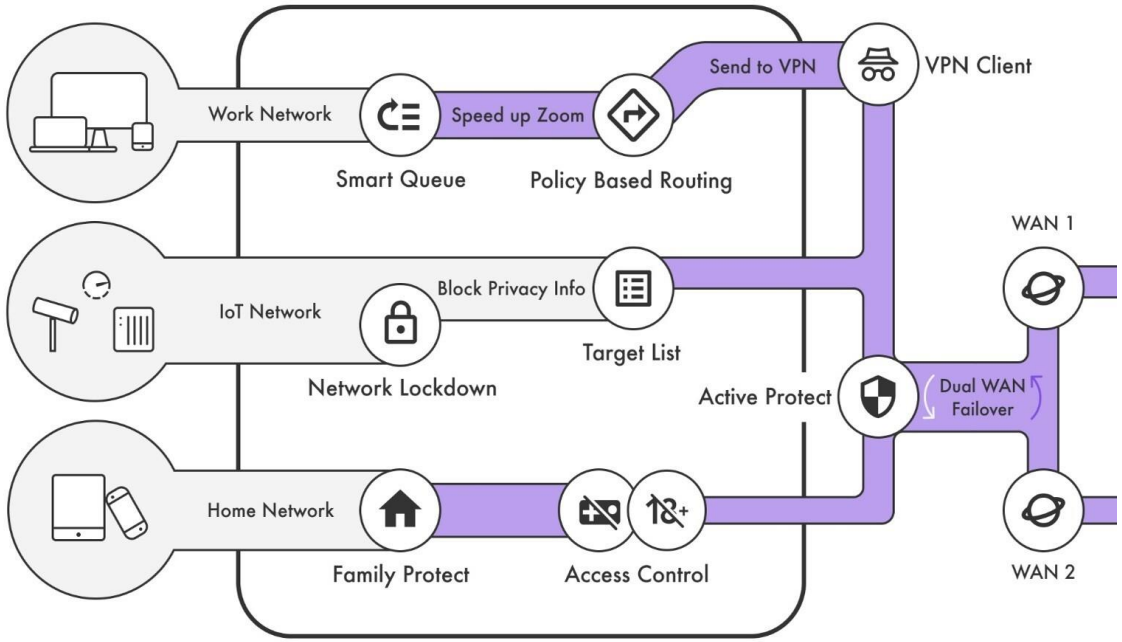
ネットワーク防御②　ルール設定

ネットワークの防御

ネットワークとデバイスを可視化したら、次は、ネットワークの「ルール」または「ポリシー」を作成します。
Firewallaは、ネットワーク上のトラフィックをブロック、許可、規制するためのさまざまな方法を提供します。
ネットワーク トラフィックを制御することで、ネットワークの攻撃対象とリスクを軽減します。



Firewallaでは、次のことが可能です。
1. ブロックルールで不要なアクセスをブロック
2. 「許可」ルールで信頼できるネットワークを許可する
3. 認識されない、または未使用のポートをブロックする
4. 子供向けにファミリーモードを有効にする
5. ネットワークセグメンテーションによるトラフィックの分離
6. デバイスグループによるデバイスの管理
7. ルートによるトラフィックの制御
8. Smart Queueでトラフィックを規制する
9. 広告ブロックでプライバシーを保護
10. DoH、アンバウンド、および DNS ルールを使用してDNSトラフィックを制御する
11. Firewalla VPNによる安全なネットワーク アクセス
12. 新しいデバイスを隔離する

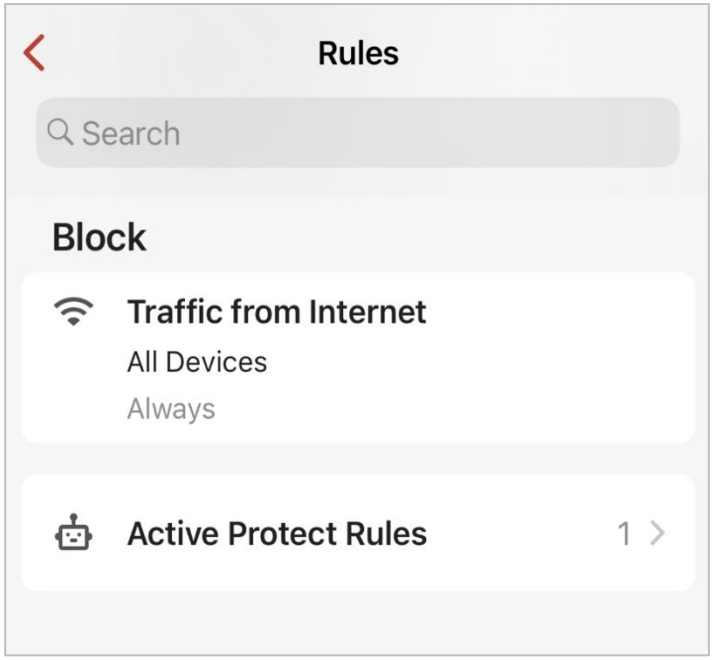
1. ブロックルールで不要なアクセスをブロックする

ブロック機能を利用すると、デバイスのネットワーク アクセスを制限可能です。
次のような一連のブロック機能を通じて、望ましくないネットワークの使用を制限することができます。

- 1.1. デフォルトのステートフル ファイアウォール
- 1.2. [ルール] ボタンによるドメイン/IP/IP範囲のブロック
- 1.3. アラーム経由のブロック
- 1.4. ネットワークフロー経由のブロック
- 1.5. アクティビティカテゴリブロック
- 1.6. 地域ブロック (Geo-IPフィルタリング)
- 1.7. TLDブロック
- 1.8. アプリケーションブロック

1.1. デフォルトのステートフル ファイアウォール

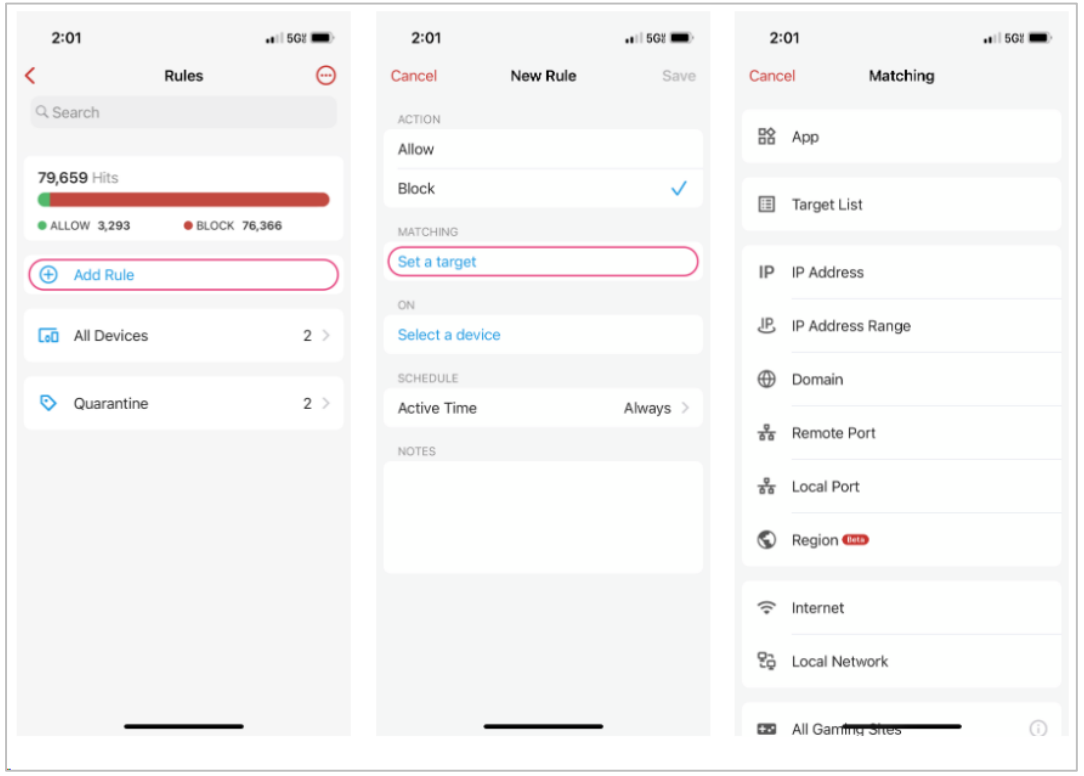
Firewllaをルーター モードで使用している場合、Firewallaはデフォルトで「ステートフル」ファイアウォールを実行し、すべての受信トラフィック (ネットワークの外部から内部へ) をブロックします。
このルールを削除したり一時停止したりしないでください。



1.2. [ルール] ボタンによるドメイン/ IP/IP 範囲のブロック

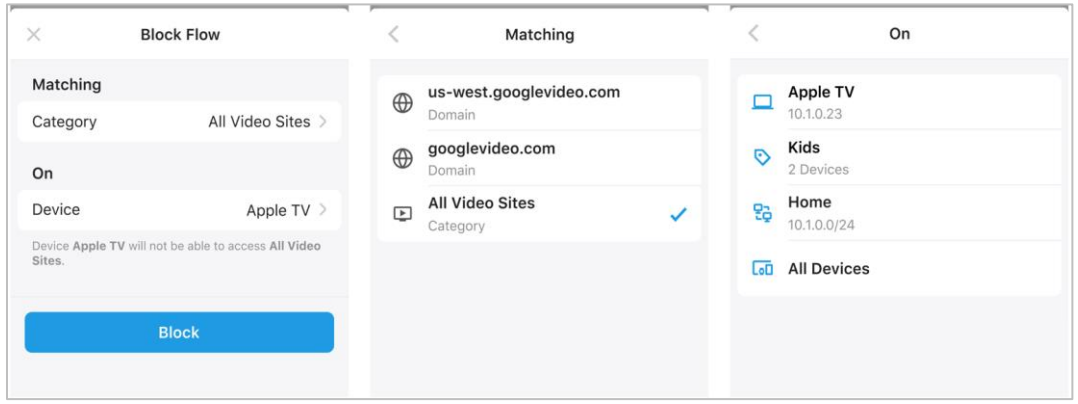
「ルール」ボタンを使用してターゲットをブロックできます。
次の項目の 1 つまたは組み合わせに基づいて、許可/ブロックするターゲットを設定できます。

- IPアドレス (およびオプションのポート)
- IPアドレス範囲 (およびオプションのポート)
- ドメイン名 (およびオプションのポート)
- リモート ポート (任意のIPまたはドメインに適用)
- 地域
- ローカル ネットワーク (Gold PlusとPurple SEはルーターモードでのみ実行)
- インターネット (すべてのインターネット サイト)
- インターネットサイトのカテゴリリスト



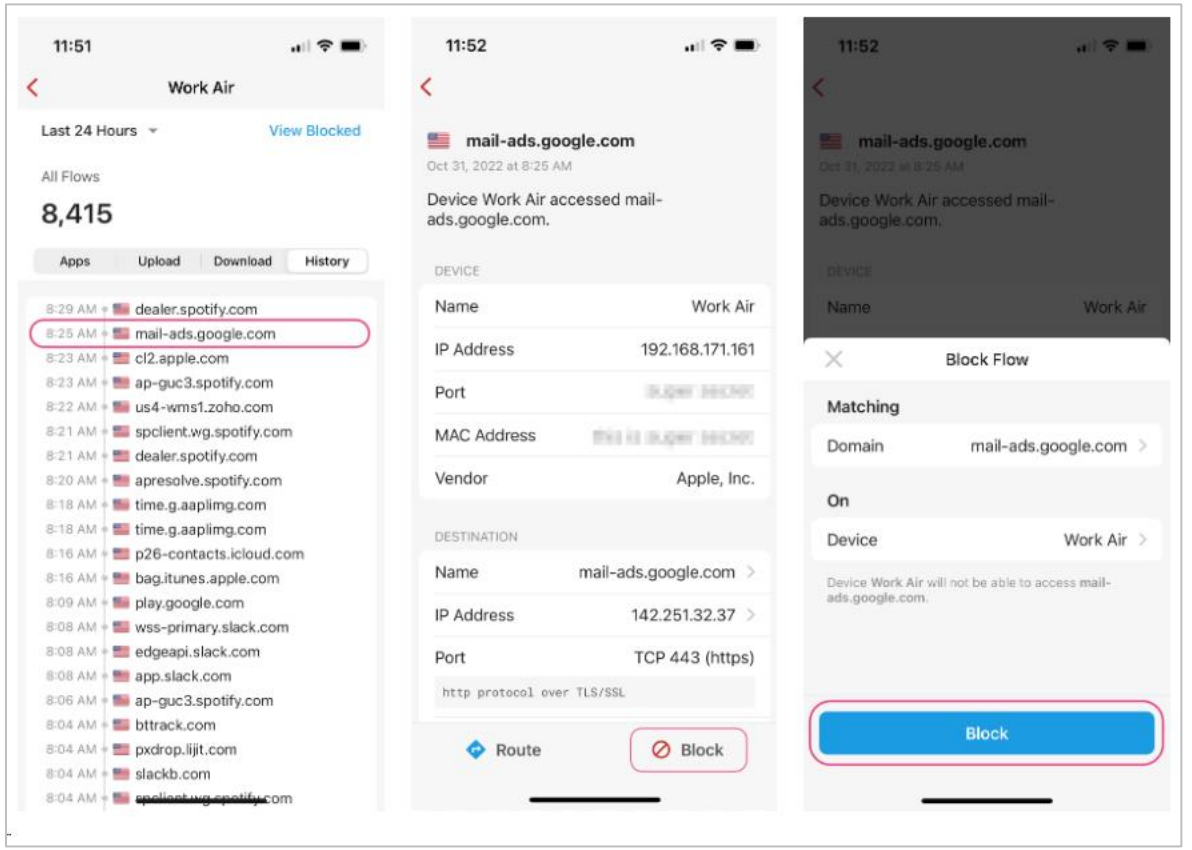
1.3. アラーム経由のブロック

ブロックはアラーム インターフェイスから設定することもできます。
あるデバイスが悪意のあるサイトにアクセスしているというアラームを受け取った場合、
アラーム通知画面からドメインまたはIP全体をブロックできます。



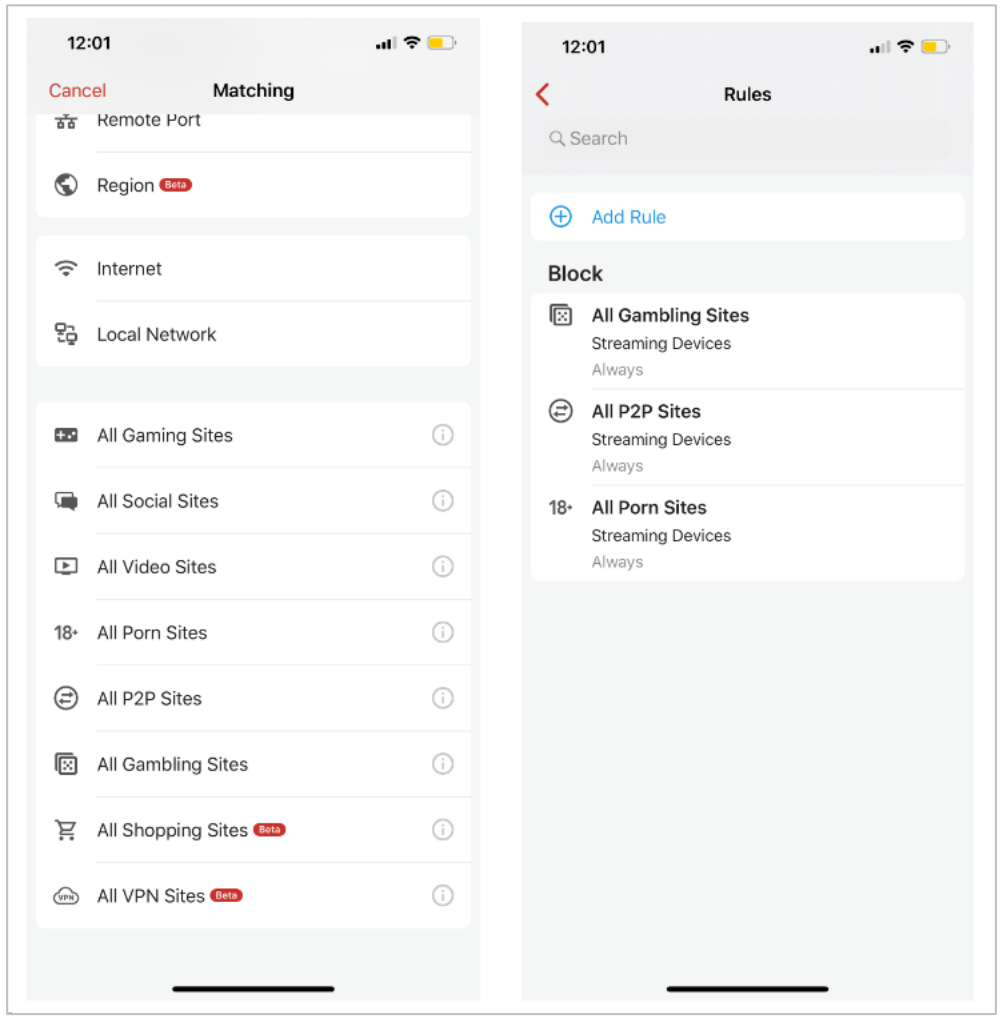
1.4. ネットワークフロー経由のブロック

デバイスのネットワーク フローを確認しているときに、そのフロー エントリをタップして詳細画面を表示できます。
詳細画面から、フローをブロックできます。



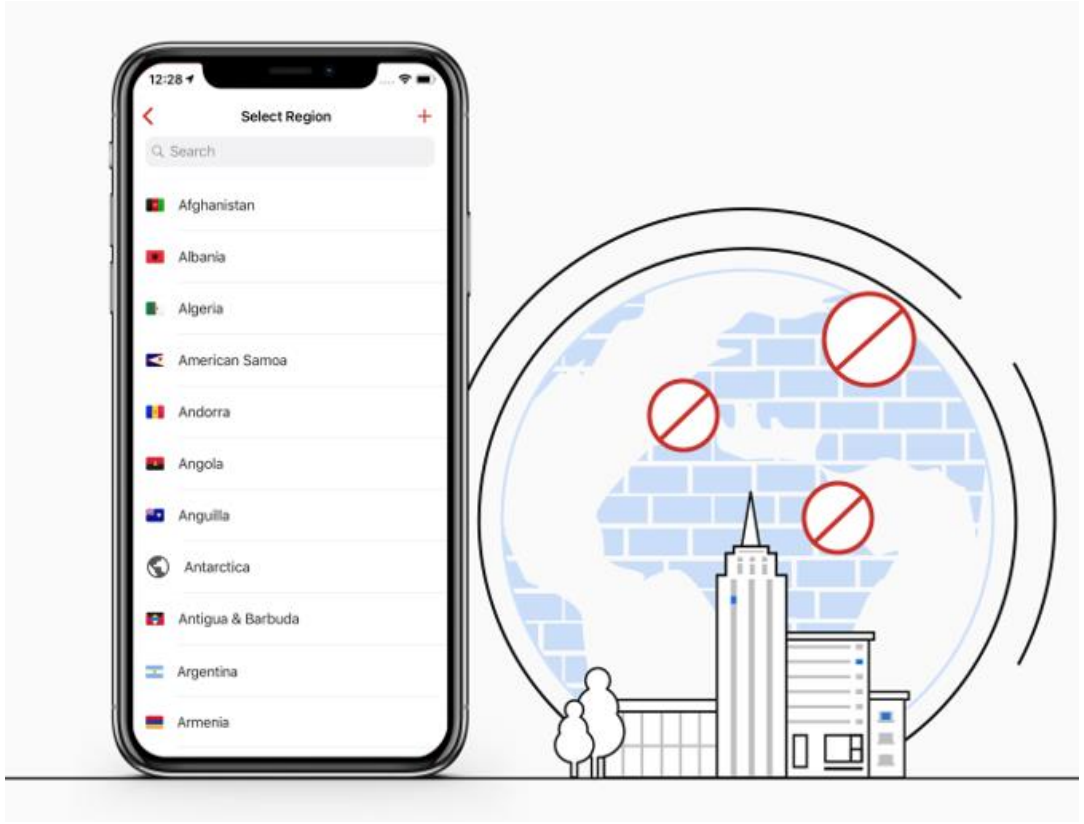
1.5. アクティビティカテゴリブロック

汎用コンピュータに近い機能を持つスマートデバイスの場合は、コンピュータやスマートフォンと同様の制御を実装する必要があります。
たとえば、子供がスマートTVを使用している場合、カテゴリのブロック機能を使用して、子供がアクセスしてはいけないサイトにアクセスしないようにすることができます。



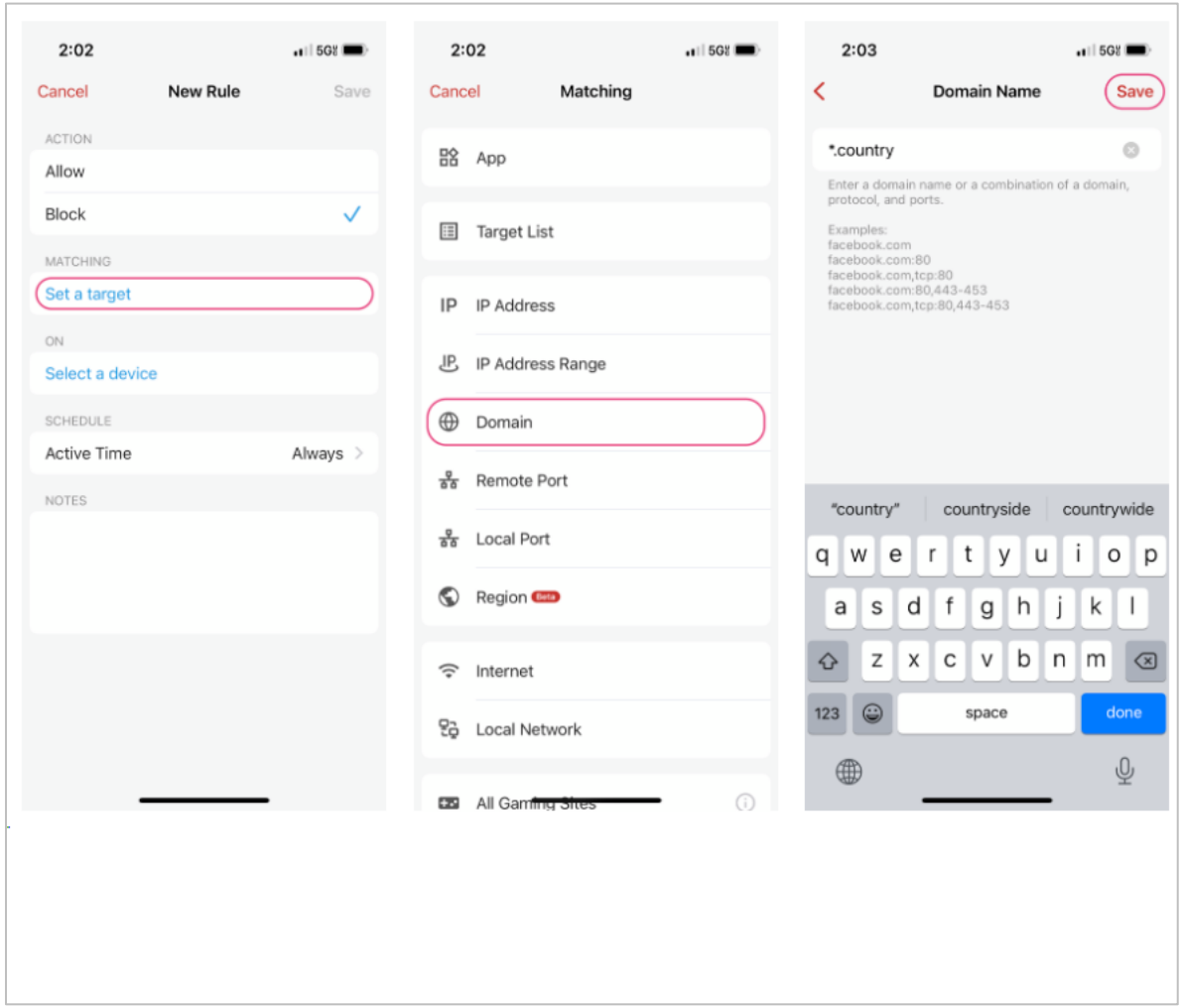
1.6. 地域ブロック (Geo-IP フィルタリング)

Firewallaを使用すると、地理的な場所からの接続をブロックするブロック ルールを作成できます。
この機能は、ネットワークが特定の国のIPアドレスと通信できないようにする場合に有効です。
これは、ハッカーによるIoTデバイスへの攻撃を阻止する効果的な方法となります。
ほとんどの場合、地域ブロック機能は外向けトラフィックのブロックに使用します。
入力トラフィックはデフォルトのステートフル ファイアウォールによってすでにブロックされているはずです。



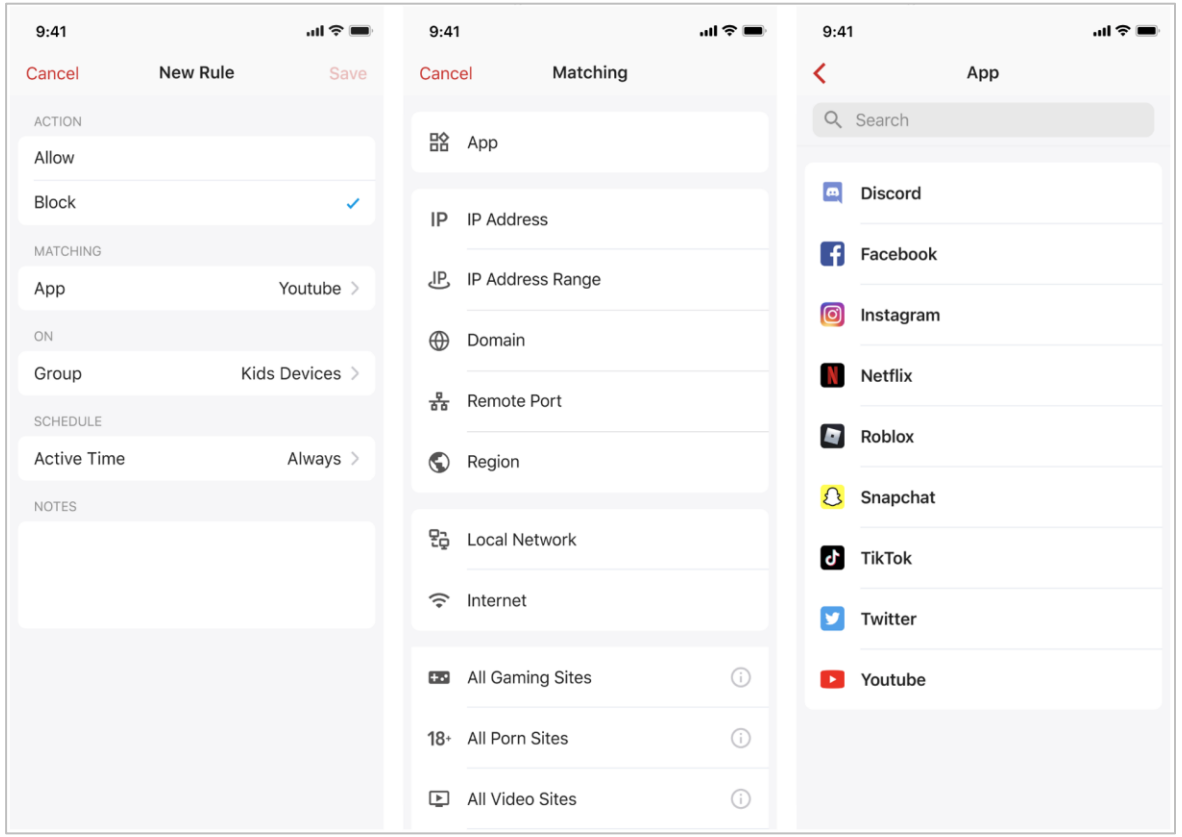
1.7. TLD ブロック (トップレベル ドメイン)

Firewallaは、firewalla.com や *.firewalla.comなどの完全なドメインのブロックに加えて、*.country、*.stream、*.download などのトップレベル ドメインのブロックもサポートしています。



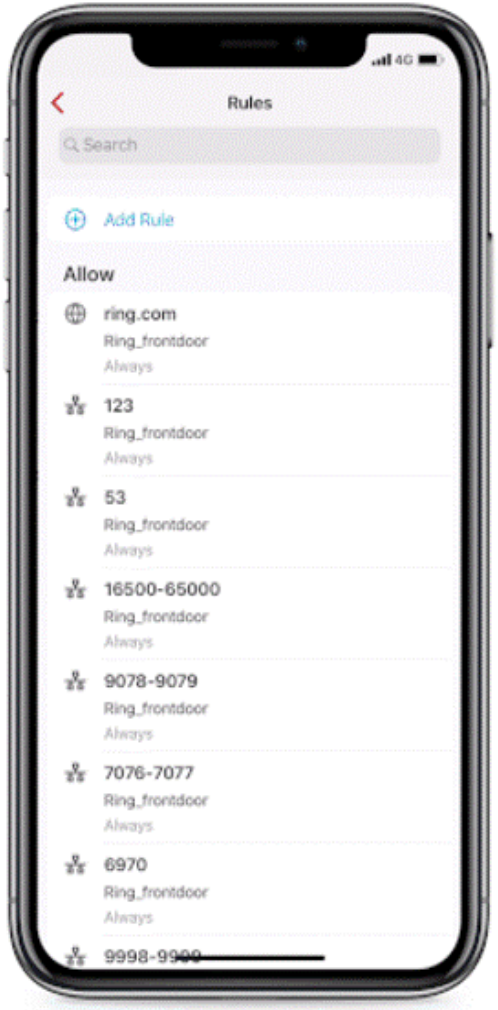
1.8. アプリケーションブロック

特定のアプリ (YouTube、TikTok、Instagram など) へのアクセスを管理したい場合は、Firewallaのルールを使用して、デバイスまたはデバイスのグループが使用できるアプリを制限できます。
これを行うには、新しいブロック ルールを作成し、ルールのターゲットをブロックするアプリに設定します。



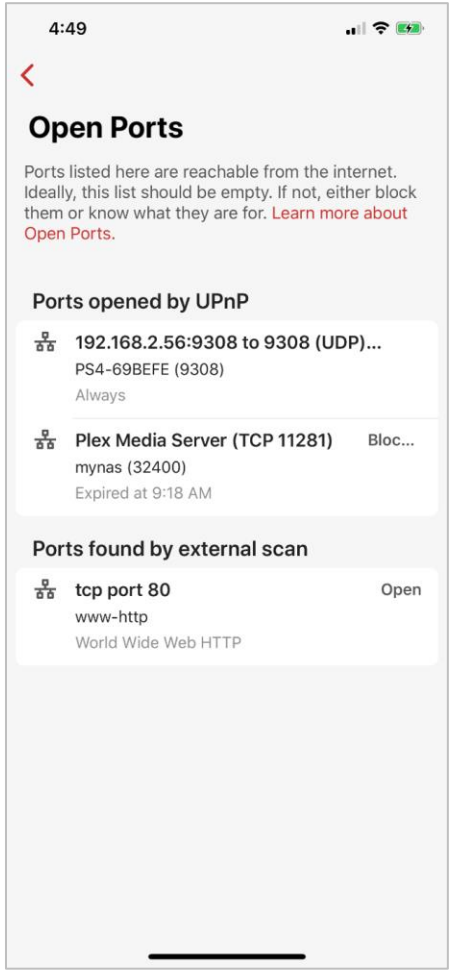
2.「許可」ルールで信頼できるネットワークを許可する

特定のサービスへのアクセスのみが必要なデバイスの場合は、信頼された接続のみを許可するようにルールを構成できます。



3. 認識されない、または未使用の開いているポートをブロックする

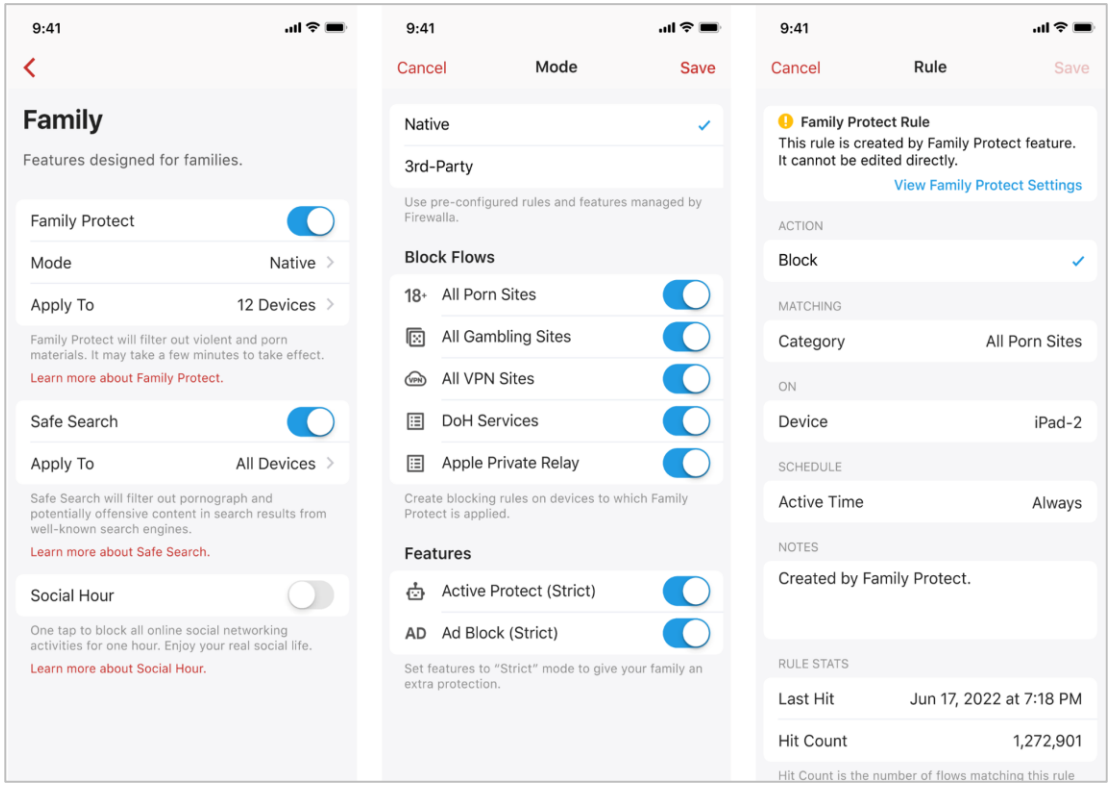
ネットワーク上で開いているポートを確認します (**[ホーム] > [ポートを開く]**)。認識できないポートがある場合、またはポートが意図的に開かれたが今後開くべきではない場合は、それらをブロックする必要があります。



4.子供向けにファミリーモードを有効にする

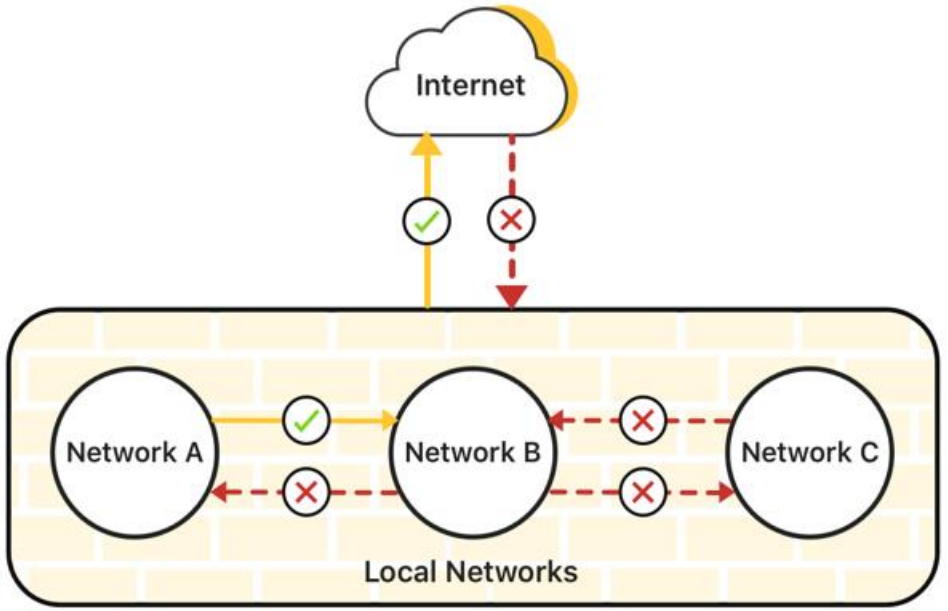
Firewallaのファミリー モードには、家族にとって不適切なコンテンツ (ポルノや暴力的な素材) を自動的に除外するサービスが含まれています。

- Family Protect：不快なコンテンツを含む Web サイトへのアクセスをブロックします。
- Native Family Protect：Firewallaボックス上で何をブロックするかを完全に制御できる新機能
- セーフサーチ: 検索結果をフィルタリングします。
- ソーシャル アワー: ソーシャル ネットワークの使用を制限します。
  家に子供がいる場合は、子供がアクセスできるすべてのコンピューターとスマートデバイス (Apple TV など) でファミリー モードを有効にしてください。



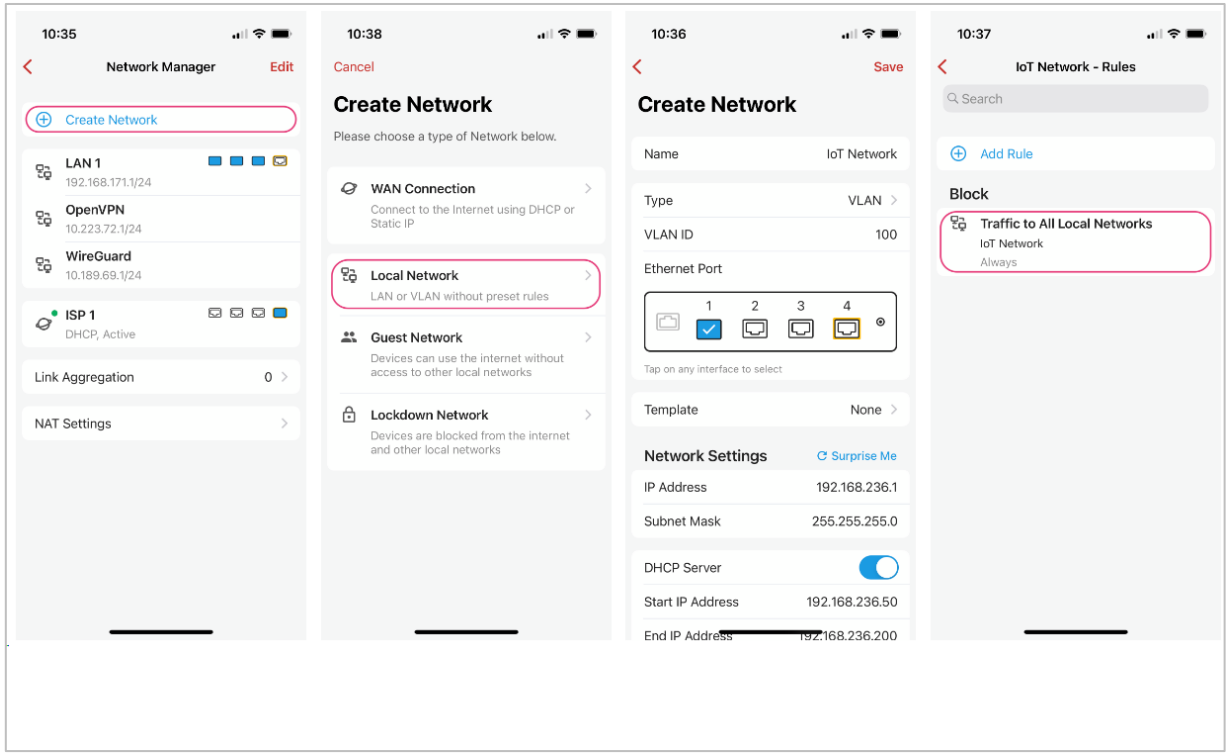
5. ネットワークセグメンテーションによるトラフィック分離

ネットワーク セグメンテーションを使用して、自宅内に複数のローカル ネットワークを作成し、1 つをIoTデバイス専用にすることができます。
このようにして、IoTデバイスのトラフィックをネットワークの残りの部分から分離し、IoTデバイスが侵害された場合のリスクを軽減できます。
ネットワーク セグメンテーションは、Gold Plusでメイン ルーターとして実行されている場合に使用できます。
VLANによるネットワーク セグメンテーションをサポートし、最大 3 つのポートベースのLANをサポートします。



6. デバイスグループによるデバイスの管理

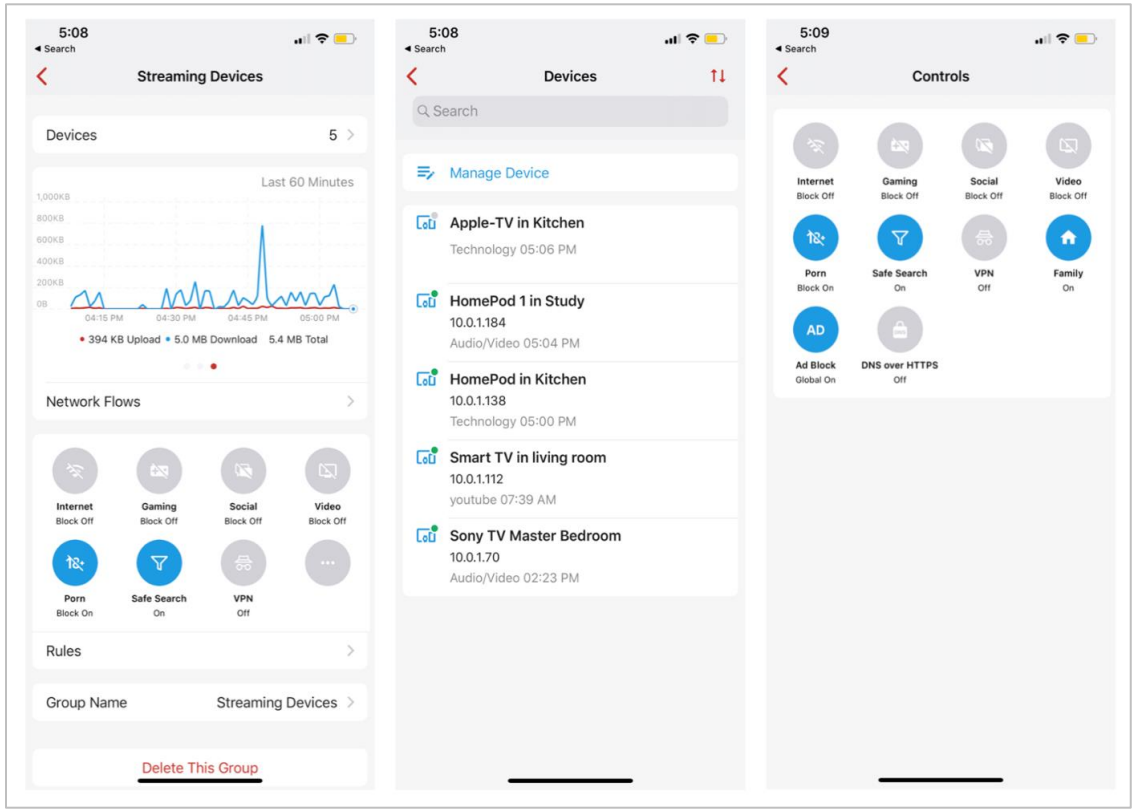
次の方法で IoT デバイスのネットワーク セグメントをセットアップできます。
●IoTデバイス用のVLANの作成
●VLAN上にルールを作成して、ネットワークの他の部分へのすべての送信トラフィックをブロックする



ネットワークのセグメンテーションは非常に強力です。同じネットワーク セグメント上のデバイス間でトラフィックを分離することは不可能ですが、VLANおよびポートベースのネットワークを使用すると、重要度が低く、テストがそれほど厳密ではないデバイスを安全に分離することができます。

デバイス グループはソフトウェア ベースのセグメント化です。
デバイス グループを使用して、同じルールとポリシーを共有するデバイスを管理できます。
これにより、デバイスとポリシーの日常的な管理が大幅に簡素化されます。
次に、デバイス グループの使用方法の例を示します。

- ストリーミングデバイスのデバイスグループを作成する
- すべてのスマート テレビ、スピーカー、セットトップ ボックスをグループに追加します
- ネットワーク全体で一貫したルールとポリシーを使用してグループを管理します

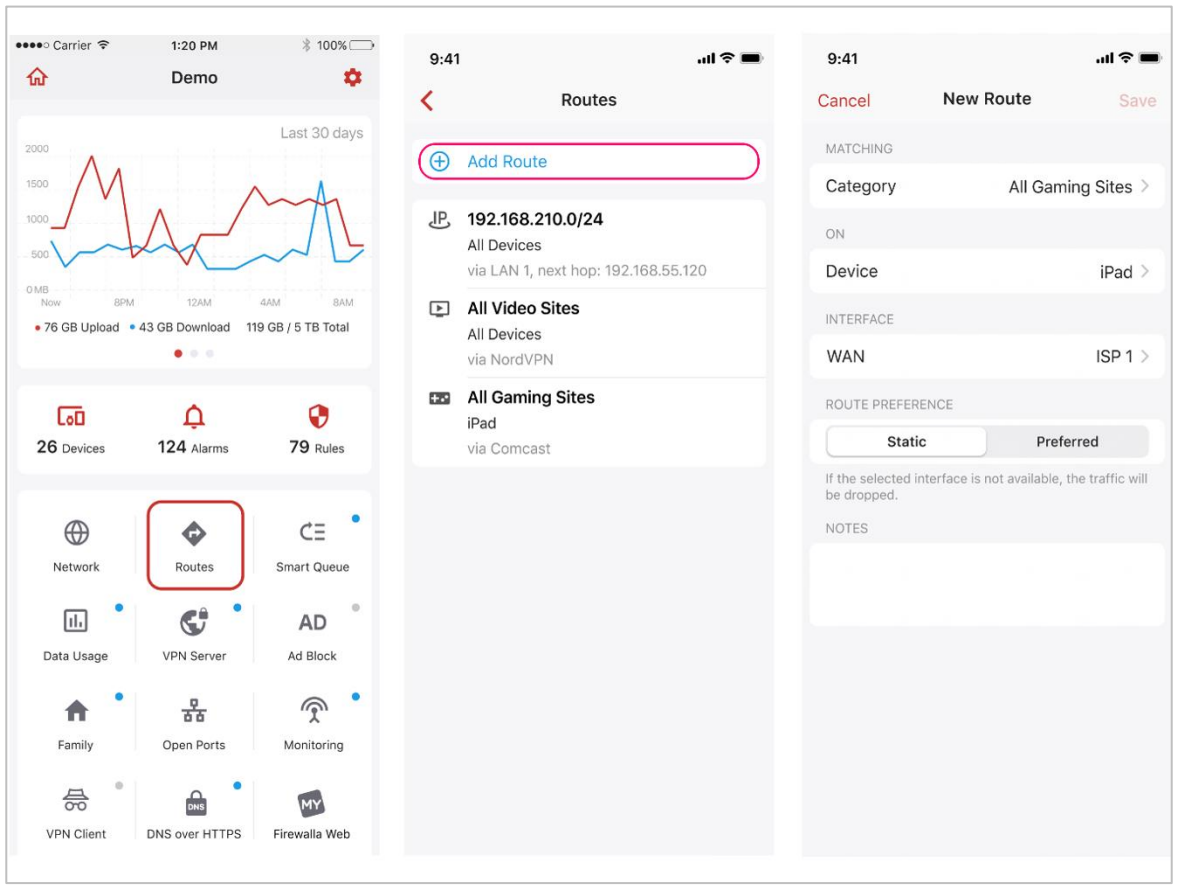


7. ルートによるトラフィックの制御

次のような複数のトラフィックがある場合に使用可能です。

- VPNクライアント (または多くの VPN クライアント)
- セカンダリWAN
- サイト間VPN

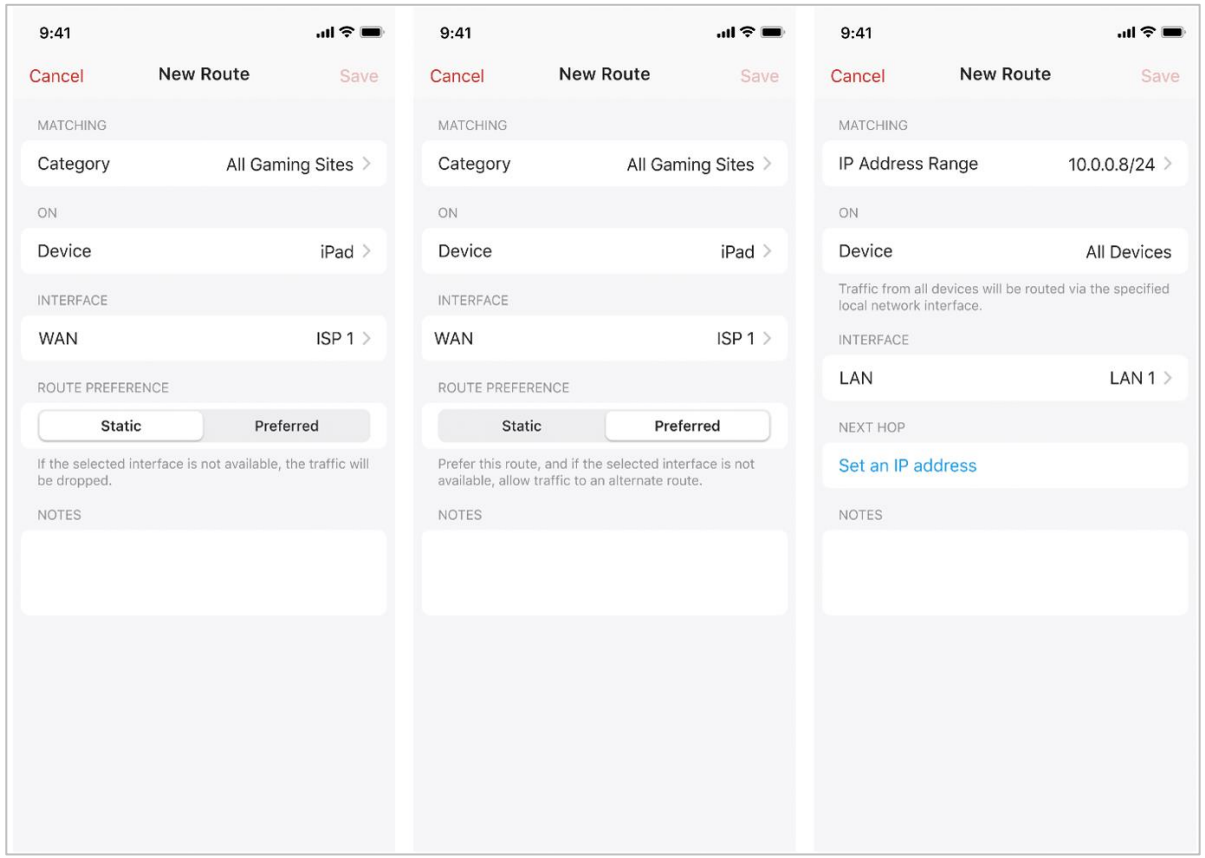
Firewallaを介したスマート ルーティング ポリシーを使用して、任意のIoTデバイスのネットワーク トラフィックを上記の任意の宛先に送信できます。



ルートごとに、次の 2 つのオプションが提供されます。

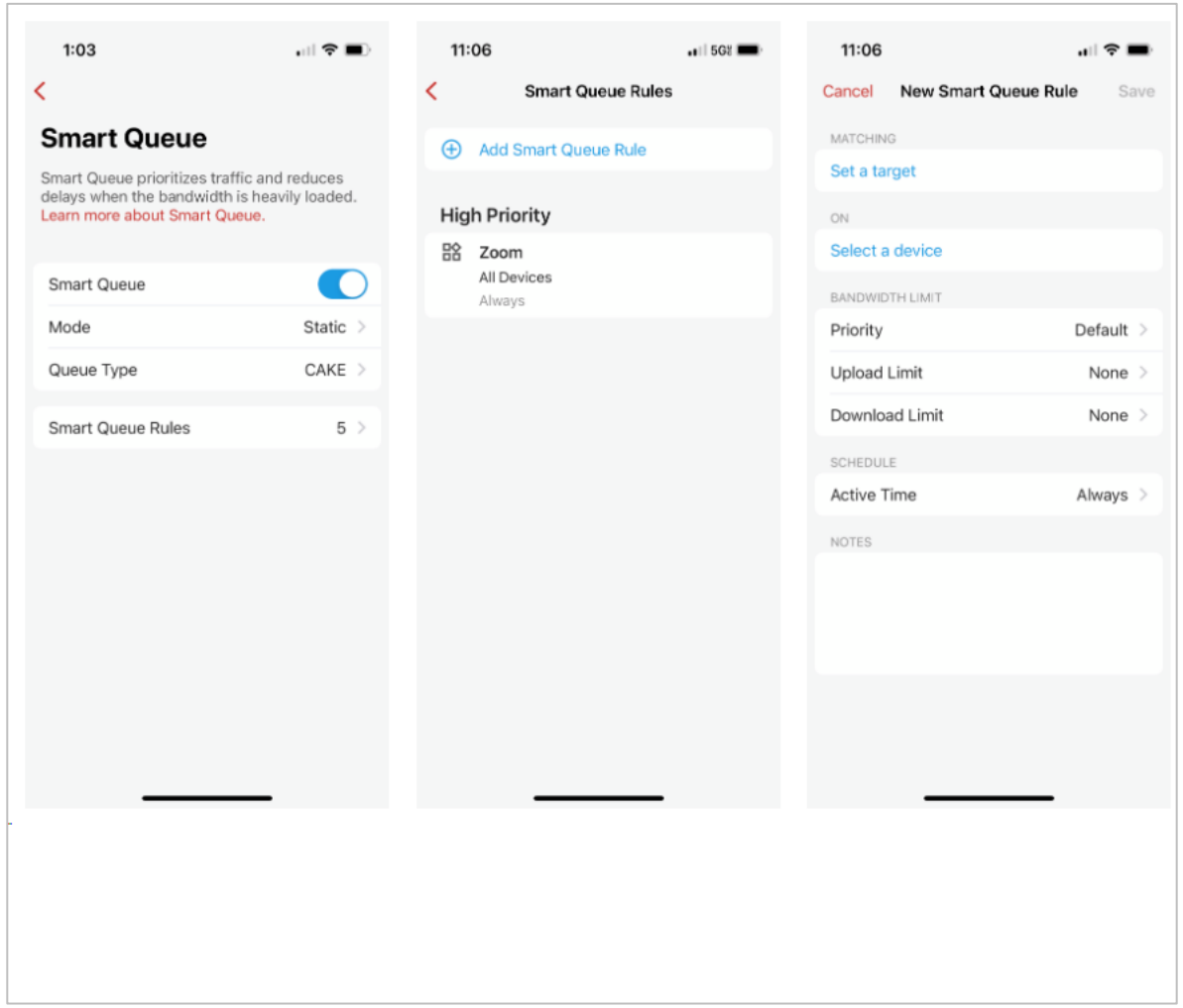
- 静的:選択したインターフェイスが利用できない場合、トラフィックはドロップされます。これがデフォルトの設定です。
- 優先:選択したインターフェイスが使用できない場合は、代替ルートを経由するトラフィックを許可します。

選択したVPNへのトラフィックを「ロック」するには、VPNのインターネット キル スイッチが有効になっていることも確認する必要があることに注意してください。



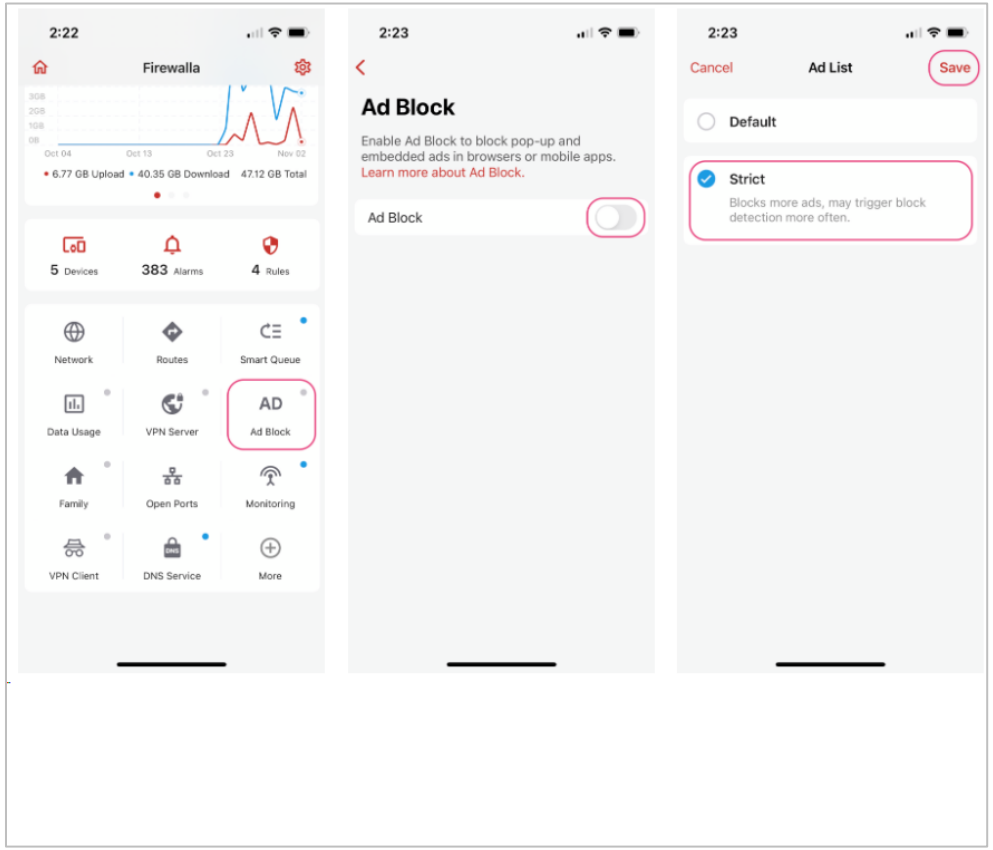
8. Smart Queueを使用してトラフィックを調整する

IoTデバイスが帯域幅を過剰に消費することが心配な場合は、デバイスまたは宛先ごとにトラフィックを制限するポリシーを簡単に適用できます。



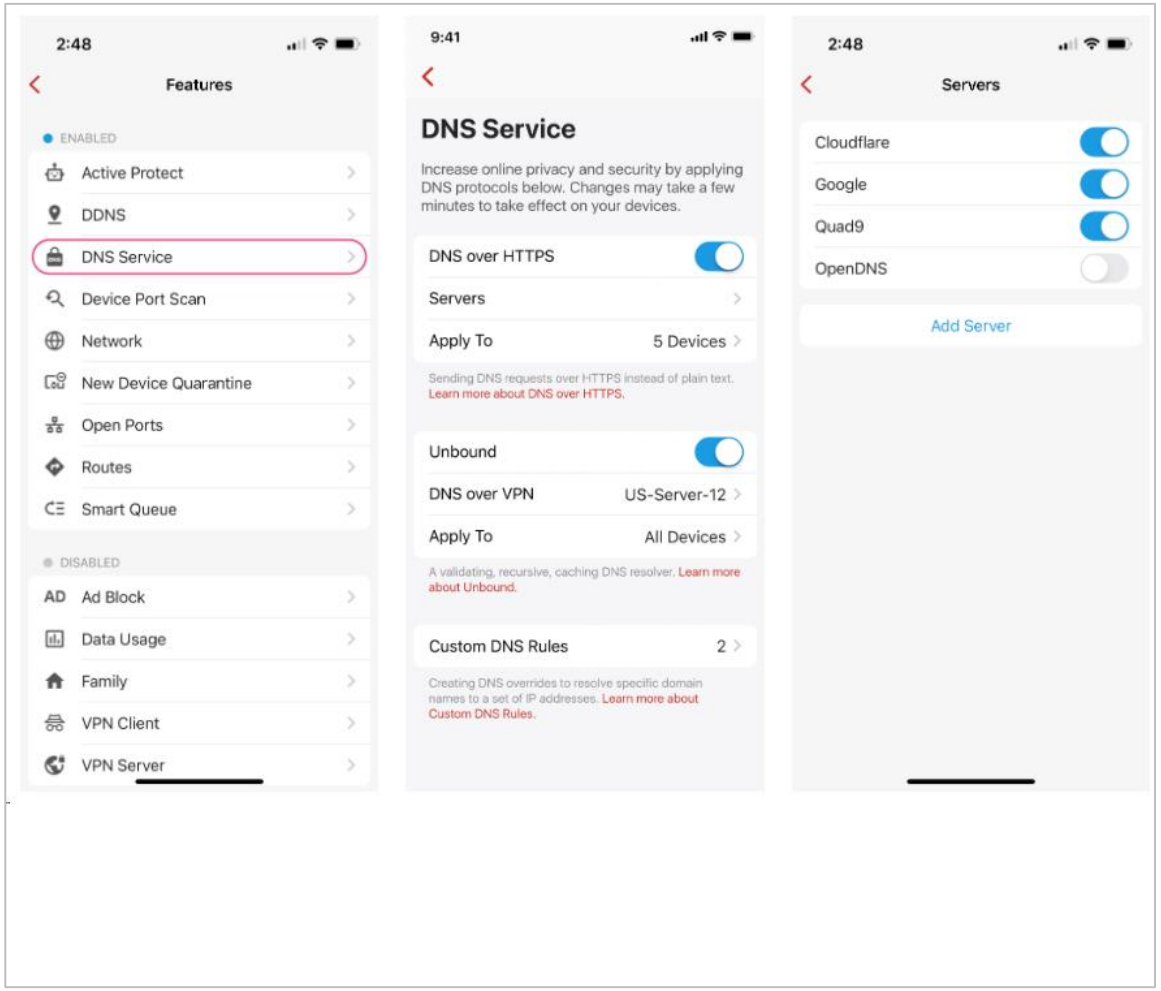
9. 広告ブロックでプライバシーを保護する

広告ブロックは、Firewallaに組み込まれている広告ブロッカーです。
単に広告をブロックするだけではなく、広告によるオンライン行動の追跡を防ぎ、プライバシーも保護します。
これは、インターネットに一般的にアクセスできるものの、ユーザーにプライバシー設定や制御を提供しないスマート デバイスに特に役立ちます。
広告ブロックには、デフォルト モードに加えて、より積極的に広告をブロックするストリクト モードも設定できます。
すべてのデバイスで広告ブロックをオンにすると、ネットワーク全体に広告が表示されなくなります。

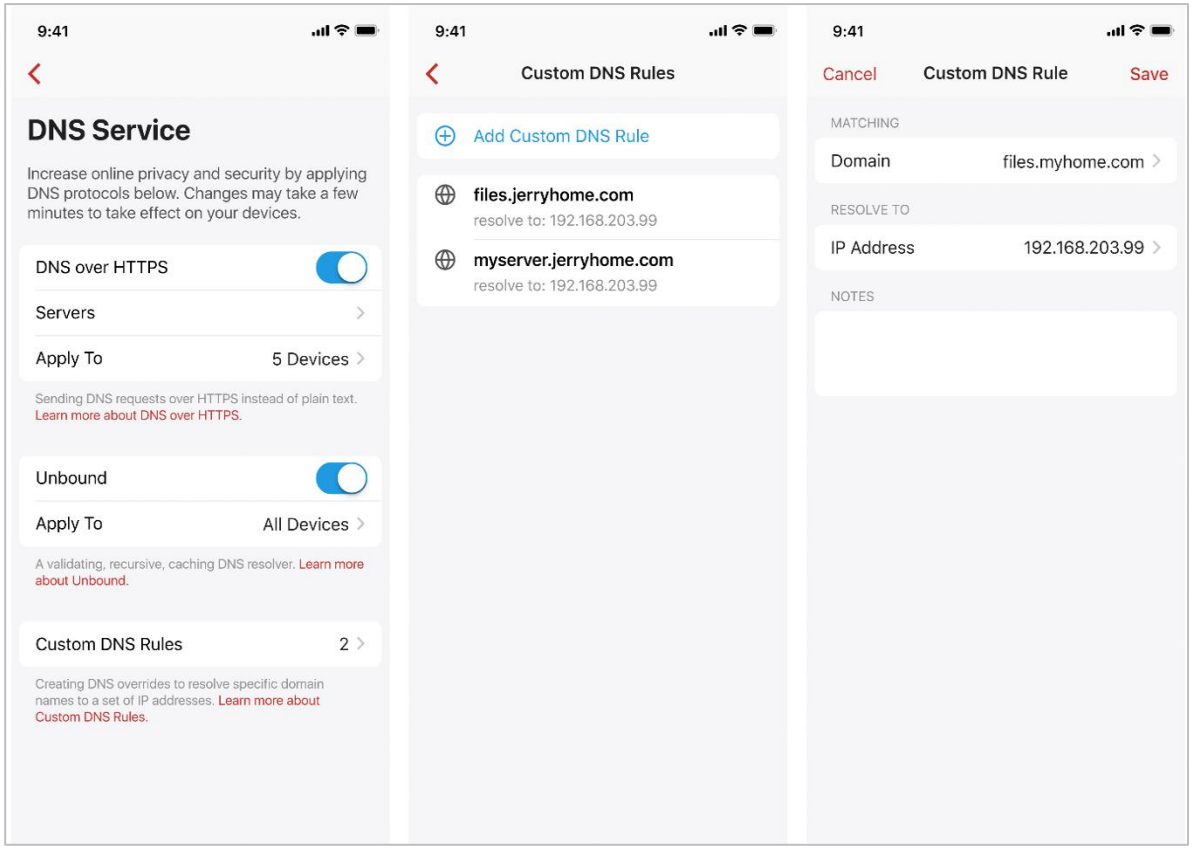


10. DoH、アンバウンド、および DNS ルールを使用して DNS トラフィックを制御する

DNS over HTTPS (DoH) は、HTTP経由でプレーン テキストでリクエストを送信する従来のDNSとは対照的に、HTTPS経由で暗号化された DNSリクエストを送信します。
デバイスがアクセスしているWebサイト、ドメイン、サービスを第三者がスパイすることを防ぎます。
FirewallaでDoHを有効にすると、ネットワーク内のすべてのデバイス、特にこの種のサービスを構成できないIoTデバイスが保護されます。

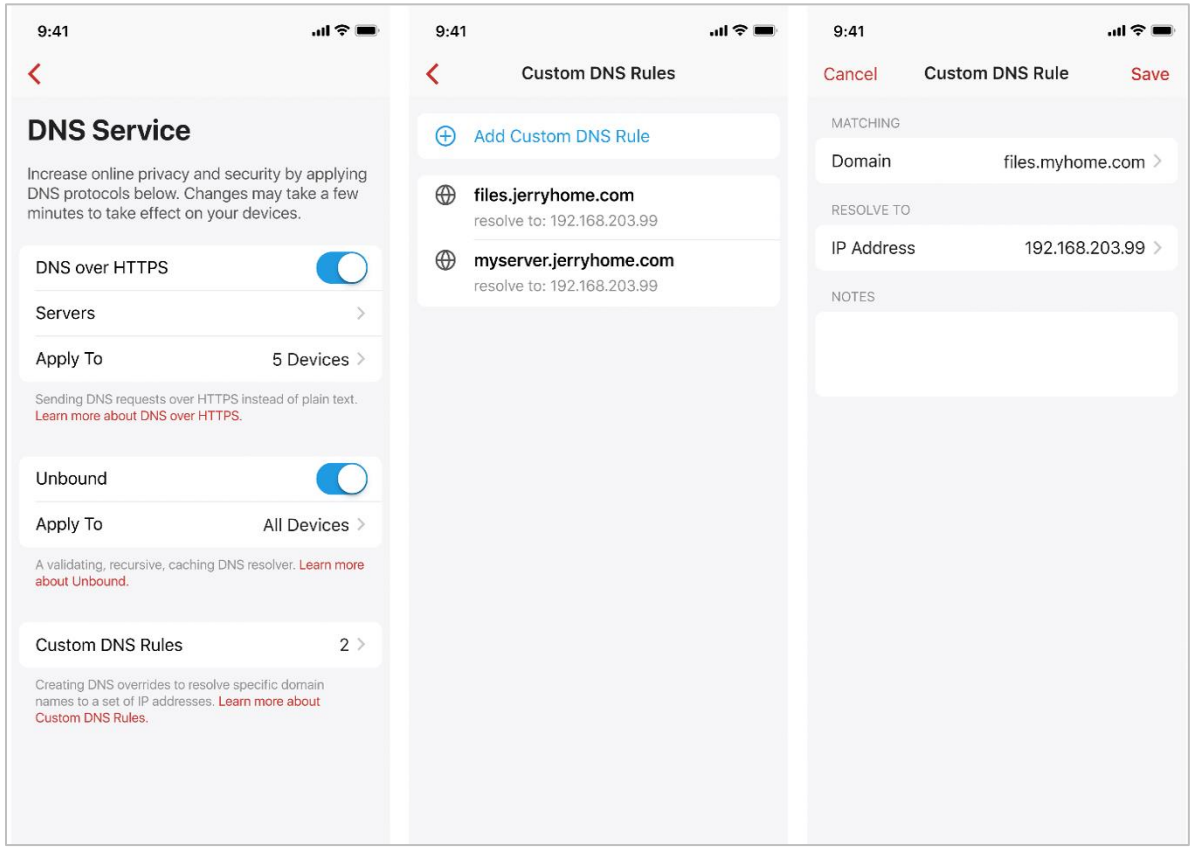


DoHに加えて、Firewallaは別のDNSサービスUnboundをサポートしています。
これは、オンラインのプライバシーとセキュリティの向上に役立つ検証、再帰、キャッシュDNSリゾルバーであり、Firewallaボックスにローカルにインストールされます。
Unboundにより、単一のパブリックDNSサーバーがすべてのDNSレコードを保持できなくなります。
追加の保護層として、Unbound over VPNを有効にすることで、ISPの代わりにVPN 経由でUnbound DNSリクエストを送信することもできます。



11. Firewalla VPN による安全なネットワーク アクセス

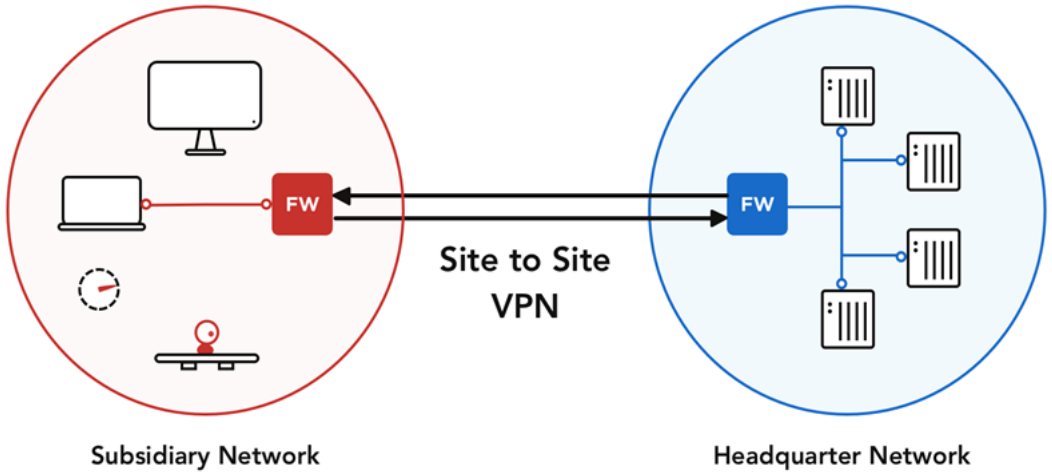
スマートフォンアプリ経由でカスタムDNSエントリ ルールを追加することが可能です。



FirewallaにはVPNクライアントが組み込まれており、IoTトラフィックを含むすべてのホーム ネットワーク トラフィックをVPN経由で簡単かつ無料でトンネリングできます。

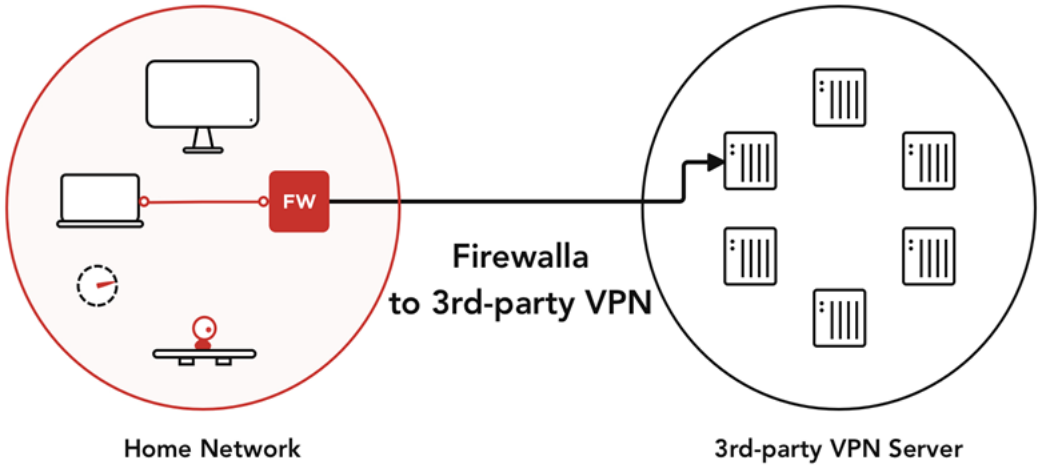
11.1.サイト間 VPN

FirewallaにはVPNクライアントが組み込まれており、IoTトラフィックを含むすべてのホーム ネットワーク トラフィックをVPN経由で簡単かつ無料でトンネリングできます。

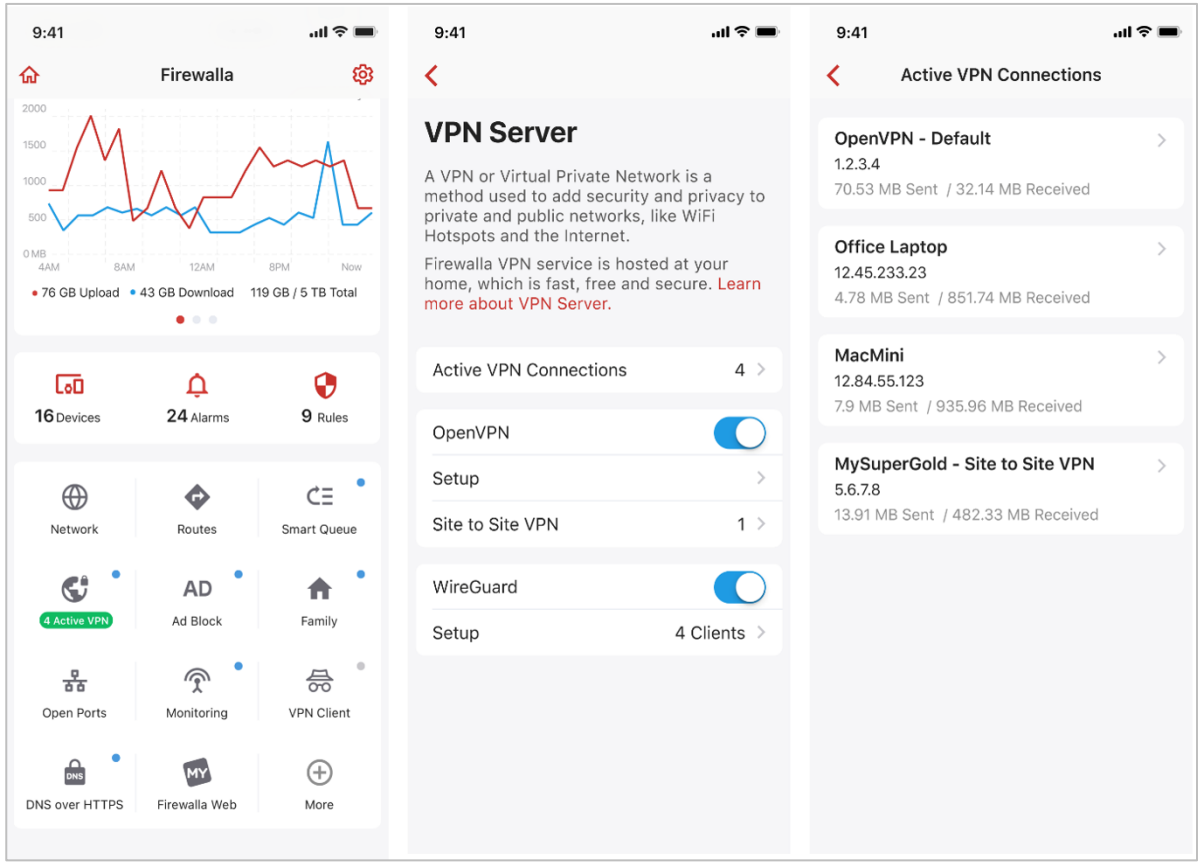


11.2.サードパーティVPN

サードパーティのVPNサーバーを使用している場合は、Firewalla VPNクライアントを有効にしてVPNサーバーに接続できます。
これにより、すべてのIoTデバイスが同じVPNサービスを簡単に使用できるようになります。



FirewallaにはVPNサーバーも組み込まれています。
旅行中や公共Wi-Fiを使用しているときは、自宅のVPNサーバーに再度接続して、セキュリティ カメラやホーム オートメーション コントローラーなどのホーム デバイスに安全にアクセスできます。
この方法は、ルーターで単純なポート転送を使用するよりもはるかに安全です。追加の暗号化により、トラフィックが隠蔽され、同時にネットワーク層での認証が提供されます。



12. 新しいデバイスを隔離する

Firewallaで新しいデバイス隔離を有効にすると、認識されないデバイスがネットワークに参加した場合に、そのデバイスをすぐに別の隔離グループに配置できます。
こうすることで、見慣れないデバイスを完全に可視化し、そのアクセスを制御するためのルールを設定できます。
いつでも必要に応じて、デバイスを隔離グループから解放できます。