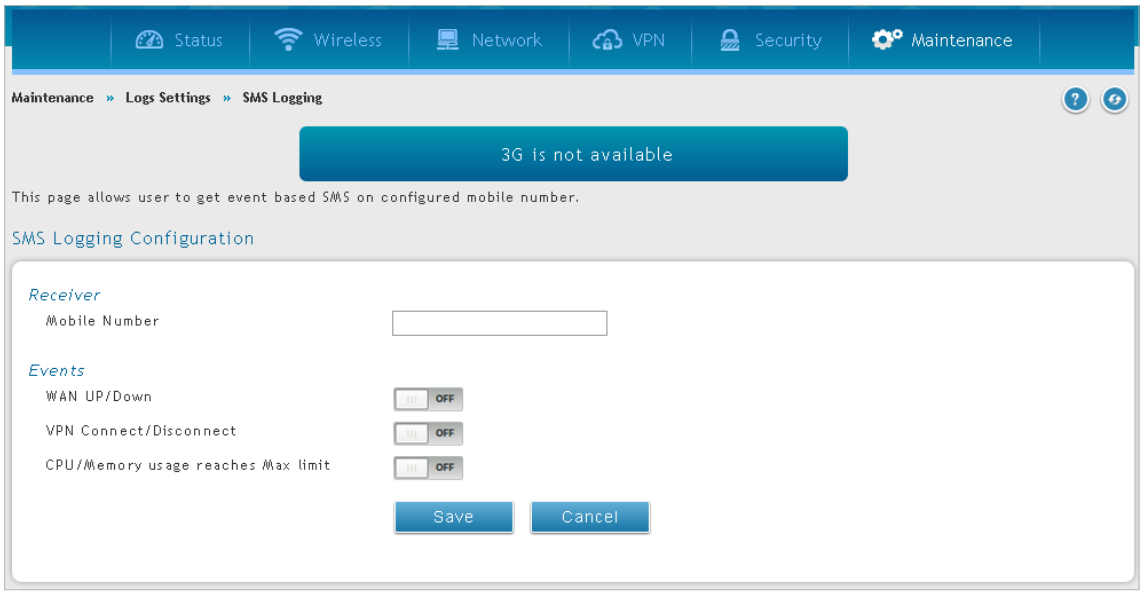

図 9-55　SMS Logging 画面

2. 以下の項目を設定します。

項目	説明
Mobile Number	ログを送信する SMS の携帯端末番号を入力します。
WAN UP/Down	WAN の有効 / 無効に関するログについて SMS 送信を行います。
VPN Connect/Disconnect	VPN の接続 / 切断に関するログについて SMS 送信を行います。
CPU/Memory usage reaches Max limit	CPU 使用率が 50%、Memory 使用率が 80% に到達したときに SMS 送信を行います。

3. 「Save」をクリックし、設定を適用します。

第 10 章　ステータス情報（Status）

本製品のステータス情報と統計情報を表示する、以下のページについて説明します。

メニュー	説明
「Dashboard（ダッシュボード画面）」	ルータは、システムが使用しているリソースについて表示するダッシュボードを提供します。
「System Information（システム状態の参照）」	ルータのシステム情報について参照します。
「Network Information（ネットワーク情報の参照）」	ルータのネットワーク情報について参照します。

Dashboard（ダッシュボード画面）

Status > Dashboard メニュー

ダッシュボード画面では、WAN ポートや VPN の使用状況やトラフィックの量など、本製品のリソースを確認できます。
各項目にある「Detail」をクリックすると、より詳細な情報が表示されます。

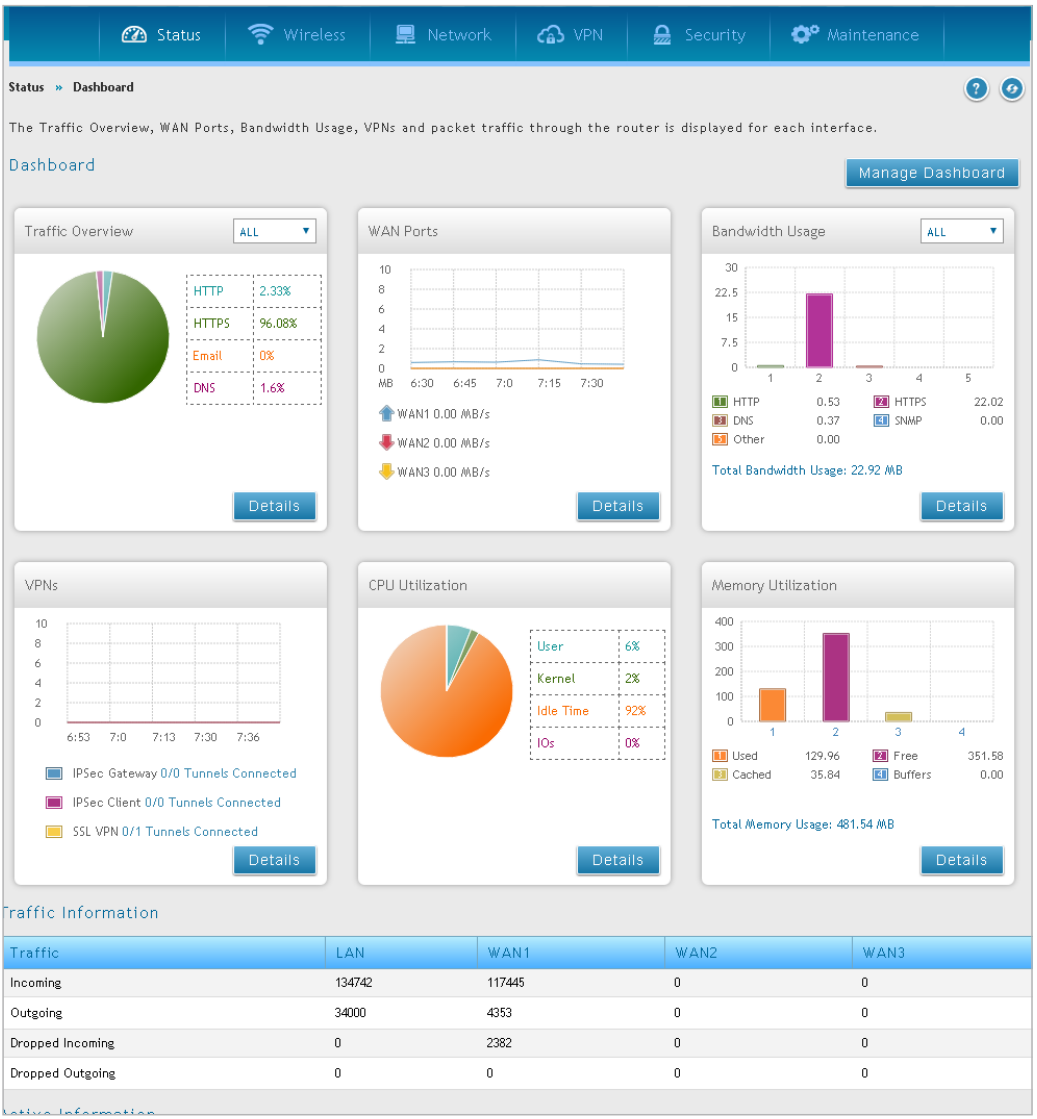

図 10-1　Dashboard 画面

項目	説明
Traffic Overview	各インタフェースのサービス毎のトラフィック概要についてグラフを表示します。
WAN Ports	WAN トラフィックのパケット情報や帯域についてグラフを表示します。
Bandwidth Usage	「WLAN」や「LAN」などのネットワークセグメントに使用された帯域の使用率を表示します。データは「HTTP」「HTTPS」「DNS」「SNMP」などのアプリケーションサービス毎に表示されます。
VPNs	帯域やトンネル数など VPN トラフィックについてのチャートを表示します。
Memory Utilization	メモリの使用率について表示します。
CPU Utilization	CPU の使用率について表示します。
Traffic Information	各インタフェースのトラフィック統計を表示します。
Active Information	受信 ICMP パケット数、利用可能な VLAN、アクティブなインタフェースの情報を表示します。

■ ダッシュボードの管理

ダッシュボードに表示する項目を選択できます。

1. 「Manage Dashboard」をクリックします。

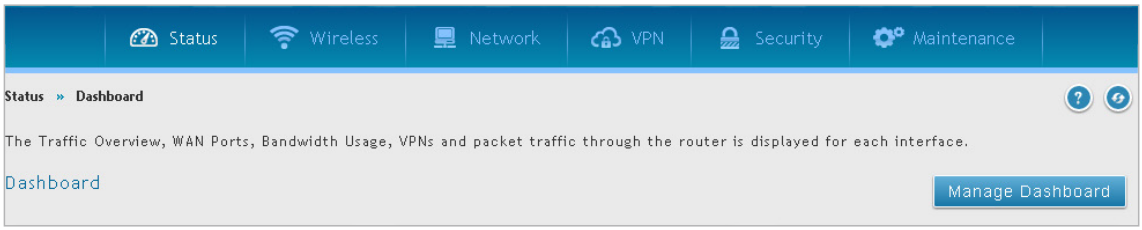

図 10-2　Dashboard 画面

2. 以下の画面で、各項目の「ON」「OFF」を選択します。

図 10-3　Managed Dashboard 画面

3. 「ON」にした項目がダッシュボード画面に表示されます。
4. 「Save」をクリックし、設定を適用します。

System Information（システム状態の参照）

Status > System Information メニュー

Device（デバイス状態の参照）

Status > System Information > Device メニュー
本製品の状態について表示します。

System（システム）

本製品のシステムや LAN、WAN などの状態を確認できます。

1. **Status > System Information > Device > System タブ**の順にメニューをクリックし、以下の画面を表示します。

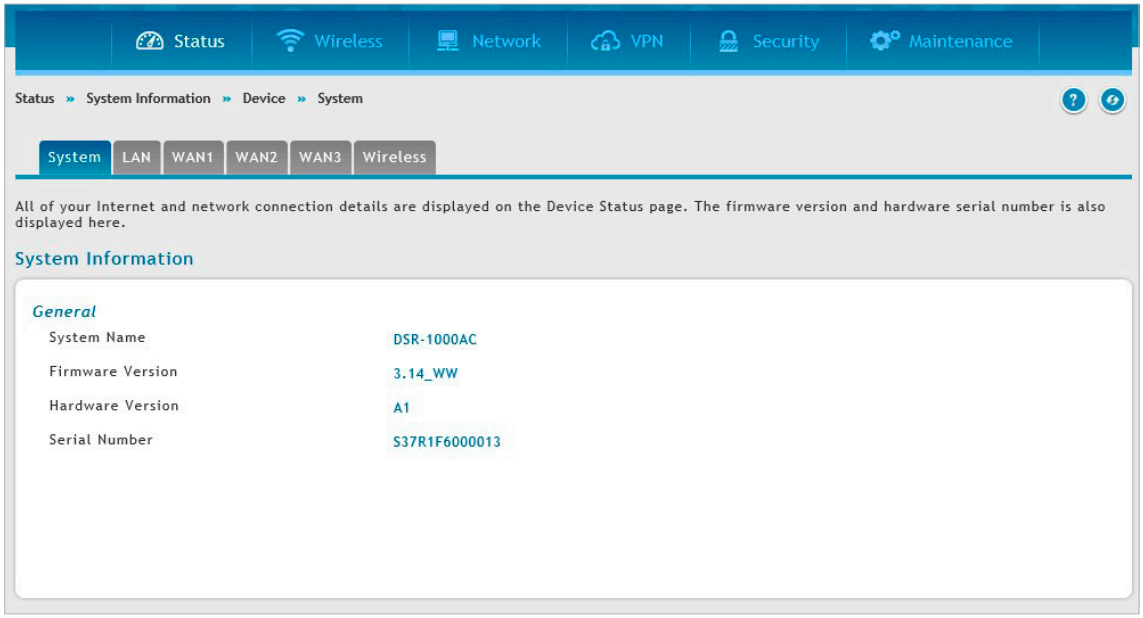

図 10-4　System > System タブ画面

項目	説明
General	
System Name	ルータ名が表示されます。
Firmware Version	現在使用しているファームウェアのバージョンが表示されます。
Hardware Version	ハードウェアバージョンが表示されます。
Serial Number	シリアル番号が表示されます。

LAN

本製品の MAC アドレス、IP アドレスやリンクステータスなど LAN 状態について表示します。

1. **Status > System Information > Device > LAN タブ**の順にメニューをクリックし、以下の画面を表示します。

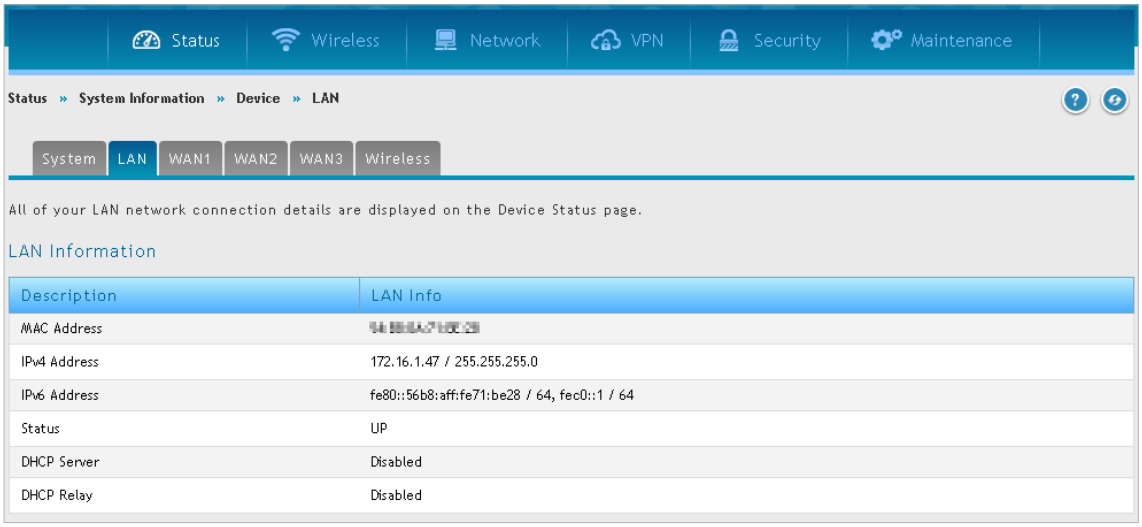

図 10-5　Device > LAN タブ画面

WAN1

本製品の WAN1 ポートの状態について表示します。

1. **Status > System Information > Device > WAN1 タブ**の順にメニューをクリックし、以下の画面を表示します。

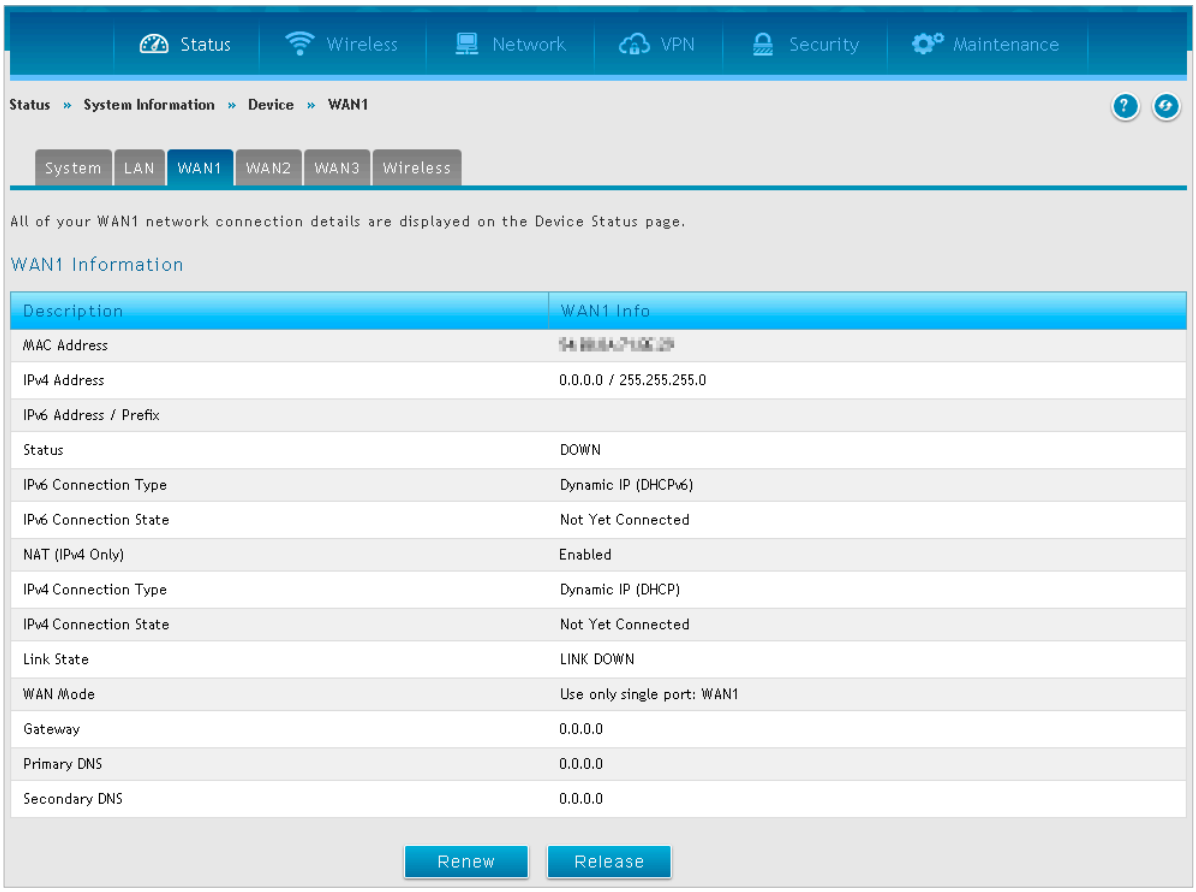

図 10-6　Device > WAN1 タブ画面

「Renew」：表示情報を更新します。
「Release」：インターネット接続設定の更新を行います。

WAN2

本製品の WAN2 ポートの状態について表示します。

1. **Status > System Information > Device > WAN2 タブ**の順にメニューをクリックし、以下の画面を表示します。

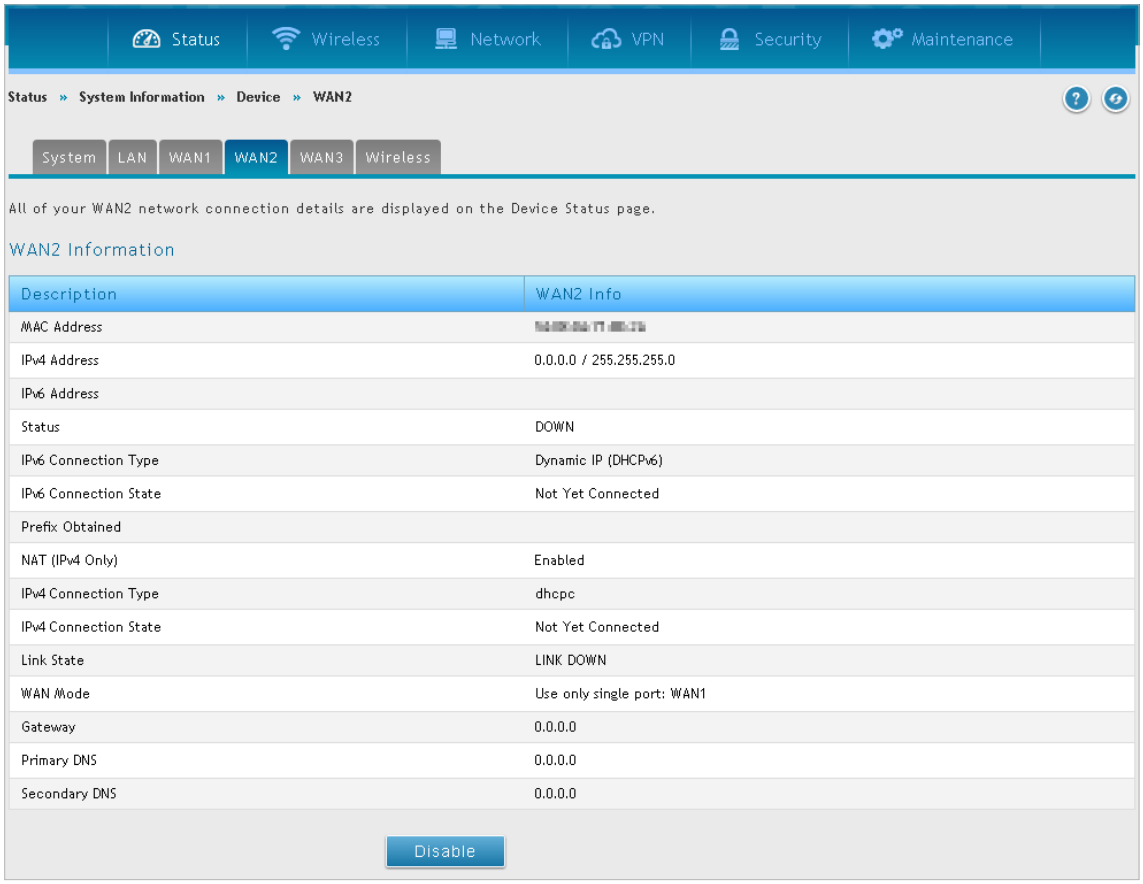

図 10-7　Device > WAN2 タブ画面

「Disable」：WAN2 ポートを無効にします。

WAN3

本製品の WAN3 ポートの状態について表示します。

1. **Status > System Information > Device > WAN3 タブ**の順にメニューをクリックし、以下の画面を表示します。

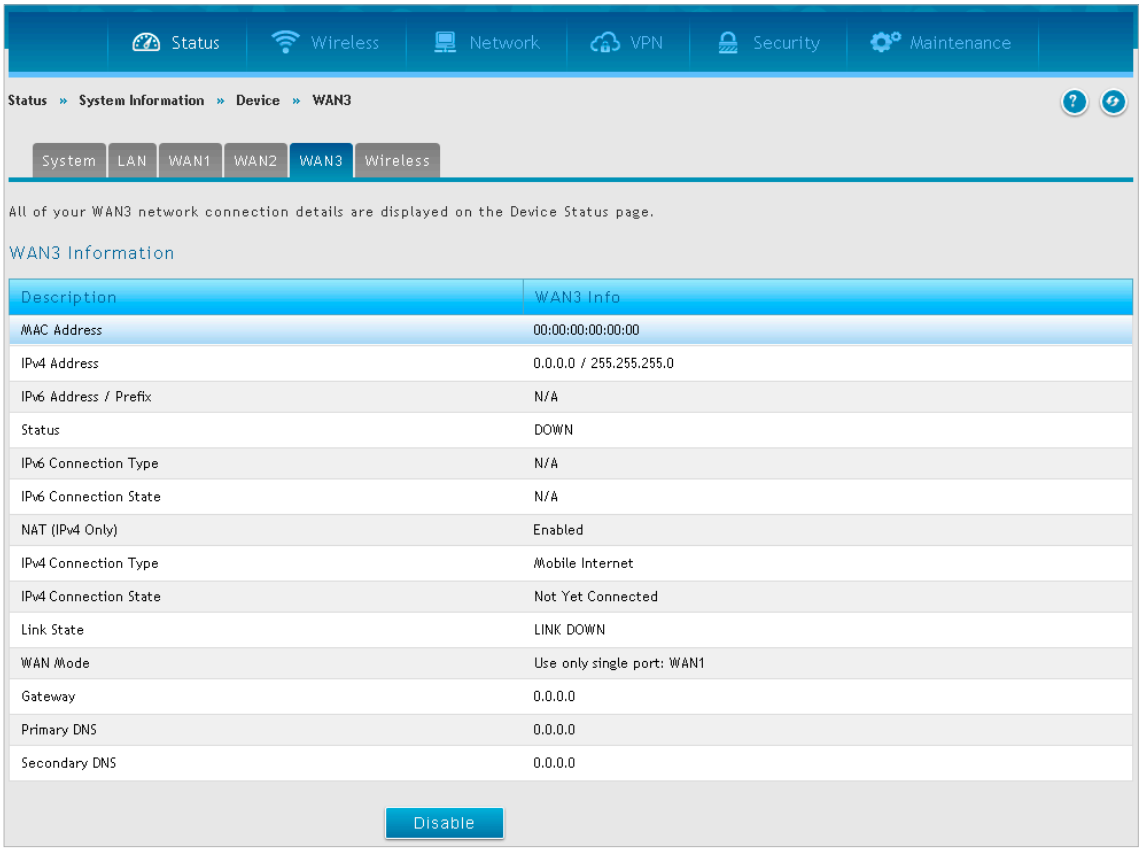

図 10-8　Device > WAN3 タブ画面

「Disable」：WAN3 ポートを無効にします。

Wireless（無線ネットワーク）

本製品の無線ネットワーク設定について表示します。

1. **Status > System Information > Device > Wireless タブ**の順にメニューをクリックし、以下の画面を表示します。

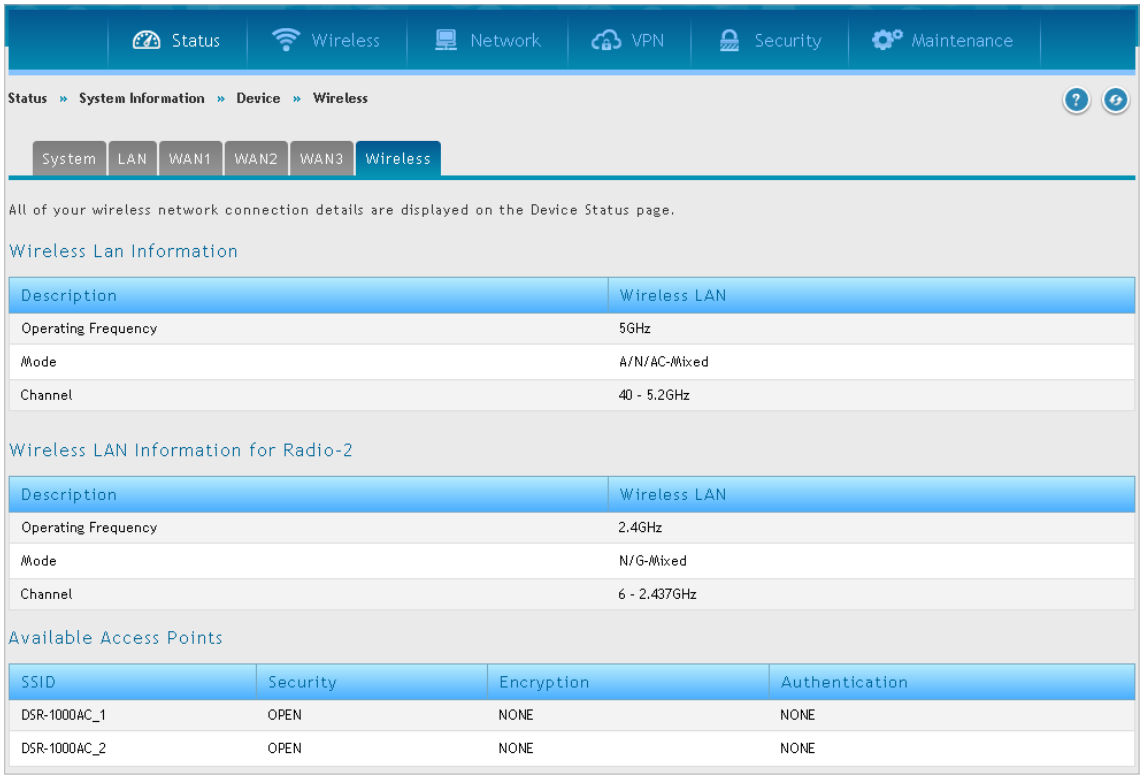

図 10-9　Device > Wireless タブ画面

All Logs（ログ）

Status > System Information > All Logs メニュー

ルータで設定したログメッセージを表示します。各ログは、ルータの設定時刻に従って定められたタイムスタンプと共に表示されます。Syslog サーバやメールログ出力などのリモートログ出力が設定されると、ここに表示されるだけでなく、同じログをリモートインタフェースにも送信します。

1. **Status > System Information > All Logs** の順にメニューをクリックし、以下の画面を表示します。

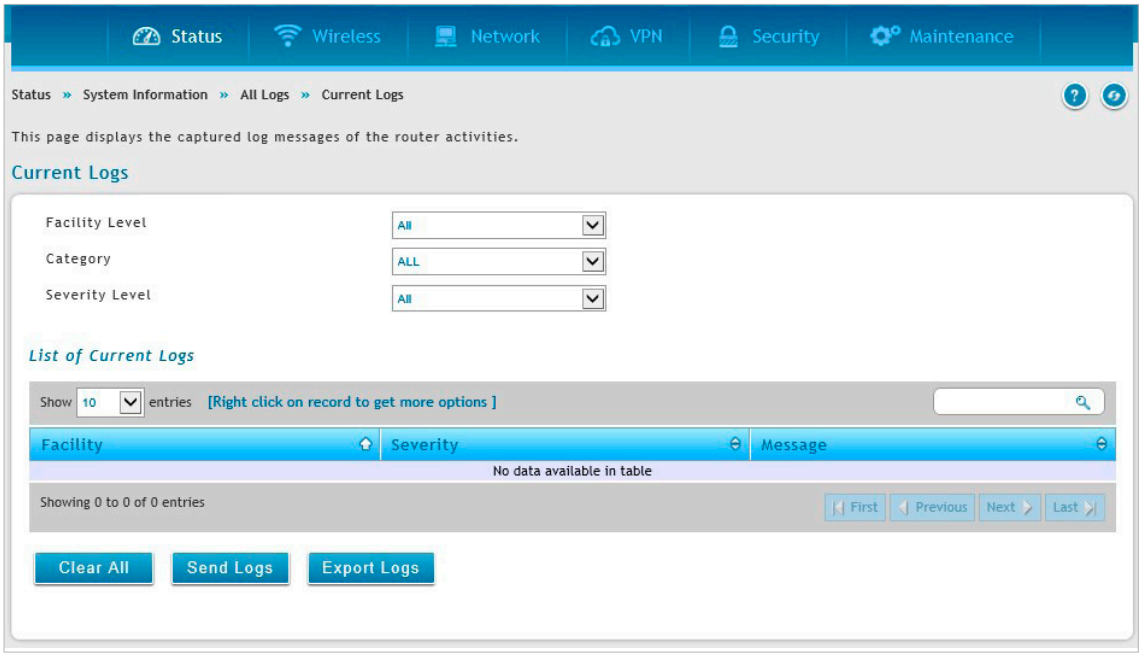

図 10-10　Current Logs 画面

2. 以下の項目を設定します。

項目	説明
Facility Level	ログの定義を以下から選択します。 • 「Kernel」：カーネル関連のログです。 • 「System 」：アプリケーションまたは管理レベルの機能、またはユニット管理に関する管理者による変更に対応するログです。 • 「Wireless」：無線（AP）関連の設定と動作に関するログです。 • 「Network 」：ネットワーク関連のログです。 • 「VPN」：「sslvpn」「openvpn」「ipsec」など VPN 関連のログです。 • 「Firewall」：ファイアウォール関連のログです。
Category	表示するログのカテゴリを指定します。
Severity Level	表示するログのセベリティレベルを以下から選択します。 • 「Emergency」：システムは使用不能 • 「Alert」：即時処理が必要 • 「Critical」：クリティカルな状態 • 「Error」：エラー状態 • 「Warning」：警告状態 • 「Notification」：正常だが注意を要する状態 • 「Information」：情報メッセージ • 「Debugging」：デバッグッセージ

3. 以下のいずれかを実行します。
- 「Clear All」：画面内のすべてのエントリをクリアします。
- 「Send Logs」：画面内のすべてのエントリを設定済みのメール受信者に送信します。
- 「Export Logs」：画面内のすべてのエントリを TXT ファイル形式でエクスポートします。

USB Status（USB ステータス）

Status > System Information > USB Status メニュー

ルータに接続する USB デバイスの情報について概要を表示しています。ルータには、USB プリンタや USB ストレージ デバイス を直接接続できます。

1. **Status > System Information > USB Status** の順にメニューをクリックし、以下の画面を表示します。

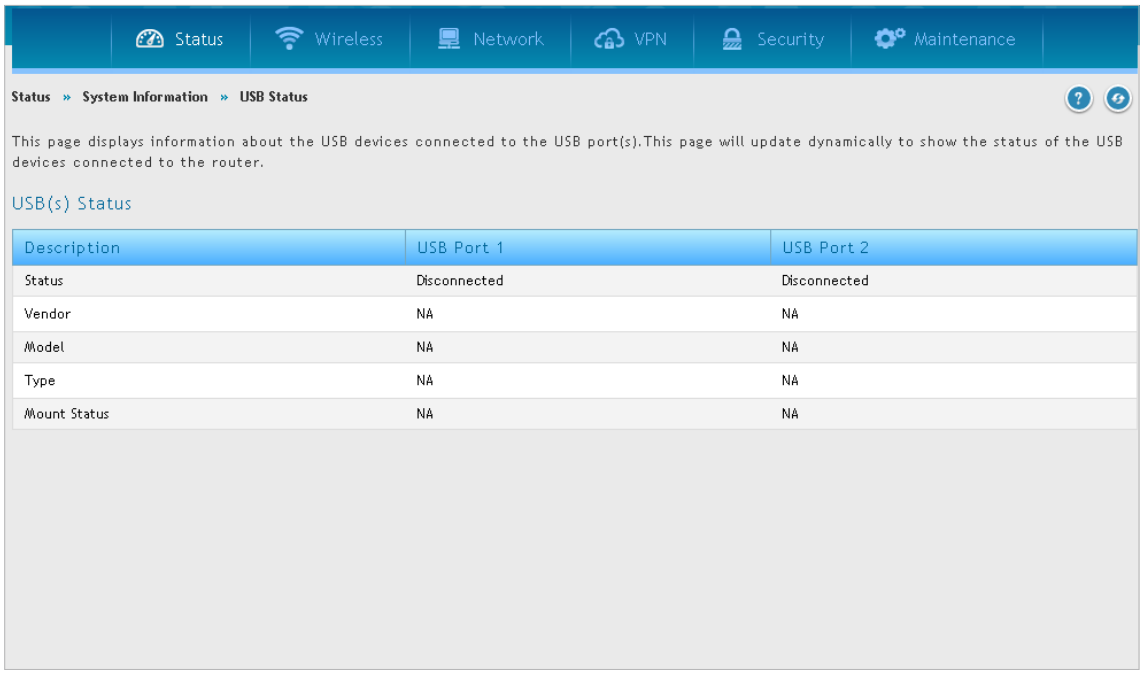

図 10-11　USB Status 画面

2. 以下の項目が表示されます。

項目	説明
Status	接続 / 切断されたデバイスの状態を表示します。
Vendor	ルータに接続する USB デバイスのベンダ名を表示します。
Model	ルータに接続する USB デバイスのモデル名を表示します。
Type	ルータは、USB ディスクドライブ（メモリスティック）デバイス、インターネット USB モデム（アダプタ）、または USB プリンタに接続するインタフェースをサポートしています。
Mount Status	ルータに接続する USB デバイスのマウント状態を表示します。
USB Port 1	USB ポート 1 に接続するデバイスに関する情報を表示します。
USB Port 2	USB ポート 2 に接続するデバイスに関する情報を表示します。

Network Information（ネットワーク情報の参照）

Status > Network Information メニュー
DHCP リースクライアント情報や VPN の接続状況など、ネットワーク情報の確認を行います。

DHCP クライアントの参照

Status > Network Information > DHCP Leased Clients メニュー
ルータから IP をリースしているクライアントのリストを表示します。
リストには以下の種類があります。

- LAN リースクライアント
- IPv6 リースクライアント
- DMZ リースクライアント

LAN Leased Clients（LAN リースクライアント）

1. **Status > Network Information > DHCP Leased Clients > LAN Leased Clients タブ**の順にメニューをクリックし、以下の画面を表示します。

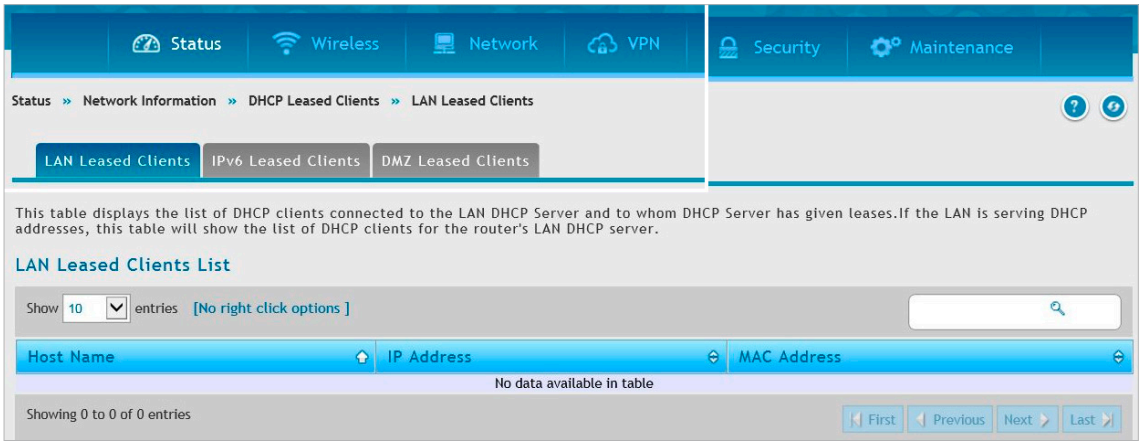

図 10-12　DHCP Leased Clients > LAN Leased Clients タブ画面

2. 以下の項目が表示されます。

項目	説明
Host Name	接続しているクライアントのホスト名が表示されます。
IP Address	予約 IP リストに一致するクライアントの LAN IP アドレスが表示されます。
MAC Addresses	設定済みの IP アドレス予約を持つ LAN クライアントの MAC アドレスが表示されます。

IPv6 Leased Clients（IPv6 リースクライアント）

1. **Status > Network Information > DHCP Leased Clients > IPv6 Leased Clients タブ**の順にメニューをクリックし、以下の画面を表示します。

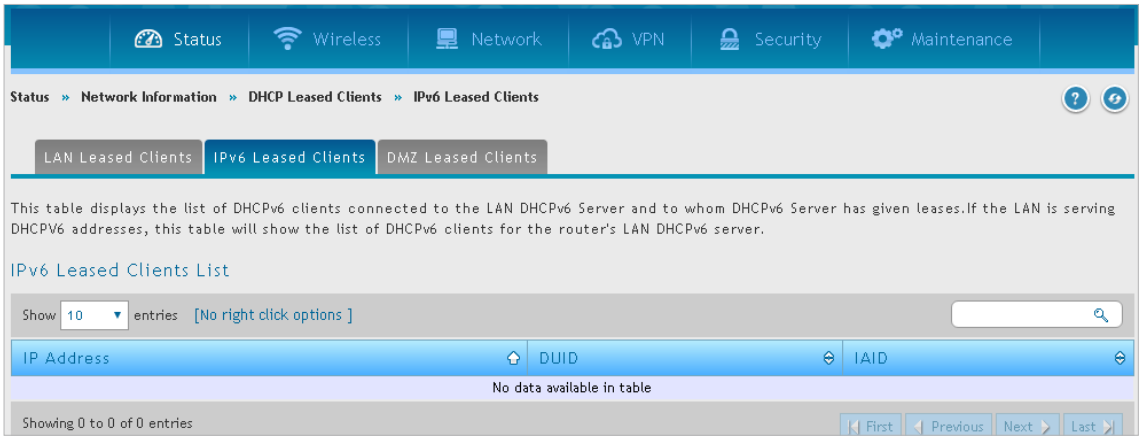

図 10-13　DHCP Leased Clients > IPv6 Leased Clients タブ画面

2. 以下の項目が表示されます。

項目	説明
IP Address	予約 IP リストに一致するクライアントの LAN IPv6 アドレスが表示されます。
DUID	設定済みの IPv6 アドレス予約を持つ LAN クライアントの DUID（DHCP Unique Identifier）が表示されます。
IAID	設定済みの IPv6 アドレス予約を持つ LAN クライアントの IAID（Identity Association Identifier）が表示されます。

DMZ Leased Clients（DMZ リースクライアント）

1. **Status > Network Information > DHCP Leased Clients > DMZ Leased Clients タブ**の順にメニューをクリックし、以下の画面を表示します。

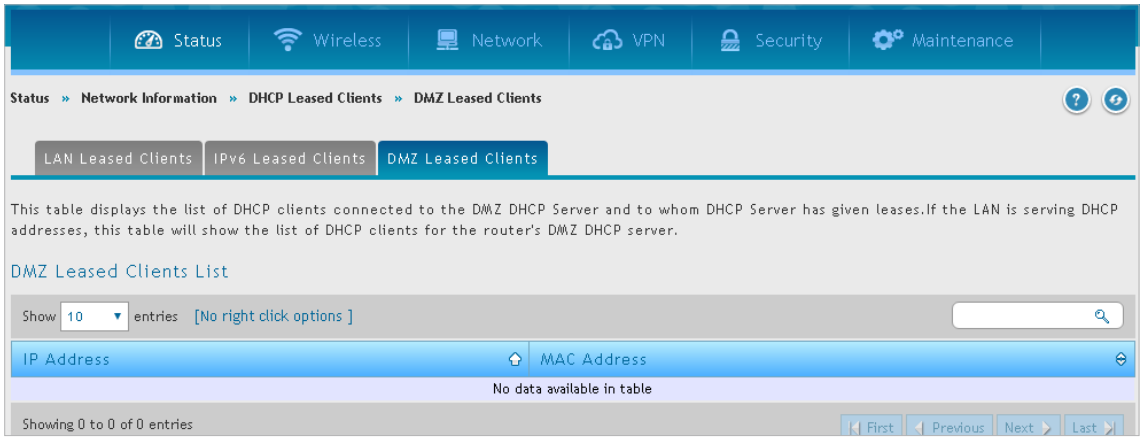

図 10-14　DHCP Leased Clients > DMZ Leased Clients タブ画面

2. 以下の項目が表示されます。

項目	説明
IP Address	予約 IP リストに一致するホストの LAN IP アドレスが表示されます。
MAC Address	定義済みの IP アドレスの予約を持つ LAN ホストの MAC アドレスが表示されます。

CaptivePortal Sessions（キャプティブポータルセッションの参照）

Status > Network Information > CaptivePortal Sessions メニュー
キャプティブポータルセッションについての情報を表示します。

1. **Status > Network Information > CaptivePortal Sessions** の順にメニューをクリックし、以下の画面を表示します。

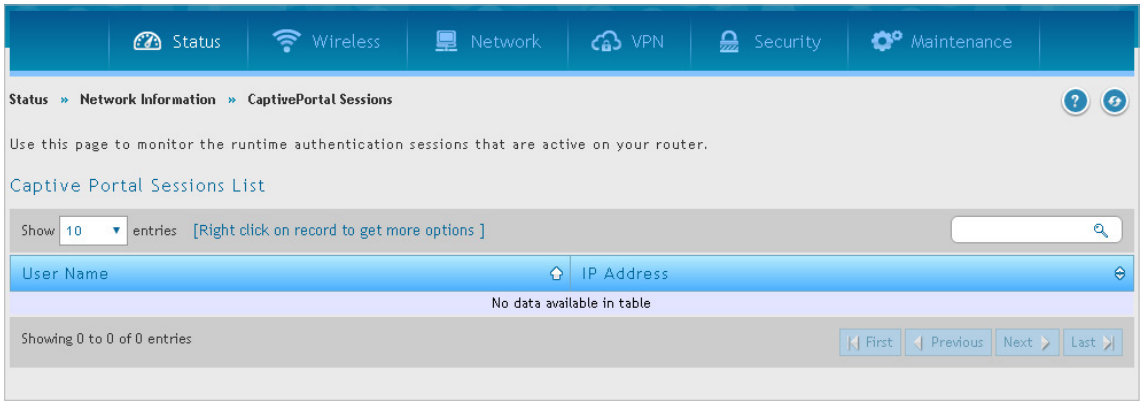

図 10-15　CaptivePortal Sessions 画面

2. 以下の項目が表示されます。

項目	説明
User Name	キャプティブポータルにログイン中のユーザ名が表示されます。
IP Address	キャプティブポータルにログイン中のユーザの IP アドレスが表示されます。

キャプティブポータルセッションのエントリを右クリックし、以下のアクションを実行することができます。
- 「Block」: ユーザ名と IP アドレスをブロックします。
- 「Disconnect」: 選択したユーザの現在のセッションを削除します。

Active Sessions（アクティブセッションの参照）

Status > Network Information > Active Sessions メニュー

アクティブセッションでは、ルータのファイアウォール経由のアクティブなインターネットセッションについて、以下の項目の情報を表示します。

- 「Source」：送信元
- 「Destination」：宛先
- 「Protocol」：プロトコル
- 「State」：状態

1. **Status > Network Information > Active Sessions** の順にメニューをクリックし、以下の画面を表示します。

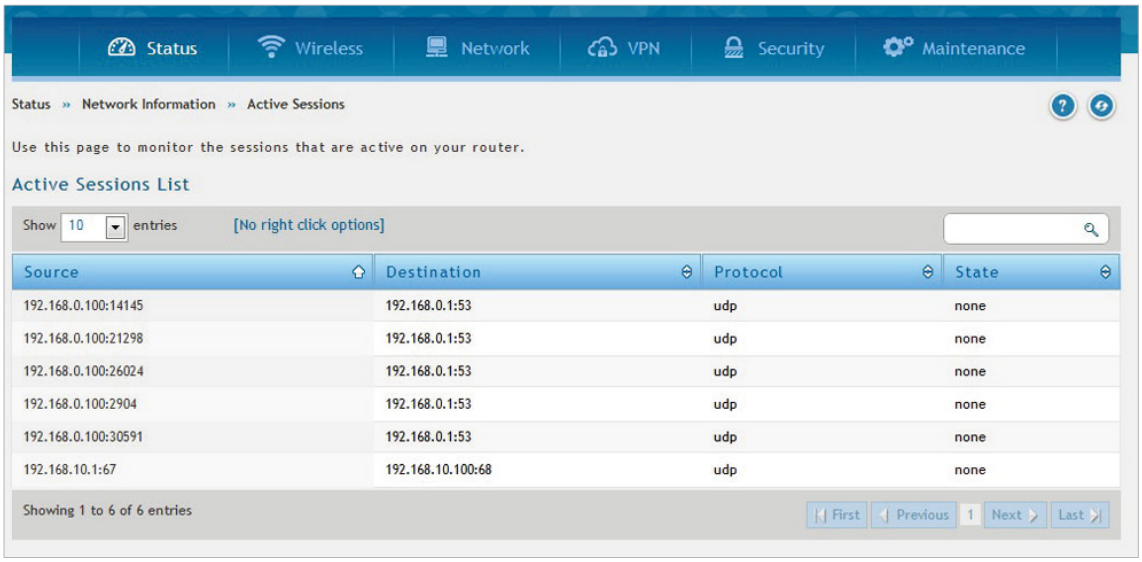

図 10-16　Active Sessions 画面

Active VPNs（VPN セッションの参照）

Status > Network Information > Active VPNs メニュー

ルータの VPN 接続に関するステータス（接続 / 破棄）について表示、変更します。アクティブな VPN 接続のトラフィック詳細やトンネル状態についてリスト化しています。トラフィックについてはトンネル確立後の送受信パケットの累積総量で表示されます。

表示する VPN セッションの内容を以下のタブから選択します。

- IPSec SAs
- SSL VPN Connections
- PPTP Connections
- Open VPN Connections
- L2TP VPN Connections
- GRE Tunnel Sessions

IPSec SAs

1. **Status > Network Information > Active VPNs > IPSec SAs タブ**の順にメニューをクリックし、以下の画面を表示します。

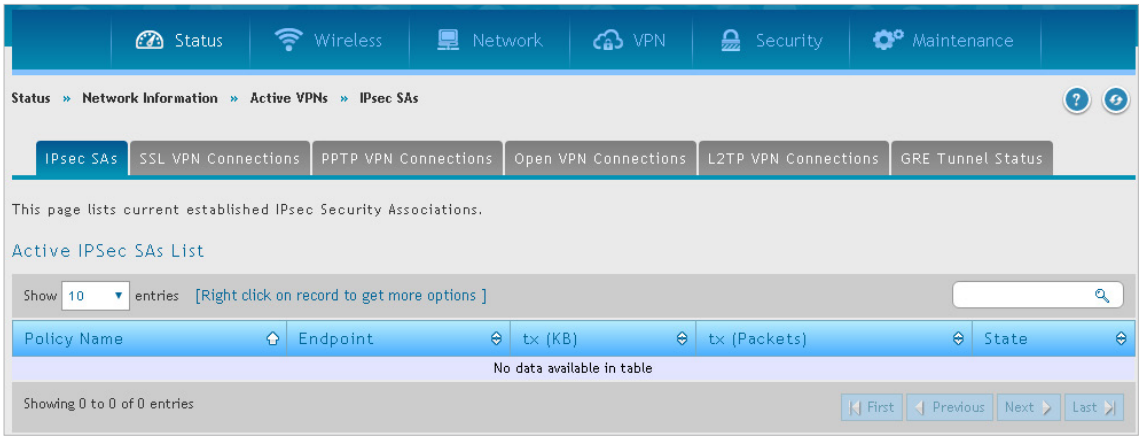

図 10-17　Active VPNs > IPsec SAs タブ画面

SSL VPN Connections

1. **Status > Network Information > Active VPNs > SSL VPN Connections タブ**の順にメニューをクリックし、以下の画面を表示します。

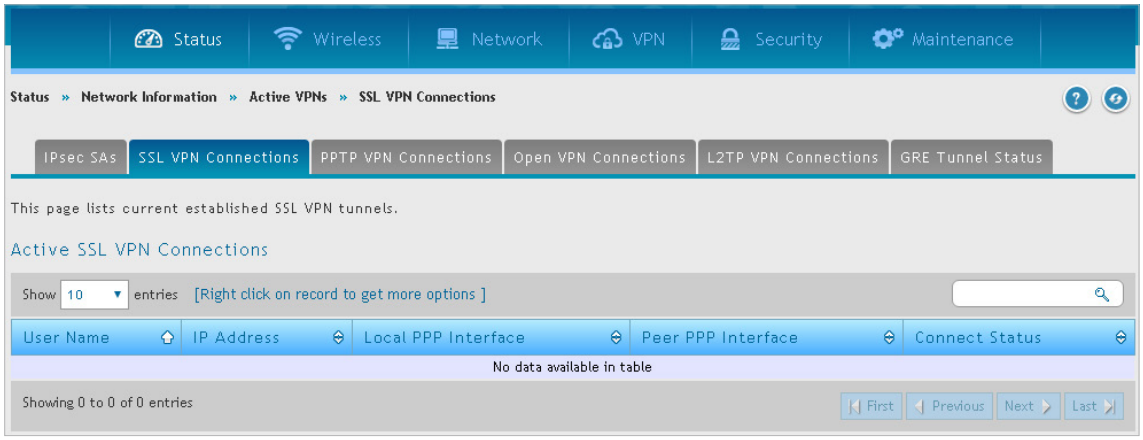

図 10-18　Active VPNs > SSL VPN Connections タブ画面

PPTP VPN Connections

1. **Status > Network Information > Active VPNs > PPTP VPN Connections タブ**の順にメニューをクリックし、以下の画面を表示します。

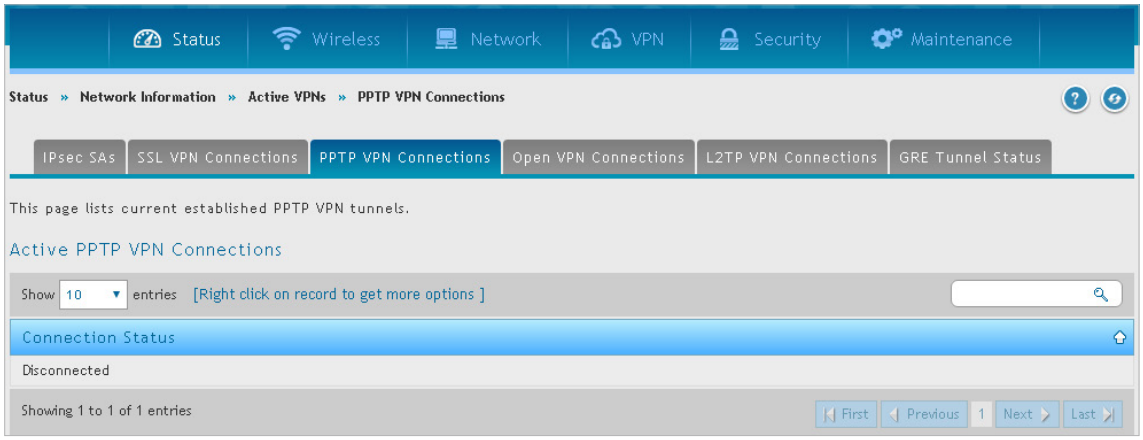

図 10-19　Active VPNs > PPTP VPN Connections タブ画面

Open VPN Connections

1. **Status > Network Information > Active VPNs > Open VPN Connections タブ**の順にメニューをクリックし、以下の画面を表示します。

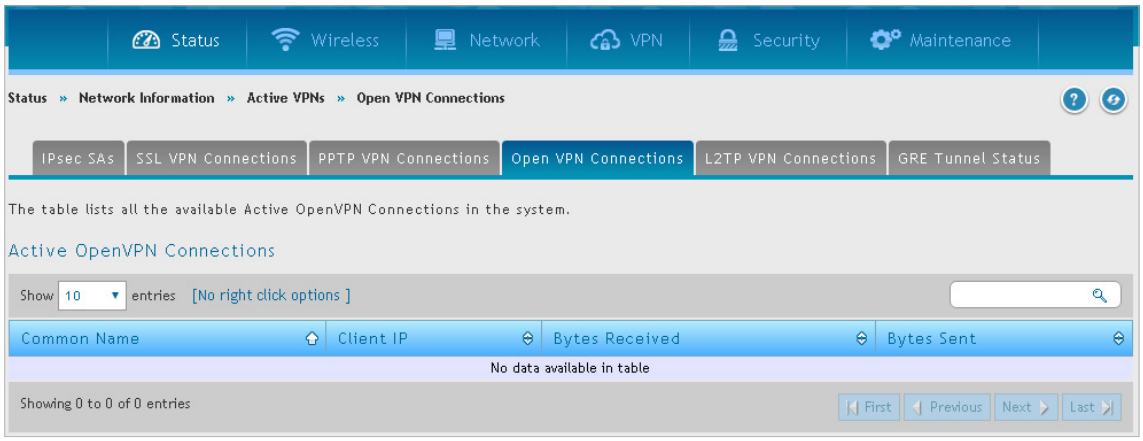

図 10-20　Active VPNs > OpenVPN Connections タブ画面

L2TP VPN Connections

1. **Status > Network Information > Active VPNs > L2TP VPN Connections タブ**の順にメニューをクリックし、以下の画面を表示します。

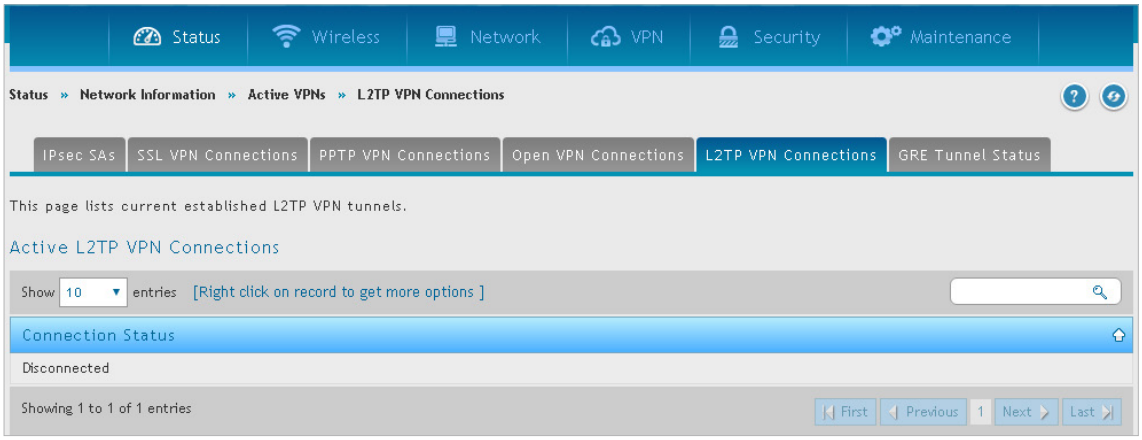

図 10-21　Active VPNs > L2TP VPN Connections タブ画面

GRE Tunnel Status

1. **Status > Network Information > Active VPNs > GRE Tunnel Status タブ**の順にメニューをクリックし、以下の画面を表示します。

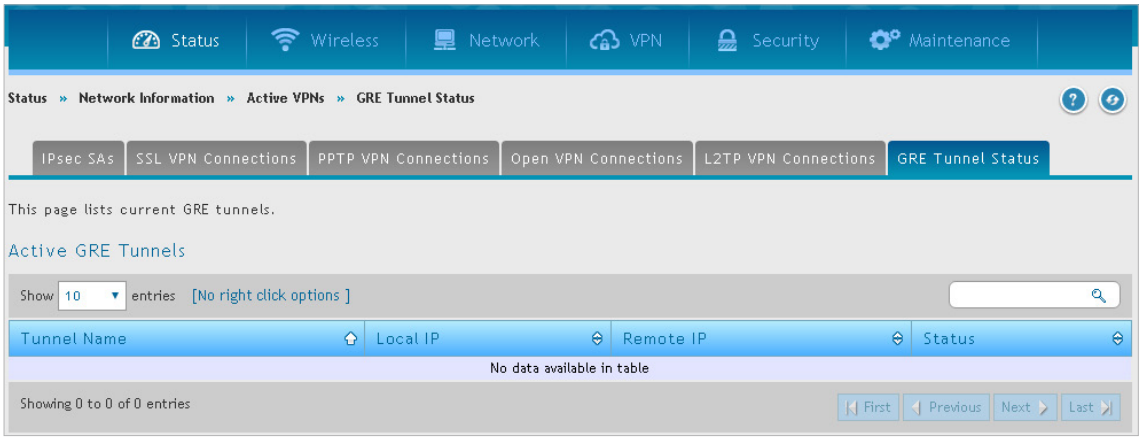

図 10-22　Active VPNs > GRE Tunnel Status タブ画面

Interfaces Statistics（インタフェースの統計）

Status > Network Information > Interfaces Statistics メニュー

LAN、VLAN および WLAN インタフェースにおけるパケット情報を表示します。

1. **Status > Network Information > Interfaces Statistics** の順にメニューをクリックし、以下の画面を表示します。

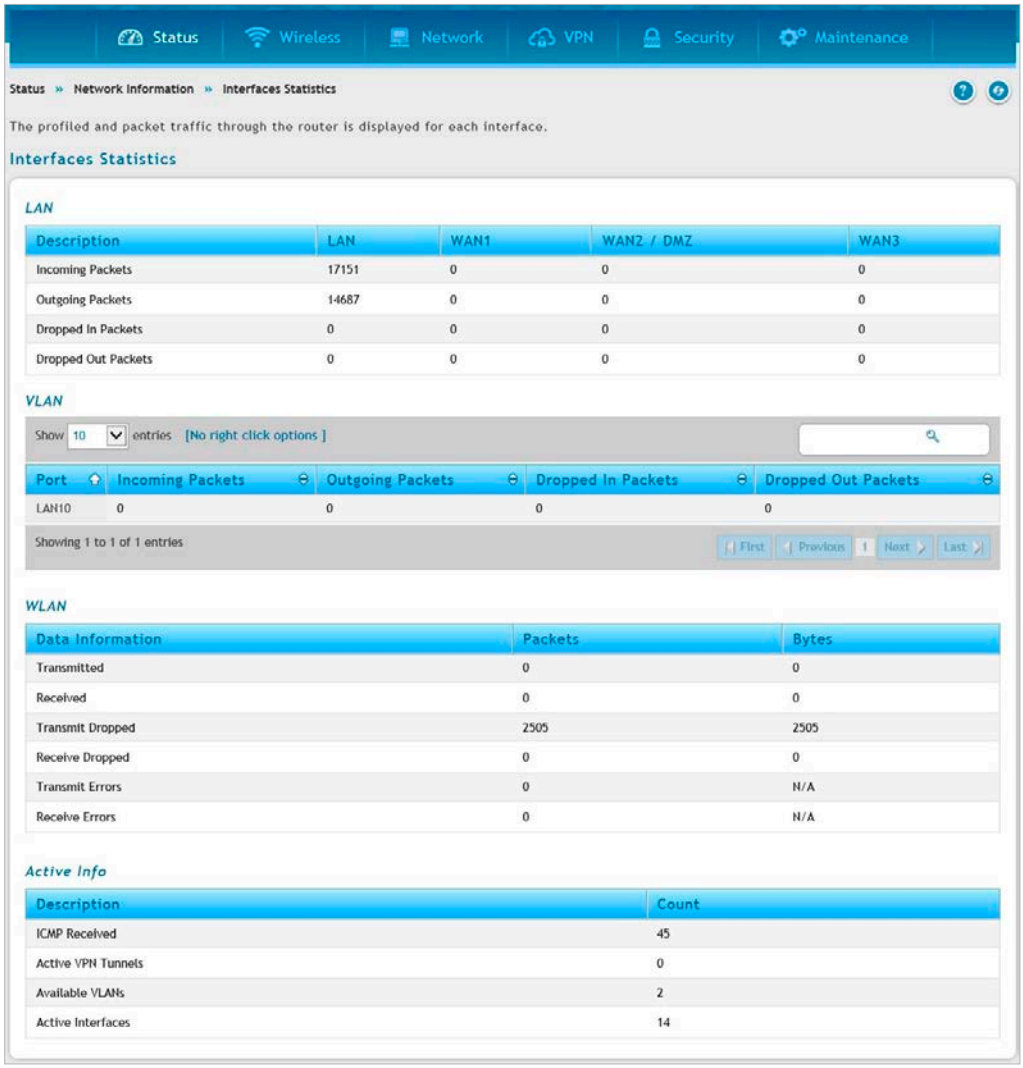

図 10-23　Interfaces Statistics 画面

2. 以下の項目が表示されます。

項目	説明
LAN	
Incoming Packets	ポートに入力する IP パケット数が表示されます。
Outgoing Packets	ポートから出力するパケット数が表示されます。
Dropped In Packets	インタフェースのインバウンド方向で破棄されたパケットが表示されます。
Dropped Out Packets	インタフェースのアウトバウンド方向で破棄されたパケットが表示されます。
VLAN	
Port	VLAN に対応するポート番号が表示されます。
Incoming Packet	ポートに入力する IP パケット数が表示されます。
Outgoing Packet	ポートから出力するパケット数が表示されます。
Dropped In Packet	インタフェースのインバウンド方向で破棄されたパケットが表示されます。
Dropped Out Packet	インタフェースのアウトバウンド方向で破棄されたパケットが表示されます。
WLAN	
Transmitted	ルータの管理下にあるすべてのアクセスポイントが送信したパケット数が表示されます。
Received	ルータの管理下にあるすべてのアクセスポイントが受信したパケット数が表示されます。
Transmit Dropped	ルータの管理下にあるすべてのアクセスポイントが送信し、破棄された総パケット数が表示されます。
Receive Dropped	ルータの管理下にあるすべてのアクセスポイントが受信し、破棄された総パケット数が表示されます。
Transmit Errors	ルータの管理下にあるすべてのアクセスポイントが送信し、エラーが発生した総パケット数が表示されます。
Receive Errors	ルータの管理下にあるすべてのアクセスポイントが受信し、エラーが発生した総パケット数が表示されます。

項目	説明
Active Info	
ICMP Received	インタフェースで受信した ICMP パケットの総数が表示されます。
Active VPN Tunnels	現在のアクティブな VPN トンネルセッション数が表示されます。
Available VLAN	現在のアクティブな有効 VLAN インタフェース数が表示されます。
Active Interfaces	有効なインタフェースの数が表示されます。

Wireless Clients（無線クライアントの参照）

Status > Network Information > Wireless Clients メニュー

AP に接続するクライアントについて表示します。接続クライアントは MAC アドレスによってソートされ、対応する AP への接続時間や、無線リンクで使用されるセキュリティパラメータが表示されます。統計テーブルには、ページが更新されるたびに最新のデータを表示できるようにする自動更新機能があります。自動更新は 10 秒ごとに行われます。

本項目は DSR-1000AC でのみ表示されます。

Status > Network Information > Wireless Clients の順にメニューをクリックし、以下の画面を表示します。

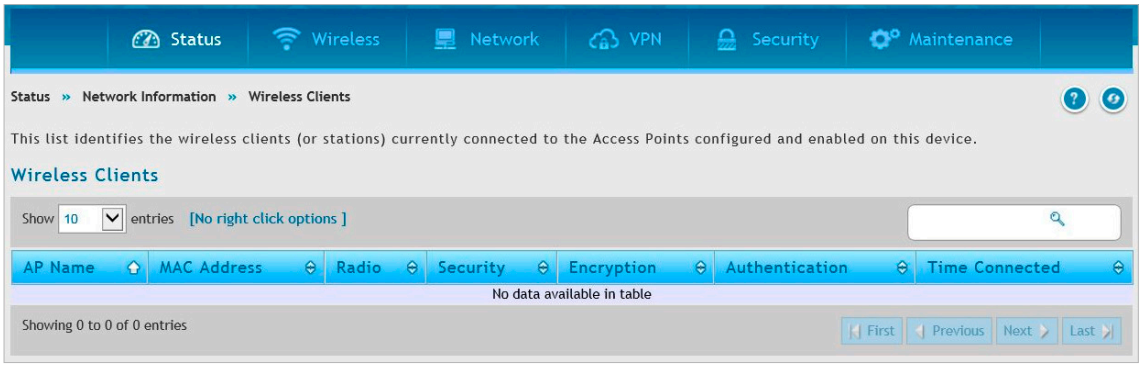

図 10-24　Wireless Clients 画面

Wireless Statistics（無線の統計情報）

Status > Network Information > Wireless Statistics メニュー

本画面では、有効化された各アクセスポイントについて、トラフィック統計を表示します。各無線リンクで送信されるトラフィック量を確認することができます。無線帯域または VAP の不具合が発生している場合、本項目でトラフィックが VAP 経由で送受信されているかどうかを確認します。

本項目は DSR-1000AC でのみ表示されます。

1. **Status > Network Information > Wireless Statistics** の順にメニューをクリックし、以下の画面を表示します。

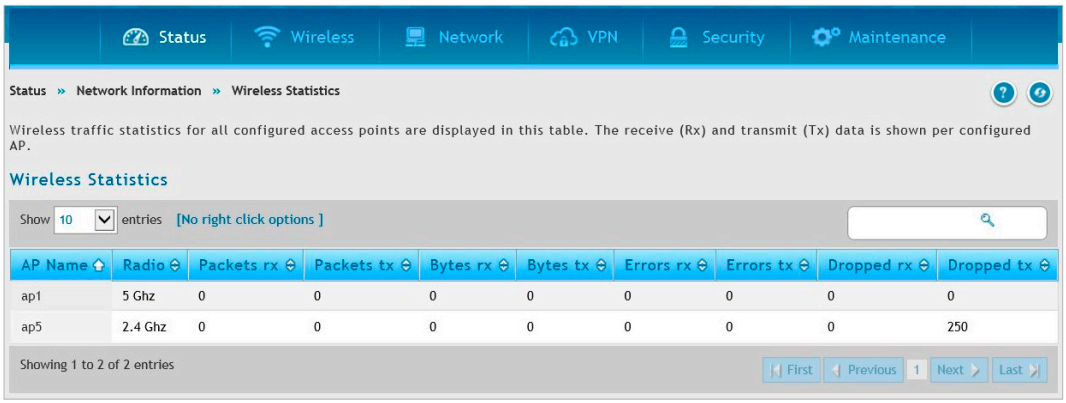

図 10-25　Wireless Statistics 画面

Device Statistics（デバイス統計情報）

Status > Network Information > Device Statistics メニュー

本製品の物理ポートの送受信統計情報を表示します。
各インタフェース（WAN1、WAN2 / DMZ、LAN、および VLAN）には、確認のために提供されている、ポート固有のパケットレベル情報があります。送信 / 受信パケット、ポートの衝突、および送信 / 受信方向の累積バイト / 秒が、ポートの稼働時間とともに各インタフェースに提供されます。有線ポートに問題があると思われる場合は、この表を参照し、アップタイムまたはポートの伝送レベルの問題を診断してください。
統計テーブルには、画面が更新されるたびに最新のデータを表示できるようにする自動更新機能があります。自動更新は 10 秒ごとに行われます。

1. **Status > Network Information > Device Statistics** の順にメニューをクリックし、以下の画面を表示します。

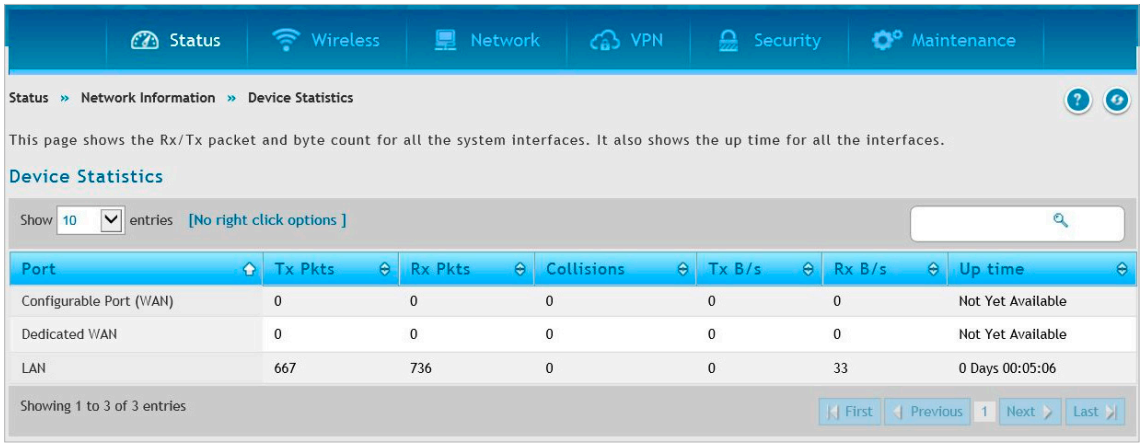

図 10-26　Device Statistics 画面

LAN Clients（LAN クライアント）

Status > Network Information > LAN Clients メニュー

ルータに接続する LAN クライアントを LAN スイッチ経由の ARP スキャンによって識別します。
検出された LAN ホストの NetBIOS 名（利用可能である場合）、IP アドレス、および MAC アドレスを表示します。

1. **Status > Network Information > LAN Clients** の順にメニューをクリックし、以下の画面を表示します。

図 10-27　LAN Clients 画面

Session Limiting Status（セッション制限ステータス）

Status > Network Information > Session Limiting Status メニュー

セッション制限のステータスが表示されます。

1. **Status > Network Information > Session Limiting Status** の順にメニューをクリックし、以下の画面を表示します。

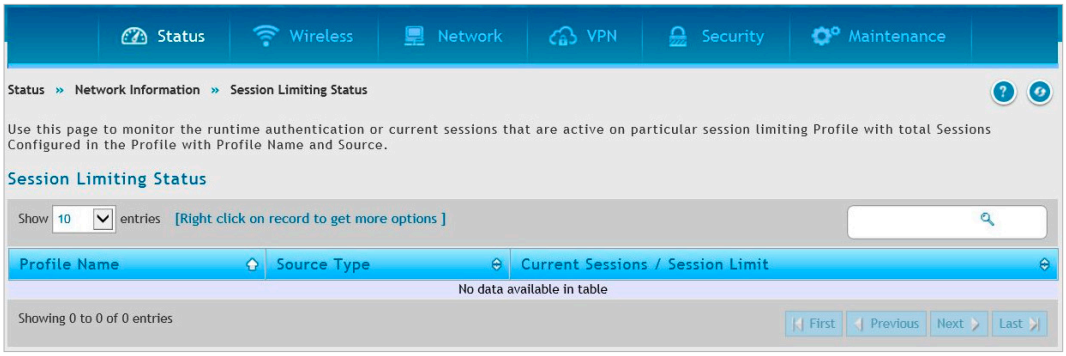

図 10-28　Session Limiting Status 画面

第 11 章　トラブルシューティング

本製品の操作時にトラブルが発生した場合、本章をご参照ください。

インターネット接続

症状 :

ご使用の LAN 上の PC からルータの Web 設定インタフェースにアクセスできない。

■ 推奨される操作 :

1. PC とルータ間のイーサネット接続をチェックしてください。
2. ご使用の PC の IP アドレスがルータと同じサブネットにあることを確認してください。推奨されるアドレス指定の体系を使用している場合、ご使用の PC のアドレスは「192.168.10.2 - 192.168.10.254」の範囲にする必要があります。
3. PC の IP アドレスをチェックしてください。PC が DHCP サーバに到達できない場合、Windows と Mac OS のいくつかのバージョンでは IP アドレスを生成して、割り当てています。これらの自動生成アドレスは「169.254.x.x」の範囲にあります。IP アドレスがこの範囲にある場合、PC からファイアウォールまでの接続をチェックして、PC を再起動してください。
4. ご使用のルータの IP アドレスを変更した後、IP アドレスを忘れた場合には、ルータのコンフィグレーションを工場出荷時設定にリセットしてください（リセットにより、ファイアウォールの IP アドレスが 192.168.10.1 に設定されます）。
5. 工場出荷時設定にリセットしてコンフィグレーションを失いたくない場合、パケットスニッファー（Ethereal など）を使用して、ルータの再起動時に送信されたパケットをキャプチャしてください。ARP（Address Resolution Protocol）パケットを見て、ルータの LAN インタフェースアドレスの位置を見つけます。
6. ブラウザを起動し、Java、JavaScript、または ActiveX が有効であることを確認してください。Internet Explorer を使用している場合、「更新」をクリックして、Java アプレットがロードされていることを確認してください。ブラウザを閉じて、再度起動します。
7. 正しいログイン情報を使用していることを確認してください。工場出荷時のユーザ名とパスワードの初期値は「admin」です。この情報を入力する時、「CAPS LOCK」がオフであることを確認してください。

症状 :

ルータがコンフィグレーションの設定を保存しない。

■ 推奨される操作 :

1. コンフィグレーション設定を入力する場合、別のメニューまたはタブに移行する前に「Save」をクリックしてください。
「Save」をクリックしない場合、行った変更は失われます。
2. ブラウザで「更新」または「リロード」をクリックしてください。変更が行われた可能性がありますが、ブラウザは古いコンフィグレーションをキャッシュしているかもしれません。

症状 :

ルータがインターネットにアクセスできない。

■ 考えられる原因 :

ダイナミック IP アドレスを使用している場合、ご使用のルータが ISP に IP アドレスを要求していない可能性があります。

■ 推奨される操作 :

1. ブラウザを起動して、www.google.com などの外部サイトに接続してください。
2. 「https://192.168.10.1」でファイアウォールコンフィグレーションのメインメニューにアクセスしてください。
3. ステータス画面で IP アドレスが WAN ポートに表示されていることを確認してください。「0.0.0.0」が示される場合、ファイアウォールはご契約の ISP から IP アドレスを取得していません。次の症状を参照してください。

症状 :

ルータが ISP から IP アドレスを取得できない。

■ 推奨される操作 :

1. ケーブルまたは ADSL モデムの電源をオフにします。
2. ルータの電源をオフにします。
3. 5 分後にケーブルまたは ADSL モデムの電源を再度オンにします。
4. モデムの LED が、ISP に再度同期したことを示した後、ルータの電源を再度オンにします。ルータがまだ ISP のアドレスを取得できない場合、次の症状を参照してください。

症状 :

ルータがまだ ISP から IP アドレスを取得できない。

■ 推奨される操作 :

1. ログインプログラムを必要とするかどうか ISP に問い合わせてください。 - PPP over Ethernet（PPPoE）または他のログインタイプ
2. ログインプログラムが必要な場合、設定したログイン名とパスワードが正しいことを確認してください。
3. ご使用の PC のホスト名をチェックするかどうか ISP に問い合わせてください。
4. チェックが行われる場合、**Network Configuration > WAN Settings > Ethernet ISP Settings** を選択して、アカウント名を ISP のアカウントの PC ホスト名に設定します。
5. ご使用のイーサネット MAC アドレスが検証され、許可された MAC アドレス 1 つだけがインターネットに接続できるのかどうか ISP に問い合わせてください。
6. MAC アドレスの検証が行われる場合、新しいネットワークデバイスを購入したことを ISP に知らせて、ファイアウォールの MAC アドレスを使用するように依頼してください。
7. または、**Network Configuration > WAN Settings > Ethernet ISP Settings** を選択して、ルータがご使用の PC の MAC アドレスになり代わるように設定してください。

症状 :

ルータは IP アドレスを取得できるが、PC でインターネットページをロードできない。

■ 推奨される操作 :

1. 指定のドメインネームシステム（DNS）サーバのアドレスを ISP に問い合わせてください。PC がそれらのアドレスを認識するように設定してください。詳しくは、オペレーティングシステムのドキュメントを参照してください。
2. ご使用の PC でルータが TCP/IP ゲートウェイとなるように設定します。

日付と時間

症状 :

表示される日付が、January 1, 1970（1970 年 1 月 1 日）である。

■ 考えられる原因 :

ルータはまだネットワークタイムサーバ（NTS）への到達に成功していません。

■ 推奨される操作 :

1. ルータを設定したばかりである場合、5 分以上待ってから Maintenance > Administration > Date and Time メニューで日付を確認してください。
2. インターネットアクセス設定を確認してください。

症状 :

時間が 1 時間遅れています。

■ 考えられる原因 :

ルータは自動的にサマータイム（DST : Daylight Savings Time）の調整をしません。

■ 推奨される操作 :

1. **Maintenance > Administration > Date and Time** メニューをクリックします。
2. 「Daylight Saving」を「ON」または「OFF」にします。
3. 「Save」をクリックし、設定を適用します。

LAN の接続性をテストするために Ping する

多くの TCP/IP 端末デバイスとファイアウォールには ping ユーティリティが備わっており、ICMP エコーリクエストパケットを指定したデバイスに送信することができます。デバイスはエコーリプライで応答します。ご使用の PC またはワークステーションで ping ユーティリティを使用することによって、TCP/IP ネットワークの障害調査が非常に簡単になります。

ご使用の PC からルータまでの LAN パスをテストする

1. PC の Windows ツールバーから、「スタート」>「ファイル名を指定して実行」を選択し、「cmd」を入力して Enter キーを押します。
2. コマンドプロンプトで「ping <IP アドレス >」とタイプしてください。<IP アドレス > はルータの IP アドレスです。例 : ping 192.168.10.1
3. Enter キーを押します。
4. 表示をモニタする :
   - パスが動作している場合、以下のメッセージシーケンスが表示されます。
     Pinging <IP アドレス > with 32 bytes of data
     Reply from <IP アドレス > : bytes=32 time=NN ms TTL=xxx
   - パスが動作していない場合、以下のメッセージシーケンスが表示されます。
     Pinging <IP アドレス > with 32 bytes of data Request timed out
5. パスが動作していない場合、PC とルータ間の物理接続をテストしてください。
   - LAN ポート LED が消灯している場合、「」を参照してください。
   - 対応するリンクの LED が、ワークステーションとファイアウォールに接続するネットワークインタフェースカードおよびハブポートについても点灯していることを確認してください。
6. パスがまだ動作していない場合、ネットワークのコンフィグレーションをテストしてください。
   - イーサネットカードのドライバソフトウェアと TCP/IP ソフトウェアが PC にインストールされて、設定済みであることを確認してください。
   - ルータと PC の IP アドレスが正しく、同じサブネットにあることを確認してください。

ご使用の PC からリモートデバイスまでの LAN パスをテストする

1. PC の Windows ツールバーから、「スタート」>「ファイル名を指定して実行」を選択し、「cmd」を入力して Enter キーを押します。
2. コマンドプロンプトで「ping-n10 <IP アドレス >」と入力してください。「-n 10」は最大 10 回行うことを示し、<IP アドレス > はご契約の ISP の DNS サーバなどリモートデバイスの IP アドレスです。例 : ping -n 10 10.1.1.1
3. Enter キーを押して、表示をモニタします。（前述の手順を参照してください。）
4. パスが動作していない場合、以下を確認してください。
   - PC にファイアウォールの IP アドレスがデフォルトゲートウェイとして設定されているかをチェックしてください。（PC の IP 設定が DHCP によって割り当てられている場合、この情報は PC のネットワークコントロールパネルで見ることはできません。）
   - PC のネットワーク（サブネット）アドレスがリモートデバイスのネットワークアドレスと異なることを確認してください。
   - ケーブルまたは DSL モデムが接続されて、機能していることを確認してください。
   - ご使用の PC にホスト名を割り当てたかどうか ISP に問い合わせてください。

     ホスト名が割り当てられている場合、**Network Configuration > WAN Settings > Ethernet ISP Settings** を選択して、そのホスト名を ISP のアカウント名として入力してください。
   - 特定の PC のイーサネット MAC アドレス以外が拒否される仕様かどうかを ISP に問い合わせてください。

ブロードバンドの ISP の多くは、ユーザが利用するブロードバンドモデムにおける MAC アドレスからのトラフィックだけを許可することによって、アクセスを制限します。ISP によっては、さらにそのモデムに接続する特定の PC の MAC アドレスに対するアクセスを制限します。
そのような場合は、ファイアウォールをクローンに設定するか、認可された PC からの MAC アドレスになり代わるようにしてください。

工場出荷時設定へのリセット

工場出荷時のコンフィグレーション設定を復元するには、以下のいずれかの手順を実施します。

1. アカウントのパスワードと IP アドレスをご存じですか ?
   - 知っている場合、**Maintenance > Firmware & Config > Soft Reboot** を選択し、「Default」をクリックします。
   - 知らない場合、以下の手順を行ってください。

     ルータの背面パネルで、リセットボタンを 10 秒程度押し続けます。全ての LED ライトが点灯し、点滅したらボタンを離して、ルータが再起動するのを待ってください。
2. ルータが自動的に再起動しない場合、手動で再起動を行い、初期設定を有効にしてください。
3. コンフィグレーションインタフェースまたは「Reset」から工場出荷時設定に復元した後、以下の設定が適用されます。

項目	設定
LAN IP アドレス	192.168.10.1
ユーザ名	admin
パスワード	admin
LAN の DHCP サーバ	enabled
WAN ポート設定	DHCP 経由で設定を取得

付録

【付録 A】用語解説

用語	説明
ARP	Address Resolution Protocol。IP アドレスを MAC アドレスにマップするブロードキャストプロトコル。
CHAP	Challenge-Handshake Authentication Protocol。ISP に対してユーザを認証するためのプロトコル。
DDNS	Dynamic DNS。リアルタイムでドメイン名を更新するシステム。ドメイン名がダイナミック IP アドレスを持つデバイスに割り当てられます。
DHCP	Dynamic Host Configuration Protocol。ホストが IP アドレスを必要としなくなった時にアドレスを再利用できるようにダイナミックに IP アドレスを割り当てるプロトコル。
DNS	Domain Name System。H.323 ID、URL、またはメール ID を IP アドレスに変換するメカニズム。また、リモートゲートキーパの場所を見つけるのを補助して、IP アドレスを管理ドメインのホスト名にマップするために使用されます。
FQDN	FQDN（完全修飾ドメイン名）。ホスト部分を含む完全なドメイン名。例 : serverA.companyA.com
FTP	File Transfer Protocol。ネットワークノード間でファイルを転送するプロトコル。
HTTP	Hypertext Transfer Protocol。ファイルの転送のために Web ブラウザと Web サーバに使用されるプロトコル。
IKE	Internet Key Exchange。VPN トンネルを構築する処理の中で、ISAKMP で安全に暗号化鍵を交換するモード。
IPSec	IP security。データストリームにおける IP パケットの認証、または暗号化によって VPN トンネルを保証するプロトコルセット。IPSec は、「transport」モード（パケットヘッダではなく、ペイロードを暗号化する）または「tunnel」モード（ペイロードとパケットヘッダの両方を暗号化する）のいずれかで動作します。
ISAKMP	Internet Key Exchange Security Protocol。インターネットでセキュリティ結合と暗号鍵を確立するプロトコル。
ISP	Internet service provider（インターネットサービスプロバイダ）。
MAC Address	Media-access-control address。ネットワークアダプタに割り当てられている固有の物理アドレス識別子。
MTU	Maximum transmission unit。通過可能な最も大きいパケットサイズ（バイト）。イーサネットの MTU は 1500 バイトのパケットです。
NAT	Network Address Translation。ルータまたはファイアウォールを通過するパケットとして IP アドレスを書き換える処理。NAT は、LAN のゲートウェイルータにおける単一のパブリック IP アドレスを使用して、LAN 上の複数ホストがインターネットにアクセスするのを可能にします。
NetBIOS	ファイル共有、プリンタ共有、メッセージング、認証、および名前解決のためのマイクロソフトの Windows プロトコル。
NTP	Network Time Protocol。クロックマスタとして知られているルータをネットワークにおける単一のクロックに同期させるプロトコル。
PAP	Password Authentication Protocol。リモートアクセスサーバまたは ISP に対してユーザを認証するためのプロトコル。
PPPoE	Point-to-Point Protocol over Ethernet。ISP が IP アドレスの割り当てを管理することなくホストのネットワークを ISP に接続するためのプロトコル。
PPTP	Point-to-Point Tunneling Protocol。インターネット上のリモートクライアントからプライベートサーバまでの安全なデータ転送のために VPN を作成するプロトコル。
RADIUS	Remote Authentication Dial-In User Service。リモートユーザ認証とアカウンティングのためのプロトコル。ユーザ名とパスワードの集中管理を提供します。
RSA	Rivest-Shamir-Adleman。公開鍵 暗号化アルゴリズム。
TCP	Transmission Control Protocol。信頼性と順序通りの配信を保証したインターネットにおけるデータ送信のプロトコル。
UDP	User Data Protocol。信頼性と順序通りの配信を保証せずにインターネットにおけるデータを送信するプロトコル。
VPN	Virtual private network。異なるネットワーク間のトラフィックすべてを暗号化することによって、IP トラフィックがパブリックな TCP/IP ネットワークを安全に通過することを可能とするネットワーク。IP レベルで全情報を暗号化するためにトンネリングを使用します。
WINS	Windows Internet Name Service。名前解決のためのサービス。異なる IP サブネットのクライアントがブロードキャストを送信せずに、ダイナミックにアドレスの解決、自身の登録、およびネットワークのブラウズを行うことができます。
XAUTH	IKE Extended Authentication。IKE プロトコルに基づいて（IKE が認証する）デバイスだけではなく、ユーザも認証する方式。ユーザ認証はデバイス認証後と IPSec ネゴシエーション前に実行されます。

【付録 B】工場出荷時設定

機能	説明	初期値
デバイスログイン	ユーザログイン	URL https://192.168.10.1
	ユーザ名（大文字小文字区別あり）	admin
	ログインパスワード（大文字小文字区別あり）	admin
インターネット接続	WAN MAC アドレス	初期アドレスを使用
	WAN MTU サイズ	1500
	ポート速度	Auto Sense
ローカルエリアネットワーク（LAN）	IP アドレス	192.168.10.1
	IPv4 サブネットマスク	255.255.255.0
	RIP ディレクション	なし
	RIP バージョン	無効
	RIP 認証	無効
	DHCP サーバ	有効
	DHCP 開始 IP アドレス	192.168.10.2
	DHCP 終了 IP アドレス	192.168.10.100
	タイムゾーン	GMT
	サマータイム	無効
	SNMP	無効
	リモート管理	無効
ファイアウォール	インターネットからのインバウンド通信	無効（HTTP 80 番ポートを除く）
	インターネットへのアウトバウンド通信	有効（すべて）
	送信元 MAC フィルタ	無効
	ステルスモード	有効

【付録 C】ポートフォワーディングとファイアウォール設定に利用可能な標準サービス

ANY	ICMP-TYPE-8	RLOGIN
AIM	ICMP-TYPE-9	RTELNET
BGP	ICMP-TYPE-10	RTSP:TCP
BOOTP_CLIENT	ICMP-TYPE-11	RTSP:UDP
BOOTP_SERVER	ICMP-TYPE-13	SFTP
CU-SEEME:UDP	ICQ	SMTP
CU-SEEME:TCP	IMAP2	SNMP:TCP
DNS:UDP	IMAP3	SNMP:UDP
DNS:TCP	IRC	SNMP-TRAPS:TCP
FINGER	NEWS	SNMP-TRAPS:UDP
FTP	NFS	SQL-NET
HTTP	NNTP	SSH:TCP
HTTPS	PING	SSH:UDP
ICMP-TYPE-3	POP3	STRMWORKS
ICMP-TYPE-4	PPTP	TACACS
ICMP-TYPE-5	RCMD	TELNET
ICMP-TYPE-6	REAL-AUDIO	TFTP
ICMP-TYPE-7	REXEC	VDOLIVE

【付録 D】ログメッセージ

■ ファシリティ：システム（ネットワーク）

ログメッセージ	緊急度	ログメッセージ	緊急度
DBUpdate event: Table: %s opCode:%drowId:%d	DEBUG	BridgeConfig: too few arguments to command %s	ERROR
networkIntable.txt not found	DEBUG	BridgeConfig: too few arguments to command %s	ERROR
sqlite3QueryResGet failed	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Interface is already deleted in bridge	DEBUG	ddnsDisable failed	ERROR
removing %s from bridge %s... %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
adding %s to bridge %s... %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
stopping bridge...	DEBUG	ddnsDisable failed	ERROR
stopping bridge...	DEBUG	failed to call ddns enable	ERROR
stopping bridge...	DEBUG	ddnsDisable failed	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Wan is not up	DEBUG	Error in executing DB update handler	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
doDNS:failed	DEBUG	Illegal invocation of ddnsView (%s)	ERROR
doDNS:failed	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
doDNS:Result = FAILED	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
doDNS:Result SUCCESS	DEBUG	ddns: SQL error: %s	ERROR
Write Old Entry: %s %s %s: to %s	DEBUG	Illegal operation interface got deleted	ERROR
Write New Entry: %s %s #%s : to %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Write Old Entry: %s %s %s: to %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Write New Entry: %s %s #%s : to %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
ifStaticMgmtDBUpdateHandler: returning with "	DEBUG	ddnsDisable failed	ERROR
nimfLinkStatusGet: buffer: \	DEBUG	ddns: SQL error: %s	ERROR
nimfLinkStatusGetErr: returning with status: %d	DEBUG	Failed to call ddns enable	ERROR
nimfAdvOptSetWrap: current Mac Option: %d	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: current Port Speed Option: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: current Mtu Option: %d	DEBUG	Failed to call ddns enable	ERROR
nimfAdvOptSetWrap: looks like we are reconnecting. "	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: Mtu Size: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: NIMF table is %s	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap:WAN_MODE TRIGGER	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: MTU: %d	DEBUG	Failed to call ddns enable	ERROR
nimfAdvOptSetWrap: MacAddress: %s	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: old Mtu Flag: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: user has changed MTU option	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: MTU: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: old MTU size: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: old Port Speed Option: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: old Mac Address Option: %d	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: MacAddress: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Setting LED [%d]:[%d] For %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
l2tpEnable: command string: %s	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: handling reboot scenario	DEBUG	failed to call ddns enable	ERROR
nimfAdvOptSetWrap: INDICATOR = %d	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: UpdateFlag: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: returning with status: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfGetUpdateMacFlag: MacTable Flag is: %d	DEBUG	Error in executing DB update handler	ERROR
nimfMacGet: Mac Option changed	DEBUG	Failed to open the resolv.conf file. Exiting./n	ERROR
nimfMacGet: Update Flag: %d	DEBUG	Could not write to the resolv.conf file. Exiting.	ERROR
nimfMacGet: MacAddress: %s	DEBUG	Error opening the lanUptime File	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
nimfMacGet: MacAddress: %s	DEBUG	Error Opening the lanUptime File.	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to open %s	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to open %s	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to query networkInterface table	ERROR
nimfMacGet:Mac option Not changed \	DEBUG	failed to query networkInterface table	ERROR
nimfMacGet: MacAddress: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to enable IPv6 forwarding	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to set capabilities on the "	ERROR
nimfMacGet: returning with status: %s	DEBUG	failed to enable IPv6 forwarding	ERROR
Now in enableing LanBridge function	DEBUG	failed to set capabilities on the "	ERROR
sucessfully executed the command %s	DEBUG	failed to disable IPv6 forwarding	ERROR
Now in disableing LanBridge function	DEBUG	failed to set capabilities on the "	ERROR
sucessfully executed the command %s	DEBUG	failed to open %s	ERROR
configPortTblHandler:Now we are in Sqlite Update "	DEBUG	Could not create ISATAP Tunnel	ERROR
The Old Configuration of ConfiPort was:%s	DEBUG	Could not destroy ISATAP Tunnel	ERROR
The New Configuration of ConfiPort was:%s	DEBUG	Could not configure ISATAP Tunnel	ERROR
The user has deselected the configurable port	DEBUG	Could not de-configure ISATAP Tunnel	ERROR
failed query %s	DEBUG	nimfStatusUpdate: updating NimfStatus failed	ERROR
failed query %s	DEBUG	nimfStatusUpdate: updating NimfStatus failed	ERROR
failed query %s	DEBUG	nimfLinkStatusGet: determinig link's status failed	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	nimfLinkStatusGet: opening status file failed	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	Failed to commit	ERROR
%s:%d SIP ENABLE: %s	DEBUG	ifStatusDBUpdate: Failed to begin "	ERROR
sipTblHandler:failed to update ifStatic	DEBUG	%s: SQL error: %s	ERROR
sipTblHandler:failed to update Configport	DEBUG	%s: Failed to commit "	ERROR
%s:%d SIP DISABLE: %s	DEBUG	nimfNetIfaceTblHandler: unable to get LedPinId	ERROR
%s:%d SIP SET CONF: %s	DEBUG	nimfNetIfaceTblHandler: unable to get LedPinId	ERROR
Failed to open %s: %s	DEBUG	nimfNetIfaceTblHandler: unable to get LedPinId	ERROR
Failed to start sipalg	DEBUG	%s: unable to kill dhclient	ERROR
Failed to stop sipalg	DEBUG	nimfAdvOptSetWrap: unable to get current Mac Option	ERROR
Failed to get config info	DEBUG	nimfAdvOptSetWrap: unable to get current Port "	ERROR
Network Mask: 0x%x	DEBUG	nimfAdvOptSetWrap: unable to get current MTU Option	ERROR
RTP DSCP Value: 0x%x	DEBUG	nimfAdvOptSetWrap: error getting Mac Address from "	ERROR
Need more arguments	DEBUG	nimfAdvOptSetWrap: unable to get the MTU	ERROR
Invalid lanaddr	DEBUG	nimfAdvOptSetWrap: error setting interface advanced "	ERROR
Invalid lanmask	DEBUG	nimfAdvOptSetWrap: error getting MTU size	ERROR
Invalid option	DEBUG	nimfAdvOptSetWrap: unable to get Mac Address	ERROR
Failed to set config info	DEBUG	nimfAdvOptSetWrap: error setting interface advanced "	ERROR
Unknown option	DEBUG	nimfAdvOptSetWrap: failed to get old connectiontype	ERROR
sshdTblHandler	DEBUG	nimfAdvOptSetWrap: old connection type is: %s	ERROR
pPort: %s	DEBUG	nimfAdvOptSetWrap: failed to get old MTU Option	ERROR
pProtocol: %s	DEBUG	nimfAdvOptSetWrap: error getting MTU size	ERROR
pListerAddr: %s	DEBUG	nimfOldFieldValueGet: failed to get old "	ERROR
pKeyBits: %s	DEBUG	nimfOldFieldValueGet: user has changed MTU size	ERROR
pRootEnable: %s	DEBUG	nimfAdvOptSetWrap: failed to get old Port Speed "	ERROR
pRsaEnable: %s	DEBUG	nimfAdvOptSetWrap: user has changed Port Speed	ERROR
pDsaEnable: %s	DEBUG	nimfAdvOptSetWrap: failed to get old Mac Address "	ERROR
pPassEnable: %s	DEBUG	nimfAdvOptSetWrap: user has changed Mac Address "	ERROR
pEmptyPassEnable: %s	DEBUG	nimfAdvOptSetWrap: unable to get Mac Address	ERROR
pSftpEnable: %s	DEBUG	nimfAdvOptSetWrap:Failed to RESET the flag	ERROR
pScpEnable: %s	DEBUG	nimfAdvOptSetWrap: setting advanced options failed	ERROR
pSshdEnable: %s	DEBUG	nimfAdvOptSetWrap: interface advanced options applied	ERROR
pPrivSep: %s	DEBUG	nimfGetUpdateMacFlag: unable to get Flag from MacTable	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	nimfMacGet: Updating MAC address failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Re-Starting sshd daemon....	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
sshd re-started successfully.	DEBUG	error executing the command %s	ERROR
sshd stopped .	DEBUG	error executing the command %s	ERROR
failed query %s	DEBUG	error executing the command %s	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	disableLan function is failed to disable ConfigPort"	ERROR
failed query %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
failed query %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
no ports present in this vlanId %d	DEBUG	Unable to Disable configurable port from	ERROR
failed query %s	DEBUG	configPortTblHandler has failed	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
disabling vlan	DEBUG	Error in executing DB update handler	ERROR
enabling vlan	DEBUG	sqlite3QueryResGet failed	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	Failed to execute switchConfig for port\	ERROR
no ports present in this vlanId %d	DEBUG	Failed to execute switchConfig for port enable	ERROR
failed query %s	DEBUG	Failed to execute ifconfig for port enable	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	Failed to execute ethtool for\	ERROR
removing %s from bridge%s... %s	DEBUG	Failed to execute switchConfig for port disable	ERROR
adding %s to bridge%d... %s	DEBUG	Failed to execute ifconfig for port disable	ERROR
restarting bridge...	DEBUG	sqlite3QueryResGet failed	ERROR
[switchConfig] Ignoring event on port number %d	DEBUG	sqlite3_mprintf failed	ERROR
restarting bridge...	DEBUG	sqlite3QueryResGet failed	ERROR
executing %s ... %s	DEBUG	Failed to execute switchConfig for port mirroring	ERROR
removing %s from bridge%s... %s	DEBUG	Usage:%s <DB Name> <Entry Name> <logFile> <subject>	ERROR
adding %s to bridge%d... %s	DEBUG	sqlite3QueryResGet failed	ERROR
[switchConfig] Ignoring event on %s	DEBUG	Could not get all the required variables to email the Logs.	ERROR
restarting bridge...	DEBUG	runSmtpClient failed	ERROR
[switchConfig] Ignoring event on port number %d	DEBUG	getaddrinfo returned %s	ERROR
[switchConfig] executing %s ... %s	DEBUG	file not found	ERROR
restarting bridge...	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
UserName: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Password: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
IspName: %s	DEBUG	No memory to allocate	ERROR
DialNumber: %s	DEBUG	Failed to Open SSHD Configuration File	ERROR
Apn: %s	DEBUG	Ipaddress should be provided with accessoption 1	ERROR
GetDnsFromIsp: %s	DEBUG	Subnetaddress should be provided with accessoption 2	ERROR
IdleTimeOutFlag: %s	DEBUG	Failed to restart sshd	ERROR
IdleTimeOutValue: %d	DEBUG	unable to open the "	ERROR
AuthMetho: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
executing %s ... %s	DEBUG	Error in executing DB update handler	ERROR
removing %s from bridge%d... %s	DEBUG	Error in executing DB update handler	ERROR
adding %s to bridge%d... %s	DEBUG	unknown vlan state	ERROR
stopping bridge...	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
restarting bridge...	DEBUG	sqlite3_mprintf failed	ERROR
Could not configure 6to4 Tunnel Interface	DEBUG	Access port can be present only in single vlan	ERROR
Could not de-configure 6to4 Tunnel Interface	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
failed to restart 6to4 tunnel interfaces	DEBUG	unknown vlan state	ERROR
BridgeConfig: too few arguments to command %s	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
BridgeConfig: unsupported command %d	DEBUG	Failed to clear vlan for oldPVID %d	ERROR
BridgeConfig returned error=%d	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
sqlite3QueryResGet failed	DEBUG	Failed to clear vlan for %d	ERROR
Error in executing DB update handler	DEBUG	Failed to set vlan entry for vlan %d	ERROR
sqlite3QueryResGet failed	DEBUG	Failed to set vlan entries, while enabling \	ERROR
Failed to remove vlan Interface for vlanId \	DEBUG	sqlite3QueryResGet failed	ERROR
sqlite3QueryResGet failed	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Invalid oidp passed	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
Invalid oidp passed	DEBUG	Failed to enable vlan	ERROR
Failed to get oid from the tree	DEBUG	Failed to disable vlan	ERROR
threegEnable: Input to wrapper %s	DEBUG	Failed to set vlanPort table entries, while \	ERROR
threegEnable: spawning command %s	DEBUG	Failed to enable vlan	ERROR
threegMgmtHandler: query string: %s	DEBUG	unknown vlan state	ERROR
threegMgmtHandler: returning with status: %s	DEBUG	Error in executing DB update handler	ERROR
adding to dhcprealy ifgroup failed	DEBUG	unknown vlan state	ERROR
adding to ipset fwDhcpRelay failed	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
Disabling Firewall Rule for DHCP Relay Protocol	DEBUG	sqlite3_mprintf failed	ERROR
Enabling Firewall Rule for DHCP Relay Protocol	DEBUG	Access port can be present only in single vlan	ERROR
prerouting Firewall Rule add for Relay failed	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
prerouting Firewall Rule add for Relay failed	DEBUG	unknown vlan state	ERROR
%s: SQL get query: %s	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
%s: sqlite3QueryResGet failed	DEBUG	Failed to clear vlan for oldPVID %d	ERROR
%s: no result found	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
%s: buffer overflow	DEBUG	Failed to clear vlan for %d	ERROR
%s: value of %s in %s table is: %s	DEBUG	Failed to set vlan entry for vlan %d	ERROR
%s: returning with status: %s	DEBUG	Failed to set vlan entries, while enabling \	ERROR
dnsResolverConfigure: addressFamily: %d	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
dnsResolverConfigure: LogicalIfName: %s	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
chap-secrets File found	DEBUG	Failed to enable vlan	ERROR
PID File for xl2tpd found	DEBUG	Failed to disable vlan	ERROR
pid: %d	DEBUG	Failed to set vlanPort table entries, while \	ERROR
options.xl2tpd file found	DEBUG	Failed to enable vlan	ERROR
options.xl2tpd file not found	DEBUG	unknown vlan state	ERROR
Conf File for xl2tpd found	DEBUG	threegMgmtInit: unable to open the database file %s	ERROR
xl2tpd.conf not found	DEBUG	threegConnEnable: failed to get the WanMode	ERROR
Chap Secrets file found	DEBUG	threegEnable:spawning failed	ERROR
Chap Secrets file not found	DEBUG	threegDisable: unable to kill ppp daemon	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	threegMgmtHandler: Query: %s	ERROR
chap-secrets File found	DEBUG	threegMgmtHandler: error in executing database update	ERROR
PID File for pptpd found	DEBUG	Error in executing DB update handler	ERROR
pid: %d	DEBUG	are we getting invoked twice ??	ERROR
PID File for pptpd interface found	DEBUG	could not open %s to append	ERROR
pid: %d	DEBUG	could not write nameserver %s to %s	ERROR
options.pptpd file found	DEBUG	could not write nameserver %s to %s	ERROR
options.pptpd file not found	DEBUG	could not open %s to truncate	ERROR
Conf File for pptpd found	DEBUG	dnsResolverConfigMgmtInit: unable to open the "	ERROR
pptpd.conf not found	DEBUG	resolverConfigDBUpateHandler: sqlite3QueryResGet "	ERROR
Chap Secrets file found	DEBUG	could not configure DNS resolver	ERROR
Chap Secrets file not found	DEBUG	dnsResolverConfigure: could not write nameserver:%s,"	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	unboundMgmt: unable to open the "	ERROR
chap-secrets File found	DEBUG	ioctl call Failed-could not update active user Details	ERROR
pppoeMgmtTblHandler: MtuFlag: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pppoeMgmtTblHandler: Mtu: %d	DEBUG	Can't kill xl2tpd	ERROR
pppoeMgmtTblHandler: IdleTimeOutFlag: %d	DEBUG	xl2tpd restart failed	ERROR
pppoeMgmtTblHandler: IdleTimeOutValue: %d	DEBUG	failed to get field value	ERROR
pppoeMgmtTblHandler: UserName: %s	DEBUG	failed to get field value	ERROR
pppoeMgmtTblHandler: Password: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pppoeMgmtTblHandler: DNS specified: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pppoeMgmtTblHandler: Service: %s	DEBUG	unboundMgmt: unable to open the "	ERROR
pppoeMgmtTblHandler: StaticIp: %s	DEBUG	writing options.xl2tpd failed	ERROR
pppoeMgmtTblHandler: NetMask: %s	DEBUG	xl2tpdStop failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
pppoeMgmtTblHandler: AuthOpt: %d	DEBUG	writing xl2tpd.conf failed	ERROR
pppoeMgmtTblHandler: Satus: %d	DEBUG	writing options.xl2tpd failed	ERROR
pppoeEnable: ppp dial string: %s	DEBUG	xl2tpdStop failed	ERROR
pppoeMgmtDBUpdateHandler: returning with status: %s	DEBUG	xl2tpdStart failed	ERROR
pptpMgmtTblHandler: MtuFlag: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pptpMgmtTblHandler: Mtu: %d	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pptpMgmtTblHandler: IdleTimeOutFlag: %d	DEBUG	xl2tpdStop failed	ERROR
pptpMgmtTblHandler: IdleTimeOutValue: %d	DEBUG	xl2tpdStart failed	ERROR
pptpMgmtTblHandler: GetDnsFromIsp: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pptpMgmtTblHandler: UserName: %s	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pptpMgmtTblHandler: Password: %s	DEBUG	xl2tpdStop failed	ERROR
pptpMgmtTblHandler: dynamic MyIp configured	DEBUG	xl2tpdStart failed	ERROR
pptpMgmtTblHandler: MyIp: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pptpMgmtTblHandler: ServerIp: %s	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pptpMgmtTblHandler: StaticIp: %s	DEBUG	Error in executing DB update handler	ERROR
pptpMgmtTblHandler: NetMask: %s	DEBUG	unboundMgmt: unable to open the "	ERROR
pptpMgmtTblHandler: MppeEncryptSupport: %s	DEBUG	Can't kill pptpd	ERROR
pptpMgmtTblHandler: SplitTunnel: %s	DEBUG	pptpd restart failed	ERROR
pptpEnable: ppp dial string: %s	DEBUG	Can't kill pptpd	ERROR
pptpEnable: spawning command %s	DEBUG	failed to get field value	ERROR
PID File for dhcpc found	DEBUG	failed to get field value	ERROR
pid: %d	DEBUG	unboundMgmt: unable to open the "	ERROR
pptpMgmtDBUpdateHandler: query string: %s	DEBUG	writing options.pptpd failed	ERROR
pptpMgmtDBUpdateHandler: returning with status: %s	DEBUG	pptpdStop failed	ERROR
dhcpcReleaseLease: dhcpc release command: %s	DEBUG	writing pptpd.conf failed	ERROR
dhcpcMgmtTblHandler: MtuFlag: %d	DEBUG	writing options.pptpd failed	ERROR
dhcpcMgmtTblHandler: Mtu: %d	DEBUG	pptpdStop failed	ERROR
DHCPv6 Server started successfully.	DEBUG	pptpdStart failed	ERROR
DHCPv6 Server stopped successfully	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
DHCPv6 Client started successfully.	DEBUG	Error in executing DB update handler	ERROR
DHCPv6 Client stopped successfully.	DEBUG	pppStatsUpdate: unable to get default MTU	ERROR
DHCPv6 Client Restart successful	DEBUG	pppoeMgmtInit: unable to open the database file %s	ERROR
l2tpMgmtTblHandler: MtuFlag: %d	DEBUG	pppoeDisable: unable to kill ppp daemon	ERROR
l2tpMgmtTblHandler: Mtu: %d	DEBUG	pppoeMultipleEnableDisable: pppoe enable failed	ERROR
l2tpMgmtTblHandler: IspName: %s	DEBUG	pppoeMultipleEnableDisable: pppoe disable failed	ERROR
l2tpMgmtTblHandler: UserName: %s	DEBUG	pppoeMgmtTblHandler: unable to get current Mtu Option	ERROR
l2tpMgmtTblHandler: Password: %s	DEBUG	pppoeMgmtTblHandler: unable to get the Mtu	ERROR
l2tpMgmtTblHandler: AccountName: %s	DEBUG	pppoeMgmtTblHandler: pppoe enable failed	ERROR
l2tpMgmtTblHandler: DomainName: %s	DEBUG	pppoeMgmtDBUpdateHandler: failed query: %s	ERROR
l2tpMgmtTblHandler: Secret: not specified	DEBUG	pppoeMgmtDBUpdateHandler: error in executing "	ERROR
l2tpMgmtTblHandler: Secret: %s	DEBUG	pptpMgmtInit: unable to open the database file %s	ERROR
l2tpMgmtTblHandler: dynamic MyIp configured	DEBUG	pptpEnable: error executing command: %s	ERROR
l2tpMgmtTblHandler: MyIp: %s	DEBUG	pptpEnable: unable to resolve address: %s	ERROR
l2tpMgmtTblHandler: ServerIp: %s	DEBUG	pptpEnable: inet_aton failed	ERROR
l2tpMgmtTblHandler: StaticIp: %s	DEBUG	pptpEnable: inet_aton failed	ERROR
l2tpMgmtTblHandler: NetMask: %s	DEBUG	pptpEnable:spawning failed	ERROR
l2tpMgmtTblHandler: SplitTunnel: %s	DEBUG	pptpDisable: unable to kill ppp daemon	ERROR
needToStartHealthMonitor: returning with status: %s	DEBUG	pptpMgmtTblHandler: unable to get current MTU Option	ERROR
l2tpEnable: command string: %s	DEBUG	pptpMgmtTblHandler: unable to get the Mtu	ERROR
l2tpEnable: command: %s	DEBUG	pptpMgmtTblHandler: dbRecordValueGet failed for %s "	ERROR
l2tpEnable: command string: %s	DEBUG	pptpMgmtTblHandler: pptp enable failed	ERROR
PID File for dhcpc found	DEBUG	pptpMgmtTblHandler: pptp disable failed	ERROR
pid: %d	DEBUG	pptpMgmtDBUpdateHandler: sqlite3QueryResGet "	ERROR
l2tpMgmtDBUpdateHandler: query string: %s	DEBUG	pptpMgmtDBUpdateHandler: error in executing "	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
l2tpMgmtDBUpdateHandler: returning with status: %s	DEBUG	Illegal invocation of dhcpConfig (%s)	ERROR
RADVD started successfully	DEBUG	dhcpLibInit: unable to open the database file %s	ERROR
RADVD stopped successfully	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
empty update. nRows=%d nCols=%d	WARN	dhcpcMgmtInit: unable to open the database file %s	ERROR
Wan is not up or in load balencing mode	WARN	dhcpcReleaseLease: unable to release lease	ERROR
threegMgmtHandler: no row found. nRows = %d nCols = %d	WARN	dhcpcEnable: unable to kill dhclient	ERROR
pppoeMgmtDBUpdateHandler: empty update.	WARN	dhcpcEnable: enabling dhcpc failed on: %s	ERROR
dhcpcEnable: dhclient already running on: %s	WARN	dhcpcDisable: unable to kill dhclient	ERROR
dhcpcDisable: deleted dhclient.leases	WARN	dhcpcDisable: delete failed for dhclient.leases	ERROR
l2tpMgmtInit: unable to open the database file %s	ERROR	dhcpcDisable: failed to reset the ip	ERROR
l2tpEnable: unable to resolve address: %s	ERROR	dhcpcMgmtTblHandler: unable to get current Mtu Option	ERROR
l2tpEnable: inet_aton failed	ERROR	dhcpcMgmtTblHandler: unable to get the Mtu	ERROR
The Enable Command is %s	ERROR	dhcpcMgmtTblHandler: dhclient enable failed	ERROR
l2tpEnable:Executing the Command failed	ERROR	dhcpcMgmtTblHandler: dhcpc release failed	ERROR
l2tpDisable: command string: %s	ERROR	dhcpcMgmtTblHandler: dhcpc disable failed	ERROR
l2tpDisable: unable to stop l2tp session	ERROR	dhcpcMgmtDBUpdateHandler: failed query: %s	ERROR
l2tpMgmtTblHandler: unable to get current MTU option	ERROR	dhcpcMgmtDBUpdateHandler: error in executing "	ERROR
l2tpMgmtTblHandler: unable to get the Mtu	ERROR	DHCPv6 Client start failed.	ERROR
l2tpMgmtTblHandler: dbRecordValueGet failed for %s "	ERROR	DHCPv6 Client stop failed.	ERROR
l2tpMgmtTblHandler: l2tpEnable failed	ERROR	failed to create/open DHCPv6 client "	ERROR
l2tpMgmtTblHandler: disabling l2tp failed	ERROR	failed to write DHCPv6 client configuration file	ERROR
l2tpMgmtDBUpdateHandler: sqlite3QueryResGet "	ERROR	failed to restart DHCPv6 Client	ERROR
l2tpMgmtDBUpdateHandler: error in executing	ERROR	failed to create/open DHCPv6 Server "	ERROR
Illegal invocation of tcpdumpConfig (%s)	ERROR	Restoring old configuration..	ERROR
Failed to start tcpdump	ERROR	DHCPv6 Server configuration update failed	ERROR
Failed to stop tcpdump	ERROR	DHCPv6 Server Restart failed	ERROR
Invalid tcpdumpEnable value	ERROR	sqlite3QueryResGet failed.Query:%s	ERROR

■ ファシリティ：システム（VPN）

ログメッセージ	緊急度	ログメッセージ	緊急度
%d command not supported by eapAuth	DEBUG	PEAP key derive: ERROR	ERROR
pCtx NULL.	DEBUG	PEAP context is NULL: ERROR	ERROR
Current cert subject name= %s	DEBUG	Constructing P2 response: ERROR	ERROR
X509_STORE_CTX_get_ex_data failed.	DEBUG	innerEapRecv is NULL: ERROR	ERROR
Cannot get cipher, no session est.	DEBUG	Decrypting TLS data: ERROR	ERROR
%s: SSL_ERROR_WANT_X509_LOOKUP	DEBUG	Wrong identity size: ERROR	ERROR
err code = (%d) in %s	DEBUG	Wrong size for extensions packet: ERROR	ERROR
BIO_write: Error	DEBUG	innerEapRecv is NULL: ERROR.	ERROR
Decrypting: BIO reset failed	DEBUG	Inner EAP processing: ERROR	ERROR
Encrypting BIO reset: ERROR	DEBUG	TLS handshake: ERROR.	ERROR
BIO_read: Error	DEBUG	Sending P1 response: ERROR	ERROR
EAP state machine changed from %s to %s.	DEBUG	Unexpected tlsGlueContinue return value.	ERROR
EAP state machine changed from %s to %s.	DEBUG	No more fragments in message. ERROR	ERROR
Received EAP Packet with code %d	DEBUG	No phase 2 data or phase 2 data buffer NULL: ERROR	ERROR
Response ID %d	DEBUG	Allocating memory for PEAP Phase 2 payload: ERROR	ERROR
Response Method %d	DEBUG	TLS encrypting response: ERROR	ERROR
Created EAP/PEAP context: OK	DEBUG	Setting message in fragment buffer: ERROR	ERROR
Deleted EAP/PEAP context: OK	DEBUG	Allocating TLS read buffer is NULL: ERROR	ERROR
Upper EAP sent us: decision = %d method state = %d	DEBUG	Setting last fragment: ERROR	ERROR
P2 decision=(%d); methodState=(%d)	DEBUG	Getting message: ERROR	ERROR
Writing message to BIO: ERROR.	DEBUG	Processing PEAP message: ERROR	ERROR
Encrypted (%d) bytes for P2	DEBUG	Setting fragment: ERROR	ERROR
P2: sending fragment.	DEBUG	Creating receive buffer: ERROR	ERROR
P2: message size = %d	DEBUG	Setting first fragment: ERROR	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
P2: sending unfragmented message.	DEBUG	Sending P1 response: ERROR	ERROR
P1: Sending fragment.	DEBUG	NULL request (or response) PDU or NULL context: ERROR	ERROR
P1: Total TLS message size = (%d)	DEBUG	Expecting start packet, got something else: ERROR	ERROR
P1: sending unfragmented message.	DEBUG	Protocol version mismatch: ERROR	ERROR
peapFragFirstProcess: TLS record size to receive = (%d)	DEBUG	Processing PEAP message (from frag): ERROR	ERROR
Setting version %d	DEBUG	Processing PEAP message: ERROR	ERROR
PEAP pkt rcvd: data len=(%d) flags=(%d) version=(%d)	DEBUG	Processing PEAP message: ERROR	ERROR
Got PEAP/Start packet.	DEBUG	Indicated length not valid: ERROR	ERROR
Got first fragment	DEBUG	Did not get Acknowledged result: ERROR	ERROR
Got fragment (n)	DEBUG	Cannot understand AVP value: ERROR	ERROR
Got last fragment	DEBUG	eapExtResp is NULL: ERROR	ERROR
Got unfragmented message	DEBUG	eapWscCtxCreate: EAPAUTH_MALLOC failed.	ERROR
Got frag ack.	DEBUG	eapWscProcess: umiloctl req to WSC failed, status = %d	ERROR
Ext AVP parsed: flags=(0x%x)	DEBUG	eapWscCheck: Invalid frame	ERROR
Mandatory bit not set: WARNING	DEBUG	eapWscBuildReq: Invalid state %d	ERROR
Ext AVP parsed: type=(%d)	DEBUG	eapWscProcessWscResp: Invalid data recd pData = %p, dataLen"	ERROR
Ext AVP parsed: value=(%d)	DEBUG	Data received for invalid context, dropping it	ERROR
Got PEAPv0 success!	DEBUG	eapWscProcessWscResp: Build Request failed	ERROR
Got PEAPv0 failure!	DEBUG	eapWscProcessWscResp: Invalid state %d	ERROR
pCtx NULL.	DEBUG	eapWscProcessWscResp: Message processing failed 0x%X	ERROR
Authenticator response check: Error	DEBUG	eapWscProcessWscData: Invalid notification recd %d	ERROR
Authenticator response check: Failed	DEBUG	unable to initialize MD5	ERROR
MS-CHAP2 Response AVP size = %u	DEBUG	MDString: adpDigestInit for md5 failed	ERROR
Created EAP/MS-CHAP2 context: OK.	DEBUG	EAPAUTH_MALLOC failed.	ERROR
pCtx NULL.	DEBUG	EAPAUTH_MALLOC failed.	ERROR
Deleted EAP/MS-CHAPv2 context: OK	DEBUG	NULL context created: Error	ERROR
Not authenticated yet.	DEBUG	NULL context received: Error	ERROR
Authenticator response invalid	DEBUG	Authenticator ident invalid.	ERROR
EAP-MS-CHAPv2 password changed.	DEBUG	Success request message invalid: Error	ERROR
rcvd. opCode %d.	DEBUG	Plugin context is NULL	ERROR
pCtx NULL.	DEBUG	Deriving implicit challenge: Error	ERROR
TLS message len changed in the fragment, ignoring.	DEBUG	Generating NT response: Error	ERROR
no data to send while fragment ack received.	DEBUG	NULL in/out buffer: Error	ERROR
TLS handshake successful.	DEBUG	Incorrect vendor id.	ERROR
Created EAP/TTLS context: OK	DEBUG	Allocating memory for outBuff: ERROR	ERROR
Deleted EAP/TTLS context: OK	DEBUG	AVP code not recognized	ERROR
No more fragments in message. ERROR	DEBUG	EAPAUTH_MALLOC failed.	ERROR
Upper EAP sent us: method state = %d; decision = %d	DEBUG	Converting password to unicode: Error	ERROR
P2: sending fragment.	DEBUG	Generating password hash: Error.	ERROR
P2 send unfragmented message.	DEBUG	Generating password hash hash: Error.	ERROR
P1: sending fragment.	DEBUG	Generating master key: Error.	ERROR
P1: sending unfragmented message.	DEBUG	Generating first 16 bytes of session key: Error.n	ERROR
\tTLSMsgLen = 0x%x	DEBUG	Generating second 16 bytes of session key: Error.n	ERROR
Send req ptr = 0x%x; Send resp ptr = 0x%x	DEBUG	Converting password to unicode: Error	ERROR
P2 decision=(%d); methodState=(%d)	DEBUG	Constructing failure response: ERROR	ERROR
Default EAP: method state = %d; decision = %d	DEBUG	Error checking authenticator response.	ERROR
TTLS pkt: data len=(%d) flags=(0x%x)	DEBUG	Error generating NT response.	ERROR
Got start	DEBUG	Username string more than 256 ASCII characters: ERROR	ERROR
Got first fragment (n).	DEBUG	Invalid Value-Size.	ERROR
Got fragment (n).	DEBUG	Invalid MS-Length. Got (%d), expected (%d)	ERROR
Got last fragment	DEBUG	Error constructing response.	ERROR
Got unfragmented message.	DEBUG	Got type (%d), expecting (%d)	ERROR
Got frag ack.	DEBUG	Cannot handle message; opCode = %d	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Rcvd. AVP Code-%u: flags-0x%x: len- %u: vendorId-%u: "	DEBUG	EAPAUTH_MALLOC failed.	ERROR
MOD EAP: method state from upper = %d; decision = %d	DEBUG	tlsGlueCtxCreate failed.	ERROR
Got AVP len = %ul. Should be less than 16777215	DEBUG	client certificate must be set in the profile.	ERROR
AVP length extract: Error	DEBUG	received tls message length too big.	ERROR
pFB is NULL	DEBUG	total frags len > initial total tls length.	ERROR
Requesting message before assembly complete	DEBUG	total frags len > initial total tls length.	ERROR
pFB is NULL	DEBUG	total data rcvd(%d) doesnt match the initial "	ERROR
pFB is NULL	DEBUG	couldnt write %d data to TLS buffer.	ERROR
Buffer cannot hold message: ERROR	DEBUG	invalid flags %s passed to eapTlsBuildResp.	ERROR
pFB is NULL: Error	DEBUG	EAPAUTH_MALLOC failed.	ERROR
pFB is NULL	DEBUG	tlsGlueCtxCreate failed.	ERROR
TLS_FB* is NULL.	DEBUG	Context NULL: ERROR	ERROR
pFB->msgBuff is NULL.	DEBUG	Setting profile to glue layer: ERROR.	ERROR
Error calculating binary.	DEBUG	_eapCtxCreate failed.	ERROR
Error calculating binary.	DEBUG	%d authentication not enabled in the system.	ERROR
adpDigestInit for SHA1 failed.	DEBUG	Initializing inner non-EAP auth plugin: ERROR	ERROR
adpDigestInit for SHA1 failed.	DEBUG	TTLS key derive: ERROR	ERROR
E = %d	DEBUG	TTLS context from EAP plugin is NULL: ERROR	ERROR
R = %d	DEBUG	Allocating memory for TTLS Phase 2 payload: ERROR	ERROR
Could not initialize des-ecb	DEBUG	TLS Encrypting response: ERROR	ERROR
adpDigestInit for MD4 failed.	DEBUG	Allocating TLS read buffer is NULL: ERROR	ERROR
adpDigestInit for SHA1 failed.	DEBUG	Inner authentication (id: %d) unhandled	ERROR
adpDigestInit for SHA1 failed.	DEBUG	innerEapRecv is NULL: ERROR.	ERROR
Error converting received auth reponse to bin.	DEBUG	Decrypting TLS data: ERROR	ERROR
Gnerating challenge hash: Error	DEBUG	Processing Phase 2 method: Error	ERROR
Generating password hash: Error	DEBUG	Writing message to BIO: ERROR.	ERROR
Generating challenge response: Error	DEBUG	TLS handshake: ERROR.	ERROR
Conn cipher name=%s ver=%s: %s	DEBUG	Unexpected tlsGlueContinue return value.	ERROR
Send req ptr = 0x%x; Send resp ptr = 0x%x	DEBUG	NULL request (or response) PDU or NULL context	ERROR
Request ptr = 0x%x;	DEBUG	Protocol version mismatch: ERROR	ERROR
Response ptr = 0x%x	DEBUG	Creating receive buffer: ERROR	ERROR
Rcvd. AVP Code - %ul	DEBUG	Setting first fragment: ERROR	ERROR
Rcvd. AVP flags - 0x%02x	DEBUG	Setting fragment: ERROR	ERROR
Rcvd. AVP len - %ul	DEBUG	Setting last fragment: ERROR	ERROR
Rcvd. AVP vendor id - %ul	DEBUG	Getting message: ERROR	ERROR
\tCode = %d	DEBUG	Processing TTLS message: ERROR	ERROR
\tIdent = %d	DEBUG	Processing TTLS message: ERROR	ERROR
\tLen = %d	DEBUG	Processing TTLS message: ERROR	ERROR
\tType = %d	DEBUG	Decapsulating AVP: ERROR	ERROR
\tOpCode = %d	DEBUG	Processing EAP receive: Error	ERROR
\tMSID = %d	DEBUG	AVP code not EAP: Error	ERROR
\tmsLen = %d	DEBUG	Encapsulating AVP: ERROR	ERROR
\tvalSize = %d	DEBUG	profile %s doesnt exist.	ERROR
Frag Buffer bytes left = (%d)	DEBUG	profile %s is in use.	ERROR
Stripped username=(%s)	DEBUG	profile %s already exists.	ERROR
digestLen = %d.	DEBUG	EAPAUTH_MALLOC failed	ERROR
ClearText =	DEBUG	User not found.	ERROR
CipherText =	DEBUG	EAP-MD5 not enabled in system configuration.	ERROR
digestLen = %d.	DEBUG	EAP-MSCHAPV2 not enabled in system configuration.	ERROR
digestLen1 = %d.	DEBUG	EAP-TLS not enabled in system configuration.	ERROR
digestLen2 = %d.	DEBUG	EAP-TTLS not enabled in system configuration.	ERROR
password change is not allowed for this user	DEBUG	EAP-PEAP not enabled in system configuration.	ERROR
completed writing the policy	DEBUG	EAP-WSC not enabled in system configuration.	ERROR
completed writing the SA	DEBUG	PAP not enabled in system configuration.	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
completed writing the proposal block	DEBUG	CHAP not enabled in system configuration.	ERROR
cmdBuf: %s	DEBUG	MSCHAP not enabled in system configuration.	ERROR
X509_DEBUG : Invalid Certificate for the generated"	DEBUG	MSCHAPV2 not enabled in system configuration.	ERROR
X590_ERROR : Failed to create File '%s'	DEBUG	PAP/Token not enabled in system configuration.	ERROR
x509TblHandler	DEBUG	EAP-MD5 not enabled in system configuration.	ERROR
pCertType: %s	DEBUG	EAP-MSCHAPV2 not enabled in system config.	ERROR
pRowQueryStr: %s	DEBUG	EAP-TLS not enabled in system configuration.	ERROR
x509SelfCertTblHandler	DEBUG	EAP-TTLS and EAP-PEAP are not valid as inner"	ERROR
pRowQueryStr: %s	DEBUG	invalid innerAuth %d.	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	profile %s doesnt exist.	ERROR
umiRegister failed	ERROR	Re-assembling fragments incorrect size	ERROR
eapAuthHandler: Invalid data received	ERROR	Error creating cipher context.	ERROR
EAPAUTH_MALLOC failed.	ERROR	Error initializing cipher context.	ERROR
malloc failed.	ERROR	Error creating digest context.	ERROR
BIO_new_mem_buf failed.	ERROR	Error initializing digest context.	ERROR
malloc failed.	ERROR	Error initializing DES in Klite	ERROR
BIO_new_mem_buf failed.	ERROR	Error initializing MD4 in Klite	ERROR
SSL_CTX_new (TLSv1_client_method) failed.	ERROR	Error initializing RC4 in Klite	ERROR
unable to set user configured CIPHER list %s	ERROR	Error initializing SHA in Klite	ERROR
Certificate verification failed.	ERROR	Error cleaning cipher context.	ERROR
Server name match failed. Got (%s) expected "	ERROR	Error destroying cipher context.	ERROR
SSL_CTX_use_certificate_file (cert, PEM) failed.	ERROR	Error cleaning digest context.	ERROR
SSL_CTX_use_PrivateKey_file failed.	ERROR	Error destroying digest context.	ERROR
private key does not match public key	ERROR	Error stripping domain name.	ERROR
SSL_CTX_load_verify_locations failed	ERROR	Error cleaning digest context.	ERROR
SSL_new failed.	ERROR	Error cleaning digest context.	ERROR
Both SSL_VERIFY_PEER and SSL_VERIFY_NONE set: Error	ERROR	Challenge not present in failure packet.	ERROR
EAPAUTH_MALLOC failed.	ERROR	Wrong challenge length.	ERROR
EAPAUTH_MALLOC failed.	ERROR	Incorrect password change version value.	ERROR
eapTimerCreate failed.	ERROR	Error generating password hash.	ERROR
eapCtxDelete:pCtx == NULL	ERROR	Error generating password hash.	ERROR
eapRole != EAP_ROLE_PEER or EAP_ROLE_AUTHENTICATOR	ERROR	Error encrypting password hash with block	ERROR
pEapCtx == NULL or pPDU == NULL.	ERROR	Could not initialize des-ecb	ERROR
received EAP pdu bigger than EAP_MTU_SIZE.	ERROR	Error cleaning cipher context.	ERROR
received EAP pdu bigger than EAP_MTU_SIZE.	ERROR	Error cleaning cipher context.	ERROR
state machine is in invalid state.	ERROR	Error cleaning digest context.	ERROR
unable to create method context.	ERROR	Error cleaning digest context.	ERROR
method ctxCreate failed.	ERROR	adpDigestInit for SHA1 failed.	ERROR
method profile set failed.	ERROR	X509_ERROR : .Query:%s	ERROR
state machine is in invalid state.	ERROR	X509_ERROR : Invalid Certificate for the "	ERROR
Only StandAlone authenticator supported currently.	ERROR	invalid x509 certificate	ERROR
state machine is in invalid state.	ERROR	Couldn't get the x509 cert hash	ERROR
BuildReq operation failed	ERROR	Memory allocation failed	ERROR
No method ops defined for current method	ERROR	FileName too lengthy	ERROR
Process operation failed	ERROR	Couldn't execute command	ERROR
state machine is in invalid state.	ERROR	Memory allocation failed	ERROR
Packet length mismatch %d, %d	ERROR	Memory allocation failed	ERROR
eapAuthTypeToType: Invalid eapAuthType %d	ERROR	invalid certificate data	ERROR
eapTypeToAuthType: Invalid eapType %d	ERROR	.Query:%s	ERROR
unable to create method context.	ERROR	.Query:%s	ERROR
method ctxCreate failed.	ERROR	Memory allocation failed	ERROR
Invalid condition, methodState = %d, respMethod = %d	ERROR	X509_ERROR : Failed to validate the certficate "	ERROR
A EAP Ctx map already exists	ERROR	Memory allocation failed	ERROR
eapTimerCreate: Currently unsupported for Peer role	ERROR	.Query:%s	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
eapTimerStart: Currently unsupported for Peer role	ERROR	Invalid Sign Key Length : %d	ERROR
eapTimerDestroy: Currently unsupported for Peer role	ERROR	Invalid Hash Alg : %d	ERROR
eapTimerCancel: Currently unsupported for Peer role	ERROR	Invalid Sign Alg : %d	ERROR
eapTimerHandler: Currently unsupported for Peer role	ERROR	No Memory Available	ERROR
pCtx is NULL: ERROR	ERROR	Certificate Request Failed	ERROR
tlsGlueCtxCreate failed	ERROR	File Open Failed	ERROR
eapVars is NULL	ERROR	File is Empty	ERROR
Context NULL: ERROR	ERROR	Memory Allocation Failed	ERROR
Initializing inner EAP auth: ERROR	ERROR	File Open Failed	ERROR
pCtx is NULL: ERROR	ERROR	File is Empty	ERROR
Memory Allocation Failed	ERROR	Error in executing DB update handler	ERROR

■ ファシリティ：システム（Admin）

ログメッセージ	緊急度	ログメッセージ	緊急度
Usage:%s <DBFile>	DEBUG	unable to register to UMI	ERROR
Could not open database: %s	DEBUG	sqlite3QueryResGet failed	ERROR
CPU LOG File not found	DEBUG	radSendtoServer: socket: %s	ERROR
MEM LOG File not found	DEBUG	radSendtoServer: bind() Failed: %s: %s	ERROR
cpuMemUsageDBUpdateHandler: update query: %s	DEBUG	radRecvfromServer: recvfrom() Failed: %s	ERROR
Printing the whole list after inserting	DEBUG	radRecvfromServer: Packet too small from %s:%d: %s	ERROR
%s at %d(minute) %d(hour) %d(dayOfMonth) %d(month)"	DEBUG	radCheckMsgAuth: Invalid Message- Authenticator length in"	ERROR
adpCmdExec exited with return code=%d	DEBUG	radDictLoad: couldn't open dictionary %s: %s	ERROR
%s op=%d row=%d	DEBUG	radBuildAndSendReq: Invalid Request Code %d	ERROR
sqlite3_mprintf failed	DEBUG	radPairAssign: bad attribute value length	ERROR
sqlite3QueryResGet failed: query=%s	DEBUG	radPairAssign: unknown attribute type %d	ERROR
Printing the whole list after delete	DEBUG	radPairNew: unknown attribute %d	ERROR
%s at %d(minute) %d(hour) %d(dayOfMonth) %d(month)"	DEBUG	radPairGen: Attribute(%d) has invalid length	ERROR
Printing the whole list after inserting	DEBUG	radPairValue: unknown attribute type %d	ERROR
%s at %d(minute) %d(hour) %d(dayOfMonth) %d(month)"	DEBUG	radPairValueLen: unknown attribute type %d	ERROR
email logs: No logging events enabled	DEBUG	radPairLocate: Attribute(%d) has invalid length	ERROR
%s	DEBUG	radPairUnpackDefault: Unknown- Attribute[%d]:	ERROR
Mail sent and the Database is reset.	DEBUG	radConfigure: can't open %s: %s	ERROR
Disabled syslog server	DEBUG	radConfigure: %s: line %d: bogus format: %s	ERROR
Event logs are full, sending logs to email	DEBUG	radConfAssert: No AuthServer Specified	ERROR
Email logs sending failed	DEBUG	radConfAssert: No Default Timeout Specified	ERROR
Packing attribute: %s	DEBUG	radConfAssert: No Default Retry Count Specified	ERROR
Server found: %s, secret: %s	DEBUG	radExtractMppeKey: Invalid MSMPPE- Key Length	ERROR
Packed Auth. Reqest: code:%d, id:%d, len:%d	DEBUG	radVendorMessage: Invalid Length in Vendor Message	ERROR
Sending Packet to %x:%d	DEBUG	radVendorMessage: Unknown Vendor ID received:%d	ERROR
Receiving Reply Packet....	DEBUG	radVendorAttrGet: Invalid Length in Vendor Message	ERROR
Verified Reply Packet Integrity	DEBUG	radVendorAttrGet: Unknown Vendor ID:%d	ERROR
Generated Reply Attribute-Value pairs	DEBUG	radVendorMessagePack: Unknown Vendor ID:%d	ERROR
Verified Message-Authenticator	DEBUG	radGetIPByName: couldn't resolve hostname: %s	ERROR
Unloaded RADIUS Dictionary	DEBUG	radGetHostIP: couldn't get hostname	ERROR
Adding Dictionary Attribute %s	DEBUG	radGetHostIP: couldn't get host IP address	ERROR
Adding Dictionary Value %s	DEBUG	radius dictionary loading failed	ERROR
Loaded Dictionary %s	DEBUG	Failed to set default timeout value	ERROR
Adding Dictionary Attribute '%s'	DEBUG	Failed to set default retries value	ERROR
Adding Dictionary Value %s	DEBUG	ERROR: incomplete DB update information.	ERROR
Receiving attribute: %s	DEBUG	old values result does not contain 2 rows	ERROR
Processing attribute: %s	DEBUG	sqlite3QueryResGet failed	ERROR
Processing attribute: %s	DEBUG	empty update. nRows=%d nCols=%d	ERROR
Processing attribute: %s	DEBUG	Error in executing DB update handler	ERROR
Processing attribute: %s	DEBUG	sqlite3QueryResGet failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
radConfGet: "	DEBUG	Invalid SQLITE operation code - %d	ERROR
Added Server %s:%d with "	DEBUG	sqlite3QueryResGet failed	ERROR
Added Server %s:%d with "	DEBUG	empty result. nRows=%d nCols=%d	ERROR
Default Timeout Set to %d	DEBUG	sqlite3QueryResGet failed	ERROR
Default Retry Count Set to %d	DEBUG	empty result. nRows=%d nCols=%d	ERROR
%s - %s : %d	DEBUG	RADIUS Accounting Exchange Failed	ERROR
Deleting Server %s:%d with "	DEBUG	Unable to set debug for radAcct.	ERROR
Adding RowId:%d to Server %s:%d with "	DEBUG	Unable to set debug level for radAcct.	ERROR
rowIds: %d - %d	DEBUG	ERROR: option value not specified	ERROR
Deleting Server %s:%d with "	DEBUG	ERROR: option value not specified	ERROR
RADIUS Deconfigured	DEBUG	Unable to initialize radius	ERROR
Found Option %s on line %d of file %s	DEBUG	radEapMsgQueueAdd: Invalid EAP packet length(%d)	ERROR
Setting Option %s with value %s	DEBUG	radEapRecvTask: invalid EAP code:%d	ERROR
RADIUS Configured	DEBUG	radEapRecvTask: Packet length mismatch %d, %d	ERROR
%d : Server %s:%d with "	DEBUG	No attributes received in Access- Challenge message	ERROR
DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	No State Attribute in Access- Challenge message	ERROR
Host IP address: %s	DEBUG	radEapRecvTask: "	ERROR
Adding Packet for existing cookie:%p	DEBUG	failed to initialize UMI	ERROR
Adding Packet and cookie:%p	DEBUG	umiRegister failed. errno=%d	ERROR
Releasing Packet and cookie:%p	DEBUG	Invalid arguments to ioctl handler	ERROR
Releasing Packet with cookie:%p	DEBUG	radEapSendRtn: Invalid Arguments	ERROR
Received EAP-Identity from Pnac: %s	DEBUG	radEapSendRtn: failed to allocate buffer	ERROR
Filling User-Name: %s	DEBUG	umiIoctl failed	ERROR
Filling State:	DEBUG	failed to initialize EAP message queue	ERROR
Filling EAP-Message:	DEBUG	Unable to set debug for radEap.	ERROR
Filling Service-Type: %d	DEBUG	Unable to set debug level for radEap.	ERROR
Filling Framed-MTU: %d	DEBUG	ERROR: option value not specified	ERROR
Received Access-Challenge from Server	DEBUG	ERROR: option value not specified	ERROR
Sending Reply EAP Packet to Pnac	DEBUG	could not initialize MGMT framework	ERROR
Error sending packet to Pnac	DEBUG	Unable to initialize radius	ERROR
RADIUS Authentication Failed; "	DEBUG	Unable to set debug for radEap.	ERROR
RADIUS Authentication Successful; "	DEBUG	Unable to set debug level for radEap.	ERROR
Got Packet with cookie:%p	DEBUG	ERROR: option value not specified	ERROR
Next DNS Retry after 1 min	DEBUG	Unable to initialize radius	ERROR
Next Synchronization after"	DEBUG	Invalid username or password	ERROR
Next Synchronization after"	DEBUG	Unable to set debug for radAuth.	ERROR
Next Synchronization after %d \	DEBUG	Unable to set debug level for radAuth.	ERROR
Primary is not available, "	DEBUG	ERROR: option value not specified	ERROR
Secondary is not available, "	DEBUG	Unable to initialize radius	ERROR
Invalid value for use default servers, "	DEBUG	Invalid username, challenge or response	ERROR
No server is configured, "	DEBUG	Unable to set debug for radAuth.	ERROR
Backing off for %d seconds	DEBUG	Unable to set debug level for radAuth.	ERROR
Requesting time from %s	DEBUG	ERROR: option value not specified	ERROR
Synchronized time with %s	DEBUG	Unable to initialize radius	ERROR
Received KOD packet from %s	DEBUG	Invalid username or password	ERROR
No suitable server found %s	DEBUG	usage : %s <DB fileName>	ERROR
Received Invalid Length packet from %s	DEBUG	ntpd : umi initialization failed	ERROR
Received Invalid Version packet from %s	DEBUG	ntpd : ntpInit failed	ERROR
Received Invalid Mode packet from %s	DEBUG	ntpd : ntpMgmtInit failed	ERROR
Request Timed out from %s	DEBUG	There was an error while getting the timeZoneChangeScript."	ERROR
Looking Up %s	DEBUG	unexpected reply from %d cmd=%d !	ERROR
Timezone difference :%d	DEBUG	cmd %d not supported. caller %d	ERROR
Could not open file: %s	DEBUG	default reached	ERROR
Could not read data from file	DEBUG	Unable to initialize ntpControl	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
ntpTblHandler	DEBUG	ntpMgmt : Couldn't open database %s	ERROR
status: %d	DEBUG	ERROR : incomplete DB update information	ERROR
tz: %d	DEBUG	empty update. nRows=%d nCols=%d	ERROR
DayLightsaving: %d	DEBUG	Error in executing DB update handler	ERROR
pNtpControl- >ServerNames[PRIMARY_SERVER]: %s	DEBUG	requestNtpTime: Invalid addr	ERROR
pNtpControl- >ServerNames[SECONDARY_SERVER] : %s	DEBUG	failed to take lock for compId: %d	ERROR
DS: %d	DEBUG	failed to convert ioctl args to buffer for"	ERROR
pPriServ %s	DEBUG	request timeout dst(%d) <-- src(%d)	ERROR
pSecServ %s	DEBUG	failed to take lock for compId: %d	ERROR
Making request from %d --> %d	DEBUG	umiloctlArgsToBuf: failed to allocate memory	ERROR
sent request dst(%d) <-- src(%d) using option %d	DEBUG	umiRecvFrom: could not allocate memory	ERROR
received request too small!(%d bytes)	DEBUG	adpMalloc failed	ERROR
Received a UMI request from %d	DEBUG	context with ID: %d already registered	ERROR
sent a reply src(%d) ---> dst(%d)	DEBUG	Failed to allocate memory for creating UMI context	ERROR
umiRegister (%x,%x,%x,%x)	DEBUG	Failed to create recvSem for UMI context	ERROR
srcId=%d(%s) --> destId=%d(%s) cmd=%d inLen=%d outLen=%d	DEBUG	Failed to create mutex locks for UMI context	ERROR
waiting for reply...Giving Up	DEBUG	Failed to create mutex recvQLock for UMI context	ERROR
No request in the list after semTake	DEBUG	Invalid arguments to umiloctl	ERROR
reply timeout	DEBUG	could not find the destination context	ERROR
timeout after semTake	DEBUG	memPartAlloc for %d size failed	ERROR
srcId=%d(%s) <-- destId=%d(%s) cmd=%d	DEBUG	memPartAlloc for %d size failed	ERROR
Un-registerting component with Id %d	DEBUG	No Handler registered for this UMI context	ERROR
failed to send ioctl request: dst(%d) <--- src(%d)	DEBUG	Couldn't find component with ID (%d),"	ERROR
processed a reply dst(%d) <-- src(%d)	DEBUG	id=%d handler=%x	ERROR
request with no result option dst(%d) <-- src(%d)	DEBUG	Received NULL buffer in umiBufToIoctlArgs()	ERROR
cmd = %s	DEBUG	usbMgmtInit: unable to open the database file %s	ERROR
cmdstring is %s %s:%d	DEBUG	call to printConfig failed	ERROR
Calling printerConfig binary ...	DEBUG	Failed to Disable Network Storage" ERROR	
Calling unmount for USB ...	DEBUG	Some error occurred while removing device	ERROR
Calling mount for USB ...	DEBUG	Some error occurred while removing device	ERROR
usbdevice is %d %s:%d	DEBUG	Sqlite update failed	ERROR
Query string: %s	DEBUG	Failed to enable printer properly	ERROR
sqlite3QueryResGet failed.Query:%s	DEBUG	Failed to mount device on system	ERROR
%s: 1. usb is already disconnected for old usb type. "	DEBUG	Failed to enable network storage device"	ERROR
%s: 2.call disable for new usb type !	DEBUG	Failed to mount device on system	ERROR
%s: 3. usb is already disconnected for old usb type. "	DEBUG	Sqlite update failed	ERROR
%s: 4. Disabled old usb type . Now "	DEBUG	USB1 Touch failed	ERROR
usbdevice is %d %s:%d	DEBUG	USB2 Touch failed	ERROR
USB: failed to begin transaction: %s	DEBUG	Sqlite update failed	ERROR
USB: SQL error: %s pSetString = %s	DEBUG	Failed query: %s	ERROR
USB: failed to commit transaction: %s	DEBUG	Failed to execute usb database update handler	ERROR
USB: updated table: %s	DEBUG	Usage:%s <DBFile> <opType> <tblName> <rowId>	ERROR
USB: returning with status: %s	DEBUG	Illegal invocation of snmpConfig (%s)	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	Invalid Community Access Type	ERROR
executing %s status =%d	DEBUG	Invalid User Access Type	ERROR
executing %s	DEBUG	Invalid Security Level	ERROR
%s returned status=%d	DEBUG	Invalid Authentication Algorithm	ERROR
%s returned status=%d	DEBUG	Invalid Privacy Algorithm	ERROR
snmpd.conf not found	DEBUG	Invalid Argument	ERROR
[SNMP_DEBUG] : Fwrite Successful	DEBUG	Failed to allocate memory for engineID	ERROR
[SNMP_DEBUG] : Fwrite failed	DEBUG	[SNMP_DEBUG]: Failed to get host address	ERROR
radPairGen: received unknown attribute %d of length %d	WARN	[SNMP_DEBUG] : FOPEN failed	ERROR
radPairGen: %s has unknown type	WARN	sqlite3QueryResGet failed.Query:%s	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
radPairLocate: unknown attribute %ld of length %d	WARN	sqlite3QueryResGet failed.Query:%s	ERROR
radPairLocate: %s has unknown type	WARN	Invalid Security Level	ERROR
Illegal invocation of cpuMemUsage (%s)	ERROR	Invalid Authentication Algorithm	ERROR
cpuMemUsageDBUpdateHandler: SQL error: %s	ERROR	Invalid Privacy Algorithm	ERROR
unable to open the DB file %s	ERROR	Failed to Get Host Address	ERROR
umiInit failed	ERROR	Invalid version	ERROR
unable to register to UMI	ERROR	snmp v3 Trap Configuration Failed	ERROR
Error Reading from the Database.	ERROR	sqlite3QueryResGet failed query:%s	ERROR
short DB update event request!	ERROR	sqlite3QueryResGet failed.Query:%s	ERROR
Error in executing DB update handler	ERROR	Failed to Open Snmp Configuration File	ERROR
adpListNodeRemove : Returned with an error	ERROR	Failed to write access control entries	ERROR
command too long. Try increasing "	ERROR	Failed to write snmpv3 users entries	ERROR
failed to allocate memory for CRON_NODE	ERROR	Failed to write snmp trap entries	ERROR
sqlite3QueryResGet failed	ERROR	Failed to write system entries.	ERROR
There was an error while reading the schedules.	ERROR	Failed to restart snmp	ERROR
unable to register to UMI	ERROR	%s failed with status	ERROR
short DB update event request!	ERROR	Error in executing DB update handler	ERROR
malloc(DB_UPDATE_NODE) failed	ERROR	%s: Unable to open file: %s	ERROR
short ifDev event request!	ERROR	RADVD start failed	ERROR
sqlite3_mprintf failed	ERROR	RADVD stop failed	ERROR
no component id matching %s	ERROR	failed to create/open RADVD configuration file %s	ERROR
umiIoctl (%s, UMI_CMD_DB_UPDATE(%d)) failed.	ERROR	Restoring old configuration..	ERROR
sqlite3_mprintf failed	ERROR	failed to write/update RADVD configuration file	ERROR
sqlite3_mprintf failed	ERROR	upnpDisableFunc failed	ERROR
no component id matching %s	ERROR	upnpEnableFunc failed	ERROR
umiIoctl (%s, UMI_CMD_IFDEV_EVENT(%d)) failed.	ERROR	sqlite3QueryResGet failed.Query:%s	ERROR
klogctl(9) failed	ERROR	Error in executing DB update handler	ERROR
malloc failed for %d bytes	ERROR	unable to open the DB file %s	ERROR
klogctl(4) failed	ERROR	umiInit failed	ERROR
emailLogs: Invalid Number of Arguments!! Exiting.	ERROR	unable to register to UMI	ERROR
sqlite3QueryResGet failed	ERROR	short DB update event request!	ERROR
Could not execute the smtpClient.	ERROR	short ifDev event request!	ERROR
Error while cleaning the database.Exiting. %s	ERROR	sqlite3_mprintf failed	ERROR
		%s failed. status=%d	ERROR

■ ファシリティ：システム（Firewall）

ログメッセージ	緊急度	ログメッセージ	緊急度
Enabling rule for protocol binding.	DEBUG	Disable all NAT rules.	DEBUG
Disabling rule for protocol binding.	DEBUG	Enable all NAT rules.	DEBUG
Enabling Remote SNMP on WAN.	DEBUG	Enabling NAT URL filter rules.	DEBUG
Disabling Remote SNMP on WAN	DEBUG	Restarting all NAT rules.	DEBUG
wan traffic counters are restared	DEBUG	Deleting schedule based firewall rules.	DEBUG
Traffic limit has been reached	DEBUG	Deleting schedule based firewall rules from DB.	DEBUG
Traffic meter monthly limit has been changed to %d.	DEBUG	Update schedule based firewall rules in DB.	DEBUG
Enabling traffic meter for only dowload.	DEBUG	Restart schedule based firewall rules.	DEBUG
Enabling traffic meter for both directions.	DEBUG	inter vlan routing enabled	DEBUG
Enabling traffic meter with no limit.	DEBUG	inter vlan routing disabled	DEBUG
Email alert in traffic meter disabled.	DEBUG	Disabling Content Filter for %d	DEBUG
Email alert in traffic meter enabled.	DEBUG	Enabling Content Filter for %d	DEBUG
Traffic Meter:Monthly limit %d MB has been "	DEBUG	./src/firewall/linux/user/firewalld.c:59:#u ndef ADP_DEBUG2	DEBUG
Traffic Metering: Adding rule to drop all traffic	DEBUG	./src/firewall/linux/user/firewalld.c:61:#d efine ADP_DEBUG2 printf	DEBUG
Traffic Metering: %sabling Email traffic	DEBUG	Enabling Source MAC Filtering	DEBUG
Disabling attack checks for IPv6 rules.	DEBUG	Disabling Source MAC Filtering	DEBUG
Enabling attack checks for IPv6 rules.	DEBUG	Adding MAC Filter Policy for Block & Permit Rest	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
Configuring one to one NAT settings with %s private start IP "	DEBUG	Adding MAC Filter Policy for Permit & Block Rest	DEBUG
Deleting forward one to one NAT having setting %s private start"	DEBUG	Restarting Source MAC Address Policy	DEBUG
Disabling attack check for Block ping to WAN interface.	DEBUG	Disabling Firewall Rule for DHCP Relay Protocol	DEBUG
Disabling attack check for Stealth mode for tcp	DEBUG	Enabling Firewall Rule for DHCP Relay Protocol	DEBUG
Disabling attack check for Stealth mode for udp	DEBUG	prerouting Firewall Rule add for Relay failed	DEBUG
Disabling attack check for TCP Flood.	DEBUG	prerouting Firewall Rule add for Relay failed	DEBUG
Disabling attack check for UDP Flood.	DEBUG	Deleting MAC Filter Policy for Address %s	DEBUG
Disabling attack check for IPSec.	DEBUG	Adding MAC Filter Policy for Address %s	DEBUG
Disabling attack check for PPTP.	DEBUG	Disabling Firewall Rules for DMZ host	DEBUG
Disabling attack check for L2TP.	DEBUG	Enabling Firewall Rules for DMZ host	DEBUG
Disabling attack check for UDP Flood.	DEBUG	Disabling Firewall Rules for Spill Over Load Balancing	DEBUG
Disabling attack check for IPSec.	DEBUG	Disabling Firewall Rules for Load Balancing	DEBUG
Disabling attack check for PPTP.	DEBUG	Enabling Firewall Rules for Load Balancing	DEBUG
Disabling attack check for L2TP.	DEBUG	Enabling Firewall Rules for Spill Over Load Balancing	DEBUG
Enabling attack check for Block ping to WAN "	DEBUG	Enabling Firewall Rules for Auto Failover	DEBUG
Enabling attack check for Stealth Mode for tcp.	DEBUG	Enabling Firewall Rules for Load Balancing .	DEBUG
Enabling attack check for Stealth Mode for udp.	DEBUG	Enabling Firewall Rules for Spill Over Load Balancing .	DEBUG
Enabling attack check for TCP Flood.	DEBUG	Enabling Firewall Rules for Auto Failover	DEBUG
Enabling attack check for UDP Flood.	DEBUG	Deleting BlockSites Keyword \	DEBUG
Enabling attack check for IPSec.	DEBUG	Enabling BlockSites Keyword \	DEBUG
Enabling attack check for PPTP.	DEBUG	Disabling BlockSites Keyword \	DEBUG
Enabling attack check for L2TP.	DEBUG	Updating BlockSites Keyword from \	DEBUG
Enabling attack check for UDP Flood.	DEBUG	Inserting BlockSites Keyword \	DEBUG
Enabling attack check for IPSec.	DEBUG	Deleting Trusted Domain \	DEBUG
Enabling attack check for PPTP.	DEBUG	Adding Trusted Domain \	DEBUG
Enabling attack check for L2TP.	DEBUG	Restarting Schedule Based Firewall Rules	DEBUG
Enabling DoS attack check with %d SyncFlood detect rate, "	DEBUG	Enabling Remote SNMP	DEBUG
Disabling DoS attack check having %d SyncFlood detect rate,"	DEBUG	Disabling Remote SNMP	DEBUG
Enabling ICSA Notification Item for ICMP notification.	DEBUG	Enabling Remote SNMP	DEBUG
Enabling ICSA Notification Item for Fragmented Packets.	DEBUG	Disabling DOS Attacks	DEBUG
Enabling ICSA Notification Item for Multi cast Packets.	DEBUG	Enabling DOS Attacks	DEBUG
Disabling ICSA Notification Item for ICMP notification.	DEBUG	Enabling DOS Attacks	DEBUG
Disabling ICSA Notification Item for Fragmented Packets.	DEBUG	Restarting Firewall [%d]:[%d] For %s	DEBUG
Disabling ICSA Notification Item for Multicast Packets.	DEBUG	restartStatus = %d for LogicalIfName = %s	DEBUG
Adding IP/MAC binding rule for %s MAC address "	DEBUG	Deleting Lan Group %s	DEBUG
Deleting IP/MAC binding rule for %s MAC "	DEBUG	Adding Lan Group %s	DEBUG
./src/firewall/linux/user/firewalld.c:60:#un def ADP_DEBUG	DEBUG	Deleting lan host %s from group %s	DEBUG
./src/firewall/linux/user/firewalld.c:62:#def ine ADP_DEBUG printf	DEBUG	Adding lan host %s from group %s	DEBUG
Restarting traffic meter with %d mins, %d hours, "	DEBUG	Disabling Firewall Rule for IGMP Protocol	DEBUG
Updating traffic meter with %d mins, %d hours, "	DEBUG	Enabling Firewall Rule for IGMP Protocol	DEBUG
Deleting traffic meter.	DEBUG	Deleting IP/MAC Bind Rule for MAC address %s and IP "	DEBUG
Disabling block traffic for traffic meter.	DEBUG	Adding IP/MAC Bind Rule for MAC address %s and IP	DEBUG
Enabling traffic meter.	DEBUG	Deleting Protocol Bind Rule for Service %s	DEBUG
Adding lan group %s.	DEBUG	Deleting Protocol Bind Rule for Service %s	DEBUG
Deleting lan group %s.	DEBUG	Deleting Protocol Bind Rule for Service %s	DEBUG
Renaming lan group from %s to %s.	DEBUG	Adding Protocol Bind Rule for Service %s	DEBUG
Deleting host %s from %s group.	DEBUG	%s Session Settings	DEBUG
Adding host %s to %s group.	DEBUG	Restarting IPv6 Firewall Rules...	DEBUG
Enabling Keyword blocking for %s keyword.	DEBUG	Deleting Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Disabling keyword Blocking for %s keyword .	DEBUG	Deleting Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Deleting trusted domain with keyword %s.	DEBUG	Enabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Adding %s keyword to trusted domain.	DEBUG	Disabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
Enabling Management Access from Internet on port	DEBUG	Enabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Enabling remote access management for IP address range"	DEBUG	Disabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Enabling remote access management to only this PC.	DEBUG	Adding Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Disabling Management Access from Internet on port %d	DEBUG	Enabling Content Filter	DEBUG
Disabling remote access management for IP address range"	DEBUG	Disabling Content Filter	DEBUG
Disabling remote access management only to this PC.	DEBUG	Enabling Content Filter	DEBUG
MAC Filtering %sabled for BLOCK and PERMIT REST.	DEBUG	Setting NAT mode for pLogicalIfName = %s	DEBUG
MAC Filtering %sabled for PERMIT and BLOCK REST.	DEBUG	Enabling DROP for INPUT	DEBUG
Enabling Content Filtering.	DEBUG	Enabling DROP for FORWARD	DEBUG
Disabling Content Filtering.	DEBUG	Enabling NAT based Firewall Rules	DEBUG
Deleting rule, port triggering for protocol TCP.	DEBUG	Setting transparent mode for pLogicalIfName \	DEBUG
Deleting rule, port triggering for protocol UDP.	DEBUG	Enabling Accept for INPUT	DEBUG
Deleting rule, port triggering for protocol TCP.	DEBUG	Enabling Accept for FORWARD	DEBUG
Deleting rule, port triggering for protocol UDP.	DEBUG	Setting Routing mode for pLogicalIfName \	DEBUG
Enabling rule, port triggering for protocol TCP.	DEBUG	Enabling DROP for INPUT	DEBUG
Enabling rule, port triggering for protocol UDP.	DEBUG	Enabling DROP for FORWARD	DEBUG
Enabling rule, port triggering for protocol TCP.	DEBUG	Disabling NAT based Firewall Rules	DEBUG
Enabling rule, port triggering for protocol UDP.	DEBUG	Enabling Firewall Rules for URL Filtering & "	DEBUG
Enabling DNS proxy.	DEBUG	Adding Firewall Rule for RIP Protocol	DEBUG
Restarting DNS proxy.	DEBUG	Restarting Schedule Based Firewall Rules	DEBUG
checking DNS proxy for Secure zone.	DEBUG	enabling IPS checks between %s and %s zones.	DEBUG
checking DNS proxy for Public zone.	DEBUG	disabling IPS checks between %s and %s zones.	DEBUG
Enabling Block traffic from %s zone.	DEBUG	Stopping IPS...%s	DEBUG
Configuring firewall session settings for "	DEBUG	IPS started.	DEBUG
Disabling DMZ	DEBUG	Route already exists	DEBUG
Disabling WAN-DMZ rules .	DEBUG	Route addition failed: Network Unreachable	DEBUG
Enabling WAN DMZ rules .	DEBUG	Route addition failed: Network is down	DEBUG
Restarting DMZ rule having %s address with %s address.	DEBUG	Route addition failed	DEBUG
Enabling LAN DHCP relay.	DEBUG	Failed to add rule in iptables	DEBUG
OneToOneNat configured successfully	DEBUG	Failed to delete rule from iptables	DEBUG
OneToOneNat configuration failed	DEBUG	fwLBSpillOverConfigure: Something going wrong here	ERROR
Deleting scheduled IPv6 rules.	DEBUG	fwLBSpillOverConfigure: unable to get interfaceName	ERROR
delete from FirewallRules6 where ScheduleName = '%s'.	DEBUG	fwLBSpillOverConfigure: Could not set PREROUTING rules	ERROR
Update FirewallRules6 where ScheduleName = '%s' to New "	DEBUG	fwLBSpillOverConfigure: Could not set POSTROUTING rules	ERROR
Dns proxy Restart failed	DEBUG	fwLBSpillOverConfigure: Something going wrong Here	ERROR
deleting interface to ifgroup failed	DEBUG	fwL2TPGenericRules.c: unable to open the database file "	ERROR
adding interface to ifgroup failed	DEBUG	fwL2TPGenericRules.c: inet_aton failed	ERROR
deleting interface pVirtIface %s from ifgroup %d"	DEBUG	fwPPTPGenericRules.c: unable to open the database file "	ERROR
adding interface pVirtIface %s to ifgroup %d failed	DEBUG	fwPPTPGenericRules.c: inet_aton failed	ERROR
Deleting IP address %s.	DEBUG	DNS proxy firewall rule add failed for %s	ERROR
Adding new IP address %s.	DEBUG	deleting interface %s from ifgroup %d failed	ERROR
Updating old IP address %s to new IP address %s.	DEBUG	adding interface %s to ifgroup %d failed	ERROR
Restarting Firewall For %s Address Update from %s:%s	DEBUG	nimfBridgeTblHandler: unable to get interfaceName	ERROR
Disabling Firewall Rule for MSS packet marking	DEBUG	nimfBridgeTblHandler: \	ERROR
Enabling Firewall Rule for MSS packet marking	DEBUG	nimfBridgeTblHandler: unable to get \	ERROR
Enabling packet marking rule for %s IDLE timer	DEBUG	Failed to %s traffic from %s to %s to IPS.	ERROR
Deleted firewall rule %s for service %s with action %s	DEBUG	Failed to %s traffic from %s to %s to IPS.	ERROR
%s firewall rule %s for service %s with action %s	DEBUG	failed to start IPS service.	ERROR
Added firewall rule %s for service %s with action %s	DEBUG	Timeout in waiting for IPS service to start.	ERROR
Deleting inbound(WAN-LAN) firewall rule.	DEBUG	Usage:%s <DBFile> <opType> <tblName> <rowId> "	ERROR
Deleting inbound(WAN-DMZ) firewall rule.	DEBUG	xlr8NatConfig: illegal invocation of (%s)	ERROR
RIPng disabled.	DEBUG	Illegal invocation of [%s]	ERROR
RIPng enabled.	DEBUG	xlr8NatMgmtTblHandler: failed query: %s	ERROR
Disable IPv6 firewall rule.	DEBUG	Could not open file: %s	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Enable IPv6 firewall rule.	DEBUG	Rip Error Command Too Long	ERROR
Deleting IGMP proxy rule.	DEBUG	No authentication for Ripv1	ERROR
Enable IGMP proxy rule.	DEBUG	Invalid Rip Direction	ERROR
Restarting IGMP rule.	DEBUG	Invalid Rip Version	ERROR
Traffic meter enabled with no limit type.	DEBUG	Invalid Password for 1st Key	ERROR
Traffic meter enabled for only download.	DEBUG	Invalid Time for 1st Key	ERROR
Traffic meter enabled for both directions.	DEBUG	Invalid Password for 2nd Key	ERROR
Deleted firewall rule %s for service %s with action %s	DEBUG	Invalid Time for 2nd Key	ERROR
%s firewall rule %s for service %s with action %s	DEBUG	Invalid First KeyId	ERROR
Added firewall rule %s for service %s with action %s	DEBUG	Invalid Second KeyId	ERROR
Enabling Inter VLAN routing.	DEBUG	Invalid Authentication Type	ERROR
Updating inter VLAN routing status.	DEBUG	ripDisable failed	ERROR
Deleting inter VLAN routing.	DEBUG	ripEnable failed	ERROR

■ ファシリティ：システム（無線）

ログメッセージ	緊急度	ログメッセージ	緊急度
(node=%s) setting %s to val = %d	DEBUG	sqlite3QueryResGet failed	ERROR
Custom wireless event: '%s'	DEBUG	sqlite3QueryResGet failed	ERROR
Wireless event: cmd=0x%x len=%d	DEBUG	VAP(%s) set beacon interval failed	ERROR
New Rogue AP (%02x:%02x:%02x:%02x:%02x:%02x) detected	DEBUG	VAP(%s) set DTIM interval failed	ERROR
WPS session in progress, ignoring enrolle assoc request	DEBUG	VAP(%s) set RTS Threshold failed	ERROR
ran query %s	DEBUG	VAP(%s) set Fragmentation Threshold failed	ERROR
DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	VAP(%s) set Protection Mode failed	ERROR
%sing VAPs using profile %s	DEBUG	VAP(%s) set Tx Power failed	ERROR
%sing VAP %s	DEBUG	WDS Profile %s not found	ERROR
ran query %s	DEBUG	Failed to initalize WPS on %s	ERROR
%sing VAP instance %s	DEBUG	failed to get profile %s	ERROR
VAP(%s) set Short Preamble failed	DEBUG	could not initialize MGMT framework	ERROR
VAP(%s) set Short Retry failed	DEBUG	could not initialize MGMT framework	ERROR
VAP(%s) set Long Retry failed	DEBUG	dot11VapBssidUpdt SQL error: %s	ERROR
Decrypting context with key %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Unknown IAPP command %d received.	DEBUG	KDOT11_GET_PARAM(IEEE80211_I OC_CHANNEL) failed	ERROR
unexpected reply from %d cmd=%d !	DEBUG	Failed to get the channel setting for %s	ERROR
unexpected reply from %d cmd=%d !	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Recvied DOT11_EAPOL_KEYMSG	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
shutting down AP:%s	DEBUG	profile %s not found	ERROR
APCtx Found	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
APCtx Not-Found	DEBUG	Interface name and policy must be specified	ERROR
node not found *:*:*:%x:%x:%x	DEBUG	Interface name and policy must be specified	ERROR
error installing unicast key for %s	DEBUG	invalid ACL type %d	ERROR
cmd =%d i_type =%d i_val=%d	DEBUG	interface name not specified	ERROR
join event for new node %s	DEBUG	interface name not specified	ERROR
wpa/rsn IE id %d/%d not supported	DEBUG	Invalid interface - %s specified	ERROR
wpa IE id %d not supported	DEBUG	buffer length not specified	ERROR
leave event for node %s	DEBUG	Invalid length(%d) specified	ERROR
NodeFree request for node : %s	DEBUG	failed created iappdLock	ERROR
installing key to index %d	DEBUG	failed to create cipher contexts.	ERROR
iReq.i_val : %d	DEBUG	unable to register to UMI	ERROR
plfName : %s	DEBUG	iappSockInit() failed	ERROR
iReq.i_val : %d	DEBUG	iappInit got error, unregistering it with UMI	ERROR
setting mode: %d	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) failed	ERROR
Global counter wrapped, re-generating...	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) failed	ERROR
Got PNAC_EVENT_PREAUTH_SUCCESS event for : %s	DEBUG	UDP failed, received Length is %d	ERROR
event for non-existent node %s	DEBUG	umiloctl(UMI_COMP_KDOT11,	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
PNAC_EVENT_EAPOL_START event received	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) \	ERROR
PNAC_EVENT_EAPOL_LOGOFF event received	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) \	ERROR
PNAC_EVENT_REAUTH event received	DEBUG	No IAPP Node found for req id %d	ERROR
PNAC_EVENT_AUTH_SUCCESS event received	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) \	ERROR
PNAC_EVENT_PORT_STATUS_CHAN GED event received	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) \	ERROR
unsupported event %d from PNAC	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) failed	ERROR
event for non-existent node %s. Create new node.	DEBUG	UDP socket is not created	ERROR
Add new node to DOT11 Node list	DEBUG	UDP send failed	ERROR
Update dot11STA database	DEBUG	IAPP: socket (SOCK_STREAM) failed.	ERROR
Add PMKSA to the list	DEBUG	IAPP: TCP connect failed to %s.	ERROR
eapolRecvAuthKeyMsg: received key message	DEBUG	cmd %d not supported.sender=%d	ERROR
node not found	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) failed	ERROR
eapolRecvKeyMsg: replay counter not incremented	DEBUG	IAPP-CACHE-NOTIFY-REQUEST send to	ERROR
eapolRecvKeyMsg: replay counter is not same	DEBUG	./src/dot11/iapp/iappLib.c:1314: ADP_ERROR (	ERROR
processing pairwise key message 2	DEBUG	BSSID value passed is NULL	ERROR
RSN IE matching: OK	DEBUG	reserved requestId is passed	ERROR
processing pairwise key message 4	DEBUG	interface name is NULL	ERROR
processing group key message 2	DEBUG	IP address value passed is NULL	ERROR
processing key request message from client	DEBUG	opening receive UDP socket failed	ERROR
WPA version %2x %2x not supported	DEBUG	enabling broadcast for UDP socket failed	ERROR
(%s) group cipher %2x doesn't match	DEBUG	opening receive TCP socket for new AP failed	ERROR
(%s)Pairwise cipher %s not supported	DEBUG	./src/dot11/iapp/iappLib.c:1784: ADP_ERROR(	ERROR
(%s) authentication method %d not supported	DEBUG	./src/dot11/iapp/iappLib.c:1794: ADP_ERROR(	ERROR
%s:Auth method=%s pairwise cipher=%s IE size=%d	DEBUG	./src/dot11/iapp/iappLib.c:1803: ADP_ERROR(	ERROR
WPA version %2x %2x not supported	DEBUG	failed created dot11dLock.	ERROR
Unable to obtain IE of type %d	DEBUG	failed initialize profile library.	ERROR
PTK state changed from %s to %s	DEBUG	failed to create cipher contexts.	ERROR
using PMKSA from cache	DEBUG	unable to register to UMI	ERROR
PTK GK state changed from %s to %s	DEBUG	could not create MIB tree	ERROR
GK state changed from %s to %s	DEBUG	unable to register to PNAC	ERROR
Sending PTK Msg1	DEBUG	Max registration attempts by DOT11 to PNAC exceeded	ERROR
Sending PTK Msg3	DEBUG	Creation of EAP WPS Profile Failed	ERROR
Sending GTK Msg1	DEBUG	umiloctl(UMI_COMP_IAPP,%d) failed	ERROR
sending EAPOL pdu to PNAC...	DEBUG	DOT11_RX_EAPOL_KEYMSG: unknown ifname %s	ERROR
creating pnac authenticator with values %d %d - %s	DEBUG	cmd %d not supported.sender=%d	ERROR
Profile %s does not exist	DEBUG	inteface name passed is NULL	ERROR
IAPP initialized.	DEBUG	BSSID passed is NULL	ERROR
Encrypting context key=%s for	DEBUG	inteface name passed is NULL	ERROR
could not find access point context for %s	DEBUG	unable to allocate memory for DOT11_CTX	ERROR
join event for existing node %s	DEBUG	unable to install wme mapping on %s	ERROR
failed to send PNAC_FORCE_AUTHORIZED "	DEBUG	unable to get %s mac address	ERROR
failed to send PNAC_AUTHORIZED "	DEBUG	Failed to set %s SSID	ERROR
failed to send PNAC_VAR_KEY_AVAILABLE (TRUE) "	DEBUG	Failed to set SSID broadcast status	ERROR
failed to send PNAC_VAR_KEY_TX_EN (TRUE) "	DEBUG	Failed to set PreAuth mode	ERROR
failed to send PNAC_VAR_KEY_TX_EN (FALSE) "	DEBUG	unable to install key	ERROR
failed to send PNAC_FORCE_AUTHORIZED "	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_AUTHMODE failed	ERROR
failed to send PNAC_AUTHORIZED "	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_PRIVACY failed	ERROR
mic verification: OK	DEBUG	wpaInit failed	ERROR
pnacIfConfig: Invalid supplicant"	DEBUG	dot11InstallProfile: unable to get interface index	ERROR
Failed to process user request	DEBUG	adpHmacInit(%s) failed	ERROR
Failed to process user request - %s(%d)	DEBUG	interface %s not found	ERROR
pnacIfConfigUmiloctl: umiloctl failed	DEBUG	AP not found on %s	ERROR
pnacIfConfigUmiloctl: usrPnac returned %d	DEBUG	keyLen > PNAC_KEY_MAX_SIZE	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
pnacIfConfigUmiIoctl: usrPnac returned %d	DEBUG	Invalid profile name passed	ERROR
pnacIfConfigUmiIoctl: usrPnac returned %d	DEBUG	Creation of WPS EAP Profile failed	ERROR
pnacKernNotifier: invalid PAE configuration "	DEBUG	unsupported command %d	ERROR
From pnacEapDemoAuthRecv: unsupported response "	DEBUG	device %s not found	ERROR
From pnacEapDemoAuthRecv: invalid codes received	DEBUG	unsupported command %d	ERROR
From pnacRadXlateDemoRecv: received unknown "	DEBUG	dot11NodeAlloc failed	ERROR
From pnacRadXlateDemoRecv: invalid codes received	DEBUG	Getting WPA IE failed for %s	ERROR
Error from pnacRadXlateDemoRecv: malloc failed	DEBUG	Getting WPS IE failed for %s	ERROR
From pnacRadXlateRadPktHandle: received a non-supported"	DEBUG	Failed initialize authenticator for node %s	ERROR
Only md5 authentication scheme currently supported. "	DEBUG	Failed to get the system up time while adding node %s	ERROR
Message from authenticator:	DEBUG	error creating PNAC port for node %s	ERROR
from pnacPDUXmit: bufsize = %d, pktType = %d,"	DEBUG	dot11NodeAlloc failed	ERROR
pnacPDUXmit: sending eap packet. code = %d, "	DEBUG	Invalid arguments.	ERROR
pnacRecvRtn: no corresponding pnac port pae found	DEBUG	umiIoctl(UMI_COMP_IAPP,%d) failed	ERROR
sending unicast key	DEBUG	Invalid IE.	ERROR
sending broadcast key	DEBUG	umiIoctl(UMI_COMP_KDOT11_VAP, %d) failed	ERROR
from pnacAuthPAEDisconnected: calling pnacTxCannedFail	DEBUG	umiIoctl(UMI_COMP_KDOT11,%d ,%d) failed	ERROR
from pnacAuthPAEForceUnauth: calling pnacTxCannedFail	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_CWMIN failed	ERROR
state changed from %s to %s	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_CWMAX failed	ERROR
PNAC user comp id not set. dropping event %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_AIFS failed	ERROR
sending event %d to %d	DEBUG	KDOT11_SET_PARAM:80211_IOC_WME_TXOPLIMIT failed	ERROR
requesting keys informantion from %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_ACM failed	ERROR
pnacUmiPortPaeParamSet: error in getting port pae	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME failed	ERROR
pnacUmiPortPaeParamSet: invalid param - %d	DEBUG	invalid group cipher %d	ERROR
pnacRecvASInfoMessage: Skey of length %d set	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_MCASTCIPHER failed	ERROR
pnacRecvASInfoMessage: reAuthPeriod set to: %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_MCASTKEYLEN failed	ERROR
pnacRecvASInfoMessage: suppTimeout set to: %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_UCASTCIPHERS failed	ERROR
PORT SUCCESSFULLY DESTROYED	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_KEYMGTALGS failed	ERROR
creating physical port for %s	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WPA failed	ERROR
pnacAuthInit: using defualt pnacAuthParams	DEBUG	unknow cipher type = %d	ERROR
pnacSuppInit: using defualt pnacSuppParams	DEBUG	umiIoctl(UMI_COMP_IAPP,%d) failed	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	invalid media value=%d	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	invalid mediaOpt value=%d	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	invalid mode value=%d	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	dot11PnacIfCreate failed	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	wpaPRF failed	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	Error generating global key counter	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	wpaCalcMic: unsupported key descriptor version	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	integrity failed. need to stop all stations "	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	couldn't find AP context for %s interface	ERROR
received a pdu on %s	DEBUG	dot11Malloc failed	ERROR
pnacRecvMapi: protoType: %04x pPhyPort-> authToASSendRtn:%p	DEBUG	dot11Malloc failed	ERROR
port not found	DEBUG	eapolRecvKeyMsg: unknown descType =%d	ERROR
from pnacRecvMapi: pkt body len = %d, pktType = %d	DEBUG	eapolRecvKeyMsg: invalid descriptor version	ERROR
from pnacPDUProcess: received PNAC_EAP_PACKET	DEBUG	eapolRecvKeyMsg: incorrect descriptor version	ERROR
from pnacPDUProcess: currentId = %d	DEBUG	eapolRecvKeyMsg: Ack must not be set	ERROR
from pnacPDUProcess: code = %d, identifier = %d, "	DEBUG	eapolRecvKeyMsg: MIC bit must be set	ERROR
from pnacPDUProcess: setting rxResp true	DEBUG	wpaAuthRecvPTKMsg2: unexpected packet received	ERROR
from pnacPDUProcess: code = %d, identifier = %d, "	DEBUG	wpaAuthRecvPTKMsg2: mic check failed	ERROR
from pnacPDUProcess: received "	DEBUG	wpaAuthRecvPTKMsg2: rsn ie mismatch	ERROR
from pnacPDUProcess: received "	DEBUG	wpaAuthRecvPTKMsg4: unexpected packet received	ERROR
from pnacPDUProcess: received PNAC_EAPOL_KEY_PACKET	DEBUG	wpaAuthRecvPTKMsg4: keyDataLength not zero	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
doing pnacTxCannedFail	DEBUG	wpaAuthRecvPTKMsg4: mic check failed	ERROR
doing pnacTxCannedSuccess	DEBUG	wpaAuthRecvGTKMsg2: unexpected packet received	ERROR
doing pnacTxReqId	DEBUG	secureBit not set in GTK Msg2	ERROR
doing pnacTxReq	DEBUG	wpaAuthRecvGTKMsg2: keyDataLength not zero	ERROR
doing pnacTxStart	DEBUG	wpaAuthRecvGTKMsg2: mic check failed	ERROR
doing pnacTxLogoff	DEBUG	wpaAuthRecvKeyReq: unexpected packet received	ERROR
doing pnacTxRspId: 1st cond	DEBUG	wpaAuthRecvKeyReq: keyDataLength not zero	ERROR
doing pnacTxRspId: entering 2nd cond	DEBUG	wpaAuthRecvKeyReq: mic check failed	ERROR
from pnacTxRspId: code = %d, identifier = %d, length = %d, "	DEBUG	invalid OUI %x %x %x	ERROR
doing pnacTxRspId: 2nd cond	DEBUG	(%s) invalid OUI %x %x %x	ERROR
doing pnacTxRspAuth: 1st cond	DEBUG	[%s:%d] Cipher in WPA IE : %x	ERROR
doing pnacTxRspAuth: 2nd cond	DEBUG	(%s) invalid OUI %x %x %x	ERROR
message for unknown port PAE	DEBUG	short WPA IE (length = %d) received	ERROR
from pnacACToSuppRecvRtn: calling pnacEapPktRecord	DEBUG	PTK state machine in unknown state.	ERROR
from pnacEapPktRecord: code = %d, identifier = %d, "	DEBUG	dot11InstallKeys failed	ERROR
from pnacEapPktRecord: received success pkt	DEBUG	group state machine entered into WPA_AUTH_GTK_INIT	ERROR
from pnacEapPktRecord: received failure pkt	DEBUG	dot11Malloc failed	ERROR
from pnacEapPktRecord: received request pkt	DEBUG	dot11Malloc failed	ERROR
unknown EAP-code %d	DEBUG	dot11Malloc failed	ERROR
Authenticator[%d]:	DEBUG	aesWrap failed	ERROR
Auth PAE state = %s	DEBUG	unknown key descriptor version %d	ERROR
Auth Reauth state = %s	DEBUG	dot11Malloc failed	ERROR
Back auth state = %s	DEBUG	could not initialize AES128ECB	ERROR
Supplicant[%d]:	DEBUG	could not initialize AES-128-ECB	ERROR
Supp Pae state = %s	DEBUG	MD5 initialization failed	ERROR
from pnacBackAuthFail: calling pnacTxCannedFail	DEBUG	RC4 framework initialization failed	ERROR
%s returned ERROR	DEBUG	PNAC framework initialization failed	ERROR
pnacUmiloctlHandler: cmd: %s(%d)	DEBUG	ERROR: option value not specified	ERROR
%s not configured for 802.1x	DEBUG	ERROR: -u can be used only with -s	ERROR
could not process PDU received from the wire	DEBUG	ERROR: user-name not specified	ERROR
pnacPDUForward: failed to foward the received PDU	DEBUG	failed to enable debug	ERROR
Creating PHY port with AUTH backend : %s SendRtn: %p RecvRtn:%p	DEBUG	[%s]: failed to convert string to MAC "	ERROR
pnacUmiAuthConfig: %s not configured for 802.1x	DEBUG	failed to initialize UMI	ERROR
pnacSuppRegisterUserInfo: not a valid AC	DEBUG	pnacPhyPortParamSet:invalid arguments	ERROR
pnacIfConfig: autoAuth Enabled	DEBUG	pnacPhyPortParamSet:Failed to create socket	ERROR
pnacSendRtn: no pnac port pae found for "	DEBUG	Error from pnacPhyPortParamSet:%sdevice invalid	ERROR
sending portStatus: %s[%d] to dot11	DEBUG	Error from pnacPhyPortParamSet:%s- Getting MAC address "	ERROR
pnacRecvASInfoMessage: Rkey of length %d set	DEBUG	pnacPhyPortParamSet:Failed to add 802.1X multicast "	ERROR
ASSendRtn: %p ASToAuthRecv: %p	DEBUG	pnacIsInterfaceUp: failed to create a raw socket	ERROR
adpRand failed:unable to generate random unicast key	WARN	pnacIsInterfaceUp: failed to get interface flags	ERROR
using group key as unicast key	WARN	failed to allocate buffer	ERROR
Integrity check failed more than once in last 60 secs.	WARN	UMI initialization failed	ERROR
MIC failed twice in last 60 secs, taking countermeasures	WARN	UMI initialization failed	ERROR
Failed to set dot11 port status	WARN	Error from pnacEapDemoAuthLibInit: malloc failed	ERROR
PTK state machine in NO_STATE.	WARN	Error from pnacEapDemoAuthRecv: received null EAP pkt	ERROR
PTK state machine in NO_STATE!!	WARN	Error from pnacEapDemoAuthRecv: send "	ERROR
PMKSA refcount not 1	WARN	Error from pnacRadXlateASAdd: cannot open socket	ERROR
IV verification failednknown subtype>	WARN	Error from pnacRadXlateDemoRecv: received null EAP pkt	ERROR
pnacIfConfig: overwriting previous interface "	WARN	From pnacRadXlateDemoRecv: send "	ERROR
pnacIfConfig: overwriting previous "	WARN	Error from pnacRadXlateDemoRecv: radius "	ERROR
pnacIfConfig: overwriting previous username"	WARN	Error from pnacRadXlateDemoRecv: radius "	ERROR
pnacIfConfig: overwriting previous password"	WARN	Error from pnacRadXlateRadIdRespSend: send to failed	ERROR
%s: Failed to set port status	WARN	Error from pnacRadXlateRadNonIdRespSend: send to failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: Failed to notify event to dot11	WARN	Error from pnacRadXlateRadRecvProc: recvfrom failed	ERROR
pnacLibDeinit: Failed to destroy the phyPort:%s	WARN	From pnacRadXlateRadPktIntegrityChk: no corresponding "	ERROR
pnacPortPaeDeconfig:kpnacPortPaeDec onfig failed	WARN	Error from pnacRadXlateRadPktIntegrityChk: no message "	ERROR
pnacPortPaeDeconfig:kpnacPortPaeDec onfig failed	WARN	Error from pnacRadXlateRadPktIntegrityChk: "	ERROR
pnacBackAuthSuccess: failed to notify the destination "	WARN	From pnacRadXlateRadChalPktHandle: no encapsulated eap "	ERROR
could not initialize MGMT framework	ERROR	Error from pnacRadXlateRadChalPktHandle: malloc for eap "	ERROR
umiInit failed	ERROR	Error from pnacEapDemoSuppUserInfoRegister: invalid "	ERROR
iappInit failed	ERROR	Error from pnacEapDemoSuppRecv: received null EAP pkt	ERROR
could not initialize IAPP MGMT.	ERROR	Error from pnacEapDemoSuppRecv: send ptr to pnac supplicant"	ERROR
dot11Malloc failed	ERROR	From pnacEapDemoSuppRecv: user info not entered yet	ERROR
buffer length not specified	ERROR	Error from pnacEapDemoSuppRecv: couldn't "	ERROR
Invalid length(%d) specified	ERROR	MDString: adpDigestInit for md5 failed	ERROR
Failed to get information about authorized AP list.	ERROR	pnacUmiInit: UMI initialization failed	ERROR
Recd IE data for non-existent AP %s	ERROR	could not start PNAC task	ERROR
Recd IE data for wrong AP %s	ERROR	invalid aruments	ERROR
Received Invalid IE data from WSC	ERROR	pnacIfNameToIndex failed	ERROR
Recd IE data for non-existent AP %s	ERROR	pnacPhyPortParamSet: device invalid %s%d	ERROR
Recd WSC Start command without interface name	ERROR	pnacPhyPortParamSet: EIOCGADDR ioctl failed	ERROR
Recd WSC start for non-existent AP %s	ERROR	pnacPhyPortParamSet: multicast addr add ioctl failed	ERROR
Recd WSC start for wrong AP %s	ERROR	pnacPhyPortParamUnset: multicast addr del ioctl failed	ERROR
Unable to send WSC_WLAN_CMD_PORT to WSC	ERROR	pnacPDUXmit: Invalid arguments	ERROR
Failed to get the ap context for %s	ERROR	pnacPDUXmit: failed to get M_BLK_ID	ERROR
WPS can only be applied to WPA/WPA2 security profiles	ERROR	from pnacIsInterfaceUp: device %s%d invalid	ERROR
wpsEnable: running wsccmd failed	ERROR	pnacRecvRtn: dropping received packet as port is"	ERROR
Failed to get the ap context for %s	ERROR	pnacSendRtn: Invalid arguments	ERROR
WPS conf. under non WPA/WPA2 security setting	ERROR	pnacSendRtn: no physical port corresponding to"	ERROR
Failed to reset the Beacon Frame IE in the driver	ERROR	pnacSendRtn: dropping packet as port"	ERROR
Failed to reset the Beacon Frame IE in the driver	ERROR	pnacAuthBuildRC4KeyDesc: adpEncryptInit(RC4) failed	ERROR
WPS method cannot be NULL	ERROR	pnacAuthBuildRC4KeyDesc: adpCipherContextCtrl"	ERROR
PIN value length should be a multiple of 4 !!	ERROR	pnacDot11UserSet: incorrect buffer length	ERROR
Failed to initiate PIN based association, PIN = %s	ERROR	PNAC user component id not set.	ERROR
Failed to initiate PBC based enrolle association	ERROR	pnacKeyInfoGet:failed to allocate buffer	ERROR
Invalid association mode. (Allowed modes : PIN/PBC)	ERROR	PNAC user comp id not set. dropping EAPOL key pkt	ERROR
wpsEnable: running wsccmd failed	ERROR	pnacUmiPortPaeParamSet: invalid buffer received	ERROR
Failed to send QUIT command to WSC from DOT11	ERROR	Error from pnacRecvASInfoMessage: "	ERROR
Failed to clear off the WPS process	ERROR	pnacRecvASInfoMessage: "	ERROR
missing profile name	ERROR	pnacRecvASInfoMessage: Bad info length	ERROR
A profile exists with the same name	ERROR	Error from pnacLibInit: malloc failed	ERROR
Error in allocating memory for profile	ERROR	could not create phy ports lock	ERROR
missing profile name	ERROR	could not create nodes ports lock	ERROR
missing profile name	ERROR	port exists for iface - %s	ERROR
Profile name and interface name must be specified	ERROR	pnacPhyPortCreate failed	ERROR
Profile %s does not exist	ERROR	kpnacPhyPortCreate failed	ERROR
Could not set profile %s on the interface %s	ERROR	invalid argument	ERROR
missing profile name	ERROR	pnacAuthConfig: maxAuth limit reached	ERROR
Profile %s does not exist	ERROR	pnacAuthConfig: malloc failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthConfig: pAsArg cannot be NULL	ERROR
SSID should not be longer than %d	ERROR	Error from pnacAuthConfig: receive routine hook "	ERROR
Profile %s does not exist	ERROR	pnacAuthConfig: pnacAuthInit failed	ERROR
Profile %s does not exist	ERROR	kpnacPortPaeConfig failed	ERROR
Profile %s does not exist	ERROR	Invalid arguments	ERROR
Profile %s does not exist	ERROR	Error from pnacSuppConfig: malloc failed	ERROR
Profile %s does not exist	ERROR	Error from pnacSuppConfig: receive routine hook "	ERROR
Profile %s does not exist	ERROR	Error from pnacSuppConfig: pnacSuppInit failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
SSID not set. SSID is needed to generate password hash	ERROR	kpnacPortPaeConfig failed	ERROR
Password string too big	ERROR	pnacAuthDeconfig failed: pPortPae NULL	ERROR
dot11Malloc failed	ERROR	Error from pnacPhyPortDestroy: port not configured	ERROR
Profile %s does not exist	ERROR	pnacPhyPortDestroy: Failed to deconfigure port	ERROR
Hex string should only have %d hex chars	ERROR	pnacPhyPortParamUnset FAILED	ERROR
dot11Malloc failed	ERROR	Error from pnacPhyPortCreate: malloc failed	ERROR
Profile %s does not exist	ERROR	Error from pnacPhyPortCreate: pnacPhyPortParamSet"	ERROR
invalid key index %d. key index should be 0-3.	ERROR	error from pnacPhyPortCreate: malloc failed	ERROR
wepKey length incorrect	ERROR	Error from pnacAuthInit: pnacPortTimersInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacAuthPAEInit failed	ERROR
Invalid Cipher type %d	ERROR	Error from pnacAuthInit: pnacAuthKeyTxInit failed	ERROR
Profile supports WEP stas,Group cipher must be WEP	ERROR	Error from pnacAuthInit: pnacReauthTimerInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacBackAuthInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacCtrlDirInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacKeyRecvInit failed	ERROR
invalid pairwise cipher type %d	ERROR	Error from pnacSupplnit: malloc failed	ERROR
Cipher %s is already in the list.	ERROR	Error from pnacSupplnit: pnacPortTimersInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacSupplnit: pnacKeyRecvInit failed	ERROR
Invalid Cipher type %d	ERROR	Error from pnacSupplnit: pnacSuppKeyTxInit failed	ERROR
Cipher %s not found in the list.	ERROR	Error from pnacSupplnit: pnacSuppPAEInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacRecvRtn: invalid arguments	ERROR
Profile %s does not exist	ERROR	Error from pnacRecvMapi: unsupported PDU received	ERROR
Auth method %s is already in the list	ERROR	suppToACSendRtn returned not OK!	ERROR
Profile %s does not exist	ERROR	Error from pnacBasicPktCreate: malloc failed	ERROR
Auth method %s not found in the list.	ERROR	Error from pnacEAPPktCreate: basic pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxCannedFail: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxCannedSuccess: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxReqId: eap pkt create failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacTxReq: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacSendRespToServer: malloc failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacSendRespToServer: no AS configured	ERROR
Profile %s does not exist	ERROR	Error from pnacTxStart: basic pkt create failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacTxStart: basic pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxRspId: eap pkt create failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacTxRspAuth: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacEapPktRecord: EAP packet too"	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacEapPktRecord: "	ERROR
Profile %s does not exist	ERROR	from pnacBackAuthTimeout: calling pnacTxCannedFail	ERROR
ERROR: incomplete DB update information.	ERROR	hmac_md5: adpHmacContextCreate failed	ERROR
old values result does not contain 2 rows	ERROR	hmac_md5:adpHmacInit failed	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiloctlHandler: invalid cmd: %d	ERROR
Error in executing DB update handler	ERROR	pnacEapRadAuthSend: Invalid arguments	ERROR
sqlite3QueryResGet failed	ERROR	pnacEapRadAuthSend: failed to allocate inbuffer	ERROR
ERROR: incomplete DB update information.	ERROR	pnacXmit : umiloctl failed[%d]	ERROR
old values result does not contain 2 rows	ERROR	pnacPDUForward: Invalid input	ERROR
sqlite3QueryResGet failed	ERROR	pnacPDUForward: error in getting port pae information	ERROR
Error in executing DB update handler	ERROR	pnacPDUForward: error allocating memory	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiIfMacAddrChange: %s not configured for 802.1x	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiIfMacAddrChange: could not process PDU received"	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiPhyPortConfig: Invalid config data	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiPhyPortConfig: Invalid backend name specified	ERROR
startStopVap failed to stop %s	ERROR	pnacUmiPhyPortConfig: could not create PNAC physical"	ERROR
Invalid SQLITE operation code - %d	ERROR	pnacUmiAuthConfig: Invalid config data	ERROR
./src/dot11/mgmt/dot11Mgmt.c:1177: ADP_ERROR (	ERROR	pnacUmiAuthConfig: Invalid backend name specified	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
only delete event expected on dot11RogueAP.	ERROR	unable to create new EAP context.	ERROR
sqlite3QueryResGet failed	ERROR	unable to apply %s profile on the EAP context.	ERROR
unhandled database operation %d	ERROR	pnacUmiAuthConfig: could not configure PNAC PAE "	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: Invalid config data	ERROR
failed to configure WPS on %s	ERROR	pnacUmiSuppConfig: Invalid backend name specified	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: %s not configured for 802.1x	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: could not PNAC port Access"	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: Failed to register user information	ERROR
sqlite3QueryResGet failed	ERROR	pnacPortByMacDeconfig: port not found	ERROR
sqlite3QueryResGet failed	ERROR	pnacPortByMacDeconfig: port not found	ERROR
no VAP rows returned. expected one	ERROR	pnacUmiIfDown: Invalid config data	ERROR
multiple VAP rows returned. expected one	ERROR	pnacUmiIfDown: Invalid config data	ERROR
sqlite3QueryResGet failed	ERROR	Error from pnacPortDeconfig: port not configured	ERROR
invalid query result. ncols=%d nrows=%d	ERROR	pnacUmiIfDown: could not deconfigure port	ERROR
%s:VAP(%s) create failed	ERROR	pnacUmiPhyPortDestroy: Invalid config data	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiPhyPortDestroy: Invalid config data	ERROR
invalid query result. ncols=%d nrows=%d	ERROR	pnacUmiPhyPortDestroy: Failed to destroy the port	ERROR
Invalid config data	ERROR		

■ ファシリティ：システム（カーネル）

ログメッセージ	緊急度	ログメッセージ	緊急度
DNAT: multiple ranges no longer supported	DEBUG	%s: %s%s:%d -> %s:%d %s,	DEBUG
DNAT: Target size %u wrong for %u ranges,	DEBUG	%s: %s%s:%d %s,	DEBUG
DNAT: wrong table %s, tablename	DEBUG	%s: Failed to add WDS MAC: %s, dev- >name,	DEBUG
DNAT: hook mask 0x%x bad, hook_mask	DEBUG	%s: Device already has WDS mac address attached,	DEBUG
%s%d: resetting MPPC/MPPE compressor,	DEBUG	%s: Added WDS MAC: %s, dev- >name,	DEBUG
%s%d: wrong offset value: %d,	DEBUG	%s: WDS MAC address %s is not known by this interface,	DEBUG
%s%d: wrong length of match value: %d,	DEBUG	[madwifi] %s() : Not enough space., __FUNCTION__	DEBUG
%s%d: too big offset value: %d,	DEBUG	Returning to chan %d, ieeeChan	DEBUG
%s%d: cannot decode offset value,	DEBUG	WEP	DEBUG
%s%d: wrong length code: 0x%X,	DEBUG	AES	DEBUG
%s%d: short packet (len=%d), __FUNCTION__,	DEBUG	AES_CCM	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	CKIP	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	TKIP	DEBUG
PPPIOCDETACH file->f_count=%d,	DEBUG	%s: cannot map channel to mode; freq %u flags 0x%x,	DEBUG
PPP: outbound frame not passed	DEBUG	%s: %s, vap->iv_dev->name, buf	DEBUG
PPP: VJ decompression error	DEBUG	%s: [%s] %s, vap->iv_dev->name,	DEBUG
PPP: inbound frame not passed	DEBUG	%s: [%s] %s, vap->iv_dev->name, ether_sprintf(mac), buf	DEBUG
PPP: reconstructed packet	DEBUG	[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG
PPP: no memory for	DEBUG	[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG
missed pkts %u..%u,	DEBUG	[%s:%s] discard %s information element, %s,	DEBUG
%s%d: resetting MPPC/MPPE compressor,	DEBUG	[%s:%s] discard information element, %s,	DEBUG
%s%d: wrong offset value: %d,	DEBUG	[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG
%s%d: wrong length of match value: %d,	DEBUG	[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG
%s%d: too big offset value: %d,	DEBUG	ifmedia_add: null ifm	DEBUG
%s%d: cannot decode offset value,	DEBUG	Adding entry for	DEBUG
%s%d: wrong length code: 0x%X,	DEBUG	ifmedia_set: no match for 0x%x/0x%x,	DEBUG
%s%d: short packet (len=%d), __FUNCTION__,	DEBUG	ifmedia_set: target	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	ifmedia_set: setting to	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	ifmedia_ioctl: no media found for 0x%x,	DEBUG
PPPIOCDETACH file->f_count=%d,	DEBUG	ifmedia_ioctl: switching %s to , dev- >name	DEBUG
PPP: outbound frame not passed	DEBUG	ifmedia_match: multiple match for	DEBUG
PPP: VJ decompression error	DEBUG	<unknown type>	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
PPP: inbound frame not passed	DEBUG	desc->ifmt_string	DEBUG
PPP: reconstructed packet	DEBUG	mode %s, desc->ifmt_string	DEBUG
PPP: no memory for	DEBUG	<unknown subtype>	DEBUG
missed pkts %u..%u,	DEBUG	%s, desc->ifmt_string	DEBUG
%s: INC_USE_COUNT, now %d, __FUNCTION__, mod_use_count \	DEBUG	%s%s, seen_option++ ? , : ,	DEBUG
%s: DEC_USE_COUNT, now %d, __FUNCTION__, mod_use_count \	DEBUG	%s%s, seen_option++ ? , : ,	DEBUG
PPPOL2TP %s: _fmt,	DEBUG	%s, seen_option ? > :	DEBUG
PPPOL2TP: --> %s, __FUNCTION__)	DEBUG	%s: %s, dev->name, buf	DEBUG
PPPOL2TP: <-- %s, __FUNCTION__)	DEBUG	%s: no memory for sysctl table!, __func__	DEBUG
%s: recv: , tunnel->name	DEBUG	%s: no memory for VAP name!, __func__	DEBUG
%s: xmit:, session->name	DEBUG	%s: failed to register sysctls!, vap- >iv_dev->name	DEBUG
%s: xmit:, session->name	DEBUG	%s: no memory for new proc entry (%s)!, __func__,	DEBUG
%s: module use_count is %d, __FUNCTION__, mod_use_count	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
PPPOL2TP %s: _fmt,	DEBUG	%03d:, i	DEBUG
PPPOL2TP: --> %s, __FUNCTION__)	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
PPPOL2TP: <-- %s, __FUNCTION__)	DEBUG	first difference at byte %u, i	DEBUG
%s: recv: , tunnel->name	DEBUG	%s: , t->name	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: ieee80211_crypto_newkey failed	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: ieee80211_crypto_setkey failed	DEBUG
PPPOL2TP %s: _fmt,	DEBUG	FAIL: unable to allocate skbuff	DEBUG
PPPOL2TP: --> %s, __FUNCTION__)	DEBUG	FAIL: wep decap failed	DEBUG
PPPOL2TP: <-- %s, __FUNCTION__)	DEBUG	FAIL: decap botch; length mismatch	DEBUG
%s: recv: , tunnel->name	DEBUG	FAIL: decap botch; data does not compare	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: wep encap failed	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: encap data length mismatch	DEBUG
IRQ 31 is triggered	DEBUG	FAIL: encrypt data does not compare	DEBUG
[%s:%d] , __func__, __LINE__\	DEBUG	PASS	DEBUG
\t[R%s %#0x %#0x 0x%08x%08x], (status == ERROR ? # :), page, addr, (uint32_t)(*pValue >> 32), (uint32_t)(*pValue & 0xffffffff)	DEBUG	%u of %u 802.11i WEP test vectors passed, pass, total	DEBUG
\t[W%s %#0x %#0x 0x%08x%08x], (status == ERROR ? # :), page, addr, (uint32_t)(value >> 32), (uint32_t)(value & 0xffffffff)	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
%s: mac_add %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	%03d:, i	DEBUG
%s: mac_del %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
%s: mac_kick %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	first difference at byte %u, i	DEBUG
%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	%s: , t->name	DEBUG
%s: addr_add %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	FAIL: ieee80211_crypto_newkey failed	DEBUG
%s: addr_del %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	FAIL: ieee80211_crypto_setkey failed	DEBUG
%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	FAIL: unable to allocate skbuff	DEBUG
%s: set_float %d;%d,	DEBUG	FAIL: ccmp encap failed	DEBUG
IRQ 32 is triggered	DEBUG	FAIL: encap data length mismatch	DEBUG
ip_finish_output2: No header cache and no neighbour!	DEBUG	FAIL: encrypt data does not compare	DEBUG
a guy asks for address mask. Who is it?	DEBUG	FAIL: ccmp decap failed	DEBUG
icmp v4 hw csum failure)	DEBUG	FAIL: decap botch; length mismatch	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	FAIL: decap botch; data does not compare	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	PASS	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	%u of %u 802.11i AES-CCMP test vectors passed, pass, total	DEBUG
rt_bind_peer(0) @%p, NET_CALLER(iph)	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
ip_rt_advice: redirect to	DEBUG	%03d:, i	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
udp cork app bug 2)	DEBUG	first difference at byte %u, i	DEBUG
udp cork app bug 3)	DEBUG	ieee80211_crypto_newkey failed	DEBUG
udp v4 hw csum failure.)	DEBUG	ieee80211_crypto_setkey failed	DEBUG
UDP: short packet: From %u.%u.%u.%u:%u %d/%d to %u.%u.%u.%u:%u,	DEBUG	unable to allocate skbuff	DEBUG
UDP: bad checksum. From %d.%d.%d.%d:%d to %d.%d.%d.%d:%d ulen %d,	DEBUG	tkip enmic failed	DEBUG
%s: lookup policy [list] found=%s,	DEBUG	enmic botch; length mismatch	DEBUG
%s: called: [output START], __FUNCTION__	DEBUG	enmic botch	DEBUG
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_dst, family)	DEBUG	tkip encap failed	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_src, family)	DEBUG	encrypt phase1 botch	DEBUG
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_dst, family)	DEBUG	encrypt data length mismatch	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_src, family)	DEBUG	encrypt data does not compare	DEBUG
a guy asks for address mask. Who is it?	DEBUG	tkip decap failed	DEBUG
icmp v4 hw csum failure)	DEBUG	decrypt phase1 botch	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	decrypt data does not compare	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	decap botch; length mismatch	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	decap botch; data does not compare	DEBUG
rt_bind_peer(0) @%p, NET_CALLER(iph)	DEBUG	tkip demic failed	DEBUG
ip_rt_advice: redirect to	DEBUG	802.11i TKIP test vectors passed	DEBUG
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	%s, buf	DEBUG
UDP: short packet: From %u.%u.%u.%u:%u %d/%d to %u.%u.%u.%u:%u,	DEBUG	Atheros HAL assertion failure: %s: line %u: %s,	DEBUG
UDP: bad checksum. From %d.%d.%d.%d:%d to %d.%d.%d.%d:%d ulen %d,	DEBUG	ath_hal: logging to %s %s, ath_hal_logfile,	DEBUG
a guy asks for address mask. Who is it?	DEBUG	ath_hal: logging disabled	DEBUG
fib_add_ifaddr: bug: prim == NULL	DEBUG	%s%s, sep, ath_hal_buildopts[i]	DEBUG
fib_del_ifaddr: bug: prim == NULL	DEBUG	ath_pci: No devices found, driver not installed.	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	_fmt, __VA_ARGS__	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	%s: Warning, using only %u entries in %u key cache,	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	%s: TX99 support enabled, dev->name	DEBUG
rt_bind_peer(0) @%p,	DEBUG	%s:grppoll Buf allocation failed ,__func__	DEBUG
ip_rt_advice: redirect to	DEBUG	%s: %s: unable to start recv logic,	DEBUG
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	%s: %s: unable to start recv logic,	DEBUG
%s: lookup policy [list] found=%s,	DEBUG	%s: no skbuff, __func__	DEBUG
%s: called: [output START], __FUNCTION__	DEBUG	%s: hardware error; resetting, dev- >name DEBUG	
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_dst, family)	DEBUG	%s: rx FIFO overrun; resetting, dev- >name	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_src, family)	DEBUG	%s: unable to reset hardware: '%s' (HAL status %u)	DEBUG
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_dst, family)	DEBUG	%s: unable to start recv logic, dev- >name	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_src, family)	DEBUG	%s: %s: unable to reset hardware: '%s' (HAL status %u),	DEBUG
a guy asks for address mask. Who is it?	DEBUG	%s: %s: unable to start recv logic,	DEBUG
icmp v4 hw csum failure)	DEBUG	ath_mgtstart: discard, no xmit buf	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	%s: [%02u] %-7s , tag, ix, ciphers[hk- >kv_type]	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	%02x, hk->kv_val[i]	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	mac %s, ether_sprintf(mac)	DEBUG
rt_bind_peer(0) @%p, NET_CALLER(iph)	DEBUG	%s , sc->sc_splitmic ? mic : rxmic	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
ip_rt_advice: redirect to	DEBUG	%02x, hk->kv_mic[i]	DEBUG
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	txmic	DEBUG
UDP: short packet: From %u.%u.%u.%u:%u %d/%d to %u.%u.%u.%u:%u,	DEBUG	%02x, hk->kv_txmic[i]	DEBUG
UDP: bad checksum. From %d.%d.%d.%d:%d to %d.%d.%d.%d:%d ulen %d,	DEBUG	%s: unable to update h/w beacon queue parameters,	DEBUG
REJECT: ECHOREPLY no longer supported.	DEBUG	%s: stuck beacon; resetting (bmiss count %u),	DEBUG
ipt_rpc: only valid for PRE_ROUTING, FORWARD, POST_ROUTING, LOCAL_IN and/or LOCAL_OUT targets.	DEBUG	move data from NORMAL to XR	DEBUG
ip_nat_init: can't setup rules.	DEBUG	moved %d buffers from NORMAL to XR, index	DEBUG
ip_nat_init: can't register in hook.	DEBUG	move buffers from XR to NORMAL	DEBUG
ip_nat_init: can't register out hook.	DEBUG	moved %d buffers from XR to NORMAL, count	DEBUG
ip_nat_init: can't register adjust in hook.	DEBUG	%s:%d %s, __FILE__, __LINE__, __func__	DEBUG
ip_nat_init: can't register adjust out hook.	DEBUG	%s:%d %s, __FILE__, __LINE__, __func__	DEBUG
ip_nat_init: can't register local out hook.	DEBUG	%s: no buffer (%s), dev->name, __func__	DEBUG
ip_nat_init: can't register local in hook.	DEBUG	%s: no skbuff (%s), dev->name, __func__	DEBUG
ipt_hook: happy cracking.	DEBUG	%s: HAL qnum %u out of range, max %u!,	DEBUG
ip_conntrack: can't register pre-routing defrag hook.	DEBUG	grppoll_start: grppoll Buf allocation failed	DEBUG
ip_conntrack: can't register local_out defrag hook.	DEBUG	%s: HAL qnum %u out of range, max %u!,	DEBUG
ip_conntrack: can't register pre-routing hook.	DEBUG	%s: AC %u out of range, max %u!,	DEBUG
ip_conntrack: can't register local out hook.	DEBUG	%s: unable to update hardware queue	DEBUG
ip_conntrack: can't register local in helper hook.	DEBUG	%s: bogus frame type 0x%x (%s), dev- >name,	DEBUG
ip_conntrack: can't register postrouting helper hook.	DEBUG	ath_stoprecv: rx queue 0x%x, link %p,	DEBUG
ip_conntrack: can't register post-routing hook.	DEBUG	%s: %s: unable to reset channel %u (%u MHz)	DEBUG
ip_conntrack: can't register local in hook.	DEBUG	%s: %s: unable to restart recv logic,	DEBUG
ip_conntrack: can't register to sysctl.	DEBUG	%s: unable to allocate channel table, dev->name	DEBUG
ip_conntrack_rtsp v IP_NF_RTSP_VERSION loading	DEBUG	%s: unable to allocate channel table, dev->name	DEBUG
ip_conntrack_rtsp: max_outstanding must be a positive integer	DEBUG	%s: unable to collect channel list from HAL;	DEBUG
ip_conntrack_rtsp: setup_timeout must be a positive integer	DEBUG	R (%p %llx) %08x %08x %08x %08x %08x %08x %c,	DEBUG
ip_conntrack_rtsp: ERROR registering port %d, ports[i]	DEBUG	T (%p %llx) %08x %08x %08x %08x %08x %08x %08x %08x %c,	DEBUG
ip_nat_rtsp v IP_NF_RTSP_VERSION loading	DEBUG	%s: no memory for sysctl table!, __func__	DEBUG
%s: Sorry! Cannot find this match option., __FILE__	DEBUG	%s: no memory for device name storage!, __func__	DEBUG
ipt_time loading	DEBUG	%s: failed to register sysctls!, sc- >sc_dev->name	DEBUG
ipt_time unloaded	DEBUG	%s: mac %d.%d phy %d.%d, dev- >name,	DEBUG
ip_conntrack_irc: max_dcc_channels must be a positive integer	DEBUG	5 GHz radio %d.%d 2 GHz radio %d.%d,	DEBUG
ip_conntrack_irc: ERROR registering port %d,	DEBUG	radio %d.%d, ah->ah_analog5GhzRev >> 4,	DEBUG
ip_nat_h323: ip_nat_mangle_tcp_packet	DEBUG	radio %d.%d, ah->ah_analog5GhzRev >> 4,	DEBUG
ip_nat_h323: ip_nat_mangle_udp_packet	DEBUG	%s: Use hw queue %u for %s traffic,	DEBUG
ip_nat_h323: out of expectations	DEBUG	%s: Use hw queue %u for CAB traffic, dev->name,	DEBUG
ip_nat_h323: out of RTP ports	DEBUG	%s: Use hw queue %u for beacons, dev->name,	DEBUG
ip_nat_h323: out of TCP ports	DEBUG	Could not find Board Configuration Data	DEBUG
ip_nat_q931: out of TCP ports	DEBUG	Could not find Radio Configuration data	DEBUG
ip_nat_ras: out of TCP ports	DEBUG	ath_ahb: No devices found, driver not installed.	DEBUG
ip_nat_q931: out of TCP ports	DEBUG	_fmt, __VA_ARGS__	DEBUG
ip_conntrack_core: Frag of proto %u.,	DEBUG	_fmt, __VA_ARGS__	DEBUG
Broadcast packet!	DEBUG	xlr8NatIpFinishOutput: Err.. skb2 == NULL !	DEBUG
Should bcast: %u.%u.%u.%u- >%u.%u.%u.%u (sk=%p, ptype=%u),	DEBUG	xlr8NatSoftCtxEnqueue: Calling xlr8NatIpFinishOutput () .., status	DEBUG
ip_conntrack version %s (%u buckets, %d max)	DEBUG	xlr8NatSoftCtxEnqueue: xlr8NatIpFinishOutput () returned [%d], status	DEBUG
ERROR registering port %d,	DEBUG	icmpExceptionHandler: Exception!	DEBUG
netfilter PSD loaded - (c) astaro AG	DEBUG	fragExceptionHandler: Exception!	DEBUG
netfilter PSD unloaded - (c) astaro AG	DEBUG	algExceptionHandler: Exception!	DEBUG
%s , SELF	DEBUG	dnsExceptionHandler: Exception!	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
%s , LAN	DEBUG	ipsecExceptionHandler: Exception!	DEBUG
%s , WAN	DEBUG	ESP Packet Src:%x Dest:%x Sport:%d dport:%d secure:%d spi:%d isr:%p,	DEBUG
TRUNCATED	DEBUG	xlr8NatConntrackPreHook: We found the valid context,	DEBUG
SRC=%u.%u.%u.%u DST=%u.%u.%u.%u ,	DEBUG	xlr8NatConntrackPreHook: Not a secured packet.	DEBUG
LEN=%u TOS=0x%02X PREC=0x%02X TTL=%u ID=%u ,	DEBUG	xlr8NatConntrackPreHook: isr=[%p], plsr	DEBUG
FRAG:%u , ntohs(ih->frag_off) & IP_OFFSET	DEBUG	xlr8NatConntrackPreHook: secure=[%d], secure	DEBUG
TRUNCATED	DEBUG	Context found for ESP %p,pFlowEntry- >post.plsr[0]	DEBUG
PROTO=TCP	DEBUG	xlr8NatConntrackPreHook: New connection.	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	xlr8NatConntrackPostHook: postSecure=[%d] postIsr=[%p %p],	DEBUG
SPT=%u DPT=%u ,	DEBUG	proto %d spi %d <-------> proto %d spi %d,pPktInfo->proto,pPktInfo->spi,	DEBUG
SEQ=%u ACK=%u ,	DEBUG	IPSEC_INF Clock skew detected	DEBUG
WINDOW=%u , ntohs(th->window)	DEBUG	IPSEC_ERR [%s:%d]: Max (%d) No of SA Limit reached,	DEBUG
RES=0x%02x , (u8)(ntohl(tcp_flag_word(th) & TCP_RESERVED_BITS) >> 22)	DEBUG	IPSEC_ERR [%s:%d]: Max (%d) No of SA Limit reached,	DEBUG
URGP=%u , ntohs(th->urg_ptr)	DEBUG	IPSEC_ERR [%s:%d]: time(secs): %u	DEBUG
TRUNCATED	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
%02X, op[i]	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PROTO=UDP	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
SPT=%u DPT=%u LEN=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
SPT=%u DPT=%u LEN=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PROTO=ICMP	DEBUG	unknown oid '%s', varName	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	could not find oid pointer for '%s', varName	DEBUG
TYPE=%u CODE=%u , ich->type, ich- >code	DEBUG	unRegistering ipsecMib	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
ID=%u SEQ=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PARAMETER=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
GATEWAY=%u.%u.%u.%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
MTU=%u , ntohs(ich->un.frag.mtu)	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PROTO=AH	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	unknown oid '%s', varName	DEBUG
SPI=0x%x , ntohl(ah->spi)	DEBUG	could not find oid pointer for '%s', varName	DEBUG
PROTO=ESP	DEBUG	unRegistering ipsecMib	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
SPI=0x%x , ntohl(eh->spi)	DEBUG	%02x, *p	DEBUG
PROTO=%u , ih->protocol	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
UID=%u , skb->sk->sk_socket->file- >f_uid	DEBUG	%02x, *p	DEBUG
<%d>%sIN=%s OUT=%s , loginfo- >u.log.level,	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
level_string	DEBUG	%02x, *p	DEBUG
%sIN=%s OUT=%s ,	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
%s , prefix == NULL ? loginfo->prefix : prefix	DEBUG	%02x, *p	DEBUG
IN=	DEBUG	unable to register vipsec kernel comp to UMI	DEBUG
OUT=	DEBUG	unregistering VIPSECK from UMI	DEBUG
PHYSIN=%s , physindev->name	DEBUG	in vipsecKIoctlHandler cmd - %d, cmd	DEBUG
PHYSOUT=%s , physoutdev->name	DEBUG	%s: Error. DST Refcount value less than 1 (%d),	DEBUG
MAC=	DEBUG	for %s DEVICE refcnt: %d ,pDst- >dev->name,	DEBUG
%02x%c, *p,	DEBUG	%s: Got Null m:%p *m:%p sa:%p *sa:%p,__func__,ppBufMgr,	DEBUG
NAT: no longer support implicit source local NAT	DEBUG	%s Got Deleted SA:%p state:%d,__func__,pIpsecInfo,pIpsecInfo->state	DEBUG
NAT: packet src %u.%u.%u.%u -> dst %u.%u.%u.%u,	DEBUG	%s: %s: fmt, __FILE__, __FUNCTION__ , ## args)	INFO
SNAT: multiple ranges no longer supported	DEBUG	%s: %s: fmt, __FILE__, __FUNCTION__ , ## args)	INFO
format,##args)	DEBUG	ipt_TIME: format, ## args)	INFO

ログメッセージ	緊急度	ログメッセージ	緊急度
version	DEBUG	IPT_ACCOUNT_NAME : checkentry() wrong parameters (not equals existing table parameters).	INFO
offset_before=%d, offset_after=%d, correction_pos=%u, x->offset_before, x- >offset_after, x->correction_pos	DEBUG	IPT_ACCOUNT_NAME : checkentry() too big netmask.	INFO
ip_ct_h323:	DEBUG	IPT_ACCOUNT_NAME : checkentry() failed to allocate %zu for new table %s., sizeof(struct t_ipt_account_table), info->name	INFO
ip_ct_h323: incomplete TPKT (fragmented?)	DEBUG	IPT_ACCOUNT_NAME : checkentry() wrong network/ netmask.	INFO
ip_ct_h245: decoding error: %s,	DEBUG	account: Wrong netmask given by netmask parameter (%i). Valid is 32 to 0., netmask	INFO
ip_ct_h245: packet dropped	DEBUG	IPT_ACCOUNT_NAME : checkentry() failed to create procfs entry.	INFO
ip_ct_q931: decoding error: %s,	DEBUG	IPT_ACCOUNT_NAME : checkentry() failed to register match.	INFO
ip_ct_q931: packet dropped	DEBUG	failed to create procfs entry .	INFO
ip_ct_ras: decoding error: %s,	DEBUG	MPPE/MPPC encryption/compression module registered	INFO
ip_ct_ras: packet dropped	DEBUG	MPPE/MPPC encryption/compression module unregistered	INFO
ERROR registering port %d,	DEBUG	PPP generic driver version PPP_VERSION	INFO
ERROR registering port %d,	DEBUG	MPPE/MPPC encryption/compression module registered	INFO
ipt_connlimit [%d]: src=%u.%u.%u.%u:%d dst=%u.%u.%u.%u:%d %s,	DEBUG	MPPE/MPPC encryption/compression module unregistered	INFO
ipt_connlimit [%d]: src=%u.%u.%u.%u:%d dst=%u.%u.%u.%u:%d new,	DEBUG	PPP generic driver version PPP_VERSION	INFO
ipt_connlimit: Oops: invalid ct state ?	DEBUG	PPPoL2TP kernel driver, %s,	INFO
ipt_connlimit: Hmm, kmalloc failed :-(	DEBUG	PPPoL2TP kernel driver, %s,	INFO
ipt_connlimit: src=%u.%u.%u.%u mask=%u.%u.%u.%u	DEBUG	PPPoL2TP kernel driver, %s,	INFO
_lvl PPPOL2TP: _fmt, ##args	DEBUG	failed to create procfs entry .	INFO
%02X, ptr[length]	DEBUG	proc dir not created ..	INFO
%02X, ((unsigned char *) m- >msg_iov[i].iov_base)[j]	DEBUG	Initialzing Product Data modules	INFO
%02X, skb->data[i]	DEBUG	De initializing by \	INFO
_lvl PPPOL2TP: _fmt, ##args	DEBUG	kernel UMI module loaded	INFO
%02X, ptr[length]	DEBUG	kernel UMI module unloaded	INFO
%02X, ((unsigned char *) m- >msg_iov[i].iov_base)[j]	DEBUG	Loading bridge module	INFO
%02X, skb->data[i]	DEBUG	Unloading bridge module	INFO
_lvl PPPOL2TP: _fmt, ##args	DEBUG	unsupported command %d, cmd	INFO
%02X, ptr[length]	DEBUG	Loading ifDev module	INFO
%02X, ((unsigned char *) m- >msg_iov[i].iov_base)[j]	DEBUG	Unloading ifDev module	INFO
%02X, skb->data[i]	DEBUG	ERROR#%d in alloc_chrdev_region, result	INFO
KERN_EMERG THE value read is %d,value*/	DEBUG	ERROR#%d in cdev_add, result	INFO
KERN_EMERG Factory Reset button is pressed	DEBUG	using bcm switch %s, bcmswitch	INFO
KERN_EMERG Returing error in INTR registration	DEBUG	privlegedID %d wanporttNo: %d, privlegedID,wanportNo	INFO
KERN_EMERG Initialzing Factory defaults modules	DEBUG	Loading mii	INFO
Failed to allocate memory for pSipListNode	DEBUG	Unloading mii	INFO
SIPALG: Memeory allocation failed for pSipNodeEntryTbl	DEBUG	%s: Version 0.1	INFO
pkt-err %s, pktInfo.error	DEBUG	%s: driver unloaded, dev_info	INFO
pkt-err %s, pktInfo.error	DEBUG	wlan: %s backend registered, be- >iab_name	INFO
pkt-err %s, pktInfo.error	DEBUG	wlan: %s backend unregistered,	INFO
%s Len=%d, msg, len	DEBUG	wlan: %s acl policy registered, iac- >iac_name	INFO
%02x , ((uint8_t *) ptr)[i]	DEBUG	wlan: %s acl policy unregistered, iac- >iac_name	INFO
End	DEBUG	%s, tmpbuf	INFO
CVM_MOD_EXP_BASE MISMATCH cmd=%x base=%x, cmd,	DEBUG	VLAN2	INFO
op->sizeofptr = %ld, op->sizeofptr	DEBUG	VLAN3	INFO
opcode cmd = %x, cmd	DEBUG	VLAN4 <%d %d>,	INFO
modexp opcode received	DEBUG	%s: %s, dev_info, version	INFO

ログメッセージ	緊急度	ログメッセージ	緊急度
Memory Allocation failed	DEBUG	%s: driver unloaded, dev_info	INFO
modexpcrt opcode received	DEBUG	%s, buf	INFO
kmalloc failed	DEBUG	%s: %s (, dev_info, ath_hal_version	INFO
kmalloc failed	DEBUG	%s: driver unloaded, dev_info	INFO
kmalloc failed	DEBUG	%s: %s: mem=0x%lx, irq=%d hw_base=0x%p,	INFO
kmalloc failed	DEBUG	%s: %s, dev_info, version	INFO
kmalloc Failed	DEBUG	%s: driver unloaded, dev_info	INFO
kmalloc failed	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
unknown cyrpto ioctl cmd received %x, cmd	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
register_chrdev returned ZERO	DEBUG	%s: %s, dev_info, version	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	%s: driver unloaded, dev_info	INFO
F password, &pdata	DEBUG	%s, buf	INFO
test key, key	DEBUG	%s: %s (, dev_info, ath_hal_version	INFO
pre-hashed key, key	DEBUG	%s: driver unloaded, dev_info	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	%s: driver unloaded, dev_info	INFO
AES 128-bit key, &key	DEBUG	%s: Version 2.0.0	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	%s: driver unloaded, dev_info	INFO
test key, key	DEBUG	%s: driver unloaded, dev_info	INFO
pre-hashed key, key	DEBUG	wlan: %s backend registered, be- >iab_name	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	wlan: %s backend unregistered,	INFO
128-bit AES key,&dk	DEBUG	wlan: %s acl policy registered, iac- >iac_name	INFO
256-bit AES key, &dk	DEBUG	wlan: %s acl policy unregistered, iac- >iac_name	INFO
WARNING:	DEBUG	%s: %s, dev_info, version	INFO
bwMonMultipathNxtHopSelect:: checking rates	DEBUG	%s: driver unloaded, dev_info	INFO
hop :%d dev:%s usableBwLimit = %d currBwShare = %d lastHopSelected = %d weightedHopPrefer = %d ,	DEBUG	%s: %s (, dev_info, ath_hal_version	INFO
1. selecting hop: %d lastHopSelected = %d , selHop, lastHopSelected	DEBUG	%s: driver unloaded, dev_info	INFO
4. hop :%d dev:%s usableBwLimit = %d currBwShare = %d lastHopSelected = %d weightedHopPrefer = %d ,	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
2. selecting hop: %d lastHopSelected = %d , selHop, lastHopSelected	DEBUG	%s: %s, dev_info, version	INFO
3. selecting hop: %d lastHopSelected = %d , selHop, lastHopSelected	DEBUG	%s: driver unloaded, dev_info	INFO
bwMonitor multipath selection enabled	DEBUG	ath_pci: switching rfkill capability %s,	INFO
bwMonitor multipath selection disabled	DEBUG	Unknown autocreate mode: %s,	INFO
weightedHopPrefer set to %d ,weightedHopPrefer	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
bwMonitor sysctl registration failed	DEBUG	%s: %s, dev_info, version	INFO
bwMonitor sysctl registered	DEBUG	%s: driver unloaded, dev_info	INFO
bwMonitor sysctl not registered	DEBUG	%s: %s, dev_info, version	INFO
Unregistered bwMonitor sysctl	DEBUG	%s: unloaded, dev_info	INFO
CONFIG_SYSCTL enabled ...	DEBUG	%s: %s, dev_info, version	INFO
Initialized bandwidth monitor ...	DEBUG	%s: unloaded, dev_info	INFO
Removed bandwidth monitor ...	DEBUG	%s: %s, dev_info, version	INFO
Oops.. AES_GCM_encrypt failed (keylen:%u),key->cvm_keylen	DEBUG	%s: unloaded, dev_info	INFO
Oops.. AES_GCM_decrypt failed (keylen:%u),key->cvm_keylen	DEBUG	failed to create procfs entry .	INFO
%s, msg	DEBUG	ICMP: %u.%u.%u.%u:	INFO
%02x%s, data[i],	DEBUG	ICMP: %u.%u.%u.%u: Source	INFO
Failed to set AES encrypt key	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set AES encrypt key	DEBUG	Redirect from %u.%u.%u.%u on %s about INFO	
AES %s Encrypt Test Duration: %d:%d, hard ? Hard : Soft,	DEBUG	IP: routing cache hash table of %u buckets, %ldKbytes,	INFO
Failed to set AES encrypt key	DEBUG	source route option %u.%u.%u.%u -> %u.%u.%u.%u,	INFO
Failed to set AES encrypt key	DEBUG	ICMP: %u.%u.%u.%u:	INFO
AES %s Decrypt Test Duration: %d:%d, hard ? Hard : Soft,	DEBUG	ICMP: %u.%u.%u.%u: Source	INFO

ログメッセージ	緊急度	ログメッセージ	緊急度
Failed to set AES encrypt key	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set AES encrypt key	DEBUG	Redirect from %u.%u.%u.%u on %s about	INFO
Failed to set AES encrypt key	DEBUG	IP: routing cache hash table of %u buckets, %ldKbytes,	INFO
Failed to set AES encrypt key	DEBUG	source route option %u.%u.%u.%u -> %u.%u.%u.%u,	INFO
Failed to set DES encrypt key[%d], i	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set DES decrypt key[%d], i	DEBUG	Redirect from %u.%u.%u.%u on %s about	INFO
Failed to set DES encrypt key[%d], i	DEBUG	source route option	INFO
Failed to set DES decrypt key[%d], i	DEBUG	ICMP: %u.%u.%u.%u:	INFO
Failed to set DES encrypt key	DEBUG	ICMP: %u.%u.%u.%u: Source	INFO
Failed to set DES decrypt key	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set DES encrypt key	DEBUG	Redirect from %u.%u.%u.%u on %s about	INFO
Failed to set DES decrypt key	DEBUG	IP: routing cache hash table of %u buckets, %ldKbytes,	INFO
AES Software Test:	DEBUG	source route option %u.%u.%u.%u -> %u.%u.%u.%u,	INFO
AES Software Test %s, aesSoftTest(0) ? Failed : Passed	DEBUG	IPsec: device unregistering: %s, dev- >name	INFO
AES Hardware Test:	DEBUG	IPsec: device down: %s, dev->name	INFO
AES Hardware Test %s, aesHardTest(0) ? Failed : Passed	DEBUG	mark: only supports 32bit mark	WARNING
3DES Software Test:	DEBUG	ipt_time: invalid argument	WARNING
3DES Software Test %s, des3SoftTest(0) ? Failed : Passed	DEBUG	ipt_time: IPT_DAY didn't matched	WARNING
3DES Hardware Test:	DEBUG	./Logs_kernel.txt:45:KERN_WARNING	WARNING
3DES Hardware Test %s, des3HardTest(0) ? Failed : Passed	DEBUG	./Logs_kernel.txt:59:KERN_WARNING	WARNING
DES Software Test:	DEBUG	ipt_LOG: not logging via system console	WARNING
DES Software Test %s, desSoftTest(0) ? Failed : Passed	DEBUG	%s: wrong options length: %u, fname, opt_len	WARNING
DES Hardware Test:	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
DES Hardware Test %s, desHardTest(0) ? Failed : Passed	DEBUG	%s: wrong options length: %u,	WARNING
SHA Software Test:	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
SHA Software Test %s, shaSoftTest(0) ? Failed : Passed	DEBUG	%s: don't know what to do: o[5]=%02x,	WARNING
SHA Hardware Test:	DEBUG	%s: wrong options length: %u, fname, opt_len	WARNING
SHA Hardware Test %s, shaHardTest(0) ? Failed : Passed	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
MD5 Software Test:	DEBUG	%s: wrong options length: %u,	WARNING
MD5 Software Test %s, md5SoftTest(0) ? Failed : Passed	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
MD5 Hardware Test:	DEBUG	%s: don't know what to do: o[5]=%02x,	WARNING
MD5 Hardware Test %s md5HardTest(0) ? Failed : Passed,	DEBUG	*** New port %d ***, ntohs(expinfo- >natport)	WARNING
AES Software Test: %d iterations, iter	DEBUG	** skb len %d, dlen %d,(*pskb)->len,	WARNING
AES Software Test Duration: %d:%d,	DEBUG	********** Non linear skb	WARNING
AES Hardware Test: %d iterations, iter	DEBUG	End of sdp %p, nexthdr	WARNING
AES Hardware Test Duration: %d:%d,	DEBUG	%s: unknown pairwise cipher %d,	WARNING
3DES Software Test: %d iterations, iter	DEBUG	%s: unknown group cipher %d,	WARNING
3DES Software Test Duration: %d:%d,	DEBUG	%s: unknown SIOCSIWAUTH flag %d,	WARNING
3DES Hardware Test: %d iterations, iter	DEBUG	%s: unknown SIOCGIWAUTH flag %d,	WARNING
3DES Hardware Test Duration: %d:%d,	DEBUG	%s: unknown algorithm %d,	WARNING
DES Software Test: %d iterations, iter	DEBUG	%s: key size %d is too large,	WARNING
DES Software Test Duration: %d:%d,	DEBUG	try_module_get failed \	WARNING
DES Hardware Test: %d iterations, iter	DEBUG	%s: request_irq failed, dev->name	WARNING
DES Hardware Test Duration: %d:%d,	DEBUG	try_module_get failed	WARNING
SHA Software Test: %d iterations, iter	DEBUG	try_module_get failed \	WARNING
SHA Software Test Duration: %d:%d,	DEBUG	%s: unknown pairwise cipher %d,	WARNING
SHA Hardware Test: %d iterations, iter	DEBUG	%s: unknown group cipher %d,	WARNING
SHA Hardware Test Duration: %d:%d,	DEBUG	%s: unknown SIOCSIWAUTH flag %d,	WARNING
MD5 Software Test: %d iterations, iter	DEBUG	%s: unknown SIOCGIWAUTH flag %d,	WARNING
MD5 Software Test Duration: %d:%d,	DEBUG	%s: unknown algorithm %d,	WARNING
MD5 Hardware Test: %d iterations, iter	DEBUG	%s: key size %d is too large,	WARNING
MD5 Hardware Test Duration: %d:%d,	DEBUG	unable to load %s, scan_modnames[mode]	WARNING
./pnac/src/pnac/linux/kernel/xcalibur.c:20 9:#define DEBUG_PRINTK printk	DEBUG	Failed to mkdir /proc/net/madwifi	WARNING

ログメッセージ	緊急度	ログメッセージ	緊急度
bcmDeviceInit: registration failed	DEBUG	try_module_get failed	WARNING
bcmDeviceInit: pCdev Add failed	DEBUG	%s: request_irq failed, dev->name	WARNING
REG Size == 8 Bit	DEBUG	too many virtual ap's (already got %d), sc->sc_nvaps	WARNING
Value = %x ::: At Page = %x : Addr = %x	DEBUG	%s: request_irq failed, dev->name	WARNING
REG Size == 16 Bit	DEBUG	rix %u (%u) bad ratekbps %u mode %u,	WARNING
Value = %x ::: At Page = %x : Addr = %x	DEBUG	cix %u (%u) bad ratekbps %u mode %u,	WARNING
REG Size == 32 Bit	DEBUG	%s: no rates for %s?,	WARNING
Value = %x ::: At Page = %x : Addr =%x	DEBUG	no rates yet! mode %u, sc- >sc_curmode	WARNING
REG Size == 64 Bit	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
REG Size is not in 8/16/32/64	DEBUG	dst cache overflow	WARNING
Written Value = %x ::: At Page = %x : Addr = %x	DEBUG	Neighbour table overflow.	WARNING
bcm_ioctl :Unknown Ioctl Case :	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
==========Register Dump for Port Number # %d==========,port	DEBUG	martian destination %u.%u.%u.%u from	WARNING
%s : Read Status=%s data=%#x,regName[j],	DEBUG	martian source %u.%u.%u.%u from	WARNING
%s : Read Status=%s data=%#x,regName[j],	DEBUG	ll header:	WARNING
powerDeviceInit: device registration failed	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
powerDeviceInit: adding device failed	DEBUG	dst cache overflow	WARNING
%s: Error: Big jump in pn number. TID=%d, from %x %x to %x %x.	DEBUG	Neighbour table overflow.	WARNING
%s: The MIC is corrupted. Drop this frame., __func__	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
%s: The MIC is OK. Still use this frame and update PN., __func__	DEBUG	martian destination %u.%u.%u.%u from	WARNING
ADDBA send failed: recipient is not a 11n node	DEBUG	martian source %u.%u.%u.%u from	WARNING
Cannot Set Rate: %x, value	DEBUG	ll header:	WARNING
Getting Rate Series: %x,vap- >iv_fixed_rate.series	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
Getting Retry Series: %x,vap- >iv_fixed_rate.retries	DEBUG	dst cache overflow	WARNING
IC Name: %s,ic->ic_dev->name	DEBUG	Neighbour table overflow.	WARNING
usage: rtparams rt_idx <0|1> per <0..100> probe_intval <0..100>	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
usage: acparams ac <0|3> RTS <0|1> aggr scaling <0..4> min mbps <0..250>	DEBUG	martian source %u.%u.%u.%u from	WARNING
usage: hbrparams ac <2> enable <0|1> per_low <0..50>	DEBUG	ll header:	WARNING
%s(): ADDBA mode is AUTO, __func__	DEBUG	martian destination %u.%u.%u.%u from	WARNING
%s(): Invalid TID value, __func__	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
%s(): ADDBA mode is AUTO, __func__	DEBUG	dst cache overflow	WARNING
%s(): Invalid TID value, __func__	DEBUG	Neighbour table overflow.	WARNING
%s(): Invalid TID value, __func__	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
Addba status IDLE	DEBUG	martian destination %u.%u.%u.%u from	WARNING
%s(): ADDBA mode is AUTO, __func__	DEBUG	martian source %u.%u.%u.%u from	WARNING
%s(): Invalid TID value, __func__	DEBUG	ll header:	WARNING
Error in ADD- no node available	DEBUG	Unable to create ip_set_list	ERROR
%s(): Channel capabilities do not match, chan flags 0x%x,	DEBUG	Unable to create ip_set_hash	ERROR
%s: cannot map channel to mode; freq %u flags 0x%x,	DEBUG	ip_conntrack_in: Frag of proto %u (hook=%u),	ERROR
ic_get_currentCountry not initialized yet	DEBUG	Unable to register netfilter socket option	ERROR
Country ie is %c%c%c,	DEBUG	Unable to create ip_conntrack_hash	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_conntrack slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_expect slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_set_iptreeb slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_set_iptreed slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	%s: cannot allocate space for %scompressor, fname,	ERROR
%s: wrong state transition from %d to %d,	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
ieee80211_deliver_l2uf: no buf available	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
%s: %s, vap->iv_dev->name, buf /* NB: no */	DEBUG	%s: cannot load ARC4 module, fname	ERROR
%s: [%s] %s, vap->iv_dev->name,	DEBUG	%s: cannot load SHA1 module, fname	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: [%s] %s, vap->iv_dev->name, ether_sprintf(mac), buf	DEBUG	%s: CryptoAPI SHA1 digest size too small, fname	ERROR
[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG	%s: cannot allocate space for SHA1 digest, fname	ERROR
[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG	%s%d: trying to write outside history	ERROR
[%s:%s] discard %s information element, %s,	DEBUG	%s%d: trying to write outside history	ERROR
[%s:%s] discard information element, %s,	DEBUG	%s%d: trying to write outside history	ERROR
[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG	%s%d: too big uncompressed packet: %d,	ERROR
[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG	%s%d: encryption negotiated but not an	ERROR
HBR list dumpNode\tAddress\t\t\tState\tTrigger\tB lock	DEBUG	%s%d: error - not an MPPC or MPPE frame	ERROR
Nodes informationAddress\t\t\tBlock\t\tDroped Vl frames	DEBUG	Kernel doesn't provide ARC4 and/or SHA1 algorithms	ERROR
%d\t %2.2x:%2.2x:%2.2x:%2.2x:%2.2x:%2.2x \t%s\t%s\t%s,	DEBUG	PPP: not interface or channel??	ERROR
%2.2x:%2.2x:%2.2x:%2.2x:%2.2x:%2.2x \t%s\t\t%d,	DEBUG	PPP: no memory (VJ compressor)	ERROR
[%d]\tFunction\t%s, j, ni- >node_trace[i].funcp	DEBUG	failed to register PPP device (%d), err	ERROR
[%d]\tMacAddr\t%s, j,	DEBUG	PPP: no memory (VJ comp pkt)	ERROR
[%d]\tDescp\t\t%s, j, ni- >node_trace[i].descp	DEBUG	PPP: no memory (comp pkt)	ERROR
[%d]\tValue\t\t%llu(0x%llx), j, ni- >node_trace[i].value,	DEBUG	ppp: compressor dropped pkt	ERROR
ifmedia_add: null ifm	DEBUG	PPP: no memory (fragment)	ERROR
Adding entry for	DEBUG	PPP: VJ uncompressed error	ERROR
ifmedia_set: no match for 0x%x/0x%x,	DEBUG	ppp_decompress_frame: no memory	ERROR
ifmedia_set: target	DEBUG	ppp_mp_reconstruct bad seq %u < %u,	ERROR
ifmedia_set: setting to	DEBUG	PPP: couldn't register device %s (%d),	ERROR
ifmedia_ioctl: switching %s to , dev- >name	DEBUG	ppp: destroying ppp struct %p but dead=%d	ERROR
ifmedia_match: multiple match for	DEBUG	ppp: destroying undead channel %p !,	ERROR
<unknown type>	DEBUG	PPP: removing module but units remain!	ERROR
desc->ifmt_string	DEBUG	PPP: failed to unregister PPP device	ERROR
mode %s, desc->ifmt_string	DEBUG	%s: cannot allocate space for %scompressor, fname,	ERROR
<unknown subtype>	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
%s, desc->ifmt_string	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
%s%s, seen_option++ ? , : ,	DEBUG	%s: cannot load ARC4 module, fname	ERROR
%s%s, seen_option++ ? , : ,	DEBUG	%s: cannot load SHA1 module, fname	ERROR
%s, seen_option ? > :	DEBUG	%s: CryptoAPI SHA1 digest size too small, fname	ERROR
%s: %s, dev->name, buf	DEBUG	%s: cannot allocate space for SHA1 digest, fname	ERROR
%s: no memory for sysctl table!, __func__	DEBUG	%s%d: trying to write outside history	ERROR
%s: failed to register sysctls!, vap- >iv_dev->name	DEBUG	%s%d: trying to write outside history	ERROR
Atheros HAL assertion failure: %s: line %u: %s,	DEBUG	%s%d: trying to write outside history	ERROR
ath_hal: logging to %s %s, ath_hal_logfile,	DEBUG	%s%d: too big uncompressed packet: %d,	ERROR
ath_hal: logging disabled	DEBUG	%s%d: encryption negotiated but not an	ERROR
%s%s, sep, ath_hal_buildopts[i]	DEBUG	%s%d: error - not an MPPC or MPPE frame	ERROR
ath_pci: No devices found, driver not installed.	DEBUG	Kernel doesn't provide ARC4 and/or SHA1 algorithms	ERROR
---:%d pri:%d qd:%u ad:%u sd:%u tot:%u amp:%d %02x:%02x:%02x,	DEBUG	PPP: not interface or channel??	ERROR
SC Pushbutton Notify on %s::%s,dev- >name,vap->iv_dev->name	DEBUG	PPP: no memory (VJ compressor)	ERROR
Could not find Board Configuration Data	DEBUG	failed to register PPP device (%d), err	ERROR
Could not find Radio Configuration data	DEBUG	PPP: no memory (comp pkt)	ERROR
%s: No device, __func__	DEBUG	ppp: compressor dropped pkt	ERROR
ath_ahb: No devices found, driver not installed.	DEBUG	PPP: no memory (VJ comp pkt)	ERROR
PKTLOG_TAG %s:proc_dointvec failed, __FUNCTION__	DEBUG	PPP: no memory (comp pkt)	ERROR
PKTLOG_TAG %s:proc_dointvec failed, __FUNCTION__	DEBUG	PPP: no memory (fragment)	ERROR
%s: failed to register sysctls!, proc_name	DEBUG	PPP: VJ uncompressed error	ERROR
PKTLOG_TAG %s: proc_mkdir failed, __FUNCTION__	DEBUG	ppp_decompress_frame: no memory	ERROR
PKTLOG_TAG %s: pktlog_attach failed for %s,	DEBUG	ppp_mp_reconstruct bad seq %u < %u,	ERROR
PKTLOG_TAG %s:allocation failed for pl_info, __FUNCTION__	DEBUG	PPP: couldn't register device %s (%d),	ERROR
PKTLOG_TAG %s:allocation failed for pl_info, __FUNCTION__	DEBUG	ppp: destroying ppp struct %p but dead=%d	ERROR
PKTLOG_TAG %s: create_proc_entry failed for %s,	DEBUG	ppp: destroying undead channel %p !,	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
PKTLOG_TAG %s: sysctl register failed for %s,	DEBUG	PPP: removing module but units remain!	ERROR
PKTLOG_TAG %s: page fault out of range, __FUNCTION__	DEBUG	PPP: failed to unregister PPP device	ERROR
PKTLOG_TAG %s: page fault out of range, __FUNCTION__	DEBUG	JBD: bad block at offset %u,	ERROR
PKTLOG_TAG %s: Log buffer unavailable, __FUNCTION__	DEBUG	JBD: corrupted journal superblock	ERROR
PKTLOG_TAG	DEBUG	JBD: bad block at offset %u,	ERROR
Logging should be disabled before changing bufer size	DEBUG	JBD: Failed to read block at offset %u,	ERROR
%s:allocation failed for pl_info, __func__	DEBUG	JBD: error %d scanning journal, err	ERROR
%s: Unable to allocate buffer, __func__	DEBUG	JBD: IO error %d recovering block	ERROR
%s:allocation failed for pl_info, __func__	DEBUG	./Logs_kernel.txt:303:KERN_ERR	ERROR
%s: Unable to allocate buffer, __func__	DEBUG	./Logs_kernel.txt:304:KERN_ERR	ERROR
Atheros HAL assertion failure: %s: line %u: %s,	DEBUG	JBD: recovery pass %d ended at	ERROR
ath_hal: logging to %s %s, ath_hal_logfile,	DEBUG	%s: %s:%d: BAD SESSION MAGIC \	ERROR
ath_hal: logging disabled	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC \	ERROR
%s%s, sep, ath_hal_buildopts[i]	DEBUG	msg->msg_namelen wrong, %d, msg- >msg_namelen	ERROR
failed to allocate rx descriptors: %d, error	DEBUG	addr family wrong: %d, usin->sin_family	ERROR
ath_stoprecv: rx queue %p, link %p,	DEBUG	udp addr=%x/%hu, usin- >sin_addr.s_addr, usin->sin_port	ERROR
no mpdu (%s), __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
Reset rx chain mask. Do internal reset. (%s), __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
OS_CANCEL_TIMER failed!!	DEBUG	socki_lookup: socket file changed!	ERROR
%s: unable to allocate channel table, __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
%s: unable to collect channel list from hal;	DEBUG	%s: %s:%d: BAD SESSION MAGIC \	ERROR
%s: cannot map channel to mode; freq %u flags 0x%x,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC \	ERROR
%s: unable to reset channel %u (%uMhz)	DEBUG	msg->msg_namelen wrong, %d, msg- >msg_namelen	ERROR
%s: unable to restart recv logic,	DEBUG	addr family wrong: %d, usin->sin_family	ERROR
%s: start DFS WAIT period on channel %d, __func__,sc->sc_curchan.channel	DEBUG	udp addr=%x/%hu, usin- >sin_addr.s_addr, usin->sin_port	ERROR
%s: cancel DFS WAIT period on channel %d, __func__, sc- >sc_curchan.channel	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
Non-DFS channel, cancelling previous DFS wait timer channel %d, sc- >sc_curchan.channel	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
%s: unable to reset hardware; hal status %u	DEBUG	socki_lookup: socket file changed!	ERROR
%s: unable to start recv logic, __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
%s: unable to start recv logic, __func__	DEBUG	%s: %s:%d: BAD SESSION MAGIC \	ERROR
%s: unable to reset hardware; hal status %u,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC \	ERROR
hardware error; reseting	DEBUG	msg->msg_namelen wrong, %d, msg- >msg_namelen	ERROR
rx FIFO overrun; reseting	DEBUG	addr family wrong: %d, usin->sin_family	ERROR
%s: During Wow Sleep and got BMISS, __func__	DEBUG	udp addr=%x/%hu, usin- >sin_addr.s_addr, usin->sin_port	ERROR
AC\tRTS \tAggr Scaling\tMin Rate(Kbps)\tHBR \tPER LOW THRESHOLD	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
BE\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
BK\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	socki_lookup: socket file changed!	ERROR
VI\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
VO\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	rebootHook: null function pointer	ERROR
--%d,%p,%lu:0x%x 0x%x 0x%p 0x%x 0x%x 0x%x 0x%x,	DEBUG	Bad ioctl command	ERROR
bb state: 0x%08x 0x%08x, bbstate(sc, 4ul), bbstate(sc, 5ul)	DEBUG	fResetMod: Failed to configure gpio pin	ERROR
%08x %08x %08x %08x %08x %08x %08x %08x%08x %08x %08x %08x,	DEBUG	fResetMod: Failed to register interrupt handler	ERROR
noise floor: (%d, %d) (%d, %d) (%d, %d),	DEBUG	registering char device failed	ERROR
%p: %08x %08x %08x %08x %08x %08x %08x %08x %08x %08x %08x %08x,	DEBUG	unregistering char device failed	ERROR
--%d,%p,%lu:0x%x 0x%x 0x%p 0x%x 0x%x 0x%x 0x%x,	DEBUG	proc entry delete failed	ERROR
%08x %08x %08x %08x %08x %08x %08x %08x%08x %08x %08x %08x,	DEBUG	proc entry initialization failed	ERROR
%s: unable to allocate device object., __func__	DEBUG	testCompHandler: received %s from %d, (char *)pInBuf,	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: unable to attach hardware; HAL status %u,	DEBUG	UMI proto registration failed %d,ret	ERROR
%s: HAL ABI msmatch;	DEBUG	AF_UMI registration failed %d,ret	ERROR
%s: Warning, using only %u entries in %u key cache,	DEBUG	umi initialization failed %d,ret	ERROR
unable to setup a beacon xmit queue!	DEBUG	kernel UMI registration failed!	ERROR
unable to setup CAB xmit queue!	DEBUG	./Logs_kernel.txt:447:KERN_ERR	ERROR
unable to setup xmit queue for BE traffic!	DEBUG	ERROR msm not found properly %d, len %d, msm,	ERROR
%s DFS attach failed, __func__	DEBUG	ModExp returned Error	ERROR
%s: Invalid interface id = %u, __func__, if_id	DEBUG	ModExp returned Error	ERROR
%s:grppoll Buf allocation failed ,__func__	DEBUG	%s: 0x%p len %u, tag, p, (unsigned int)len	ERROR
%s: unable to start recv logic,	DEBUG	%03d:, i	ERROR
%s: Invalid interface id = %u, __func__, if_id	DEBUG	%02x, ((unsigned char *)p)[i]	ERROR
%s: unable to allocate channel table, __func__	DEBUG	mic check failed	ERROR
%s: Tx Antenna Switch. Do internal reset., __func__	DEBUG	%s: 0x%p len %u, tag, p, (unsigned int)len	ERROR
Radar found on channel %d (%d MHz),	DEBUG	%03d:, i	ERROR
End of DFS wait period	DEBUG	%02x, ((unsigned char *)p)[i]	ERROR
%s error allocating beacon, __func__	DEBUG	mic check failed	ERROR
failed to allocate UAPSD QoS NULL tx descriptors: %d, error	DEBUG	[%s] Wrong parameters, __func__	ERROR
failed to allocate UAPSD QoS NULL wbuf	DEBUG	[%s] Wrong Key length, __func__	ERROR
%s: unable to allocate channel table, __func__	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: unable to update h/w beacon queue parameters,	DEBUG	[%s] Wrong Key length, __func__	ERROR
ALREADY ACTIVATED	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: missed %u consecutive beacons,	DEBUG	[%s] Wrong Key length, __func__	ERROR
%s: busy times: rx_clear=%d, rx_frame=%d, tx_frame=%d, __ func__, rx_clear, rx_frame, tx_frame	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: unable to obtain busy times, __func__	DEBUG	[%s] Wrong Key length, __func__	ERROR
%s: beacon is officially stuck,	DEBUG	[%s]: Wrong parameters, __func__	ERROR
Busy environment detected	DEBUG	[%s] Wrong Key Length %d, __func__, des_key_len	ERROR
Inteference detected	DEBUG	[%s] Wrong parameters %d, __func__, des_key_len	ERROR
rx_clear=%d, rx_frame=%d, tx_frame=%d,	DEBUG	[%s] Wrong Key Length %d, __func__, des_key_len	ERROR
%s: resume beacon xmit after %u misses,	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: stuck beacon; resetting (bmiss count %u),	DEBUG	[%s] Wrong Key Length, __func__	ERROR
EMPTY QUEUE	DEBUG	[%s] Wrong parameters, __func__	ERROR
SWRInfo: seqno %d isswRetry %d retryCnt %d,wh ? (*(u_int16_ t *)&wh- >i_seq[0]) >> 4 : 0, bf->bf_isswretry,bf- >bf_swretries	DEBUG	[%s] Wrong Key Length, __func__	ERROR
Buffer #%08X --> Next#%08X Prev#%08X Last#%08X,bf, TAILQ_NEXT(bf,bf_list),	DEBUG	[%s] Wrong parameters, __func__	ERROR
Stas#%08X flag#%08X Node#%08X, bf->bf_status, bf->bf_ flags, bf->bf_node	DEBUG	[%s] Wrong parameters, __func__	ERROR
Descr #%08X --> Next#%08X Data#%08X Ctl0#%08X Ctl1#%08X, bf- >bf_daddr, ds->ds_link, ds->ds_data, ds->ds_ ctl0, ds->ds_ctl1	DEBUG	[%s] Wrong parameters, __func__	ERROR
Ctl2#%08X Ctl3#%08X Sta0#%08X Sta1#%08X,ds->ds_hw[0], ds->ds_hw[1], lastds->ds_hw[2], lastds- >ds_hw[3]	DEBUG	[%s] Wrong parameters, __func__	ERROR
Error entering wow mode	DEBUG	device name=%s not found, pReq- >ifName	ERROR
Wakingup due to wow signal	DEBUG	unable to register KIFDEV to UMI	ERROR
%s, wowStatus = 0x%x, __func__, wowStatus	DEBUG	ERROR: %s: Timeout at page %#0x addr %#0x	ERROR
Pattern added already	DEBUG	ERROR: %s: Timeout at page %#0x addr %#0x	ERROR
Error : All the %d pattern are in use. Cannot add a new pattern , MAX_NUM_PATTERN	DEBUG	Invalid IOCTL %#08x, cmd	ERROR
Pattern added to entry %d ,i	DEBUG	%s: unable to register device, dev- >name	ERROR
Remove wake up pattern	DEBUG	ath_pci: 32-bit DMA not available	ERROR
mask = %p pat = %p ,maskBytes,patternBytes	DEBUG	ath_pci: cannot reserve PCI memory region	ERROR
mask = %x pat = %x ,(u_int32_t)maskBytes, (u_int32_t) patternBytes	DEBUG	ath_pci: cannot remap PCI memory region) ;	ERROR
Pattern Removed from entry %d ,i	DEBUG	ath_pci: no memory for device state	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Error : Pattern not found	DEBUG	%s: unable to register device, dev- >name	ERROR
PPM STATE ILLEGAL %x %x, forcePpmStateCur, afp->forceState	DEBUG	ath_dev_probe: no memory for device state	ERROR
FORCE_PPM %4d %6.6x %8.8x %8.8x %8.8x %3.3x %4.4x,	DEBUG	%s: no memory for device state, __func__	ERROR
failed to allocate tx descriptors: %d, error	DEBUG	kernel MIBCTL registration failed!	ERROR
failed to allocate beacon descripotrs: %d, error	DEBUG	Bad ioctl command	ERROR
failed to allocate UAPSD descripotrs: %d, error	DEBUG	WpsMod: Failed to configure gpio pin	ERROR
hal qnum %u out of range, max %u!,	DEBUG	WpsMod: Failed to register interrupt handler	ERROR
HAL AC %u out of range, max %zu!,	DEBUG	registering char device failed	ERROR
HAL AC %u out of range, max %zu!,	DEBUG	unregistering char device failed	ERROR
%s: unable to update hardware queue %u!,	DEBUG	%s:%d - ERROR: non-NULL node pointer in %p, %p<%s>!	ERROR
Multicast Q:	DEBUG	%s:%d - ERROR: non-NULL node pointer in %p, %p<%s>!	ERROR
%p , buf	DEBUG	can't alloc name %s, name	ERROR
buf flags - 0x%08x --------- , buf- >bf_flags	DEBUG	%s: unable to register device, dev- >name	ERROR
buf status - 0x%08x, buf->bf_status	DEBUG	failed to automatically load module: %s; \	ERROR
# frames in aggr - %d, length of aggregate - %d, length of frame - %d, sequence number - %d, tidno - %d,	DEBUG	Unable to load needed module: %s; no support for \	ERROR
isdata: %d isaggr: %d isampdu: %d ht: %d isretried: %d isxretried: %d shpreamble: %d isbar: %d ispspoll: %d aggrburst: %d calcairtime: %d qosnulleosp: %d,	DEBUG	Module \%s\ is not known, buf	ERROR
%p: 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x,	DEBUG	Error loading module \%s\, buf	ERROR
0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x,	DEBUG	Module \%s\ failed to initialize, buf	ERROR
0x%08x 0x%08x 0x%08x 0x%08x,	DEBUG	ath_pci: 32-bit DMA not available	ERROR
sc_txq[%d] : , i	DEBUG	ath_pci: cannot reserve PCI memory region	ERROR
tid %p pause %d : , tid, tid->paused	DEBUG	ath_pci: cannot remap PCI memory region) ;	ERROR
%d: %p , j, tid->tx_buf[j]	DEBUG	ath_pci: no memory for device state	ERROR
%p , buf	DEBUG	%s: unable to attach hardware: '%s' (HAL status %u),	ERROR
axq_q:	DEBUG	%s: HAL ABI mismatch;	ERROR
%s: unable to reset hardware; hal status %u, __func__, status	DEBUG	%s: failed to allocate descriptors: %d,	ERROR
****ASSERTION HIT****	DEBUG	%s: unable to setup a beacon xmit queue!,	ERROR
MacAddr=%s,	DEBUG	%s: unable to setup CAB xmit queue!,	ERROR
TxBufIdx=%d, i	DEBUG	%s: unable to setup xmit queue for %s traffic!,	ERROR
Tid=%d, tidno	DEBUG	%s: unable to register device, dev- >name	ERROR
AthBuf=%p, tid->tx_buf[i]	DEBUG	%s: autocreation of VAP failed: %d,	ERROR
%s: unable to reset hardware; hal status %u,	DEBUG	ath_dev_probe: no memory for device state	ERROR
%s: unable to reset hardware; hal status %u,	DEBUG	kdot11RogueAPEnable called with NULL argument.	ERROR
%s: unable to start recv logic,	DEBUG	kdot11RogueAPEnable: can not add more interfaces	ERROR
_fmt, __VA_ARGS__ \	DEBUG	kdot11RogueAPGetState called with NULL argument.	ERROR
sample_pri=%d is a multiple of refpri=%d, sample_pri, refpri	DEBUG	kdot11RogueAPDisable called with NULL argument.	ERROR
==========ft- >ft_numfilters=%u==========, ft->ft_numfilters	DEBUG	%s: SKB does not exist., __FUNCTION__	ERROR
filter[%d] filterID = %d rf_numpulses=%u; rf->rf_minpri=%u; rf->rf_maxpri=%u; rf->rf_threshold=%u; rf- >rf_filterlen=%u; rf->rf_mindur=%u; rf- >rf_maxdur=%u,j, rf->rf_pulseid,	DEBUG	%s: recvd invalid skb	ERROR
NOL	DEBUG	unable to register KIFDEV to UMI	ERROR
WARNING!!! 10 minute CAC period as channel is a weather radar channel	DEBUG	The system is going to factory defaults.....!!!	CRITICAL
%s disable detects, __func__	DEBUG	%s, msg	CRITICAL
%s enable detects, __func__	DEBUG	%02x, *(data + i)	CRITICAL
%s disable FFT val=0x%x , __func__, val	DEBUG	Inside crypt_open in driver ######	CRITICAL
%s enable FFT val=0x%x , __func__, val	DEBUG	Inside crypt_release in driver ######	CRITICAL
%s debug level now = 0x%x , __func__, dfs_debug_level	DEBUG	Inside crypt_init module in driver @@@@@@@@	CRITICAL
RateTable:%d, maxvalidrate:%d, ratemax:%d, pRc->rateTableSize,k,pRc- >rateMaxPhy	DEBUG	Inside crypt_cleanup module in driver @@@@@@@@	CRITICAL

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: txRate value of 0x%x is bad., __FUNCTION__, txRate	DEBUG	SKB is null : %p ,skb	CRITICAL
Valid Rate Table:-	DEBUG	DST is null : %p ,dst	CRITICAL
Index:%d, value:%d, code:%x, rate:%d, flag:%x, i, (int) validRateIndex[i],	DEBUG	DEV is null %p %p ,dev,dst	CRITICAL
RateTable:%d, maxvalidrate:%d, ratemax:%d, pRc- >rateTableSize,k,pRc- >rateMaxPhy	DEBUG	Packet is Fragmented %d,pBufMgr- >len	CRITICAL
Can't allocate memory for ath_vap.	DEBUG	Marked the packet proto:%d sip:%x dip:%x sport:%d dport:%d spi:%d,isr:%p:%p %p	CRITICAL
Unable to add an interface for ath_dev.	DEBUG	SAV CHECK FAILED IN DECRYPTION	CRITICAL
%s: [%02u] %-7s , tag, ix, ciphers[hk- >kv_type]	DEBUG	FAST PATH Breaks on BUF CHECK	CRITICAL
%02x, hk->kv_val[i]	DEBUG	FAST PATH Breaks on DST CHECK	CRITICAL
mac %02x-%02x-%02x-%02x-%02x-%02x, mac[0], mac[1], mac[2], mac[3], mac[4], mac[5]	DEBUG	FAST PATH Breaks on MTU %d %d %d, bufMgrLen(pBufMgr),mtu,dst_mtu(p Dst->path)	CRITICAL
mac 00-00-00-00-00-00	DEBUG	FAST PATH Breaks on MAX PACKET %d %d, bufMgrLen(pBufMgr),IP_MAX_PACKET	CRITICAL
%02x, hk->kv_mic[i]	DEBUG	SAV CHECK FAILED IN ENCRYPTION	CRITICAL
txmic	DEBUG	Match Found proto %d spi %d,pPktInfo->proto, pFlowEntry- >pre.spi	CRITICAL
%02x, hk->kv_txmic[i]	DEBUG	PRE: proto: %u srcip:%u.%u.%u.%u sport :%u dstip: %u.%u.%u.%u dport: %u,	CRITICAL
Cannot support setting tx and rx keys individually	DEBUG	POST: proto: %u srcip:%u.%u.%u.%u sport :%u dstip: %u.%u.%u.%u dport: %u,	CRITICAL
bogus frame type 0x%x (%s),	DEBUG	Clearing the ISR %p,p	CRITICAL
ERROR: ieee80211_encap ret NULL	DEBUG	PROTO:%d %u.%u.%u.%u--- >%u.%u.%u.%u,	CRITICAL
ERROR: ath_amsdu_attach not called	DEBUG	ESP-DONE: %p %p,sav,m	CRITICAL
%s: no memory for cwm attach, __func__	DEBUG	ESP-BAD: %p %p,sav,m	CRITICAL
%s: error - acw NULL. Possible attach failure, __func__	DEBUG	Bug in ip_route_input_slow().	CRITICAL
%s: unable to abort tx dma, __func__	DEBUG	Bug in ip_route_input_slow().	CRITICAL
%s: no memory for ff attach, __func__	DEBUG	Bug in ip_route_input \	CRITICAL
Failed to initiate PBC based enrolle association	DEBUG	Bug in ip_route_input_slow().	CRITICAL
KERN_EMERG Returing error in INTR registration	DEBUG	AH: Assigning the secure flags for sav :%p,sav	CRITICAL
KERN_EMERG Initialzing Wps module	DEBUG	ESP: Assigning the secure flags for sav :%p skb:%p src:%x dst:%x,sav,skb,ip- >ip_src.s_addr,ip->ip_dst.s_addr	CRITICAL
%s:%d %s, __FILE__, __LINE__, __func__	DEBUG	%s Buffer %d mtu %d path mtu %d header %d trailer %d,__func__,bufMgrLen(pBufMgr),mtu, dst_mtu(pDst- >path),pDst- >header_len,pDst->trailer_len	CRITICAL