

IoT/M2M ゲートウェイ

MMLink-GWL

**ユーザーマニュアル
(基本編)**

株式会社 YE DIGITAL

内容

第1章 はじめに.....	6
1.1 はじめに.....	6
1.2 内容品リスト.....	6
1.2.1 梱包の内容.....	6
1.3 ハードウェア構成.....	7
1.4 LED 表示.....	8
1.5 設置および保守に関する注意事項.....	9
1.5.1 システム要件.....	9
1.5.2 警告.....	9
1.5.3 金属筐体の表面温度に関する注意事項.....	10
1.6 ハードウェアの設置.....	11
1.6.1 ユニットを取り付ける.....	11
1.6.2 SIM カードを挿入する.....	11
1.6.3 電源の接続.....	12
1.6.4 シリアルデバイスの接続.....	12
1.6.5 ネットワークまたはホストへの接続.....	12
1.6.6 Web UI による設定.....	13
第2章 基本ネットワーク.....	14
2.1 WAN および Uplink.....	14
2.1.1 物理インターフェイス.....	15
2.1.2 インターネット設定.....	16
2.2 LAN.....	29
2.2.1 イーサネット LAN.....	29
2.2.2 DHCP サーバー.....	32
2.3 ポート転送.....	40
2.3.1 設定.....	41
2.3.2 仮想サーバーおよび仮想コンピュータ.....	42

2.3.3 DMZ およびパススルー	48
2.4 ルーティング	51
2.4.1 静的ルーティング	52
2.4.2 動的ルーティング	55
2.4.3 ルーティング情報	63
2.5 DNS および DDNS	64
2.5.1 DNS および DDNS 設定	64
第3章 オブジェクト定義	68
3.1 スケジュール	68
3.1.1 スケジュール設定	68
3.2 グループ	70
3.2.1 ホストグループ	70
3.3 外部サーバー	72
3.3.1 設定	72
3.4 証明書	76
3.4.1 設定	76
3.4.2 自己署名証明書	79
3.4.3 信頼済み証明書	86
3.4.4 証明書発行	93
第4章 フィールド通信	96
4.1 バスおよびプロトコル	96
4.1.1 ポート設定	96
4.1.2 仮想 COM	98
第5章 セキュリティ	109
5.1 VPN	109
5.1.1 IPSec	110
5.1.2 OpenVPN	125
5.1.3 L2TP	138

5.1.4 PPTP	146
5.1.5 GRE	153
5.2 ファイアウォール	158
5.2.1 パケットフィルタ	158
5.2.2 MAC 制御	164
5.2.3 IPS	167
5.2.4 オプション	171
第 6 章 管理	175
6.1 設定および管理	175
6.1.1 コマンドスクリプト	176
6.1.2 TR-069	179
6.1.3 SNMP	185
6.1.4 Telnet & SSH	195
6.2 システム操作	199
6.2.1 パスワードおよび MMI	199
6.2.2 システム情報	203
6.2.3 システム時刻	204
6.2.4 システムログ	208
6.2.5 バックアップおよび復元	214
6.2.6 再起動およびリセット	215
6.3 診断	217
6.3.1 診断ツール	217
第 7 章 サービス	219
7.1 セルラーツールキット	219
7.1.1 データ使用量	220
7.1.2 SMS	223
7.1.3 SIM PIN	227
7.1.4 USSD	232

7.1.5 ネットワークスキャン.....	236
7.2 イベント処理.....	238
7.2.1 設定.....	239
7.2.2 管理イベント.....	243
7.2.3 通知イベント.....	246
第8章 ステータス.....	249
8.1 基本ネットワーク.....	249
8.1.1 WAN および Uplink ステータス.....	249
8.1.2 LAN ステータス.....	254
8.1.3 DDNS ステータス.....	255
8.2 セキュリティ.....	256
8.2.1 VPN ステータス.....	256
8.2.2 ファイアウォールステータス.....	261
8.3 管理.....	264
8.3.1 設定および管理ステータス.....	264
8.4 統計およびレポート.....	266
8.4.1 接続状況.....	266
8.4.2 デバイス管理.....	267
8.4.3 セルラー使用状況.....	268
第9章 Fieldbus.....	269
付録 A GNU ライセンスについて.....	271

第1章 はじめに

1.1 はじめに

MMLink-GWL（以降、本製品と略称します）をお買い上げいただき、誠にありがとうございます。本製品はLTE通信モジュールを搭載しており、IoT（Internet of things）／M2M（Machine to machine）システムでの通信機器として、最適にご利用いただけます。

主な機能：

- 4G/LTE 無線ネットワーク網への接続ができます。
- デュアルSIMが使用可能で、フェールセーフ機能を実現できます。
- VPNなどの様々な通信プロトコルを標準搭載しており、高性能ルーターとしてご利用いただけます。
- 本体は頑丈で取り付けがしやすい金属製で、ビジネス環境や様々なIoT/M2M用途に最適です。

1.2 内容品リスト

1.2.1 梱包の内容

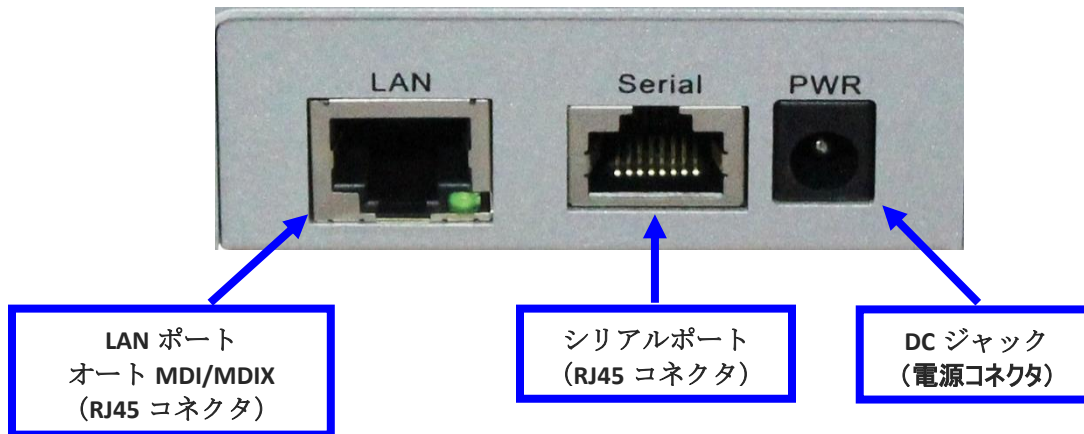
標準パッケージ

項目	説明	内容品	数量
1	MMLink-GWL（本体）		1個
2	セルラーアンテナ		2個
3	電源アダプター (DC 5V/2A) (*1)		1個

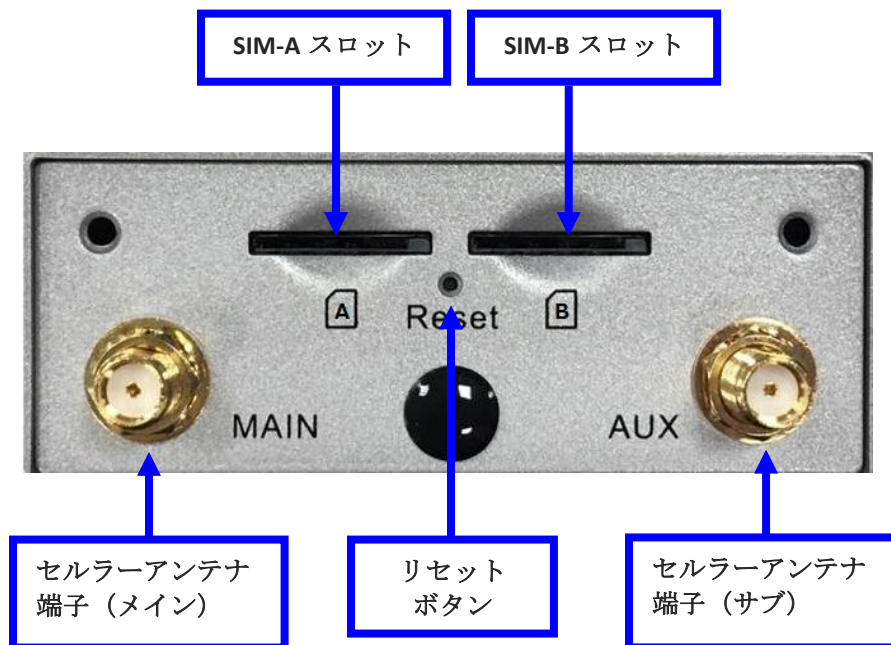
1 本製品の最大消費電力は、5.5Wです。

1.3 ハードウェア構成

➤ 左側



➤ 右側



※リセットボタン

電源投入時にリセットボタンを6秒間押し続けてから放すと、本製品内の設定値は工場出荷時のデフォルト設定に戻ります。

1.4 LED 表示



表示	LED の色	説明
Signal LTE/3G	青 紫色 赤色	<p>本 LED は表示色でセルラー網との接続状態を、表示パターンで信号強度を表します。</p> <p>■LED 表示色</p> <ul style="list-style-type: none"> ・青色：LTE 網に接続 ・紫色：3G 網に接続 ・赤色：2G 網に接続 <p>■LED 表示パターン</p> <ul style="list-style-type: none"> ・高速点滅：信号強度は 0～30% ・低速点滅(*1)：信号強度は 31～60% ・常時点灯：信号強度は 61～100% <p>(*1) 低速点滅は約 1.5～2 秒周期で点滅</p>
Uplink SIM-A/B	青色 紫色 赤色	<p>本 LED は表示色で利用している SIM スロット(SIM-A or B)を、表示パターンで WAN 側との PPP 接続状態を表します。</p> <ul style="list-style-type: none"> ・LED 無点灯：WAN 側との PPP 未接続 ・青色で点滅：SIM-A を利用して、WAN 側との PPP 接続中 ・青色で常時点灯：SIM-A を利用して、WAN 側との PPP 接続確立 ・青色と紫色が交互に点滅：SIM-A を利用して、WAN 側とのデータ通信中 ・赤色で点滅：SIM-B を利用して、WAN 側との PPP 接続中 ・赤色で常時点灯：SIM-B を利用して、WAN 側との PPP 接続確立 ・赤色と紫色が交互に点滅：SIM-B を利用して、WAN 側とのデータ通信中
Serial	青色	<p>点滅：シリアルデータ送受信中</p>
Status	青色	<p>常時点灯：ファームウェアが起動中</p> <p>1 秒周期に点滅 (500msec 点灯/500msec 消灯)：ファームウェアが正常動作している。</p> <p>高速点滅：リカバリモードまたは異常状態。</p> <p>注：電源のオフ/オンをしても Status LED の高速点滅が解消されない場合、販売元までお問い合わせください。</p>
LAN	緑色	<p>常時点灯：LAN のイーサネット接続が確立</p> <p>点滅：データパケット転送中</p>

1.5 設置および保守に関する注意事項

1.5.1 システム要件

ネットワーク要件	<ul style="list-style-type: none">イーサネットRJ45ケーブル3G /4Gセルラーサービスに加入契約しているPCに10/100Mbpsイーサネットアダプターが搭載されている
ブラウザ要件	<p>次の仕様のコンピュータ：</p> <ul style="list-style-type: none">Windows®、Macintosh、Linuxベースのオペレーティングシステムイーサネットアダプター <p>ブラウザの要件:</p> <ul style="list-style-type: none">Internet Explorer 6.0以降Chrome 2.0以降Firefox 3.0以降Safari 3.0以降

1.5.2 警告



注意

- 電源アダプターはパッケージに付属のもののみを使用してください。電圧定格が異なる電源アダプターの使用は危険をともない、本製品を損傷する可能性があります。
- ケースを自分で開いたり修理したりしないでください。製品が非常に高温になっている場合は、ただちに電源を切断し、販売元へ修理を依頼してください。
- 本製品は安定した場所に設置してください。本製品と付属品は屋外で使用しないでください。

1.5.3 金属筐体の表面温度に関する注意事項



注意： 本製品の金属製筐体の表面温度は、非常に高くなる恐れがあります。特に、空調のない閉じたキャビネットに設置された環境や周囲温度が高い環境で長時間動作させた後に発生します。保守点検等で、本製品の熱された金属筐体表面に直接指で触れないよう注意してください。

1.6 ハードウェアの設置

本章では、ハードウェアの設置および使用方法について説明します。

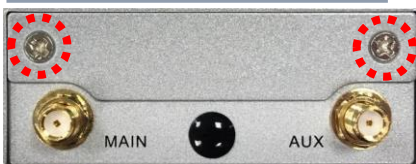
1.6.1 ユニットを取り付ける

本製品は、デスクトップ上、または、壁に取り付けることができます。

1.6.2 SIM カードを挿入する

SIM カードスロットは、本製品のハウジングの右側にあり、SIM カードを保護する役割があります。SIM カードの取り付けや取り外しを行う場合、次の手順に従ってください。

ステップ 1:
ネジを緩め、SIM カバーを取り外します。



ステップ 2:
SIM カードをスロット A (SIM-A) またはスロット B (SIM-B) に押し込みます。



ステップ 3:
SIM カードを取り外す場合、挿入した SIM カードを再度押して、SIM スロットから取り出します。



注意

- 本製品はmicroSIMのみサポートしております。
- SIMカードを挿入する際に、SIMスロットの奥までしっかり差し込んでください。
- SIMカードの挿入や取り外しを行う前に、必ず本製品の電源をオフにしてください。
- 本製品稼働中にSIMカードの挿入や取り外しを行うと、SIMカードが破損する恐れがあります。

1.6.3 電源の接続

本製品の標準付属品には、DC5V/2A 電源アダプター¹があります。本製品に他の DC 電源を使って給電する場合は、DC 電源の電圧が 5V で、電極がその割り当て（「+」は DC 電源用、「-」は GND 線用）に従って正しく接続されていることを確認してください。

1.6.4 シリアルデバイスの接続

本製品は、1 つの RJ45 コネクタのシリアルポートを有します。以下にシリアルコネクタのピン配置を示します。

RJ45 シリアルソケットのピン出力

RJ45 ソケット



8 1

ピン出力の定義

	ピン 1	ピン 2	ピン 3	ピン 4	ピン 5	ピン 6	ピン 7	ピン 8
RS-232	DCD	RXD	TXD	DTR	GND	DSR	RTS	CTS
RS-485			DATA+	DATA-	GND			

注：ピン出力が、ご利用のシリアルデバイスと互換性があることを確認してください。互換性がない場合、適切なピン割り当てを持つ特殊変換ケーブルを準備しなければなりません。

1.6.5 ネットワークまたはホストへの接続

本製品には 1 つの RJ45 コネクタの LAN ポートを有し、10/100Mbps イーサネットに接続できます。本製品の LAN ポートは、Auto MDI/MDI-X をサポートしています。

¹ 本製品の最大消費電力は、5.5W です。

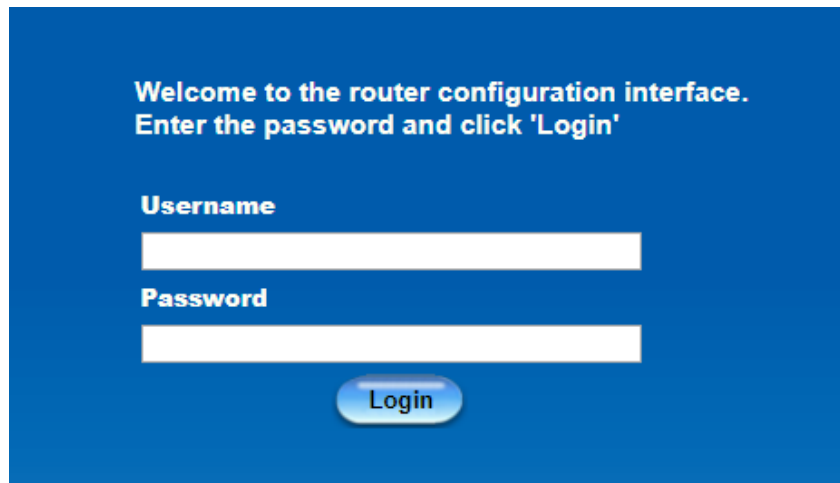
1.6.6 Web UI による設定

デバイスの設定は Web UI (Web ブラウザ) から行います。

Web ブラウザを開き、アドレス欄に IP アドレス (<http://192.168.123.254>) を入力します。¹



ログインページでユーザ名「admin」パスワード「admin」²を入力し、[Login] ボタンをクリックします。

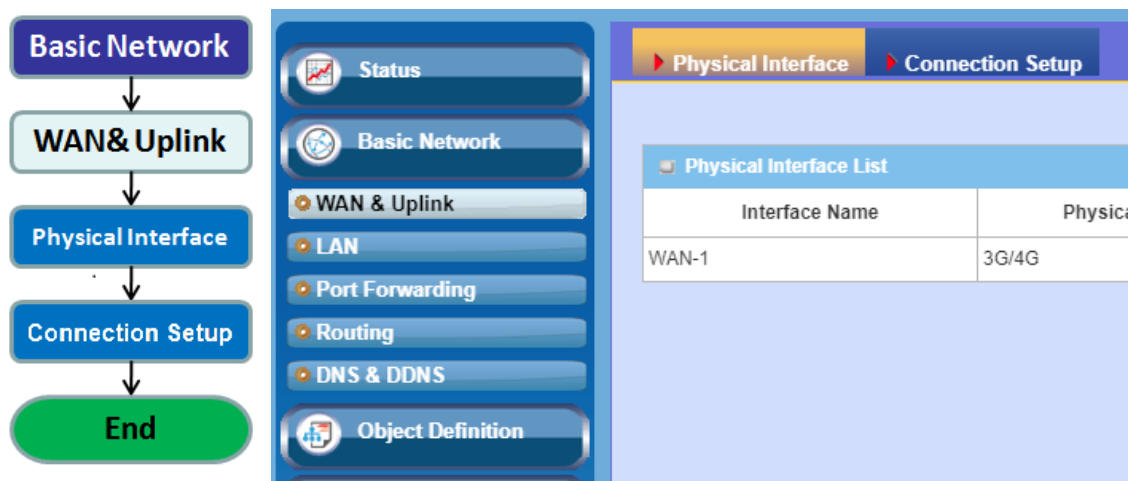
A screenshot of a login page for a router configuration interface. The background is a solid blue color. At the top, white text reads: "Welcome to the router configuration interface. Enter the password and click 'Login'". Below this text are two white input fields. The first field is labeled "Username" and the second is labeled "Password". At the bottom center of the form is a blue, rounded rectangular button with the word "Login" written in white.

¹ 本製品のデフォルトの LAN IP アドレスは 192.168.123.254 です。

² ログインパスワードは、デフォルト値から変更することを推奨します。

第 2 章 基本ネットワーク

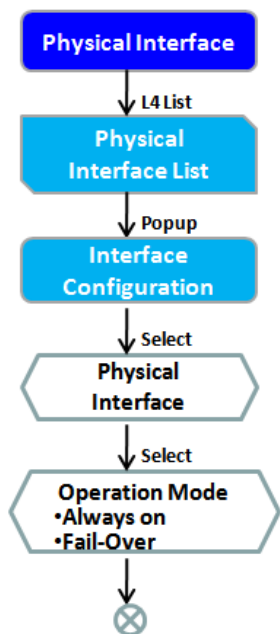
2.1 WAN および Uplink



本製品は 1 つの WAN インターフェイスを提供し、イントラネット内の全クライアントホストが ISP を介してインターネットにアクセスできるようになります。

本章では、WAN 接続するための設定手順について説明します。

2.1.1 物理インターフェイス



Physical Interface List			
Interface Name	Physical Interface	Operation Mode	Action
WAN-1	3G/4G	Always on	<input type="button" value="Edit"/>

Interface Configuration (WAN - 1)	
Item	Setting
▶ Physical Interface	3G/4G ▾
▶ Operation Mode	Always on ▾
▶ VLAN Tagging	<input type="checkbox"/> Enable <input type="text" value="0"/> (1-4095)

物理インターフェイスの設定

本製品の物理インターフェイスの設定は不要です。

2.1.2 インターネット設定

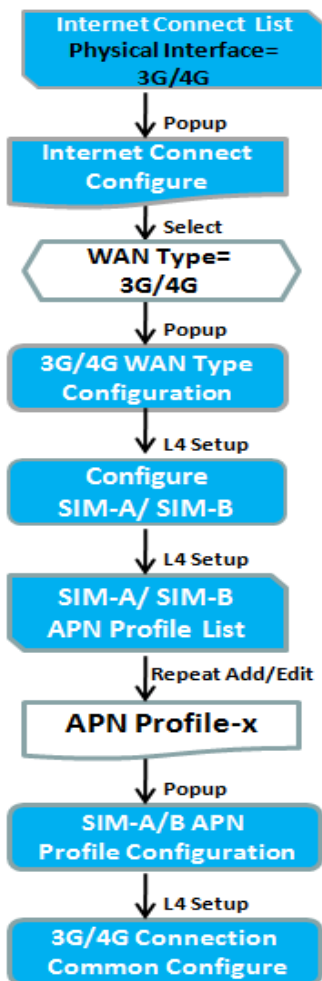
Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	<input type="button" value="Edit"/>

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	3G/4G ▼

3G/4G WAN Type Configuration	
Item	Setting
▶ Preferred SIM Card	SIM-A Only ▼
▶ Auto Flight Mode	<input type="checkbox"/> Enable

「Internet Connection List」ウィンドウで、WAN-1 インターフェイスの「Edit」ボタンをクリックすると、「Internet Connection Configuration」ウィンドウが表示されます。このウィンドウで、インターネット接続するために必要な各種パラメータを設定します。

インターネット接続 - 3G/4G WAN



Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	<input type="button" value="Edit"/>

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	3G/4G ▼

3G/4G WAN Type Configuration	
Item	Setting
▶ Preferred SIM Card	SIM-A First ▼ Failback: <input type="checkbox"/> Enable
▶ Auto Flight Mode	<input type="checkbox"/> Enable

Connection with SIM-A Card	
Item	Setting
▶ Network Type	Auto ▼
▶ Dial-Up Profile	Manual-configuration ▼
▶ APN	<input type="text"/>
▶ IP Type	IPv4 ▼
▶ PIN Code	<input type="text"/> (Optional)
▶ Dial Number	*99***1# (Optional)
▶ Account	<input type="text"/> (Optional)
▶ Password	<input type="text"/> (Optional)
▶ Authentication	Auto ▼
▶ IP Mode	Dynamic IP ▼
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Roaming	<input type="checkbox"/> Enable

優先 SIM カード - デュアル SIM フェールオーバー

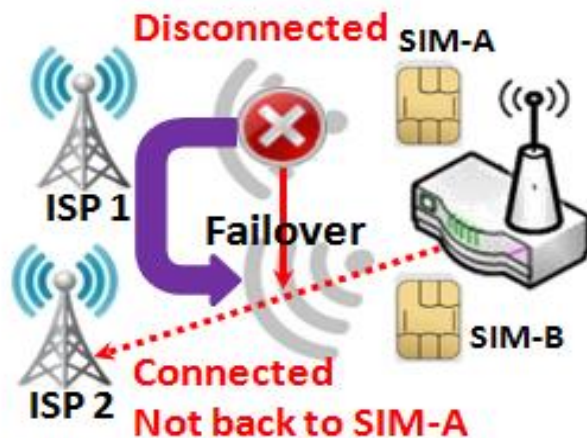
本製品は、デュアルSIMカードによるフェールオーバー機能を備えています。この機能は、移動体での利用時の地理的位置が変更された場合や、ISP 切り替えを行う場合に有用です。

本製品の SIM カード設定には、「Failback」を有効化または無効化した状態での「SIM-A First」、「SIM-B First」、「SIM-A Only」および「SIM-B Only」を含む様々なユースケースがあります。

SIM-A/SIM-B Only

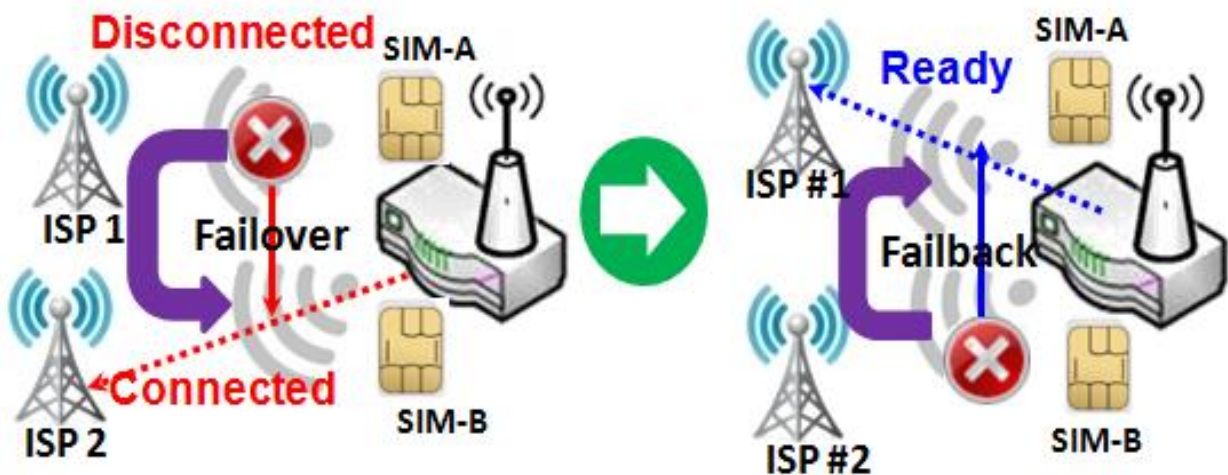
「SIM-A Only」または「SIM-B Only」を設定した場合、本製品とセルラーISP 間の接続には、指定した SIM カードスロットしか使用しません。

SIM-A / SIM-B First (Failback 有効化無し)



「SIM-A First」を設定した場合、本製品は初めに SIM-A を使用してインターネットへの接続を試みます（他方、「SIM-B First」を設定した場合、本製品は初めに SIM-B を使用してインターネットへの接続を試みます）。その後、インターネット接続が切断されると、本製品は自動的に代替用の他の SIM カードを使用するように切り替わります（「SIM-A First」の場合、SIM-B を使用するように切り替わります）。そして、現在の接続が切断されない限り、元の SIM カードを使用するように、スイッチバックすることはありません。つまり、SIM-A と SIM-B は現在のインターネット切断を契機に交互に使用されますが、現在のインターネット接続が切断されない限り、その SIM カードが継続して使用されます。

SIM-A / SIM-B First (Failback 有効化有り)



Failback オプションを有効化した「SIM-A First」では、インターネット接続が切断された場合に、本製品は SIM-B を使用するように切り替わりますが、SIM-A カードの接続が回復すると、SIM-A カードを使用するようにスイッチバックします。

インターネット設定

Basic Network > WAN & Uplink > Connection Setup タブに進みます。

Connection Setup より、本製品の WAN 接続を設定することができます。**Internet Connection List** ウィンドウに各 WAN の基本情報が表示されます。

[Edit] ボタンをクリックして設定します。

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	<input type="button" value="Edit"/>

Internet Connection List		
項目	値設定	説明
Interface Name	-	WAN インターフェ이스の名称を表示します。
Physical Interface	-	Physical Interface (3G/4G) には、 Interface Name と共にマッピングするために設定するインターフェ이스のタイプが表示されます。
Operation Mode	-	インターフェ이스の動作モードを定義します。 この WAN を常に有効にするには、Always on (常にオン) を選択します。 (注 : WAN-1 の場合、Always on (常にオン) オプションのみが利用可能です。
WAN Type	-	WAN Type には、ご利用の ISP に対する接続タイプが表示されます。 本製品では、次の WAN 接続タイプのみをサポートしています。 • 3G/4G

インターネット設定 - 3G/4G WAN

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	<input type="button" value="Edit"/>

3G/4G WAN 設定を行う

Edit ボタンをクリックされると、Internet Connection Configuration および 3G/4G WAN Type Configuration ウィンドウが表示されます。

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	3G/4G ▼

3G/4G WAN Type Configuration	
Item	Setting
▶ Preferred SIM Card	SIM-A Only ▼
▶ Auto Flight Mode	<input type="checkbox"/> Enable

Internet Connection Configuration WAN Type Configuration

項目	値設定	説明
WAN Type	1. 必須入力項目 2. デフォルト値： 3G/4G	ドロップダウンボックスから、3G/4G WAN 接続に対するインターネット接続方法を選択します。 3G/4G のみが利用可能です。
Preferred SIM	1. 必須入力項目 2. デフォルト値： SIM-A Only	<p>接続用にどの SIM カードを使用するかを選択します。 SIM-A First または SIM-B First が選択されている場合、初めに SIM A/SIM B を使って接続が確立されることを意味します。そして接続に失敗した場合、他の SIM カードに切り替わり、接続が確立するまで再度ダイヤルアップを試みます。 SIM-A only または SIM-B only が選択されている場合、選択した SIM カードのみを使って、ダイヤルアップを試みます。 Failback の Enable チェックボックスにチェックが入っている場合、代替 SIM から優先 SIM にフェールバックします。</p> <p>注_1： SIM カードを 1 枚のみ利用する場合、SIM-A Only をご利用ください。 注_2： Failback は、SIM-A First または SIM-B First が選択されているときのみ利用可能です。</p>

Auto Flight Mode

デフォルト値 :
チェック外す

Enable ボックスをチェックして機能を有効にします。
デフォルトでは、オートフライトモードを無効にすると、セルラーモジュールは常に携帯電話タワーで物理チャンネルを占有します。それは即座にデータ接続を得ることができ、管理 SMS は常に必要な時に受信できます。
自動機内モードを有効にすると、ゲートウェイは「フライトモードでデータセッションがオフラインになると携帯機能が誤動作する」というメッセージを表示し、携帯電話モジュールを**自動機内モード**にします。
注：セルラーISPが接続されているゲートウェイから自動機内モードを有効にするよう要求されない限り、チェックしないでください。

SIM-A/SIM-B カードを設定する

ここでは、利用する SIM カードに応じた 3G/4G ネットワーク接続のためのパラメータ設定を行います。

Connection with SIM-A Card	
Item	Setting
▶ Network Type	Auto ▼
▶ Dial-Up Profile	Manual-configuration ▼
▶ APN	<input type="text"/>
▶ IP Type	IPv4 ▼
▶ PIN Code	<input type="text"/> (Optional)
▶ Dial Number	*99***1# (Optional)
▶ Account	<input type="text"/> (Optional)
▶ Password	<input type="text"/> (Optional)
▶ Authentication	Auto ▼
▶ IP Mode	Dynamic IP ▼
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Roaming	<input type="checkbox"/> Enable

注_1：SIM-B カードの構成は、SIM-A カードの構成と同じ規則に従います。ここでは、例として SIM-A の一覧を表示しています。

注_2：Preferred SIM Card で SIM-A First または SIM-B First が選択されている場合のみ、Connection with SIM-A Card および Connection with SIM-B Card の両方がポップアップ表示されます。そうでない場合は、どちらか一方のみがポップアップ表示されます。

Connection with SIM-A/SIM-B Card		
項目	値設定	説明
Network Type	1. 必須入力項目 2. デフォルト値 : Auto	Auto、3G Only、3G prefer、LTE Only が選択可能です。 Auto オプションを選択すると、どのネットワークへレジストレーションするかは自動的に選択されます。 Only オプションが選択されている場合は、選択したネットワークのみへ、接続を試みます。 Prefer オプションが選択されている場合は、そのネットワークを優先し、接続を試みます。
Dial-Up Profile	1. 必須入力項目 2. デフォルト値 : Manual-Configuration	3G/4G ネットワークへの接続に使用するダイヤルアッププロファイル種別を指定します。 Auto-detection 、 Manual-configuration 、 APN Profile List から選択可能です。 Manual-configuration を選択した場合、 APN 、 Dial Number 、 Account 、 Password の 4 つのパラメータ設定が必要です。利用するキャリアから提供された内容を設定してください。 Dial Number のデフォルト値は*99***1#になります。 APN Profile List を選択した場合、接続が確立されるまで順番にダイヤルアップするプロファイルを複数設定します。詳細については、 Basic Network > WAN & Uplink > Connection Setup > SIM-A/B APN Profile List に進んでください。 ダイヤルアップに必要なすべての設定を自動的に取得するには、 Auto-Detection を選択します。 注 1 : 回線契約したネットワークを指定するために、 Manual-configuration または APN Profile List を選択することを強く推奨します。ISP は、加入者に対してこのようなネットワーク設定を必ず提供します。 注 2 : Auto-detection を選択した場合、不適切なネットワークに接続する可能性があります。また、ご利用の ISP に対する有効な APN を検索できない可能性があります。
APN	1. 必須入力項目 2. 文字列形式 : 任意のテキスト	ダイヤルアップ接続先となる APN (アクセスポイント名) を入力します。 Dial-Up Profile で Manual-configuration を選択した場合に表示され、必須入力です。
IP Type	1. 設定を入力しなければなりません 2. 文字列形式 : IP アドレス (IPv4 タイプ)	3G / 4G ネットワークが提供するネットワークサービスの IP タイプを指定します。IPv4、IPv6、または IPv4 / 6 が選択可能です。 本機は IPv4 のみサポートします。

PIN Code	文字列形式：整数	ご利用のSIMカードのロック解除が必要な場合、PIN（個人識別番号）を入力してください。
Authentication	1. 必須入力項目 2. デフォルト値： Auto	PAP を選択した場合、パスワード認証プロトコルを使って、キャリアのサーバーとの認証を試みます。 CHAP を選択した場合、チャレンジハンドシェイク認証プロトコルを使って、キャリアのサーバーとの認証を試みます。 Auto を選択した場合、 PAP または CHAP いずれかのプロトコルを用いて、サーバーとの認証を試みます。
IP Mode	1. 必須入力項目 2. デフォルト値： Dynamic IP	Dynamic IP を選択した場合、キャリアのサーバーから全ての IP 設定情報を取得し、直接本製品に対して設定されます。 キャリアにより提供された IP アドレスを設定をする場合は、 Static IP を選択します。 IP Address 、 IP Subnet Mask 、 IP Gateway のフィールドが表示されるので、必要なすべてのパラメータを入力します。 注：Static IP 選択時の IP Subnet Mask は、必須入力設定です。正しく設定されていない場合、接続に問題が生じます。
Primary DNS	文字列形式：IPアドレス（IPv4タイプ）	本フィールドが空白の場合、プライマリ DNS（ドメインネームサービス）の IP アドレスは、ダイヤルアップ接続でキャリアより与えられた IP アドレスを使用します。 本フィールドに IP アドレスを入力した場合、プライマリ DNS の IP アドレスは入力値を使用します。
Secondary DNS	文字列形式：IPアドレス（IPv4タイプ）	本フィールドが空白の場合、セカンダリ DNS（ドメインネームサービス）の IP アドレスは、ダイヤルアップ接続でキャリアより与えられた IP アドレスを使用します。 本フィールドに IP アドレスを入力した場合、セカンダリ DNS の IP アドレスは入力値を使用します。
Roaming	デフォルト値：チェックなし	レジストレーション状態がホームネットワークではなく、ローミングであるとき、接続を確立するにはチェックボックスにチェックを入れます。 注 1： 接続がローミング下にあるとき、追加費用が請求される場合があります。

SIM-A / SIM-B APN Profile List の作成編集

接続用に新しい APN プロファイルの追加や、追加した APN プロファイルの編集をすることができます。これは、**Dial-Up Profile** で **APN Profile List** が選択されているときのみ、利用可能です。

SIM-A APN Profile List <input type="button" value="Add"/> <input type="button" value="Delete"/>									
ID	Profile Name	APN	IP Type	Account	Password	Authentication	Priority	Enable	Actions

作成したすべての APN プロファイルが一覧表示されます。[Add] ボタンがクリックされると、**APN Profile Configuration** ウィンドウが表示されます。

SIM-A APN Profile Configuration	
Item	Setting
▶ Profile Name	<input type="text" value="Profile-1"/>
▶ APN	<input type="text"/>
▶ IP Type	IPv4 <input type="button" value="v"/>
▶ Account	<input type="text"/> (Optional)
▶ Password	<input type="text"/> (Optional)
▶ Authentication	Auto <input type="button" value="v"/>
▶ Priority	<input type="text"/>
▶ Profile	<input type="checkbox"/> Enable

APN Profile List APN Profile Configuration		
項目	値設定	説明
Profile Name	1. デフォルト値： Profile-x が一覧表示 2. 文字列形式：任意のテキスト	このプロファイルの名前を入力します。
APN	文字列形式：任意のテキスト	ダイヤルアップ接続先となる APN（アクセスポイント名）を入力します。
IP Type	1. 設定を入力しなければなりません 2. デフォルトでは、 IPv4 が選択されています。	IPv4 ネットワークを利用するには、 IPv4 を選択します。 IPv6 ネットワークを利用するには、 IPv6 を選択します。 IPv4 と IPv6 ネットワークを利用するには、 IPv4/6 を選択します。
Account	文字列形式：任意のテキスト	認証で使用するアカウントを入力します。 値の範囲：0~53 文字
Password	文字列形式：任意のテキスト	認証で使用するパスワードを入力します。
Authentication	1. 必須入力項目 2. デフォルト値： Auto	3G/4G 接続に対する認証方法を選択します。 Auto 、 PAP 、 CHAP 、または、 None を選択することができます。 PAP を選択した場合、パスワード認証プロトコルを使って、キャリアのサーバーと認証します。 CHAP を選択した場合、チャレンジハンドシェイク認証プロトコルを使って、キャリアのサーバーと認証します。 Auto を選択した場合、 PAP または CHAP いずれかのサーバーと認証します。
Priority	1. 必須入力項目 2. 文字列形式：整数	ダイヤルアップする順序の値を入力します。有効な値は、1~16 です。最も小さい番号が割り当てられたプロファイル順に、ダイヤルアップを開始します。 値の範囲：1~16。
Profile	デフォルト値：チェックなし	チェックボックスにチェックを入れて、このプロファイルを有効化します。ダイヤルアップからこのプロファイルが無効化するには、チェックボックスのチェックを外します。
Save	-	Save ボタンをクリックして、設定を保存します。
Close	-	Close ボタンをクリックすると、画面が前ページに戻ります。

3G/4G 接続の共通設定

ここで、3G/4G WAN に対する共通設定を変更することができます。

3G/4G Connection Common Configuration	
Item	Setting
▶ Connection Control	Auto-reconnect ▼
▶ Time Schedule	(0) Always ▼
▶ MTU Setup	<input type="checkbox"/> Enable
▶ IP Passthrough (Cellular Bridge)	<input type="checkbox"/> Enable Fixed MAC : <input type="text"/>
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ IGMP	Disable ▼
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>

3G/4G Connection Common Configuration		
項目	値設定	説明
Connection Control	デフォルト値 : Auto-reconnect	<p>Auto-reconnect が選択されている場合、常にインターネット接続を維持することを意味します。</p> <p>Connect-on-demand が選択されている場合、データトラフィックが検出されます。</p> <p>Connect Manually が選択されている場合、Connect ボタンをクリックされたとき、インターネット接続が確立されません。詳細は、Basic Network > WAN & Uplink タブに進んでください。</p> <p>注 1 : このフィールドは、Basic Network > WAN & Uplink > Physical Interface > Operation Mode が、Always on に選択されている場合のみ利用可能です。</p> <p>注 2 : Auto-reconnect が選択されている場合、自動再接続が正常に動作していることを確認するため、ネットワーク監視機能がオプションで選択可能です。</p>
Maximum Idle Time	1. 任意の設定 2. デフォルト値 : 600 秒	<p>接続アイドルタイムアウト時にインターネット接続を切断する最大アイドル時間を指定します。</p> <p>値の範囲 : 300~86400。</p> <p>注 : このフィールドは、Connect-on-demand または Connect Manually が選択されている場合のみ利用可能です。</p>
Time Schedule	1. 必須入力項目 2. デフォルト値 :	<p>(0) Always が選択されている場合、この WAN は、常に動作中であることを意味します。別のスケジュールルールを設定</p>

	(0) Always	した場合、他のオプションが選択可能です。詳細については、 Object Definition > Scheduling に進んでください。
MTU	1. 必須入力項目 2. デフォルト値 : 0 3. 文字列形式 : 整数	3G/4G 接続に対する MTU (最大伝送単位) を指定します。 値の範囲 : 512~1500 (自動の場合は、0 を設定します)。
IP Pass-through (Cellular Bridge)	1. デフォルト値 : チェックなし 2. Fixed MAC に対する文字列形式 : MAC アドレス (例えば、00:50:18:aa:bb:cc)	Enable チェックボックスにチェックが入っている場合、本製品は、初めて接続するローカル LAN クライアントに対して、直接 WAN IP を割り当てることを意味します。しかし、オプションの Fixed MAC にゼロでない値が入力されている場合、この MAC アドレスを持つクライアントのみが、WAN IP アドレスを取得できることを意味します。 注_1 : このフィールドは、3G/4G-n が、 WAN-1 に設定されている場合のみ利用可能です。 注_2 : IP Pass-through がオンである場合、 NAT および WAN IP Alias は、機能が再度無効化されるまで利用できません。
NAT	デフォルト値 : チェックあり	NAT (ネットワークアドレス変換) 機能を無効化するには、チェックボックスのチェックを外します。
IGMP	デフォルト値 : Disable	Auto を選択すると、 IGMP 機能を有効化します。 Enable チェックボックスにチェックを入れると、 IGMP Proxy を有効化します。
WAN IP Alias	1. デフォルト値 : チェックなし 2. 文字列形式 : IP アドレス (IPv4 タイプ)	チェックボックスにチェックを入れて、 WAN IP Alias を有効化し、割り当てる IP アドレスを入力します。

Network Monitoring Configuration	
Item	Setting
▶ Network Monitoring Configuration	<input type="checkbox"/> Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	<input checked="" type="checkbox"/> Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)
▶ Fail Threshold	5 (Times)
▶ Target1	DNS1 ▼
▶ Target2	None ▼

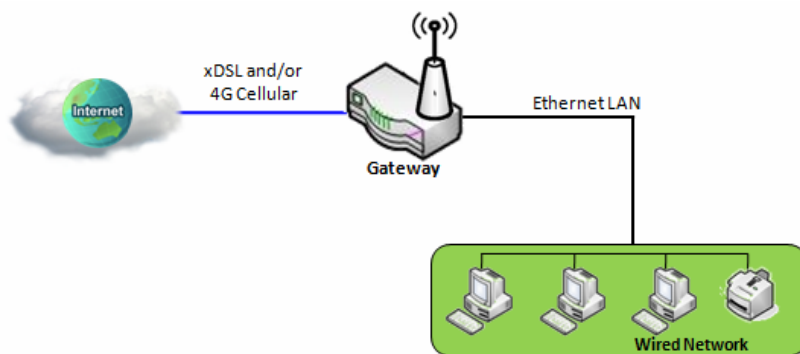
ネットワーク監視構成		
項目	値設定	説明
Network Monitoring Configuration	1. オプション設定 2. デフォルト値： チェックなし	[Enable]チェックボックスをオンにすると、ネットワーク監視機能が有効になります。 注：オンデマンド接続または手動接続の場合、それを無効化しても、自動再接続に変更すると、Enable チェックボックスに自動的にチェックが入ります。
Checking Method	1. オプション設定 2. デフォルト値： DNS Query	DNS Query (DNS クエリ) または ICMP Checking (ICMP チェッキング) を選択して、WAN リンクを検出します。 DNS Query (DNS クエリ) を使って、システムは、DNS クエリパケットをターゲット1 およびターゲット2 で指定される宛先に送信することにより、接続を確認します。 ICMP Checking (ICMP チェッキング) を使って、システムは、ICMP 要求パケットを指定された宛先に送信することにより、接続を確認します。
Loading Check	1. オプション設定 2. デフォルト値： チェックあり	本機能を有効化すると、帯域幅が完全に占有されている場合、本製品に未応答の DNS クエリまたは ICMP 要求を無視することを許可します。これにより、ネットワーク監視機能による意図しないネットワーク切断を防ぐことができます。
Query Interval	1. オプション設定 2. デフォルト値：5	DNS クエリまたは ICMP チェックの通信周期を定義します。 値の範囲：2～14400 秒。
Latency Threshold	1. オプション設定 2. デフォルト値： 3000	応答時間のしきい値を定義します。 通信先が無応答の場合、60 秒後にタイムアウトが発生します。 値の範囲：2000～60000 ミリ秒。
Fail Threshold	1. オプション設定 2. デフォルト値：5	WAN のリンクダウンを検出する為の切断を確認するしきい値を定義します。 値の範囲：1～10 回。
Target 1	1. オプションの設定 2. デフォルト値： DNS1	Target1 (デフォルトでは、 DNS1 設定されます) は、DNS クエリ/ICMP 要求を送信する最初のターゲットを指定します。 DNS1 ：ターゲットにあるプライマリ DNS を設定します。 DNS2 ：ターゲットであるセカンダリ DNS を設定します。 ゲートウェイ ：現在のゲートウェイをターゲットに設定します。 Other Host (他のホスト) ：ターゲットである IP アドレスを入力します。
Target 2	1. オプションの設定 2. デフォルト値： None	Target1 は、DNS クエリ/ICMP 要求を送信する 2 番目のターゲットを指定します。 なし：2 番目のターゲットは必要ありません。 DNS1 ：ターゲットにあるプライマリ DNS を設定します。 DNS2 ：ターゲットであるセカンダリ DNS を設定します。 ゲートウェイ ：現在のゲートウェイをターゲットに設定します。 Other Host (他のホスト) ：ターゲットである IP アドレスを入

		力します。
Save (保存)	-	Save (保存) ボタンをクリックして、構成を保存します。
Undo (元に戻す)	-	Undo (元に戻す) ボタンをクリックして、構成した内容を元の設定に復元します。

2.2 LAN

このセクションでは、LAN の設定について説明します。

2.2.1 イーサネット LAN



ローカルエリアネットワーク（LAN）を使い、ネットワークに接続されたコンピュータ間で、データまたはファイルを共有することができます。左の図は、コンピュータを配線して相互接続するネットワークを示しています。

IPv4イーサネットLAN設定を行うには、次の手順に従ってください。

Basic Network > LAN > Ethernet LAN タブに進みます。

Configuration	
Item	Setting
▶ IP Mode	Static IP
▶ LAN IP Address	<input type="text" value="192.168.123.254"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>

Configuration		
項目	値設定	説明
IP Mode	-	<p>関連する構成に従って、ゲートウェイの LAN IP モードを示します。</p> <p>Static IP: 少なくとも 1 つの WAN インターフェイスが有効になっている場合、LAN IP モードは、静的 IP モードで固定されます。</p> <p>Dynamic IP: 使用可能な WAN インターフェイスがすべて無効になっている場合、LAN IP モードは、動的 IP モードになります。</p>

LAN IP Address	1. 必須入力項目 2. デフォルト値： 192.168.123.254	本製品のローカル IP アドレスを入力します。 ネットワーク上のネットワークデバイスは、本製品の LAN IP アドレスをデフォルトゲートウェイとして使用する必要があります。この設定は必要があれば変更することができます。 注：これは Web UI の IP アドレスでもあります。変更した場合、Web UI を表示するにはブラウザに新しい IP アドレスを入力する必要があります。
Subnet Mask	1. 必須入力項目 2. デフォルト値： 255.255.255.0 (/24)	ドロップダウンリストから、本製品に対するサブネットマスクを選択します。サブネットマスクは、1つのネットワークまたはサブネットで使用できるクライアントの数を定義します。デフォルトのサブネットマスクは 255.255.255.0 (/24) です。これは、このサブネットで最大 254 個の IP アドレスを使用できることを表します。実際には、そのうちの 1つは本製品の LAN IP アドレスとして使用されるため、LAN ネットワークで使用できるクライアント数は最大で 253 台です。 値の範囲： 255.0.0.0 (/8)~255.255.255.252 (/30)。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定した内容を元の内容に復元します。

Create / Edit Additional IP

本製品は、特別な管理のために LAN IP エイリアス機能が備わっています。本製品に LAN IP を追加し、その追加された IP を使って、本製品にアクセスすることができます。

Additional IP <input type="button" value="Add"/> <input type="button" value="Delete"/>						
ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

Add ボタンをクリックされると、Additional IP Configuration ウィンドウが表示されます。

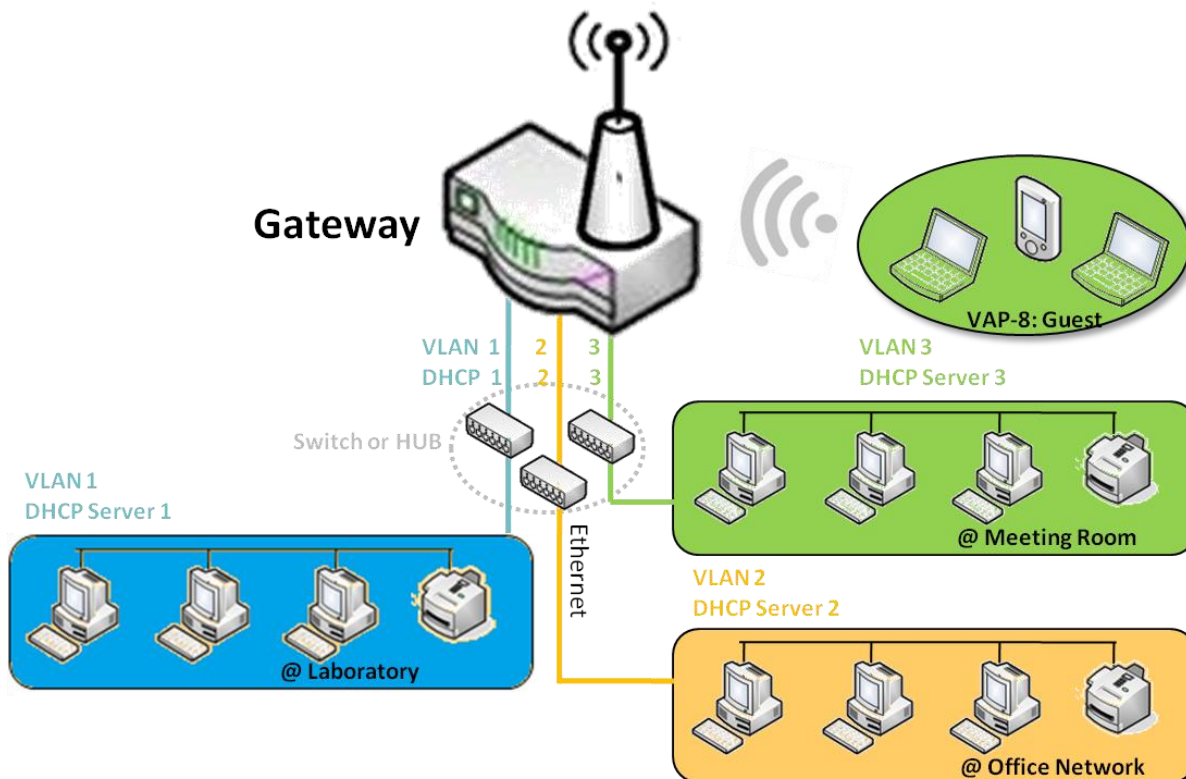
Additional IP Configuration	
Item	Setting
▶ Name	<input type="text"/>
▶ Interface	lo ▼
▶ IP Address	<input type="text"/>
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ Enable	<input type="checkbox"/>
<input type="button" value="Save"/>	

Additional IP Configuration		
項目	値設定	説明
Name	任意の設定	エイリアス IP アドレスの名称を入力します。
Interface	1. 必須入力項目 2. デフォルト値 : lo	インターフェイスタイプを指定します。lo または br0 が選択可能です。
IP Address	1. 任意の設定 2. デフォルト値 : なし	本製品に対する追加 IP アドレスを入力します。
Subnet Mask	1. 必須入力項目 2. デフォルト値 : 255.255.255.0 (/24)	ドロップダウンリストから、本製品に対するサブネットマスクを選択します。サブネットマスクは、1つのネットワークまたはサブネットで使用できるクライアントの数を定義します。デフォルトのサブネットマスクは 255.255.255.0 (/24) です。これは、このサブネット内で最大 254 個の IP アドレスを使用できることを表します。実際には、そのうちの 1 つは本製品の LAN IP アドレスとして使用されるため、LAN ネットワークで使用できるクライアント数は最大で 253 台です。 値の範囲 : 255.0.0.0 (/8) ~ 255.255.255.255 (/32)。
Enable	デフォルト値 : チェックなし	Enabl チェックボックスをクリックして、本設定を有効化します。
Save	-	Save ボタンをクリックして、設定を保存します

2.2.2 DHCP サーバー

➤ DHCP サーバー

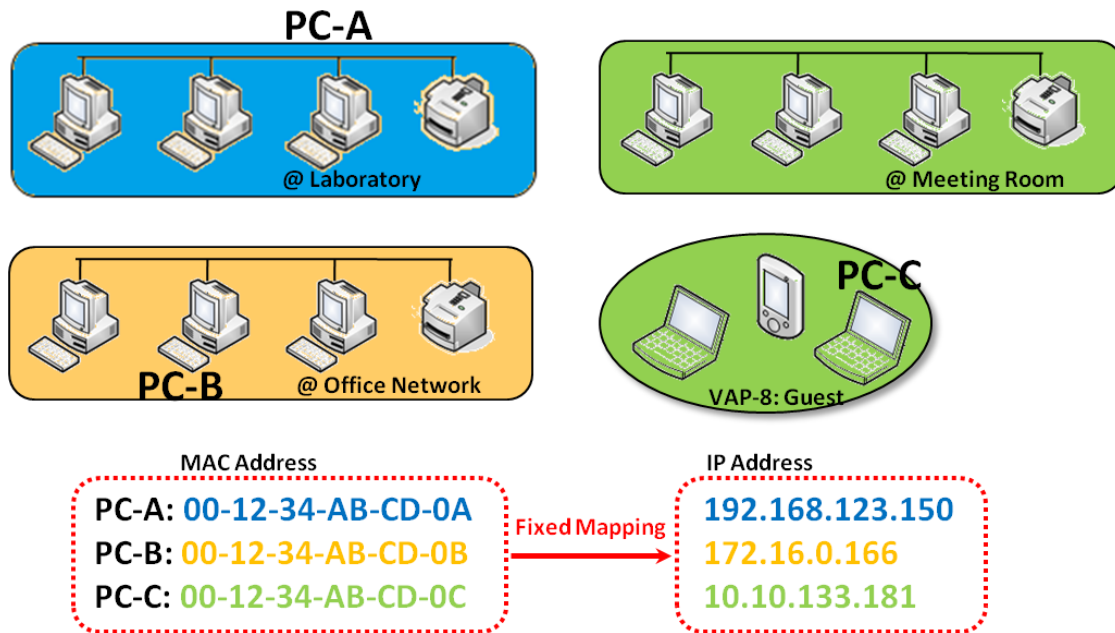
VLAN サポート機種では、異なる VLAN グループからの DHCP 要求を満たすために最大 4 台の DHCP サーバーをサポートします。但し、本製品は VLAN をサポートしていない為、DHCP サーバーを 1 つに設定して使用してください。



ユーザーは、「DHCP Server List」の「Add」ボタンをクリックすることで、DHCP サーバー設定を追加することができます。またリスト内の各 DHCP サーバーの右側にある「Edit」ボタンをクリックし、現在の設定を編集することができます。また、DHCP サーバーの「Select」チェックボックスをチェックし「Delete」ボタンをクリックすることにより、削除することができます。

➤ 固定マッピング

DHCP Client List にターゲットがすでに存在している場合、ユーザーは、固定 IP アドレスを割り当て、特定のクライアント MAC アドレスを選択し、そのターゲットをマッピングルールにコピーすることができます。または、ターゲットの MAC アドレスの接続準備ができていないとき、事前に手動でいくつかの他のマッピングルールを追加することができます。



DHCP サーバーリスト

Basic Network > LAN > DHCP Server タブに進みます。

DHCP サーバー設定では、DHCP サーバーポリシーを作成およびカスタマイズして、ローカルエリアネットワーク（LAN）上のデバイスに IP アドレスを割り当てることができます。

DHCP サーバーポリシーの作成/編集

DHCP サーバーポリシーをカスタム設定することができます。複数の LAN ポートが利用可能な場合、LAN（または VLAN グループ）ごとに 1 つのポリシーを定義し、最大 4 つのポリシーをサポートできます。

DHCP Server List												Add	Delete	DHCP Client List	[Help]
DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions			
DHCP 1	192.168.123.254	255.255.255.0	192.168.123.100-192.168.123.200	3600		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	Edit	Fixed Mapping		

Add ボタンがクリックされると、DHCP Server Configuration ウィンドウが表示されます。

DHCP Server Configuration	
Item	Setting
▶ DHCP Server Name	<input type="text" value="DHCP 2"/>
▶ LAN IP Address	<input type="text" value="192.168.2.254"/>
▶ Subnet Mask	<input type="text" value="255.0.0.0 (/8)"/> ▼
▶ IP Pool	Starting Address: <input type="text"/> Ending Address: <input type="text"/>
▶ Lease Time	<input type="text" value="86400"/> seconds
▶ Domain Name	<input type="text"/> (Optional)
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Primary WINS	<input type="text"/> (Optional)
▶ Secondary WINS	<input type="text"/> (Optional)
▶ Gateway	<input type="text"/> (Optional)
▶ Server	<input type="checkbox"/> Enable

DHCP Server List DHCP Server Configuration		
項目	値設定	説明
DHCP Server Name	1.文字列形式：任意のテキスト 2. 必須入力項目	DHCP サーバー名を入力します。
LAN IP Address	1. IPv4 形式です。 2. 必須入力項目	DHCP サーバーの IP アドレスです。
Subnet Mask	デフォルト値： 255.255.255.0 (/24)	DHCP サーバーのサブネットマスクです。
IP Pool	1. IPv4 形式です。 2. 必須入力項目	DHCP サーバーの IP プールです。開始アドレスと終了アドレスで構成されます。
Lease Time	1. 数値文字列形式です。 2. 必須入力項目	DHCP サーバーのリース時間です。 <u>値の範囲</u> ：300～604800 秒。
Domain Name	文字列形式：任意のテキスト	DHCP サーバーのドメイン名です。
Primary DNS	IPv4 形式です	DHCP サーバーのプライマリ DNS です。
Secondary DNS	IPv4 形式です	DHCP サーバーのセカンダリ DNS です。
Primary WINS	IPv4 形式です	DHCP サーバーのプライマリ WINS です。
Secondary WINS	IPv4 形式です	DHCP サーバーのセカンダリ WINS です。
Gateway	IPv4 形式です	DHCP サーバーのゲートウェイです。
Server	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本 DHCP サーバーを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックすると、設定した内容が元の設定に復元されます。
Back	-	Back ボタンをクリックすると、画面が DHCP Server Configuration ページに戻ります。

DHCP サーバー上のマッピングルールの作成/編集

DHCP サーバー上のマッピングルールをカスタム設定することができます。これは、最大 64 のルールセットをサポートします。Fixed Mapping ボタンをクリックされると、Mapping Rule List ウィンドウが表示されます。

Mapping Rule List <input type="button" value="Add"/> <input type="button" value="Delete"/> [Help]			
MAC Address	IP Address	Enable	Actions

Add ボタンがクリックされると、Mapping Rule Configuration ウィンドウが表示されます。

Mapping Rule Configuration	
Item	Setting
▶ MAC Address	<input type="text"/>
▶ IP Address	<input type="text"/>
▶ Rule	<input type="checkbox"/> Enable

Mapping Rule Configuration		
項目	値設定	説明
MAC Address	1. MAC アドレスの文字列形式です 2. 必須入力項目	本マッピングルールの MAC アドレスです。
IP Address	1. IPv4 形式です。 2. 必須入力項目	本マッピングルールの IP アドレスです。
Rule	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本ルールを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定した内容を元の設定に復元します。
Back	-	Back ボタンをクリックすると、DHCP Server Configuration 画面に戻ります。

DHCP クライアントリストの表示/コピー

DHCP Client List ボタンがクリックされると、DHCP Client List ウィンドウが表示されます。

DHCP Client List Copy to Fixed Mapping					
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic /192.168.123.100	James-P45V	74:D0:2B:62:8D:42	00:49:07	<input type="checkbox"/> Select

リストに表示された DHCP クライアントの **Select** チェックボックスにチェックを入れ、**Copy to Fixed Mapping** ボタンがクリックされると、IP および MAC アドレスが特定の DHCP サーバー上の **Mapping Rule List** に自動的に反映されます。

DHCP サーバーオプションの有効化/無効化

DHCP Server Option Configuration を有効化することで、DHCP サーバ機能を利用することができます。
Enable ボタンをクリックして、DHCP オプション機能を有効化します。

Configuration	
Item	Setting
DHCP Server Options	<input type="checkbox"/> Enable

DHCP サーバーオプションの作成/編集

本製品は、最大 99 のオプション設定をサポートします。

DHCP Server Option List Add Delete							
ID	Option Name	DHCP Sever Select	Option Select	Type	Value	Enable	Actions

Add/Edit ボタンをクリックされると、DHCP Server Option Configuration ウィンドウが表示されます。

DHCP Server Option Configuration Save Undo	
Item	Setting
Option Name	<input type="text" value="Option 1"/>
DHCP Sever Select	<input type="text" value="DHCP 1"/>
Option Select	<input type="text" value="DHCP OPTION 66"/>
Type	<input type="text" value="Single IP Address"/>
Value	<input type="text"/>
Enable	<input type="checkbox"/> Enable

DHCP Server Option Configuratio		
項目	値設定	説明
Option Name	1. 文字列形式：任意のテキスト 2. 必須入力項目	DHCP サーバーオプション名を入力します。
DHCP Server Select	利用可能な全 DHCP サーバーのドロップダウンリストです。	このオプションが適用される DHCP サーバーを選択します。
Option Select	1. 必須入力項目 2. デフォルト値： Option 66	ドロップダウンリストから特定のオプションを選択します。これは、Option 66、Option 72、Option 114、Option 42、Option 150、または Option 160 のいずれかになります。

		TFTP サーバ名の場合は Option 66 WWW サーバアドレスの場合は、 Option 72 URL の場合は、 Option 114 NTP サーバアドレスの場合は、 Option 42 TFTP サーバのアドレス、イーサネット、GRUB 設定の場合は、 Option 150 TFTP の場合は Option 160	
Type	DHCP サーバオプションの値のタイプのドロップダウンリスト	Option Select により、異なる値のタイプを持ちます。	
		66 単一 IP アドレス	
		単一 FQDN	
		72 「,」により区切られた IP アドレスリスト	
		114 単一 URL	
		42 「,」により区切られた IP アドレスリスト	
		150 「,」により区切られた IP アドレスリスト	
Value	1. IPv4 形式です 2. FQDN 形式です 3. IP リストです 4. URL 形式です 5. 必須入力項目	次のタイプに準拠する必要があります：	
		Type	Value
		66 単一 IP アドレス	IPv4 形式です
		単一 FQDN	FQDN 形式です
		72 「,」により区切られた IP アドレスリスト	「,」により区切られた IPv4 形式
		114 単一 URL	URL 形式です
		42 「,」により区切られた IP アドレスリスト	「,」により区切られた IPv4 形式
150 「,」により区切られた IP アドレスリスト	「,」により区切られた IPv4 形式		
160	単一 IP アドレス	IPv4 形式です	
	単一 FQDN	FQDN 形式です	
Enable	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本設定を有効化します。	
Save	-	Save ボタンをクリックして、設定を保存します。	
Undo	-	Undo ボタンをクリックすると、画面が元に戻ります。	

DHCP リレーの作成/編集

本製品は、最大 6 の DHCP リレー構成をサポートします。

DHCP Relay Configuration List Add Delete							
ID	Agent Name	LAN interface	WAN interface	Server IP	DHCP Relay Option 82	Enable	Actions

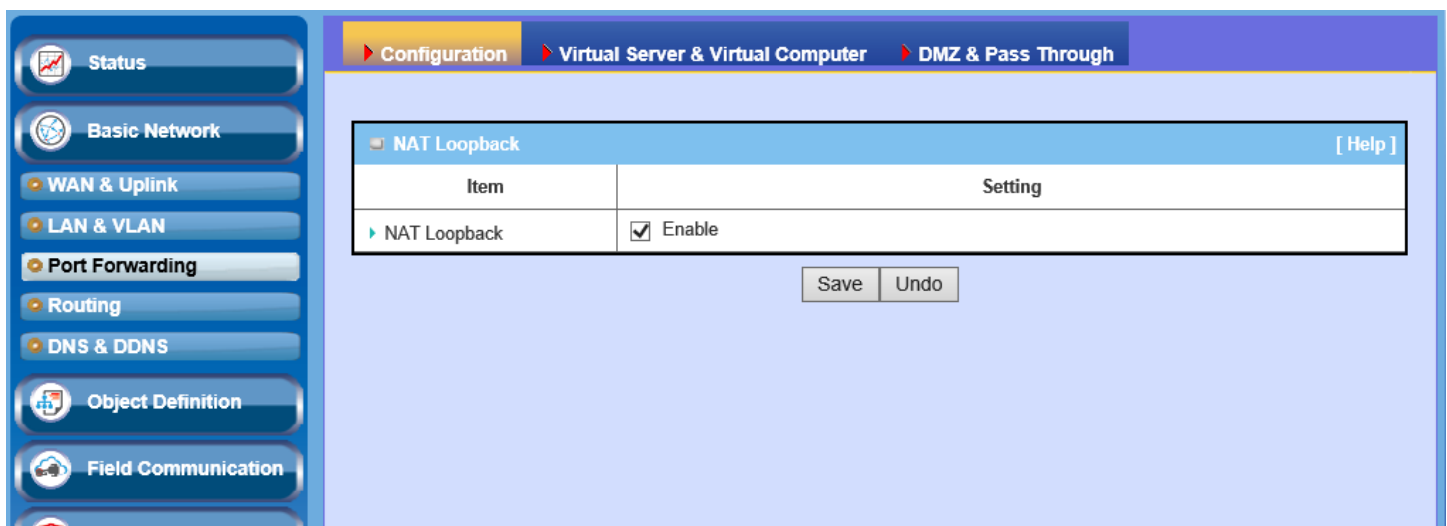
Add/Edit ボタンがクリックされると、DHCP Relay Configuration ウィンドウが表示されます。

DHCP Relay Configuration	
	Save Undo
Item	Setting
Agent Name	<input type="text"/>
LAN interface	LAN ▼
WAN interface	WAN - 1 ▼
Server IP	<input type="text"/>
DHCP OPTION 82	<input type="checkbox"/>
Enable	<input type="checkbox"/>

DHCP Server Option Configuratio		
項目	値設定	説明
Agent Name	1. 文字列形式：任意のテキスト 2. 必須入力項目	DHCP リレー名を入力します。
LAN Interface	1. 必須入力項目 2. デフォルト値：LAN	DHCP リレー機能で適用するドロップダウンリストの LAN インターフェースを選択します。
WAN Interface	1. 必須入力項目 2. デフォルト値：WAN1	DHCP リレー機能で適用するドロップダウンリストの WAN インターフェースを選択します。使用可能な WAN インターフェース、および L2TP 接続にすることができます。
Server IP	1. 必須入力項目 2. デフォルト値：null	ゲートウェイが指定された WAN インターフェースを介して割り当てられた DHCP サーバーに DHCP 要求を中継する DHCP サーバーの IP アドレスを割り当てます。
DHCP OPTION 82	デフォルト値：チェックなし	チェックボックスをクリックして、DHCP OPTION 82 を有効化します。 DHCP Option 82 は、DHCP リレーエージェントでパケットを中継するときに、リレーエージェント固有の情報を付けてからサーバに転送するためのオプションです。リレーエージェントが必要な場合だけ本設定を有効にしてください。
Enable	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本設定を有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックすると、画面が元に戻ります。

2.3 ポート転送

ネットワークアドレス変換（NAT）とは、トラフィックルーティングデバイスを通途中に、インターネットプロトコル（IP）データグラムパケットヘッダー内のネットワークアドレス情報を変更することによって、1つのIPアドレス空間を別のIPアドレス空間に再マッピングする方法です。この技術は、もともとすべてのホストの番号再設定を行うことなく、IPネットワーク内のトラフィックを容易に再ルーティングするために使用されていました。これは、IPv4アドレスの枯渇に直面し、グローバルアドレス空間への割り当てを節約するための一般的で不可欠なツールとなっています。また、**[[Basic Network] - [WAN & Uplink] - [Connection Setup] - [Connection Common Configuration]**ページで NAT 機能を有効/無効化することができます。



通常、企業ゲートウェイの後にあるすべてのローカルホストまたはサーバーは、NATファイアウォールで保護されています。NATファイアウォールは、認識できないパケットをフィルタリングしてイントラネットを保護します。したがって、すべてのローカルホストは外部には見えません。ポート転送またはポートマッピングとは、通信要求を1つのアドレスとポート番号の組み合わせから、割り当てられたものにリダイレクトする機能です。この技術は、宛先IPアドレスとポート番号を再マッピングすることにより、ゲートウェイ（外部ネットワーク）の反対側のホストに利用可能な保護または偽装（内部）ネットワーク上に存在するホスト上のサービスを行うために使用されます。

2.3.1 設定

[NATループバック](#)

この機能を使用すると、内部 NAT ローカルネットワークから WAN グローバル IP アドレスにアクセスできます。サーバーをネットワーク内で実行する場合に便利です。例えば、LAN 側でメールサーバーを設定した場合、NAT ループバック機能を有効化すると、ローカルデバイスは本製品のグローバル IP アドレスを使用して、このメールサーバーにアクセスできます。いずれの側でも、LAN 側または WAN 側で電子メールサーバーにアクセスしている場合は、メールサーバーの IP アドレスを変更する必要はありません。

設定

Basic Network > Port Forwarding > Configuration タブに進みます。

NAT ループバックにより、ローカルネットワーク内から WAN IP アドレスにアクセスできます。

NAT ループバックの有効化

NAT Loopback [Help]	
Item	Setting
▶ NAT Loopback	<input checked="" type="checkbox"/> Enable

NAT Loopback		
項目	値設定	説明
NAT Loopback	デフォルト値：チェックあり	Enable チェックボックスにチェックを入れると、この NAT 機能が有効化されます。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

2.3.2 仮想サーバーおよび仮想コンピュータ

Configuration								
Item	Setting							
▶ Virtual Server	<input checked="" type="checkbox"/> Enable							
▶ Virtual Computer	<input checked="" type="checkbox"/> Enable							

Virtual Server List <input type="button" value="Add"/> <input type="button" value="Delete"/>								
ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions
1	All	10.0.75.101	TCP(6) & UDP(17)	25	25	(0) Always	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="checkbox"/> Select
2	All	10.0.75.101	TCP(6) & UDP(17)	110	110	(0) Always	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="checkbox"/> Select

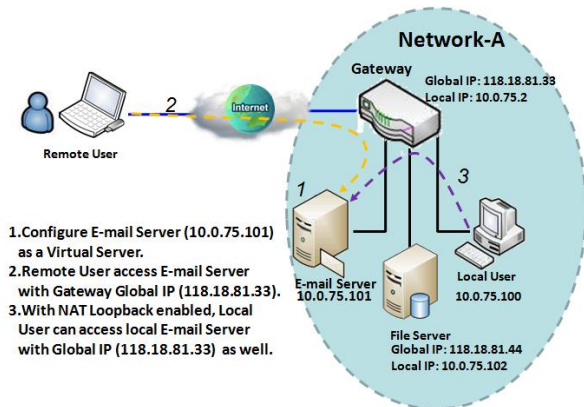
Virtual Computer List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Global IP	Local IP	Enable	Actions
1	118.18.81.44	10.0.75.102	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="checkbox"/> Select

本製品内で実装されているポート転送機能として、「仮想サーバー」、「NAT ループバック」、「仮想コンピュータ」があります。

これは、外出先でオフィス内のゲートウェイの後にある様々なサーバーにアクセスする必要がある企業スタッフにとっては必要です。「仮想サーバー」機能を使って、これらのサーバーを設定することができます。出張後、元の設定を変更せずに LAN 側からグローバル IP を使って、これらのサーバーにアクセスする場合は、「NAT ループバック」を用いて、実現することができます。

「仮想コンピュータ」とは、NAT ゲートウェイの後にあるホストであり、その IP アドレスはグローバルなもので、外部から見えます。また NAT の後にあるため、ゲートウェイファイアウォールによって保護されています。仮想コンピュータを設定するには、仮想コンピュータのローカル IP をグローバル IP にマッピングしてください。

仮想サーバーおよびNAT ループバック

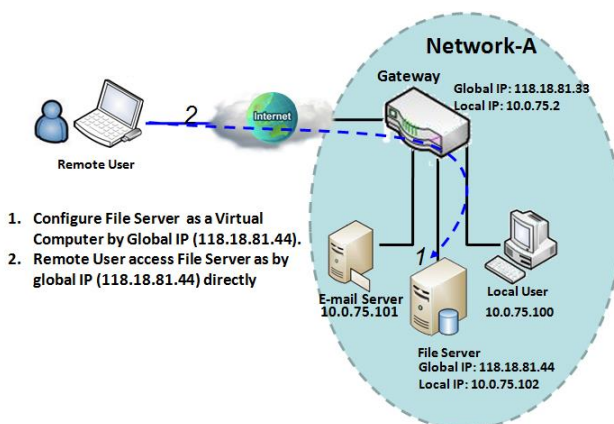


「仮想サーバー」を用いることにより、インターネットに存在するサーバーであるかのように、ゲートウェイのグローバル IP アドレスまたは FQDN を使用してサーバーにアクセスすることができます。しかし、実際にはこれらのサーバーは、イントラネットに配置され、物理的にゲートウェイの後にあります。ゲートウェイは、ポートによるサービス要求を LAN サーバーに転送し、LAN サーバーから WAN 側の要求者に応答を転送します。例に示すように、Eメール仮想サーバーは、SMTP サービスポート 25 と POP3 サービスポート 110 を含む、ネットワーク A のイントラネットに、IP アドレス 10.0.75.101 のサーバーに配置されるように定義されています。したがって、リモートユーザーは、WAN 側からゲートウェイ

のグローバル IP 118.18.81.33 を使って、Eメールサーバーにアクセスすることができます。しかし、実際の Eメールサーバーは LAN 側にあり、ゲートウェイは、電子メールサービス用のポート転送を担当します。

「NAT ループバック」を使用すると、内部 NAT ローカルネットワークから WAN グローバル IP アドレスにアクセスできます。サーバーをネットワーク内で実行する場合に便利です。例えば、LAN 側でメールサーバーを設定した場合、NAT ループバック機能を有効化すると、ローカルデバイスはゲートウェイのグローバル IP アドレスを使用して、このメールサーバーにアクセスできます。いずれの側でも、LAN 側または WAN 側で電子メールサーバーにアクセスしている場合は、メールサーバーの IP アドレスを変更する必要はありません。

仮想コンピュータ



「仮想コンピュータ」を使用すると、LAN ホストをグローバル IP アドレスに割り当て、外部に見えるようにすることができます。その間、これらは、ゲートウェイファイアウォールにより、イントラネット内のクライアントホストとして保護されます。例えば、ローカル IP アドレスが 10.0.75.102、グローバル IP アドレスが 118.18.81.44 の LAN 側の FTP ファイルサーバーを設定した場合、リモートユーザーは、NAT ゲートウェイの後に隠れている、ファイルサーバーにアクセスできます。これは、ゲートウェイが、IP アドレス 118.18.81.44 に対するすべてのアクセスを処理し、アクセス要求をファイルサーバーに転送し、サーバーからの応答を外部に送信するためです。

仮想サーバーおよび仮想コンピュータの設定

Basic Network > Port Forwarding > Virtual Server & Virtual Computer タブに進みます。

仮想サーバーおよび仮想コンピュータの有効化

Configuration	
Item	Setting
▶ Virtual Server	<input checked="" type="checkbox"/> Enable
▶ Virtual Computer	<input checked="" type="checkbox"/> Enable

Configuration 項目	値設定	説明
Virtual Server	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、ポート転送機能が有効化されます。
Virtual Computer	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、ポート転送機能が有効化されます。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

仮想サーバーの作成/編集

仮想サーバールールをカスタム設定することができます。最大 20 のルールベースの仮想サーバーセットをサポートします。

Virtual Server List Add Delete								
ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

Add ボタンをクリックされると、Virtual Server Rule Configuration ウィンドウが表示されます。

Virtual Server Rule Configuration	
Item	Setting
▶ WAN Interface	<input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1
▶ Server IP	<input type="text"/>
▶ Protocol	TCP(6) & UDP(17) ▼
▶ Public Port	Single Port ▼ <input type="text"/>
▶ Private Port	Single Port ▼ <input type="text"/>
▶ Time Schedule	(0) Always ▼
▶ Rule	<input type="checkbox"/> Enable

Virtual Server List

Virtual Server Rule Configuration

項目	値設定	説明
WAN Interface	1. 必須入力項目 2. デフォルト値 : ALL	選択したインターフェイスが、本製品の packets 入力インターフェイスになるように定義します。 フィルタリングする packets が、WAN-1 から来ている場合は、このフィールドで WAN-1 を選択します。 任意のインターフェイスから本製品に入ってくる packets に対して、ALL を選択します。
Server IP	必須入力項目	このフィールドは、上記の WAN Interface で選択されたインターフェイスの IP アドレスを指定するためのフィールドです。
Protocol	必須入力項目	「ICMPv4」が選択されているとき これは packets フィルタルールの Protocol オプションが、ICMPv4 であることを意味します。 Time Schedule をこのルールに適用、もしくは Always を設定します。（「オブジェクト定義」の「スケジュール設定」を参照） その後、Enable チェックボックスにチェックを入れ、このルールを有効化します。 「TCP」が選択されているとき これは packets フィルタルールの Protocol のオプションが、TCP であることを意味します。 Public Port を Well-known Service から事前定義されたポートを選択した場合、Private Port は、Public Port 番号と同じになります。 Public Port で Single Port を選択した場合、Private Port では自動的に Single Port が選択されます。 Public Port で Port Range を選択した場合、Private Port では Single Port または Port Range いずれかを選択できます。 <u>値の範囲</u> ：パブリックポート、プライベートポートの場合、1～65535 です。

「UDP」が選択されているとき
これは、パケットフィルタールの Protocol のオプションが、UDPであることを意味します。
Public Port を Well-known Service から事前定義されたポートを選択した場合、Private Port は、Public Port 番号と同じになります。
Public Port で Single Port を選択した場合、Private Port では自動的に Single Port が選択されます。
Public Port で Port Range を選択した場合、Private Port では Single Port または Port Range いずれかを選択できます。
値の範囲：パブリックポート、プライベートポートの場合、1～65535 です。

「TCP&UDP」が選択されているとき
これは、パケットフィルタールの Protocol オプションが、TCP & UDPであることを意味します。
Public Port を Well-known Service から事前定義されたポートを選択した場合、Private Port は、Public Port 番号と同じになります。
Public Port で Single Port を選択した場合、Private Port では自動的に Single Port が選択されます。
Public Port で Port Range を選択した場合、Private Port では Single Port または Port Range いずれかを選択できます。
値の範囲：パブリックポート、プライベートポートの場合、1～65535 です。

「GRE」が選択されているとき
これは、パケットフィルタールの Protocol オプションが、GREであることを意味します。

「ESP」が選択されているとき
これは、パケットフィルタールの Protocol オプションが、ESPであることを意味します。

「SCTP」が選択されているとき
これは、パケットフィルタールの Protocol オプションが、SCTPであることを意味します。

「User-defined」が選択されているとき
これは、パケットフィルタールの Protocol オプションが、User-definedであることを意味します。
プロトコル番号に対して、ポート番号を入力します。

Time Schedule	1. 任意入力項目 2. デフォルト値 : (0)Always	Time Schedule を適用、もしくは (0)Always を選択します。 (「オブジェクト定義」の「スケジュール設定」を参照)
Rule	1. 任意入力項目 2 デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れると、ルールが有効になります。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。
Back	-	Back ボタンをクリックすると、画面が前ページに戻ります。

仮想コンピュータの作成/編集

仮想コンピュータルールをカスタム設定することができます。最大 20 のルールベースの仮想コンピュータセットをサポートします。

Virtual Computer List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Global IP	Local IP	Enable	Actions

Add ボタンがクリックされると、Virtual Computer Rule Configuration ウィンドウが表示されます。

Virtual Computer Rule Configuration [Help]		
Global IP	Local IP	Enable
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/>		

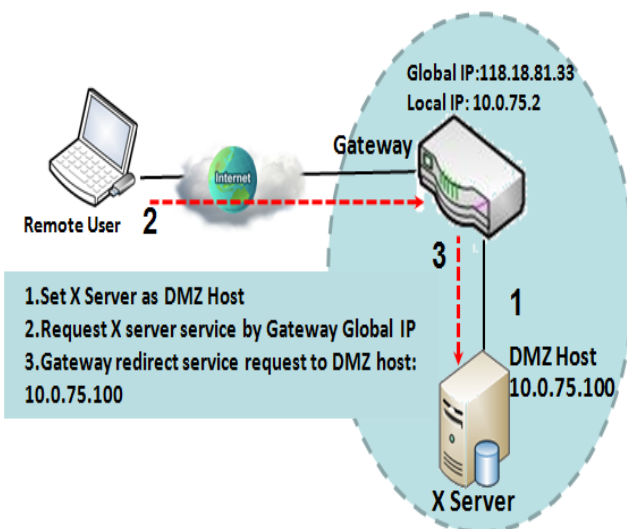
Virtual Computer Rule Configuration		
項目	値設定	説明
Global IP	必須入力項目	このフィールドは、WAN IP の IP アドレスを指定するためのフィールドです。
Local IP	必須入力項目	このフィールドは、LAN IP の IP アドレスを指定するためのフィールドです。
Enable	-	その後、Enable チェックボックスにチェックを入れ、このルールを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。

2.3.3 DMZ およびパススルー

DMZ (De Militarized Zone) ホストとは、インターネット空間に公開されていますが、ゲートウェイデバイスによるファイアウォール保護範囲内にあるホストです。したがって、この機能により、コンピュータは、インターネットゲーム、テレビ会議、インターネット電話および他の特別なアプリケーションの双方向通信を実行することができます。特定のアプリケーションが、NAT メカニズムによってブロックされている場合、この問題を解決するために LAN コンピュータを DMZ ホストとして指定することができます。

DMZ 機能を使用すると、NAT ゲートウェイの後にある DMZ ホストに対するすべての通常パケットをゲートウェイが通過させるよう要求することができます (これは、これらのパケットが、ゲートウェイ内のアプリケーションまたはイントラネット内の他のクライアントホストによって受信されることが予想されない場合に限りです)。確かに、DMZ ホストも、ゲートウェイのファイアウォールにより保護されています。機能を有効にし、必要に応じて、イントラネットにホストを持つ DMZ ホストを指定します。

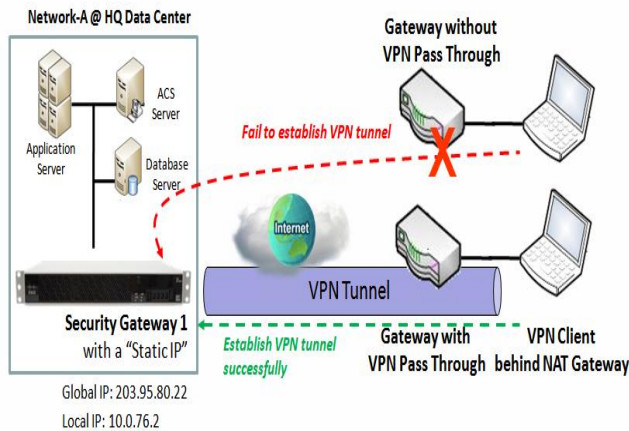
Configuration [Help]	
Item	Setting
DMZ	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 DMZ Host : <input type="text" value="10.0.75.100"/> x
Pass Through Enable	<input checked="" type="checkbox"/> IPSec <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP



DMZ のシナリオ

ネットワーク管理者が、NAT ゲートウェイの後にあるホストにいくつかのサービスデーモンを設定して、リモートユーザーが、サーバーからのサービスを積極的に要求できるようにする場合、このホストを DMZ ホストとして設定する必要があります。図に示すように、IP アドレスが 10.0.75.100 の DMZ ホストとして、X サーバーがインストールされています。次に、リモートユーザーは、グローバル IP アドレスが 118.18.81.33 であるゲートウェイが提供するように、X サーバーからサービスを要求することができます。ゲートウェイは、設定された仮想サーバーまたはアプリケーションに属さないパケットを直接 DMZ ホストに転送します。

VPN パススルーのシナリオ



VPN トラフィックは、TCP または UDP 接続と異なるため、NAT ゲートウェイによりブロックされます。NAT ゲートウェイの後にある VPN クライアントから開始される VPN 接続のパススルー機能をサポートするため、ゲートウェイは、そのようなアプリケーションに対して、何らかの種類の VPN パススルー機能を実装する必要があります。ゲートウェイは、IPSec、PPTP、および、L2TP 接続のパススルー機能をサポートしています。対応するチェックボックスにチェックを入れて、有効化してください。

DMZ およびパススルーの設定

Basic Network > Port Forwarding > DMZ & Pass Through タブに進みます。

DMZ ホストとは、インターネット空間に公開されていますが、ゲートウェイデバイスによるファイアウォール保護範囲内にあるホストです。

DMZ およびパススルーの有効化

Configuration [Help]	
Item	Setting
▶ DMZ	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 DMZ Host : <input type="text"/>
▶ Pass Through Enable	<input checked="" type="checkbox"/> IPSec <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP

Configuration		
項目	値設定	説明
DMZ	1. 必須入力項目 2. デフォルト値 : ALL	Enable チェックボックスにチェックを入れると、DMZ 機能が有効化されます。

		<p>選択したインターフェイスを本製品の packets 入力インターフェイスに定義し、DMZ Host フィールドにホスト LAN IP の IP アドレスを入力します。</p> <p>フィルタリングするパケットが、WAN-1 から来ている場合は、このフィールドで WAN-1 を選択します。</p> <p>任意のインターフェイスからルーターに入ってくるパケットに対して、ALL を選択します。</p>
Pass Through Enable	デフォルト値：チェックあり	<p>チェックボックスにチェックを入れ、IPSec、PPTP および L2TP に対するパススルー機能を有効化します。</p> <p>パススルー機能を有効化すると、本製品の後にある VPN ホストは、引き続きリモート VPN サーバーに接続できます。</p>
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

2.4 ルーティング

The screenshot shows the 'Static Routing' configuration page. The 'Configuration' section contains the following table:

Item	Setting
Static Routing	<input type="checkbox"/> Enable

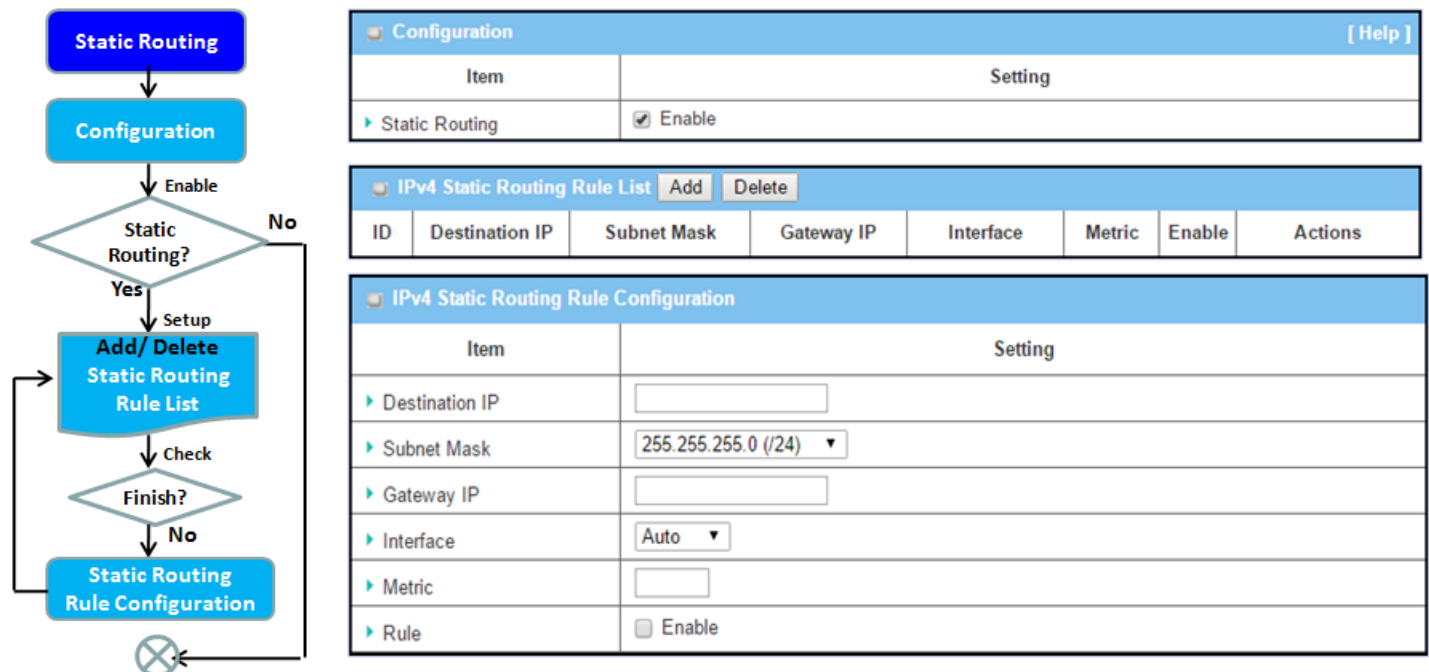
The 'IPv4 Static Routing Rule List' section contains the following table:

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions
----	----------------	-------------	------------	-----------	--------	--------	---------

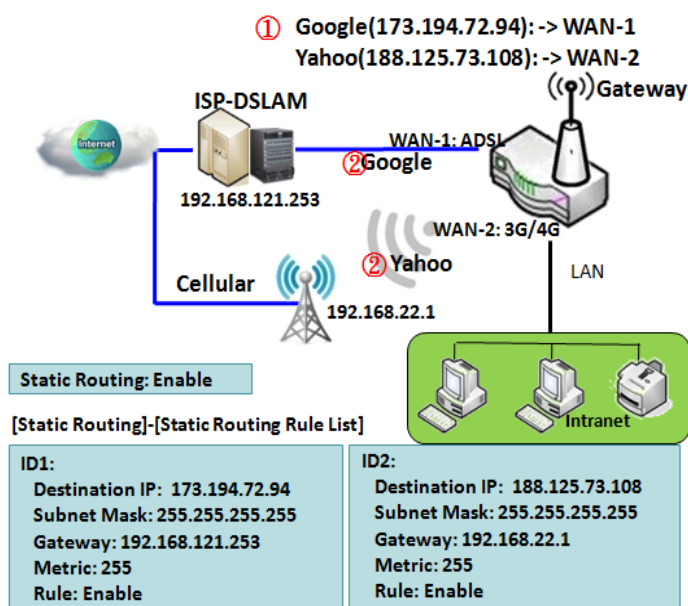
ルーターやサブネットが複数ある場合は、ルーティング機能を有効にして、パケットが適切なルーティングパスを経由し、複数のサブネットが相互に通信できるようにする必要があります。ルーティングとは、ネットワーク内で最適なパスを選択するプロセスです。これはパケット交換技術を使用して、電子データネットワーク（インターネットなど）のような多くの種類のネットワークで実行されます。ルーティングプロセスは通常、様々なネットワーク宛先へのルート記録を保持するルーティングテーブルに基づいて転送を指示します。したがって、効率的なルーティングのためには、ルーターのメモリに保持されているルーティングテーブルを構築することが非常に重要です。ほとんどのルーティングアルゴリズムは、一度に1つのネットワークパスしか使用しません。

ルーティングテーブルには、特定の宛先サブネットの事前定義されたルーティングパスが記録されます。これは**静的ルーティング**です。他方、ルーティングテーブルの内容が RIP、OSPF、BGP などのプロトコルを使用して、取得したルーティングパスを近隣のルーターから記録する場合は**動的ルーティング**となります。本セクションではこれらの両方のルーティングアプローチについて説明します。

2.4.1 静的ルーティング



「静的ルーティング」機能を使用すると、ゲートウェイのルーティングテーブルに格納する一部の専用ホスト/サーバーまたはサブネットのルーティングパスを定義することができます。ゲートウェイは、着信パケットをルーティングテーブルに基づき、異なるピアゲートウェイにルーティングします。静的ルーティング情報をゲートウェイルーティングルールリストに定義する必要があります。



ゲートウェイの管理者が、どの種類のパケットをどのゲートウェイインターフェイス経由で転送するか、どのピアゲートウェイをその宛先に転送するかを指定する場合は、これは「静的ルーティング」機能によって実現することができます。イントラネットからの専用パケットフローは、手動でシステムルーティングテーブルに定義されている、事前定義されたピアゲートウェイと対応するゲートウェイインターフェイスを経由して宛先にルーティングされます。

図に示すように、宛先が Google アクセスの場合、ルール 1 は、ADSL として、インターフェイスを設定し、IP-DSLAM ゲートウェイ 192.168.121.253 として、ルーティングゲートウェイを設定します。Google に対するすべてのパケットは、WAN-1 を経由します。同じように、Yahoo にアクセスするルール 2 にも適用されます。ルール 2 は、インターフェイスとして 3G/4G を設定します。

静的ルーティングの設定

Basic Network > Routing > Static Routing タブに進みます。

静的ルーティング機能には、「**Configuration**」、「**Static Routing Rule List**」、「**Static Routing Rule Configuration**」の3つの設定ウィンドウがあります。「**Configuration**」ウィンドウでは、グローバル静的ルーティング機能を有効化することができます。既にルーティングルールがある場合でも、ルーティングを一時的に無効化する場合は、「**Enable**」チェックボックスのチェックを外して、無効化します。「**Static Routing Rule List**」ウィンドウには、定義済みのすべての静的ルーティングルールエントリが一覧表示されます。「**Add**」または「**Edit**」ボタンを使って、1つの新しい静的ルーティングルールを追加および作成する、または、既存の静的ルーティングルールを変更します。

「**Add**」または「**Edit**」ボタンがクリックされると、静的ルーティングルールを定義するための「**Static Routing Rule Configuration**」ウィンドウが表示されます。

静的ルーティングの有効化

Enable チェックボックスにチェックを入れ、「**Static Routing**」機能を有効化します。

Configuration [Help]	
Item	Setting
Static Routing	<input checked="" type="checkbox"/> Enable

Configuration		
項目	値設定	説明
Static Routing	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、この機能が有効化されます。

静的ルーティングルールの作成/編集

Static Routing Rule List には、すべての静的ルーティングルールエントリの設定パラメータが表示されます。静的ルーティングルールを設定するには、専用ホスト/サーバーまたはサブネットの宛先 IP アドレスおよびサブネットマスク、ピアゲートウェイの IP アドレス、メトリックおよびルールアクティベーションを含む関連パラメータを指定する必要があります。

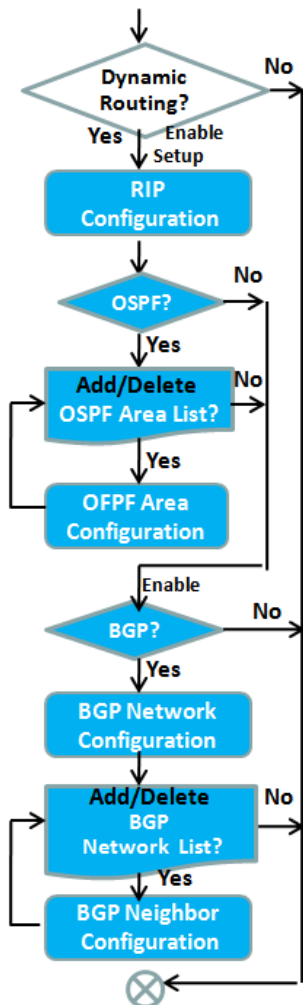
IPv4 Static Routing Rule List Add Delete							
ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

静的ルーティングルールをカスタム設定することができます。これは、最大 64 のルールセットをサポートします。**Add** ボタンがクリックされると、**Static Routing Rule Configuration** ウィンドウが表示されます。一方、各静的ルーティングルールの終端の **Edit** ボタンを使って、ルールを変更することができます。

IPv4 Static Routing Rule Configuration	
Item	Setting
▶ Destination IP	<input type="text"/>
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ Gateway IP	<input type="text"/>
▶ Interface	Auto ▼
▶ Metric	<input type="text"/>
▶ Rule	<input type="checkbox"/> Enable

Static Routing Rule Configuration		
項目	値設定	説明
Destination IP	1.IPv4 形式です 2. 必須入力項目	この静的ルーティングルールの宛先 IP を指定します。
Subnet Mask	デフォルト値： 255.255.255.0 (/24)	この静的ルーティングルールのサブネットマスクを指定します。
Gateway IP	1.IPv4 形式です 2. 必須入力項目	この静的ルーティングルールのゲートウェイ IP を指定します。
Interface	デフォルト値：Auto	この静的ルーティングルールのインターフェイスを選択します。これは、Auto または the available WAN / LAN interfaces にすることができます。
Metric	1. 数値文字列形式です 2. 必須入力項目	この静的ルーティングルールのメトリックです。 <u>値の範囲</u> ：0～255。
Rule	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本ルールを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定した内容を元の設定に復元します。
Back	-	Back ボタンをクリックすると、画面が Static Routing Configuration ページに戻ります。

2.4.2 動的ルーティング



RIP Configuration [Help]	
Item	Setting
▶ RIP Enable	Disable ▾

OSPF Configuration	
Item	Setting
▶ OSPF	<input checked="" type="checkbox"/> Enable
▶ Router ID	<input type="text"/>
▶ Authentication	None ▾
▶ Backbone Subnet	<input type="text"/>

OSPF Area List Add Delete				
ID	Area Subnet	Area ID	Enable	Actions

BGP Configuration	
Item	Setting
▶ BGP	<input checked="" type="checkbox"/> Enable
▶ ASN	<input type="text"/>
▶ Router ID	<input type="text"/>

BGP Network List Add Delete			
ID	Network Subnet	Enable	Actions

BGP Neighbor List Add Delete				
ID	Neighbor IP	Remote ASN	Enable	Actions

BGP Neighbor Configuration	
Item	Setting
▶ Neighbor IP	<input type="text"/>
▶ Remote ASN	<input type="text"/>
▶ Neighbor	<input type="checkbox"/> Enable

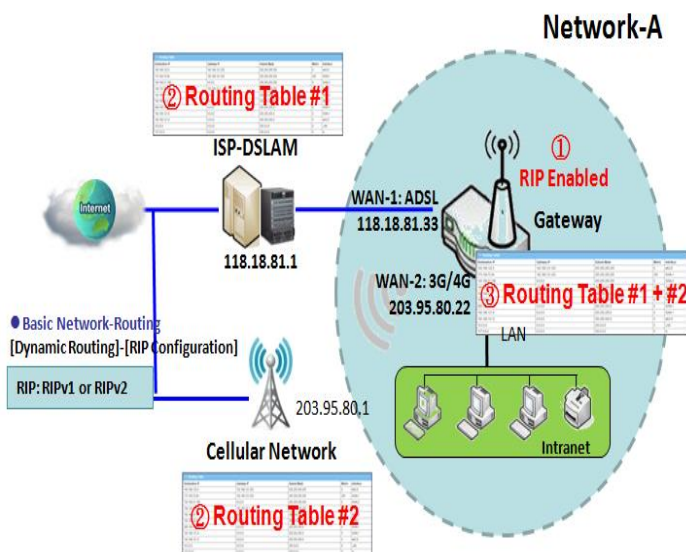
Save

適応型ルーティングとも呼ばれる動的ルーティングは、パスが宛先によって特徴付けられるシステムの能力を記述し、パスがネットワーク状態の変化にตอบสนองして、システムを通過するパスを変更します。

本製品は、ルーティングテーブルを自動的に確立するために、RIPv1 / RIPv2（ルーティング情報プロトコル）、OSPF（オープン最短パスファースト）、BGP（ボーダーゲートウェイプロトコル）などの動的ルーティングプロトコルをサポートしています。動的ルーティング機能は、ネットワークに多数のサブネットがある場合に非常に便利です。一般的に、RIPは小規模のネットワークに適しています。OSPFは中規模のネットワークに適しています。BGPは大規模なネットワークインフラストラクチャで多く使用されます。

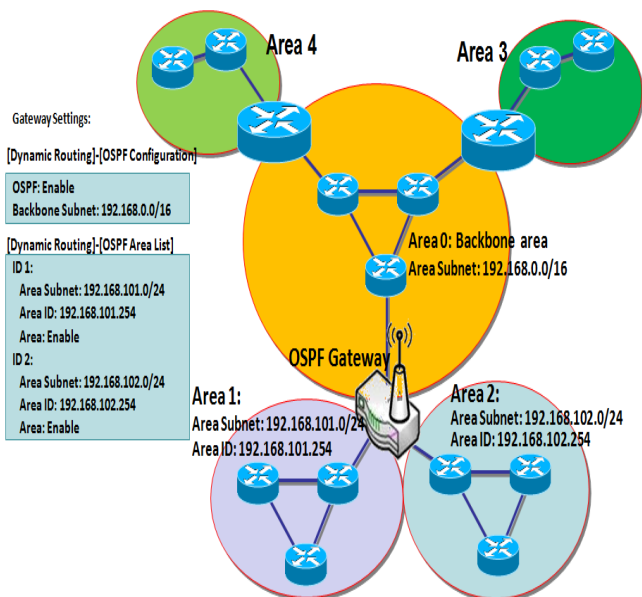
本製品がサポートする動的ルーティングについて、説明します。

RIP のシナリオ



ルーティング情報プロトコル（RIP）とは、ルートメトリックとしてホップカウントを使用する、最も古い距離ベクトルルーティングプロトコルの 1 つです。RIP は、送信元から宛先に対するパスで許可されるホップカウントに制限を実装することによって、ルーティングループを防止します。許可される RIP の最大ホップカウントは 15 です。しかし、このホップ制限により、RIP がサポートできるネットワークサイズも制限されます。16 のホップカウントは無限遠とみなされます。つまり、パスは到達不能とみなされます。RIP は、スプリットホライズン、ルートポイズニングおよびホールドダウンメカニズムを実装して、間違ったルーティング情報が伝播されないようにします。

OSPF のシナリオ

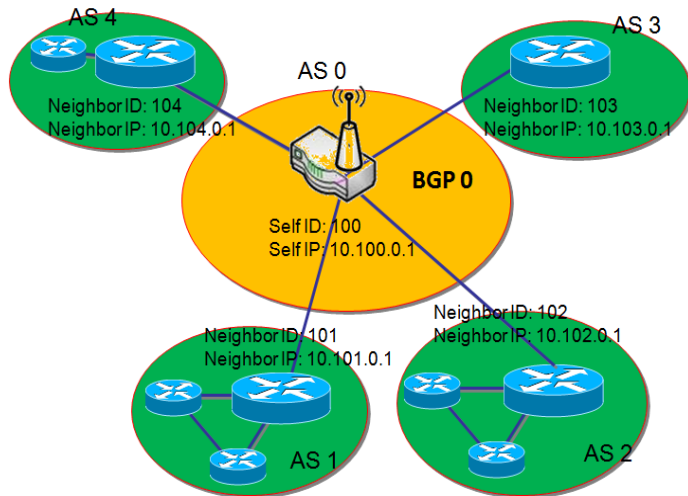


OSPF（Open Shortest Path First）とは、リンクステートルーティングアルゴリズムを使用するルーティングプロトコルです。これは、大規模な企業ネットワークで最も広く使用されている IGP（Interior Gateway Protocol）です。使用可能なルーターからリンクステート情報を収集し、ネットワークのトポロジマップを構築します。トポロジは、宛先 IP アドレスのみに基づいてデータグラムをルーティングするルーティングテーブルとして提示されます。

ネットワーク管理者は、企業バックボーンからルーティングテーブルを取得し、企業バックボーンにリンクされていない他のルーターにルーティング情報を転送するために、大規模な企業ネットワークに OSPF ゲートウェイを配置することができます。通常、OSPF ネットワークは、ルーティング領域に細分され、管理を簡素化し、トラフィックとリソースの使用率を最適化します。

図に示すように、OSPF ゲートウェイは、エリア 0 のバックボーンゲートウェイからルーティング情報を収集し、そのルーティング情報をバックボーンにないエリア 1 とエリア 2 のルーターに転送します。

BGP のシナリオ



Border Gateway Protocol (BGP) とは、インターネット上の自律システム (AS) 間でルーティングと到達可能性の情報を交換するために設計された標準的な外部ゲートウェイプロトコルです。通常、パス、ネットワークポリシー、または、ルールセットに基づいてルーティングを決定します。

ほとんどの ISP は、BGP を使って、相互間のルーティングを確立します。非常に大規模なプライベート IP ネットワークも内部的に BGP を使用します。ある AS 内の主要な BGP ゲートウェイは、ルーティング情報を交換するため、いくつかの他の境界ゲートウェイとリンクします。これは、AS 内で収集したデータを他の AS 内のすべてのルーターに配布します。

図に示すように、BGP 0 は AS0 を支配するゲートウェイです (自己 IP は 10.100.0.1、および、自己 ID は 100 です)。これは、インターネット内の他の BGP ゲートウェイとリンクします。このシナリオは、ある ISP のサブネットと他の ISP のサブネットがリンクするようなものです。BGP プロトコルで動作することにより、BGP 0 は、インターネット内の他の BGP ゲートウェイからルーティング情報を収集することができます。そして、ルーティングデータをその支配された AS 内のルーターに転送します。最後に、AS 0 にあるルーターは、パケットを他の AS にルーティングする方法を理解します。

動的ルーティングの設定

Basic Network > Routing > Dynamic Routing タブに進みます。

動的ルーティング設定により、オフィス設定に基づき、ルーター経由で RIP、OSPF、および、BGP プロトコルをカスタマイズすることができます。

「Dynamic Routing」ページには、動的ルーティング機能用の 7 つの設定ウィンドウがあります。「RIP Configuration」ウィンドウ、「OSPF Configuration」ウィンドウ、「OSPF Area List」、「OSPF Area Configuration」、「BGP Configuration」、「BGP Neighbor List」、および「BGP Neighbor Configuration」ウィンドウです。RIP、OSPF、および、BGP プロトコルは、個別に設定することができます。

「RIP Configuration」ウィンドウでは、有効化または無効化する RIP プロトコルのバージョンを選択することができます。「OSPF Configuration」ウィンドウでは、OSPF 動的ルーティングプロトコルを有効化し、そのバックボーンサブネットを指定することができます。さらに、「OSPF Area List」ウィンドウには、OSPF ネットワーク内のすべての定義済み領域が一覧表示されます。ただし、「BGP Configuration」ウィンドウでは、BGP 動的ルーティングプロトコルを有効化して、自己 ID を指定することができます。「BGP Neighbor List」ウィンドウには、BGP ネットワーク内のすべての定義済みの近隣が一覧表示されます。

RIP Configuration

RIP Configuration では、オフィス設定に基づき、ルーター経由で RIP プロトコルをカスタマイズすることができます。

RIP Configuration [Help]	
Item	Setting
▶ RIP Enable	Disable ▾

RIP Configuration		
項目	値設定	説明
RIP Enable	デフォルト値 : Disable	Disable を選択すると、RIP プロトコルが無効化されます。 RIP v1 を選択すると、RIPv1 プロトコルが有効化されます。 RIP v2 を選択すると、RIPv2 プロトコルが有効化されます。

OSPF Configuration

OSPF Configuration は、オフィス設定に基づき、ルーター経由で OSPF プロトコルをカスタマイズすることができます。

OSPF Configuration	
Item	Setting
▶ OSPF	<input type="checkbox"/> Enable
▶ Router ID	<input type="text"/>
▶ Authentication	None ▼
▶ Backbone Subnet	<input type="text"/>

OSPF Configuration		
項目	値設定	説明
OSPF	デフォルト値 : Disable	Enable チェックボックスをクリックして、OSPF プロトコルを有効化します。
Router ID	1.IPv4 形式です 2. 必須入力項目	OSPF プロトコル上のこのルーターのルーターID です
Authentication	デフォルト値 : None	OSPF プロトコル上の認証方法です。 None を選択すると、OSPF プロトコル上の認証が無効化されま す。 Text を選択すると、テキスト認証が有効化されます。Key の入 力が必要になります。 MD5 を選択すると、MD5 認証が有効化されます。ID と KEY の 入力が必要になります。
Backbone Subnet	1.Classless Inter Domain Routing (CIDR) サブネッ トマスク表記法で す。(例 : 192.168.1.0/24) 2. 必須入力項目	OSPF プロトコル上の Backbone Subnet です

OSPF Area Rule の作成/編集

ゲートウェイにより、**OSPF Area List** のルールをカスタマイズすることができ、32 のルールセットが設定可能です。

OSPF Area List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Area Subnet	Area ID	Enable	Actions

Add ボタンをクリックされると、OSPF Area Rule Configuration ウィンドウが表示されます。

OSPF Area Configuration	
Item	Setting
▶ Area Subnet	<input type="text"/>
▶ Area ID	<input type="text"/>
▶ Area	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

OSPF Area Configuration		
項目	値設定	説明
Area Subnet	1. Classless Inter Domain Routing (CIDR) サブネットマスク表記法です。 (例 : 192.168.1.0/24) 2. 必須入力項目	OSPF 領域リスト上のこのルーターの Area Subnet です。
Area ID	1. IPv4 形式です 2. 必須入力項目	OSPF 領域リスト上のこのルーターの Area ID です。
Area	デフォルト値 : チェックなし	Enable チェックボックスをクリックして、本ルールを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。

BGP Configuration

BGP Configuration では、BGP プロトコルをカスタマイズすることができます。

BGP Configuration	
Item	Setting
▶ BGP	<input type="checkbox"/> Enable
▶ ASN	<input type="text"/>
▶ Router ID	<input type="text"/>

BGP Configuration		
項目	値設定	説明
BGP	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、BGP プロトコルを有効化します。
ASN	1. 数値文字列形式です 2. 必須入力項目	BGP プロトコル上のこのルーターの ASN 番号です。 <u>値の範囲</u> ：1～4294967295。
Router ID	1. IPv4 形式です 2. 必須入力項目	BGP プロトコル上のこのルーターのルーターID です。

BGP Network Rule の作成/編集

BGP ネットワークルールをカスタム設定することができます。これは、最大 32 のルールセットをサポートします。

BGP Network List <input type="button" value="Add"/> <input type="button" value="Delete"/>			
ID	Network Subnet	Enable	Actions

Add ボタンをクリックされると、BGP Network Rule Configuration ウィンドウが表示されます。

BGP Network Configuration	
Item	Setting
▶ Network Subnet	IP : <input type="text"/> <input type="text" value="255.255.255.0 (/24)"/> ▼
▶ Network	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

項目	値設定	説明
Network Subnet	1. IPv4 形式です 2. 必須入力項目	BGP Network List 上のこのルーターのネットワークサブネットです。このフィールドには IP アドレスと選択されたサブネットマスクが入力されています。
Network	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本ルールを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します

BGP Neighbor ルールの作成/編集

BGP Neighbor ルールをカスタム設定することができます。最大 32 のルールセットが設定できます。

BGP Neighbor List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Neighbor IP	Remote ASN	Enable	Actions

Add ボタンをクリックされると、BGP Neighbor Rule Configuration ウィンドウが表示されます。

BGP Neighbor Configuration	
Item	Setting
▶ Neighbor IP	<input type="text"/>
▶ Remote ASN	<input type="text"/>
▶ Neighbor	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

BGP Neighbor Configuration		
項目	値設定	説明
Neighbor IP	1. IPv4 形式です 2. 必須入力項目	BGP Neighbor List 上のこのルーターの Neighbor IP です
Remote ASN	1. 数値文字列形式です 2. 必須入力項目	BGP Neighbor List 上のこのルーターの Remote ASN です <u>値の範囲</u> ： 1～4294967295。
Neighbor	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本ルールを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。

2.4.3 ルーティング情報

ルーティング情報により、ルーティングテーブルを表示することができます。

Basic Network > Routing > Routing Information タブに進みます。

Routing Table				
Destination IP	Subnet Mask	Gateway IP	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

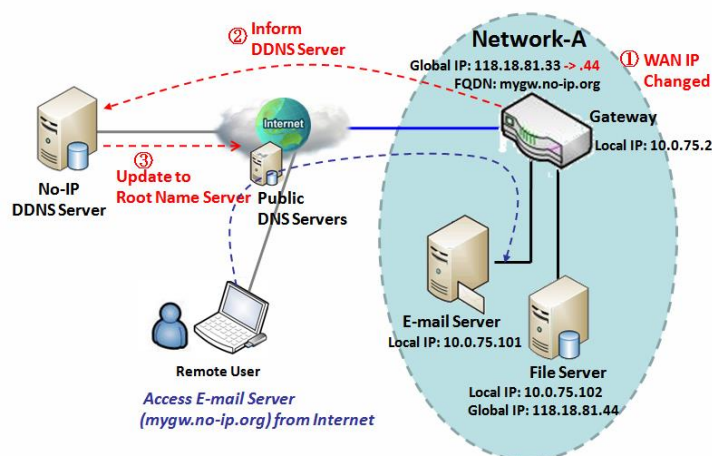
Routing Table		
項目	値設定	説明
Destination IP	-	宛先 IP のルーティング記録です。IPv4 形式です。
Subnet Mask	-	サブネットマスクのルーティング記録です。IPv4 形式です。
Gateway IP	-	ゲートウェイ IP のルーティング記録です。IPv4 形式です。
Metric	-	メトリックのルーティング記録です。数値文字列形式です。
Interface	-	インターフェイスタイプのルーティング記録です。文字列形式です。

2.5 DNS および DDNS

WAN IP アドレスが常時変動する場合、ユーザーはどのようにしてサーバーにアクセスすることになるでしょうか。1つの方法として、新しいドメイン名を登録して、独自の DNS サーバーを使用することがあげられます。もっと簡単な方法として、ドメイン名をサードパーティ DDNS サービスプロバイダに適用することがあげられます。DNS サービスは、無料または有料があります。DNS および動的 DNS の基本的な概念を理解したい場合は、Wikipedia の Web サイトを参照してください^{1,2}。

2.5.1 DNS および DDNS 設定

Dynamic DNS



変更 IP アドレスでサーバーをホストするには、動的ドメインネームサービス (DDNS) を使用する必要があります。そのため、ホストにアクセスしようとする人は、そのドメイン名さえわかればよいということになります。動的 DNS はホストの名前を現在の IP アドレスにマッピングします。IP アドレスはインターネットサービスプロバイダに接続するたびに変更されます。

動的 DNS サービスを使用すると、ゲートウェイはパブリック動的 IP アドレスを静的なドメイン名にエイリアスすることができるため、インターネット上のさまざまな場所からゲートウェイに簡単にアクセス

することができます。図に示すように、ユーザーは、DDNS 機能を使用するために、第三者 DDNS サービスプロバイダ (NO-IP) にドメイン名を登録しました。指定された WAN インターフェ이스の IP アドレスが変更されると、ゲートウェイの動的 DNS エージェントは、新しい IP アドレスを DDNS サーバーに通知します。サーバーは、変更された IP アドレスを使って、ドメイン名を自動的に再マッピングします。したがって、インターネット世界の他のホストやリモートユーザーは、グローバル IP アドレスの変更に関係なく、ドメイン名を使用してゲートウェイにリンクすることができます。

1 http://en.wikipedia.org/wiki/Domain_Name_System

2 http://en.wikipedia.org/wiki/Dynamic_DNS

DNS および DDNS 設定

Basic Network > DNS & DDNS > Configuration タブに進みます。

DNS および DDNS 設定により、動的 DNS 機能を設定することができます。

Dynamic DNS

Dynamic DNS をカスタム設定することができます。

Dynamic DNS [Help]	
Item	Setting
▶ DDNS	<input type="checkbox"/> Enable
▶ WAN Interface	WAN-1 ▼
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	<input type="text"/>
▶ User Name / E-Mail	<input type="text"/>
▶ Password / Key	<input type="text"/>

Dynamics DNS		
項目	値設定	説明
DDNS	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、この機能が有効化されます。
WAN Interface	デフォルト値：WAN-1	本製品の WAN インターフェイス IP アドレスを選択します。
Provider	デフォルト値：DynDNS.org	DDNS プロバイダを選択します。DynDNS.org（動的）、DynDNS.org（カスタム）、NO-IP.comなどを指定できます。
Host Name	1.文字列形式：任意のテキスト 2. 必須入力項目	動的 DNS の登録ホスト名です。 <u>値の範囲</u> ：0～63 文字。
User Name / E-Mail	1.文字列形式：任意のテキスト 2. 必須入力項目	動的 DNS のユーザー名または E メールアドレスを入力します。
Password / Key	1.文字列形式：任意のテキスト 2. 必須入力項目	動的 DNS のパスワードまたはキーを入力します。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします。

DNS リダイレクトの設定

DNS リダイレクトとは、特定のトラフィックを指定されたホストにリダイレクトする特別な機能です。管理者は、制限された DNS にアクセスしようとするインターネット/イントラネットのトラフィックを管理し、それらのトラフィックを指定されたホストにリダイレクトさせることができます。

DNS Redirect	
Item	Setting
▶ DNS Redirect	<input type="checkbox"/> Enable

DNS Redirect		
項目	値設定	説明
DNS Redirect	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、この機能が有効化されます。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします。

DNS リダイレクト機能を有効にした場合、リダイレクトルールをさらに指定する必要があります。このルールに従い、本製品は、DNS と一致するトラフィックを対応する予め定義された IP アドレスにリダイレクトすることができます。

Redirect Rule Add Delete					
ID	Mapping Rule	Condition	Description	Enable	Action

Add ボタンをクリックされると、**Redirect Rule** ウィンドウが表示されます。

Redirect Rule Save Back					
Item	Setting				
Mapping Rule	<table border="1"> <thead> <tr> <th>Domain Name</th> <th>IP</th> </tr> </thead> <tbody> <tr> <td><input type="text"/> (* for Any)</td> <td><input type="text"/></td> </tr> </tbody> </table>	Domain Name	IP	<input type="text"/> (* for Any)	<input type="text"/>
Domain Name	IP				
<input type="text"/> (* for Any)	<input type="text"/>				
Condition	<input type="text" value="Always"/> ▼				
Description	<input type="text"/>				
Enable	<input type="checkbox"/> Enable				

Redirect Rule		
項目	値設定	説明
Domain Name	1.文字列形式：任意のテキスト 2. 必須入力項目	リダイレクトするドメイン名を入力します。指定されたドメイン名へのトラフィックは、次の IP アドレスにリダイレクトされます。 <u>値の範囲</u> ：少なくとも1つの文字が必要です。*
IP	1.IPv4 形式です 2. 必須入力項目	DNS リダイレクトのターゲットとして、IP アドレスを入力します。
Condition	1.必須入力項目 2. デフォルト値 ： Always	DNS リダイレクトアクションをいつ適用できるかを指定します。Always または、WAN Block の設定が可能です。 Always：DNS リダイレクト機能は、常に一致する DNS に適用することができます。 WAN Block：DNS リダイレクト機能は、WAN 接続が切断された場合、または到達不能な場合にのみ、一致した DNS に適用することができます。
Description	1.文字列形式：任意のテキスト 2. 必須入力項目	このルールの簡単な説明を入力します。 <u>値の範囲</u> ：0～63 文字。
Enable	デフォルト値：チェックなし	Enable ボタンをクリックして、このルールを有効化します。
Save	-	Save をクリックして、設定を保存します。
Back	-	Back をクリックして、画面が前ページに戻ります。

第 3 章 オブジェクト定義

3.1 スケジュール

スケジュールは、他の機能に適用可能なタイムスケジュールルールを追加/削除する機能を提供します。

3.1.1 スケジュール設定

Object Definition > Scheduling > Configuration タブに進みます。

Time Schedule List Add Delete		
ID	Rule Name	Actions

Time Schedule List		
項目	値設定	説明
Add	-	Add ボタンをクリックして、タイムスケジュールルールを追加します。
Delete	-	Delete ボタンをクリックして、選択したルールを削除します。

Add ボタンをクリックされると、Time Schedule Configuration および Time Period Definition ウィンドウが表示されます。

Time Schedule Configuration	
Item	Setting
▶ Rule Name	<input type="text"/>
▶ Rule Policy	Inactivate ▼ the Selected Days and Hours Below.

Time Schedule Configuration		
項目	値設定	説明
Rule Name	文字列：任意のテキスト	ルール名を記載します。
Rule Policy	デフォルト値： Inactive	以下の期間において、機能の無効化/有効化を適用します。

Time Period Definition			
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
2	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
3	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
4	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
5	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
6	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
7	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
8	-- choose one -- ▼	<input type="text"/>	<input type="text"/>

Time Period Definition		
項目	値設定	説明
Week Day	メニューから選択します	毎日または曜日のいずれかを選択します。
Start Time	時間フォーマット (hh:mm)	選択した曜日の開始時間です。
End Time	時間フォーマット (hh:mm)	選択した曜日の終了時間です。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします。

3.2 グループ

グループ機能により、ファイアウォールサービスで使用できるグループを作成することができます。

3.2.1 ホストグループ

Go to Object Definition > Grouping > Host Grouping tab

ホストグループ機能により、ファイアウォールサービスで使用できるグループを作成することができます。

Host Group List Add Delete						
ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions

Add ボタンをクリックすると、Host Group Configuration ウィンドウが表示されます。

Host Group Configuration	
Item	Setting
▶ Group Name	<input type="text"/>
▶ Group Type	IP Address-based ▼
▶ Member to Join	<input type="text"/> Join
▶ Member List	
▶ Bound Services	<input type="checkbox"/> Firewall
▶ Group	<input type="checkbox"/> Enable

Host Group List Host Group Configuration		
項目	値設定	説明
Group Name	1. 文字列形式：任意のテキスト 2. 必須入力項目	グループ名を指定します。
Group Type	1. 初期値：IP Address-based 2. 必須入力項目	ホストグループのグループタイプを選択します。IP Address-based, MAC Address-based から選択可能です。IP Address-based が選択された場合、IP アドレスのみが Member to Join で入力可能になります。

Member to Join	-	グループに参加するメンバーを入力し、[Join] ボタンをクリックすると、そのメンバーがグループに追加されます。上記 Member Type で指定された情報で入力が可能です。一度の追加は 1 メンバーのみ入力が可能な為、1 メンバーずつ追加する必要があります。
Member List	-	グループのメンバーのリストを表示します。削除ボタン ⊗ が各メンバーの後ろにあります。このボタンを使用すると、メンバーをグループから削除することができます。
Bound Services	デフォルト値：チェックなし	ホストグループが適用される機能を制限できます。 Firewall：チェックをするとファイアウォール機能で使用可能になります。
Group	デフォルト値：チェックなし	Enable チェックボックスを有効にすると、グループ定義が有効になります。
Save	-	Save クリックして、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします。

3.3 外部サーバー

Object Definition > External Server > External Server タブに進みます。

外部サーバー設定により、外部サーバーを追加することができます。

3.3.1 設定

外部サーバーの作成

External Server List <input type="button" value="Add"/> <input type="button" value="Delete"/>						
ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

Add ボタンがクリックされると、**External Server Configuration** ウィンドウが表示されます。

External Server Configuration	
Item	Setting
▶ Server Name	<input type="text"/>
▶ Server Type	Email Server <input type="button" value="v"/> User Name: <input type="text"/> Password: <input type="text"/>
▶ Server IP/FQDN	<input type="text"/>
▶ Server Port	<input type="text" value="25"/>
▶ Server	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

External Server List		
External Server Configuration		
項目	値設定	説明
Sever Name	1.文字列形式：任意のテキスト 2. 必須入力項目	サーバー名を入力します。
		外部サーバーのサーバータイプを指定し、サーバーにアクセスするために必要な設定を入力します。
		Email Server : Email Server を選択するときは、次の設定も必要です。
		User Name (文字列形式：任意のテキスト) Password (文字列形式：任意のテキスト)
		RADIUS Server (必須入力項目) : RADIUS Server を選択するときは、次の設定も必要です。
		Primary / Secondary : Shared Key (文字列形式：任意のテキスト) Authentication Protocol (認証プロトコル) (デフォルト値 : CHAP) Session Timeout (デフォルト値 : 1) 値は 1 から 60 の間でなければなりません。 Idle Timeout (デフォルト値 : 1) 値は 1 から 15 の間でなければなりません。
Server Type	必須入力項目	Active Directory Server (必須入力項目) : Active Directory Server を選択するとき、Domain 設定も必要です。 Domain (文字列形式：任意のテキスト)
		LDAP Server (必須入力項目) : LDAP Server を選択するときは、次の設定も必要です。
		Base DN (文字列形式：任意のテキスト) Identity (ID) (文字列形式：任意のテキスト) Password (文字列形式：任意のテキスト)
		UAM Server (必須入力項目) : UAM Server を選択するときは、次の設定も必要です。 Login URL (文字列形式：任意のテキスト) Shared Secret (文字列形式：任意のテキスト) NAS/Gateway ID (文字列形式：任意のテキスト) Location ID (文字列形式：任意のテキスト) Location Name (文字列形式：任意のテキスト)
		TACACS+ Server (必須入力項目) : TACACS+ Server を選択するときは、次の設定も必要です。

		<p>Shared Key (文字列形式: 任意のテキスト)</p> <p>Session Timeout (文字列形式: 任意のテキスト) 値は、1 から 60 の間でなければなりません。</p> <p>SCEP Server: SCEP Server を選択するときは、次の設定も必要です。</p> <p>Path (文字列形式: 任意のテキスト、デフォルト値: cgi-bin)</p> <p>Application (文字列形式: 任意のテキスト、デフォルト値: pkiclient.exe)</p> <p>FTP(SFTP) Server (必須入力項目): FTP(SFTP) Server を選択するときは、次の設定も必要です。</p> <p>User Name (文字列形式: 任意のテキスト)</p> <p>Password (文字列形式: 任意のテキスト)</p> <p>Protocol (FTP または SFTP を選択します。)</p> <p>Encryption (Plain、Explicit FTPS または Implicit FTPS を選択します。)</p> <p>Transfer mode (Passive または Active を選択します。)</p>
Server IP/FQDN	必須入力項目	外部サーバーの IP アドレスまたは FQDN を指定します。
Server Port	必須入力項目	<p>外部サーバーのポートを指定します。特定の Server Type を選択した場合、デフォルトサーバーポート番号が設定されます。</p> <p>Email Server の場合、デフォルト値: ポート 25</p> <p>Syslog Server の場合、デフォルト値: ポート 514</p> <p>RADIUS Server の場合、デフォルト値: ポート 1812</p> <p>Active Directory Server の場合、デフォルト値: ポート 389</p> <p>LDAP Server の場合、デフォルト値: ポート 389</p> <p>TACACS+ Server の場合、デフォルト値: ポート 49</p> <p>SCEP Server の場合、デフォルト値: ポート 80</p> <p>FTP(SFTP) Server の場合、デフォルト値: ポート 21</p> <p><u>値の範囲</u>: 1~65535。</p>
Authentication Port	1.必須入力項目 2.デフォルト値: 1812	<p>外部 RADIUS サーバーを選択する場合は、使用する認証ポートを指定してください。</p> <p><u>値の範囲</u>: 1~65535。</p>
Accounting Port	1.必須入力項目 2.デフォルト値: 1813	<p>外部 RADIUS サーバーを選択する場合は、使用するアカウントポートを指定してください。</p> <p><u>値の範囲</u>: 1~65535。</p>
UAM Port	1.必須入力項目 2.デフォルト値: 1813	<p>外部 UAM サーバーを選択する場合は、使用する UAM ポートを指定してください。</p> <p><u>値の範囲</u>: 1~65535。</p>
UAM UI Port	1.必須入力項目 2.デフォルト値: 1813	<p>外部 UAM サーバーを選択する場合は、使用する UAM UI ポートを指定してください。</p> <p><u>値の範囲</u>: 1~65535。</p>
Server	デフォルト値: チェックなし	Enable チェックボックスをクリックして、外部サーバーを有効化します。
Save	-	Save クリックして、設定を保存します。

Undo	-	Undo をクリックして、設定をキャンセルします。
Refresh	-	Refresh ボタンをクリックして、外部サーバーリストを更新します。

3.4 証明書

暗号化技術において、公開キー証明書（デジタル証明書、識別証明書とも呼ばれています）とは公開キーの所有者を示す電子文書です。この証明書には、キーに関する情報、所有者の識別情報、証明書の内容が本物であることを証明する機関によるデジタル署名が含まれています。署名が有効であり、証明書の検査者が署名者を信頼した場合、そのキーを使用してキーの所有者と通信できると判断できます。¹

一般的な公開キーインフラストラクチャ（PKI）スキームでは、署名者は証明機関（CA）です。通常、CAはVeriSignなどの企業で、有料で顧客に証明書を発行しています。「信頼の輪」方式では、署名者はキーの所有者（自己署名証明書）、または証明書の検査者が知っていて信頼している他のユーザー（保証）です。本製品はCAとしても機能します。

証明書はトランスポート層セキュリティ（TLS、従来のSSL）の重要な要素で、攻撃者が安全なWebサイトやその他のサーバーを偽装することを防ぎます。また、電子メールの暗号化やコード署名などの重要な用途でも使用されます。ここでは、ユーザー認証用のIPSecトンネリングで使用できます。

3.4.1 設定

ルート認証局（CA）証明書を作成し、SCEPの有効化をすることができます。ルートCAはツリーの最上位の証明書で、その秘密キーは他の証明書の「署名に」使用します。

Object Definition > Certificate > Configuration タブに進みます。

Root CA の作成

Root CA Generate					
ID	Name	Subject	Issuer	Valid To	Action

Generate ボタンがクリックされると、**Root CA Certificate Configuration** ウィンドウが表示されます。ルートCAに必要な情報には、名前、キー、サブジェクト名、および妥当性が含まれます。

¹ http://en.wikipedia.org/wiki/Public_key_certificate.

Root CA Certificate Configuration	
Item	Setting
▶ Name	<input type="text"/>
▶ Key	Key Type : <input type="text" value="RSA"/> Key Length : <input type="text" value="512-bits"/> Digest Algorithm : <input type="text" value="MD5"/>
▶ Subject Name	Country(C) : <input type="text"/> State(ST) : <input type="text"/> Location(L) : <input type="text"/> Organization(O) : <input type="text"/> Organization Unit(OU) : <input type="text"/> Common Name(CN) : <input type="text"/> Email : <input type="text"/>
▶ Validity Period	<input type="text" value="20-years"/>

Root CA Certificate Configuration		
項目	値設定	Description
Name	1.文字列形式：任意のテキスト 2. 必須入力項目	ルート CA 証明書名を入力します。これが、証明書ファイル名になります
Key	必須入力項目	このフィールドは、証明書のキー属性を指定するためのフィールドです。 Key Type : 公開鍵暗号システムを設定するためのキータイプを設定します。現在、RSA のみをサポートしています。 Key Length : 暗号化アルゴリズムにおいて使用されるキービット単位で測定されるサイズを設定します。 Digest Algorithm : 証明書の署名アルゴリズム識別子に識別子を設定します。
Subject Name	必須入力項目	このフィールドは、証明書の情報を指定するためのフィールドです。 Country(C) : 組織が所在する国の 2 文字の ISO コードです。 State(ST) : 組織が所在する州です。 Location(L) : 組織が所在する場所です。 Organization(O) : 組織の名称です。 Organization Unit(OU) : 組織単位の名称です。 Common Name(CN) : 組織の名称です。 Email : 組織の E メールです。これは、E メールアドレスのスタイルでなければなりません。
Validity Period	必須入力項目	このフィールドは、証明書の有効期間を指定するためのフィールドです。

SCEP の設定

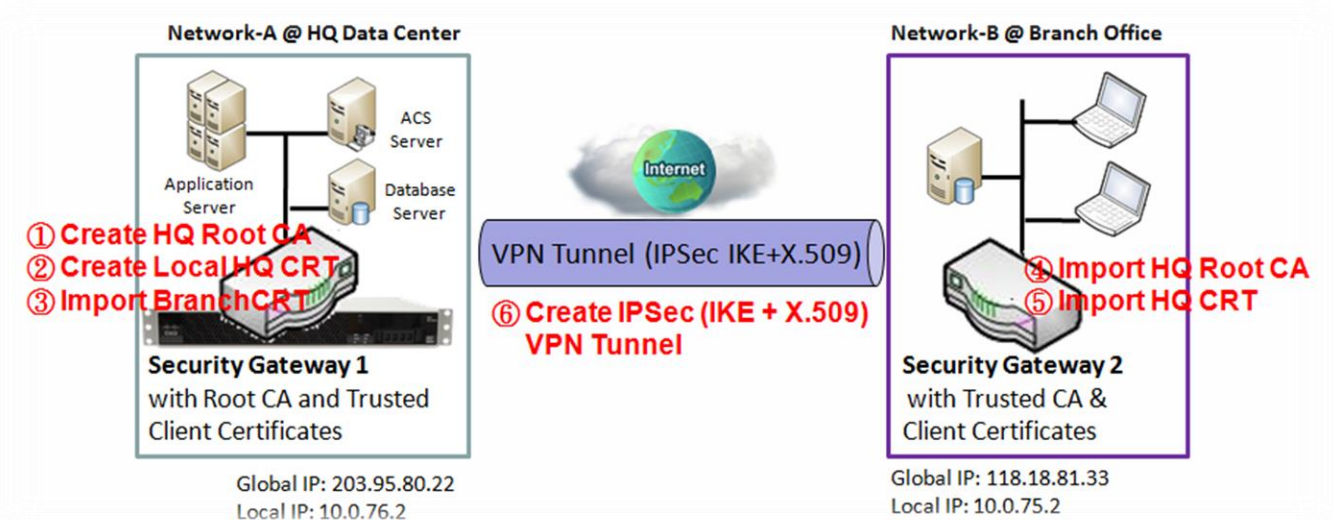
SCEP Configuration	
Item	Setting
▶ SCEP	<input type="checkbox"/> Enable
▶ Automatically re-enroll aging certificates	<input type="checkbox"/> Enable

SCEP Configuration		
項目	値設定	説明
SCEP	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、SCEP 機能が有効化されます。
Automatically re-enroll aging certificates	デフォルト値：チェックなし	SCEP が有効化されているとき、Enable チェックボックスにチェックを入れ、この機能を有効化します。これは、どの証明書が期限しているかを自動的に確認します。証明書が期限切れしている場合、SCEP 機能を有効化し、自動的に再登録します。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします。

3.4.2 自己署名証明書

自己署名証明書には、ローカル証明書リストが含まれます。ローカル証明書リストには、本製品のルート CA により生成されたすべての証明書が表示されます。また、生成された証明書署名要求 (CSR) も格納され、他の外部 CA によって署名されます。署名付き証明書は、本製品のローカル証明書としてインポートすることができます。

自己署名付き証明書の使用シナリオ



シナリオの適用タイミング

企業ゲートウェイが、ルート CA および VPN トンネリング機能を有する場合、企業ゲートウェイは、自身で署名した独自のローカル証明書を生成したり、他の外部 CA によって署名されたローカル証明書をインポートしたりすることができます。また、他の CA およびクライアントの信頼済み証明書もインポートします。さらに、ルート CA を持つため、証明書署名要求 (CSR) に署名して、他ユーザーに対応する証明書を作成することもできます。これらの証明書は、2つのリモートピアに対して使用し、VPN トンネルを確立する際に ID を確認することができます。

シナリオ説明

ゲートウェイ 1 は、ルート CA とそれ自身が署名したローカル証明書 (HQCRT) を生成します。また、信頼済み証明書 (BranchCRT) がゲートウェイ 1 のルート CA により署名されたゲートウェイ 2 の BranchCSR 証明書をインポートします。

ゲートウェイ 2 は、CSR (BranchCSR) を作成し、ゲートウェイ 1 のルート CA に BranchCRT 証明書として署名します。ゲートウェイ 2 に証明書をローカル証明書としてインポートします。さらに、ゲートウェイ 1 のルート CA の証明書を信頼済みとして、ゲートウェイ 2 にインポートします。(また、以下の 2 つのサブセクションを参照してください)

いずれかのピアから開始して、これらのサブネット内のすべてのクライアントホストが互いに通信できるように、IKE および X.509 プロトコルを使用して IPsec VPN トンネルを確立します。

パラメータの設定例

HQ におけるネットワーク-A の場合

以下の表に、上図に示すように、IPsec VPN トンネル確立のユーザー認証で使用される「My Certificate」機能の例として、パラメータ設定を示します。設定例は、次の 2 つのセクションの設定例と組み合わせて、ユーザー全体のシナリオを完了する必要があります。

表に記載されていないパラメータには、デフォルト値を使用します。

Configuration Path	[My Certificate] - [Root CA Certificate Configuration]
Name	HQRootCA
Key	Key Type : RSA Key Length : 1024 ビット
Subject Name	Country(C) : JP State(ST) : Fukuoka Location(L) : Kitakyushu Organization(O) : YSKHQ Organization Unit(OU) : HQRD Common Name(CN) : HQRootCA E-mail : hqrootca@ysknet.co.jp

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	HQCRT Self-signed
Key	Key Type : RSA Key Length : 1024 ビット
Subject Name	Country(C) : JP State(ST) : Fukuoka Location(L) : Kitakyushu Organization(O) : YSKHQ Organization Unit(OU) : HQRD Common Name(CN) : HQCRT E-mail : hqcrt@ysknet.co.jp

Configuration Path	[IPsec]-[Configuration]
IPsec	■ Enable

Configuration Path	[IPsec]-[Tunnel Configuratio]
Tunnel	■ Enable
Tunnel Name	s2s-101
Interfac	WAN 1
Tunnel Scenario	Site to Site
Operation Mode	Always on

Configuration Path	[IPsec]-[Local & Remote Configuration]
Local Subnet	10.0.76.0
Local Netmask	255.255.255.0
Full Tunnel	Disable
Remote Subnet	10.0.75.0
Remote Netmask	255.255.255.0
Remote Gateway	118.18.81.33

Configuration Path	[IPSec]-[Authentication]
Key Management	<i>IKE+X.509 Local Certificate : HQCRT Remote Certificate : BranchCRT</i>
Local ID	<i>User Name Network-A</i>
Remote ID	<i>User Name Network-B</i>

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	<i>Main Mode</i>
X-Auth	<i>None</i>

支社におけるネットワーク-Bの場合

以下の表に、上図に示すように、IPSec VPN トンネル確立のユーザー認証で使用される「My Certificate」機能の例として、パラメータ設定を示します。設定例は、次の2つのセクションの設定例と組み合わせて、ユーザー全体のシナリオを完了する必要があります。

表に記載されていないパラメータには、デフォルト値を使用します。

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	<i>BranchCRT Self-signed : <input type="checkbox"/></i>
Key	<i>Key Type : RSA Key Length : 1024 ビット</i>
Subject Name	<i>Country(C) : TW State(ST) : Taiwan Location(L) : Tainan Organization(O) : YSKHQ Organization Unit(OU) : HQRD Common Name(CN) : HQRootCA E-mail : hqrootca@ysknet.co.jp</i>

Configuration Path	[IPSec]-[Configuration]
IPSec	<input checked="" type="checkbox"/> <i>Enable</i>

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	<input checked="" type="checkbox"/> <i>Enable</i>
Tunnel Name	<i>s2s-102</i>
Interface	<i>WAN 1</i>
Tunnel Scenario	<i>Site to Site</i>
Operation Mode	<i>Always on</i>

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	<i>10.0.75.0</i>
Local Netmask	<i>255.255.255.0</i>
Full Tunnel	<i>Disable</i>
Remote Subnet	<i>10.0.76.0</i>
Remote Netmas	<i>255.255.255.0</i>
Remote Gatewa	<i>203.95.80.22</i>

Configuration Path	[IPSec]-[Authentication]
---------------------------	--------------------------

Key Management	<i>IKE+X.509 Local Certificate : BranchCRT Remote Certificate : HQCRT</i>
Local ID	<i>User Name Network-B</i>
Remote ID	<i>User Name Network-A</i>

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	<i>Main Mode</i>
X-Auth	<i>None</i>

シナリオ操作手順

上図において、「ゲートウェイ 1」は、本社のネットワーク-A のゲートウェイであり、イントラネットのサブネットは 10.0.76.0/24 です。これは、LAN インターフェイスに対して 10.0.76.2、WAN-1 インターフェイスに対して 203.95.80.22 の IP アドレスを持っています。上図において、「ゲートウェイ 2」は、支社のネットワーク-B のゲートウェイであり、イントラネットのサブネットは 10.0.75.0/24 です。これは、LAN インターフェイスに対して 10.0.75.2、WAN-1 インターフェイスに対して 118.18.81.33 の IP アドレスを持っています。両方とも NAT セキュリティゲートウェイとして機能します。

ゲートウェイ 1 は、ルート CA とそれ自身が署名しローカル証明書（HQCRT）を生成します。ルート CA と HQCRT の証明書をゲートウェイ 2 の「信頼済み CA 証明書リスト」と「信頼済みクライアント証明書リスト」にインポートします。

ゲートウェイ 2 は、自身の証明書（BranchCRT）用の証明書署名要求（BranchCSR）を生成します（ゲートウェイ 2 で自己署名証明書ではないものを生成し、その CSR の「View」ボタンをクリックしてください。それをダウンロードします）。ゲートウェイ 1 のルート CA によって署名された CSR を取得し、BranchCRT 証明書を取得します（名前を変更する必要があります）。ゲートウェイ 1 の「信頼済みクライアント証明書リスト」とゲートウェイ 2 の「ローカル証明書リスト」に証明書をインポートします。

ゲートウェイ 2 は、「Site to Site」シナリオと IKE および X.509 プロトコルを使用して、ゲートウェイ 1 に IPSec VPN トンネルを確立することができます。

最後に、10.0.75.0/24 と 10.0.76.0/24 の 2 つのサブネットにあるクライアントホストは、互いに通信することができます。

自己署名証明書設定

Object Definition > Certificate > My Certificate タブに進みます。

自己署名証明書設定では、ローカル証明書を作成できます。「My Certificate」ページには、「My Certificate」機能用の設定ウィンドウが2つあります。「Local Certificate List」ウィンドウには、本製品を表すために格納されている証明書または CSR が表示されます。「Local Certificate Configuration」ウィンドウでは、それ自体で生成される対応する証明書、または、他の CA によって署名される対応する CSR に必要な情報を記入することができます。

Local Certificate List の作成

Local Certificate List					
<input type="button" value="Add"/> <input type="button" value="Import"/> <input type="button" value="Delete"/>					
ID	Name	Subject	Issuer	Valid To	Actions

Add ボタンをクリックされると、Local Certificate Configuration ウィンドウが表示されます。証明書または CSR に記入するのに必要な情報には、名前、キーおよびサブジェクト名が含まれます。「Self-signed」チェックボックスにチェックが入っている場合は証明書、それ以外の場合は CSR です。

Local Certificate Configuration	
Item	Setting
▶ Name	<input type="text"/> Self-signed: <input type="checkbox"/>
▶ Key	Key Type: <input type="text" value="RSA"/> Key Length: <input type="text" value="1024-bits"/> Digest Algorithm: <input type="text" value="SHA-1"/>
▶ Subject Name	Country(C): <input type="text"/> State(ST): <input type="text"/> Location(L): <input type="text"/> Organization(O): <input type="text"/> Organization Unit(OU): <input type="text"/> Common Name(CN): <input type="text"/> Email: <input type="text"/>
▶ Extra Attributes	Challenge Password: <input type="text"/> Unstructured Name: <input type="text"/>
▶ SCEP Enrollment	Enable: <input type="checkbox"/> SCEP Server: <input type="text" value="-- Option --"/> <input type="button" value="Add Object"/> CA Certificate: <input type="text"/> CA Encryption Certificate: <input type="text" value="-- Option --"/> (Optional) CA Identifier: <input type="text"/> (Optional)

Local Certificate Configuration		
項目	値設定	説明
Name	1.文字列形式：任意のテキスト	証明書名を入力します。これが、証明書ファイル名になります。 Self-signed チェックが入っている場合は、ルート CA により署名

	2. 必須入力項目	名されます。 Self-signed にチェックが入っていない場合、証明書署名要求 (CSR) が生成されます。
Key	必須入力項目	<p>このフィールドは、証明書のキー属性を指定するためのフィールドです。</p> <p>Key Type : 公開鍵暗号システムを設定するためのキータイプを設定します。現在、RSA のみをサポートしています。</p> <p>Key Length : 暗号化アルゴリズムにおいて使用されるキービット単位で測定されるサイズを設定します。512/768/1024/1536/2048 から選択可能です。</p> <p>Digest Algorithm : 証明書の署名アルゴリズム識別子に識別子を設定します。MD5/SHA-1 から選択可能です。</p>
Subject Name	必須入力項目	<p>このフィールドは、証明書の情報を指定するためのフィールドです。</p> <p>Country(C) : 組織が所在する国の2文字のISOコードです。</p> <p>State(ST) : 組織が所在する州です。</p> <p>Location(L) : 組織が所在する場所です。</p> <p>Organization(O) : 組織の名称です。</p> <p>Organization Unit(OU) : 組織単位の名称です。</p> <p>Common Name(CN) : 組織の名称です。</p> <p>Email : 組織のEメールです。これは、Eメールアドレス設定でなければなりません。</p>
Extra Attributes	必須入力項目	<p>このフィールドは、証明書を生成するための追加情報を指定するためのフィールドです。</p> <p>Challenge Password : 将来、証明書失効を要求するために使用します。</p> <p>Unstructured Name : 追加情報を記載します。</p>
SCEP Enrollment	必須入力項目	<p>このフィールドは、SCEPの情報を指定するためのフィールドです。</p> <p>証明書署名要求 (CSR) を生成し、次に、SCEPサーバーにより、オンラインで署名する場合、Enable チェックボックスにチェックを入れることができます。</p> <p>SCEP Server を選択し、使用する SCEP サーバーを識別します。サーバーの詳細情報は、外部サーバーで指定できます。</p> <p>Object Definition > External Server > External Server を参照してください。Add Object ボタンを押して、生成することができます。</p> <p>どの証明書が認証のために SCEP サーバーにより、受け入れられるかを識別するために、CA Certificate を選択します。これは、信頼済み証明書で生成される可能性があります。</p> <p>必要に応じて、オプションの CA Encryption Certificate を選択して、どの証明書が、データ情報の暗号化のために、SCEP サーバーにより受け入れられるかを識別します。これは、信頼済み証明書で生成される可能性があります。</p> <p>オプションの CA Identifier を入力して、証明書に署名するため</p>

		に使用できる CA を識別します。
Save	-	Save ボタンをクリックして、設定を保存します。
Back	-	Back ボタンをクリックすると、画面が前ページに戻ります。

Import ボタンをクリックされると、**Import** ウィンドウが表示されます。存在する証明書ファイルから証明書をインポート、または証明書として PEM でエンコードされた文字列を直接貼り付けることができます。

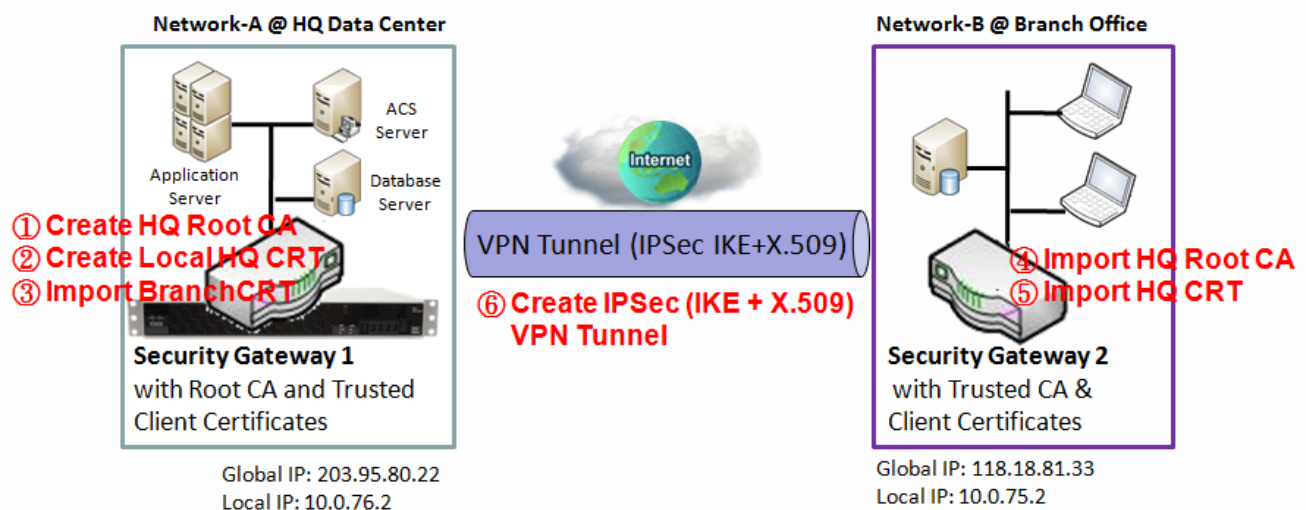


Import PEM Encoded 項目	値設定	説明
Import	必須入力項目	ユーザーのコンピュータから証明書ファイルを選択し、 Apply ボタンをクリックして、指定した証明書ファイルを本製品にインポートします。
PEM Encoded	1. 文字列形式：任意のテキスト 2. 必須入力項目	これは、証明書をインポートする別の方法です。PEM エンコードされた証明書文字列を直接入力（コピーアンドペースト）することができます。また、 Apply ボタンをクリックして、指定した証明書を本製品にインポートすることができます。
Appl	-	Apply ボタンをクリックして、証明書をインポートします。
Cancel	-	Cancel ボタンをクリックして、インポート操作を破棄し、 My Certificates ページに戻ります。

3.4.3 信頼済み証明書

Trusted Certificate（信頼済み証明書）には、Trusted CA Certificate List（信頼済み CA 証明書リスト）、Trusted Client Certificate List（信頼済みクライアント証明書リスト）、および、Trusted Client Key List（信頼済みクライアントキーリスト）が含まれます。Trusted CA Certificate List には、外部の信頼済み CA の証明書が一覧表示されます。Trusted Client Certificate List には、信頼済み他の証明書が一覧表示されます。また、Trusted Client Key List は、他のユーザーが信頼するもののキーを配置します。

自己署名付き証明書の使用シナリオ



シナリオの適用タイミング（「自己署名証明書」セクションで説明したものと同一）

企業ゲートウェイが、ルート CA および VPN トンネリング機能を有している場合、企業ゲートウェイは、自身で署名した独自のローカル証明書を生成することができます。また、他の CA およびクライアントの信頼済み証明書もインポートします。これらの証明書は、2つのリモートピアに対して使用し、VPN トンネルを確立する際に ID を確認することができます。

シナリオの説明（「自己署名証明書」セクションで説明したものと同一）

ゲートウェイ 1 は、ルート CA とそれ自身が署名したローカル証明書（HQCRT）を生成します。また、信頼済み証明書（BranchCRT）—ゲートウェイ 1 のルート CA により署名されたゲートウェイ 2 の BranchCSR 証明書をインポートします。

ゲートウェイ 2 は、CSR（BranchCSR）を作成し、ゲートウェイ 1 のルート CA に BranchCRT 証明書として署名します。ゲートウェイ 2 に証明書をローカル証明書としてインポートします。さらに、ゲートウェイ 1 のルート CA の証明書を信頼済みとして、ゲートウェイ 2 にインポートします。（また、「自己署名証明書」および「証明書の発行」セクションも参照してください）。

いずれかのピアから開始して、これらのサブネット内のすべてのクライアントホストが互いに通信

できるように、IKE および X.509 プロトコルを使用して IPsec VPN トンネルを確立します。

パラメータの設定例（「自己署名証明書」セクションで説明したものと同一）

HQ におけるネットワーク-A の場合

以下の表に、上図に示すように、IPsec VPN トンネル確立のユーザー認証で使用される「Trusted Certificate」機能の例として、パラメータ設定を示します。設定例は、「自己署名証明書」と「証明書の発行」セクションの設定と組み合わせて、ユーザー全体のシナリオの設定を完了する必要があります。

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	<i>Import</i>

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	<i>BranchCRT.crt</i>

支社におけるネットワーク-B の場合

以下の表に、上図に示すように、IPsec VPN トンネル確立のユーザー認証で使用される「Trusted Certificate」機能の例として、パラメータ設定を示します。設定例は、「My Certificate」と「Issue Certificate」セクションの設定と組み合わせて、ユーザー全体のシナリオの設定を完了する必要があります。

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate List]
Command Button	<i>Import</i>

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate Import from a File]
File	<i>HQRootCA.crt</i>

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	<i>Import</i>

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	<i>HQCRT.crt</i>

シナリオ操作手順（「自己署名証明書」セクションで説明したものと同一）

上図において、「ゲートウェイ 1」は、本社のネットワーク-A のゲートウェイであり、イントラネットのサブネットは 10.0.76.0/24 です。これは、LAN インターフェイスに対して 10.0.76.2、WAN-1 インターフェイスに対して 203.95.80.22 の IP アドレスを持っています。「ゲートウェイ 2」は、支社のネットワーク-B のゲートウェイであり、イントラネットのサブネットは 10.0.75.0/24 です。これは、LAN インターフェイスに対して 10.0.75.2、WAN-1 インターフェイスに対して 118.18.81.33 の IP アドレスを持っています。両方とも NAT セキュリティゲートウェイとして機能

します。

ゲートウェイ 2 において、ゲートウェイ 1 により生成され、署名されたルート CA および HQCRT の証明書を、ゲートウェイ 2 の「**Trusted CA Certificate List**」および「**Trusted Client Certificate List**」にインポートします。

取得した BranchCRT 証明書（ゲートウェイ 1 のルート CA 署名の後に派生した BranchCSR 証明書）をゲートウェイ 1 の「**Trusted Client Certificate List**」とゲートウェイ 2 の「**Local Certificate List**」にインポートします。詳細については、本マニュアルの「自己署名証明書」セクションのネットワーク-B 操作手順を参照してください。

ゲートウェイ 2 は、「**Site to Site**」シナリオと IKE および X.509 プロトコルを使用して、ゲートウェイ 1 に IPSec VPN トンネルを確立することができます。

最後に、10.0.75.0/24 と 10.0.76.0/24 の 2 つのサブネットにあるクライアントホストは、互いに通信することができます。

信頼済み証明書設定

Object Definition > Certificate > Trusted Certificate タブに進みます。

信頼済み証明書設定では、信頼済み証明書とキーをインポートすることができます。

信頼済み CA 証明書のインポート

Trusted CA Certificate List					
ID	Name	Subject	Issuer	Vaild To	Actions

Import ボタンがクリックされると、**Trusted CA import** ウィンドウが表示されます。存在する証明書ファイルか信頼済み CA 証明書をインポートすること、または、証明書として PEM でエンコードされた文字列を直接貼り付けることができます。

Trusted CA Certificate Import from a File

参照...

Apply Cancel

Trusted CA Certificate Import from a PEM

Apply Cancel

Trusted CA Certificate List
 Trusted CA Certificate Import from a File
 Trusted CA Certificate Import from a PEM

項目	値設定	説明
Import from a File	必須入力項目	ユーザーのコンピュータから CA 証明書ファイルを選択し、 Apply ボタンをクリックして、指定した CA 証明書ファイルを本製品にインポートします。
Import from a PEM	1.文字列形式：任意のテキスト 2. 必須入力項目	これは、CA 証明書をインポートする別の方法です。PEM エンコードされた CA 証明書文字列を直接入力（コピーアンドペースト）することができます。また、 Apply ボタンをクリックして、指定した CA 証明書を本製品にインポートすることができます。

Apply	-	Apply ボタンをクリックして、証明書をインポートします。
Cancel	-	Cancel ボタンをクリックして、インポート操作を破棄し、 Trusted Certificates ページに戻ります。

上記の方法で信頼済み CA 証明書をインポートする代わりに、SEC 証明書を SECP サーバーから取得することもできます。

SCEP が有効化されている場合 (オブジェクト定義 > 証明書 > 設定を参照)、**Get CA** ボタンをクリックすると、**Get CA Configuration** ウィンドウが表示されます。

Get CA Configuration

Item	Setting
▶ SCEP Server	--- Option --- ▼ <input type="button" value="Add Object"/>
▶ CA Identifier	<input type="text"/> (Optional)

Get CA Configuration		
項目	値設定	説明
SCEP Server	必須入力項目	SCEP Server を選択し、使用する SCEP サーバーを識別します。サーバーの詳細情報は、外部サーバーで指定できます。 Object Definition > External Server > External Server を参照してください。 Add Object ボタンを押して、生成することができます。
CA Identifier	1.文字列形式：任意のテキスト	オプションの CA Identifier を入力して、証明書に署名するために使用できる CA を識別します。
Save	-	Save をクリックして、設定を保存します。
Close	-	Close ボタンをクリックして、 Trusted Certificates ページに戻ります。

信頼済みクライアント証明書のインポート

Trusted Client Certificate List

ID	Name	Subject	Issuer	Vaild To	Actions

Import ボタンをクリックされると、**Trusted Client Certificate Import** ウィンドウが表示されます。存在する証明書ファイルか信頼済み CA 証明書をインポートすること、または、証明書として PEM でエンコードされた文字列を直接貼り付けることができます。

Trusted Client Certificate Import from a File

参照...

Trusted Client Certificate Import from a PEM

Trusted Client Certificate List

Trusted Client Certificate Import from a File

Trusted Client Certificate Import from a PEM

項目	値設定	説明
Import from a File	必須入力項目	ユーザーのコンピュータから証明書ファイルを選択し、 Apply ボタンをクリックして、指定した証明書ファイルを本製品にインポートします。
Import from a PEM	1. 文字列形式：任意のテキスト 2. 必須入力項目	これは、証明書をインポートする別の方法です。PEM エンコードされた証明書文字列を直接入力（コピーアンドペースト）することができます。また、 Apply ボタンをクリックして、指定した証明書を本製品にインポートすることができます。
Apply	-	Apply ボタンをクリックして、証明書をインポートします。
Cancel	-	Cancel ボタンをクリックして、インポート操作を破棄し、 Trusted Certificates ページに戻ります。

信頼済みクライアントキーのインポート

Trusted Client Key List

ID	Name	Actions

Import ボタンをクリックされると、**Trusted Client Key import** ウィンドウが表示されます。存在するファイルから信頼済みクライアントキーをインポートすること、または、キーとして PEM でエンコードされた文字列を直接貼り付けることができます。

Trusted Client Key Import from a File

参照...

Apply
Cancel

Trusted Client Key Import from a PEM

Apply
Cancel

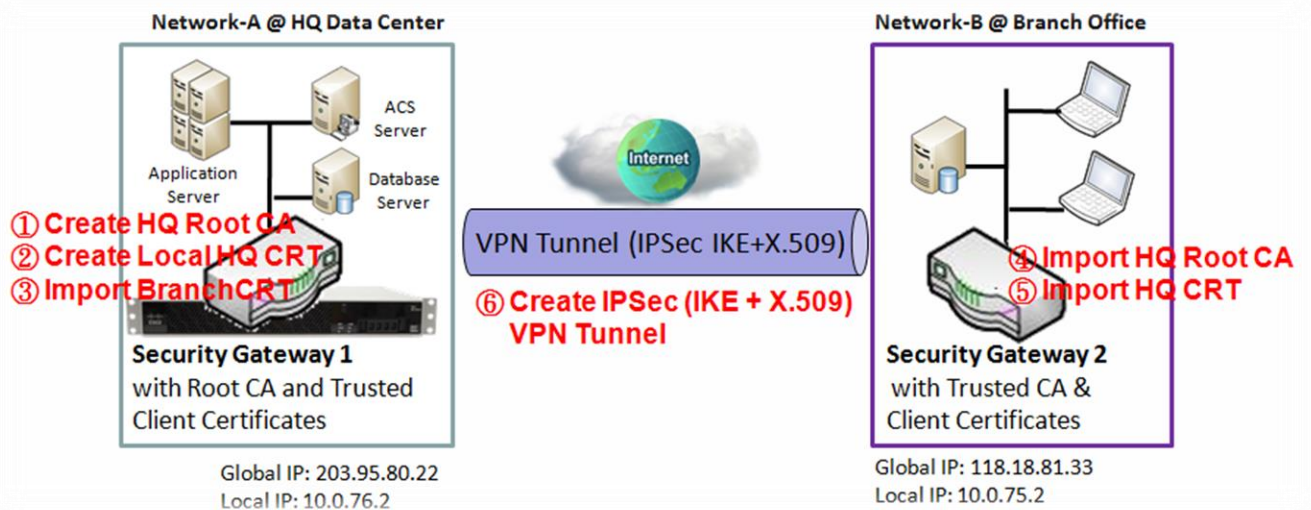
Trusted Client Key List		
Trusted Client Key Import from a File		
Trusted Client Key Import from a PEM		
項目	値設定	説明
Import from a File	必須入力項目	ユーザーのコンピュータからキーファイルを選択し、 Apply ボタンをクリックして、指定したキーファイルを本製品にインポートします。
Import from a PEM	1.文字列形式：任意のテキスト 2. 必須入力項目	これは、証明書をキーインポートする別の方法です。PEM エンコードされたキー文字列を直接入力（コピーアンドペースト）することができます。また、 Apply ボタンをクリックして、指定したキーを本製品にインポートすることができます。
Apply	-	Apply ボタンをクリックして、証明書キーをインポートします。
Cancel	-	Cancel ボタンをクリックして、インポート操作を破棄し、 Trusted Certificates ページに戻ります。

3.4.4 証明書発行

本製品のルート CA により証明する必要がある証明書署名要求 (CSR) がある場合、ここで要求を発効してルート CA に署名させることができます。証明書の発行には 2 通りの方法があります。1 つは管理用 PC からインポートした CSR ファイルから発行する方法です。別の方法は、ゲートウェイの Web ベースユーティリティに CSR コードをコピーアンドペーストし、「Sign」ボタンをクリックする方法です。

ゲートウェイが CSR に正常に署名すると、「Signed Certificate View」ウィンドウに結果の証明書の内容が表示されます。また、管理用 PC のファイルに証明書をダウンロードするための「Download」ボタンが利用可能です。

自己署名付き証明書の使用シナリオ



シナリオの適用タイミング（「自己署名証明書」セクションで説明したものと同一）

企業ゲートウェイが、ルート CA および VPN トンネリング機能を有している場合、企業ゲートウェイは、自身で署名した独自のローカル証明書を生成することができます。また、他の CA およびクライアントの信頼済み証明書もインポートします。これらの証明書は、2 つのリモートピアに対して使用し、VPN トンネルを確立する際に ID を確認することができます。

シナリオの説明（「自己署名証明書」セクションで説明したものと同一）

ゲートウェイ 1 は、ルート CA とそれ自身が署名したローカル証明書 (HQCRT) を生成します。また、信頼済み証明書 (BranchCRT) - ゲートウェイ 1 のルート CA により署名されたゲートウェイ 2 の BranchCSR 証明書をインポートします。

ゲートウェイ 2 は、CSR (BranchCSR) を作成し、ゲートウェイ 1 のルート CA に BranchCRT 証明書として署名します。ゲートウェイ 2 に証明書をローカル証明書としてインポートします。さらに、ゲートウェイ 1 のルート CA の証明書を信頼済みとして、ゲートウェイ 2 にインポートします。(また、「自己署名証明書」および「信頼済み証明書」セクションも参照してください)。

いずれかのピアから開始して、これらのサブネット内のすべてのクライアントホストが互いに通信できるように、IKE および X.509 プロトコルを使用して IPsec VPN トンネルを確立します。

パラメータの設定例 (「自己署名証明書」セクションで説明したものと同一)

HQ におけるネットワーク-A の場合

以下の表に、上図に示すように、IPsec VPN トンネル確立のユーザー認証で使用される「Issue Certificate」機能の例として、パラメータ設定を示します。設定例は、「自己署名証明書」と「信頼済み証明書」セクションの設定と組み合わせて、ユーザー全体のシナリオの設定を完了する必要があります。

Configuration Path	[Issue Certificate] - [Certificate Signing Request Import from a File]
Browse	C:/BranchCSR
Command Button	Sign

Configuration Path	[Issue Certificate] - [Signed Certificate View]
Command Button	Download (デフォルト名は、「issued.crt」です)

シナリオ操作手順 (「自己署名証明書」セクションで説明したものと同一)

上図において、「ゲートウェイ 1」は、本社のネットワーク-A のゲートウェイであり、イントラネットのサブネットは 10.0.76.0/24 です。これは、LAN インターフェイスに対して 10.0.76.2、WAN-1 インターフェイスに対して 203.95.80.22 の IP アドレスを持っています。「ゲートウェイ 2」は、支社のネットワーク-B のゲートウェイであり、イントラネットのサブネットは 10.0.75.0/24 です。これは、LAN インターフェイスに対して 10.0.75.2、WAN-1 インターフェイスに対して 118.18.81.33 の IP アドレスを持っています。両方とも NAT セキュリティゲートウェイとして機能します。

ゲートウェイ 1 は、ルート CA とそれ自身が署名しローカル証明書 (HQCRT) を生成します。ルート CA と HQCRT の証明書をゲートウェイ 2 の「信頼済み CA 証明書リスト」と「信頼済みクライアント証明書リスト」にインポートします。

ゲートウェイ 2 は、ルート CA により署名される自身の証明書 BranchCRT 用の証明書署名要求 (BranchCSR) を生成します (ゲートウェイ 2 で自己署名証明書ではないものを生成し、その CSR の「View (表示)」ボタンをクリックしてください。それをダウンロードします)。ゲートウェイ 1 のルート CA によって署名された CSR を取得し、BranchCRT 証明書を取得します (名前を変更する必要があります)。ゲートウェイ 1 の「信頼済みクライアント証明書リスト」とゲートウェイ 2 の「ローカル証明書リスト」に証明書をインポートします。

ゲートウェイ 2 は、「Site to Site (サイト間)」シナリオと IKE および X.509 プロトコルを使用し

て、ゲートウェイ 1 に IPSec VPN トンネルを確立することができます。

最後に、10.0.75.0/24 と 10.0.76.0/24 の 2 つのサブネットにあるクライアントホストは、互いに通信することができます。

証明書発行の設定

Object Definitio > Certificate > Issue Certificate タブに進みます。

証明書発行の設定では、証明書署名要求 (CSR) をインポートして、ルート CA によって署名されます。

証明書のインポートおよび発行

項目	値設定	説明
Certificate Signing Request (CSR) Import from a File	必須入力項目	ゲートウェイにインポートするコンピュータの証明書署名要求ファイルを選択します。
Certificate Signing Request (CSR) Import from a PEM	1. 文字列形式：任意のテキスト 2. 必須入力項目	署名要求 PEM エンコードされた証明書を本製品に入力（コピーアンドペースト）します。
Sign	-	ルート CA が存在する場合は、Sign ボタンをクリックし、インポートした証明書をルート CA により発行します。

第4章 フィールド通信

4.1 バスおよびプロトコル

本製品は、RS-232 または RS-485 シリアルデバイスを IP ベースのイーサネット LAN に接続することにより、さまざまなシリアル通信用のシリアルポートを装備することができます。これらの通信プロトコルにより、ユーザーはローカル LAN またはインターネット経由でどこからでも簡単にシリアルデバイスにアクセスできるようになります。

4.1.1 ポート設定

仮想 COM のように、サポートされているフィールド通信機能を使用する前に、まず物理通信ポートを設定する必要があります。

ポート設定画面では、各シリアルインターフェイスの動作モードと物理レイヤを設定することができます。また、シリアルポートの通信プロトコル間を素早く切り替えることもできます。

購入した製品モデルにより、ポート数およびサポートされるプロトコルの種類が異なる場合があります。

ポート設定

Field Communication > Bus & Protocol > Port Configuration タブに進みます。

「Port Configuration」ページには、シリアルポート設定用のウィンドウが1つあります。「Serial Port Definition」ウィンドウを使って、「Virtual COM」または「Modem」の動作モードと、「RS-232」または「RS-485」のインターフェイス、ボーレート、データビット長、ストップビット長、「RTS/CTS」、「DTS/DSR」または「None」のフロー制御およびパリティを含むシリアルポートパラメータを指定することができます。

Serial Port Definition								
Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Disable ▼	RS-232 ▼	9600 ▼	8 ▼	1 ▼	None ▼	None ▼	Edit

Serial Port Definition		
項目	値設定	説明
Serial Port	-	シリアルポートのシリアルポート ID が表示されます。
Operation Mode	デフォルト値 : Disable	シリアルインターフェイスでは、Disable、または Virtual COM / Modem mode の動作モードを選択します。 Modem mode は動作検証用の為、通常設定しないでください。
Interface	デフォルト値 : RS-232	同じインターフェイス仕様のアクセスデバイスに接続するために、 RS-232 または RS-485 物理インターフェイスを選択します。
Baud Rate	デフォルト値 : 9600	シリアルデバイス通信に適したボーレートを選択します。 RS-232 : 1200 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200 RS-485では、230400および460800のより高いボーレートを使用することができます。これは、ケーブルの長さや設置環境によって異なります。ケーブル長が長くなると、ボーレートが低くなります。
Data Bits	デフォルト値 : 8	データビットは、8または7を選択します。
Stop Bits	デフォルト値 : 1	ストップビットは、1または2を選択します。
Flow Control	デフォルト値 : None	RS-232モードでは、フロー制御には、None / RTS、CTS / DTS、DSRを選択します。 フロー制御のサポートは、購入したモデルにより異なります。
Parity	デフォルト値 : None	パリティビットには、None/Even/Odd を選択します。
Action	-	Edit ボタンをクリックして、動作モードを変更するか、シリアルインターフェイス通信に対する上記パラメータを変更します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

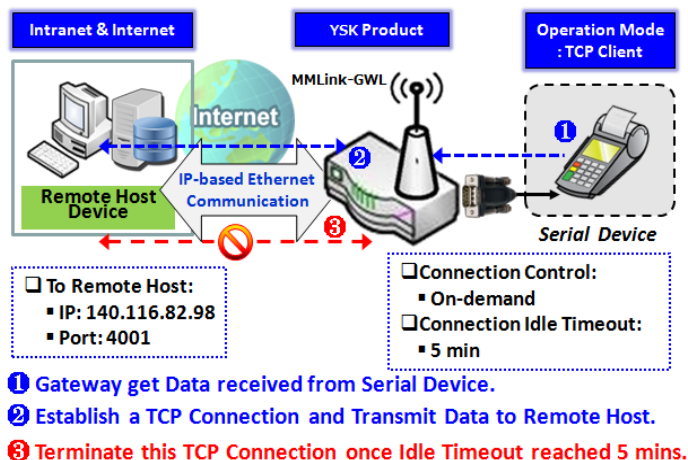
4.1.2 仮想 COM

ユーザーのPC/ホスト上に仮想COMポートを作成して、本製品のシリアルポートに接続されたシリアルデバイスへのアクセスを提供します。したがって、ユーザーは、インターネット（固定回線またはセルラーネットワーク）を介して、接続されたシリアルデバイスにアクセス、制御、および管理することができます。このアプリケーションは、イーサネットパススルー通信とも呼ばれます。

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Client	4001 (1~65535)	Allow All	1	Always on	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit
Data Buffer Length Delimiter Character 1 Delimiter Character 2 Data Timeout Transmit									

仮想COM設定画面により、仮想COMポートベースのデバイスをインターネットに接続することができます。これにより、ユーザーは、シリアルデータに遠隔からアクセスすることができます。接続されたシリアルデバイスにリモートアクセスするためのTCP Client、TCP Server、UDP、およびRFC2217モードがあります。これらの動作モードを以下に示します。

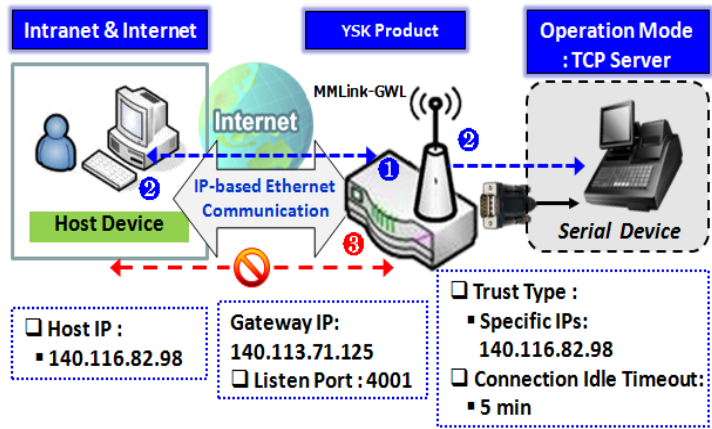
TCP クライアントモード



管理者が、シリアルデータが到着したときに本製品が事前定義されたホストコンピュータへのTCP接続をアクティブに確立することを期待する場合、「Virtual COM」機能の動作モードは「TCP Client)」である必要があります。そして、仮想COMの接続制御が「On-demand」の場合、ゲートウェイは接続されたシリアルデバイスからデータを受信すると、受信したシリアルデータをリモートホストに転送するためにTCP接続を確立します。さらに、データが転送された後、ゲートウェイは、TCPアライブチェックタイムアウトまたはアイドルタイムアウトの設定を使用して、確立されたTCPセッションをホストコンピュータから自動的に切断しま

す。

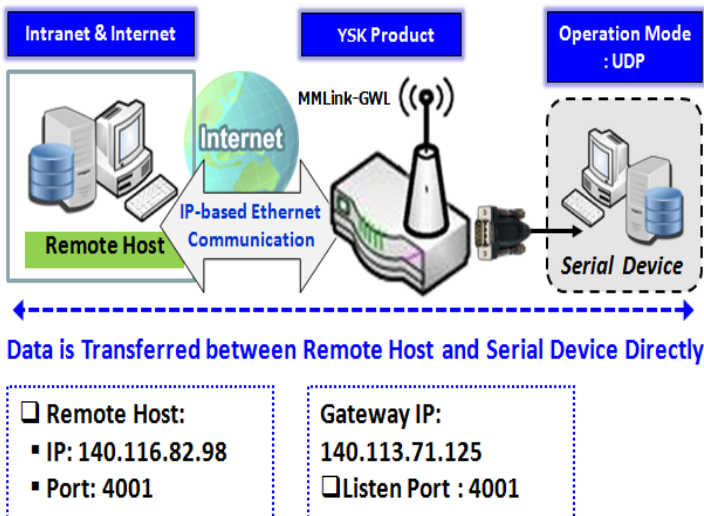
TCP サーバーモード



- ① Gateway remain Listening and Host will Establish a TCP Connection with it.
- ② Host Send Data then Gateway Transmit it to the Serial Device.
- ③ Terminate this TCP Connection once Idle Timeout reached 5 mins. から自動的に切断します。

管理者が、ゲートウェイがホストデバイスからのリアルデータ要求を受動的に待機することを期待し（通常、ホストとして機能させるためコンピュータを使用します）、ホストが、TCP 接続を確立してリアルデバイスからデータを取得するとき、「Virtual COM」機能の動作モードは、「TCP Server」である必要があります。このモードでは、ゲートウェイは、TCP/IP ネットワーク上で、一意の「IP : Port」アドレスを提供します。これは、複数のホストが同じリアルデバイスから同時にデータを収集できるように、最大 4 つの同時接続をサポートしています。データが転送されると、TCP 接続チェックタイムアウトまたはアイドルタイムアウト設定を使用して、TCP 接続は、ホストコンピュータ

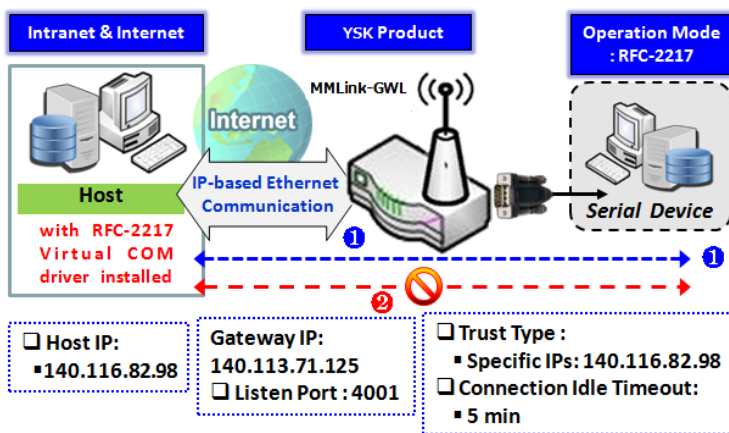
UDP モード



リモートホストコンピュータとリアルデバイスの両方で、データ転送を開始する必要がある場合、ゲートウェイの「Virtual COM」機能の動作モードは、「UDP」である必要があります。このモードでは、ゲートウェイと複数のホストコンピュータの間で UDP データを転送することができ、メッセージ表示アプリケーションに最適です。

リモートホストコンピュータは、ゲートウェイを介してリアルデバイスに UDP データを直接送信し、同時にゲートウェイを介して、リアルデバイスから UDP データを受信することもできます。ゲートウェイは、ゲートウェイ経由でリアルデバイスに同時に接続するために、最大 4 つの有効なホストをサポートします。

RFC-2217 モード



① Send data to each other directly via a transparent connection established

② Terminate this Connection once Idle Timeout reached 5 mins.

リアルデバイス間のトランスペアレントな接続を確立します。ゲートウェイのシリアルポートの IP : ポートをホストコンピュータの仮想ローカル COM ポートにマッピングします。

ホストコンピュータは、ゲートウェイを介してシリアルデバイスにデータを直接送信し、同時にゲートウェイを介して、シリアルデバイスからデータを受信することもできます。ゲートウェイは、最大 4 つのインターネットホストコンピュータをサポートします。

RFC-2217 は、Telnet プロトコルに基づいて、一般的な COM ポート制御オプションを定義します。RFC 2217 ドライバがインストールされたホストコンピュータは、ローカルシリアルポートに接続されているかのように、ゲートウェイのシリアルポートに接続されているリモートシリアルデバイスを監視および管理することができます。ローカルシリアルデバイス上の仮想シリアルポートを作成するときは、接続を確立するホストコンピュータの IP アドレスを指定する必要があります。

RFC2217 をサポートするサードパーティ製ドライバを使用して、ホストコンピュータにインストールすると、ドライバは、ホストコンピュータとシ

仮想 COM 設定

仮想 COM 設定画面により、仮想 COM ポートベースのデバイスをインターネットに接続することができます。これにより、ユーザーは、シリアルデータに遠隔からアクセスすることができます。接続されたシリアルデバイスにリモートアクセスするための TCP Client、TCP Server、UDP、および RFC2217 モードがあります。

仮想 COM 機能を使用するには、まず多機能シリアルポートの動作モードを指定する必要があります。Field Communication > Bus&Protocol > Port Configuration タブに進み、Virtual COM を予想される動作モードとして選択し、関連するポート設定を行います。

その後、Field Communication > Bus&Protocol > Virtual COM タブに進み、Virtual COM 設定の詳細な設定を行います。

TCP クライアントモードの有効化

本製品を TCP (Transmission Control Protocol) クライアントとして設定します。TCP クライアントモードでは、送信するデータがある場合、デバイスは TCP サーバーとの TCP 接続を開始します。指定した期間、接続がアイドルの場合、デバイスはサーバーから切断されます。また、TCP サーバーとの常時接続を有効化することもできます。

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Client	N/A	N/A	N/A	Always on	N/A	N/A	<input type="checkbox"/>	Edit

Operation Mode Definition for each Serial Port		
項目	値設定	説明
Operation Mode	必須入力項目	TCP Client を選択します。
Connection Control	デフォルト値 : Always on	TCP 常時接続の場合は、 Always on を選択します。それ以外の場合は、 On-Demand を選択して、送信が必要な場合にのみ TCP 接続を開始し、アイドルタイムアウト時に切断します。
Connection Idle Timeout	1. デフォルト値 : 0	アイドルタイムアウトを分単位で入力します。 アイドルタイムアウトは、アイドル時間が経過したときに、TCP 接続を切断するために使用されます。 Connection Control フィールドで、 On-Demand が選択されている場合にのみ利用可能です。 値の範囲 : 0~3600 秒。
Alive Check Timeout	1. デフォルト値 : 0	アライブチェックタイムアウトの期間を入力します。アライブチェックの応答がこのタイムアウト設定値より長い時間なかった場合、TCP 接続が終了します。 値の範囲 : 0~3600 秒。
Enable	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れ、指定された動作モードで対応するシリアルポートを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。

データパッキングパラメータの指定

Data Packing (for TCP Client, TCP Server and UDP operation mode)				
Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	<input type="text" value="0"/> (0~1024)	<input type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input type="text" value="0"/> (0~1000ms)

Legal Host IP/EQDN Definition(for TCP Client operation mode)		
項目	値設定	説明
Data Buffer Length	1. 任意の設定項目 2. デフォルト値 : 0	シリアルポートのデータバッファ長を入力します。 値の範囲 : 0~1024。
Delimiter Character 1	1. 任意の設定項目 2. デフォルト値 : 0	Enable チェックボックスをオンにしてデリミタ文字 1 を有効にし、その文字コードの 16 進数を入力します。 値の範囲 : 0x00~0xFF。
Delimiter Character 2	1. 任意の設定項目 2. デフォルト値 : 0	Enable チェックボックスをオンにして、デリミタ文字 2 を有効にし、その文字コードを入力します。 値の範囲 : 0x00~0xFF。
Data Timeout Transmi	1. 任意の設定項目 2. デフォルト値 : 0	シリアルデータをポートから送信するためのデータタイムアウト間隔を入力します。 デフォルトでは 0 に設定されており、タイムアウト機能は無効になっています。 値の範囲 : 0~1000ms
Save	-	Save ボタンをクリックして、設定を保存します
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

リモート TCP サーバーの指定

Legal Host IP/ FQDN Definition (for TCP Client operation mode)					
ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	<input type="checkbox"/>	Edit
2		4001	SPort-0	<input type="checkbox"/>	Edit
3		4001	SPort-0	<input type="checkbox"/>	Edit
4		4001	SPort-0	<input type="checkbox"/>	Edit

Legal Host IP/EQDN Definition(for TCP Client operation mode)		
項目	値設定	説明
To Remote Host	必須入力項目	Edit ボタンを押して、シリアルデータを送信するリモート TCP サーバーの IP アドレスまたは FQDN を入力します。
Remote Port	1. 必須入力項目 2. デフォルト値 : 4001	TCP ポート番号を入力します。これは、リモート TCP サーバーのリスンポートです。 値の範囲 : 1~65535。
Serial Poort	デフォルト値 : SPort-0	選択したシリアルポートに対して、TCP サーバー接続を適用します。シリアルポートごとに最大 4 つの TCP サーバーを同時に設定することができます。
Definition Enable	デフォルト値 : チェックなし	Enable ボックスにチェックを入れ、TCP サーバーの設定を有効化します。
Save	-	Save ボタンをクリックして、設定を保存します
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

TCP サーバーモードの有効化

本製品をTCP（Transmission Control Protocol）サーバーとして設定します。TCPサーバーは、シリアルデータを受信するリモートTCPクライアントデバイスにより開始される接続を待機します。この設定により、ユーザーは特定のTCPクライアントを指定したり、シリアルデータ送信帯域幅制御とアクセス制御に対してシリアルデータを送信したりすることができます。TCPサーバーは、複数のTCPクライアントからシリアルデータを受信するために、最大4つの同時接続をサポートしています。

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Server	4001	Allow All	1	N/A	0 sec(s)	0 sec(s)	<input type="checkbox"/>	Edit

Operation Mode Definition for each Serial Port		
項目	値設定	説明
Operation Mode	必須入力項目	TCP Server モードを選択します。
Listen Port	デフォルト値： 4001	TCP 接続のリスニングポートを指定します。 値の範囲：1～65535。
Trust Type	デフォルト値： Allow All	Allow All を選択すると、全 TCP クライアントが接続できるようになります。それ以外の場合は、 Specific IP を選択して、特定の TCP クライアントを制限します。
Max Connection	1. 最大 4 接続 2. デフォルト値：1	同時 TCP 接続の最大数を設定します。同時に最大 4 つの TCP 接続を確立することができます。 値の範囲：1～128。
Connection Idle Timeout	デフォルト値：0	アイドルタイムアウトを分単位で入力します。アイドルタイムアウトは、アイドル時間が経過したときに、TCP 接続を切断するために使用されます。 Connection Control フィールドで、 On-Demand が選択されている場合にのみ利用可能です。 値の範囲：0～3600 秒。
Alive Check Timeout	デフォルト値：0	ライブチェックタイムアウトの期間を入力します。ライブチェックの応答がこのタイムアウト設定値より長い時間なかった場合、TCP 接続が終了します。 値の範囲：0～3600 秒。
Enable	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、指定された動作モードで対応するシリアルポートを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

TCP サーバーアクセスに対する TCP クライアントを指定する

Trust Type として、Specific IPs を選択した場合、Trusted IP Definition ウィンドウが表示されます。この設定は、TCP Server モードと RFC 2217 モードの両方で有効です。

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)				
ID	Host	Serial Port	Definition Enable	Action
1			<input type="checkbox"/>	Edit
2			<input type="checkbox"/>	Edit
3			<input type="checkbox"/>	Edit
4			<input type="checkbox"/>	Edit
5			<input type="checkbox"/>	Edit
6			<input type="checkbox"/>	Edit
7			<input type="checkbox"/>	Edit
8			<input type="checkbox"/>	Edit

Trusted IP Definition(for TCP Server & RF-2217 operation mode)		
項目	値設定	説明
Host	必須入力項目	許可された TCP クライアントの IP アドレス範囲を入力します。
Serial Port	デフォルト値：チェックなし	チェックボックスのチェックと入れて、選択したシリアルポートのルールを指定します。
Definition Enable	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れて、ルールを有効化します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします。

UDP モードの有効化

UDP (User Datagram Protocol) により、UDPソケットプログラムを使用するアプリケーションは、シリアルサーバー上のシリアルポートと通信できるようになります。UDPモードは、コネクションレス通信を提供します。これにより、シリアルデバイスから複数のホストコンピュータにデータをマルチキャストできるようになります (また、その逆も行われます)。これは、メッセージ表示アプリケーションに最適にします。

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	UDP	4001	N/A	N/A	N/A	N/A	N/A	<input type="checkbox"/>	Edit

Operation Mode Definition for each Serial Port		
項目	値設定	説明
Operation Mode	必須入力項目	UDP モードを選択します。
Listen Port	デフォルト値 : 4001	UDP 接続のリスニングポートを指定します。 値の範囲 : 1~65535。
Enable	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れ、指定された動作モードで対応するシリアルポートを有効化します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

リモート UDP の指定

Legal Host IP Definition (for UDP operation mode)					
ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	<input type="checkbox"/>	Edit
2		4001	SPort-0	<input type="checkbox"/>	Edit
3		4001	SPort-0	<input type="checkbox"/>	Edit
4		4001	SPort-0	<input type="checkbox"/>	Edit

Legal Host IP Definition(for UDP operation mode)		
項目	値設定	説明
Host	必須入力項目	Edit ボタンを押して、リモート UDP ホストの IP アドレス範囲を入力します。
Remote Port	デフォルト値 4001 が設定されています。	ピア UDP ホストの UDP ポートを指定します。 値の範囲 : 1~65535。
Serial Port	デフォルト値 : SPort-0 が設定されています。	選択したシリアルポートに UDP ホストを適用します。シリアルポートごとに最大 4 つの UDP サーバーを同時に設定することができます。
Definition Enable	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れて、ルールを有効化します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

RFC-2217 モードの有効化

RFC-2217 は、Telnet プロトコルに基づいて、一般的な COM ポート制御オプションを定義します。RFC 2217 モードにより、リモートホストは、リモートシリアル接続デバイスを、ローカルシリアルポートに接続されているかのように監視および管理することができます。ローカルシリアルデバイス上の仮想シリアルポートを作成するときは、接続を確立するリモートホストの IP アドレスを指定する必要があります。

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	RFC-2217	4001	Allow All	N/A	N/A	0 sec(s)	0 sec(s)	<input type="checkbox"/>	Edit

Operation Mode Definition for each Serial Port		
項目	値設定	説明
Operation Mode	必須入力項目	RFC-2217 モードを選択します。
Listen Port	デフォルト値 : 4001	RFC-2217 接続のリスニングポートを指定します。 値の範囲 : 1~65535。
Trust Type	デフォルト値 : Allow All	Allow All を選択すると、全クライアントが接続できるようになります。それ以外の場合は、 Specific IP を選択して、特定のクライアントを制限します。
Connection Idle Timeout	デフォルト値 : 0	アイドルタイムアウトを分単位で入力します。アイドルタイムアウトは、アイドル時間が経過したときに、接続を切断するために使用されます。 値の範囲 : 0~3600 秒。
Alive Check Timeout	デフォルト値 : 0	アライブチェックタイムアウトの期間を入力します。アライブチェックの応答がこのタイムアウト設定値より長い時間なかった場合、接続が終了します。 値の範囲 : 0~3600 秒。
Enable	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れ、指定された動作モードで対応するシリアルポートを有効化します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします。

アクセス用にリモートホストを指定する

Trust Type として、Specific IPs を選択した場合、Trusted IP Definition ウィンドウが表示されます。この設定は、TCP Server モードと RFC 2217 モードの両方で有効です。

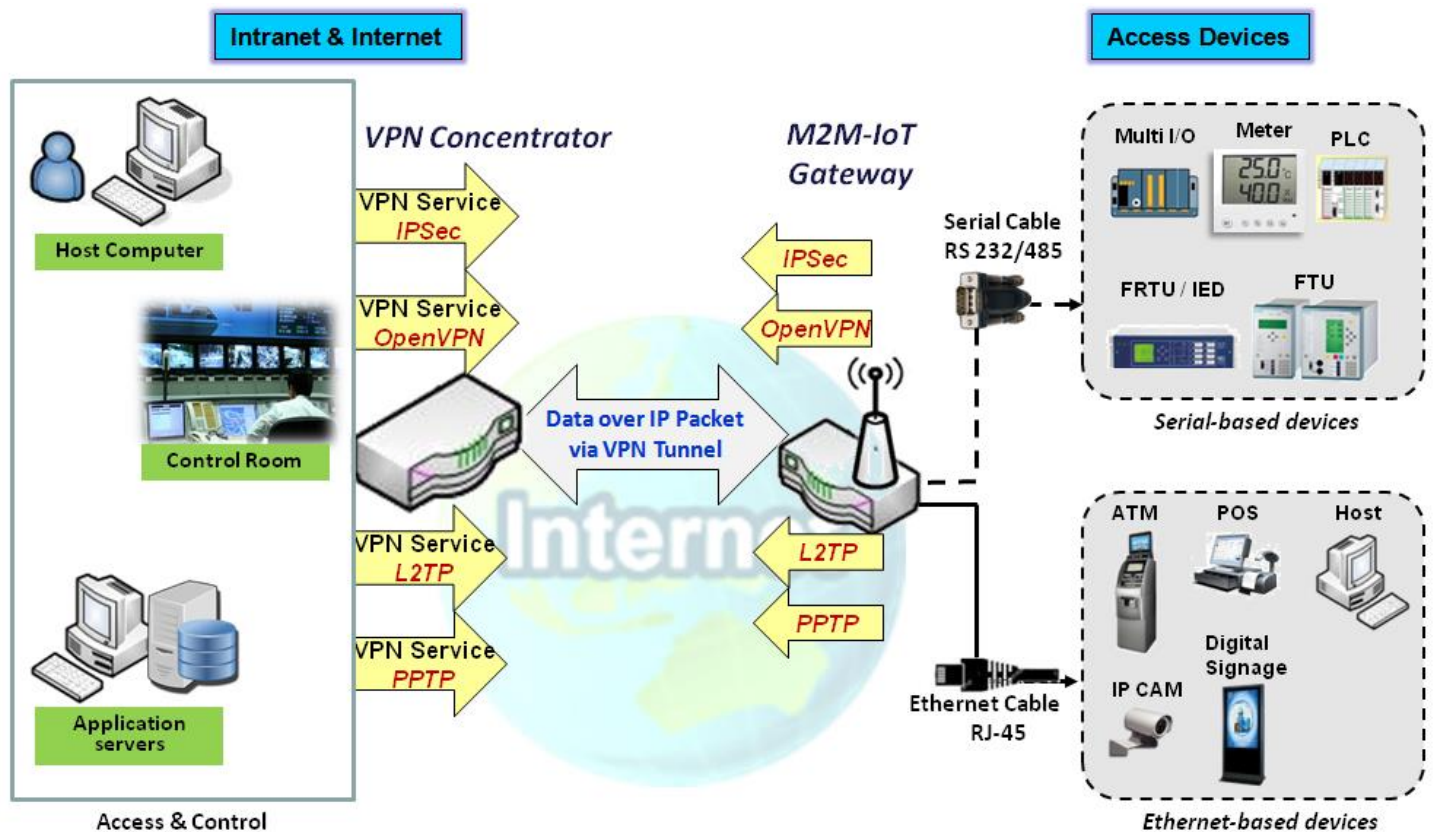
Trusted IP Definition (for TCP Server & RFC-2217 operation mode)				
ID	Host	Serial Port	Definition Enable	Action
1			<input type="checkbox"/>	Edit
2			<input type="checkbox"/>	Edit
3			<input type="checkbox"/>	Edit
4			<input type="checkbox"/>	Edit
5			<input type="checkbox"/>	Edit
6			<input type="checkbox"/>	Edit
7			<input type="checkbox"/>	Edit
8			<input type="checkbox"/>	Edit

Trusted IP Definition(for TCP Server & RFC-2217 operation mode)		
項目	値設定	説明
Host	必須入力項目	許可されたクライアントの IP アドレス範囲を入力します。
Serial Port	デフォルト値：チェックなし	チェックボックスのチェックと入れて、選択したシリアルポートのルールを指定します。
Definition Enable	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れて、ルールを有効化します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

第5章 セキュリティ

5.1 VPN

仮想プライベートネットワーク（VPN）はプライベートネットワークをインターネットなどのパブリックネットワークにまたがって拡張する機能です。これにより、コンピュータはプライベートネットワークに直接接続しているかのように、共有ネットワークやパブリックネットワークにまたがってデータの送受信を行うことができます。また、プライベートネットワークの機能、セキュリティ、管理ポリシーを利用することができます。この機能を利用するには、専用の接続や暗号化、またはその両方を使用して仮想ポイントツーポイント接続を確立します。トンネル技術では、カプセル化プロトコル、暗号化アルゴリズム、ハッシュアルゴリズムを利用することにより、データの機密性、データの送信元認証、データの統合性を実現します。



本製品シリーズは、IPsec、OpenVPN、L2TP（over IPsec）、PPTP、GREなど、データ転送のために複数サイト間で安全なトンネルを確立するためのさまざまなトンネリング技術をサポートしています。さらに、Full Tunnel、Tunnel Failover、NetBIOS over IPsec、NAT Traversal、Dynamic VPNなどの高度な機能もサポートされています。

5.1.1 IPsec

Configuration [Help]	
Item	Setting
▶ IPsec	<input type="checkbox"/> Enable
▶ NetBIOS over IPsec	<input type="checkbox"/> Enable
▶ NAT Traversal	<input checked="" type="checkbox"/> Enable
▶ Max. Concurrent IPsec Tunnels	3

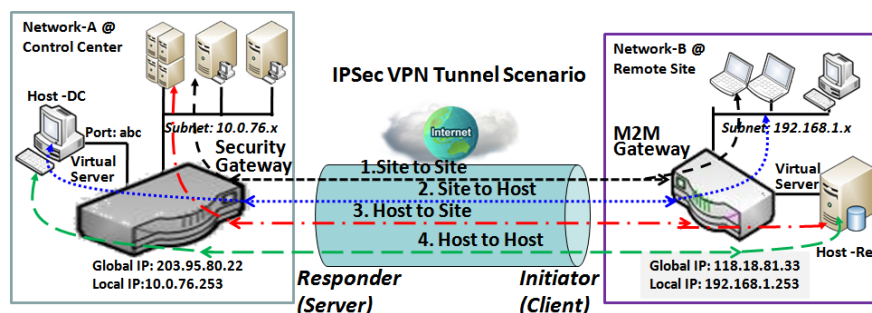
Dynamic server List [Add] [Delete]					
ID	Tunnel Name	Interface	Connected Client	Enable	Actions

IPsec Tunnel List [Add] [Delete] [Refresh]								
ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions

IPsec（インターネットプロトコルセキュリティ）は、IP（インターネットプロトコル）通信をセキュリティ保護するために、通信セッションの各IPパケットを認証および暗号化するプロトコルスイートです。IPsecには、セッション開始時にエージェント間で相互認証を行い、セッション中に使用する暗号キーのネゴシエーションを行うためのプロトコルが含まれます。

IPsecクライアントとサーバーの間で、IPsec VPNトンネルが確立されます。IPsec VPNクライアントは「イニシエーター」、IPsec VPNサーバーは「レスポнда」と呼ばれることもあります。この本製品は、さまざまな役割として設定したり、さまざまなリモートデバイスとのトンネル数を確立したりすることができます。VPN接続を設定する前に、トンネリングのシナリオタイプを決定する必要があります。

IPsec トンネルのシナリオ



- ←----- Site to Site: Tunnel between M2M gateway /w 192.168.1.x subnet and UTM /w 10.0.76.x subnet
- ←----- Site to Host: Tunnel between M2M gateway /w 192.168.1.x subnet and Host-DC under UTM
- ←----- Host to Site: Tunnel between Host-Re under M2M Gateway and UTM /w 10.0.76.x subnet
- ←----- Host to Host: Tunnel between Host-Re under M2M Gateway and Host-DC under UTM

IPsec トンネルを構築するには、IPsec ピアの後にあるホストがリモートサイトまたはホストにアクセスできる場合は、リモートゲートウェイのグローバルIPとオプションのサブネットを入力する必要があります。このような設定では、次の4つのシナリオがあります。

Site to Site : 両方のゲートウェイのリモートゲートウェイIPとサブネットを設定する必要があります。IPsecトンネルが確立すると、両方のゲートウェイの後にあるホストは、トンネルを介

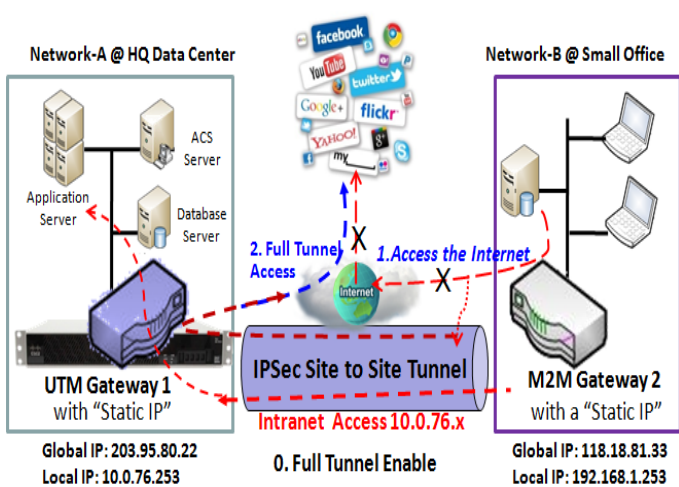
して互いに通信することができます。

Site to Host : Site to Host は、サブネット内のクライアントとアプリケーションサーバー（ホスト）間のトンネリングに適しています。図のように、M2M ゲートウェイの後にあるクライアントは、Site to Host VPN トンネルを介して、コントロールセンターにあるホスト「Host-DC」にアクセスすることができます。

Host to Site : 対照的に、単一ホスト（またはモバイルユーザー）がイントラネット内のリソースにアクセスするためには、ホストからサイトへのシナリオを適用することができます。

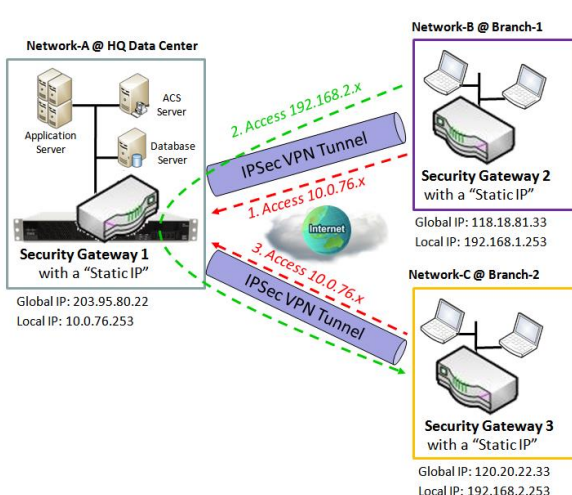
Host to Host : Host to Host は、2つの単一ホストの間に VPN トンネルを構築するための特別な設定です。

「Full Tunnel」を有効化した Site to Site



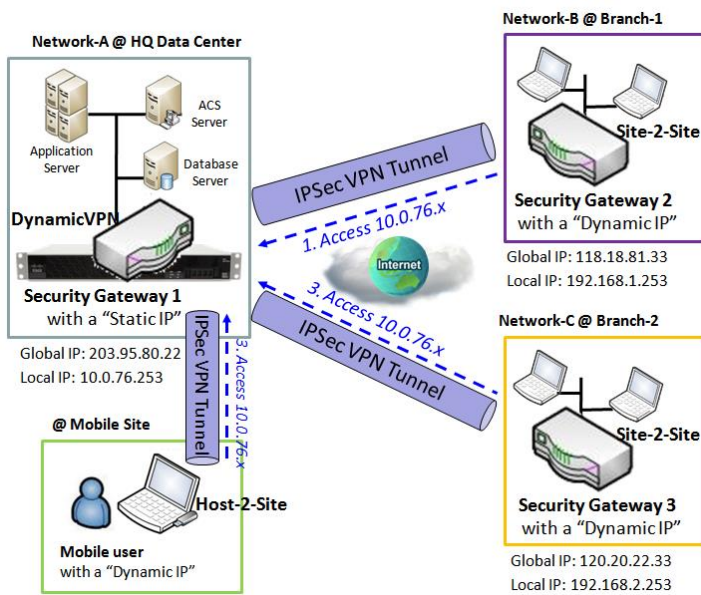
「Site to Site」シナリオでは、リモートサイトのクライアントホストは、前述のように、確立された IPsec トンネルを介して HQ ゲートウェイのイントラネット内のエンタープライズリソースにアクセスできます。しかし、インターネットアクセスはリモートサイトから発生し、通常の WAN 接続をそのまま使用します。リモートサイトからのすべてのパケットを HQ サーバーアクセスまたはインターネットアクセスを含むこの IPsec トンネル経由でルーティングする場合は、「フルトンネル」設定を有効にしてください。その結果、ユーザーが、インターネット上の Web サーフィンやデータ検索、個人メールや HQ サーバーアクセスの確認を行うたびに、すべてのトラフィックが安全な IPsec トンネルを通過し、コントロールセンターのセキュリティゲートウェイによってルーティングされます。

「ハブアンドスポーク」メカニズムを備えたサイト間



コントロールセンターがすべてのリモートサイトの中で、安全なイントラネットを管理するために、VPN ネットワーク全体に対して、ハブアンドスポークと呼ばれる簡単な設定があります。ハブアンドスポーク VPN ネットワークは、店舗やオフィスなどのすべてのリモートサイトに集中管理センターを持つ組織に設置されています。コントロールセンターはハブの役割を果たし、遠隔の店舗やオフィスはスポークの役割を果たします。リモートサイトからのすべての VPN トンネルは、このハブで終了します。そして、このハブはコンソリデータとして機能します。スポーク間のサイト間接続は存在しません。1つのスポークから発信される別のスポーク宛のトラフィックは、ハブを経由しなければなりません。このような構成では、2つのリモートクライアント間に VPN トンネルを維持する必要はありません。

動的 VPN サーバーのシナリオ



動的 VPN サーバーのシナリオは、特に動的 IP を使用するモバイルクライアントの場合、リモートサイトで複数のトンネルを構築する効率的な方法です。このシナリオでは、ゲートウェイはサーバー（レスポンス）の役割のみになり、「Static IP」または「FQDN」が必要です。

これにより、多くの VPN クライアント（イニシエータ）が、さまざまなトンネルシナリオに接続できるようになります。要するに、単純な動的 VPN サーバー設定では、多くの VPN クライアントが、サーバーに接続することができます。しかし、ハブアンドスポークのメカニズムと比較して、動的 VPN サーバー経由で、任意の 2 つのクライアント間で直接通信することはできません。

本製品の場合は、WAN インターフェイスごとに 1 つの動的 VPN サーバーを設定することができます。

IPSec 設定

Security > VPN > IPSec タブに進みます。

IPSec 設定により、IPSec トンネルを作成および設定することができます。

IPSec の有効化

Configuration [Help]	
Item	Setting
▶ IPSec	<input type="checkbox"/> Enable
▶ NetBIOS over IPSec	<input type="checkbox"/> Enable
▶ NAT Traversal	<input checked="" type="checkbox"/> Enable
▶ Max. Concurrent IPSec Tunnels	3

Configuration		
項目	値設定	説明
IPsec	デフォルト値：チェックなし	Enable チェックボックスをクリックして、IPSec 機能を有効化します。
NetBIOS over IPsec	デフォルト値：チェックなし	Enable チェックボックスをクリックして、NetBIOS over IPsec 機能を有効化します。
NAT Traversal	デフォルト値：チェックあり	Enable チェックボックスをクリックして、NAT Traversal 機能を有効化します。
Max.Concurrent IPsec Tunnels	デフォルト値：3	指定された値は、IPsec トンネルの同時接続の最大数を制限します。購入したモデルのデフォルト値は異なる場合があります。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

IPsec トンネルの作成/編集

IPsec トンネル設定をさらに設定する前に、IPsec 有効化チェックボックスにチェックが入っていることを確認して有効にしてください。

IPsec Tunnel List								
ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>								

Add/Edit ボタンをクリックされると、設定ウィンドウが表示されます。**Tunnel Configuration**、**Local & Remote Configuration**、**Authentication**、**IKE Phase**、**IKE Proposal Definition**、**IPsec Phase**、および、**IPsec Proposal Definition** です。ローカルとリモートの両方の VPN デバイスのトンネルの詳細を設定する必要があります。

Tunnel Configuration	
Item	Setting
▶ Tunnel	<input type="checkbox"/> Enable
▶ Tunnel Name	IPsec #1
▶ Interface	WAN1 ▼
▶ Tunnel Scenario	Site to Site ▼
▶ Tunnel TCP MSS	Auto ▼ 0 (64~1500 Bytes)
▶ Hub and Spoke	None ▼
▶ Operation Mode	Always on ▼
▶ Encapsulation Protocol	ESP ▼

Tunnel Configuration

項目	値設定	説明
Tunnel	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、IPSec トンネルを有効化しります。
Tunnel Name	1. 必須入力項目 2. 文字列形式：任意のテキスト	トンネル名を入力します。識別しやすい名称を入力します。 <u>値の範囲</u> ：1～19 文字。
Interface	1. 必須入力項目 2. デフォルト値： WAN 1	IPSec トンネルを確立するインターフェイスを選択します。これは、利用可能な WAN および LAN インターフェイスにすることができます。
Tunnel Scenario	1. 必須入力項目 2. デフォルト値：Site to site	アプリケーションのドロップダウンボックスから、IPSec トンネリングシナリオを選択します。Site-to-Site、Site-to-Host、Host-to-Site、または、Host-to-Host を選択します。LAN インターフェイスが選択されている場合は、Host-to-Host シナリオのみが利用可能です。 Site-to-Site、Site-to-Host、Host-to-Site、または IPSec は、トンネルモードでのみ動作します。それらの違いは、サブネットの数です。Host-to-Host では、IPSec は、転送モードで動作します。
Tunnel TCP MSS	1. 必須入力項目 2. デフォルト値： Auto	IPSec トラフィックの場合、項目は、自動的に TCP MSS を 3 方向ハンドシェイクで調整します。これは、VPN 外部インターフェイスで有効になっている [Adjust TCP MSS (TCP MSS の調整)] オプションに関係なく発生します。 <u>値の範囲</u> ：64～1500Bytes
Hub and Spoke	1. 任意の設定 2. デフォルト値： None	ドロップダウンボックスから選択して、ハブアンドスポーク IPsec VPN デプロイメントに対するゲートウェイを設定します。 デプロイメントで、ハブまたはスポークの暗号化がサポートされない場合は、None を選択します。 IPsec 設計におけるハブ役割に対して、Hub を選択します。 IPsec 設計におけるスポークの役割に対して、Spoke を選択します。 注：ハブおよびスポークは、トンネルシナリオで指定されたサイト間 VPN トンネリングでのみ使用できます。動的 VPN トンネリングアプリケーションでは使用できません。
Operation Mode	1. 必須入力項目 2. デフォルト値： Always on	IPSec トンネルの動作モードを定義します。Always on または Failover にすることができます。 このトンネルがフェールオーバートンネルとして設定されている場合は、フェールオーバー先のプライマリトンネルをさらに選択する必要があります。 注：Failover モードは、WAN が 1 つのゲートウェイでは使用できません。
Encapsulation Protocol	1. 必須入力項目 2. デフォルト値： ESP	この IPsec トンネルのドロップダウンボックスから、カプセル化プロトコルを選択します。 利用可能なカプセル化は ESP と AH です。

Local & Remote Configuration			
Item	Setting		
▶ Local Subnet List	ID	Subnet IP Address	Subnet Mask
	1	<input type="text" value="192.168.123.0"/>	<input type="text" value="255.255.255.0(/24)"/> ▼
	<input type="button" value="Delete"/>		
<input type="button" value="Add"/>			
▶ Redirect Traffic	<input type="checkbox"/> Enable		
▶ Full Tunnel	<input type="checkbox"/> Enable		
▶ Remote Subnet List	ID	Subnet IP Address	Subnet Mask
	1	<input type="text"/>	<input type="text" value="255.255.255.0(/24)"/> ▼
	<input type="button" value="Delete"/>		
<input type="button" value="Add"/>			
▶ Remote Gateway	<input type="text"/> (IP Address/FQDN)		

Local & Remote Configuration		
項目	値設定	説明
Local Subnet List	必須入力項目	<p>ローカルサブネット IP アドレスとサブネットマスクを指定します。</p> <p>Add または Delete ボタンをクリックして、ローカルサブネットを追加または削除します。</p> <p>注_1： Tunnel Scenario の Dynamic VPN オプションを選択すると、使用できるサブネットは 1 つだけになります。</p> <p>注_2： Tunnel Scenario の Host-to-Site または Host-to-Host オプションを選択すると、ローカルサブネットは使用できなくなります。</p> <p>注_3： Hub and Spoke の Hub and Spoke オプションを選択すると、使用できるサブネットは 1 つだけになります。</p>
Redirect Traffic	デフォルト値：チェックなし	<p>Enable ボックスにチェックを入れ、Redirect Traffic (トラフィックのリダイレクト) 機能を有効します。</p> <p>注： Redirect Traffic (トラフィックのリダイレクト) は、Tunnel Scenario (トンネルシナリオ) で指定された Host-to-Site (ホストからサイト) に対してのみ使用できます。デフォルトでは無効になっているため、ピアサブネットへの予期しない危険なアクセスを防ぐことができます。このような機能を有効にすると、VPN ホストの後にあるすべてのネットワークデバイス (実際には NAT ゲートウェイ) は、ホスト IP を使用してピアサブネットにアクセスできます。</p>

Full Tunnel	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れて、Full Tunnel を有効化します。 注： Full Tunnel は、Tunnel Scenario で Site-to-Site を指定した場合のみ使用できます。
Remote Subnet List	必須入力項目	リモートサブネット IP アドレスとサブネットマスクを指定します。Add または Delete ボタンをクリックして、Remote Subnet 設定を追加または削除します。
Remote Gateway	1. 必須入力項目。 2. フォーマットには、ipv4 アドレスまたは FQDN を使用することができます	リモートゲートウェイを指定します。

Authentication	
Item	Setting
▶ Key Management	IKE+Pre-shared Key ▼ <input type="text"/> (Min. 8 characters)
▶ Local ID	Type: User Name ▼ ID: <input type="text"/> (Optional)
▶ Remote ID	Type: User Name ▼ ID: <input type="text"/>

Authentication		
項目	値設定	説明
Key Management	1. 必須入力項目 2. 事前共有キー：8~32 文字。	ドロップダウンボックスから、この IPSec トンネルに対する Key Management を選択します。 IKE+Pre-shared Key：キー（8~32 文字）を設定する必要があります。 IKE+X.509：認証するための証明書が必要です。IKE + X.509 は、証明書が正しく設定されている場合にのみ使用できます。このマニュアルの「証明書」セクション、および、Web ベースユーティリティの Object Definition > Certificate を参照してください。 Manually：認証するためのキーIDを入力する必要があります。マニュアルによるキー設定については、後述の Manually Key Management のセクションで説明します。
Local ID	任意の設定	この IPSec トンネルを認証するローカル ID を指定します。 Local ID の User Name を選択し、ユーザー名を入力します。ユーザー名には数字を含めることはできません。 Local ID の FQDN を選択し、FQDN を入力します。 Local ID の User@FQDN を選択し、User@FQDN を入力します。

		Local ID の Key ID を選択し、キー ID（英字または数字）を入力します。
Remote ID	任意の設定	<p>この IPSec トンネルを認証するリモート ID を指定します。ユーザー名には数字を含めることはできませんが、すべてを数字にすることはできません。</p> <p>Local ID の FQDN を選択し、FQDN を入力します。</p> <p>Remote ID の User@FQDN を選択し、User@FQDN を入力します。</p> <p>Remote ID の Key ID を選択し、キー ID（英字または数字）を入力します。</p> <p>注： Tunnel Scenario の Dynamic VPN オプションを選択すると、Remote ID は、使用することができません。</p>

IKE Phase	
Item	Setting
▶ IKE Version	v1 ▼
▶ Negotiation Mode	Main Mode ▼
▶ X-Auth	None ▼ X-Auth Account (Optional) User Name : <input type="text"/> Password : <input type="text"/>
▶ Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable Timeout : <input type="text" value="180"/> (seconds) Delay : <input type="text" value="30"/> (seconds)
▶ Phase1 Key Life Time	<input type="text" value="3600"/> (seconds) (Max. 86400)

IKEPhase		
項目	値設定	説明
IKE Version	1. 必須入力項目 2. デフォルト値 : v1	この IPSec トンネルの IKE バージョンを指定します。v1 または v2 を選択します。注： Tunnel Scenario の Dynamic VPN オプションが選択されている場合、または、Encapsulation Protocol（カプセル化プロトコル）の AH オプションが選択されている場合、IKE バージョンは使用できません。
Negotiation Mode	デフォルト値 : Main Mode	この IPSec トンネルの Negotiation Mode を指定します。Main Mode または Aggressive Mode を選択します。
X-Auth	デフォルト値 : None	<p>この IPSec トンネルの X-Auth の役割を指定します。Server、Client、または、None を選択します。</p> <p>None が選択された場合：X-Auth 認証は不要です。</p> <p>Server が選択された場合：本製品は、X-Auth サーバーになります。X-Auth Account ボタンをクリックして、リモート X-Auth クライアントアカウントを作成します。</p>

		Client が選択された場合：本製品は、X-Auth クライアントになります。X-Auth サーバーゲートウェイによって認証されるユーザー名とパスワードを入力します。 注： Tunnel Scenario で、Dynamic VPN オプションを選択すると、X-Auth クライアントは使用できなくなります。
Dead Peer Detection (DPD)	1.デフォルト値： Enable にチェックあり Default Timeout：180 秒 Delay：30 秒	Enable チェックボックスにチェックを入れて、DPD 機能を有効化します。Timeout および Delay 時間を秒単位で指定します。 <u>値の範囲</u> ： Timeout, Delay 0～999 秒です。
Phase1 Key Life Time	1.必須入力項目 2. デフォルト値： 3600 秒 3.最大 86400 秒	Phase1 Key Life Time（フェーズ 1 キーライフタイム）を指定します。 <u>値の範囲</u> ： 30～86400。

IKE Proposal Definition				
ID	Encryption	Authentication	DH Group	Definition
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-auto ▼	MD5 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable

IKE Proposal Definition		
項目	値設定	説明
IKE Proposal Definition	必須入力項目	<p>Encryption：Phase 1 の暗号化方式を指定します。DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256 が選択範囲となります。</p> <p>Authentication：認証方法を指定します。None / MD5 / SHA1 / SHA2-256 が選択範囲となります。</p> <p>DH Group：DH Group を指定します。None/Group1 /Group2 /Group5 /Group14 /Group15 /Group16 /Group17 /Group18 が選択範囲となります。</p> <p>Enable チェックボックスにチェックを入れて、この設定を有効化します。</p>

IPSec Phase	
Item	Setting
▶ Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPSecPhase		
項目	値設定	説明
Phase2 Key Life Time	1.必須入力項目 2. デフォルト値 : 28800 秒 3.最大 86400 秒	Phase2 Key Life Time を指定します。 <u>値の範囲</u> : 30~86400。

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-auto ▼	MD5 ▼		<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable

IPSec Proposal Definition		
項目	値設定	説明
IPSec Proposal Definition	必須入力項目	<p>Encryption : Phase 2 の暗号化方式を指定します。これは、None / DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256 が選択範囲です。 注 : None は、カプセル化プロトコルが、AH として設定されている場合にのみ使用できます。ESP カプセル化には使用できません。</p> <p>Authentication : 認証方法を指定します。None / MD5 / SHA1 / SHA2-256 が選択範囲です。 注 : None および SHA2-256 は、Encapsulation Protocol (カプセル化プロトコル) が、ESP として設定されている場合にのみ使用できます。AH カプセル化には使用できません。</p> <p>PFS Group : PFS Group を指定します。None/Group1 /Group2 /Group5 /Group14 /Group15 /Group16 /Group17 /Group18 が選択範囲となります。</p> <p>Enable チェックボックスをクリックして、この設定を有効化します。</p>

Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします
Back	-	Back をクリックして、前ページに戻ります。

Manually Key Management

Authentication Configuration ウィンドウで説明した Key Management で、Manually オプションを選択すると、Manual IPsec Tunnel 設定用の一連の設定ウィンドウが表示されます。設定ウィンドウは、Local & Remote Configuration、Authentication、および、Manual Proposal です。

Authentication	
Item	Setting
▶ Key Management	Manually ▼
▶ Local ID	Type: KEY ID ▼ ID: <input type="text"/> (Optional)
▶ Remote ID	Type: KEY ID ▼ ID: <input type="text"/>

Authentication		
項目	値設定	説明
Key Management	必須入力項目	ドロップダウンボックスから、IPsec トンネルに対する Key Management を選択します。 本セクションでは、Manually オプションが選択されています。
Local ID	任意の設定	認証する IPsec トンネルのローカル ID を指定します。 Local ID の Key ID を選択し、キーID（英字または数字）を入力します。
Remote ID	任意の設定	認証する IPsec トンネルのリモート ID を指定します。 Remote ID の Key ID を選択し、キーID（英字または数字）を入力します。

Local & Remote Configuration	
Item	Setting
▶ Local Subnet	<input type="text"/>
▶ Local Netmask	<input type="text" value="255.255.255.0"/>
▶ Remote Subnet	<input type="text"/>
▶ Remote Netmask	<input type="text"/>
▶ Remote Gateway	<input type="text"/> (IP Address/FQDN)

Local & Remote Configuration

項目	値設定	説明
Local Subnet	必須入力項目	ローカルサブネット IP アドレスとサブネットマスクを指定します。
Local Netmask	必須入力項目	ローカルサブネットマスクを指定します。
Remote Subnet	必須入力項目	リモートサブネット IP アドレスを指定します。
Remote Netmask	必須入力項目	リモートサブネットマスクを指定します。
Remote Gateway	1. 必須入力項目 2. ipv4 アドレスまたは FQDN フォーマットです	リモートゲートウェイを指定します。

Manually Key Management の認証設定では、ローカル IPSec ピアとリモート IPSec ピアの両方でサポートされるサブネットは 1 つだけです。

Manual Proposal	
Item	Setting
▶ Outbound SPI	0x <input type="text"/>
▶ Inbound SPI	0x <input type="text"/>
▶ Encryption	DES ▼ <input type="text"/>
▶ Authentication	None ▼ <input type="text"/>

Manual Proposal		
項目	値設定	説明
Outbound SPI	16 進フォーマット	IPSec トンネルの送信 SPI を指定します。 <u>値の範囲</u> : 0~FFFF。
Inbound SPI	16 進フォーマット	IPSec トンネルの受信 SPI を指定します。 <u>値の範囲</u> : 0~FFFF。
Encryption	1. 必須入力項目 2. 16 進フォーマット	暗号化方式および暗号化キー指定します。 利用可能な暗号化方式は、DES / 3DES / AES-128 / AES-192 / AES-256 です。 DES のキーの長さは 16、3DES は 48、AES-128 は 32、AES-192 は 48、AES-256 は 64 です。 注： Encapsulation Protocol (カプセル化プロトコル) の AH オプションが選択されている場合、暗号化は使用できません。
Authentication	1. 必須入力項目 2. 16 進フォーマット	認証方法と認証キーを指定します。 利用可能な暗号化は、None / MD5 / SHA1 / SHA2-256 です。 MD5 のキー長は 32、SHA1 は 40、SHA2-256 は 64 です。 注： Encapsulation Protocol (カプセル化プロトコル) の AH オプションが選択されている場合、None オプションは使用できません。

Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします
Back	-	Back をクリックして、前ページに戻ります。

動的 VPN リストの作成/編集

Dynamic VPN List					
ID	Tunnel Name	Interface	Connected Client	Enable	Actions

サイト/ホスト/サイト/ホストシナリオ用の IPSec VPN トンネルを作成する場合と同様に、**Edit** ボタンをクリックされると、一連の設定ウィンドウが表示されます。**Tunnel Configuration**、**Local & Remote Configuration**、**Authentication**、**IKE Phase**、**IKE Proposal Definitio**、**IPSec Phase**、および **IPSec Proposal Definition** です。動的 VPN サーバーとして本製品のトンネルの詳細を設定する必要があります。

注：購入したゲートウェイの場合は、WAN インターフェイスごとに 1 つの動的 VPN サーバーを設定することができます。

Tunnel Configuration	
Item	Setting
▶ Tunnel	<input type="checkbox"/> Enable
▶ Tunnel Name	<input type="text" value="Dynamic IPSec1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ Tunnel Scenario	<input type="text" value="Dynamic VPN"/>
▶ Operation Mode	<input type="text" value="Always on"/>
▶ Encapsulation Protocol	<input type="text" value="ESP"/>

Tunnel Configuration		
項目	値設定	説明
Tunnel	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、動的 IPSec VPN トンネルを有効化します。
Tunnel Name	1. 必須入力項目 2. 文字列形式：任意のテキスト	トンネル名を入力します。 <u>値の範囲</u> ：1～19 文字。
Interface	1. 必須入力項目 2. デフォルト値： WAN 1	IPSec トンネルを確立する WAN インターフェイスを選択します。
Tunnel Scenario	1. 必須入力項目 2. デフォルト値：Dynamic VPN	IPSec トンネリングシナリオは、Dynamic VPN に固定されています。

Operation Mode	1. 必須入力項目 2. デフォルト値 Always on	利用可能な動作モードは、Always on です。Failover オプションは、動的 IPsec シナリオでは使用できません。
Encapsulation Protocol	1. 必須入力項目 2. デフォルト値： ESP	この IPsec トンネルのドロップダウンボックスから、カプセル化プロトコルを選択します。利用可能なカプセル化は、ESP と AH です。

Local & Remote Configuration	
Item	Setting
▶ Local Subnet	<input type="text"/>
▶ Local Netmask	<input type="text"/>

Local & Remote Configuration		
項目	値設定	説明
Local Subnet	必須入力項目	ローカルサブネット IP アドレスを指定します。
Local Netmask	必須入力項目	ローカルサブネットマスクを指定します。

Authentication	
Item	Setting
▶ Key Management	IKE+Pre-shared Key ▼ <input type="text"/> (Min. 8 characters)
▶ Local ID	Type: User Name ▼ ID: <input type="text"/> (Optional)
▶ Remote ID	Type: User Name ▼ ID: <input type="text"/>

Authentication		
項目	値設定	説明
Key Management	1. 必須入力項目 2. 事前共有キー： 8~32 文字。	ドロップダウンボックスから、IPsec トンネルに対する Key Management を選択します。 IKE+Pre-shared Key：キー（8~32 文字）を設定する必要があります。
Local ID	任意の設定	IPsec トンネルを認証するローカル ID を指定します。 Local ID の User Name を選択し、ユーザー名を入力します。ユーザー名には数字を含めることはできません。 Local ID の FQDN を選択し、FQDN を入力します。 Local ID の User@FQDN を選択し、User@FQDN を入力します。 Local ID の Key ID を選択し、キーID（英字または数字）を入力します。

Remote ID

任意の設定

認証する IPSec トンネルのリモート ID を指定します。
Remote ID の User Name を選択し、ユーザー名を入力します。
ユーザー名には数字を含めることはできませんが、すべてを数字にすることはできません。
Local ID の FQDN を選択し、FQDN を入力します。
Remote ID の User@FQDN を選択し、User@FQDN を入力します。
Remote ID の Key ID を選択し、キーID（英字または数字）を入力します。
注： Tunnel Scenario の Dynamic VPN オプションを選択すると、Remote ID は、使用することができません。

残りの **IKE Phase**、**IKE Proposal Definition**、**IPSec Phase**、および、**IPSec Proposal Definition** の設定については、前のセクションで説明した **IPSec Tunnel** の作成と同じです。関連する説明を参照してください。

5.1.2 OpenVPN

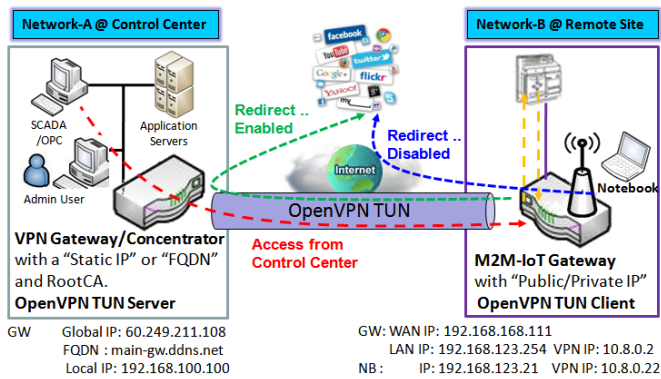
OpenVPN とは、ルーティングまたはブリッジ設定やリモートアクセス機能において、安全なポイントツーポイント接続またはサイトツーサイト接続を作成するための仮想プライベートネットワーク（VPN）技術を実装するアプリケーションです。これは、鍵交換のために SSL/TLS を利用するカスタムセキュリティプロトコルを使用します。ネットワークアドレストランスレータ（NAT）およびファイアウォールを通過することができます。

OpenVPN を使用すると、ピアは、静的キー（事前共有キー）または証明書を使って、互いを認証できます。マルチクライアントサーバー設定で使用すると、サーバーは署名および認証機関を使って、すべてのクライアントの認証証明書をリリースすることができます。これは、SSLv3/TLSv1 プロトコルだけでなく、OpenSSL 暗号化ライブラリも幅広く使用し、多くのセキュリティ機能と制御機能を備えています。

OpenVPN トンネリングとは、クライアントとサーバーベースのトンネリング技術です。OpenVPN サーバーには、静的 IP または FQDN があり、クライアントリストが維持されている必要があります。OpenVPN クライアントは、パブリック IP またはプライベート IP を有するモバイルユーザーまたはモバイルサイトであり、OpenVPN トンネル接続を要求することができます。この製品は、OpenVPN サーバーと OpenVPN クライアントの両方の機能をサポートし、さまざまなアプリケーション要件を満たします。

2 つの OpenVPN 接続シナリオがあります。TAP シナリオと TUN シナリオです。この製品は、レイヤ 3 ベースの IP トンネル（TUN）、または、あらゆるタイプのイーサネットトラフィックを伝送できるレイヤ 2 ベースのイーサネット TAP のいずれかを作成することができます。本製品をサーバーまたはクライアントとして設定することに加えて、どのタイプの OpenVPN 接続シナリオを採用するかを指定する必要があります。

OpenVPN TUN シナリオ

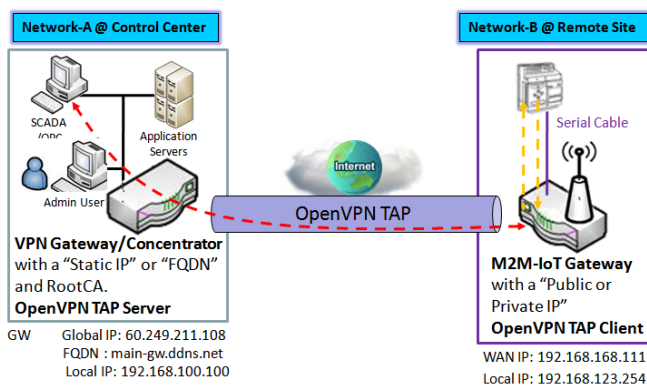


1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection established. (10.8.0.x is a virtual subnet)
3. Local networked device will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection (when NAT disabled & Redirect Internet Traffic enabled).
4. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 10.8.0.2.

用語「TUN」モードは、ルーティングモードと呼ばれ、レイヤ 3 パケットで動作します。ルーティングモードでは、VPN クライアントには、OpenVPN サーバーのローカル LAN とは異なるサブネット上の IP アドレスが与えられます。この仮想サブネットは、リモート VPN コンピュータに接続するために作成されます。ルーティングモードでは、OpenVPN サーバーは、ローカル LAN とは異なる独自の IP アドレスプールを持つ「TUN」インターフェイスを作成します。ダイヤルアップするリモートホストは、仮想ネットワーク内で IP アドレスを取得し、OpenVPN が存在するサーバーにのみアクセスすることができます。クライアントから VPN サーバーへのリモートアクセスを提供し、VPN サーバーでリモート LAN リソースへのアクセスを禁止する場合は、OpenVPN TUN モードが最も簡単なソリューションです。

図に示すように、M2M-IoT ゲートウェイは、OpenVPN TUN クライアントとして設定され、OpenVPN TUN サーバーに接続します。OpenVPN TUN 接続が確立すると、接続された TUN クライアントには、Control Center のローカルサブネットとは異なる仮想サブネットに属する仮想 IP (10.8.0.2) が割り当てられます。そのような接続では、インターネットトラフィックのリダイレクト設定が有効になっているときに、OpenVPN TUN 接続を経由すると、ローカルネットワークデバイスは仮想 IP 10.8.0.x を取得します。また、コントロールセンターの SCADA サーバーは、仮想 IP アドレス (10.8.0.2) を持つリモート接続のシリアルデバイスにアクセスすることができます。

OpenVPN TAP シナリオ



1. M2M-IoT Gateway (as OpenVPN TAP Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TAP Server).
2. M2M-IoT Gateway will be assigned 192.168.100.210 IP Address after OpenVPN TAP Connection established. (same subnet as in Control Center)
3. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 192.168.100.210.

用語「TAP」はブリッジモードと呼ばれ、レイヤ 2 パケットで動作します。ブリッジモードでは、VPN クライアントには、OpenVPN サーバーの下にある LAN と同じサブネット上の IP アドレスが与えられます。このような設定では、OpenVPN クライアントは、LAN 内のリソースに直接アクセスできます。VPN クライアント用のリモート LAN 全体へのリモートアクセスを提供する場合は、OpenVPN を「TAP」ブリッジモードで設定する必要があります。

図に示すように、M2M-IoT ゲートウェイは、OpenVPN TAP クライアントとして設定され、OpenVPN TAP サーバーに接続します。OpenVPN TAP 接続が確立すると、接続された TAP クライアントには、コントロールセンターのローカルサブネットと同じサブネットである仮想 IP (192.168.100.210) が割り当てられます。このような接続により、コントロールセンターの SCADA サーバーは、仮想 IP アドレス (192.168.100.210) を持つリモート接続シリアルデバイスにアクセスすることができます。

Open VPN 設定

Security > VPN > OpenVPN タブに進みます。

OpenVPN 設定により、OpenVPN トンネルを作成および設定することができます。

OpenVPN の有効化

OpenVPN を有効化し、ゲートウェイが動作するために必要なサーバーまたはクライアントの設定を選択します。

Configuration	
Item	Setting
▶ OpenVPN	<input type="checkbox"/> Enable
▶ Server / Client	Server ▼

Configuration		
項目	値設定	説明
OpenVPN	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、OpenVPN 機能を有効化します。
Server/Client	デフォルト値：Server	Server が選択されると、示された名前として、さらに設定するためにサーバー設定が以下に表示されます。 Client が選択されると、別のクライアント設定ウィンドウでクライアント設定を指定することができます。

OpenVPN サーバー

Server を選択すると、**OpenVPN Server Configuration** ウィンドウが表示されます。**OpenVPN Server Configuration** ウィンドウでは、OpenVPN サーバー機能を有効にしたり、OpenVPN サーバーの仮想 IP アドレスを指定したり、リモート OpenVPN クライアントがダイヤルアップするとき、認証プロトコルを指定することができます。

OpenVPN Server Configuration	
Item	Setting
▶ OpenVPN Server	<input checked="" type="checkbox"/> Enable
▶ Protocol	TCP ▼
▶ Port	4430
▶ Tunnel Scenario	TUN ▼
▶ Authorization Mode	Static Key ▼
▶ Local Endpoint IP Address	
▶ Remote Endpoint IP Address	
▶ Static Key	
▶ Server Virtual IP	10.8.0.0
▶ DHCP-Proxy Mode	<input checked="" type="checkbox"/> Enable
▶ IP Pool	Starting Address: <input type="text"/> ~ Ending Address: <input type="text"/>
▶ Gateway	<input type="text"/>
▶ Netmask	255.255.255.0(/24) ▼
▶ Redirect Default Gateway	<input type="checkbox"/> Enable
▶ Encryption Cipher	Blowfish ▼
▶ Hash Algorithm	SHA-1 ▼
▶ LZO Compression	Adaptive ▼
▶ Persist Key	<input checked="" type="checkbox"/> Enable
▶ Persist Tun	<input checked="" type="checkbox"/> Enable
▶ Advanced Configuration	Edit

OpenVPN Server Configuration		
項目	値設定	説明
OpenVPN Server	デフォルト値：チェックなし	Enable をクリックして、OpenVPN サーバー機能を有効にします。
Protocol	1. 必須入力項目 2. デフォルト値： TCP	OpenVPN サーバーに接続するために選択したプロトコルを定義します。 TCP または UDP を選択します。-> TCP プロトコルは OpenVPN サーバーへのアクセスに使用され、 Port は 4430 として自動的に設定されます。 UDP を選択します。-> UDP プロトコルは OpenVPN サーバーへのアクセスに使用され、 Port は 1194 として自動的に設定されます。
Port	1. 必須入力項目 2. デフォルト値： 4430	OpenVPNサーバーに接続するためのポートを指定します。 値の範囲：1～65535。
Tunnel Scenario	1. 必須入力項目 2. デフォルト値： TUN	OpenVPNサーバーに接続するためのトンネルシナリオを指定します。TUNトンネルシナリオでは TUN 、TAPトンネルシナリオでは TAP になります。
Authorization Mode	1. 必須入力項目 2. デフォルト値： TLS	OpenVPNサーバーの認証モードを指定します。 <ul style="list-style-type: none"> • TLS -> OpenVPN は、TLS 認証モード、および、以下の項目 CA Cert. (CA 証明書)、Server Cert. (サーバー証明書) を使用します。そして、DH PEM が表示されます。 CA Cert. (CA 証明書) が、Certificate (証明書) で生成される可能性があります。Object Definition > Certificate > Trusted Certificate を参照してください。 Server Cert. が、Certificate (証明書) で生成される可能性があります。Object Definition > Certificate > My Certificate を参照してください。 • Static Key -> OpenVPN は、静的キー (事前共有) 認証モードを使用し、Local Endpoint IP Address、Remote Endpoint IP Address、および、Static Key の項目が表示されます。 注：Static Key は、Tunnel Scenario で、TUN が選択されている場合にのみ利用可能です。
Local Endpoint IP Address	必須入力項目	OpenVPN ゲートウェイの仮想ローカルエンドポイント IP アドレスを指定します。 値の範囲：IPフォーマットは10.8.0.x、xの範囲は1～254です。 注： Authorization Mode で、 Static Key が選択されている場合にのみ利用可能です。

Remote Endpoint IP Address	必須入力項目	ピア OpenVPN ゲートウェイの仮想リモートエンドポイント IP アドレスを指定します。 値の範囲 ： IPフォーマットは10.8.0.x、xの範囲は1～254です。 注： Authorization Mode で、 Static Key が選択されている場合にのみ利用可能です。
Static Key	必須入力項目	静的キーを指定します。 注： Authorization Mode で、 Static Key が選択されている場合にのみ利用可能です。
Server Virtual IP	必須入力項目	サーバー仮想IPを指定します。 値の範囲 ： IPフォーマットは10.y.0.0、yの範囲は1～254です。 注： Authorization Mode で、 TLS が選択されている場合にのみ利用可能です。
DHCP-Proxy Mode	1.必須入力項目 2. デフォルト値：チェックあり	Enable チェックボックスにチェックを入れ、DHCP-プロキシモードを有効化します。 注： Tunnel Device で、 TAP が選択されている場合にのみ利用可能です。
IP Pool	必須入力項目	OpenVPN サーバーの仮想 IP プール設定を指定します。OpenVPN クライアントの IP アドレスプールとして、 Starting Address （開始アドレス）と Ending Address （終了アドレス）を指定する必要があります。 注： Tunnel Device で TAP が選択され、 DHCP-Proxy Mode がオフの場合にのみ使用できます。
Gateway	必須入力項目	OpenVPNサーバーのゲートウェイ設定を指定します。これは、接続されたOpenVPNクライアントに割り当てられます。 注： Tunnel Device で TAP が選択され、 DHCP-Proxy Mode がオフの場合にのみ使用できます。
Netmask	デフォルト値： select one	OpenVPNサーバーのネットマスク設定を指定します。これは、接続されたOpenVPNクライアントに割り当てられます。 値の範囲 ： 255.255.255.0/24（クラスCのみをサポート） 注_1： Netmask Tunnel Device で TAP が選択され、 DHCP-Proxy Mode がオフの場合に使用できます。 注_2： また、 Tunnel Device で、 TUN が選択されている場合に利用可能です。
Redirect Default Gateway	1.任意入力項目。 2. デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、リダイレクトデフォルトゲートウェイ機能を有効化します。
Encryption Cipher	1.必須入力項目 2. デフォルト値： Blowfish	ドロップダウンリストから、暗号化アルゴリズムを指定します。これは、 Blowfish/AES-256/AES-192/AES-128/None から選択可能です。
Hash Algorithm	デフォルト値： SHA-1	ドロップダウンリストから、ハッシュアルゴリズムを指定します。

		これは、SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable から選択可能です。
LZO Compression	デフォルト値： Adaptive	LZO 圧縮方法を指定します。 これは、 Adaptive/YES/NO/Default から選択可能です。
Persis Key	1.任意入力項目。 2. デフォルト値：チェックあり	Enable チェックボックスにチェックを入れ、Persisキー機能を有効化します。
Persis Tun	1.任意入力項目。 2. デフォルト値：チェックあり	Enable チェックボックスにチェックを入れ、 Persis Tun 機能を有効化します。
Advanced Configuration	-	Edit ボタンをクリックして、OpenVPNサーバーの詳細設定を設定します。 ボタンをクリックすると、下に Advanced Configuration が表示されます。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、変更をキャンセルします。

Advanced Configuration が選択されると、OpenVPN Server Advanced Configuration ウィンドウが表示されます。

OpenVPN Server Advanced Configuration	
Item	Setting
▶ TLS Cipher	None <input type="button" value="v"/>
▶ TLS Auth. Key	<input type="text"/> (Optional) <input type="button" value="v"/>
▶ Client to Client	<input checked="" type="checkbox"/> Enable
▶ Duplicate CN	<input checked="" type="checkbox"/> Enable
▶ Tunnel MTU	1500 <input type="text"/>
▶ Tunnel UDP Fragment	0 <input type="text"/>
▶ Tunnel UDP MSS-Fix	<input type="checkbox"/> Enable
▶ CCD-Dir Default File	<input type="text"/> <input type="button" value="v"/>
▶ Client Connection Script	<input type="text"/> <input type="button" value="v"/>
▶ Additional Configuration	<input type="text"/> <input type="button" value="v"/>

OpenVPN Server Advanced Configuration		
項目	値設定	説明
TLS Cipher	1. 必須入力項目 2. デフォルト値： None	ドロップダウンリストから、TLS 暗号化アルゴリズムを指定します。 これは、 None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SH が選択可能です。 注： Authorization Mode で、 TLS が選択されている場合にのみ利用可能です。
TLS Auth.Key (TLS 認証キー)	1. 任意入力項目。 2. 文字列形式：任意のテキスト	TLS認証キーを指定します。 注： Authorization Mode で、 TLS が選択されている場合にのみ利用可能です。
Client to Client	デフォルト値：チェックあり	Enable チェックボックスにチェックを入れ、異なる OpenVPN クライアント間のトラフィックを有効化します。 注： Authorization Mode で、 TLS が選択されている場合にのみ利用可能です。
Duplicate CN	デフォルト値：チェックあり	Enable チェックボックスにチェックを入れ、CNの複製機能を有効化します。 注： Authorization Mod で、 TLS が選択されている場合にのみ利用可能です。
Tunnel MTU	1. 必須入力項目 2. デフォルト値： 1500	トンネルMTUを指定します。 値の範囲：0～1500。
Tunnel UDP Fragment	1. 必須入力項目 2. デフォルト値：0	トンネルUDPフラグメントを指定します。 値の範囲：0～1500。 注： Protocol で UDP が選択されている場合にのみ利用可能です。
Tunnel UDP MSS-Fix	1. 任意入力項目。 2. デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、トンネルUDP MSS-Fix機能を有効化します。 注： Protocol で UDP が選択されている場合にのみ利用可能です。
CCD-Dir Default File	1. 任意入力項目。 2. 文字列形式：任意のテキスト	CCD-Dirデフォルトファイルを指定します。 値の範囲：0～256文字。
Client Connection Script	1. 任意入力項目。 2. 文字列形式：任意のテキスト	クライアント接続スクリプトを指定します。 値の範囲：0～256文字。
Additional Configuration	1. 任意入力項目。 2. 文字列形式：任意のテキスト	追加設定を指定します。 値の範囲：0～256文字。

OpenVPN クライアント

Client を選択すると、OpenVPN Client List ウィンドウが表示されます。

OpenVPN Client List Add Delete														
ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	NAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions

Add ボタンがクリックされると、OpenVPN Client Configuration ウィンドウが表示されます。OpenVPN Client Configuration ウィンドウにより、「OpenVPN Client Name」、「Interface」、「Protocol」、「Tunnel Scenario」、「Remote IP/FQDN」、「Remote Subnet」、「Authorization Mode」、「Encryption Cipher」、「Hash Algorithm」およびトンネルアクティベーションなどの OpenVPN クライアントに必要なパラメータを指定することができます。

OpenVPN Client Configuration	
Item	Setting
▶ OpenVPN Client Name	<input type="text" value="OpenVPN Client #1"/>
▶ Interface	<input type="text" value="WAN 1"/>
▶ Protocol	<input type="text" value="TCP"/> Port: <input type="text" value="443"/>
▶ Tunnel Scenario	<input type="text" value="TUN"/>
▶ Remote IP/FQDN	<input type="text"/>
▶ Remote Subnet	<input type="checkbox"/> Enable <input type="text" value="255.255.255.0"/> <input type="text" value="(24)"/>
▶ Redirect Internet Traffic	<input type="checkbox"/> Enable
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Authorization Mode	<input type="text" value="TLS"/> CA Cert.: <input type="text"/> Client Cert.: <input type="text"/> Client Key.: <input type="text"/> Please set the Certificate.
▶ Encryption Cipher	<input type="text" value="Blowfish"/>
▶ Hash Algorithm	<input type="text" value="SHA-1"/>
▶ LZO Compression	<input type="text" value="Adaptive"/>
▶ Persist Key	<input checked="" type="checkbox"/> Enable
▶ Persist Tun	<input checked="" type="checkbox"/> Enable
▶ Advanced Configuration	<input type="button" value="Edit"/>
▶ Tunnel	<input type="checkbox"/> Enable

OpenVPN Client Configuration

項目	値設定	説明
OpenVPN Client Name	必須入力項目	OpenVPN クライアント名は、トンネルリスト内のクライアントを識別するために使用されます。 値の範囲 ： 1～32 文字。
Interface	1.必須入力項目 2.デフォルト値： WAN-1	OpenVPN クライアントトンネルに使用する物理インターフェイスを定義します。
Protocol	1.必須入力項目 2.デフォルト値： TCP	OpenVPN クライアントのプロトコルを定義します。 TCP を選択します。-> OpenVPN は、TCP プロトコルを使用し、 Port は 443 として自動的に設定されます。 UDP を選択します。-> OpenVPN は、UDP プロトコルを使用し、 Port は自動的に 1194 として設定されます。
Port	1.必須入力項目 2. デフォルト値： 443	使用するOpenVPNクライアントの Port を指定します。 値の範囲 ： 1～65535。
Tunnel Scenario	1.必須入力項目 2. デフォルト値： TUN	OpenVPNクライアントが使用するトンネルシナリオのタイプを指定します。TUNトンネルシナリオでは TUN 、TAPトンネルシナリオでは TAP になります。
Remote IP/FQDN	必須入力項目	OpenVPN クライアントトンネルのピア OpenVPN サーバーのリモート IP/FQDN を指定します。 IP アドレスまたは FQDN を入力します。
Remote Subnet	1.必須入力項目 2.デフォルト値： チェックなし	Enable チェックボックスにチェックを入れ、リモートサブネット機能を有効化します。 OpenVPNクライアントトンネルのピアOpenVPNサーバーのリモートサブネットを指定します。 リモートサブネットアドレスとリモートサブネットマスクを入力します。
Redirect Internet Traffic	1.任意入力項目。 2.デフォルト値： チェックなし	Enable チェックボックスにチェックを入れ、リダイレクトインターネットトラフィック機能を有効化します。
NAT	1.任意入力項目。 2.デフォルト値： チェックなし	Enable チェックボックスにチェックを入れ、 NAT 機能を有効化します。
Authorization Mode	1.必須入力項目 2. デフォルト値： TLS	OpenVPNサーバーの認証モードを指定します。 <ul style="list-style-type: none"> • TLS -> OpenVPNは、TLS認証モード、および、以下の項目CA Cert. (CA証明書)、Client Cert. (クライアント証明書)を使用します。そして、Client Keyが表示されます。 <p>CA Cert. (CA証明書) は、Trusted CA Certificate Listで選択することができます。Object Definition > Certificate > Trusted Certificateを参照してください。</p> <p>Client Cert. (クライアント証明書) は、Local Certificate Listで</p>

		<p>選択することができます。 Object Definition > Certificate > My Certificateを参照してください。</p> <p>Client Keyで、 Client Keyを選択することができます。 Object Definition > Certificate > Trusted Certificateを参照してください。</p> <ul style="list-style-type: none"> • Static Key <p>-> OpenVPN は、静的キー認証モードを使用し、 Local Endpoint IP Address、 Remote Endpoint IP Address、 および、 Static Key の項目が表示されます。</p>
Local Endpoint IP Address	必須入力項目	<p>OpenVPN ゲートウェイの仮想ローカルエンドポイント IP アドレスを指定します。</p> <p>値の範囲: IPフォーマットは10.8.0.x、 xの範囲は1~254です。</p> <p>注: Authorization Mode で、 Static Key が選択されている場合にのみ利用可能です。</p>
Remote Endpoint IP Address	必須入力項目	<p>ピア OpenVPN ゲートウェイの仮想リモートエンドポイント IP アドレスを指定します。</p> <p>値の範囲: IPフォーマットは10.8.0.x、 xの範囲は1~254です。</p> <p>注: Authorization Mode で、 Static Key が選択されている場合にのみ利用可能です。</p>
Static Key	必須入力項目	<p>静的キーを指定します。</p> <p>注: Authorization Mode で、 Static Key が選択されている場合にのみ利用可能です。</p>
Encryption Cipher	デフォルト値: Blowfish	<p>暗号化アルゴリズムを指定します。</p> <p>これは、 Blowfish/AES-256/AES-192/AES-128/None から選択可能です。</p>
Hash Algorithm	デフォルト値: SHA-1	<p>ハッシュアルゴリズムを指定します。</p> <p>これは、 SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable から選択可能です。</p>
LZO Compression	デフォルト値: Adaptive	<p>LZO 圧縮方法を指定します。</p> <p>これは、 Adaptive/YES/NO/Default から選択可能です。</p>
Persis Key	1.任意入力項目。 2.デフォルト値: チェックあり	<p>Enable チェックボックスにチェックを入れ、 Persis キー機能を有効化します。</p>
Persis Tun	1.任意入力項目。 2.デフォルト値: チェックあり	<p>Enable チェックボックスにチェックを入れ、 Persis Tun 機能を有効化します。</p>
Advanced Configuration	-	<p>Edit ボタンをクリックして、 OpenVPN サーバーの詳細を設定します。</p> <p>ボタンをクリックすると、下に Advanced Configuration が表示されます。</p>
Tunnel	デフォルト値: チェックなし	<p>Enable チェックボックスにチェックを入れ、 OpenVPN トンネルを有効化します。</p>
Save	-	<p>Save をクリックして、設定を保存します。</p>

Undo	-	Undo をクリックして、変更をキャンセルします。
Back	-	Back をクリックして、最後のページに戻ります。

Advanced Configuration が選択されると、OpenVPN Client Advanced Configuration ウィンドウが表示されます。

OpenVPN Client Advanced Configuration	
Item	Setting
▶ TLS Cipher	None ▼
▶ TLS Auth. Key(Optional)	<input type="text"/> (Optional)
▶ User Name(Optional)	<input type="text"/> (Optional)
▶ Password(Optional)	<input type="text"/> (Optional)
▶ Bridge TAP to	VLAN 1 ▼
▶ Firewall Protection	<input type="checkbox"/> Enable
▶ Client IP Address	Dynamic IP ▼
▶ Tunnel MTU	<input type="text" value="1500"/>
▶ Tunnel UDP Fragment	<input type="text" value="1500"/>
▶ Tunnel UDP MSS-Fix	<input type="checkbox"/> Enable
▶ nsCertType Verification	<input type="checkbox"/> Enable
▶ TLS Renegotiation Time(seconds)	<input type="text" value="3600"/> (seconds)
▶ Connection Retry(seconds)	<input type="text" value="-1"/> (seconds)
▶ DNS	Automatically ▼
▶ Additional Configuration	<input type="text"/>

OpenVPN 詳細クライアント設定

項目	値設定	説明
TLS Cipher	1. 必須入力項目 2. デフォルト値 : None	ドロップダウンリストから、TLS 暗号化アルゴリズムを指定します。 これは、None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA から選択可能です。 注： Authorization Mode で、TLS が選択されている場合にのみ利用可能です。
TLS Auth.Key	1. 任意入力項目。 2. 文字列形式：任意のテキスト	TLS Auth.OpenVPNサーバーに接続するためのキー（サーバーが必要な場合）。 注： Authorization Mode で、TLS が選択されている場合にのみ利用可能です。

User Name	任意入力項目。	サーバーが必要な場合、OpenVPNサーバーに接続するための User account を入力します。 注： Authorization Mode で、 TLS が選択されている場合にのみ利用可能です。
Password	任意入力項目。	サーバーが必要な場合、OpenVPNサーバーに接続するためのパスワードを入力します。 注： Authorization Mode で、 TLS が選択されている場合にのみ利用可能です。
Bridge TAP to	デフォルト値： VLAN 1	TAPインターフェイスを特定のローカルネットワークインターフェイスまたはVLANにブリッジするには、「 Bridge TAP to 」の設定を指定します。 注： Tunnel Scenario でTAPが選択され、 NAT がチェックされていない場合にのみ利用可能です。
Firewall Protection	デフォルト値：チェックなし	チェックボックスにチェックを入れ、ファイアウォール保護機能を有効化します。 注： NAT が有効な場合にのみ利用可能です。
Client IP Address	デフォルト値： Dynamic IP	OpenVPNクライアントの仮想IPアドレスを指定します。 Client IP Address
Tunnel MTU	1. 必須入力項目 2. デフォルト値： 1500	トンネルMTUの値を指定します。 値の範囲 ： 0～1500。
Tunnel UDP Fragment	デフォルト値： 1500	トンネルUDPフラグメントの値を指定します。 値の範囲 ： 0～1500。 注： Protocol で UDP が選択されている場合にのみ利用可能です。
Tunnel UDP MSS-Fix	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、トンネルUDP MSS-Fix機能を有効化します。 注： Protocol で UDP が選択されている場合にのみ利用可能です。
nsCerType Verification	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、nsCerType検機能を有効化します。 注： Authorization Mode で、 TLS が選択されている場合にのみ利用可能です。
TLS Renegotiation Time (seconds)	デフォルト値： 3600	TLS再ネゴシエーション時間の時間間隔を指定します。 値の範囲 ： -1～86400。
Connection Retry(seconds)	デフォルト値：-1	接続再試行の時間間隔を指定します。 デフォルトの-1は、接続再試行を実行する必要がないことを意味します。 値の範囲 ： -1～86400。-1は、再試行の必要がないことを意味します。
DNS	デフォルト値： Automatically	DNS の設定を指定します。 これは、 Automatically / Manually から選択可能です。
Addition Configuration	任意の設定	オプションの設定文字列をここに入力します。最大256文字まで入力できます。 値の範囲 ： 1～32文字。

5.1.3 L2TP

Configuration [Help]	
Item	Setting
▶ L2TP	<input type="checkbox"/> Enable
▶ Client/Server	Server ▼

L2TP Server Configuration	
Item	Setting
▶ L2TP Server	<input type="checkbox"/> Enable
▶ Interface	All WANs ▼
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key <input type="text" value=""/> (Min. 8 characters)
▶ Server Virtual IP	<input type="text" value="192.168.10.1"/>
▶ IP Pool Starting Address	<input type="text" value="10"/>
▶ IP Pool Ending Address	<input type="text" value="17"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable <input type="text" value="40 bits"/> ▼
▶ Service Port	<input type="text" value="1701"/>

L2TP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

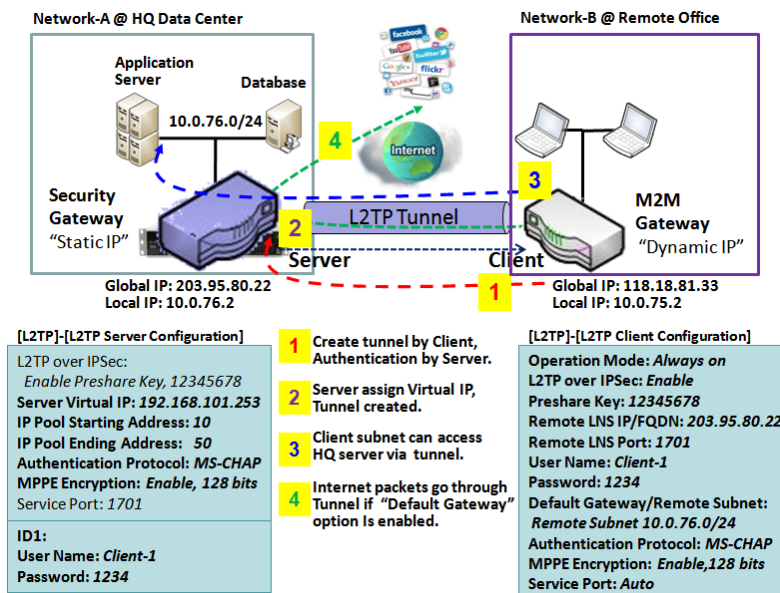
User Account List Add <input type="button" value="Delete"/>				
ID	User Name	Password	Enable	Actions

L2TP（レイヤー2 トンネリングプロトコル）とは、仮想プライベートネットワーク（VPN）をサポートするためのトンネリングプロトコルで、ISP のサービスの一環として提供されることもあります。これ自体には暗号化や機密保持機能はありません。トンネル内を通過する暗号化プロトコルによりプライバシーを実現しています。このゲートウェイは、同時に L2TP サーバーと L2TP クライアントの動作を行います。

L2TP Server（L2TP サーバー）：クライアントが、L2TP トンネルを作成するには、静的 IP または FQDN が必要です。また、クライアントログイン認証用の「ユーザーアカウントリスト」（ユーザー名/パスワード）も保持します。接続された各 L2TP クライアントに仮想 IP を割り当てるための仮想 IP プールがあります。

L2TP Client（L2TP クライアント）：これは、動的 IP を備えたりリモートオフィス内のモバイルユーザーまたはゲートウェイです。トンネルを設定するには、「ユーザー名」、「パスワード」、および、サーバーのグローバル IP を取得する必要があります。さらに、メイン接続としての各トンネルの動作モード、別のトンネル

のフェールオーバー、または、負荷バランストンネルを識別して全体の帯域幅を増やす必要があります。パケットフローのために「Default Gateway（デフォルトゲートウェイ）」または「Remote Subnet（リモートサブネット）」を決定する必要があります。さらに、「Default Gateway（デフォルトゲートウェイ） / Remote Subnet リモートサブネット）」パラメータで、L2TP トンネルを通過するトラフィックの種類を定義することもできます。



「Default Gateway（デフォルトゲートウェイ）/Remote Subnet（リモートサブネット）」設定項目には、「Default Gateway（デフォルトゲートウェイ）」と「Remote Subnet（リモートサブネット）」という2つのオプションがあります。「Remote Subnet（リモートサブネット）」を選択すると、リモートサブネットというもう1つの設定を指定する必要があります。これは、L2TP VPN サーバーのイントラネット用です。したがって、L2TP クライアントピアでは、宛先が専用サブネット内にあるパケットは、L2TP VPN トンネル経由で転送されます。その他は、L2TP クライアントピアのセキュリティゲートウェイの現在のルーティングポリシーに基づいて転送されます。しかし、L2TP クライアント

ピアの「Default Gateway（デフォルトゲートウェイ）」オプションを選択すると、L2TP クライアントピアのインターネットアクセスを含むすべてのパケットが、確立された L2TP VPN トンネルを通過します。つまり、リモート L2TP VPN サーバーは、L2TP クライアントピアからのパケットフローを制御します。確かに、これらのパケットは L2TP VPN トンネルを経由します。

L2TP 設定

Security > VPN > L2TP タブに進みます。

L2TP 設定により、L2TP トンネルを作成および設定することができます。

L2TP の有効化

Configuration [Help]	
Item	Setting
▶ L2TP	<input type="checkbox"/> Enable
▶ Client/Server	Server ▼

Configuration 項目	値設定	説明
L2TP	デフォルト値：チェックなし	Enable チェックボックスをクリックし、L2TP 機能を有効化します。
Client/Server	必須入力項目	L2TP の役割を指定します。ゲートウェイが使用する Server または Client の役割を選択します。以下は、L2TP サーバーとクライアントの設定ウィンドウです。
Save	-	Save ボタンをクリックして、設定を保存します。

L2TP サーバー

Client/Server で **Server** を選択すると、L2TP サーバー設定が表示されます。

L2TP Server Configuration	
Item	Setting
▶ L2TP Server	<input type="checkbox"/> Enable
▶ Interface	All WANs ▼
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key <input type="text"/> (Min. 8 characters)
▶ Server Virtual IP	<input type="text" value="192.168.10.1"/>
▶ IP Pool Starting Address	<input type="text" value="10"/>
▶ IP Pool Ending Address	<input type="text" value="17"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable <input type="text" value="40 bits"/> ▼
▶ Service Port	<input type="text" value="1701"/>

L2TP Server Configuration		
項目	値設定	説明
L2TP Server	デフォルト値：チェックなし	Enable チェックボックスをクリックすると、L2TP サーバーが有効化されます
Interface	1.必須入力項目 2.デフォルト値：ALL WANs	選択したインターフェイスをこの L2TP トンネルに使用するように定義します。
L2TP over IPsec	デフォルト値：チェックなし	Enable チェックボックスをクリックすると、L2TP over IPsec が有効になり、Pre-shared Key（事前共有キー）（8～31 文字）を入力する必要があります。
Server Virtual IP	必須入力項目	L2TP サーバー仮想 IP を指定します。 L2TP サーバーローカル仮想 IP として設定されます
IP Pool Starting Address	必須入力項目	仮想 IP プールの L2TP サーバー開始 IP を指定します。L2TP クライアントに割り当てる開始 IP として設定されます。 値の範囲 ： <u>1～8</u> 。
IP Pool Ending Address	必須入力項目	仮想 IP プールの L2TP サーバー終了 IP を指定します。L2TP クライアントに割り当てる終了 IP として設定されます。 値の範囲 ： <u>1～8</u> 。
Authentication Protocol	必須入力項目	L2TP クライアントを認証する L2TP サーバーに対して、単一または複数の認証プロトコルを選択します。利用可能な認証プロトコルは、PAP / CHAP / MS-CHAP / MS-CHAP v2 です。
MPPE Encryption	必須入力項目	MPPE プロトコルをサポートするかどうかを指定します。 Enable チェックボックスをクリックして、MPPE を有効にし、ドロップダウンボックスから、40 ビット / 56 ビット / 128 ビットを選択します。 注：MPPE Encryption が有効になっている場合、Authentication Protocol の PAP/CHAP オプションは使用できません。
Service Port	必須入力項目	L2TP サーバーが使用するサービスポートを指定します。 値の範囲 ： <u>1～65535</u> 。
Save	-	Save ボタンをクリックして、設定を保存します
Undo	-	Undo ボタンをクリックして、設定を回復します。

L2TP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

L2TP Server Status		
項目	値設定	説明
L2TP Server Status	-	接続されている L2TP クライアントの User Name（ユーザー名）、Remote IP（リモート IP）、Remote Virtual IP（リモート仮想 IP）、および、Remote Call ID（リモートコール ID）が表示されます。

Refresh ボタンをクリックして、L2TP クライアント情報を更新します。

User Account List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	User Name	Password	Enable	Actions
User Account Configuration				
User Name		Password		Account
<input type="text"/>		<input type="text"/>		<input type="checkbox"/> Enable
<input type="button" value="Save"/>				

User Account Configuration		
項目	値設定	説明
User Account List	最大 10 のユーザーアカウント	<p>これは、L2TP 認証ユーザーアカウントエントリです。リモートクライアントのアカウントを作成および追加して、ゲートウェイデバイスへの L2TP VPN 接続を確立することができます。</p> <p>Add ボタンをクリックして、ユーザーアカウントを追加します。ユーザー名とパスワードを入力します。次に、Enable チェックボックスにチェックを入れて、ユーザーを有効化します。</p> <p>Save ボタンをクリックして、新規ユーザーアカウントを保存します。</p> <p>選択したユーザーアカウントは、Delete ボタンをクリックすると完全に削除できます。</p> <p><u>値の範囲</u> : 1~32 文字。</p>

L2TP クライアント

Client/Server で Client を選択すると、一連の L2TP Client Configuration ウィンドウが表示されます。

Configuration [Help]	
Item	Setting
▶ L2TP	<input checked="" type="checkbox"/> Enable
▶ Client/Server	Server ▼

L2TP クライアントの作成/編集

L2TP Client List & Status <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>								
ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status	Enable	Actions

Add/Edit ボタンがクリックされると、一連の設定ウィンドウが表示されます。

L2TP Client Configuration	
Item	Setting
▶ Tunnel Name	<input type="text" value="L2TP #1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ Operation Mode	<input type="text" value="Always on"/>
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key <input type="text"/> (Min. 8 characters)
▶ Remote LNS IP/FQDN	<input type="text"/>
▶ Remote LNS Port	<input type="text" value="1701"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Tunneling Password (Optional)	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable
▶ LCP Echo Type	<input type="text" value="Auto"/> Interval <input type="text" value="30"/> seconds Max. Failure Time <input type="text" value="6"/> times
▶ Service Port	<input type="text" value="Auto"/> <input type="text" value="0"/>
▶ Tunnel	<input type="checkbox"/> Enable

L2TP Client List & Status L2TP Client Configuration

項目	値設定	説明
Tunnel Name	必須入力項目	トンネル名を入力します。 <u>値の範囲</u> ： 1～32 文字。
Interface	必須入力項目	選択したインターフェイスを L2TP トンネルに使用するよう定義します。

		(WAN1 は、WAN1 インターフェイスが有効な場合のみ利用可能です)
Operation Mode	1. 必須入力項目 2. デフォルト値： Always on	L2TP トンネルの動作モードを定義します。Always on または Failover にすることができます。 このトンネルがフェールオーバートンネルとして設定されている場合は、フェールオーバー先のプライマリトンネルをさらに選択する必要があります。 注：Failover モードは、WAN が 1 つのゲートウェイでは使用できません。
L2TP over IPSec	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、L2TP over IPSec を有効化し、さらに、Pre-shared Key (事前共有キー) (8~31 文字) を指定します。
Remote LNS IP/FQDN	必須入力項目	L2TP サーバーのパブリック IP アドレスまたは FQDN を入力します。
Remote LNS Port	1. 必須入力項目 2. デフォルト値： 1701	L2TP トンネルのリモート LNS ポートを入力します。 <u>値の範囲</u> ：1~65535。
User Name	必須入力項目	L2TP サーバーに接続するときに認証される、L2TP トンネルのユーザー名を入力します。 <u>値の範囲</u> ：0~32 文字。
Password	必須入力項目	L2TP サーバーに接続するときに認証される、L2TP トンネルのパスワードを入力します。
Tunneling Password (Optional)	デフォルト値：チェックなし	L2TP トンネルが認証するためのトンネリングパスワードを入力します。
Remote Subnet	必須入力項目	L2TP トンネルが L2TP サーバーに到達するためのゲートウェイを指定します。 ここで、リモートサブネットという設定を指定する必要があります。これは、L2TP VPN サーバーのイントラネット用です。したがって、PPTP クライアントピアでは、宛先が専用サブネット内にあるパケットは、PPTP VPN トンネル経由で転送されます。その他は、L2TP クライアントピアのセキュリティゲートウェイの現在のルーティングポリシーに基づいて転送されます。 リモートサブネットフォーマットは、IP アドレス/ネットマスク (例：10.0.0.2/24) でなければなりません。
Authentication Protocol	必須入力項目	L2TP トンネルの認証プロトコルを指定することができます。PAP / CHAP / MS-CHAP / MS-CHAP v2 をクリックします。-> プロトコルは、どのチェックボックスをクリックするかを有効にします。
MPPE Encryption	1. デフォルト値：チェックなし 2. 任意入力項目	L2TP サーバーが、MPPE プロトコルをサポートするかどうかを指定します。Enable チェックボックスをクリックして、MPPE を有効化します。 注：MPPE 暗号化が有効になっている場合、Authentication Protocol の PAP/CHAP オプションは使用できません。

LCP Echo Type	1. デフォルト 値 : Auto	L2TP トンネルの LCP エコータイプを指定します。これは、Auto、User-defined、または、Disable から選択可能です。 Auto : システムが、Interval (間隔) および Max.Failure Time (最大故障回数) を設定します。 User-defined : Interval (間隔) および Max.Failure Time (最大故障回数) を入力します。Interval のデフォルト値は 30 秒で、Maximum Failure Times は 6 回です。 Disable : LCP エコーを無効化します。 <u>値の範囲</u> : Interval Time は、1~99999、Failure Time は、1~999 です。
Service Port	必須入力項目	L2TP トンネルが使用するサービスポートを指定します。これは、Auto、1701 (Cisco の場合)、または、User-defined から選択可能です。 Auto : システムがサービスポートを決定します。 1701 (Cisco の場合) : システムは、CISCO L2TP Server に接続するためにポート 1701 を使用します。 User-defined : サービスポートを入力します。デフォルト値は 0 です。 <u>値の範囲</u> : 0~65535。
Tunnel	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れて、L2TP トンネルを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。
Back	-	Back ボタンをクリックして、前ページに戻ります。

5.1.4 PPTP

Configuration [Help]	
Item	Setting
▶ PPTP	<input checked="" type="checkbox"/> Enable
▶ Client/Server	Server ▼

PPTP Server Configuration	
Item	Setting
▶ PPTP Server	<input type="checkbox"/> Enable
▶ Interface	All WANs ▼
▶ Server Virtual IP	192.168.0.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	17
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable 40 bits ▼

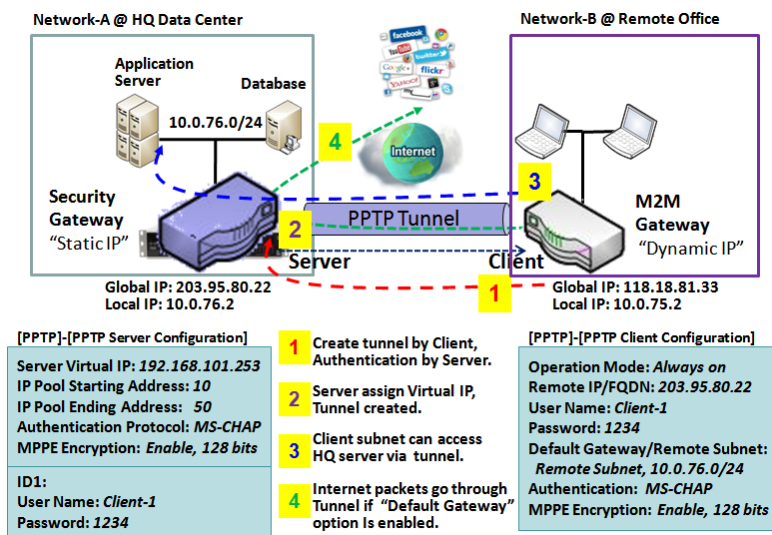
PPTP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

User Account List Add Delete				
ID	User Name	Password	Enable	Actions

PPTP（ポイントツーポイントトンネリングプロトコル）は、仮想プライベートネットワークの実装方式のひとつです。PPTP は TCP 経由の制御チャネルと GRE トンネル操作を使用して PPP パケットをカプセル化しています。これは、クライアント/サーバーベースの技術です。PPTP トンネリングの認証と暗号化には、Windows PPTP スタックの標準機能としてネイティブにさまざまなレベルがあります。セキュリティゲートウェイは、PPTP VPN トンネルの「PPTP サーバー」ロール、または「PPTP クライアント」ロール、またはそれら異なるトンネルに対するロール両方を、同時に行うことができます。PPTP トンネルプロセスは、L2TP とほぼ同じです。

PPTP Server：クライアントが、PPTP トンネルを作成するには、静的 IP または FQDN が必要です。また、クライアントログイン認証用の「ユーザーアカウントリスト」（ユーザー名/パスワード）も保持します。接続された各 PPTP クライアントに仮想 IP を割り当てるための仮想 IP プールがあります。

PPTP Client : これは、動的 IP を備えたりリモートオフィス内のモバイルユーザーまたはゲートウェイです。トンネルを設定するには、「ユーザー名」、「パスワード」、および、サーバーのグローバル IP を取得する必要があります。さらに、メイン接続としての各トンネルの動作モード、別のトンネルのフェールオーバー、または、負荷バランストンネルを識別して全体の帯域幅を増やす必要があります。パケットフローのために「Default Gateway」または「Remote Subnet」を決定する必要があります。さらに、「Default Gateway/Remote Subnet」パラメータで、PPTP トンネルを通過するトラフィックの種類を定義することもできます。



「Default Gateway/Remote Subnet」設定項目には、「Default Gateway」と「Remote Subnet」という2つのオプションがあります。「Remote Subnet」を選択すると、リモートサブネットというもう1つの設定を指定する必要があります。これは、PPTP VPNサーバーのイントラネット用です。したがって、PPTP クライアントピアでは、宛先が専用サブネット内にあるパケットは、PPTP VPN トンネル経由で転送されます。その他は、PPTP クライアントピアのセキュリティゲートウェイの現在のルーティングポリシーに基づいて転送されます。しかし、L2TP クライアントピアの「Default Gateway」オプションを選択すると、PPTP クライアントピアのインターネットアクセスを含

むすべてのパケットが、確立された PPTP VPN トンネルを通過します。つまり、リモート PPTP VPN サーバーは、PPTP クライアントピアからのパケットフローを制御します。確かに、これらのパケットは、PPTP VPN トンネルを経由します。

PPTP 設定

Security > VPN > PPTP タブに進みます。

PPTP 設定により、PPTP トンネルを作成および設定することができます。

PPTP の有効化

Configuration [Help]	
Item	Setting
▶ PPTP	<input type="checkbox"/> Enable
▶ Client/Server	Server ▼

Configuration		
項目	値設定	説明
PPTP	デフォルト値：チェックなし	Enable チェックボックスをクリックし、PPTP 機能を有効化します。
Client/Server	必須入力項目	PPTP の役割を指定します。ゲートウェイが使用する Server（サーバー）または Client（クライアント）の役割を選択します。以下は、PPTP サーバーとクライアントの設定ウィンドウです。
Save	-	Save ボタンをクリックして、設定を保存します。

PPTP サーバー

ゲートウェイは、最大 10 の PPTP ユーザーアカウントをサポートします。

Client/Server フィールドの **Server** を選択すると、PPTP サーバー設定ウィンドウが表示されます。

PPTP Server Configuration	
Item	Setting
▶ PPTP Server	<input type="checkbox"/> Enable
▶ Interface	All WANs ▼
▶ Server Virtual IP	192.168.0.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	17
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable 40 bits ▼

PPTP Server Configuration		
項目	値設定	説明
PPTP Server	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、ゲートウェイの PPTP サーバーロールを有効化します。
Interface	1. 必須入力項目 2. デフォルト値： ALL WAN	選択したインターフェイスをこの L2TP トンネルに使用するように定義します。
Server Virtual IP	1. 必須入力項目 2. デフォルト値： 192.168.0.1	PPTP サーバー仮想 IP アドレスを指定します。仮想 IP アドレスは、PPTP クライアントの仮想 DHCP サーバーとして機能します。クライアントには、PPTP トンネルが確立された後、そこから仮想 IP アドレスが割り当てられます。
IP Pool Starting Address	1. 必須入力項目 2. デフォルト値： 10	これは、PPTP サーバーの仮想 IP DHCP サーバーです。ユーザーは、PPTP クライアントの IP アドレスが割り当てられるサブネットの最初の IP アドレスを指定することができます。 <u>値の範囲</u> ：1～255。
IP Pool Ending Address	1. 必須入力項目 2. デフォルト値： 17	これは、PPTP サーバーの仮想 IP DHCP サーバーです。ユーザーは、PPTP クライアントの IP アドレスが割り当てられるサブネットの最後の IP アドレスを指定することができます。 <u>値の範囲</u> ：1～255。
Authentication Protocol	1. 必須入力項目 2. デフォルト値： チェックなし	PPTP クライアントを認証する PPTP サーバーに対して、単一または複数の認証プロトコルを選択します。利用可能な認証プロトコルは、PAP / CHAP / MS-CHAP / MS-CHAP v2 です。
MPPE Encryption	1. 必須入力項目 2. デフォルト値： チェックなし	MPPE プロトコルをサポートするかどうかを指定します。Enable チェックボックスをクリックして、MPPE を有効にし、ドロップダウンボックスから、40 ビット / 56 ビット / 128 ビットを選択します。 注：MPPE Encryption が有効になっている場合、Authentication Protocol の PAP/CHAP オプションは使用できません。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

PPTP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

PPTP Server Status		
項目	値設定	説明
PPTP Server Status	-	接続されている PPTP クライアントの User Name、Remote IP、Remote Virtual IP、および、Remote Call ID が表示されます。 Refresh ボタンをクリックして、PPTP クライアント情報を更新します。

User Account List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	User Name	Password	Enable	Actions
User Account Configuration				
User Name		Password		Account
<input type="text"/>		<input type="text"/>		<input type="checkbox"/> Enable
<input type="button" value="Save"/>				

User Account List User Account Configuration		
項目	値設定	説明
User Account List	最大 10 のユーザーアカウント	<p>これは、PPTP 認証ユーザーアカウントエントリです。リモートクライアントのアカウントを作成および追加して、ゲートウェイデバイスへの PPTP VPN 接続を確立することができます。</p> <p>Add ボタンをクリックして、ユーザーアカウントを追加します。ユーザー名とパスワードを入力します。次に、Enable チェックボックスにチェックを入れて、ユーザーを有効化します。</p> <p>Save ボタンをクリックして、新規ユーザーアカウントを保存します。</p> <p>選択したユーザーアカウントは、Delete ボタンをクリックすると完全に削除できます。</p> <p><u>値の範囲</u> : 1~32 文字。</p>

PPTP クライアント

Client/Server で Client を選択すると、一連の PPTP Client Configuration が表示されます。

PPTP Client Configuration	
Item	Setting
▶ PPTP Client	<input type="checkbox"/> Enable

PPTP Client Configuration		
項目	値設定	説明
PPTP Client	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れ、ゲートウェイの PPTP クライアントルールを有効にします。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

PPTP クライアントの作成/編集

MMLink-GWL

PPTP Client List & Status								
ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status	Enable	Actions

Add/Edit ボタンをクリックされると、一連の PPTP Client Configuration が表示されます。

PPTP Client Configuration	
Item	Setting
▶ Tunnel Name	<input type="text" value="PPTP #1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ Operation Mode	<input type="text" value="Always on"/>
▶ Remote IP/FQDN	<input type="text"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable
▶ LCP Echo Type	<input type="text" value="Auto"/> Interval <input type="text" value="30"/> seconds Max. Failure Time <input type="text" value="6"/> times
▶ Tunnel	<input type="checkbox"/> Enable

PPTP Client List & Status PPTP Client Configuration		
項目	値設定	説明
Tunnel Name	必須入力項目	トンネル名を入力します。識別しやすい名称を入力します。 <u>値の範囲</u> ： 1～32 文字。
Interface	1. 必須入力項目 2. デフォルト値： WAN 1	選択したインターフェイスを PPTP トンネルに使用するように定義します。 (WAN-1 は、WAN-1 インターフェイスが有効な場合のみ利用可能です) 他の WAN インターフェイス (WAN 2 など) でも同様です。
Operation Mode	1. 必須入力項目 2. デフォルト値： Always on	PPTP トンネルの動作モードを定義します。Always on または Failover にすることができます。

		<p>トンネルがフェールオーバートンネルとして設定されている場合は、フェールオーバー先のプライマリトンネルをさらに選択する必要があります。</p> <p>注：Failover モードは、WAN が 1 つのゲートウェイでは使用できません。</p>
Remote IP/FQDN	<p>1. 必須入力項目。 2. フォーマットには、ipv4 アドレスまたは FQDN を使用することができます</p>	<p>PPTP サーバーのパブリック IP アドレスまたは FQDN を入力します。</p>
User Name	<p>必須入力項目</p>	<p>PPTP サーバーに接続するときに認証される、PPTP トンネルのユーザー名を入力します。</p> <p><u>値の範囲</u>：1～32 文字。</p>
Password	<p>必須入力項目</p>	<p>PPTP サーバーに接続するときに認証される、PPTP トンネルのパスワードを入力します。</p>
Remote Subnet	<p>必須入力項目</p>	<p>PPTP トンネルが PPTP サーバーに到達するためのゲートウェイを指定します。</p> <p>ここで、リモートサブネットという設定を指定する必要があります。これは、PPTP VPN サーバーのイントラネット用です。したがって、PPTP クライアントピアでは、宛先が専用サブネット内にあるパケットは、PPTP VPN トンネル経由で転送されません。その他は、PPTP クライアントピアのセキュリティゲートウェイの現在のルーティングポリシーに基づいて転送されます。</p>
Authentication Protocol	<p>1. 必須入力項目 2. デフォルト値：チェックなし</p>	<p>PPTP トンネルに複数の認証プロトコルを指定します。</p> <p>利用可能な認証方法は、PAP / CHAP / MS-CHAP / MS-CHAP v2 です。</p>
MPPE Encryption	<p>1. デフォルト値：チェックなし 2. 任意入力項目</p>	<p>PPTP サーバーが、MPPE プロトコルをサポートするかどうかを指定します。Enable チェックボックスをクリックして、MPPE を有効化します。</p> <p>注：MPPE 暗号化が有効になっている場合、認証プロトコル PAP/CHAP オプションは使用できません。</p>
LCP Echo Type	<p>デフォルト値： Auto</p>	<p>TTTP トンネルの LCP エコータイプを指定します。これは Auto、User-defined または、Disable です。</p> <p>Auto：システムが、Interval（間隔）および Max.Failure Time（最大故障回数）を入力します。</p> <p>User-defined：Interval（間隔）および Max.Failure Time（最大故障回数）を入力します。Interval のデフォルト値は 30 秒で、Maximum Failure Times は 6 回です。</p> <p>Disable：LCP エコーを無効化します。</p> <p><u>値の範囲</u>：Interval Time は、1～99999、Failure Time は、1～999 です。</p>
Tunnel	<p>デフォルト値：チェックなし</p>	<p>Enable チェックボックスにチェックを入れて、TTTP トンネルを有効化します。</p>

Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。
Back	-	Back ボタンをクリックして、前ページに戻ります。

5.1.5 GRE

Configuration [Help]	
Item	Setting
▶ GRE Tunnel	<input checked="" type="checkbox"/> Enable
▶ Max. Concurrent GRE Tunnels	<input type="text" value="32"/>

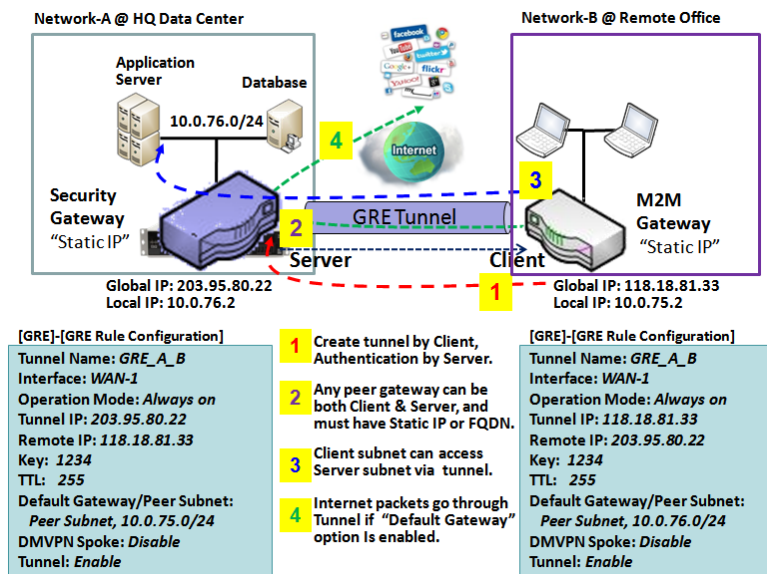
GRE Tunnel List Add Delete												
ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	MTU	Key	TTL	Keep-alive	Remote Subnet	Enable	Actions

GRE (Generic Routing Encapsulation) はシスコシステムズが開発したトンネリングプロトコルで、インターネットプロトコルネットワーク経由の仮想ポイントツーポイントリンク内の各種のネットワーク層プロトコルをカプセル化することができます。

リモートサイトのための M2M ゲートウェイを展開し、GRE トンネリングを使用して、コントロールセンターと仮想プライベートネットワークを確立します。したがって、M2M ゲートウェイの後にあるすべてのクライアントホストは、コントロールセンターゲートウェイの後にあるサーバーホストとのデータ通信を行うことができます。

GRE トンネリングは IPSec トンネリングと似ていますが、クライアントはサーバーとのトンネル確立を要求します。クライアントとサーバーの両方に、静的 IP または FQDN が必要です。すべてのピアゲートウェイは、同じ設定ルールセットを使用していても、クライアントまたはサーバーとして動作することができます。

GRE トンネルのシナリオ



GRE トンネルを設定するには、各ピアがグローバル IP をトンネル IP として設定し、相手のグローバル IP をリモート IP として入力する必要があります。

「Default Gateway/Peer Subnet」設定項目には、「Default Gateway」と「Peer Subnet」という 2 つのオプションがあります。Peer Subnet を選択すると、ピアサブネットというもう 1 つの設定を指定する必要があります。これは、GRE サーバーのイントラネット用です。したがって、GRE クライアントピアでは、宛先が専用サブネット内にあるパケットは、GRE トンネル経由で転送されます。その他は、GRE クライアントピアのゲートウェイの現在のルーティングポリシーに基づいて転送されます。しかし、GRE クライアントピアの

「Default Gateway」オプションを選択すると、GRE クライアントピアのインターネットアクセスを含むすべてのパケットが、確立された GRE トンネルを通過します。つまり、リモート GRE サーバーは、GRE クライアントピアからのパケットフローを制御します。確かに、これらのパケットは、GRE トンネルを経由します。

GRE サーバーが、VPN コンセントレータのような Cisco ルーターなどの DMVPN ハブ機能をサポートしている場合、GRE クライアントは、IPSec トンネリングによる GRE により実装されているため、ここで DMVPN スポーク機能を有効化することができます。

GRE 設定

Security > VPN > GRE タブに進みます。

GRE 設定により、GRE トンネルを作成および設定することができます。

GRE の有効化

Configuration [Help]	
Item	Setting
▶ GRE Tunnel	<input type="checkbox"/> Enable
▶ Max. Concurrent GRE Tunnels	<input type="text" value="32"/>

Configuration		
項目	値設定	説明
GRE Tunnel	デフォルト値：チェックなし	Enable チェックボックスをクリックして、GRE 機能を有効化します。
Max.Concurrent GRE Tunnels	製品仕様に依存します。	指定された値は、同時 GRE トンネル接続の最大数を制限します。購入したモデルのデフォルト値は異なる場合があります。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします

GRE トンネルの作成/編集

GRE Tunnel List Add Delete												
ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	MTU	Key	TTL	Keep-alive	Remote Subnet	Enable	Actions

Add/Edit ボタンをクリックされると、GRE Rule Configuration ウィンドウが表示されます。

GRE Rule Configuration [Help]	
Item	Setting
▶ Tunnel Name	<input type="text" value="GRE #1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ Operation Mode	<input type="text" value="Always on"/>
▶ Tunnel IP	IP: <input type="text"/> MASK: <input type="text" value="-- select one --"/> (Optional)
▶ Remote IP	<input type="text"/>
▶ MTU	<input type="text"/>
▶ Key	<input type="text"/> (Optional)
▶ TTL	<input type="text"/>
▶ Keep alive	<input type="checkbox"/> Enable Ping IP <input type="text"/> Interval <input type="text" value="5"/> (seconds)
▶ Remote Subnet	<input type="text"/>
▶ DMVPN Spoke	<input type="checkbox"/> Enable
▶ IPsec Pre-shared Key	<input type="text"/> (Min. 8 characters)
▶ IPsec NAT Traversal	<input type="checkbox"/> Enable
▶ IPsec Encapsulation Mode	<input type="text" value="Transport Mode"/>
▶ Tunnel	<input type="checkbox"/> Enable

GRE Tunnel List GRE Rule Configuration		
項目	値設定	説明
Tunnel Name	必須入力項目	トンネル名を入力します。識別しやすい名称を入力します。 <u>値の範囲</u> ：1～8文字。
Interface	1. 必須入力項目 2. デフォルト値： WAN 1	GRE トンネルを確立するインターフェイスを選択します。これは、利用可能な WAN および LAN インターフェイスにすることができます。
Operation Mode	1. 必須入力項目 2. デフォルト値： Always on	GRE トンネルの動作モードを定義します。Always on または Failover にすることができます。 トンネルがフェールオーバートンネルとして設定されている場合は、フェールオーバー先のプライマリトンネルをさらに選択する必要があります。 注： Failover モードは、WAN が 1 つのゲートウェイでは使用できません。
Tunnel IP	任意の設定	IP：トンネル IP アドレスを入力します。 MASK：トンネルサブネットマスクを選択します。

Remote IP	必須入力項目	リモート GRE トンネルゲートウェイのリモート IP アドレスを入力します。通常、これはリモート GRE ゲートウェイのパブリック IP アドレスです。
MTU	1.必須入力項目 2.デフォルト値： チェックなし	Tunnel MTU （トンネルMTU）を指定します。 <u>値の範囲</u> ：64～1500bandwidth。
Key	任意の設定	GRE 接続のキーを入力します。 <u>値の範囲</u> ：0～9999999999。
TTL	1.必須入力項目 2.1～255 の範囲 です	GRE トンネルの TTL ホップカウント値を指定します。 <u>値の範囲</u> ：1～255。
Keep alive	1.デフォルト値： チェックなし 2. デフォルト値： 5 秒	Enable チェックボックスにチェックを入れて、キープアライブ機能を有効化します。 ライブを維持し、ping する IP アドレスを入力するには、Ping IP を選択します。 ping の時間間隔を秒単位で入力します。 <u>値の範囲</u> ：5～999 秒。
Remote Subnet	必須入力項目	GRE トンネルが GRE サーバーに到達するためのゲートウェイを指定します。 リモートサブネットフォーマットは、IP アドレス/ネットマスク（例：10.0.0.2/24）でなければなりません。
DMVPN Spoke	デフォルト値：チ ェックなし	ゲートウェイが、GRE トンネルの DMVPN スポークをサポートするかどうかを指定します。Enable チェックボックスにチェックを入れて、DMVPN スポークを有効化します。
IPSec Pre-shared Key	必須入力項目	DMVPN スポーク認証事前共有キー（8～32 文字）を入力します。 注：PDMVPN Spoke が有効な場合にのみ利用可能です。
IPSec NAT Traversal	デフォルト値：チ ェックなし	Enable チェックボックスにチェックを入れて、NAT-Traversal を有効化します。 注：DMVPN が有効になっていない場合、IPSec NAT Traversal は使用できません。
IPSec Encapsulation Mode	デフォルト値：チ ェックなし	ドロップダウンボックスから IPSec カプセル化モードを指定します。Transport（転送）モードと Tunnel（トンネル）モードがサポートされています。 注：DMVPN が有効になっていない場合、IPSec Encapsulation Mode は使用できません。
Tunnel	デフォルト値：チ ェックなし	Enable ボックスにチェックを入れて、GRE トンネルを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。
Back	-	Back ボタンをクリックして、前ページに戻ります。

5.2 ファイアウォール

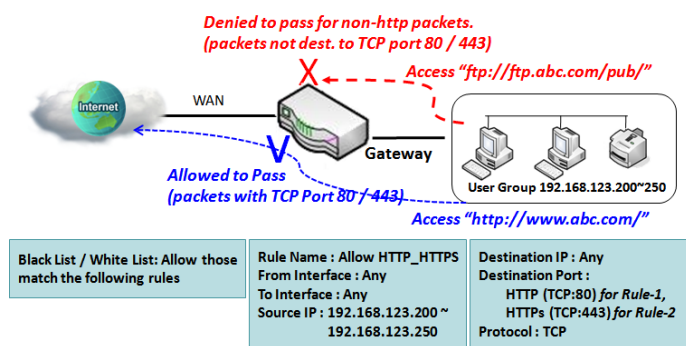
5.2.1 パケットフィルタ

Configuration [Help]											
Item	Setting										
▶ Packet Filters	<input checked="" type="checkbox"/> Enable										
▶ Black List / White List	Deny those match the following rules. ▼										
▶ Log Alert	<input type="checkbox"/> Log Alert										

Packet Filter List [Add] [Delete]												
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions

「Packet Filter（パケットフィルタ）」機能を使用すると、受信パケットと送信パケットのいくつかのフィルタリングルールを定義することができます。したがって、ゲートウェイは、通過を許可するパケットと拒否するパケットを制御することができます。パケットフィルタルールでは、パケットがゲートウェイに入り、出るインターフェイス、送信元と宛先の IP アドレス、および宛先サービスのポートタイプとポート番号を示す必要があります。さらに、ルールが有効化される予定を示す必要があります。

ホワイトリストシナリオによるパケットフィルタ



図に示すように、「パケットフィルタルールリスト」をホワイトリスト（以下のルールと一致するようにする）として指定し、ルールを定義します。ルール1はHTTPパケットの通過を許可し、ルール2はHTTPSパケットの通過を許可します。

このような構成では、ゲートウェイは、WANポートを通過するTCPポート80または443を対象とするIP範囲192.168.123.200から250までのHTTPおよびHTTPSパケットのみを許可します。

パケットフィルタ設定

Security > Firewall > Packet Filter タブに進みます。

パケットフィルタ設定では、パケットフィルタポリシーを作成およびカスタマイズして、オフィス設定に基づいて、特定の受信/送信パケットをルーター経由で許可または拒否することができます。

パケットフィルタの有効化

Configuration [Help]	
Item	Setting
▶ Packet Filters	<input type="checkbox"/> Enable
▶ Black List / White List	Deny those match the following rules. ▼
▶ Log Alert	<input type="checkbox"/> Log Alert

Configuration		
項目名	値設定	説明
Packet Filter	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、パケットフィルタ機能を有効化します
Black List / White List	デフォルト値：Deny those match the following rules	<i>Deny those match the following rules</i> (規則に一致するものを拒否する) を選択すると、名前に示されているように、ルールで指定されたパケットはブラックリストに表示されます。対照的に、 <i>Allow those match the following rules</i> (規則に一致するものを許可する) を使用して、ホワイトリストを指定し、パケットを通過させ、残りをブロックします。
Log Alert	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、イベントログが有効化されます。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

パケットフィルタールの作成/編集

ゲートウェイにより、パケットフィルタリングルールをカスタマイズすることができます。これは、最大 20 のフィルタールールセットをサポートします。

Packet Filter List												
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions

Add ボタンをクリックされると、Packet Filter Rule Configuration ウィンドウが表示されます。

Packet Filter Rule Configuration	
Item	Setting
▶ Rule Name	<input type="text" value="Rule1"/>
▶ From Interface	<input type="text" value="Any"/>
▶ To Interface	<input type="text" value="Any"/>
▶ Source IP	<input type="text" value="Any"/>
▶ Destination IP	<input type="text" value="Any"/>
▶ Source MAC	<input type="text" value="Any"/>
▶ Protocol	<input type="text" value="Any(0)"/>
▶ Source Port	<input type="text" value="User-defined Service"/> <input type="text"/> - <input type="text"/>
▶ Destination Port	<input type="text" value="User-defined Service"/> <input type="text"/> - <input type="text"/>
▶ Time Schedule	<input type="text" value="(0) Always"/>
▶ Rule	<input type="checkbox"/> Enable

Packet Filter Rule Configuration

項目名	値設定	説明
Rule Name	1. 文字列形式：任意のテキスト 2. 必須入力項目	パケットフィルタールール名を入力します。覚えやすい名称を入力します。 <u>値の範囲</u> ：1～30 文字。
From Interface	1. 必須入力項目 2. デフォルト値： Any	選択したインターフェイスが、ルーターのパケット入力インターフェイスになるように定義します。フィルタリングするパケットが、LAN から WAN に来ている場合（LAN to WAN）は、このフィールドで LAN を選択します。 任意のインターフェイスからルーターに入ってくるパケットに対して、Any を選択します。 2つの同一のインターフェイスは、ルーターにより受け入れられないことに注意してください。

To Interface	1. 必須入力項目 2. デフォルト値 : Any	<p>選択したインターフェイスが、ルーターの packets 出力インターフェイスになるように定義します。フィルタリングする packets が、LAN から WAN に入る場合 (LAN to WAN) は、このフィールドで WAN を選択します。</p> <p>任意のインターフェイスからルーターから出ていく packets に対して、Any を選択します。</p> <p>2つの同一のインターフェイスは、ルーターにより受け入れられないことに注意してください。</p>
Source IP	1. 必須入力項目 2. デフォルト値 : Any	<p>このフィールドは、ソース IP アドレスを指定するためのフィールドです。</p> <p>任意の IP アドレスからの packets をフィルタするには、Any を選択します。</p> <p>IP アドレスからの packets をフィルタリングするには、Specific IP Address を選択します。</p> <p>特定の範囲の IP アドレスからの packets をフィルタリングするには、IP Range を選択します。</p> <p>事前定義されたグループからの packets をフィルタリングするには、IP Address-based Group を選択します。注：このオプションを利用可能にするには、グループをあらかじめ定義しておく必要があります。Object Definition > Grouping > Host grouping を参照してください。Add Rule ショートカットボタンを使用してグループを作成することもできます。</p>
Destination IP	1. 必須入力項目 2. デフォルト値 : Any	<p>このフィールドは、宛先 IP アドレスを指定するためのフィールドです。</p> <p>任意の IP アドレスに入る packets をフィルタするには、Any を選択します。</p> <p>このフィールドに入力した IP アドレスに入る packets をフィルタリングするには、Specific IP Address を選択します。</p> <p>このフィールドに入力した IP アドレスの範囲に入る packets をフィルタリングするには、IP Range を選択します。</p> <p>事前定義されたグループに入る packets をフィルタリングするには、IP Address-based Group を選択します。注：このオプションを利用可能にするには、グループをあらかじめ定義しておく必要があります。Object Definition > Grouping > Host grouping を参照してください。Add Rule ショートカットボタンを使用してグループを作成することもできます。Add Rule ボタンで設定した内容は、Host grouping ウィンドウにも表示されます。</p>
Source MAC	1. 必須入力項目 2. デフォルト値 : Any	<p>このフィールドは、ソース MAC アドレスを指定するためのフィールドです。</p> <p>任意の MAC アドレスからの packets をフィルタするには、Any を選択します。</p> <p>MAC アドレスからの packets をフィルタリングするには、Specific MAC Address を選択します。</p> <p>事前定義されたグループからの packets をフィルタリングするには、MAC Address-based Group を選択します。注：このオプシ</p>

	<p>ョンを利用可能にするには、グループをあらかじめ定義しておく必要があります。Object Definition > Grouping > Host grouping を参照してください。Add Rule ショートカットボタンを使用してグループを作成することもできます。</p>
<p>Protocol</p> <p>1. 必須入力項目 2. デフォルト値 : Any (0)</p>	<p>Any を選択すると、プロトコルパケットがすべてフィルタされます。次に、Source Port で、Well-known Service を選択する場合は、predefined port ドロップダウンボックスを選択し、そうでない場合は、User-defined Service (ユーザー定義サービス) を選択して、ポート範囲を指定します。</p> <p>次に、Destination Port で、Well-known Service を選択する場合は、predefined port ドロップダウンボックスを選択し、そうでない場合は、User-defined Service (ユーザー定義サービス) を選択して、ポート範囲を指定します。</p> <p><u>値の範囲</u> : Source Port、Destination Port の範囲、1~65535 です。</p> <p>ICMPv4 を選択して、ICMPv4 パケットをフィルタリングします</p> <p>TCP を選択して、TCP パケットをフィルタリングします。</p> <p>次に、Source Port で、Well-known Service が選択されている場合は、predefined port ドロップダウンボックスを選択し、そうでない場合は、User-defined Service (ユーザー定義サービス) を選択して、ポート範囲を指定します。</p> <p>次に、Destination Port で、Well-known Service が選択されている場合は、predefined port ドロップダウンボックスを選択し、そうでない場合は、User-defined Service (ユーザー定義サービス) を選択して、ポート範囲を指定します。</p> <p><u>値の範囲</u> : Source Port (ソースポート)、Destination Port (宛先ポート) の場合、1~65535 です。</p> <p>UDP を選択して、UDP パケットをフィルタリングします。</p> <p>次に、Source Port で、Well-known Service が選択されている場合は、predefined port ドロップダウンボックスを選択し、そうでない場合は、User-defined Service (ユーザー定義サービス) を選択して、ポート範囲を指定します。</p> <p>次に、Destination Port で、Well-known Service が選択されている場合は、predefined port ドロップダウンボックスを選択し、そうでない場合は、User-defined Service (ユーザー定義サービス) を選択して、ポート範囲を指定します。</p> <p><u>値の範囲</u> : Source Port (ソースポート)、Destination Port (宛先ポート) の場合、1~65535 です。</p> <p>GRE を選択して、GRE パケットをフィルタリングします。</p> <p>GRE を選択して、GRE パケットをフィルタリングします</p> <p>SCTP を選択して、SCTP パケットをフィルタリングします。</p> <p>User-defined (ユーザー定義) を選択して、指定したポート番号のパケットをフィルタリングします。次に、Protocol Number (プロトコル番号) ボックスにポート番号を入力します。</p>

Time Schedule	必須入力項目	Time Schedule をルールに適用、もしくは Always を設定します。 ドロップダウンリストが空の場合、Time Schedule が事前設定されていることを確認してください。Object Definition > Scheduling > Configuration タブを参照します。
Rule	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本ルールを有効化し、設定を保存します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします
Back	-	Back ボタンをクリックすると、画面が Packet Filter Configuration ページに戻ります。

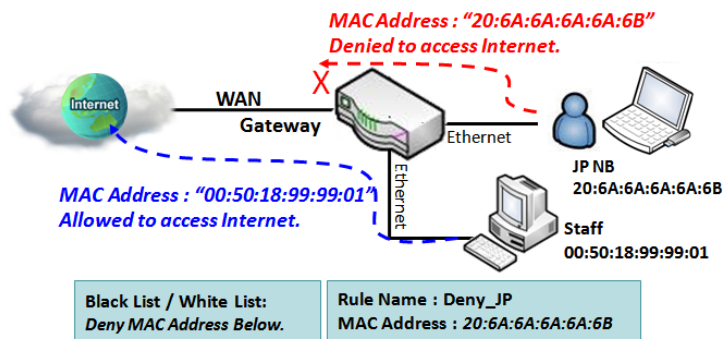
5.2.2 MAC 制御

Configuration [Help]	
Item	Setting
▶ MAC Control	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	<input type="checkbox"/> Enable
▶ Known MAC from LAN PC List	192.168.1.100(James-P45V) ▼ <input type="button" value="Copy to"/>

MAC Control Rule List <input type="button" value="Add"/> <input type="button" value="Delete"/>					
ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

「MAC Control (MAC 制御)」を使用すると、デバイスの MAC アドレスに基づいて、ユーザーごとに異なるゲートウェイにアクセス権を割り当てることができます。管理者が特定の MAC アドレスを持つクライアントホストからのトラフィックを拒否したい場合は、「MAC Control (MAC 制御)」機能を使用して、ブラックリストの設定に基づき拒否することができます。

ブラックリストシナリオによる MAC 制御



図に示すように、MAC 制御機能を有効にし、「MAC Control Rule List (MAC 制御ルールリスト)」をブラックリストとし、「JP NB」からの接続要求を自身の MAC アドレス (20:6A:6A:6A:6A:6B) で拒否するゲートウェイの MAC 制御ルールを 1 つ設定します。

システムは、「JP NB」からゲートウェイへの接続をブロックしますが、他の接続は許可します。

MAC 制御設定

Security > Firewall > MAC Control タブに進みます。

MAC 制御設定により、MAC アドレスポリシーを作成およびカスタマイズして、特定の送信元 MAC アドレスを持つパケットを許可または拒否することができます。

MAC 制御の有効化

Configuration [Help]	
Item	Setting
▶ MAC Control	<input type="checkbox"/> Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	<input type="checkbox"/> Enable
▶ Known MAC from LAN PC List	192.168.123.100(James-P45V) ▼ <input type="button" value="Copy to"/>

Configuration		
項目	値設定	説明
MAC Control	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、MAC フィルタ機能を有効化します。
Black List / White List	デフォルト値：Deny MAC Address Below	<i>Deny MAC Address Below</i> （以下の MAC アドレスを拒否する）を選択すると、名前に示されているように、ルールで指定されたパケットはブロックされます（ブラックリストに表示されません）。対照的に、 <i>Allow MAC Address Below</i> （以下の MAC アドレスを許可する）を使用して、ホワイトリストを指定し、パケットを通過させ、残りをブロックします。
Log Alert	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、イベントログが有効化されます。
Known MAC from LAN PC List	-	LAN Client のリストボックスから MAC アドレスを選択します。Copy to をクリックして、選択した MAC アドレスをフィルタルールにコピーします。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

MAC 制御ルールの作成/編集

ゲートウェイは、最大 20 のフィルタルールセットをサポートします。制御ルールを作成する前に、MAC Control が有効になっていることを確認してください。

MAC Control Rule List <input type="button" value="Add"/> <input type="button" value="Delete"/>					
ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

Add ボタンがクリックされると、Filter Rule Configuration ウィンドウが表示されます。

MAC Control Rule Configuration			
Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
<input type="text" value="Rule1"/>	<input type="text"/>	(0) Always ▼	<input type="checkbox"/>
<input type="button" value="Save"/>			

MAC Rule Configuration		
項目	値設定	説明
Rule Name	1.文字列形式：任意のテキスト 2. 必須入力項目	MAC Control（MAC 制御）ルール名を入力します。
MAC Address (Use: to Compose)	1.MAC アドレスの文字列形式です 2. 必須入力項目	ルールをフィルタリングするソース MAC アドレスを指定します。
Time Schedule	必須入力項目	Time Schedule をこのルールに適用、もしくは Always を設定します。 ドロップダウンリストが空の場合、Time Schedule が事前設定されていることを確認してください。Object Definition > Scheduling > Configuration タブを参照します
Enable	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本ルールを有効化し、設定を保存します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

5.2.3 IPS

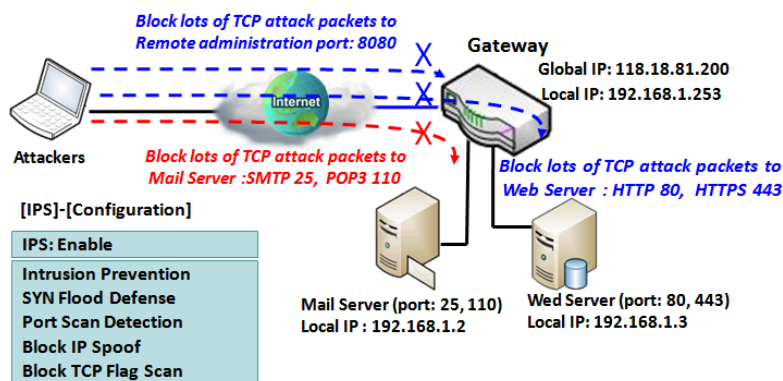
Configuration [Help]	
Item	Setting
▶ IPS	<input type="checkbox"/> Enable
▶ Log Alert	<input type="checkbox"/> Enable

Intrusion Prevention	
Item	Setting
▶ SYN Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ UDP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ ICMP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ Port Scan Detection	<input type="checkbox"/> Enable <input type="text" value="200"/> Packets/second (10~10000)

インターネットにアプリケーションサーバーを提供するには、管理者は、サービスの特定のポートを開く必要があります。しかし、インターネット上のサービスポートを開くことには、常にいくつかのリスクがあります。このような攻撃のリスクを回避するには、IPS 機能を有効化することが重要です。

IPS（侵入防止システム）は、ネットワークやシステムで悪意のあるアクティビティが実行されていないか監視するネットワークセキュリティ装置です。IPS の主な機能は、悪意のあるアクティビティを特定すること、そのアクティビティに関する情報を記録すること、およびそのアクティビティをブロック/停止して報告することです。必要があれば、IPS 機能を有効にして、リストの侵入アクティビティが存在しないか確認することができます。また、ログ警告を有効にすると、該当する侵入が検出された場合に侵入イベントがシステムにより記録されます。

IPS のシナリオ



図に示すように、ゲートウェイは、電子メールサーバー、Webサーバーとして機能し、リモート管理用の TCP ポート 8080 を提供します。したがって、リモートユーザーまたは未知のユーザーは、インターネットからこれらのサービスを要求することができます。IPS を有効にすると、ゲートウェイはサービスを含む TCP ポート（25、80、110、443、および、8080）を含む着信攻撃パケットを検出することができます。これにより、攻撃パケットをブロックし、通常アクセスがゲートウェイを通過できるようにします。

IPS 設定

Security > Firewall > IPS タブに進みます。

Intrusion Prevention System (IPS : 侵入防御システム) 設定では、侵入防止ルールをカスタマイズし、悪意のあるパケットを防ぐことができます。

IPS ファイアウォールの有効化

Configuration [Help]	
Item	Setting
▶ IPS	<input type="checkbox"/> Enable
▶ Log Alert	<input type="checkbox"/> Enable

Configuration		
項目	値設定	説明
IPS	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れ、IPS 機能を有効化します
Log Alert	デフォルト値 : チェックボックスなし	Enable チェックボックスにチェックを入れると、イベントログが有効化されます。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

侵入防止ルールの設定

ルーターにより、有効する侵入防止ルールを選択することができます。防御機能を有効にするには、IPS が有効になっていることを確認してください。

Intrusion Prevention	
Item	Setting
▶ SYN Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ UDP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ ICMP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ Port Scan Detection	<input type="checkbox"/> Enable <input type="text" value="200"/> Packets/second (10~10000)
▶ Block Land Attack	<input type="checkbox"/> Enable
▶ Block Ping of Death	<input type="checkbox"/> Enable
▶ Block IP Spoof	<input type="checkbox"/> Enable
▶ Block TCP Flag Scan	<input type="checkbox"/> Enable
▶ Block Smurf	<input type="checkbox"/> Enable
▶ Block Traceroute	<input type="checkbox"/> Enable
▶ Block Fraggle Attack	<input type="checkbox"/> Enable
▶ ARP Spoofing Defence	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)

Intrusion Prevention		
項目	値設定	説明
SYN Flood Defense	1. 必須入力項目	Enable チェックボックスをクリックして、この侵入防止ルールを有効化し、このフィールドにトラフィックしきい値を入力します。
UDP Flood Defense	2. デフォルト値：チェックなし	Enable チェックボックスをクリックして、この侵入防止ルールを有効化し、このフィールドにトラフィックしきい値を入力します。
UDP Flood Defense	3. トラフィックしきい値は、デフォルト値：300 に設定されています	Enable チェックボックスをクリックして、この侵入防止ルールを有効化し、このフィールドにトラフィックしきい値を入力します。 <u>値の範囲</u> ： 10~10000。
Port Scan Defection	1. 必須入力項目	Enable チェックボックスをクリックして、この侵入防止ルールを有効化し、このフィールドにトラフィックしきい値を入力します。
	2. デフォルト値：チェックなし	Enable チェックボックスをクリックして、この侵入防止ルールを有効化し、このフィールドにトラフィックしきい値を入力します。
	3. トラフィックしきい値は、デフォルト値：200 に設定されています	<u>値の範囲</u> ： 10~10000。
Block Land Attack	デフォルト値：チェックなし	Enable チェックボックスをクリックして、この侵入防止ルールを有効化します。
Block Ping of Death	デフォルト値：チェックなし	Enable チェックボックスをクリックして、この侵入防止ルールを有効化します。

Block IP Spoof Block TCP Flag Scan Block Smurf Block Traceroute Block Fraggle Attack		
ARP Spoofing Defence	1.必須入力項目 2. デフォルト値：チェックボックスチェックなし 3.トラフィックしきい値は、デフォルト値：300 に設定されています	Enable チェックボックスをクリックして、この侵入防止ルールを有効化し、このフィールドにトラフィックしきい値を入力します。 <u>値の範囲</u> ：10～10000。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

5.2.4 オプション

Firewall Options		[Help]					
Item	Setting						
▶ Stealth Mode	<input type="checkbox"/> Enable						
▶ SPI	<input checked="" type="checkbox"/> Enable						
▶ Discard Ping from WAN	<input type="checkbox"/> Enable						

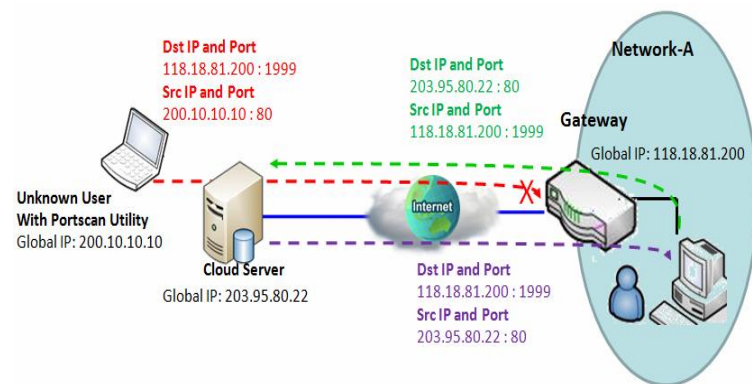
Remote Administrator Host Definition							
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
2	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
3	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
4	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
5	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit

このページには、さらに便利なファイアウォールオプションがいくつかあります。

「Stealth Mode」は、ゲートウェイがWANからのポートスキャンに回答しないようにするため、インターネット上での検出や攻撃の影響を受けにくくなります。「SPI」は、ゲートウェイがゲートウェイを通過する間に、ゲートウェイがIPアドレス、ポートアドレス、ACK、SEQ番号などのパケット情報を記録することを可能にし、ゲートウェイはすべての着信パケットをチェックしてこのパケットが有効かどうかを検出します。

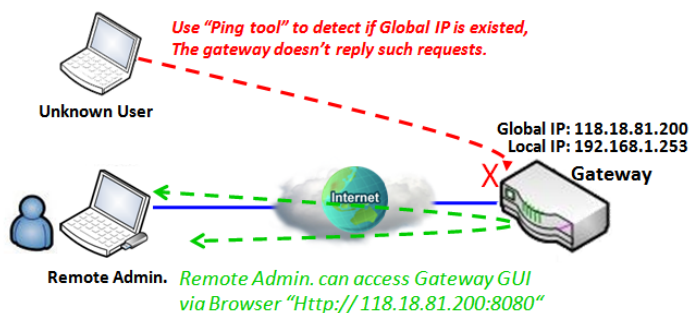
「Discard Ping from WAN (WANからのPingの破棄)」により、WAN側のホストが、このゲートウェイにpingを実行できなくなります。最後に、「Remote Administrator Hosts」を使用すると、リモートホストから管理タスクを実行することができます。この機能を有効にすると、指定したIPアドレスでのみリモート管理を実行できるようになります。

SPI 有効シナリオ



図に示すように、ゲートウェイの IP アドレスは、WAN インターフェイスについては、118.18.81.200、LAN インターフェイスについては、192.168.1.253 です。これは、NAT ゲートウェイとして機能します。ネットワーク-A のユーザーは、ゲートウェイ経由でクラウドサーバーにアクセスします。時々、未知のユーザーが、パケットをシミュレートしますが、異なるソース IP を使用してマスカレードします。SPI 機能をゲートウェイで有効化すると、未知のユーザーからのそのようなパケットがブロックされます。

WAN およびリモート管理者ホストの Ping を破棄するシナリオ



GUI にアクセスすることができます。

「Discard Ping from WAN (WAN からの Ping の破棄)」により、WAN 側のすべてのホストは、このゲートウェイが ICMP パケットに回答する ping を実行できなくなります。ローカルユーザーがインターネットをサーフィンしているときにセキュリティリークを防ぐために、「Discard Ping from WAN (WAN からの Ping の破棄)」機能を有効化します。

リモート管理者は、ゲートウェイのグローバル IP を知っており、TCP 8080 ポート経由でゲートウェイ

ファイアウォールオプション設定

Security > Firewall > Options タブに進みます。

ファイアウォールオプションの設定により、ネットワーク管理者はファイアウォールの動作を変更し、リモートルータのアクセス制御を有効化することができます。

ファイアウォールオプションの有効化

Firewall Options [Help]	
Item	Setting
▶ Stealth Mode	<input type="checkbox"/> Enable
▶ SPI	<input checked="" type="checkbox"/> Enable
▶ Discard Ping from WAN	<input type="checkbox"/> Enable

項目	値設定	説明
Stealth Mode	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、ステルスモード機能を有効化します。
SPI	デフォルト値：チェックあり	Enable チェックボックスにチェックを入れ、SPI 機能を有効化します
Discard PING from WAN	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、Discard PING from WAN（からの Ping の破棄）機能を有効化します。

リモート管理者ホストの定義

ルーターにより、ネットワーク管理者は、ルーターをリモート管理することができます。ネットワーク管理者は、特定の IP アドレスとサービスポートを割り当てて、ルーターにアクセスすることができます。

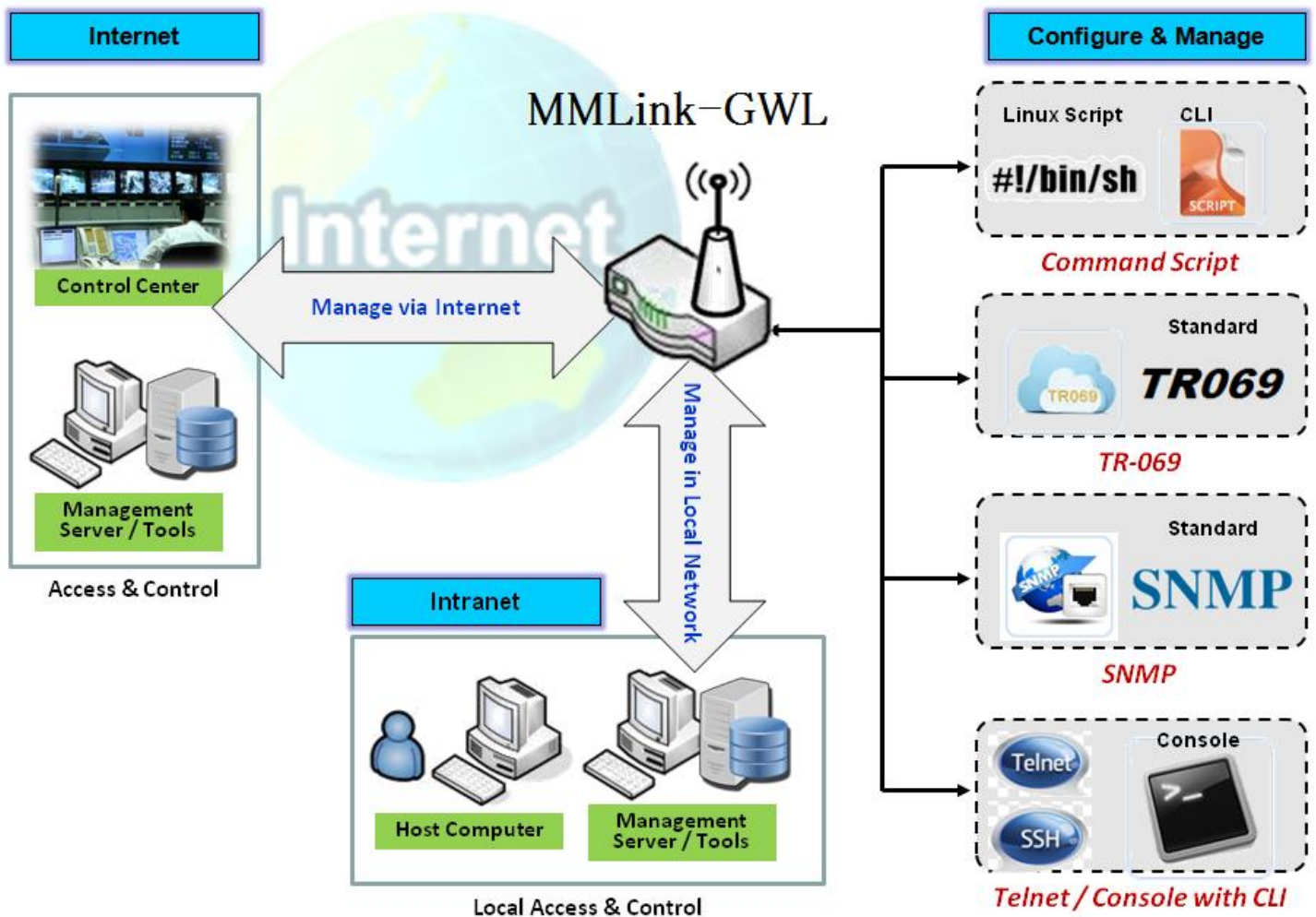
Remote Administrator Host Definition							
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
2	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
3	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
4	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
5	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit

項目	値設定	説明
Protocol	デフォルト値：HTTP	ルーターアクセスの場合、HTTP または HTTPS 方式を選択します。

IP	必須入力項目	<p>このフィールドは、リモートアクセスのアクセス権を割り当てるためのリモートホストを指定するためのフィールドです。</p> <p>すべてのリモートホストを許可するには、Any IP を選択します。</p> <p>特定のサブネットからのリモートホストを許可するには、Specific IP を選択します。IP アドレスを当フィールドに入力し、Subnet Mask でサブネット設定を選択してください。</p>
Service Port	<p>1. HTTP のデフォルト値：80</p> <p>2. HTTPS のデフォルト値：443</p>	<p>このフィールドは、サービスポートを HTTP または HTTPS 接続に指定するためのフィールドです。</p> <p><u>値の範囲</u>：1～65535。</p>
Enabling the rule	デフォルト値：チェックなし	Enable チェックボックスをクリックして、本ルールを有効化します。
Save	-	Enable チェックボックスをクリックして、本ルールを有効化し、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします

第 6 章 管理

6.1 設定および管理



設定と管理は、コンピュータシステムを含む（そして実際には実践的に）分散システムの企業全体の管理を指します。集中管理には、会社の規模、ITスタッフの専門知識、使用される技術の量に関連する時間と労力のトレードオフがあります。本製品は、Command Script（コマンドスクリプト）、TR-069、SNMP、Telnet with CLIなど、多くのシステム管理プロトコルをサポートしています。これらの設定は、「設定および管理」セッションで行うことができます。

6.1.1 コマンドスクリプト

コマンドスクリプト設定とは、管理者が事前定義された設定をプレーンテキスト形式で設定し、起動時に設定を適用できるようにするアプリケーションです。

Administration > Command Script > Configuration タブに進みます。

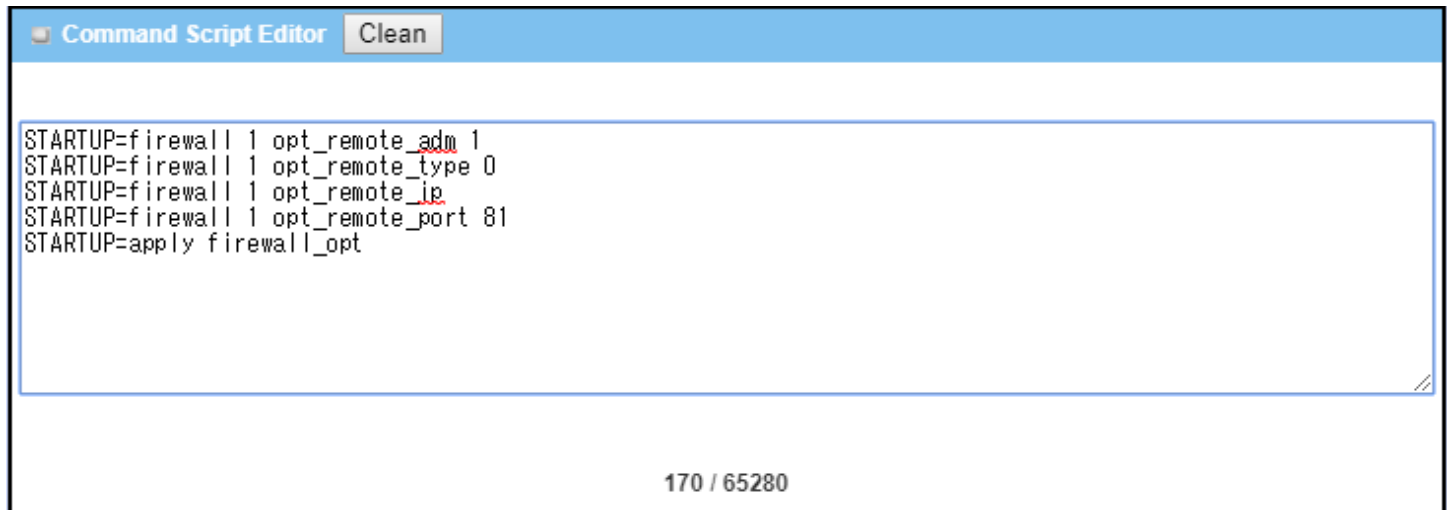
コマンドスクリプト設定の有効化

Configuration	
Item	Setting
▶ Command Script	<input type="checkbox"/> Enable
▶ Backup Script	Via Web UI
▶ Upload Script	Via Web UI
▶ Script Name	<input type="text"/>
▶ Version	<input type="text"/>
▶ Description	<input type="text"/>
▶ Update time	

Configuration 項目	値設定	説明
Configuration	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、Command Script 機能を有効化します。
Backup Script	-	[Via Web UI] または [Via Storage] ボタンをクリックして、既存のコマンドスクリプトを.txt ファイルにバックアップします。以下の [Script Name] で、スクリプトファイル名を指定することができます。
Upload Script	-	[Via Web UI] または [Via Storage] ボタンをクリックして、既存のコマンドスクリプトを指定した.txt ファイルからアップロードします。
Script Name	1.任意入力項目 2.有効ファイル名	スクリプトバックアップのスクリプトファイル名を指定するか、選択したアップロードスクリプトファイル名を表示します。 <u>値の範囲</u> ：1~64 文字。
Version	1.任意入力項目 2.文字列形式：任意	適用されたコマンドスクリプトのバージョン番号を指定します。 <u>値の範囲</u> ：1~64 文字
Description	1.任意入力項目 2.文字列形式：任意	適用されるコマンドスクリプトの簡単な説明を入力します。 <u>値の範囲</u> ：1~256 文字

Update time -	最後のコマンドスクリプトアップロードのアップロード時刻を記録します。
----------------------	------------------------------------

プレーンテキストコマンドスクリプトの編集/バックアップ



上記のように、設定ウィンドウでプレーンテキスト設定を編集することができます。

Plain Text Configuration		
項目	値設定	説明
Clean	-	テキストエリアをクリーンします。(すでに保存されている設定をさらにクリーンにするには、 Save ボタンをクリックしてください)。
Save	-	設定を保存します。

サポートされているプレーンテキスト設定の項目を次のリストに示します。標準の Linux コマンドで実行できる設定については、それらをスクリプトファイルに入れて、**STARTUP** コマンドで system configure に適用することができます。対応する Linux コマンドが設定されていない場合については、独自のコマンドセットで設定することができます。

Content of Plain Text Configuration		
キー	値設定	説明
OPENVPN_ENABLED	1 : 有効 0 : 無効	OpenVPN クライアント機能を有効または無効にします。
OPENVPN_DESCRIPTOR	必須入力項目	OpenVPN クライアント接続のトンネル名を指定します
OPENVPN_PROTO	udp tcp	OpenVPN クライアントの Protocol を定義します。 TCP または TCP/UDP を選択します。-> OpenVPN は、TCP プロトコルを使用し、 Port は 443 として自動的に設定されます。 UDP を選択します。-> OpenVPN は、UDP プロトコルを使用し、 Port は自動的に 1194 として設定されます。
OPENVPN_PORT	必須入力項目	使用する OpenVPN クライアントの Port を指定します。
OPENVPN_REMOTE_IPA	IP または FQDN	OpenVPN クライアントトンネルのピア OpenVPN サー

DDR		バーの Remote IP/FQDN を指定します。 IP アドレスまたは FQDN を入力します。
OPENVPN_PING_INTVL	秒	OpenVPN キープアライブチェックの時間間隔を指定します。
OPENVPN_PING_TOUT	秒	OpenVPN クライアントキープアライブチェックのタイムアウト値を指定します。
OPENVPN_COMP	Adaptive	OpenVPN クライアントの LZO 圧縮 アルゴリズムを指定します。
OPENVPN_AUTH	Static Key/TLS	OpenVPN トンネルの認証モードを指定します。 <ul style="list-style-type: none"> • TLS -> OpenVPN は、TLS 認証モード、および、以下の項目 CA Cert. (CA 証明書)、 Client Cert. (クライアント証明書)、および、 Client Key (クライアントキー) を指定する必要があります。
OPENVPN_CA_CERT	必須入力項目	OpenVPN クライアントの信頼済み CA 証明書を指定します。これは Base64 変換を経由します。
OPENVPN_LOCAL_CERT	必須入力項目	OpenVPN クライアントのローカル証明書を指定します。これは Base64 変換を経由します。
OPENVPN_LOCAL_KEY	必須入力項目	OpenVPN クライアントのローカルキーを指定します。これは Base64 変換を経由します。
OPENVPN_EXTRA_OPTIONS	Options	OpenVPN クライアントの追加オプション設定を指定します。
IP_ADDR1	Ip	イーサネット LAN IP
IP_NETM1	Net mask	イーサネット LAN マスク
PPP_MONITORING	1 : 有効 0 : 無効	ネットワーク監視機能が有効化されているとき、ルーターは、DNS クエリまたは ICMP を使って、インターネット接続 (接続中または切断中) を定期的に確認します。
PPP_PING	0 : DNS Query 1 : ICMP Query	DNS Query を使って、システムは、DNS クエリパケットを PPP_PING_IPADDR で指定される宛先に送信することにより、接続を確認します。 ICMP Query を使って、システムは、ICMP 要求パケットを PPP_PING_IPADDR において指定された宛先に送信することにより、接続を確認します。
PPP_PING_IPADDR	IP	DNS クエリ/ICMP 要求を送信するためのターゲットとして IP アドレスを指定します。
PPP_PING_INTVL	秒	2つの DNS クエリパケットまたは ICMP チェックパケット間の時間間隔を指定します。
STARTUP	Script file	標準の Linux コマンドで設定できる場合については、それらをスクリプトファイルに入れて、STARTUP コマンドでスクリプトファイルに適用することができます。 以下に例をあげます。 STARTUP=#!/bin/sh STARTUP=echo "startup done" > /tmp/demo

Telnet によるプレーンテキストシステム設定

前述の Web スタイルのプレーンテキスト設定に加えて、ゲートウェイシステムでは、Telnet CLI を使用した設定を行うことができます。管理者は、独自の telnet コマンド「txtConfig」と関連するアクション項目を使用して、単純なシステムを設定することができます。

コマンド形式は次のとおりです：txtConfig (action) [option]

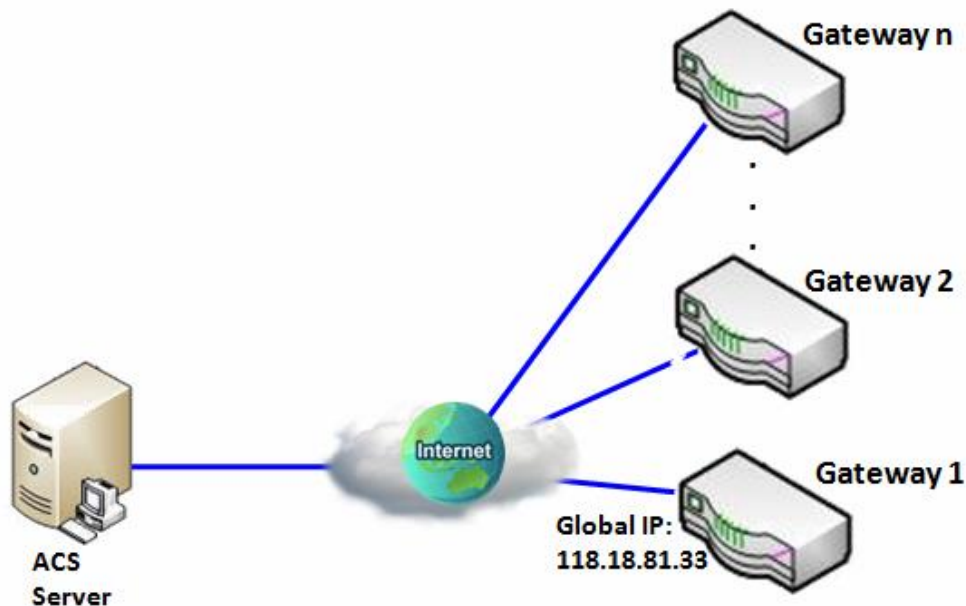
Action	オプション	説明
clone	Output file	設定コンテンツをデータベースから複製し、設定ファイルとして保管します。 (例：txtConfig clone /tmp/config) 設定ファイルの内容は、上記のプレーンテキストコマンドと同じです。このアクションは、「Backup」プレーンテキスト設定の実行とまったく同じです。
commit	既存のファイル	設定内容をデータベースにコミットします。 (例：txtConfig commit /tmp/config)
enable	-	プレーンテキストシステム設定を有効化します。 (例：txtConfig enable)
disable	-	プレーンテキストシステム設定を無効化します。 (例：txtConfig disable)
run_immediately	-	データベースでコミットされた設定内容を適用します。 (例：txtConfig run_immediately)
run_immediately	既存のファイル	適用する設定ファイルを割り当てます。 (例：txtConfig run_immediately /tmp/config)

6.1.2 TR-069

TR-069 (Technical Report 069) はBroadband Forumによる技術仕様で、CWMP (CPE WAN Management Protocol) と名付けられています。本ゲートウェイ製品のようなエンドユーザーデバイスのリモート管理に使用するアプリケーション層プロトコルを定義します。これは双方向のSOAP/HTTPベースプロトコルで、CPE (カスタマー構内設備) とACS (自動構成サーバー) を使用できます。セキュリティゲートウェイはこのCPEの一種です。

TR-069は、ISPのためにカスタマイズされた機能です。このため、設定を変更することはお勧めしません。この機能によるデバイス管理で問題が発生した場合は、ISPまたはACSプロバイダにお問い合わせください。TR-069設定画面の右上の隅には「Help」コマンドがあり、同じメッセージを表示することができます。

シナリオ-ACS サーバーを介して展開されたゲートウェイを管理する



シナリオの適用タイミング

企業データセンターで ACS サーバーを使用して、世界中の地理的に分散したリモートゲートウェイを管理する場合は、すべての支社のゲートウェイに ACS サーバーと通信するための TR-069 エージェントが組み込まれている必要があります。ACS サーバーが、これらのゲートウェイと対応するイントラネットを設定、FW アップグレード、および、監視できるようにします。

シナリオ説明

ACS サーバーは、最新の FW を使用して設定、アップグレードし、これらのゲートウェイを監視することができます。

リモートゲートウェイは、各時間帯にジョブを実行するように ACS サーバーに問い合わせます。

ACS サーバーは、ゲートウェイにいくつかの緊急ジョブを実行するように要求することができます。

パラメータの設定例

以下の表は、上図のゲートウェイ 1 の例として、「TR-069」を有効にしたパラメータ設定を示しています。

表に記載されていないパラメータには、デフォルト値を使用します。

Configuration Path	[TR-069]-[Configuration]
TR-069	■ <i>Enable</i>
ACS URL	http://qaysk.acslite.com/cpe.php
ACS User Name	<i>ACSUserName</i>
ACS Password	<i>ACSPassword</i>
ConnectionRequest Port	<i>8099</i>

ConnectionRequest User Name	<i>ConnReqUserName</i>
ConnectionRequest Password	<i>ConnReqPassword</i>
Inform	■ <i>Enable Interval 900</i>

シナリオ操作手順

上図では、ACS サーバーは、インターネット上の複数のゲートウェイを管理することができます。「Gateway 1」は、その1つで、WAN-1 インターフェイスの IP アドレスは、118.18.81.33 です。

すべてのリモートゲートウェイが起動すると、ACS サーバーに接続しようとします。

接続が正常に確立すると、ACS サーバーは、最新の FW を使用して設定、アップグレードを行い、これらのゲートウェイを監視することができます。

リモートゲートウェイは、各時間帯にジョブを実行するように ACS サーバーに問い合わせます。

ACS サーバーが、ゲートウェイにより、いくつかの緊急ジョブを実行する必要がある場合、それらのゲートウェイに「Connection Request」コマンドを発行します。そして、これらのゲートウェイは、緊急ジョブを実行するために、ACS サーバーの即時接続要求に応答して、即時接続を行います。

TR-069 設定

Administration > Configure & Manage > TR-069 タブに進みます。

「TR-069」ページには、TR-069 機能用の設定ウィンドウが1つしかありません。このウィンドウで、セキュリティゲートウェイが、ACS に接続するための関連情報を指定する必要があります。ACS サーバーの URL、ACS サーバーにログインするためのアカウント情報、ACS サーバーからの接続用のサービスポートとアカウント情報、および、ジョブ照会の時間間隔を指定することにより、機能を動作させます。照会時間以外は、次の照会サイクルまでは、ACS サーバーとゲートウェイの間に活動がありません。しかし、ACS サーバーにゲートウェイにより緊急に実行される予定の新しいジョブがある場合、問い合わせ要求のための即時接続の接続要求関連情報を使って、これらのゲートウェイに問い合わせます。

Configuration [Help]	
Item	Setting
▶ TR-069	<input type="checkbox"/> Enable
▶ Interface	WAN-1 ▼
▶ Data model	Standard ▼
▶ ACS URL	<input type="text"/>
▶ ACS UserName	<input type="text"/>
▶ ACS Password	<input type="text"/>
▶ Connection Request Port	8099
▶ Connection Request UserName	<input type="text"/>
▶ Connection Request Password	<input type="text"/>
▶ Inform	<input checked="" type="checkbox"/> Enable Interval <input type="text" value="300"/>
▶ Certification Setup	<input checked="" type="radio"/> default <input type="radio"/> Select from Certificate List Certificate: <input type="text" value="▼"/>

Configuration		
項目	値設定	説明
TR-069	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、TR-069 を有効化します。
Interface	デフォルト値： WAN-1	基本ネットワーク WAN-1 しか選択できません。Security > VPN > IPSec / OpenVPN / PPTP / L2TP / GRE の設定が完了したら、「IPSec #1」のように、IPSec / OpenVPN / PPTP / L2TP / GRE トンネル、インターフェイスを選択することができます。
Data Model	デフォルト値：Standard	リモート管理用の TR-069 データモデルを選択します。Standard：ACS Server は標準であり、TR-069 に完全に準拠しています。
ACS URL	必須入力項目	ACS 管理者に依頼し、ACS の URL を提供し、手動で設定することができます
ACS Username	必須入力項目	ACS 管理者に依頼し、ACS ユーザー名を提供し、手動で設定することができます
ACS Password	必須入力項目	ACS 管理者に依頼し、ACS パスワードを提供し、手動で設定することができます

ConnectionRequest Port	1.必須入力項目 2. デフォルト値 : 8099	ACS 管理者に依頼し、ACS 接続要求ポートを提供し、手動で設定することができます。 値の範囲 : 0~65535。
ConnectionRequest UserName	必須入力項目	ACS 管理者に依頼し、ACS 接続要求ユーザー名を提供し、手動で設定することができます
ConnectionRequest Password	必須入力項目	ACS 管理者に依頼し、ACS 接続要求パスワードを提供し、手動で設定することができます
Inform	1.デフォルト値 : チェックあり 2.デフォルトの間隔の値は 300 です	Enable チェックボックスにチェックを入れると、ゲートウェイ (CPE) は、Interval 設定に従って、定期的に ACS Server に通知メッセージを送信します。 値の範囲 : 情報間隔の場合、0~86400。
Certification Setup	デフォルト値 : default	デフォルトのままにするか、ドロップダウンリストから期待される証明書とキーを選択することができます。 証明書の構成については、Object Definition > Certificate のセクションを参照してください。
Save	-	Save をクリックして、設定を保存します。

ACS URL、ACS UserName、ACS Password を設定すると、ゲートウェイ (CPE、クライアントプレミアム機器) は ACS サーバーに通知を送信することができます。

ConnectionRequestPort、ConnectionRequestUserName、ConnectionRequestPassword を設定すると、ACS サーバーは、ACS サーバーに通知を送信するようゲートウェイ (CPE) に要求することができます。

STUN サーバ設定

STUN Settings [Help]	
Item	Setting
▶ STUN	<input checked="" type="checkbox"/> Enable
▶ Server Address	<input type="text"/>
▶ Server Port	<input type="text" value="3478"/> (1~65535)
▶ Keep Alive Period	<input type="text" value="0"/> (0~65535)second(s)

STUN Settings		
項目	値設定	説明
STUN	デフォルト値 : チェックあり	Enable チェックボックスにチェックを入れ、TR-069 を有効化します。
Server Address	1.文字列形式 : 任意の IPv4 アドレス 2.オプション項目	予想される STUN サーバーの IP アドレスを指定します。

Server Port	1.任意設定項目 2. デフォルト値： 3478	予想される STUN サーバーのポート番号を指定します。 <u>値の範囲</u> ：1～65535。
Keep Alive Period	1.任意設定項目 2. デフォルト値： 0	STUN サーバーとの接続のキープアライブ時間を指定します。 <u>値の範囲</u> ：0～65535。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、変更をキャンセルします。

6.1.3 SNMP

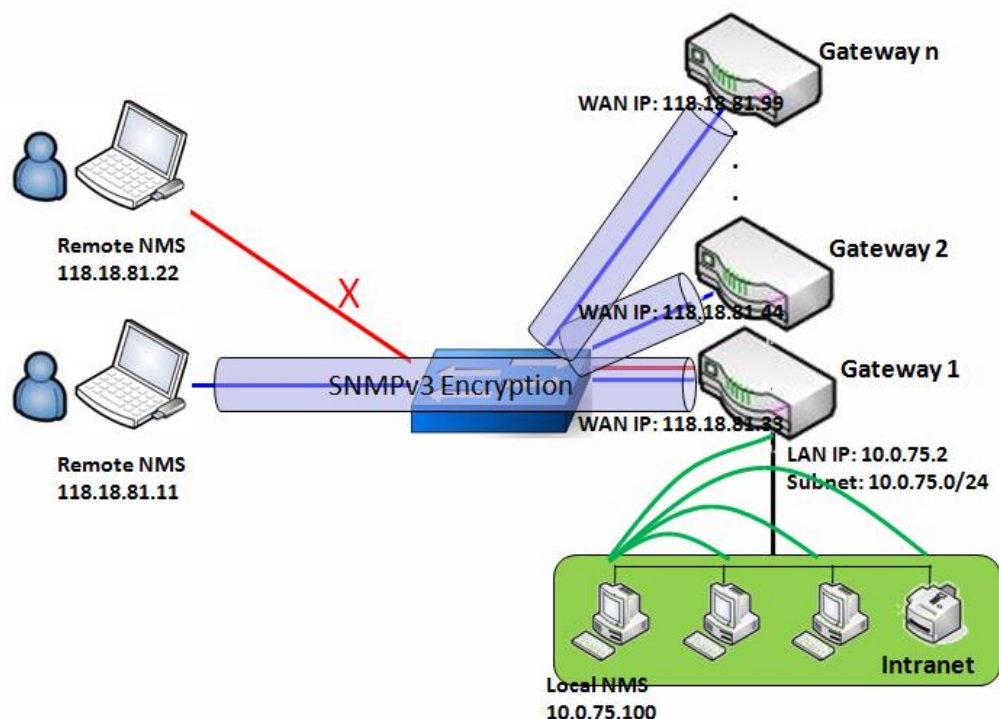
SNMP（簡易ネットワーク管理プロトコル）は、簡単に言えば、ユーザーが端末値のポーリングと設定、およびネットワークイベントの監視により、リモートでコンピュータネットワークを管理できるようにするためのプロトコルです。

一般的なSNMPの使用例では、1台または複数の管理用コンピュータ（マネージャ）が、コンピュータネットワークのホストやデバイスのグループの監視や管理を行います。管理対象システムは、エージェントと呼ばれるソフトウェアコンポーネントを常時実行し、SNMP経由で情報をマネージャに報告します。

SNMPエージェントは管理対象システムに関する管理データを変数として提供します。このプロトコルでは、これらの変数をリモートで変更することにより、アクティブな管理タスク（設定の変更と適用など）を実行することもできます。SNMP経由でアクセスできる変数は階層別にまとめられます。これらの階層やその他のメタデータ（変数の型や説明など）はMIB（管理情報ベース）に記述されています。

本製品ではSNMPエージェント用に複数の公開MIBと1つの非公開MIBを使用できます。使用できるMIBは次の通りです： MIB-II（RFC1213、IPv6を含む）、IF-MIB、IP-MIB、TCP-MIB、UDP-MIB、SMiv1およびSMiv2、SNMPv2-TMおよびSNMPv2-MIB

SNMP 管理シナリオ



シナリオの適用タイミング

SNMP ネットワーク管理システム (NMS) には、2つのアプリケーションシナリオがあります。ローカル NMS は、イントラネット上にあり、イントラネット内の SNMP プロトコルをサポートするすべてのデバイスを管理します。もう1つは、スイッチまたは UDP 転送機能を備えたルーターを使用して、WAN インターフェイスが相互に接続されているデバイスを管理する Remote NMS です。一部のデバイスを管理し、すべてが SNMP プロトコルをサポートしている場合は、アプリケーションシナリオの1つ、特にイントラネット内のデバイスの管理を使用してください。インターネットでデバイスを管理する場合、TR-069 がより良いソリューションです。最後のサブセクションを参照してください。

シナリオ説明

NMS サーバーは、SNMP プロトコルを使用して管理対象デバイスを監視および設定することができます。これらのデバイスは、UDP パケットが NMS から到達できる場所に配置されています。

管理対象デバイスは、緊急のトラップイベントを NMS サーバーに報告します。

プロトコルの SNMPv3 バージョンを使用すると、SNMP コマンドと応答の送信を保護することができます。

特権 IP アドレスを持つリモート NMS は、デバイスを管理できますが、他のリモート NMS は管理できません。

パラメータの設定例

次の表に、上図のゲートウェイ 1 の例として、LAN および WAN インターフェイスで「SNMP」を有効にした場合のパラメータ設定を示します。

表に記載されていないパラメータには、デフォルト値を使用します。

Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ LAN ■ WAN
Supported Versions	■ v1 ■ v2c ■ v3
Get/Set Community	読み取りコミュニティ/書き込みコミュニティ
Trap Event Receiver 1	118.18.81.11
WAN Access IP Address	118.18.81.11

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
User Name	UserName1	UserName2	UserName3
Password	Password1	Password2	Disable
Authetication	MD5	SHA-1	Disable
Encryption	DES	Disable	Disable
Privacy Mode	authPriv	authNoPriv	noAuthNoPriv
Privacy Key	12345678	Disable	Disable
Authority	Read/Write	Read	Read
Enable	■ Enable	■ Enable	■ Enable

シナリオ操作手順

上図では、NMS サーバーは、イントラネットまたは UDP 到達可能ネットワーク内の複数のデバイスを管理することができます。「Gateway 1」は、管理対象デバイスの 1 つであり、LAN インターフェイスでは 10.0.75.2、WAN-1 インターフェイスでは 118.18.81.33 の IP アドレスを持ちます。これは、NAT ルーターとして機能します。

最初の段階で、NMS マネージャは、すべての管理対象デバイスの関連情報を準備し、NMS システムに記録します。次に、NMS システムは、SNMP get コマンドを使用して、すべての管理対象デバイスのステータスを取得します。

管理者が、管理対象デバイスを設定したい場合、NMS システムで、SNMP set コマンドを使用して管理することができます。マネージャが、SNMPv3 プロトコルを使用して「Gateway 1」を設定する場合、「UserName1」アカウントが使用されます。アカウントの権限が「Read/Write」であるため、「UserName1」アカウントのみが、「Gateway 1」に NMS からの設定を受け入れることができます。

管理対象デバイスに緊急イベントを送信すると、デバイスはトラップイベントレシーバにトラップを発行します。NMS 自体は、その中にあります。

NMS と管理対象デバイス間で送信された SNMP コマンドと応答を保護する場合は、SNMPv3 バージョンのプロトコルを使用します。

特権 IP アドレスを持つ NMS のみ、「Gateway 1」を WAN インターフェイス経由で管理できるため、特権 IP アドレスを持たないリモート NMS は、「Gateway 1」を管理することができません。

SNMP Setting (SNMP 設定)

Administration > Configure & Manage > SNMP タブに進みます。

SNMP を使用すると、インターフェイス、バージョン、アクセス制御、トラップレシーバなどの SNMP 関連の設定をすることができます。

SNMP の有効化

Configuration	
Item	Setting
▶ SNMP Enable	<input type="checkbox"/> LAN <input type="checkbox"/> WAN
▶ WAN Interface	All WANs ▼
▶ Supported Versions	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input type="checkbox"/> v3
▶ SNMP Port	161
▶ Limited Remote Access IP	Specific IP Address ▼
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable
	<input type="text"/> (IP Address/FQDN) <input type="checkbox"/> Enable

SNMP 項目	値設定	説明
SNMP Enable	1. デフォルト値 : チェックなし	SNMP のインターフェイスを選択し、SNMP 機能を有効にします。 LAN チェックボックスにチェックを入れると、SNMP 機能が有効になり、LAN 側から SNMP にアクセスできます。 WAN チェックボックスにチェックを入れると、SNMP 機能が有効になり、WAN 側から SNMP にアクセスできます。
WAN Interface	デフォルト値 : All WANs	基本ネットワーク WAN-1~WAN-n の設定が完了したら、WAN-1~WAN-n を選択することができます。
Supported Versions	1. デフォルト値 v1 : チェックあり v2c : チェックあり	SNMP のバージョンを選択します。v1 チェックボックスにチェックが入っているとき。 バージョン 1 で、SNMP にアクセスすることができます。 v2 チェックボックスにチェックが入っているとき。 バージョン 2c で、SNMP にアクセスすることができます。 v3 チェックボックスにチェックが入っているとき。 バージョン 3 で、SNMP にアクセスすることができます。
SNMP Port	1. 文字列形式 : 任意のポート番号 2. SNMP ポートのデフォルト値 : 161 3. 必須入力項目	SNMP ポートを指定します。 任意のポート番号を入力することができます。しかし、ポート番号を使用しないようにする必要があります。 <u>値の範囲</u> : 1~65535。

Limited Remote Access IP	1.文字列形式：任意の Ipv4 アドレス 2. オプション項目	WAN のリモートアクセス IP を指定します。 Specific IP Address を選択し、1つの IP アドレスを指定して、WAN 側の指定 IP アドレスだけ SNMP にアクセスできます。 IP Range を選択し、IP アドレス範囲を指定して、WAN 側の指定範囲の IP アドレスだけ SNMP にアクセスできます。 設定を有効にするには、Enable をクリックします。 ブランクのままにしておくと、任意の IP アドレスが、WAN 側から SNMP にアクセスできることを意味します。
Save	-	Save をクリックして、設定を保存します
Undo	-	Undo をクリックして、設定をキャンセルします

複数コミュニティの作成/編集

SNMP を使用すると、バージョン 1 およびバージョン 2 のユーザーのアクセス制御をカスタマイズすることができます。ルーターは、最大 10 のコミュニティセットをサポートします。

Multiple Community List <input type="button" value="Add"/> <input type="button" value="Delete"/>			
ID	Community	Enable	Actions

Add ボタンがクリックされると、Multiple Community Rule Configuration ウィンドウが表示されます。

Multiple Community Rule Configuration	
Item	Setting
▶ Community	Read Only ▾ <input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

Multiple Community Rule Configuration		
項目	値設定	説明
Community	1. デフォルト値：Read Only 2. 必須入力項目 3. 文字列形式：任意のテキスト	バージョン 1 もしくはバージョン v2c ユーザーのコミュニティをそれぞれ指定します。それぞれ Read Only (GET and GETNEXT), Read-Write (GET, GETNEXT and SET) アクセスが許可されます。コミュニティの最大長は 32 です。
Enable	1. デフォルト値：チェックあり	有効にするには、Enable をクリックします。
Save	-	Save ボタンをクリックして、設定を保存します。しかし、SNMP 機能には適用されません。SNMP メインページに戻るとき、「Click on save button to apply your changes」(変更を適用)

		するには保存ボタンをクリックしてください) と表示され、メインページの Save ボタンをクリックするように促されます。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。
Back	-	Back ボタンをクリックして、最後のページに戻ります。

ユーザープライバシーの作成/編集

SNMP を使用すると、バージョン 3 のユーザーのアクセス制御をカスタマイズすることができます。ルーターは、最大 128 のユーザープライバシーセットをサポートします。

User Privacy List <input type="button" value="Add"/> <input type="button" value="Delete"/>										
ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

Add ボタンをクリックされると、User Privacy Rule Configuration 面が表示されます。

User Privacy Rule Configuration	
Item	Setting
▶ User Name	<input type="text"/>
▶ Password	<input type="password"/>
▶ Authentication	None ▼
▶ Encryption	None ▼
▶ Privacy Mode	noAuthNoPriv ▼
▶ Privacy Key	<input type="password"/>
▶ Authority	Read ▼
▶ OID Filter Prefix	<input type="text" value="1"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

User Privacy Rule Configuration		
項目	値設定	説明
User Name	1. 必須入力項目 2. 文字列形式：任意のテキスト	バージョン 3 ユーザーのユーザー名を指定します。 <u>値の範囲</u> ：1~32 文字。
Password	1. 文字列形式：任意のテキスト	Privacy Mode が authNoPriv または authPriv の場合、バージョン 3 ユーザーのパスワードを指定する必要があります。 <u>値の範囲</u> ：8~64 文字。
Authentication	1. デフォルト値： None	Privacy Mode が authNoPriv または authPriv の場合、バージョン 3 ユーザーの認証タイプを指定する必要があります。

Encryption	1. デフォルト値 : None	使用する認証タイプを MD5 / SHA-1 から選択します。 Privacy Mode が authPriv の場合、バージョン 3 ユーザーの暗号化プロトコルを指定する必要があります。 使用する暗号化プロトコルを DES / AES から選択します。
Privacy Mode	1. デフォルト値 : noAuthNoPriv	バージョン 3 ユーザーのプライバシーモードを指定します。 noAuthNoPriv : 認証タイプと暗号化プロトコルは使用しません。 authNoPriv : Authentication および Password を指定する必要があります。 authPriv : Authentication、Password、Encryption および Privacy Key を指定する必要があります。
Privacy Key	1. 文字列形式 : 任意のテキスト	Privacy Mode が authPriv の場合、バージョン 3 ユーザーのプライバシーキー (8~64 文字) を指定する必要があります。
Authority	1. デフォルト値 : Read	バージョン 3 ユーザーの権限をそれぞれ指定します。 Read Only (GET および GETNEXT) Read-Write (GET、GETNEXT および SET) アクセスを許可する、
OID Filter Prefix	1. デフォルト値 : 1 2. 必須入力項目 3. 文字列形式 : 任意の有効な OID	OID フィルタプレフィックスは、バージョン 3 ユーザーのアクセスを、指定された OID をルートとするサブツリーに制限します。 <u>値の範囲</u> : 1~2080768。
Enable	1. デフォルト値 : チェックあり	Enable をクリックして、バージョン 3 ユーザーを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。しかし、SNMP 機能には適用されません。SNMP メインページに戻るとき、「Click on save button to apply your changes」(変更を適用するには保存ボタンをクリックしてください) と表示され、メインページの Save ボタンをクリックするように促されます。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。
Back	-	Back ボタンをクリックして、最後のページに戻ります。

トラップイベントレシーバの作成/編集

SNMP を使用すると、トラップイベントレシーバをカスタム設定することができます。ルーターは、最大 4 つのトラップイベントレシーバセットをサポートします。

Trap Event Receiver List												
ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	Actions
<div style="display: flex; justify-content: space-between; align-items: center;"> Trap Event Receiver List Add Delete </div>												

Add ボタンをクリックされると、**Trap Event Receiver Rule Configuration** ウィンドウが表示されます。デフォルトの SNMP バージョンは v1 です。設定ウィンドウには、バージョン 1 の必須項目が表示されます。

Trap Event Receiver Rule Configuration	
Item	Setting
▶ Server IP	<input type="text"/> (IP Address/FQDN)
▶ Server Port	<input type="text" value="162"/>
▶ SNMP Version	v1 ▼
▶ Community Name	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

v2c を選択すると、設定ウィンドウはバージョンを除いて、v1 とまったく同じになります。

v3 を選択すると、設定ウィンドウにバージョン 3 トラップの設定項目が追加されます。

Trap Event Receiver Rule Configuration	
Item	Setting
▶ Server IP	<input type="text"/> (IP Address/FQDN)
▶ Server Port	<input type="text" value="162"/>
▶ SNMP Version	v3 ▼
▶ Community Name	<input type="text"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Privacy Mode	noAuthNoPriv ▼
▶ Authentication	None ▼
▶ Encryption	None ▼
▶ Privacy Key	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

Trap Event Receiver Rule Configuration(v1,v2)

Trap Event Receiver Rule Configuration(v3)

項目	値設定	説明
Server IP	1. 必須入力項目 2. 文字列形式：任	トラップサーバーIP を指定します。 DUT はサーバーIP にトラップを送信します。

	意の Ipv4 アドレス	
Server Port	1.文字列形式：任意のポート番号 2. SNMP トラップポートデフォルト値：162 3.必須入力項目	トラップサーバーポートを指定します。 任意のポート番号を入力することができます。しかし、このポート番号が使用されないようにする必要があります。 <u>値の範囲</u> ：1～65535。
SNMP Version	デフォルト値：v1	トラップのバージョンを選択します。v1 を選択すると、設定ウィンドウには、バージョン 1 の必須項目が表示されます。 v2c を選択すると、設定ウィンドウには、バージョン 2c の必須項目が表示されます。 v3 を選択すると、設定ウィンドウには、バージョン 3 の必須項目が表示されます。
Community Name	1.v1 および v2c 必須入力項目 2. 文字列形式：任意のテキスト	バージョン 1 または v2c のトラップのコミュニティ名を指定します。 <u>値の範囲</u> ：1～32 文字。
User Name	1.v3 を入力しなければなりません 2. 文字列形式：任意のテキスト	バージョン 3 のトラップのユーザー名を指定します。 <u>値の範囲</u> ：1～32 文字。
Password	1.v3 を入力しなければなりません 2. 文字列形式：任意のテキスト	Privacy Mode が authNoPriv または authPriv の場合、バージョン 3 のトラップのパスワードを指定する必要があります。 <u>値の範囲</u> ：8～64 文字。
Privacy Mode	1.v3 を入力しなければなりません 2. デフォルト値：noAuthNoPriv	バージョン 3 のトラップのプライバシーモードを指定します。 noAuthNoPriv： 認証タイプと暗号化プロトコルは使用しません。 authNoPriv： Authentication および Password を指定する必要があります。 authPriv： Authentication、Password、Encryption および Privacy Key を指定する必要があります。
Authentication	1.v3 を入力しなければなりません 2. デフォルト値：None	Privacy Mode が authNoPriv または authPriv の場合、バージョン 3 のトラップの認証タイプを指定する必要があります。 使用する認証タイプを MD5 / SHA-1 から選択します。
Encryption	1.v3 を入力しなければなりません 2. デフォルト値：None	Privacy Mode が authPriv の場合、バージョン 3 のトラップの暗号化プロトコルを指定する必要があります。 使用する暗号化プロトコルを DES / AES から選択します。
Privacy Key	1.v3 を入力しなければなりません	Privacy Mode が authPriv の場合、バージョン 3 のトラップのプライバシーキー (8～64 文字) を指定する必要があります。

	2. 文字列形式：任意のテキスト	
Enable	デフォルト値：チェックあり	Enable をクリックして、トラップレシーバを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。しかし、SNMP 機能には適用されません。SNMP メインページに戻るとき、「Click on save button to apply your changes」（変更を適用するには保存ボタンをクリックしてください）と表示され、メインページの Save ボタンをクリックするように促されます。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。
Back	-	Back ボタンをクリックして、最後のページに戻ります。

SNMP MIB-2 システムの指定

必要に応じて、MIB-2 システムに必要な情報を指定することもできます。

SNMP MIB-2 System	
Item	Setting
▶ sysContact	<input type="text"/>
▶ sysLocation	<input type="text"/>

SNMP MIB-2 System		
項目	値設定	説明
sysContact	1.任意入力項目 2. 文字列形式：任意のテキスト	MIB-2 システムの連絡先情報を指定します。 <u>値の範囲</u> ：0～128 文字。
sysLocation	1.任意入力項目 2. 文字列形式：任意のテキスト	MIB-2 システムの位置情報を指定します。 <u>値の範囲</u> ：0～128 文字。

SNMP オプションの編集

特定のプライベート MIB を使用する場合は、企業名、番号、および OID を入力する必要があります。

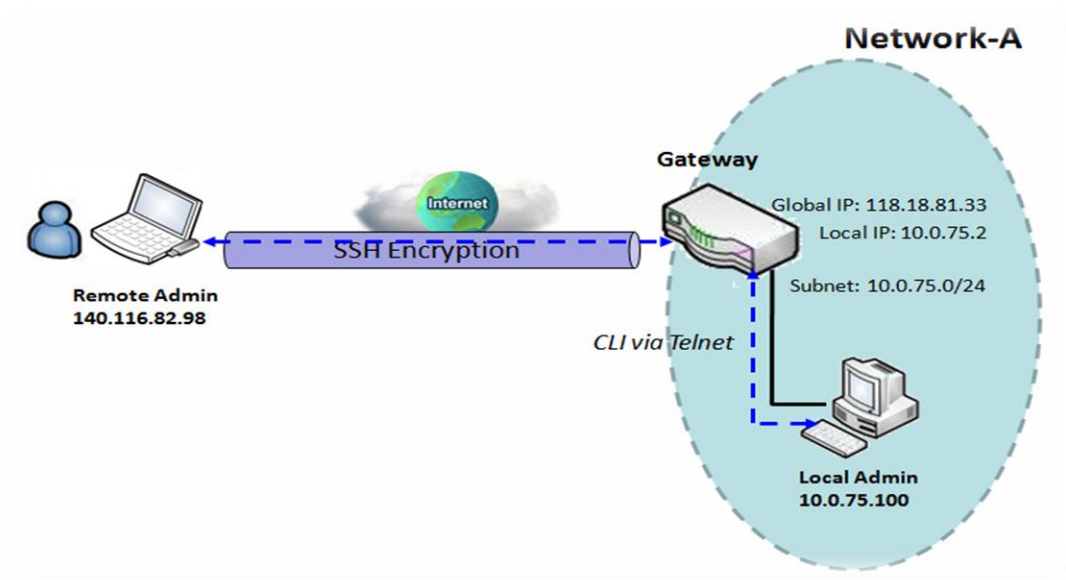
Options	
Item	Setting
▶ Enterprise Name	<input type="text" value="YSK"/>
▶ Enterprise Number	<input type="text" value="14733"/>
▶ Enterprise OID	1.3.6.1.4.1. <input type="text" value="14733"/>

Options		
項目	値設定	説明
Enterprise Name	1.デフォルト値 : YSK 2. 必須入力項目 3.文字列形式 : 任意のテキスト	特定のプライベート MIB の企業名を指定します。 <u>値の範囲</u> : 1~10 文字、A~Z、a~z、0~9、「-」、「_」
Enterprise Number	1.デフォルト値 : 14733 (YSK の企業番号) 2. 必須入力項目 3.文字列形式 : 任意の数字	特定のプライベート MIB の企業番号を指定します。 <u>値の範囲</u> : 1~2080768。
Enterprise OID	1.デフォルト値 : 1.3.6.1.4.1.14733 (YSK の企業 OID) 2. 必須入力項目 3.文字列形式 : 任意の有効な OID	特定のプライベート MIB の企業 OID を指定します。 各 OID 番号の範囲は 1~2080768 です。 企業 OID の最大長は 31 です。 7 番目の番号は、企業番号と同一でなければなりません。
Save	-	Save ボタンをクリックして設定を保存し、変更を SNMP 機能に適用します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

6.1.4 Telnet & SSH

コマンドラインインターフェイス (CLI) はコマンドラインユーザーインターフェイス、コンソールユーザーインターフェイスとも呼ばれています。これはコンピュータプログラムを操作する方法のひとつで、ユーザー (またはクライアント) がプログラムに対して、連続するテキスト行 (コマンドライン) の形式でコマンドを実行します。このインターフェイスには通常コマンドラインシェルが実装されています。これは、コマンドをテキスト入力として受け取り、所定のオペレーティングシステムの機能に変換します。一般的に、コマンドラインインターフェイスがあるプログラムの方が、スクリプトによる自動化が簡単にできます。本製品では Telnet と SSH (Secure Shell) CLI の両方が使用できます。デフォルトのサービスポートはそれぞれ 23 と 22 です。

Telnet および SSH のシナリオ



シナリオの適用タイミング

ゲートウェイ管理者が、イントラネットまたはインターネットのリモートサイトから管理する場合、「Telnet」または「SSH」ユーティリティを使用して、「Telnet & SSH」機能を使用することができます。

シナリオ説明

ローカル管理者またはリモート管理者は、特権ユーザー名とパスワードで、「Telnet」または「SSH」ユーティリティを使用して、ゲートウェイを管理することができます。

ローカル管理者とゲートウェイ間、または、リモート管理者とゲートウェイ間のデータパケットは、プレーンテキストまたは暗号化されたテキストにすることができます。ローカル管理者用のイントラネットでは、「Telnet」ユーティリティを使用するプレーンテキストであり、リモート管理者用の暗号化されたテキストは、「SSH」ユーティリティを使用することを推奨します。

パラメータの設定例

次の表に、上図のゲートウェイ 1 の例として、LAN および WAN インターフェイスで「Telnet」を有効にした場合のパラメータ設定を示します。

表に記載されていないパラメータには、デフォルト値を使用します。

Configuration Path	[Telnet & SSH]-[Configuration]
Telnet	LAN : ■ Enable WAN : ■ Enable
Connection Type	Telnet : サービスポート 23 ■ Enable SSH : サービスポート 22 ■ Enable

シナリオ操作手順

上図では、「ローカル管理者」または「リモート管理者」が、イントラネットまたはインターネットの「ゲートウェイ」を管理することができます。「ゲートウェイ」は、ネットワーク-Aのゲートウェイであり、イントラネットのサブネットは 10.0.75.0/24 です。これは、LAN インターフェイスに対して 10.0.75.2、WAN-1 インターフェイスに対して 118.18.81.33 の IP アドレスを持っています。これは、NAT ゲートウェイとして機能します。

イントラネットの「ローカル管理者」は、特権アカウントで「Telnet」ユーティリティを使用して、ゲートウェイにログインします。

または、インターネットの「リモート管理者」は、特権アカウントで「SSH」ユーティリティを使用して、ゲートウェイにログインします。

ゲートウェイ管理者は、ゲートウェイの前にいるかのようにデバイスを制御することができます。

Telnet & CLI 設定

Administration > Configure & Manage > Telnet & SSH タブに進みます。

Telnet & SSH 設定により、管理者は従来の Telnet プログラムを通じて本製品にアクセスすることができます。端末に Telnet (ログイン) する前に、関連する設定とパスワードを慎重に設定してください。パスワード管理部分では、Telnet と SSH のログインに root パスワードを設定することができます。

Configuration	
Item	Setting
▶ Telnet	LAN <input checked="" type="checkbox"/> Enable WAN <input type="checkbox"/> Enable Service Port <input type="text" value="23"/>
▶ SSH	LAN <input type="checkbox"/> Enable WAN <input type="checkbox"/> Enable Service Port <input type="text" value="22"/>

Configurations		
項目	値設定	説明
Telnet	デフォルト値： LAN Enable : チェックあり WAN Enable : チェックなし Service Port : 23	Enable ボックスにチェックを入れ、Telnetサービスを有効します。対応するサービスを提供する Service Port の数を設定することができます。 値の範囲 : 1~65535。

SSH	デフォルト値 : LAN Enable : チェックなし WAN Enable : チェックなし Service Port : 22	Enable ボックスにチェックを入れ、SSHサービスを有効します。対応するサービスを提供する Service Port の数を設定することができます。 値の範囲 : 1~65535。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします。

■ Password Management
Save
Undo

Item	Setting
▶ root	Old Password : <input style="width: 150px;" type="text"/> New Password : <input style="width: 150px;" type="text"/> New Password Confirmation : <input style="width: 150px;" type="text"/>

Password Management		
項目	値設定	説明
root	1.文字列：任意のテキスト（空白文字を含みません） 2. Telnet のデフォルトパスワード： 「m2mysk」	古いパスワードを新しいパスワードを入力して、rootパスワードを変更します。 注：本製品デバイスを展開する前に、デフォルトの Telnet パスワードを変更することを強くお勧めします。
Save	-	Save をクリックして、設定を保存します。
Undo	-	Undo をクリックして、設定をキャンセルします。

6.2 システム操作

システム操作により、ネットワーク管理者は、アクセスパスワードの変更、システム情報、システム時刻、システムログ、ファームウェア/設定のバックアップと復元、リセットおよび再起動などのシステム設定を管理することができます。

6.2.1 パスワードおよび MMI

Administration > System Operation > Password & MMI タブに進みます。

ホスト名の設定

ホスト名画面では、ネットワーク管理者は、ゲートウェイのホスト名を設定/変更できます。

Host Name	
Item	Setting
▶ Host Name	<input type="text"/>

Host Name		
項目	値設定	説明
Host Name	1.オプション項目 2.デフォルト値： MMLink-GWL	ゲートウェイのホスト名を入力します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

ユーザ名の変更

ユーザ名画面では、ネットワーク管理者は Web ベースの MMI ログインアカウントをアクセスゲートウェイに変更できます。[Modify]ボタンをクリックし、新しいユーザー名設定を入力します。

Username	
Item	Setting
▶ Username	admin <input type="button" value="Modify"/>
▶ New Username	<input type="text"/>
▶ Password	<input type="text"/>

Username		
項目	項目	項目
Username	デフォルト値： admin	現在のログインアカウント（ユーザー名）を表示します。
New Username	文字列：任意のテキスト	新しいユーザー名を入力して、現在の設定を置き換えます。
Password	文字列：任意のテキスト	現在のパスワードを入力して、ユーザー名の設定を変更する権限があるかどうかを確認します。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

パスワードの変更

パスワード変更ウィンドウでは、ネットワーク管理者は、Web ベースの MMI ログインパスワードをアクセスゲートウェイに変更することができます。

Password [Help]	
Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ New Password Confirmation	<input type="text"/>

Password		
項目	値設定	説明
Old Password	1.文字列：任意のテキスト 2. Web ベースの MMI のデフォルトパスワード：「admin」	現在のパスワードを入力します。
New Password	文字列：任意のテキスト	新パスワードを入力します
New Password Confirmation	文字列：任意のテキスト	確認のため、再度新パスワードを入力します
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

アクセスのための MMI 設定の変更

これは、管理者が管理のためにゲートウェイにアクセスできるようにするゲートウェイの Web ベースの MMI アクセスです。ゲートウェイの Web ベースの MMI は、アイドル時間が経過すると自動的にログアウトします。この設定により、管理者は自動ログアウトを有効にし、ログアウトアイドル時間を設定することができます。ログインタイムアウトを無効にすると、システムは管理者を自動的にログアウトしません。

MMI [Help]	
Item	Setting
▶ Login	Password-Guessing Attack & MAX: <input type="text" value="3"/> (times)
▶ Login Timeout	<input checked="" type="checkbox"/> Enable <input type="text" value="300"/> (seconds)
▶ GUI Access Protocol	<input type="text" value="http/https"/> ▼
▶ HTTPs Certificate Setup	<input checked="" type="radio"/> default <input type="radio"/> Select from Certificate List Certificate: <input type="text"/> ▼ Key: <input type="text"/> ▼
▶ HTTP Compression	<input type="checkbox"/> gzip <input type="checkbox"/> deflate
▶ HTTP Binding	<input checked="" type="checkbox"/> DHCP 1
▶ System Boot Mode	<input type="text" value="Normal Mode"/> ▼

Web UI 項目	値設定	説明
Login	デフォルト値 : 3 回	ログイン試行カウント値を入力します。 <u>値の範囲</u> : 3~10。 誤ったパスワードで Web GUI にログインがカウント値を超えると「 <i>Already reaching maximum Password-Guessing times, please wait a few seconds!</i> (すでに最大パスワード試行回数に達しています。数秒お待ちください!)」という警告メッセージが表示され、次のログイン試行は無視されます。
Login Timeout	デフォルト値 : Enable にチェックなし	Enable チェックボックスにチェックを入れ、自動ログアウト機能を有効化し、最大アイドル時間を指定します。 <u>値の範囲</u> : 30~65535。
GUI Access Protocol	デフォルト値 : http/https	GUI アクセスに使用するプロトコルを選択します。 http/https 、 http only 、 https only が可能です。
HTTPs Certificate Setup	デフォルト値 : default	[https Access Protocol] が選択されている場合は、HTTPs Certificate Setup オプションを使用して、さらに構成を行うことができます。 デフォルトのままにするか、ドロップダウンリストから期待される証明書とキーを選択することができます。

		証明書の構成については、Object Definition > Certificate のセクションを参照してください。
HTTP Compression	デフォルト値：チェックなし	任意の圧縮方法が望ましい場合は、ボックス（gzip または deflate）をチェックします。
HTTP Binding	1. オプション項目 2. デフォルト値：「DHCP-1」チェックあり	http アクセスでバインドする DHCP サーバーを選択します。
System Boot Mode	1. デフォルト値：Normal Mode	システムを起動するために採用されるシステム起動モードを選択します。 Normal Mode: 起動時間が約 70 秒と長くなり、デバイスの起動中に完全なファームウェアイメージチェックが行われます。 Fast Mode: デバイスの起動中にファームウェアイメージを確認することなく、起動時間が約 50 秒短縮されます。
Save	-	Save ボタンをクリックして、設定を保存します。
Undo	-	Undo ボタンをクリックして、設定をキャンセルします。

6.2.2 システム情報

ネットワーク管理者は、**System Information** ウィンドウで、使用されている WAN 接続の種類をすばやく調べることができます。ディスプレイには、現在のシステム時刻も表示されます。これはファームウェアがアップグレードされ、システム設定ファイルがロードされたときに特に便利です。

Administration > System Operation > System Information タブに進みます。

System Information	
Item	Setting
▶ Model Name	IDG500YK-0T001
▶ Device Serial Number	ZZ18700013
▶ Kernel Version	2.6.36
▶ FW Version	0BZ01X0.IA2_uA5.0BZ0_01141500
▶ System Time	Mon, 21 Jan 2019 20:11:34 +0900
▶ Device Up-Time	3day 2hr 46min 12sec

システム情報		
項目	値設定	説明
Model Name	-	本製品のモデル名が表示されます。
Device Serial Number	-	本製品のシリアル番号が表示されます。
Kernel Version	-	製品の Linux カーネルバージョンが表示されます
FW Version	-	製品のファームウェアバージョンが表示されます
Memory Usage	-	デバイスのメモリ率をパーセントで表示します。
System Time	-	この Web ページを閲覧した現在のシステム時刻を表示します。
Device Up-Time	-	前回の起動以降のデバイスの稼働時間の統計情報が表示されません。
Refresh	-	[Refresh] ボタンをクリックして、直ちにシステム情報を更新します。

6.2.3 システム時刻

ゲートウェイは、管理者がゲートウェイのシステム時刻を設定するために、手動で設定および自動同期化された方法を提供します。サポートされる時刻は、[Time Server]、[Manual]、[PC]、[Cellular Module] のいずれかです。最初に方法を選択し、次に残りの設定を構成します。

ゲートウェイのシステム時刻を手動で設定するのではなく、正しい時刻情報を設定してゲートウェイのシステム時刻として設定する簡単で迅速なソリューションが2つあります。

1つ目は「Sync with Timer Server（タイマーサーバーとの同期）」です。上記の時刻情報設定ウィンドウでのタイムゾーンとタイムサーバーの選択に基づいて、**Sync with Timer Server** ボタンをクリックすると、システムは NTP プロトコルでタイムサーバーと通信し、システムの日付と時刻を取得します。

2つ目は「Sync with my PC（自分の PC と同期する）」です。**Sync with my PC** ボタンをクリックすると、システムが日付と時刻を管理 PC の時刻に同期させます。

[Administration（管理）] > [System Operation（システム操作）] > [System Time（システム時刻）] タブに進みます。

タイムサーバーと同期する

System Time Configuration	
Item	Setting
▶ Synchronization method	Time Server ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ Auto-synchronization	Time Server: <input type="text"/> Available Time Servers (RFC-868): Auto ▼
▶ Daylight Saving Time	<input type="checkbox"/> Enable
▶ Synchronize immediately	Active

システム時刻情報

項目	項目	項目
Synchronization method	1. 必須入力項目 2. デフォルト値 : Manual	システム時刻の同期方法として Time Server を選択します。
Time Zone	1. オプション項目 2. デフォルト値 : GMT+09 :00	デバイスの所在地のタイムゾーンを選択します。

Auto-Synchronization (自動同期)	1. 必須入力項目 2. デフォルト値 : Auto	Enable ボタンにチェックを入れ、特定の NTP サーバーで時刻自動同期機能を有効します。 利用可能なサーバーが1つずつ時刻同期に使用されるよう、NTP サーバーの IP または FQDN を入力するか、または、自動モードのままにします。
Daylight Saving Time (夏時間)	1. オプション項目 2. デフォルト値 : チェックなし	Enable ボタンにチェックを入れ、夏時間機能を有効します。 この機能を有効にする際、夏時間の開始日と終了日を指定する必要があります。
NTP Service	1. オプション項目 2. デフォルト値 : チェックなし	[Enable] ボタンにチェックを入れ、NTP Service (NTP サービス) 機能を有効します。 この機能を有効にすると、ゲートウェイは、ローカルに接続されたデバイスに NTP サーバーサービスを提供できます。
Synchronize immediately (即時同期)	N/A	[アクティブ] ボタンをクリックすると、指定されたタイムサーバーとシステム時刻を即座に同期させることができます。
Save (保存)	-	Save ボタンをクリックして、設定を保存します。
Refresh (更新)	-	Refresh ボタンをクリックして、直ちにシステム時刻を更新します。

注：デバイスの正しいタイムゾーンを選択することを忘れないでください。そうしないと、デバイスの現地時間ではなく、UTC（協定世界時）の時刻が取得されます。

手動で設定と同期する

System Time Configuration	
Item	Setting
▶ Synchronization method	Manual ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ Daylight Saving Time	<input type="checkbox"/> Enable
▶ Set Date & Time Manually	2018 ▼ / January ▼ / 09 ▼ (Year/Month/Day)
	15 ▼ : 37 ▼ : 58 ▼ (Hour:Minute:Second)
▶ NTP Service	<input type="checkbox"/> Enable

システム時刻情報		
項目	項目	項目
Synchronization method	1. 必須入力項目 2. デフォルト値 : Manual	システム時刻の同期方法として、[Manual] を選択します。これは、管理者が手動で日付と時刻を設定する必要があることを意味します。

Time Zone	1.オプション項目 2. デフォルト値： GMT+09 :00	デバイスの所在地のタイムゾーンを選択します。
Daylight Saving Time	1.オプション項目 2. デフォルト値： チェックなし	Enable ボタンにチェックを入れ、夏時間機能を有効します。 この機能を有効にする際、夏時間の開始日と終了日を指定する必要があります。
Set Date & Time Manually	オプション項目	時間自動同期機能を有効にしない場合は、日付（年/月/日）と時刻（時：分：秒）を手動で設定することもできます。
NTP Service	1.オプション項目 2. デフォルト値： チェックなし	[Enable] ボタンにチェックを入れ、NTP Service（NTP サービス）機能を有効します。 この機能を有効にすると、ゲートウェイは、ローカルに接続されたデバイスに NTP サーバーサービスを提供できます。
Save	-	Save ボタンをクリックして、設定を保存します。

PC と同期する

System Time Configuration	
Item	Setting
▶ Synchronization method	PC ▼
▶ NTP Service	<input type="checkbox"/> Enable
▶ Synchronize immediately	Active

システム時刻情報		
項目	値設定	説明
Synchronization method	1.必須入力項目 2. デフォルト値： Manual	システム時刻の同期方法として [PC] を選択すると、システムが日付と時刻を管理 PC の時刻に同期させます。
NTP Service	1.オプション項目 2. デフォルト値： チェックなし	[Enable] ボタンにチェックを入れ、NTP Service（NTP サービス）機能を有効します。 この機能を有効にすると、ゲートウェイは、ローカルに接続されたデバイスに NTP サーバーサービスを提供できます。
Synchronize immediately	-	[Active] ボタンをクリックすると、指定されたタイムサーバーとシステム時刻を即時に同期させることができます。
Save	-	[Save] ボタンをクリックして、設定を保存します。
Refresh	-	[Refresh] ボタンをクリックして、直ちにシステム時刻を更新します。

セルラータイムサービスと同期する

System Time Configuration	
Item	Setting
▶ Synchronization method	Cellular Module ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ NTP Service	<input type="checkbox"/> Enable
▶ Synchronize immediately	Active

システム時刻情報		
項目	値設定	説明
Synchronization method	1. 必須入力項目 2. デフォルト値 : Manual	接続されたモバイル ISP から提供される時刻にシステムが日付と時刻を同期させるために、システム時刻の同期方法として、[Cellular Module (セルラーモジュール)] を選択します。 注 : このオプションは、Cellular WAN インターフェイスを備えた製品でのみ使用できます。
Time Zone	1. 必須入力項目 2. デフォルト値 : GMT+09 :00	デバイスの所在地のタイムゾーンを選択します。
NTP Service	1. オプション項目 2. デフォルト値 : チェックなし	[Enable] ボタンにチェックを入れ、NTP Service (NTP サービス) 機能を有効します。 この機能を有効にすると、ゲートウェイは、ローカルに接続されたデバイスに NTP サーバーサービスを提供できます。
Synchronize immediately	-	[Active] ボタンをクリックすると、指定されたタイムサーバーとシステム時刻を直ちに同期させることができます。
Save	-	[Save] ボタンをクリックして、設定を保存します。
Refresh	-	[Refresh] ボタンをクリックして、直ちにシステム時刻を更新します。

6.2.4 システムログ

System Log ウィンドウには、ネットワーク管理者がローカルイベントロギングとリモートレポートを実行する為の、さまざまなイベントログツールが用意されています。

Administration > System Operation > System Log タブに進みます。

System Log	
Item	Setting
▶ Web Log Type Category	<input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Login message <input type="checkbox"/> Debug
▶ Email Alert	<input type="checkbox"/> Enable Server: <input type="text" value="--- Option ---"/> <input type="button" value="Add Object"/> E-mail Addresses: <input type="text"/> Subject: <input type="text"/> Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug
▶ Syslogd	<input type="checkbox"/> Enable Server: <input type="text" value="--- Option ---"/> <input type="button" value="Add Object"/> Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug
▶ Log to Storage	<input type="checkbox"/> Enable Select Device: <input type="text" value="Internal"/> Log file name: <input type="text" value="syslog"/> Split file: <input type="checkbox"/> Enable Size: <input type="text" value="200"/> <input type="text" value="KB"/> Interval: <input type="checkbox"/> Enable <input type="text" value="1440"/> (1 ~ 10080 Minutes) Max Records: <input type="text" value="3000"/> (5~10000) <input type="button" value="Download log file"/> <input type="button" value="clear logs"/> Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug

ログ履歴の表示および E メール

ネットワーク管理者がゲートウェイのログ履歴を表示する為に、**View** ボタンが用意されています。インスタント E メールを分析用に送信する場合は、**Email Now** ボタンを使用します。

System Log View / EmailNow		
項目	値設定	説明
View button	-	View ボタンをクリックすると、Web Log List ウィンドウにログ履歴が表示されます。
Email Now Button	-	Email Now ボタンをクリックすると、直ちに E メール経由でログ履歴が送信されます。

Web Log List	
Time	Log
Dec 2 18:38:23	kernel: klogd started: BusyBox v1.3.2 (2015-10-29 12:52:33 CST)
Dec 2 18:38:33	BEID: BEID STATUS : 0 , STATUS OK!
Dec 2 18:38:40	commander: NETWORK Initialization finished. Result: 0
Dec 2 18:38:40	commander: Initialize MultiWAN
Dec 2 18:38:40	commander: index = 14, failover_index = 14
Dec 2 18:38:40	commander: wantype = 32, wantype index = 99, wan mode = 1, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 1, fo time = 30, fo sequence = 0
Dec 2 18:38:40	commander: wantype = 16, wantype index = 0, wan mode = 2, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 0, fo time = 0, fo sequence = 0
Dec 2 18:38:40	commander: LOAD BALANCE!
Dec 2 18:38:40	commander: ROUTING!
Dec 2 18:38:42	syslog: server_config.pool_check = 1
Dec 2 18:38:42	syslog: start = 192.168.85.100, end = 192.168.85.200, lan_ip = 192.168.85.2, interface=br0, ifindex=0
Dec 2 18:38:42	udhcpd[1413]: udhcpd (v0.9.9-pre) started
Dec 2 18:38:43	syslog: Failure parsing line 13 of /etc/udhcpd_vlan0.conf
Page: 1/8 (Log Number: 109)	

Back

Web Log List (Column)		
項目	値設定	説明
Time column	-	イベントタイムスタンプを表示します
Log column	-	ログメッセージを表示します

Web Log List (Button)		
項目	値設定	説明
Previous	-	Previous ボタンをクリックすると、前ページに移動します。
Next	-	Next ボタンをクリックすると、次ページに移動します。
First	-	First ボタンをクリックすると、最初のページにジャンプします。
Last	-	Last ボタンをクリックすると、最後のページにジャンプします。
Download	-	Download ボタンをクリックすると、tar ファイル形式で PC にログをダウンロードします。
Clear	-	Clear をクリックすると、すべてのログを消去します。
Back	-	Back ボタンをクリックすると、前ページに戻ります。

Web ログタイプカテゴリ

Web Log Type Category ウィンドウでは、ネットワーク管理者は、前のセクションで説明したように、記録するイベントのタイプを選択して、Web ログリストウィンドウに表示することができます。**View** ボタンをクリックすると、**Web Log List** ウィンドウにログ履歴が表示されます。

▶ Web Log Type Category	<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> Attacks	<input checked="" type="checkbox"/> Drop	<input checked="" type="checkbox"/> Login message	<input type="checkbox"/> Debug
-------------------------	--	---	--	---	--------------------------------

Web Log Type Category		
項目	値設定	説明
System	デフォルト値：チェックあり	システムイベントを Web Log List に表示したい場合は、チェックを入れることで、ログ取得対象となります。
Attacks	デフォルト値：チェックあり	攻撃イベントを Web Log List に表示したい場合は、チェックを入れることで、ログ取得対象となります。
Drop	デフォルト値：チェックあり	ドロップイベントを Web Log List に表示したい場合は、チェックを入れることで、ログ取得対象となります。
Login message	デフォルト値：チェックあり	ログインイベントを Web Log List に表示したい場合は、チェックを入れることで、ログ取得対象となります。
Debug	デフォルト値：チェックなし	デバッグイベントを Web Log List に表示したい場合は、チェックを入れることで、ログ取得対象となります。

E メールアラート

E Mail Alert ウィンドウでは、ネットワーク管理者が、ログに記録するイベントの種類を選択し、宛先電子メールアドレスアカウントに送信することができます。

▶ Email Alert

Enable
 Server: --- Option --- ▼ Add Object
 E-mail Addresses:
 Subject:
 Log type Category: System Attacks Drop Login message Debug

Email Alert 項目	値設定	説明
Enable	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れると、E-mail address のアカウントにイベントログメッセージを送信できるようになります。
Server	-	E メールを送信するには、 Server ドロップダウンボックスからメールサーバーを1つ選択します。使用可能サーバがない場合は、 Add Object ボタンをクリックして、送信メールサーバーを作成します。 また、Object Definition > External Server > External Server タブから、送信メールサーバーを追加することもできます。
E-mail address	文字列：E メール形式	受信者のEメールアドレスを入力します。Eメールアドレスをカンマ、セミコロン、またはセミコロンで区切ります。Eメールアドレスを「myemail@domain.com」の形式で入力します。
Subject	文字列：任意のテキスト	Eメールの件名を入力します。
Log type category	デフォルト値：チェックなし	記録するイベントのタイプを選択し、指定されたEメールアカウントに送信します。利用可能なイベントは、 System 、 Attacks 、 Drop 、 Login message および Debug です。

Syslogd

Syslogd ウィンドウでは、ネットワーク管理者が、ログに記録するイベントの種類を選択し、宛先 Syslogd サーバーに送信することができます。

Syslogd	<input type="checkbox"/> Enable Server: --- Option --- Add Object Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug
----------------	--

Syslogd 項目	値設定	説明
Enable	デフォルト値 : チェックなし	Enable チェックボックスにチェックを入れ、Syslogd 機能を有効化し、イベントログを Syslog サーバーに送信します
Server	-	イベントログを送信する syslog サーバーを 1 台、サーバードロップダウンボックスから選択します。 何も利用できない場合は、 Add Object ボタンをクリックして、システムログサーバーを作成します。 また、Object Definition > External Server > External Server タブから、システムログサーバーを追加することもできます。
Log type category	デフォルト値 : チェックなし	記録するイベントのタイプを選択し、指定されたシスログサーバーに送信します。利用可能なイベントは、 System 、 Attacks 、 Drop 、 Login message および Debug です。

ログの保管

Log to Storage ウィンドウでは、ネットワーク管理者がログに記録するイベントの種類を選択し、内部または外部のストレージに保存することができます。

Log to Storage	<input type="checkbox"/> Enable Select Device: Internal ▼ Log file name: syslog Split file: <input type="checkbox"/> Enable Size: 200 KB ▼ Interval: <input type="checkbox"/> Enable 1440 (1 ~ 10080 Minutes) Max Records: 3000 (5~10000) Download log file clear logs Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug
-----------------------	--

Log Storage 項目	値設定	説明
Enable	デフォルト値 : チェックなし	チェックを入れ、ログのストレージへの送信を有効化します。
Select Device	デフォルト値 : Internal	内部または外部ストレージを選択します。
Log file name	デフォルト値 : syslog	指定されたストレージに保存するログファイル名を入力します。

Split file Enable	デフォルト値：チェックあり	Enable にチェックを入れると、Split file Size の制限に達するたびに、ログファイルがファイル分割されます。
Split file Size	デフォルト値：200 KB	分割するファイルサイズ制限を入力します。 <u>値の範囲</u> ：10～1000。 ログ保存領域は最大 5MB であり、それ以上設定すると、ログを正常に保存できない可能性があります。
Interval	デフォルト値：1440	システムは指定された時間間隔ごとにログをストレージに保存します。 <u>値の範囲</u> ：1～10080。
Max Records	デフォルト値：24	保存可能な最大のログファイル数を指定します。 システムは、常に最大ファイル数×0.7個のログファイルが存在するようログローテーションを行います。 <u>値の範囲</u> ：5～10000。 ログ保存領域は最大 5MB であり、それ以上設定すると、ログを正常に保存できない可能性があります。
Download log file	-	Download log file ボタンをクリックすると、ログファイが tar ファイルとしてダウンロードされます。
Clear logs	-	Clear logs ボタンをクリックすると、全てのログファイルが削除されます。
Log type category	デフォルト値：チェックなし	送信するログの種類にチェックをつけます。利用可能なイベントは、 System 、 Attacks 、 Drop 、 Login message および Debug から選択可能です。

6.2.5 バックアップおよび復元

バックアップおよび復元ウィンドウでは、新しいファームウェアが使用可能になったときに本製品デバイスのファームウェアをアップグレードしたり、デバイス設定をバックアップ/復元したりすることができます。

工場出荷時の設定に加えて、特別な設定をカスタマイズされたデフォルト値としてカスタマイズすることもできます。このカスタマイズされたデフォルト値を使って、必要に応じて、デバイスを期待されるデフォルト設定にリセットすることができます。

Administration > System Operation > Backup & Restore タブに進みます。

FW Backup & Restore	
Item	Setting
▶ FW Upgrade	Via Web UI ▼ FW Upgrade
▶ Backup Configuration Settings	Download ▼ Via Web UI
▶ Auto Restore Configuration	<input type="checkbox"/> Enable Save Conf. Clean Conf. Conf. Info.
▶ Self-defined Logo	Download ▼ Via Web UI Reset
▶ Self-defined CSS	Edit : Download ▼ Via Web UI Reset

FW Backup & Restore		
項目	値設定	説明
FW Upgrade	デフォルト値 : Via Web UI	新しいファームウェアが利用可能な場合は、 FW Upgrade ボタンをクリックして、 Via Web UI (Web UI 経由) または Via Storage (ストレージ経由) でデバイスファームウェアをアップグレードします。 「FW Upgrade」コマンドをクリックし、「Browse」ボタンを使って、新しいファームウェアのファイル名を指定し、「Upgrade」ボタンをクリックして、本製品デバイスでFWアップグレードを開始します。GPL ポリシーからのファームウェアをアップグレードする場合は、「Accept unofficial firmware (非公式ファームウェアの承諾)」にチェックを入れてください。
Backup Configuration Settings	デフォルト値 : Download	Via Web UI ボタンをクリックすると、デバイスの設定をバックアップまたは復元できます。 Download : デバイス設定を config.bin ファイルにバックアップします。 Upload : 指定された設定ファイルをデバイスに復元します。 Via Web UI : Web GUI 経由で設定ファイルを取得します。
Auto Restore Configuration	デフォルト値 : Enable にチェック	Enable ボタンにチェックを入れ、カスタマイズされたデフォルト設定機能を有効化します。機能が有効になったら、 Save Conf.

	なし	(設定の保存) ボタンをクリックして、希望の設定をカスタマイズされたデフォルト設定として保存することができます。また、 Clean Conf. (設定の消去) をクリックして、保存・カスタマイズされた設定を消去します。
Self-defined Logo	デフォルト値 : Download	Via Web UI ボタンをクリックすると、ロゴファイルをバックアップまたは復元できます。 Download : ロゴファイルをダウンロードします。 Upload : 指定されたロゴファイルをデバイスに復元します。 Reset : ロゴファイルを初期状態に戻します。
Self-defined CSS	デフォルト値 : Download	Edit ボタンをクリックすると、スタイルシートファイルの編集ダイアログを表示します。ダイアログ内でスタイルを変更後、Save ボタンをクリックすると、変更内容をデバイスに反映します。 Via Web UI ボタンをクリックすると、スタイルシートファイルをバックアップまたは復元できます。 Download : ロゴファイルをダウンロードします。 Upload : 指定されたロゴファイルをデバイスに復元します。 Reset : ロゴファイルを初期状態に戻します。

6.2.6 再起動およびリセット

特別な理由または状況によっては、ゲートウェイを再起動するか、本製品の設定をデフォルト値にリセットする必要があります。これらの操作を実行は、電源オン/オフ、デバイスパネルのリセットボタンを押す、または、Web GUI でも行うことができます。

Administration > System Operation > Reboot & Reset タブに進みます。

Reboot & Reset ウィンドウで、「**Reboot**」ボタンをクリックすることで、本製品を再起動することができます。また「**Reset**」ボタンをクリックすることで、デフォルト設定にリセットすることができます。

System Operation	
Item	Setting
▶ Reboot	Now ▼ Reboot
▶ Reset to Default	Reset

System Operation		
項目	値設定	説明
Reboot	デフォルト値 : Now	Reboot ボタンを押して直ちにゲートウェイを再起動、または事前定義した時間スケジュールに再起動します。 Now : 直ちに再起動します。 Time Schedule : 指定した時刻にデバイスを自動的に再起動するには、事前定義済み自動再起動時

	間スケジュールルールを選択します。時間スケジュールを定義するには、 Object Definition > Scheduling > Configuration タブに進みます。
Reset to Default	Reset ボタンをクリックすると、デバイスの設定がデフォルト値にリセットされます。

6.3 診断

このゲートウェイは、管理者がトラブルシューティングを行い、ゲートウェイを通過する異常な動作またはトラフィックの根本的な原因を見つけるための簡単なネットワーク診断ツールをサポートしています。指定されたインターフェイスまたは特定の送信元/宛先ホストの packets を記録する Packet Analyzer（パケットアナライザ）と、ネットワーク接続の問題をテストする別の Ping および Tracert ツールがあります。

6.3.1 診断ツール

診断ツールは、ネットワーク管理者が、本製品の接続を確認するためによく使用するネットワーク接続診断ツール（アプローチ）を提供します。

Administration > Diagnostic > Diagnostic Tools タブに進みます。

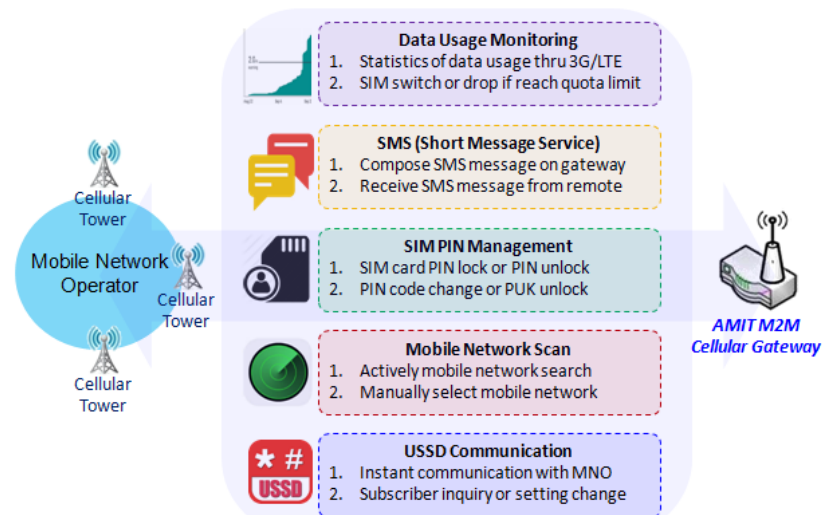
Diagnostic Tools	
Item	Setting
▶ Ping Test	Host IP: <input type="text"/> Outer Interface: <input type="text" value="Auto"/> LAN Source: <input type="text" value="Default"/> <input type="button" value="Ping"/>
▶ Tracert Test	Host IP: <input type="text"/> Interface: <input type="text" value="Auto"/> <input type="text" value="UDP"/> <input type="button" value="Tracert"/>
▶ Wake on LAN	<input type="text"/> <input type="button" value="Wake up"/>

Diagnostic Tools		
項目	値設定	説明
Ping Test	任意の設定	IP/FQDN と送信先インターフェイス（LAN、WAN-1 または Auto）を指定できます。Ping ボタンをクリックすると、システムは、alive かどうかテストする為、指定されたデバイスに対し ping 実行します。テスト結果ウィンドウは下に表示されます。
Tracert Test	任意の設定	Tracert(トレースルート)は、ネットワーク診断ツールです。IP ネットワークのルート（パス）の表示や、パケット通過の遅延測定を行います。トレースルート処理は、全て（3つ）の送信パケットが2回以上 Lost し、接続が切断され、ルートを評価できなくなるまで実行されます。 まず、IP/FQDN、テストインターフェイス（LAN、WAN-1 または Auto）とプロトコル（UDP または ICMP）を指定する必要があります。デフォルト値：は UDP です。 Tracert ボタンをクリックすると、システムは指定したホストをトレースして、稼働中であるかどうかテストします。テスト結果ウィンドウは下に表示されます。
Wake on LAN	任意の設定	ウェイクオンラン（WOL）はイーサネットネットワークの標準機能で、コンピュータをネットワークメッセージにより起動することができます。LAN ネットワークのコンピュータの MAC

		アドレスを指定できます。Wake up コマンドボタンをクリックすると、このコンピュータがリモートで起動されます。
Save	-	Save ボタンをクリックして、設定を保存します

第7章 サービス

7.1 セルラーツールキット



セルラーデータ接続以外にも、セルラーWANのデータ使用状況の監視、SMSによるテキストメッセージの送信、SIMカードのPINコードの変更、USSDコマンドによる通信事業者/ISPとの通信、診断目的のセルラーネットワークスキャンなどがあります。

Cellular Toolkit（セルラーツールキット）セクションには、セルラーの設定やアプリケーションに関連するいくつかの便利な機能が含まれています。ここでは、Data Usage（データ使用量）、SMS、SIM PIN、USSD、および、Network Scan（ネットワークスキャン）の設定ができます。このセクションの設定を続け

る前に、有効なSIMカードを本製品に挿入する必要があります。

Navigation: Status, Basic Network, Object Definition, Field Communication, Security, Administration, Service, Cellular Toolkit, Event Handling

Section: Data Usage > SMS > SIM PIN > USSD > Network Scan

3G/4G Data Usage Profile List [Add] [Delete]

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

7.1.1 データ使用量

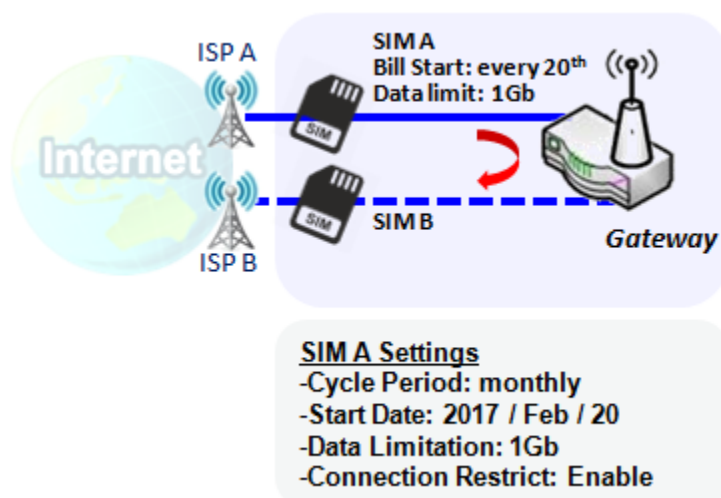
セルラー接続のデータプランの多くは、データ使用量が制限されています。データ使用量が制限容量を超えると、日々の運用に影響する可能性ある程度までデータスループットが大幅に低下したり、通信事業者/ISPが制限容量を超過したデータ使用量に課金するため、翌月に「請求が大幅に増える」現象が発生したりします。

データ使用量機能を使って、デバイスはデータ使用を継続的に監視、措置を行います。データ使用量が制限容量に達すると、デバイスが、直ちにセルラーデータ接続を切断するように設定することができます。それ以外の場合、セカンダリ SIM カードが挿入されている場合、デバイスはセカンダリ SIM に切り替わり、セカンダリ SIM を使って、別のセルラーデータ接続を自動的に確立します。

Data Usage 機能が有効になっている場合、セルラーデータ使用履歴はすべて、**Status > Statistics & Reports) > Cellular Usage** タブで確認できます。

3G/4G Data Usage Profile List Add Delete								
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
1	3G/4G SIM A	ISP A	1 Monthly	Mon Feb 20 2017 00:00:00 GMT+0800	1GB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit <input type="checkbox"/> Select

3G/4G データ使用量



データ使用量機能により、ゲートウェイ装置は、セルラーデータの使用状況を継続的に監視し、措置を行います。この図では、SIM A の制限容量は **1Gb** で、請求書の開始日は毎月 **20** 日です。このデバイスは、毎月 20 日に新しいデータ使用量の計算を開始します。Enable Connection Restrict（接続制限の有効化）は、データ使用量が、制限容量（この場合は 1Gb）に達すると、ゲートウェイデバイスに SIM A のセルラー接続を強制的に切断させます。SIM フェールオーバー機能が、**Connection Setup**（インターネット設定）で設定されている場合、ゲートウェイは、SIM B に切り替え、新しいセルラーデータ接続を自動的に確立します。

データ使用量設定

Service > Cellular Toolkit > Data Usage タブに進みます。

データ使用量の設定を完了する前に、データプランに従って、請求書の開始日、請求期間、およびデータ使用量の制限を知る必要があります。この情報は、通信事業者または ISP に問い合わせることができます。

3G/4G データ使用量プロファイルの作成/編集

3G/4G Data Usage Profile List <input type="button" value="Add"/> <input type="button" value="Delete"/>								
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

Add ボタンをクリックされると、**3G/4G Data Usage Profile Configuration** ウィンドウが表示されます。ゲートウェイで使用される SIM カードごとに1つのプロファイルを使用して、最大4つのデータ使用量プロファイルを作成することができます。

3G/4G Data Usage Profile Configuration	
Item	Setting
▶ SIM Select	3G/4G ▼ SIM A ▼
▶ Carrier Name	<input type="text"/>
▶ Cycle Period	Days ▼ 90
▶ Start Date	2016 ▼ / October ▼ / 11 ▼
▶ Data Limitation	<input type="text"/> KB ▼
▶ Connection Restrict	<input type="checkbox"/> Enable
▶ Enable	<input checked="" type="checkbox"/> Enable

3G/4G Data Usage Profile Configuration		
項目	値設定	説明
SIM Select	デフォルト値： 3G/4G-1 及び SIM A	選択したセルラーインターフェイスにバインドされたセルラーインターフェイス（ 3G/4G-1 または 3G/4G-2 ）と SIM カードを選択して、データ使用量プロファイルを設定します。 注：3G/4G-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
Carrier Name	これは、オプション項目です。	識別のために、選択した SIM カードの通信事業者名を入力します。
Cycle Period	デフォルト値： Days	最初のチェックボックスには、サイクル期間の3つのタイプがあります。 Days （日）、 Weekly （週）および Monthly （月）です。 Days ：2番目のボックスにサイクル期間の日数を指定する必要があります。 値の範囲 ：1～90日。 Weekly、Monthly ：サイクル期間は1週間、1ヶ月です
Start Date	-	ネットワークトラフィックの測定を開始する日付を指定します。過去の日付を選択しないでください。そうしないと、トラフィック統計が正しく表示されません。
Data Limitation	-	定義されたサイクル期間の許容データ制限を指定します。
Connection Restrict	デフォルト値：チェック外されています	Enable チェックボックスにチェックを入れ、接続制限機能を有効化します。 指定されたサイクル期間中、実際のデータ使用量が許容データ制限を超えた場合、セルラー接続は強制的に切断されます。
Enable	デフォルト値：チェックあり	Enable チェックボックスにチェックを入れ、データ使用量プロファイルを有効化します。

7.1.2 SMS

ショートメッセージサービス（SMS）とは、携帯電話で広く使用されているテキストメッセージングサービスです。これは、標準化された通信プロトコルを使用し、携帯電話またはセルラーデバイスが、短文テキストメッセージを瞬時かつ簡便に交換できるようにします。

SMS 設定

Service > Cellular Toolkit > SMS タブに進みます。

このゲートウェイデバイスを使用すると、携帯電話で通常行うように、SMSテキストメッセージを送信したり、受信したSMSメッセージを参照したりすることができます。

SMS 設定

Configuration	
Item	Setting
▶ Physical Interface	3G/4G-1 ▼
▶ SMS	<input checked="" type="checkbox"/> Enable SIM Status: SIM_A
▶ SMS Storage	SIM Card Only ▼
▶ SMS Space	<input type="checkbox"/> Enable & Keep Available Space <input type="text" value=""/> (1-10)

Configuration		
項目	値設定	説明
Physical Interface	デフォルト値： 3G/4G-1	次の SMS 機能設定のセルラーインターフェイス（3G/4G-1 または 3G/4G-2）を選択します。 注：3G/4G-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SMS	デフォルト値：チ ェックあり	これは SMS スイッチです。チェックボックスにチェックを入れると、SMS 機能が有効になり、チェックボックスのチェックを外すと、SMS 機能が無効になります。
SIM Status	-	現在の SIM のステータスに依存します。可能な値は、SIM_A または SIM_B です。
SMS Storage	デフォルト値： SIM Card Only	これは SMS の格納場所です。現在のオプションは、SIM Card Only（SIM カードのみ）です。
SMS Space	デフォルト値：チ ェックなし	Enable ボックスをオンにして、使用可能なストレージスペースを予約してストレージが不足するのを防ぐために、メッセージ数の数値（1~10）を指定します。

		SMS ストレージがいっぱいになると、最も古いメッセージが削除されます
Save	-	Save ボタンをクリックして、設定を保存します

SMS Summary

Unread SMS（未読の SMS）、**Received SMS**（受信済 SMS）、**Sent SMS**（発信済 SMS）、**Remaining SMS**（残りの SMS）を表示、送信 SMS 本文を編集、SIM カードから SIM を読み取りが行えます。

SMS Summary		New SMS	SMS Inbox	SMS Sent Folder
Item	Setting			
▶ Unread SMS	0			
▶ Received SMS	0			
▶ Sent SMS	0			
▶ Remaining SMS	0			

SMS Summary		
項目	値設定	説明
Unread SMS	-	初めて、SIM カードをルーターに挿入すると、未読の SMS 値はゼロになります。新しい SMS を受信し、読まなかった場合は、この値に 1 が加わります。
Received SMS	-	この値は、SIM カードからの既存の SMS 数を記録します。新しい SMS を受信すると、この値に 1 を加えた値になります。
Sent SMS	-	この値は発信 SMS の数を記録します。1 つの SMS を送信する場合、この値に 1 を加えた値です。
Remaining SMS	-	この値は SMS 容量から受信済 SMS を差し引いたものです。新しい SMS を受信すると、この値から 1 が減算されます。
New SMS	-	New SMS ボタンをクリックすると、New SMS ウィンドウが表示されます。このウィンドウから SMS の設定を行うことができます。次のページの New SMS（新規 SMS）を参照してください。
SMS Inbox	-	SMS Inbox ボタンをクリックすると SMS Inbox List（SMS 受信トレイリスト）ウィンドウが表示されます。このウィンドウから SMS を読んだり、削除したり、返信したり、SMS を転送したりすることができます。次のページの SMS Inbox List（SMS 受信トレイリスト）を参照してください。
SMS Sent Folder	-	SMS Sent Folder ボタンをクリックすると SMS Sent Folder（SMS 送信フォルダ）ウィンドウが表示されます。このウィンドウから SMS を読んだり、削除したりすることができます。
Refresh	-	Refresh ボタンをクリックすると、 SMS summary が更新されます。

New SMS

このウィンドウから新規 SMS の設定を行うことができます。

New SMS Send	
Item	Setting
▶ Receivers	<input type="text"/> (Use '+' for International Format and ';' to Compose Multiple Receivers)
▶ Text Message	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div> Length of Current Input : 0
▶ Result	

New SMS		
項目	値設定	説明
Receivers	-	SMS を送信する受信者を記述します。SMS グループ送信できる複数の受信者を作成するには;(セミコロン)を追する必要があります。
Text Message	-	SMS を送信する SMS 本文を作成します。ルーターは、SMS 本文の長さに対して最大 1023 文字をサポートします。
Send	-	Send ボタンをクリックすると、上記テキストメッセージが SMS として送信されます。
Result	-	SMS が正常に送信された場合は、Send OK と表示されます。それ以外の場合は、Send Failed が表示されます。

SMS 受信トレイリスト

このウィンドウから SMS を読んだり、削除したり、返信したり、SMS を転送したりすることができます。

SMS Inbox List Refresh Delete Close				
ID	From Phone Number	Timestamp	SMS Text Preview	Actions
SMS Inbox List				
項目	値設定	説明		
ID	-	番号または SMS。		
From Phone Number	-	SMS の発信者の電話番号です		
Timestamp	-	SMS を受信した時刻です		
SMS Text Preview	-	SMS 本文をプレビューします。Detail ボタンをクリックすると、特定のメッセージを読むことができます。		
Action	デフォルト値：チェックなし	Detail ボタンをクリックすると、SMS の詳細が読みます。Reply/Forward ボタンをクリックすると、SMS を返信/転送します。また、チェックボックスにチェックを入れ、Delete ボタンをクリックすると、チェックされている SMS が削除されます。		
Refresh	-	SMS Inbox List を更新します。		
Delete	-	Action からすべてのチェックの入った SMS を削除します。		
Close	-	SMS Inbox List ウィンドウを閉じます。		

SMS 送信フォルダ

このウィンドウから SMS を読んだり、削除したりすることができます。

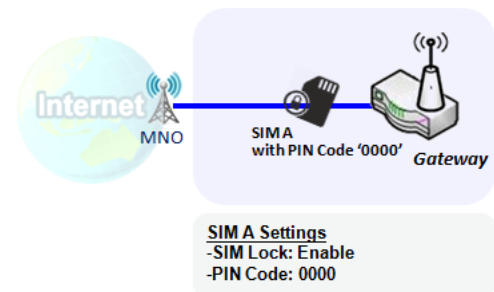
SMS Sent Folder Delete Close				
ID	Receivers	Timestamp	SMS Text Preview	Actions
SMS Sent Folder				
項目	値設定	説明		
ID	-	番号または SMS。		
Receivers	-	送信された SMS の受信者リスト		
Timestamp	-	SMS を送信した時刻です		
SMS Text Preview	-	SMS 本文をプレビューします。Detail ボタンをクリックすると、特定のメッセージを読むことができます。		
Action	デフォルト値：チェックなし	Detail ボタンをクリックすると、SMS の詳細が読みます。また、チェックボックスにチェックを入れ、Delete ボタンをクリックすると、チェックされている SMS が削除されます。		
Delete	-	Action からすべてのチェックの入った SMS を削除します。		
Close	-	SMS Sent Folder ウィンドウを閉じます。		

7.1.3 SIM PIN

世界中でほとんどの場合、音声サービスまたはデータサーフィンのためにセルラーネットワークを利用するには、エンドデバイスに SIM カード（つまり、UICC）を挿入する必要があります。SIM カードは、通常、移動体通信事業者またはサービスプロバイダによりリリースされます。各 SIM カードは、ネットワーク所有者またはサービスプロバイダが各加入者を識別するための固有の番号（いわゆる ICCID）を有します。SIM カードは、サービスプロバイダと加入者の間で重要な役割を果たすため、不正なアクセスを防ぐために SIM カードにはいくつかのセキュリティメカニズムが必要です。

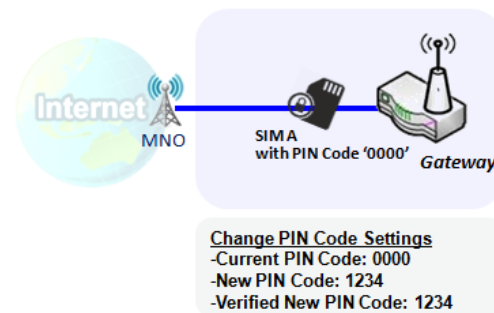
SIM カードで PIN コードを有効にすると、不正なアクセスからセルラーデバイスを簡単かつ効果的に保護することができます。本ゲートウェイデバイスを使用すると、Web GUI を通じて SIM カード上の PIN コードを有効化かつ管理することができます。

SIMカード上のPINコードの有効化



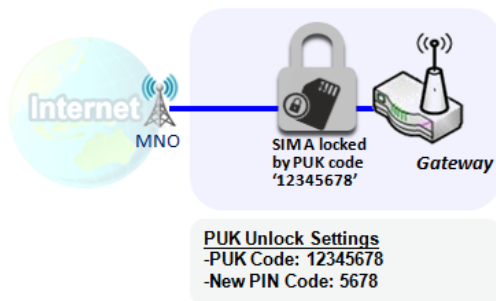
本ゲートウェイデバイスでは、SIM カード上の PIN コードを有効化することができます。この例では、デフォルトの PIN コード「0000」を使って、3G-4G-1 の SIM-A で PIN コードを有効化する方法を示します。

SIMカード上のPINコードの変更



本ゲートウェイデバイスでは、SIM カード上の PIN コードを変更することができます。上の例では、新しい PIN コードを「1234」に設定する場合は、元の PIN コード「0000」を入力し、「1234」の新しい PIN コードを入力する必要があります。入力した新しい PIN コードが正しいかどうかを確認するには、Verified New PIN Code（新しい PIN コードの検証）にもう一度 PIN コード「1234」を入力する必要があります。

PUKコードによるSIMカードのロック解除



3G/4G-1 WAN 設定ページで誤った PIN コードを 3 回以上入力すると、SIM カードが PUK コードによりロックされます。その後、SIM カードのロックを解除する PUK コードを取得するには、サービス番号に電話する必要があります。この図では、PUK コードは「12345678」であり、新しい PIN コードは「5678」です。

SIM PIN 設定

Service > Cellular Toolkit > SMS PIN タブに進みます。

SIM PIN 機能ウィンドウでは、SIM ロック（PIN コードで保護されていること）を有効または無効にするか、PIN コードを変更することができます。

また、前述したように、失敗試行の残り回数の情報を確認することもできます。これらの失敗試行を使い果たした場合は、SIM カードのロックを解除する PUK コードを取得する必要があります。

SIM カードの選択

Configuration	
Item	Setting
▶ Physical Interface	3G/4G-1 ▼
▶ SIM Status	SIM-A Ready
▶ SIM Selection	SIM-A ▼ <input type="button" value="Switch"/>

Configuration		
項目	値設定	説明
Physical Interface	デフォルト値： 3G/4G-1	選択した SIM カードの SIM PIN 設定を変更するには、セルラーインターフェイス（ 3G/4G-1 または 3G/4G-2 ）を選択します。 注： 3G/4G-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM Status	-	選択された SIM カードおよび SIM カードステータスの表示。 ステータスは、 Ready （準備完了）、 Not Insert （未挿入）、または、 SIM PIN です。 Ready -- SIM カードが挿入され、使用準備ができています。PIN 保護のない SIM カードでも、SIM カードが正しい PIN コードでロック解除されていてもかまいません。 Not Insert -- SIM スロットには SIM カードが挿入されていません。

	<p>SIM PIN -- SIM カードは PIN コードで保護されていますが、正しい PIN コードではまだロックされていません。この SIM カードはまだロックされた状態です。</p>
SIM Select -	<p>SIM PIN をさらに設定するために、SIM カードを選択します。Switch ボタンを押すと、ゲートウェイは、SIM カードを別のものに切り替えます。その後、SIM カードを設定することができます。</p>

PIN コードの有効化/変更

PIN コード（パスワード）機能を有効または無効にし、さらに PIN コード機能を変更します。

<input type="checkbox"/> SIM function <input type="button" value="Save"/> <input type="button" value="Change PIN Code"/>	
Item	Setting
▶ SIM lock	<input type="checkbox"/> Enable PIN Code: <input type="text"/> (4~8 digits)
▶ Remaining times	3

SIM function		
項目	値設定	説明
SIM lock	SIM カードに依存します	Enable ボタンをクリックして、SIM ロック機能を有効化します。初めて SIM ロック機能を有効化する場合は、PIN コードも入力し、 Save ボタンをクリックして、設定を適用します。
Remaining times	SIM カードに依存します	SIM PIN ロック解除の残りの試行回数を表示します。
Save	-	Save ボタンをクリックして、設定を適用します。
Change PIN Code	-	Change PIN Code ボタンをクリックして、PIN コード（パスワード）を変更します。 SIM Lock 機能が有効になっていない場合、 Change PIN code ボタンは無効になります。この場合、PIN コードを変更したい場合は、まず SIM ロック機能を有効化して PIN コードを入力し、 Save ボタンをクリックし、有効化する必要があります。その後、 Change PIN code ボタンをクリックして、PIN コードを変更することができます。

Change PIN code ボタンをクリックすると、以下のウィンドウが表示されます。

Item	Setting
▶ Current PIN Code	<input type="text"/> (4~8 digits)
▶ New PIN Code	<input type="text"/> (4~8 digits)
▶ Verified New PIN Code	<input type="text"/> (4~8 digits)

Apply Cancel

項目	値設定	説明
Current PIN Code	必須入力項目	SIM カードの現在の（古い）PIN コードを入力します。
New PIN Code	必須入力項目	新しい PIN コードを入力します。
Verified New PIN Code	必須入力項目	再度、新しい PIN コードを入力します。
Apply	-	Apply ボタンをクリックして、指定した新しい PIN コードを使って、PIN コードを変更します。
Cancel	-	変更をキャンセルして、現在の PIN コードを保存するには、 Cancel ボタンをクリックします。

注：特定の SIM カードの PIN コードを変更した場合は、Basic Network > WAN & Uplink > Connection Setup > Connection with SIM Card で、指定した対応する PIN コードも変更する必要があります。そうしないと、無効な（古い）PIN コードを使って、間違った SIM PIN 試行が行われる可能性があります。

PUK コードを用いるロック解除

PUK 機能ウィンドウは、SIM カードが PUK コードでロックされている場合にのみ利用可能です。SIM カードがロックされており、ロックを解除するには追加の PUK コードが必要です。通常、間違った PIN コードの試行が多すぎると、SIM 機能テーブルの残り回数が 0 になります。この場合、サービスプロバイダに連絡して SIM カード用の PUK コードを申請し、提供された PUK コードでロックされた SIM カードのロックを解除する必要があります。PUK コードで SIM カードのロックを解除すると、SIM ロック機能が自動的に有効になります。

PUK function Save	
Item	Setting
▶ PUK status	PUK unlock.
▶ Remaining times	N/A
▶ PUK Code	<input type="text"/> (8 digits)
▶ New PIN Code	<input type="text"/> (4-8 digits)

PUK function		
項目	値設定	説明
PUK Status	PUK Unlock / PUK Lock	PUK ステータスの表示。 通常の状況では、 PUK Unlock 表示されます。失敗 PIN コードの試行回数が多すぎると、PUK コードによってロックされ、 PUK Lock に変わります。
Remaining times	SIM カードに依存します	PUK ロック解除の残りの試行回数を表示します。 注： Remaining times をゼロにしないでください。これは、 SIM カードを永久的に損傷します！ PUK コードがない場合は、ISP のヘルプに電話をかけ、正しい PUK を取得し、SIM ロックを解除してください。
PUK Code	必須入力項目	PUK ロック解除状態にある SIM カードのロックを解除できる PUK コード（8 桁）を入力します。
New PIN Code	必須入力項目	SIM カードの新しい PIN コード（4~8 桁）を入力します。 忘れてしまった古い PIN コードを置き換えるには、新しい PIN コードを決定する必要があります。PIN コード（パスワード）は慎重に保管してください。
Save	-	Save ボタンをクリックして、設定を適用します。

注：特定の SIM カードの PUK コードおよび PIN コードを変更した場合は、**Basic Network > WAN & Uplink > Connection Setup > Connection with SIM Card** で、指定した対応する PIN コードも変更する必要があります。そうしなければ、無効な（古い）PIN コードを使って、間違った SIM PIN 試行が行われる可能性があります。

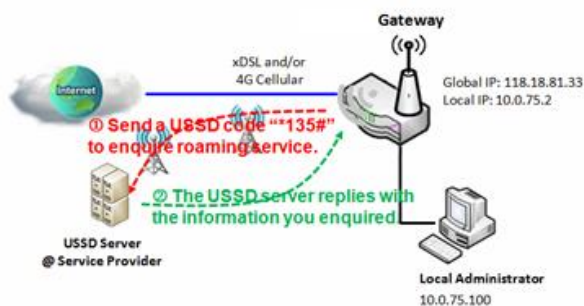
7.1.4 USSD

非構造付加サービスデータ（USSD）は、GSMセルラー電話がサービスプロバイダのコンピュータと通信するためのプロトコルです。USSDは、WAPブラウジング、プリペイドコールバックサービス、モバイルマネージャーサービス、位置ベースのコンテンツサービス、メニューベースの情報サービスで使用され、またネットワーク上での電話の設定にも使用されます。

USSDメッセージの長さは、英数字で最大182文字です。ショートメッセージサービス（SMS）とは異なり、USSDメッセージは、USSDセッション中にリアルタイム接続を作成します。接続は開いたままで、一連のデータの双方向交換が可能です。これにより、USSDは、SMSを使用するサービスよりも応答性が良くなります。

Configuration				
Item	Setting			
Physical Interface	3G/4G-1 SIM Status: SIM_A			
USSD Profile List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Profile Name	USSD Command	Comments	Actions
1	roaming setting	*135#	Roaming function	<input type="button" value="Edit"/> <input type="checkbox"/> Select
USSD Profile Configuration <input type="button" value="Save"/>				
Item	Setting			
Profile Name	roaming setting			
USSD Command	*135#			
Comments	Roaming function			
USSD Request <input type="button" value="Send"/> <input type="button" value="Clear"/>				
Item	Setting			
USSD Profile	roaming setting			
USSD Command	*135#			
USSD Response	< ChungHwa Data Roaming Services> 1 Order 2 Query 3 Setting 4 使用中文			

USSDのシナリオ



USSDでは、キャリア/ISPとの即時双方向通信を行うことができます。図において、USSDコマンド「* 135#」は、データローミングサービスと呼ばれます。そのUSSDコマンドを通信事業者に送信した後、USSD Response（USSD応答）ウィンドウで応答を取得することができます。USSDコマンドは、キャリア/ISPによって異なることに注意してください。

USSD 設定

Service > Cellular Toolkit > USSD に進みます。

「USSD」ページには、USSD機能用の4つのウィンドウがあります。「Configuration」ウィンドウで、USSD機能に使用される3G/4Gモジュール（物理インターフェイス）を指定することができます。システムは、モジュールで現在どのSIMカードが使用されているかを表示します。2番目のウィンドウは「USSD Profile List」です。これは、USSDセッションをアクティブ化するためのプリコマンドを保存している、定義済みのすべてのUSSDプロファイルを表示します。ウィンドウ内の「Add」ボタンを使用すると、新しいUSSDプロファイルを追加し、3番目のウィンドウでプロファイルのコマンド「USSD Profile Configuration」を定義することができます。USSDサーバーに対するUSSD接続セッションのアクティベーションを開始する場合は、USSDプロファイルを選択するか、適切な事前コマンドを入力して、セッションの「Send」ボタンをクリックします。USSDサーバーからの応答は、「USSD Command」行の下に表示されます。「USSD Command」フィールドに入力されたコマンドが送信されると、受信した応答が「USSD Response」の空白スペースに表示されます。ユーザーは、USSDコマンドを送信し、USSD応答をゲートウェイ経由で取得することにより、USSDサーバーと通信することができます。

USSD Configuration

Configuration	
Item	Setting
Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A

Configuration		
項目	値設定	説明
Physical Interface	デフォルト値 : 3G/4G-1	接続されたセルラーサービス (SIM_A または SIM_B で識別される) の USSD を設定するには、セルラーインターフェイス (3G/4G-1 または 3G/4G-2) を選択します。 注 : 3G/4G-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM Status	-	接続されたセルラーサービス (SIM_A または SIM_B で識別される) を表示します。

USSD プロファイルの作成/編集

セルラーゲートウェイを使用すると、USSD プロファイルをカスタム設定することができます。これは、最大 35 の USSD プロファイルをサポートします。

USSD Profile List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Profile Name	USSD Command	Comments	Actions

Add ボタンをクリックされると、**USSD Profile Configuration** ウィンドウが表示されます。

USSD Profile Configuration <input type="button" value="Save"/>	
Item	Setting
▶ Profile Name	<input type="text"/>
▶ USSD Command	<input type="text"/>
▶ Comments	<input type="text"/>

USSD Profile Configuration		
項目	値設定	説明
Profile Name	-	USSD プロファイルの名称を入力します。
USSD Command	-	プロファイル用に定義された USSD コマンドを入力します。通常、数字キーパッド「0~9」、「*」、「#」で設定されるコマンド文字列です。USSD コマンドは、セルラーサービスと非常に関連していません。詳細については、サービスプロバイダに確認してください。
Comments	-	プロファイルの簡単なコメントを入力します。

SSD Request の送信

Send ボタンをクリックすると、**USSD Response** ウィンドウが表示されます。

Clear ボタンをクリックすると、**USSD Response** ウィンドウが消えます。

USSD Request	
	<input type="button" value="Send"/> <input type="button" value="Clear"/>
Item	Setting
▶ USSD Profile	--- Option --- ▼
▶ USSD Command	<input type="text"/>

USSD Request		
項目	値設定	説明
USSD Profile	-	ドロップダウンリストから USSD プロファイル名を選択します。
USSD Command	-	選択したプロファイルの USSD コマンド文字列が、ここに表示されます。
USSD Response	-	Send ボタンをクリックすると、USSD コマンドが送信され、USSD Response ウィンドウが表示されます。対応するサービスの応答メッセージが表示され、サービス SMS が受信されます。

7.1.5 ネットワークスキャン

「ネットワークスキャン」機能により、管理者は、各3G/4Gインターフェイスにおけるデータ通信のために、モバイルシステムに接続する方法をデバイスに指定することができます。例えば、管理者は、接続、2G、3G、または、LTEに使用されるモバイルシステムの世代を指定することができます。さらに、ゲートウェイデバイスが、モバイルシステムに自動的に接続するための接続シーケンスを定義することができます。また、管理者は、手動でモバイルシステムをスキャンし、対象となる操作システムを選択して、適用することができます。手動スキャンアプローチは、問題診断に使用されます。

ネットワークスキャン

Service > Cellular Toolkit > Network Scan タブに進みます。

「Network Scan」ページには、ネットワークスキャン機能の為の2つのウィンドウがあります。「Configuration」ウィンドウでは、ネットワークスキャンを実行するために使用する3G/4Gモジュール（物理インターフェイス）を選択することができます。システムは、現在モジュールで使用されているSIMカードを表示します。ネットワークスキャンを順次実行することにより、各3G/4G WANインターフェイスを設定することができます。対象とするモバイルシステムの世代（2G/3G/LTE）の接続シーケンスを指定することもできます。

ネットワークスキャン設定

Configuration	
Item	Setting
▶ Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A
▶ Network Type	Auto ▼
▶ Scan Approach	Auto ▼

Configuration		
項目	値設定	説明
Physical Interface	デフォルト値： 3G/4G-1	ネットワークスキャン機能のセルラーインターフェイス（3G/4G-1 または 3G/4G-2）を選択します。 注：3G/4G-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM Status	-	接続されたセルラーサービス（SIM_A または SIM_B で識別される）を表示します。
Network Type	デフォルト値：Auto	ネットワークスキャン機能のネットワークタイプを指定します。Auto、2G Only、2G prefer、3G Only、3G prefer、または、LTE Only から選択可能です。Auto オプションを選択すると、ネットワークは、自動的に登録されます。 Only オプションが選択されている場合は、選択したネットワー

		クのみが登録されます。 Prefer オプションが選択されている場合は、そのネットワーク利用可能な場合、優先して登録されます。
Scan Approach	デフォルト値 : Auto	Auto を選択すると、セルラーモジュールが自動的に登録されます。 Manually オプションを選択すると、Network Provider List ウィンドウが表示されます。 Scan ボタンを押すと、最も近い基地局をスキャンします。優先基地局を選択し（チェックボックスにチェックを入れて）、Apply ボタンをクリックして、設定を適用します。
Save	-	Save をクリックして、設定を保存します

2番目のウィンドウは「**Network Provider List**」ウィンドウです。これは、**Configuration**の**Scan Approach**で**Manually**が選択されているときに表示されます。「**Scan**」ボタンをクリックして1~3分待つと、検出されたモバイルオペレータシステムが表示されます。「**Apply**」ボタンをもう一度クリックすると、専用の3G/4Gインターフェイス用のモバイルオペレータシステムに接続するためのシステムが起動します。

Network Provider List			
Provider Name	Mobile System	Network Status	Action
Chunghwa Telecom	4G	Current	<input type="checkbox"/> Select
Far EasTone	3G	Forbidden	<input type="checkbox"/> Select

7.2 イベント処理

イベント処理とは、管理者が個々のプロファイルで事前定義されたイベント、ハンドラ、または、応答の動作を設定できるようにするアプリケーションです。イベント処理機能を適切に設定することで、管理者は、購入したゲートウェイ経由で簡単にステータスと情報を取得することができます。

サポートされるイベントは、**管理イベント**と**通知イベント**の2つのグループに分類されます。

管理イベントとは、ゲートウェイを管理するため、または、ゲートウェイの特定の機能の設定/ステータスを変更するために使用されるイベントです。管理イベントを受信すると、ゲートウェイは機能を変更し、管理に必要なステータスを同時に収集します。

通知イベントとは、いくつかの関連オブジェクトがトリガーされたイベントであり、イベントの発生時に対応するアクションを実行します。

これは、SMSメッセージ、電子メール、SNMPトラップなどで起こったことを管理者に警告するイベントです。

設定を容易にするために、管理者は、特定のイベントに即座に反応したり、高度に有用な目的でデバイスを管理したりするために、一般的な定義済みの管理/通知イベントプロファイルを作成および編集することができます。例えば、ゲートウェイのルーチンをメンテナンスするためにリモート管理SMSを送受信するなどです。このような管理および通知機能はすべて、イベント処理機能によって効果的に実現することができます。

提供されたプロファイルとイベントの要約リストは次のとおりです：

- プロファイル（ルール）：
 - SMS の設定およびアカウント
 - Eメールアカウント
- 管理イベント：
 - トリガータイプ：SMS、SNMPトラップ
 - アクション：ネットワークステータスを取得する。LANの動作、NATの動作、ファイアウォールの動作、VPNの動作、システム管理、管理を設定する。
- 通知イベント：
 - トリガータイプ：接続変更（WAN、LAN、DDNS）、管理、および、データの使用。
 - アクション：SMS、Syslog、SNMPトラップ、または、Eメールアラートを使って管理者に通知します。

イベント処理機能を使用するには、まず、イベント管理設定を有効にして、提供されるプロファイル設定でイベントの詳細を設定する必要があります。個別の管理/通知イベント用に事前定義されたプロファイルを作成または編集することができます。プロファイル設定は、いくつかの項目に分かれています。つまり、SMSアカウント定義、電子メールサービス定義です。次に、各管理/通知イベントを、イベントのトリガー条件、および、イベントの対応するアクション（イベントに対する反応）を識別するように設定する必要があります。各イベントについて、複数のアクションを同時に有効化することができます。

7.2.1 設定

Service > SMS & Event > Configuration タブに進みます。

イベント処理とは、管理者が個々のプロファイルで事前定義されたイベント、ハンドラ、または、応答の動作を設定できるようにするサービスです。

イベント管理の有効化

Configuration	
Item	Setting
▶ Event Management	<input type="checkbox"/> Enable

Configuration		
項目	値設定	説明
Event Management	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、イベント管理機能を有効化します。

SMS 管理の有効化

SMS 管理機能を使用するには、最初にいくつかの重要な設定をする必要があります。

SMS Configuration	
Item	Setting
▶ Message Prefix	<input type="checkbox"/> Enable & <input type="text"/>
▶ Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A
▶ Delete Managed SMS after Processing	<input type="checkbox"/> Enable

SMS Configuration		
項目	値設定	説明
Message Prefix	デフォルト値：チェックなし	Enable チェックボックスをクリックして、受信した SMS を検証するための SMS プレフィックスを有効化します。この機能を有効化した後、チェックボックスの後にプレフィックスを入力する必要があります。 受信した管理イベント SMS は、指定されたプレフィックスを初

		期識別子として持つ必要があり、対応するハンドラは、その後の処理に有効になります。
Physical Interface	デフォルト値： 3G/4G-1	SMS 管理を設定するには、セルラーインターフェイス（3G/4G-1 または 3G/4G-2）を選択します。 注：3G/4G-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM Status	-	接続されたセルラーサービス（SIM_A または SIM_B で識別される）を表示します。
Delete Managed SMS after Processing	デフォルト値：エ ックなし	Enable チェックボックスにチェックと入れ、受信した管理イベント SMS を処理された後に削除します。

SMS アカウントの作成/編集

SMS を介してゲートウェイを管理するために、SMS アカウントを設定します。これは、最大 5 アカウントをサポートします。

SMS Account List <input type="button" value="Add"/> <input type="button" value="Delete"/>					
ID	Phone Number	Phone Description	Application	Enable	Actions

Add / Edit ボタンをクリックして、SMS アカウントを設定することができます。

SMS Account Configuration	
Item	Setting
▶ Phone Number	Specific Number ▼ <input type="text"/>
▶ Phone Description	<input type="text"/>
▶ Application	<input type="checkbox"/> Event Trigger <input type="checkbox"/> Notify Handle
▶ Send confirmed SMS	<input type="checkbox"/> Enable
▶ Enable	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/>	

SMS Account Configuration		
項目	値設定	説明
Phone Number	1. 携帯電話番号形式で す 2. 必須入力項目	SMS アカウント識別子として携帯電話番号を指定します。 値の範囲：1～32 桁。
Phone Description	1. 任意のテキスト	SMS アカウントの簡単な説明を指定します。

	2. 任意の設定	
Application	必須入力項目	アプリケーションタイプを指定します。 Event Trigger 、 Notify Handle 、またはそれら両方の選択が可能です。
Send confirmed SMS	1.任意の設定 2.デフォルト値：チェックなし	SMS 応答機能を有効にするには、[有効にする]をクリックします。ゲートウェイは、SMS 管理イベントを受信するたびに、確認されたメッセージを送信者に送り返す。確認されたメッセージは、「デバイスがコマンド xxxxx で SMS を受信しました」という形式に似ています。
Enable	デフォルト値：チェックなし	Enable チェックボックスをクリックして、このアカウントを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します。

E メールサービスアカウントの作成/編集

イベント通知の E メールサービスアカウントを設定します。これは、最大 5 アカウントをサポートします。

<input type="checkbox"/> Email Service List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Email Server	Email Addresses	Enable	Actions

Add / Edit ボタンをクリックして、E メールアカウントを設定することができます。

<input type="checkbox"/> Email Service Configuration	
Item	Setting
▶ Email Server	--- Option --- ▼
▶ Email Addresses	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/>	

Email Service Configuration		
項目	値設定	説明
Email Server	--- オプション ---	E メールアカウント設定の External Server （外部サーバー）設定から、E メールサーバープロファイルを選択します。
Email Addresses	1.インターネット E メールアドレス形式です 2. 必須入力項目	宛先 E メールアドレスを指定します
Enable	デフォルト値：チェックなし	Enable チェックボックスをクリックして、このアカウントを有効化します。
Save	-	Save ボタンをクリックして、設定を保存します

リモートホストプロファイルの作成/編集

リモートホストプロファイルを設定します。これは、最大 10 プロファイルをサポートします。

Remote Host List								Add	Delete
ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions	

Add / Edit ボタンをクリックして、プロファイルを構成することができます。

Remote Host Configuration	
Item	Setting
▶ Host Name	<input type="text"/>
▶ Host IP	<input type="text"/>
▶ Protocol Type	TCP ▼
▶ Port Number	<input type="text"/>
▶ Prefix Message	<input type="text"/>
▶ Suffix Message	<input type="text"/>
▶ Enable	<input type="checkbox"/>
Save	

リモートホスト構成		
項目	項目	項目
Host Name	1.文字列形式 2.必須入力項目	ホスト名を指定します。 値の範囲 : 1~64 文字。
Host IP	1.必須入力項目 2.IP アドレス形式	リモートホストの場合は、IP を指定します。IPv4 形式です。
Protocol Type	1.必須入力項目 2.デフォルト値 : TCP	リモートホストの場合は、プロトコルを指定します。TCP または UDP 形式です。
Port Number	1.必須入力項目	リモートホストにアクセスするためのポート番号を指定します。 値の範囲 : 1~65535。
Prefix Message	1. 文字列形式 2. 任意入力項目	プレフィックスメッセージ文字列を、リモートホストにアクセスするための事前定義された ID として指定します。 値の範囲 : 1~64 文字。
Suffix Message	1. 文字列形式 2. 任意入力項目	サフィックスメッセージ文字列を、リモートホストにアクセスするための事前定義された ID として指定します。 値の範囲 : 1~64 文字。
Enable	デフォルト値 : チェックなし	Enable ボックスをクリックして、このプロファイル設定を有効します。
Save	-	Save ボタンをクリックして、構成を保存します
Undo	-	Undo ボタンをクリックして、構成した内容を元の設定に復元します。

7.2.2 管理イベント

管理イベントにより、管理者は、イベントトリガー、ハンドラ、および、応答の関係（ルール）を定義することができます。

Service > SMS & Event > Managing Events タブに進みます。

管理イベントの有効化

Configuration	
Item	Setting
Managing Events	<input type="checkbox"/> Enable

Configuration		
項目	値設定	説明
Managing Events	デフォルト値：チェックなし	Enable チェックボックスにチェックを入れ、管理イベント機能を有効化します。

管理イベントルールの作成/編集

管理イベントルールを設定します。最大 128 ルールがサポートされます。

Managing Event List				
ID	Event	Description	Enable	Actions
<input type="button" value="Add"/> <input type="button" value="Delete"/>				

Add ボタンがクリックされると、Managing Event Configuration ウィンドウが表示されます。

Managing Event Configuration	
Item	Setting
▶ Event	None ▼ None ▼ None ▼
▶ Trigger Type	Period ▼
▶ Interval	0 (0~86400 seconds)
▶ Description	
▶ Action	<input type="checkbox"/> Network Status <input type="checkbox"/> WAN <input type="checkbox"/> LAN&VLAN <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> VPN <input type="checkbox"/> GRE <input type="checkbox"/> System Manage <input type="checkbox"/> Administration <input type="checkbox"/> Remote Host
▶ Managing Event	<input checked="" type="checkbox"/> Enable

Save

Managing Event List Managing Event Configuration		
項目	値設定	説明
Event	デフォルト値 : None	<p>イベントタイプ (SMS、SNMP Trap) およびイベント識別子/プロファイルを指定します。</p> <p>SMS : SMS を選択し、テキストボックスのメッセージをイベントのトリガー条件として入力します。</p> <p>SNMP : SNMP Trap を選択し、テキストボックスにメッセージを入力して、SNMP トラップイベントを指定します。</p> <p><i>注 : 利用可能なイベントタイプは、購入した製品によって異なる場合があります</i></p>
Trigger Type	デフォルト値 : Period	<p>イベントトリガーのタイプを間隔または Once のいずれかで指定します。</p> <p>Period : Period(期間)を選択して時間間隔を指定すると、指定されたイベント条件が成立するたびに、その期間ごとにイベントが繰り返しトリガーされます。</p> <p>Once : Once を選択すると、指定したイベント条件が成立したときにイベントが 1 回だけトリガされます。</p>

Interval	デフォルト値：0	繰り返しイベントトリガーの時間間隔を指定します。 値の範囲：0～86400 秒。
Description	文字列形式：任意のテキスト	管理イベントの簡単な説明を入力します。
Action	デフォルト値：すべてのチェックボックスのチェックなし	<p>予想されるイベントが発生した際のアクションとして、Network Status もしくは他アクションを少なくとも1つ指定します。</p> <p>Network Status：ネットワークステータスをイベントのアクションとして取得するには、Network Status チェックボックスを選択します。</p> <p>LAN&VLAN：LAN&VLAN チェックボックスと関心のあるサブ項目（ポートリンクのオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。</p> <p>NAT：NAT チェックボックスと関心のあるサブ項目（仮想サーバーのオン/オフ、DMZ オン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。</p> <p>Firewall：Firewall チェックボックスと関心のあるサブ項目（リモート管理者ホスト ID のオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。</p> <p>VPN：VPN チェックボックスと関心のあるサブ項目（IPSec トンネルのオン/オフ、PPTP クライアントのオン/オフ、L2TP クライアントのオン/オフ、OpenVPN クライアントのオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。</p> <p>GRE：GRE チェックボックスと関心のあるサブ項目（GRE トンネルのオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。</p> <p>System Manage：System Manage チェックボックスと関心のあるサブ項目（WAN SSH サービスオン/オフ、TR-069 オン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。</p> <p>Administration：Administration チェックボックスと関心のあるサブ項目（バックアップ設定、復元設定、再起動、デフォルトとして現在の設定を保存）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。</p> <p><i>注：利用可能なイベントタイプは、購入した製品によって異なる場合があります</i></p>
Managing Events	デフォルト値：チェックあり	Enable チェックボックスをクリックして、 Managing Event 設定を有効化します。
Save	-	Save ボタンをクリックして、設定を保存します
Undo	-	Undo ボタンをクリックして、設定した内容を元の設定に復元します。

7.2.3 通知イベント

Service > SMS & Event > Notifying Events タブに進みます。

通知イベント設定により、管理者は、イベントトリガーとハンドラ間の関係（ルール）を定義することができます。

通知イベントの有効化

Configuration	
Item	Setting
▶ Notifying Events	<input checked="" type="checkbox"/> Enable

Configuration		
項目	値設定	説明
Notifying Events	デフォルト値：は、 チェックなし	Enable チェックボックスにチェックを入れ、通知イベント機能を有効化します。

通知イベントルールの作成/編集

通知イベントルールを設定します。最大 128 ルールがサポートされます。

Notifying Event List							
ID	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions
<div style="display: flex; justify-content: space-between; align-items: center;"> Add Delete </div>							

Add ボタンがクリックされると、Notifying Event Configuration ウィンドウが表示されます。

Notifying Event Configuration	
Item	Setting
▶ Event	None ▼ None ▼ None ▼
▶ Trigger Type	Period ▼
▶ Interval	0 (0~86400 seconds)
▶ Description	
▶ Action	<input type="checkbox"/> SMS <input type="checkbox"/> Syslog <input type="checkbox"/> SNMP Trap (Only Support v1 and v2c) <input type="checkbox"/> Email Alert <input type="checkbox"/> Remote Host
▶ Time Schedule	(0) Always ▼
▶ Notifying Events	<input checked="" type="checkbox"/> Enable
Save	

Notifying Event Configuration		
項目	値設定	説明
Event	デフォルト値 : None	<p>イベントタイプと対応するイベント設定を指定します。サポートされているイベントタイプは次のとおりです :</p> <p>WAN : 特定の WAN イベントを指定するには、WAN とトリガー条件を選択します。</p> <p>LAN&VLAN : 特定の LAN および VLAN イベントを指定するには、LAN & VLAN とトリガー条件を選択します。</p> <p>DDNS : 特定の DDNS イベントを指定するには、DDNS とトリガー条件を選択します。</p> <p>Administration : 特定の管理イベントを指定するには、Administration とトリガー条件を選択します。</p> <p>Data Usage : 特定のデータ使用状況イベントを指定するには、Data Usage、SIM Card (Cellular Service)、およびトリガー条件を選択します。</p> <p><i>注 : 利用可能なイベントタイプは、購入した製品によって異なる場合があります</i></p>
Trigger Type	デフォルト値 : Period	<p>イベントトリガーのタイプを間隔または Once のいずれかで指定します。</p> <p>Period : Period(期間)を選択して時間間隔を指定すると、指定されたイベント条件が成立するたびに、その期間ごとにイベン</p>

		トが繰り返しトリガーされます。 Once : Once を選択すると、指定したイベント条件が成立したときにイベントが1回だけトリガされます。
Interval	デフォルト値 : 0	繰り返しイベントトリガーの時間間隔を指定します。 値の範囲 : 0~86400 秒。
Description	文字列形式 : 任意のテキスト	通知イベントの簡単な説明を入力します。
Action	デフォルト値 : すべてのチェックボックスのチェックなし	想定されるイベントが発生したときに実行するアクションを少なくとも1つ指定します。 SMS : SMS を選択すると、ゲートウェイは、イベントのアクションとして定義されたすべての SMS アカウントに SMS を送信します。 Syslog : Syslog を選択し、イベントのアクションとして、Enable Checkbox (チェックボックスを有効にする) を選択/選択解除します。 SNMP Trap : SNMP Trap を選択すると、ゲートウェイは、イベントのアクションとして定義された SNMP イベント受信者に SNMP トラップを送信します。 Email Alert : Email Alert を選択すると、ゲートウェイは、イベントのアクションとして定義されたすべての E メールアカウントに E メールを送信します。 <i>注 : 利用可能なイベントタイプは、購入した製品によって異なる場合があります</i>
Time Schedule	デフォルト値 : (0)Always	通知イベントの時間スケジューリングルールを選択します。
Notifying Events	デフォルト値 : チェックあり	Enable チェックボックスをクリックして、通知イベント設定を有効化します。
Save	-	Save ボタンをクリックして、設定を保存します
Undo	-	Undo ボタンをクリックして、設定した内容を元の設定に復元します。

第 8 章 ステータス

8.1 基本ネットワーク

[WAN & Uplink](#)
[LAN & VLAN](#)
[DDNS](#)

WAN Interface IPv4 Network Status

ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit

WAN Interface IPv6 Network Status

ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1		Disable				Edit

LAN Interface Network Status

IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	Action
192.168.1.254	255.255.255.0	fe80::250:18f:fe00:ffe	/64	Edit IPv4 Edit IPv6

3G/4G Modem Status List [Refresh](#)

8.1.1 WAN および Uplink ステータス

詳細は、Status > Basic Network > WAN & Uplink タブに進みます。

WAN&Uplink Status ウィンドウには、ネットワーク設定、接続情報、モデムステータス、トラフィック統計など、さまざまなネットワークタイプの現在のステータスが表示されます。表示は 5 秒ごとに更新されます。

WAN インターフェイス IPv4 ネットワークステータス

WAN interface IPv4 Network Status ウィンドウには、IPv4 ネットワークのステータス情報が表示されます。

WAN Interface IPv4 Network Status										
ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	NAT	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit

WAN Interface IPv4 Network Status

項目	値設定	説明
----	-----	----

ID	-	対応する WAN インターフェイスの WAN ID を表示します。
Interface	-	WAN 物理インターフェイスのタイプを表示します。 購入したモデルに応じて、Ethernet、3G/4G、USB 3G/4G を使用することができます。
WAN Type	-	ISP から公開 IP アドレスを取得する方法を表示します。購入したモデルに応じて、Static IP（静的 IP）、Dynamic IP（動的 IP）、PPPoE、PPTP、L2TP、3G/4G を使用することができます。
Network Type	-	[NAT Mode]、[Bridge Mode]、または [NAT Disable] を表示します。
IP Addr.	-	インターネット接続用に ISP から取得したパブリック IP アドレスが表示されます。未設定の場合、デフォルト値は 0.0.0.0 です。
Subnet Mask	-	インターネット接続用に ISP から取得したパブリック IP アドレスのサブネットマスクが表示されます。未設定の場合、デフォルト値は 0.0.0.0 です。
Gateway	-	インターネット接続用に ISP から取得したゲートウェイの IP アドレスが表示されます。未設定の場合、デフォルト値は 0.0.0.0 です。
DNS	-	インターネット接続用に ISP から取得した DNS サーバーの IP アドレスが表示されます。未設定の場合、デフォルト値は 0.0.0.0 です。
MAC Address	-	インターネットアクセスを許可する ISP の MAC アドレスが表示されます。注：すべての ISP がこのフィールドを必要とするわけではありません。
Conn. Status	-	ISP に対するデバイスの接続状態を表示します。 ステータスは、Connecting（接続中）、Connected（接続） Disconnecting（切断中）、または Disconnected（切断）です。
Action	-	この領域には機能ボタンがあります。 Renew ボタンを使用すると、デバイスは、DHCP サーバーから IP アドレスを要求させることができます。 注：Renew ボタンは、DHCP WAN タイプを使用し、WAN 接続が切断されている場合に利用可能です。 Release ボタンを使用すると、デバイスは IP アドレス設定をクリアし、DHCP サーバーから切断されます。 注：Release ボタンは、DHCP WAN タイプを使用し、WAN 接続が切断されている場合に利用可能です。 Connect ボタンを使用すると、デバイスをインターネットに手動で接続することができます。 注：Connect ボタンは、WAN タイプの Connection Control が Connect Manually に設定され、（Basic Network > WAN & Uplink > Connection Setup の Edit ボタンを参照）WAN 接続ステータスが切断されている時、（Conn. Status が disconnected）に利用可能です。

Disconnect ボタンを使用すると、デバイスをインターネットに手動で切断することができます。
 注： Disconnect ボタンは、WAN タイプの Connection Control が Connect Manually に設定され、(Basic Network > WAN & Uplink > Connection Setup の Edit ボタンを参照) WAN 接続ステータスが接続の時、(Conn. Status が connected) に利用可能です。

LAN インターフェイスネットワークステータス

LAN Interface Network Status ウィンドウには、LAN ネットワークの IPv4 の情報が表示されます。

LAN Interface Network Status			
IPv4 Address	IPv4 Subnet Mask	MAC Address	Action
192.168.123.254	255.255.255.0	00:50:18:21:EF:37	Edit IPv4

LAN Interface Network Status

項目	値設定	説明
IPv4 Address	-	ゲートウェイの現在の IPv4 IP アドレスを表示します。 また、これは、ルーターの Web ベースユーティリティにアクセスするために、ユーザーが使用する IP アドレスでもあります。
IPv4 Subnet Mask	-	サブネットの現在のマスクを表示します。
MAC Address	-	
Action	-	この領域には機能ボタンがあります。 Edit IPv4 ボタン 押すと、イーサネット LAN 設定ページに移動します。(Basic Network (> LAN > Ethernet LAN タブ)。

3G/4G モデムステータス

3G/4G Modem Status List (3G/4G モデムステータスリスト) ウィンドウには、3G/4G WAN ネットワークのステータス情報が表示されます。

3G/4G Modem Status List Refresh					
Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	ME3620-J	Disconnected	N/A		Detail

3G/4G Modem Status List		
項目	値設定	説明
Physical Interface	-	WAN 物理インターフェイス 3G/4G のタイプを表示します。 注： デバイスモデルによっては、2つの 3G/4G モジュールをサポートするものもあります。物理インターフェイス名は、3G/4G-1 および 3G/4G-2 になります。
Card Information	-	ベンダーの 3G/4G モデムモデル名を表示します。
Link Status	-	3G/4G 接続ステータスを表示します。ステータスは、Connecting（接続中）、Connected（接続）、Disconnecting（切断中）、および、Disconnected（切断）となります。
Signal Strength	-	3G/4G 無線信号レベルを表示します。
Network Name	-	サービスネットワーク通信事業者の名前が表示されます。
Refresh	-	Refresh ボタンをクリックして、情報を更新します。
Action	-	この領域には機能ボタンがあります。 Detail ボタン 押すと、詳細情報ウィンドウが表示されます。Modem Information（モデム情報）、SIM Status（SIM ステータス）、および、Service Information（サービス情報）です。詳細については、次のページを参照してください。 注： 現在、USB 3G/4G は、この機能をサポートしていません。

Detail ボタンを押すと、**Modem Information**（モデム情報）、**SIM Status**（SIM ステータス）、**Service Information**（サービス情報）、**Strength and Quality**（信号強度/品質）、および **Error Message**（エラー情報）、などの 3G/4G モデム情報ウィンドウが表示されます。

Modem Information							
Interface	Module Name	IMEI/MEID	HW Version	FW Version	Temperature	Band List	
N/A	EC25	861107037124444	J	EC25JFAR06A05M4G	N/A	N/A	
SIM Status							
SIM	PIN Code Status	PIN / PUK Code Remaining Times			IMSI	SMSC	MSISDN
N/A	SIM card not insert	N/A / N/A			N/A	N/A	N/A
Service Information							
Operator	MCC	MNC	Service Type	Band	LAC	TAC	Cell ID
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CS / PS Register Status			PS Attached Status		Roaming Status		
Unregistered / Unregistered			Detached		Not Roaming		
Signal Strength and Quality							
RSSI	RSRP	RSRQ	SINR	RSCP	EcIo		
N/A	N/A	N/A	N/A	N/A	N/A		
Error Message							
Profile Index	Error Description						
1	N/A						

インターフェイストラフィック統計

Interface Traffic Statistics ウィンドウには、インターフェイスの合計送信パケット数が表示されます。

Interface Traffic Statistics				
ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	3G/4G	0	0	<input type="button" value="Reset"/>

Interface Traffic Statistics		
項目	値設定	説明
ID	-	対応する WAN インターフェイスの WAN ID を表示します。
Interface	-	WAN 物理インターフェイスのタイプを表示します。

Received Packets	-	ダウンストリームパケットを表示します。デバイスが再起動するとリセットされます。
Transmitted Packets	-	アップストリームパケットを表示します。デバイスが再起動するとリセットされます。
Action	-	[Reset] ボタンをクリックして、統計情報全体がクリアされ、カウンタが0にリセットされます。

8.1.2 LAN ステータス

Status > Basic Network > LAN タブに進みます。

クライアントリスト

Client List には、このゲートウェイに接続されている各デバイスの LAN Interface、IP address、Host Name、MAC Address、および Remaining Lease Time が表示されます。表示は 5 秒ごとに更新されます。

LAN Client List				
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.1.100	amit-25611230-1	00-01-0A-10-0F-17	23:59:51

LAN Client List		
項目	値設定	説明
LAN Interface	-	LAN インターフェイスのクライアントレコード。文字列形式です。
IP Address	-	IP アドレスタイプと IP アドレスのクライアントレコード。タイプは文字列フォーマットで、IP アドレスは IPv4 フォーマットです。
Host Name	-	ホスト名のクライアントレコード。文字列形式です。
MAC Address	-	MAC アドレスのクライアントレコード。MAC アドレス形式です。
Remaining Lease Tim	-	残りリース時間のクライアントレコード。時間形式です。

8.1.3 DDNS ステータス

Status > Basic Network > DDNS タブに進みます。

DDNS Status ウィンドウには、使用中の現在の DDNS サービス、最後の更新ステータス、および、DDNS サービスサーバーへの最終更新時間が表示されます。

DDNS ステータス

DDNS Status List				
Host Name	Provider	Effective IP	Last Update Status	Last Update Time

DDNS Status List		
項目	値設定	説明
Host Name	-	DDNS サービスプロバイダを識別するために入力した名称が表示されます
Provider	-	DDNS サービスプロバイダの DDNS サーバーを表示します
Effective IP	-	DDNS サーバーに更新されたデバイスのパブリック IP アドレスを表示します
Last Update Status	-	DDNS サーバーに対するデバイスパブリック IP アドレスの最終更新が、成功したか (OK) 失敗したか (Fail) を表示します。
Last Update Time	-	パブリック IP アドレスの最終更新のタイムスタンプを DDNS サーバーに表示します。
Refresh	-	refresh ボタンを使用すると、ディスプレイに強制的に情報をリフレッシュさせることができます。

8.2 セキュリティ

8.2.1 VPN ステータス

Status > Security > VPN タブに進みます。

VPN Status ウィンドウには、VPN トンネルの全体的なステータスが表示されます。表示は 5 秒ごとに更新されます。

IPSec トンネルステータス

IPSec Tunnel Status ウィンドウには、IPSec VPN 接続と現在の接続ステータスを確立するための設定が表示されます。

IPSec Tunnel Status						
Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status

IPSec Tunnel Status		
項目	値設定	説明
Tunnel Name	-	識別するために入力したトンネル名が表示されます。
Tunnel Scenario	-	指定されたトンネルシナリオが表示されます。
Local Subnet	-	指定されたローカルサブネットが表示されます。
Remote IP/FQDN	-	指定されたリモート IP/FQDN が表示されます。
Remote Subnet	-	指定されたリモートサブネットが表示されます。
Conn. Time	-	IPSec トンネルの接続時間を表示します。

Status	-	VPN 接続のステータスが表示されます。ステータス表示は、Connected（接続）、Disconnected（切断）、Wait for traffic（トラフィック待ち）、および Connecting（接続中）です。
Edit Button	-	Edit ボタンをクリックして、IPSec 設定を変更すると、IPSec 設定ページにリダイレクトされます。（Security > VPN > IPSec タブ）

OpenVPN サーバーステータス

OpenVPN 設定に従い、OpenVPN サーバークライアントステータスは、サーバ側またはクライアント側から OpenVPN 接続のステータスおよび統計情報を表示します。

OpenVPN Server Status		Edit		
User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status
OpenVPN Server Status				
項目	値設定	説明		
User Name	-	識別のために入力したクライアント名が表示されます。		
Remote IP/FQDN	-	接続されている OpenVPN クライアントのパブリック IP アドレス（WAN IP アドレス）を表示します		
Virtual IP/MAC	-	接続された OpenVPN クライアントに割り当てられた仮想 IP/MAC アドレスが表示されます。		
Conn. Time	-	対応する OpenVPN トンネルの接続時間を表示します。		
Status	-	対応する OpenVPN トンネルの接続ステータスを表示します。ステータスは、 Connected （接続）または Disconnected （切断）です。		

OpenVPN クライアントステータス

OpenVPN Client Status										Edit
OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	TUN/TAP Read(bytes)	TUN/TAP Write(bytes)	TCP/UDP Read(bytes)	TCP/UDP Write(bytes)	Conn. Time	Conn. Status	
OpenVPN Client Status										
項目	値設定	説明								
OpenVPN Client Name	-	識別のために入力したクライアント名が表示されます。								
Interface	-	OpenVPN クライアント接続用に指定された WAN インターフェイスが表示されます。								
Remote IP/FQDN	-	OpenVPN クライアント接続用に指定された WAN インターフェイスが表示されます。								
Remote Subnet	-	指定されたリモートサブネットが表示されます。								
TUN/TAP Read(bytes)	-	OpenVPN クライアントの TUN/TAP 読み取りバイト数を表示します。								
TUN/TAP Write(bytes)	-	OpenVPN クライアントの TUN/TAP 書き込みバイト数を表示します。								

TCP/UDP Read(bytes)	-	OpenVPNクライアントのTCP/UDP読み取りバイト数を表示します。
TCP/UDP Write(bytes)	-	OpenVPNクライアントのTCP/UDP書き込みバイト数を表示します。
Conn. Time	-	対応するOpenVPNトンネルの接続時間を表示します。
Conn. Status	-	対応するOpenVPNトンネルの接続ステータスを表示します。ステータスは、 Connected （接続）または Disconnected （切断）です。

L2TP サーバー/クライアントステータス

L2TP Server/Client Status は、L2TP トンネルを確立するための設定と現在の接続状態を示します。

L2TP Server Status Edit					
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

L2TP Server Status		
項目	値設定	説明
User Name	-	接続に使用されたユーザーのログイン名が表示されます。
Remote IP	-	接続されている L2TP クライアントのパブリック IP アドレス（WAN IP アドレス）を表示します。
Remote Virtual IP	-	接続された L2TP クライアントに割り当てられた IP アドレスが表示されます。
Remote Call ID	-	L2TP クライアントのコール ID が表示されます。
Conn. Time	-	L2TP トンネルの接続時間を表示します。
Status	-	各 L2TP クライアント接続のステータスを表示します。ステータスに、Connected（接続）、Disconnect（切断）、および、Connecting（接続中）が表示されます。
Edit	-	Edit ボタンをクリックして、L2TP サーバー設定を変更すると、L2TP サーバー設定ページにリダイレクトされます。（Security > VPN > L2TP タブ）

L2TP Client Status Edit						
L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

L2TP Client Status		
項目	値設定	説明
Client Name	-	指定された L2TP クライアントの名称が表示されます。
Interface	-	ゲートウェイが、PPTP サーバーへの PPTP トンネリング接続を要求するために使用する WAN インターフェイスを表示します。
Virtual IP	-	L2TP サーバーの仮想 IP サーバーが割り当てた IP アドレスを表示します。
Remote IP/FQDN	-	L2TP サーバーのパブリック IP アドレス（WAN IP アドレス）または FQDN が表示されます。

Default Gateway / Remote Subnet	-	デフォルトゲートウェイである L2TP サーバーに接続するためのインターネット接続に使用されるゲートウェイデバイスの指定 IP アドレスが表示されます。または、デフォルトゲートウェイが L2TP サーバーに接続するために使用されていない場合は、他の指定されたサブネット（リモートサブネット）が表示されます。
Conn. Time	-	L2TP トンネルの接続時間を表示します。
Status	-	VPN 接続のステータスが表示されます。ステータスに、Connected（接続）、Disconnect（切断）、および、Connecting（接続中）が表示されます。
Edit	-	Edit ボタンをクリックして、L2TP クライアント設定を変更すると、L2TP クライアント設定ページにリダイレクトされます。（Security > VPN > L2TP タブ）

PPTP サーバー/クライアントステータス

PPTP Server/Client Status は、PPTP トンネルを確立するための設定と現在の接続状態を示します。

PPTP Server Status Edit					
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

PPTP Server Status		
項目	値設定	説明
User Name	-	接続に使用されたユーザーのログイン名が表示されます。
Remote IP	-	PPTP クライアントのパブリック IP アドレス（WAN IP アドレス）を表示します。
Remote Virtual IP	-	接続された PPTP クライアントに割り当てられた IP アドレスが表示されます。
Remote Call ID	-	PPTP クライアントのコール ID が表示されます。
Conn. Time	-	PPTP トンネルの接続時間を表示します。
Status	-	各 PPTP クライアント接続のステータスを表示します。ステータスに、Connected（接続）、Disconnect（切断）、および、Connecting（接続中）が表示されます。
Edit Button	-	Edit ボタンをクリックして、PPTP サーバー設定を変更すると、PPTP サーバー設定ページにリダイレクトされます。（Security > VPN > PPTP タブ）

PPTP Client Status							Edit
PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status	

PPTP Client Status		
項目	値設定	説明
Client Name	-	指定された PPTP クライアントの名称が表示されます。
Interface	-	ゲートウェイが、PPTP サーバーへの PPTP トンネリング接続を要求するために使用する WAN インターフェイスを表示します。
Virtual IP	-	PPTP サーバーの仮想 IP サーバーが割り当てた IP アドレスを表示します。
Remote IP/FQDN	-	PPTP サーバーのパブリック IP アドレス (WAN IP アドレス) または FQDN が表示されます。
Default Gateway / Remote Subnet	-	デフォルトゲートウェイである PPTP サーバーに接続するためにインターネットに接続するために使用されるゲートウェイデバイスの指定された IP アドレスが表示されます。または、デフォルトゲートウェイが、PPTP サーバーに接続するために使用されていない場合は、他の指定されたサブネット-リモートサブネットが表示されます。
Conn. Time	-	PPTP トンネルの接続時間を表示します。
Status	-	VPN 接続のステータスが表示されます。ステータスに、Connected (接続)、Disconnect (切断)、および、Connecting (接続中) が表示されます。
Edit Button	-	Edit ボタンをクリックして、PPTP クライアント設定を変更すると、PPTP サーバー設定ページにリダイレクトされます。(Security > VPN > PPTP タブ)

8.2.2 ファイアウォールステータス

Status > Security > Firewall Status タブに進みます。

Firewall Status は、ファイアウォールのステータスと現在のファイアウォール設定を表示します。また、ファイアウォールルールポリシーによってドロップされたパケットのログ履歴が保持され、ファイアウォールオプションで指定された管理者のリモートログイン設定も含まれます。表示は 5 秒ごとに更新されます。

アイコン[+]をクリックすると、ステータステーブルが展開され、ログ履歴が表示されます。Edit ボタンをクリックすると、画面が設定ページに切り替わります。

パケットフィルタステータス

Packet Filters Edit [+]			
Activated Filter Rule	Detected Contents	IP	Time

Packet Fileters		
項目	値設定	説明
Activated Filter Rule	-	これは、パケットフィルタルール名です。
Detected Contents	-	これは、送信元 IP、宛先 IP、プロトコル、および宛先ポート (TCP または UDP) を含む、記録されたパケット情報です。 文字列形式： ソース IP から宛先 IP へ：宛先プロトコル (TCP または UDP)
IP	-	記録されたパケットの送信元 IP (IPv4)。
Time	-	記録されたパケットの日付と時刻。日付と時刻の形式。 ("月" "日" "時間" : "分" : "秒")

注：パケットフィルタログアラートが有効になっていることを確認してください。

Security > Firewall > Packet Filter タブを参照してください。Log Alert にチェックを入れ、設定を保存します。

MAC 制御ステータス

MAC Control Edit [+]			
Activated Control Rule	Blocked MAC Addresses	IP	Time

MAC Control 項目	値設定	説明
Activated Control Rule	-	MAC 制御ルール名を表示します。
Blocked MAC Addresses	-	これは、記録されたパケットの MAC アドレスを表示します。
IP	-	記録されたパケットの送信元 IP (IPv4) を表示します。
Time	-	記録されたパケットの日付と時刻。日付と時刻の形式を表示します。 ("月" "日" "時間" : "分" : "秒")

注：MAC Control Log Alert が有効になっていることを確認します。

Security > Firewall > MAC Control タブを参照してください。Log Alert にチェックを入れ、設定を保存します。

IPS ステータス

IPS Edit [+]			
Detected Intrusion		IP	Time

IPS 項目	値設定	説明
Detected Intrusion	-	これはブロックされているパケットの侵入タイプです。
IP	-	記録されたパケットの送信元 IP (IPv4)。
Time	-	記録されたパケットの日付と時刻。日付と時刻の形式。 ("月" "日" "時間" : "分" : "秒")

注：IPS Log Alert が有効になっていることを確認します。

Security > Firewall > IPS タブを参照してください。Log Alert にチェックを入れ、設定を保存します。

ファイアウォールオプションステータス

Options Edit [+]			
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

Options 項目	値設定	説明
Stealth Mode	-	Firewall Options 上の、Stealth Mode の設定ステータスが表示されます。文字列形式： Disable （無効）または Enable （有効）
SPI	-	Firewall Options 上の、SPI の設定ステータスを表示します。文字列形式： Disable （無効）または Enable （有効）
Discard PING from WAN	-	Firewall Options 上で、WAN からの Ping 破棄の設定ステータスを表示します。 文字列形式： Disable （無効）または Enable （有効）
Remote Administrator Management	-	Remote Administrator（リモート管理者）の設定ステータスを表示します。Remote Administrator（リモート管理者）が有効になっている場合は、現在ログインしている管理者の送信元 IP アドレスとログインユーザー名とログイン時間が表示されます。 形式： IP：「 Source IP 」、ユーザー名：「 Login User Name 」、時刻：「 Date time 」 例： IP：192.168.127.39、ユーザー名：admin、時刻：Mar 3 01:34:13

注：ファイアウォールオプションログアラートが有効になっていることを確認します。

Security > Firewall > Options タブを参照してください。 **Log Alert** にチェックを入れ、設定を保存します。

8.3 管理

8.3.1 設定および管理ステータス

Status > Administration > Configure & Manage タブに進みます。

Configure & Manage Status ウィンドウには、リモートネットワークデバイスを管理するためのステータスが表示されます。デバイスで使用できる管理の種類は、購入したデバイスモデルによって異なります。よく使われるのは、SNMP、TR-069、UPnP です。表示は 5 秒ごとに更新されます。

SNMP リンクステータス

SNMP Link Status ウィンドウには、現在有効な SNMP 接続のステータスが表示されます。

SNMP Linking Status						
User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

SNMP Linking Status		
項目	値設定	説明
User Name	-	認証のためのユーザー名が表示されます。これは、SNMP バージョン 3 でのみ利用可能です。
IP Address	-	SNMP マネージャの IP アドレスを表示します。
Port	-	SNMP マネージャとの接続を維持するために使用されるポート番号が表示されます。
Communit	-	SNMP バージョン 1 またはバージョン 2c のコミュニティのみを表示します。
Auth. Mode	-	SNMP バージョン 3 の認証方法のみを表示します。
Privacy Mode	-	バージョン 3 のプライバシーモードのみを表示します。
SNMP Version	-	使用されている SNMP のバージョンが表示されます。

SNMP トラップ情報

SNMP Trap Information ウィンドウには、現在受信している SNMP トラップのステータスが表示されます。

SNMP Trap Information		
Trap Level	Time	Trap Event

SNMP Ttrap Information		
項目	値設定	説明
Trap Level	-	トラップレベルが表示されます。
Time	-	トラップイベントのタイムスタンプを表示します。
Trap Event	-	トラップ送信者の IP アドレスとイベントタイプが表示されま す。

TR-069 ステータス

TR-069 Status (TR-069 ステータス) ウィンドウには、TR-069 サーバーとの現在の接続状態が表示されます。

TR-069 Status	
Link Status	
Off	

TR-069 Status		
項目	値設定	説明
Link Status	-	TR-069 サーバーとの現在の接続状態が表示されます。機器が TR-069 サーバーに接続されている場合は On (オン)、切断されている場合は Off (オフ) です。

8.4 統計およびレポート

8.4.1 接続状況

Status > Statistics & Reports > Connection Session タブに進みます。

Internet Surfing Statistic ウィンドウには、このルーター上の接続トラックが表示されます。

Internet Surfing List (143 entries) Previous Next First Last Export (.xml) Export (.csv)					
Refresh					
User Name	Protocol	Internal IP & Port	MAC	External IP & Port	Duration Time
	UDP	192.168.1.100:52284		192.168.1.254:53	2010/01/01 07:10~
	UDP	192.168.1.100:56881		192.168.1.254:53	2010/01/01 07:10~
	UDP	192.168.1.100:58539		192.168.1.254:53	2010/01/01 07:10~

Internet Surfing List		
項目	値設定	説明
Previous	-	Previous ボタンをクリックすると、トラックリストの前のページが表示されます。
Next	-	Next ボタンをクリックすると、トラックリストの次のページが表示されます。
First	-	First ボタンをクリックすると、トラックリストの最初のページが表示されます。
Last	-	Last ボタンをクリックすると、トラックリストの最後のページが表示されます。
Export (.xml)	-	Export (.xml) ボタンをクリックすると、リストを xml ファイル形式でエクスポートします。
Export (.csv)	-	Export (.csv) ボタンをクリックすると、リストを csv ファイル形式でエクスポートします。
Refresh	-	Refresh ボタンをクリックすると、リストが更新されます。

8.4.2 デバイス管理

Status > Statistics & Reports > Device Administration タブに進みます。

Device Administration ウィンドウは、ログイン統計情報が表示されます。

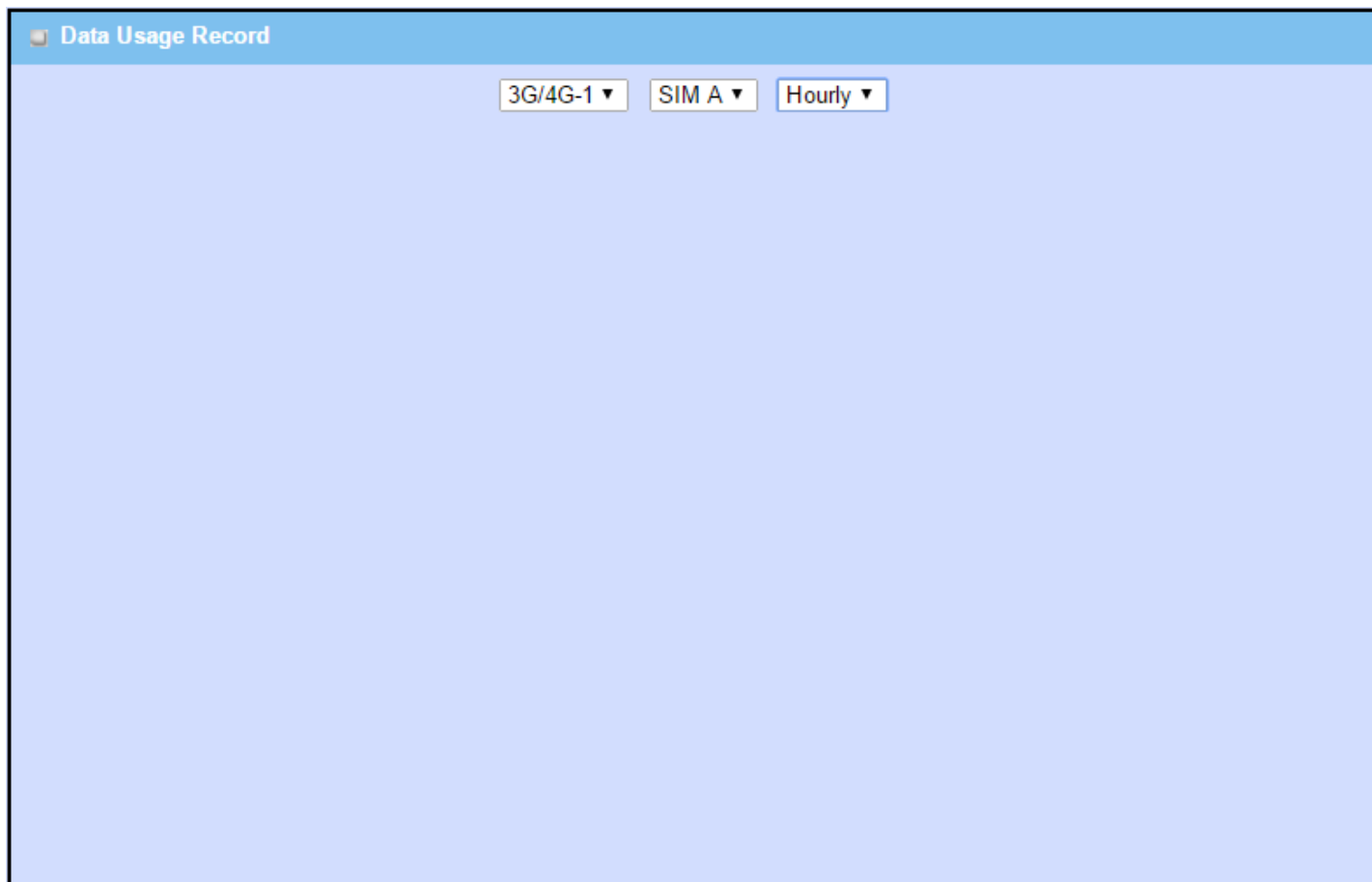
Device Manager Login Statistics				
User Name	Protocol Type	IP Address	User Level	Duration Time
admin	http/https	192.168.127.162	Admin	2015/11/12 04:17~

Manager Login Statistics		
項目	値設定	説明
Previous	-	Previous ボタンをクリックすると、ログイン統計の前のページが表示されます。
Next	-	Next ボタンをクリックすると、ログイン統計の次のページが表示されます。
First	-	First ボタンをクリックすると、ログイン統計の最初のページが表示されます。
Last	-	Last ボタンをクリックすると、ログイン統計の最後のページが表示されます。
Export (.xml)	-	Export (.xml) ボタンをクリックすると、ログイン統計を xml ファイル形式でエクスポートします。
Export (.csv)	-	Export (.csv) ボタンをクリックすると、ログイン統計を csv ファイル形式でエクスポートします。
Refresh	-	Refresh ボタンをクリックすると、ログイン統計が更新されます。

8.4.3 セルラー使用状況

Status > Statistics & Reports > Cellular Usage タブに進みます。

Cellular Usage ウィンドウには、選択したセルラーインターフェイスのデータ使用状況統計が表示されます。セルラーデータ使用状況は、1時間または1日に蓄積することができます。



第 9 章 Fieldbus

The screenshot shows the MMLink-GWL interface. On the left is a navigation menu with buttons for Field Communication, Security, Administration, Service, and Fieldbus. The main content area displays the IP address 192.168.123.254. Below this is a '3G/4G Modem Status List' section with a 'Refresh' button and a table:

Interface	Card Information	Link Status
3G/4G	ME3620-J	Disconnected

Below the modem status is an 'Interface Traffic Statistics' section with a table:

ID	Interface	Received Packets
WAN-1	3G/4G	0

ページ左部の「Fieldbus」ボタンをクリックすると、「Fieldbus 設定画面」へ遷移します。
「Fieldbus 設定画面」の詳細は、別紙「MMLink-GWL ユーザーマニュアル(Fieldbus 編)」をご参照下さい。

※ 「Fieldbus」ボタンが表示されない場合、以下の手順で Fieldbus 機能を有効化します。

- ① 「Administration > Configure & Manage > Command Script」を開く
- ② 「Configuration > Command Script > Enable」にチェック

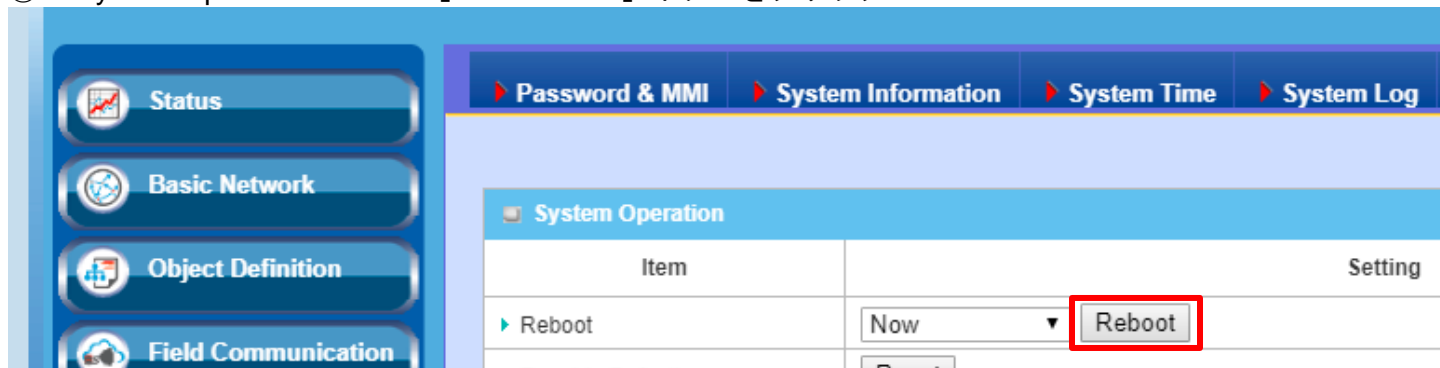
The screenshot shows the 'Command Script' configuration page. The left navigation menu includes Status, Basic Network, Object Definition, and Field Communication. The main content area has a breadcrumb trail: Command Script > TR-069 > SNMP > Telnet & SSH. Below this is a 'Configuration' section with a table:

Item	
Command Script	<input checked="" type="checkbox"/> Enable

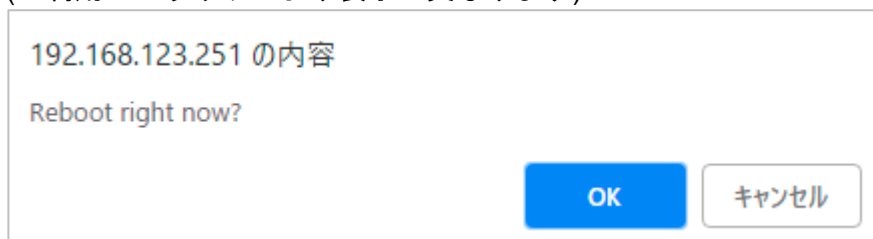
At the bottom of the page, there is a 'Save' button highlighted with a red box. The page number '42 / 65280' is also visible.

- ③ ページ下部の「Save」ボタンをクリック

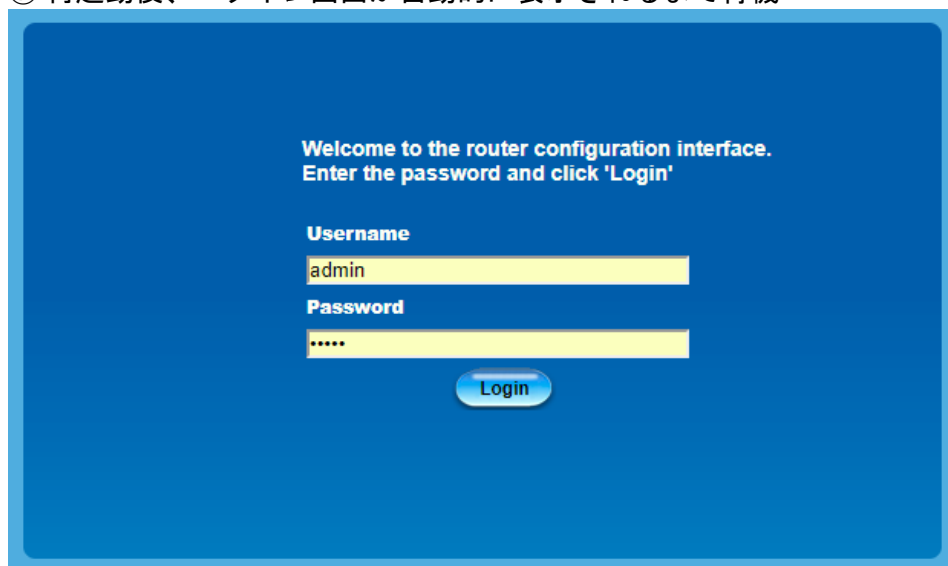
- ④ 「Administration > System Operation > Reboot & Reset」を開く
- ⑤ 「System Operation > Reboot」の「Reboot」ボタンをクリック



- ⑥ 確認ダイアログが表示されるので、「OK」ボタンをクリック
(ご利用のブラウザにより表示が異なります)



- ⑦ 再起動後、ログイン画面が自動的に表示されるまで待機



- ⑧ システム設定画面に再度ログインすると、ページ左部に「Fieldbus」ボタンが表示されます。

付録 A GNU ライセンスについて

本製品には、以下に含まれる第三者の著作権表示および使用許諾契約の条項の対象となるオープンソースソフトウェアコンポーネントが組み込まれています。

OpenSSL

バージョン 1.0.2c

著作権 (C) 1995-1998 Eric Young (eay@cryptsoft.com)

GPL ライセンス : <https://www.openssl.org/>

brctl - ethernet bridge administration

Stephen Hemminger <shemminger@osdl.org>

Lennert Buytenhek <buytenh@gnu.org>

バージョン 1.1

GNU 一般公衆利用許諾契約書バージョン 2 (1991 年 6 月)

tc - トラフィック制御設定の表示/操作

Stephen Hemminger<shemminger@osdl.org>

Alexey Kuznetsov<kuznet@ms2.inr.ac.ru>

バージョン iproute2-ss050330

GNU 一般公衆利用許諾契約書バージョン 2 (1991 年 6 月)

dhcp-fwd — DHCP 転送エージェントの開始

Enrico Scholz <enrico.scholz@informatik.tu-chemnitz.de>

バージョン 0.7

GNU 一般公衆利用許諾契約書バージョン 2 (1991 年 6 月)

dnsmasq - 軽量 DHCP サーバーとキャッシング DNS サーバー。

Simon Kelley <simon@thekelleys.org.uk>

バージョン : 2.72

dnsmasq は著作権 (c) 2000-2014 Simon Kelley

socat - 多目的リレー

バージョン : 2.0.0-b8

GPLv2

<http://www.dest-unreach.org/socat/>

Openswan

バージョン : v2.6.38 GNU 一般公衆利用許諾契約書バージョン 2 (1991 年 6 月)

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

この利用許諾契約書を、一字一句そのままに複製し頒布することは許可する。

しかし変更は認めない。

MMLink-GWL

<https://www.openswan.org/>

Opennhrp

バージョン : v0.14.1

OpenNHRP は、Linux 用の NHRP 実装です。ほとんどの RFC2332 と Cisco IOS 拡張があります。

プロジェクトのホームページ : <http://sourceforge.net/projects/opennhrp>

Git リポジトリ : <git://opennhrp.git.sourceforge.net/gitroot/opennhrp>

ライセンス

OpenNHRP は、MIT ライセンスの下でライセンスされています。詳細は、MIT-LICENSE.txt を参照してください。

OpenNHRP は libev を埋め込みます。libev は、2 節 BSD と

GPLv2 + ライセンスで二重ライセンスされています。詳細は、libev/LICENSE を参照してください。

OpenNHRP は c-ares にリンクしています。c-ares は、MIT ライセンスの下でライセンスされています。

<https://sourceforge.net/projects/opennhrp/>

IPSec-tools

バージョン : v0.8

GPL を書くことはできません

<http://ipsec-tools.sourceforge.net/>

PPTP

バージョン : pptp-1.7.1

GNU 一般公衆利用許諾契約書バージョン 2 (1991 年 6 月)

Copyright (C) 1989, 1991 Free Software Foundation, Inc.675 Mass Ave, Cambridge, MA 02139, USA

この利用許諾契約書を、一字一句そのままに複製し頒布することは許可する。

しかし変更は認めない。

<http://pptpclient.sourceforge.net/>

PPTPServ

バージョン : 1.3.4

GNU 一般公衆利用許諾契約書バージョン 2 (1991 年 6 月)

Copyright (C) 1989, 1991 Free Software Foundation, Inc.675 Mass Ave, Cambridge, MA 02139, USA

この利用許諾契約書を、一字一句そのままに複製し頒布することは許可する。

しかし変更は認めない。 <http://poptop.sourceforge.net/>

L2TP

バージョン : 0.4

コピーこのパッケージに含まれるすべてのソフトウェアは、2002Roaring

Penguin Software Inc.が著作権を所有しています お客様は、GNU 一般公衆利用許諾契約書 (

以下「GPL」) のバージョン 2、または、(お客様の選択により) それ以降のバージョンを条件として配布することができます。

<http://www.roaringpenguin.com/>

L2TPServ

バージョン : v 1.3.1 GNU 一般公衆利用許諾契約書バージョン 2 (1991 年 6 月)

MMLink-GWL

著作権 (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

この利用許諾契約書を、一字一句そのままに複製し頒布することは許可する。

しかし変更は認めない。

<http://www.xelerance.com/software/xl2tpd/>

Mpstat : Linux 用システムパフォーマンスツール sysstat から

バージョン : 10.1.6

著作権 : (C) 1999-2013 by Sebastien Godard (sysstat <at> orange.fr)

SSHD : dropbear、SSH2 サーバー

バージョン : 0.53.1

著作権 : (c) 2002-2008 Matt Johnston

Libncurses : ncurses (新しい curses) ライブラリは、System V Release 4.0 (SVr4) の curses のフリーソフトウェアエミュレーションなどです。

バージョン : 5.9

著作権 : (c) 1998,2000,2004,2005,2006,2008,2011,2015 Free Software Foundation, Inc., 51 Franklin Street, Boston, MA 02110-1301, USA

MiniUPnP : miniUPnP デモンは、ネットワーク上の UPnP 対応クライアントに NAT トラバーサルサービスを提供する UPnP IGD (インターネットゲートウェイデバイス) です。

バージョン : 1.7

著作権 : (c) 2006-2011, Thomas BERNARD

CoovaChilli は、キャプティブポータル (UAM) と 802.1X アクセスプロビジョニング用のオープンソースソフトウェアアクセスコントローラです。

バージョン : 1.3.0

著作権 : (C) 2007-2012 David Bird (Coova Technologies) <support@coova.com>

Krb5 : Kerberos は、ネットワーク認証プロトコルです。これは、秘密鍵暗号を使用して、クライアント/サーバーアプリケーションの強力な認証を提供するように設計されています。

バージョン : 1.11.3

著作権 : (C) 1985-2013 by the Massachusetts Institute of Technology and its contributors

NTPClient : UNIX 系のコンピュータ用の NTP (RFC-1305、RFC-4330) クライアント

バージョン : 2007_365

著作権 : 1997, 1999, 2000, 2003, 2006, 2007 Larry Doolittle

exFAT : FUSE ベースの exFAT 実装

バージョン : 0.9.8

著作権 : (C) 2010-2012 Andrew Nayenko

ONTFS_3G : NTFS-3G ドライバは、Linux、FreeBSD、Mac OS X、NetBSD、Solaris、および Haiku 用のオープンソースで、自由に読み書き可能な NTFS ドライバです。

MMLink-GWL

バージョン : 2009.4.4

著作権 : (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

mysql-5_1_72 : MySQL のリリース、デュアルライセンス SQL データベースサーバー

バージョン : 5.1.72

著作権 : (c) 2000, 2013, Oracle and/or its affiliates

FreeRadius : 高性能で設定可能な RADIUS サーバー

バージョン : 2.1.12

著作権 : (C) 1999-2011 The FreeRADIUS server project and contributors

LinuxIPv6 ルーター広告デーモン- radvd

バージョン : V 1.15

Copyright (c) 1996,1997 by Lars Fenneberg<lf@elemental.net>

BSD ライセンス : <http://www.litech.org/radvd/>

WIDE-DHCPv6

IPv6 (DHCPv6) クライアント、サーバー、およびリレーエージェント用の動的ホスト設定プロトコル。

バージョン : 20080615

Copyright (C) 1998-2004 WIDE Project.

BSD ライセンス : <https://sourceforge.net/projects/wide-dhcpv6/>

技術的なお問い合わせ相談窓口

●サポートセンター

TEL : (03)5500-7293

E-MAIL : mmlink_support@ye-digital.com

月～金（祝祭日及び当社休業日は除く）／9:00～12:00, 13:00～17:00

※ E-MAIL は 24 時間受け付けております。

IoT/M2M ゲートウェイ MMLink-GWL

ユーザーマニュアル（基本編）

2019年12月23日 第1.4版

販売元 株式会社 YE DIGITAL <https://www.ye-digital.com>

東京都港区芝五丁目36番7号 三田ベルジュビル9F 〒108-0014

TEL : (03)6865-8900 FAX : (03)6865-8903