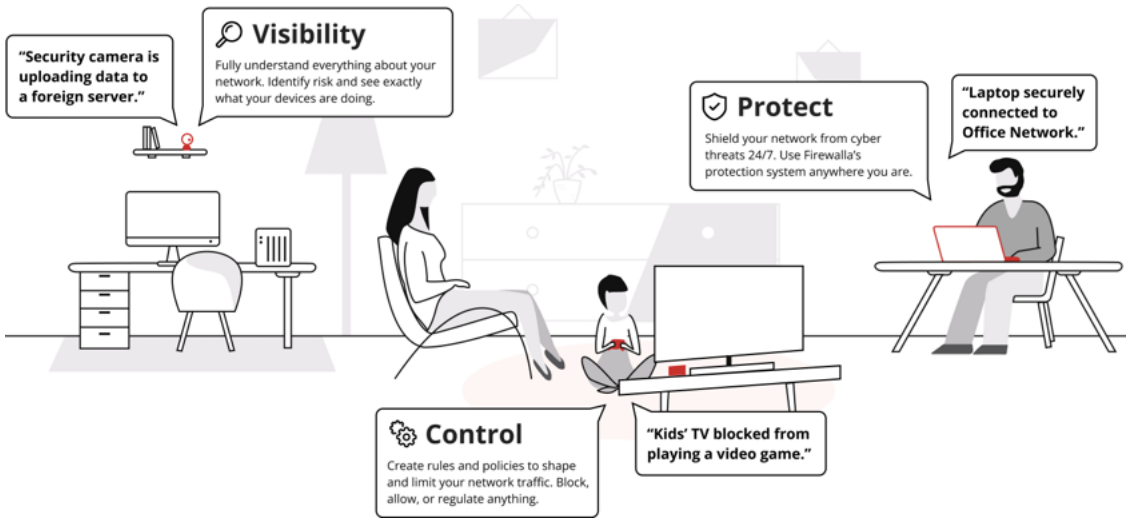
ネットワークの防御①　見える化

ネットワークの防御①　見える化

家庭や中小企業をサイバー攻撃から保護するには、ネットワーク デバイスのセキュリティを強化することが重要です。Firewallaはネットワーク全体を保護することで、すべてのIoTデバイスのセキュリティを強化します。
Firewallaは以下の機能によりネットワークのセキュリティを強化します。

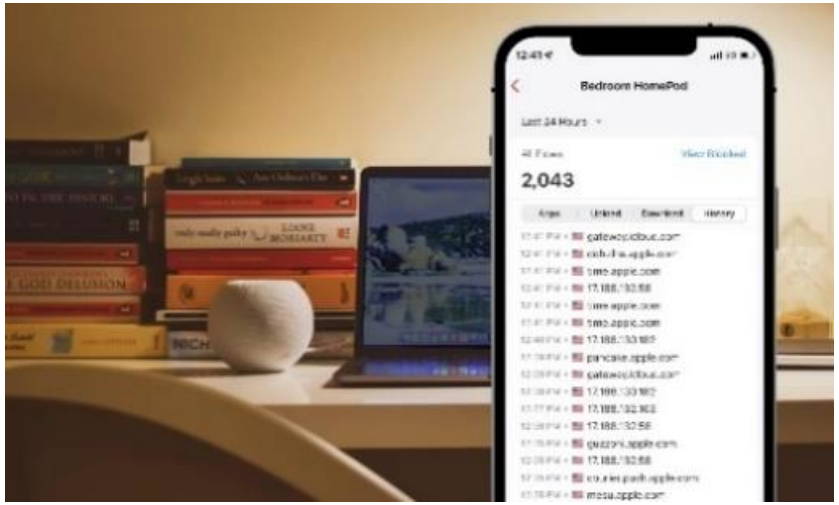
1. **見える化（Visibility）**：ネットワークを「見える化」します。ネットワークを完全に把握し、リスクを特定できるようになります。
2. **制御（Control）**：ネットワークを制御し、重要なポリシーとルールを適用します。これにより、攻撃対象領域が制限され、リスクが軽減されます。
3. **保護（Protect）**：Firewallaがルールに基づいてネットワークを自動的に保護します。



通信状況の見える化

Firewalla使用すると、自宅に接続されているデバイスの数やそれらのデバイスでどのような通信をおこなっているかを確認することができます。
ネットワークに接続されたデバイスの一部が、バックグラウンドで活発に動作している状況などを確認することができます。
Firewallaは次のことに役立ちます。

- ネットワークに接続されたデバイスを把握する
- デバイスが何をしているかを確認する
- ネットワークを理解する
- 開いているポートを調べる
- アラームの確認と管理

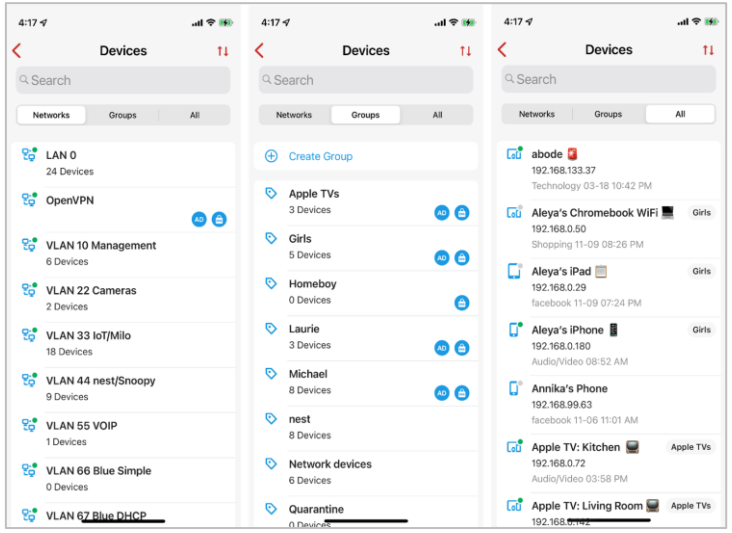


ネットワークに接続されたデバイスを把握する

Firewallaをセットアップすると、家の中に接続されているすべてのデバイス (有線または無線) が表示されます。
すべての IoT デバイスの一覧が作成されます。それらが何であるかを確認し、Firewallaアプリで簡単に認識できるようにデバイスの名前を変更することができます。
ネットワーク上のデバイスには次のものが含まれる場合があります。

- スマートテレビ
- スピーカー
- プリンター
- カメラ
- 自動化制御ユニット
  など

Firewallaは、新しいデバイスが接続されるとアプリで通知します。また、オプションで、新しいデバイスのネットワークアクセスを自動的に制限することもできます。たとえば、隣人が許可なくあなたの Wi-Fi に接続した場合、すべてのインターネット アクセスをブロックすることができます。
ネットワークとグループでフィルタリングされたデバイスのリストを表示できます。
デバイス リスト全体をスクロールし、検索機能を使用して、名前、IP、またはMACアドレスでデバイスを見つけることもできます。



デバイスが何をしているか を確認する

Firewallaによりネットワーク内の各デバイスのトラフィックを確認することができます。これは、特にバックグラウンドで動作するIoTデバイスに役立ちます。
ルーターは保護されたデータ接続の内容を確認できませんが、Firewallaは次のことを判断できます。

- ●データの送信先 (国、ドメインなど)
- ●どれくらいのデータが流れているのか
- ●どのようなトラフィック状況か
- ●インターネットへのアウトバウンド通信か、
  インターネットからのインバウンド通信か
- ●許可されたかブロックされたか
- ●なぜ許可またはブロックされたのか

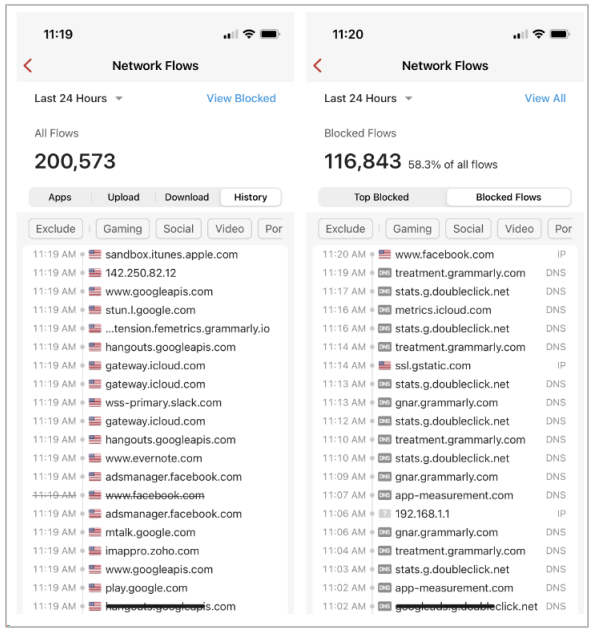
これらはデバイス、デバイス グループ、ネットワーク セグメントごとに確認できるため、常に何が起こっているかを非常に明確かつ具体的に把握できます。
Firewallaは次のことを表示できます。

1. ネットワークフロー
2. ブロックされたフロー
3. ライブスループット

デバイスのアクティビティを定期的にチェックして、その動作を常に把握することができます。異常があればFirewallaによって自動的に検出され、アラートが届きます。

1. ネットワークフロー

[Network Performanceの下部のFlows in Last24hrs] > [ネットワークのフロー]は、ネットワーク上のすべての受信および送信ネットワーク トラフィックの履歴です。
[All Flows]内の取り消し線の項目は、ブロックされた内容を示します。
ブロックされたフローのみを表示する別のフィルターされたビューがあり、詳細が表示されます。
(詳細については、以下のブロックされたフローを参照してください)



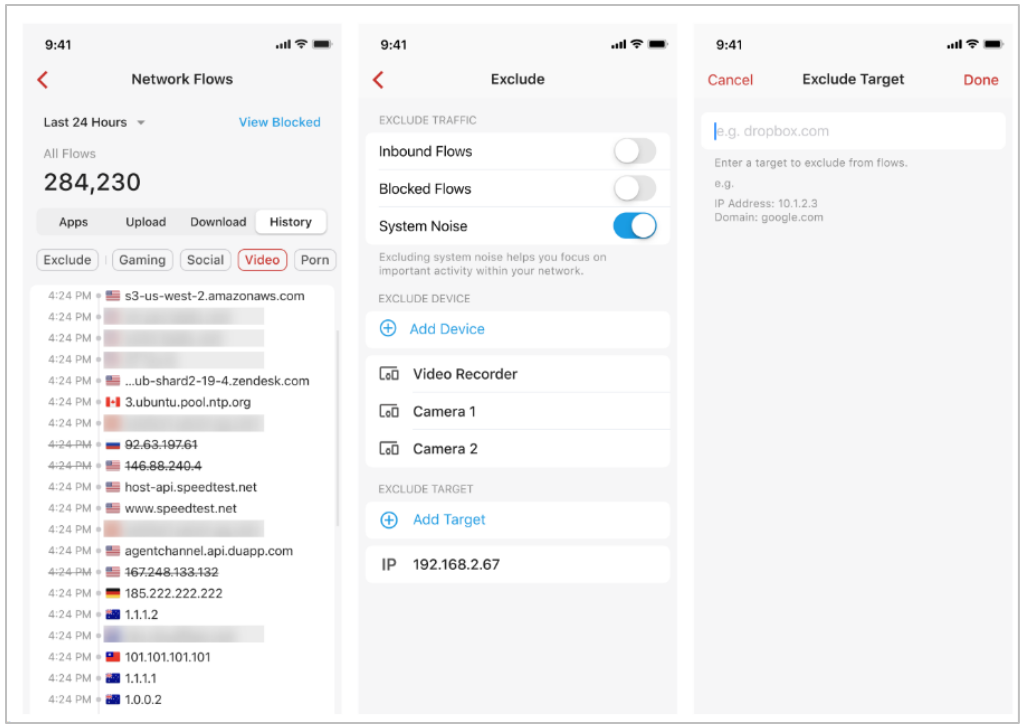
このデータは、次のような内容を把握することができます。

1. デバイスはどのサーバーに接続しているか
2. これらのサーバーはどこにあるか
3. これらのサーバーには怪しい評判があるか
4. ブロックしたいデータ収集はあるか (ロギングやデータマイニングなど)
5. ポートのスキャンが行われていないか
6. どのような攻撃をうけているか

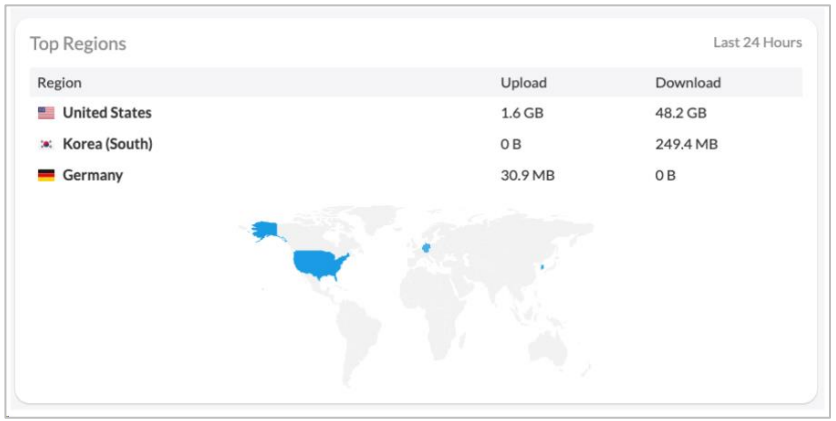
フローのリストを把握しやすくするために、除外（Exclude）機能を使用して一部のフローをビューから非表示にすることができます。

- **インバウンドフロー:**外部から入ってくるフロー。通常、これらはブロックされます。
- **ブロックされたフロー:** Firewalla によって傍受されたフロー。
- **システム ノイズ:**システム ノイズを除外すると、OSシステム上のバックグラウンド トラフィックと、よく見られるアプリ (広告、トラッキング、テレメトリ、ソフトウェア アップデート、分析、NTP、パブリック クラウド サービスを含む) がフィルタリングされます。

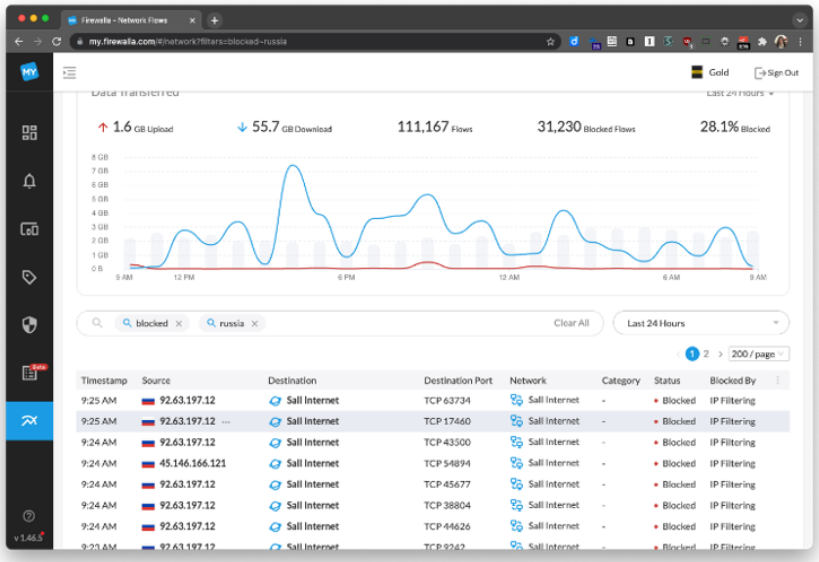
これは、ネットワーク内の重要なアクティビティに集中するのに役立ちます。
さらに、除外（Exclude）指定に特定のデバイスまたはターゲットを追加できます。
たとえば、特定の隔離されたデバイスからのブロックされたフローを表示したくない場合は、そのデバイスを [ブロックされたフロー] に表示されないようにすることができます。



Webインターフェイスでは、地域ごとのトラフィックが表示されます。



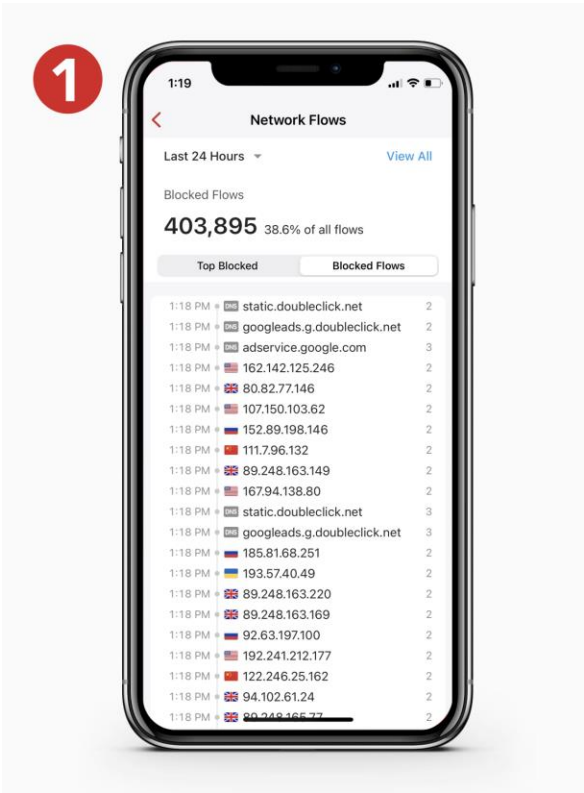
Web インターフェイスでは、より複雑な分析のためにフィルタリングを行うこともできます。
この例では、「ブロック」は「ロシア」から流れてきます。



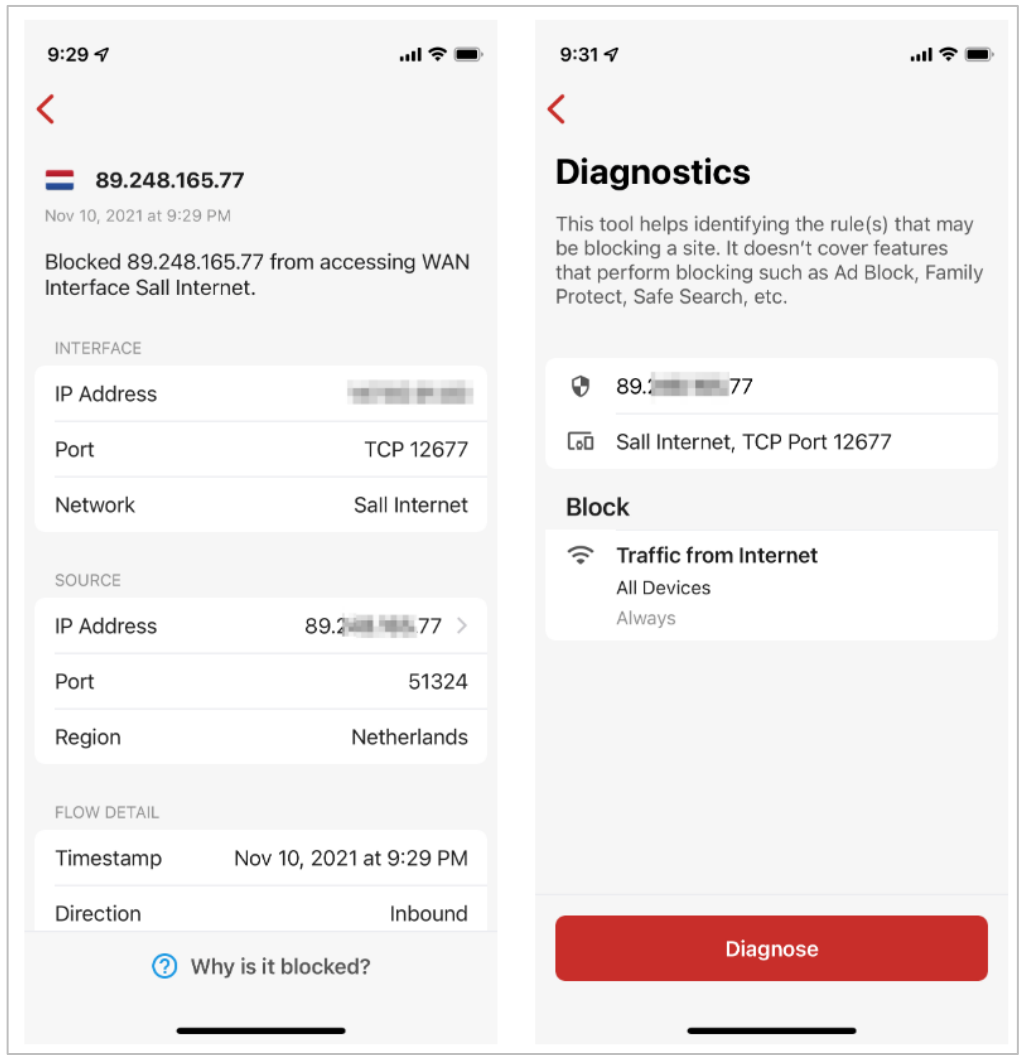
2. ブロックされたフロー

ブロックされたフローでは、Firewallaによってブロックされた通信を確認できます。例えば、広告ブロックが期待どおりに機能しているかどうかを知ることができます。これらは、設定したルールを微調整したり、アクセスを許可またはブロックする新しいルールを作成したりするのに役立ちます。
ブロックフローの右の列をタップすると、以下の表示データを順番に切り替えることができます。

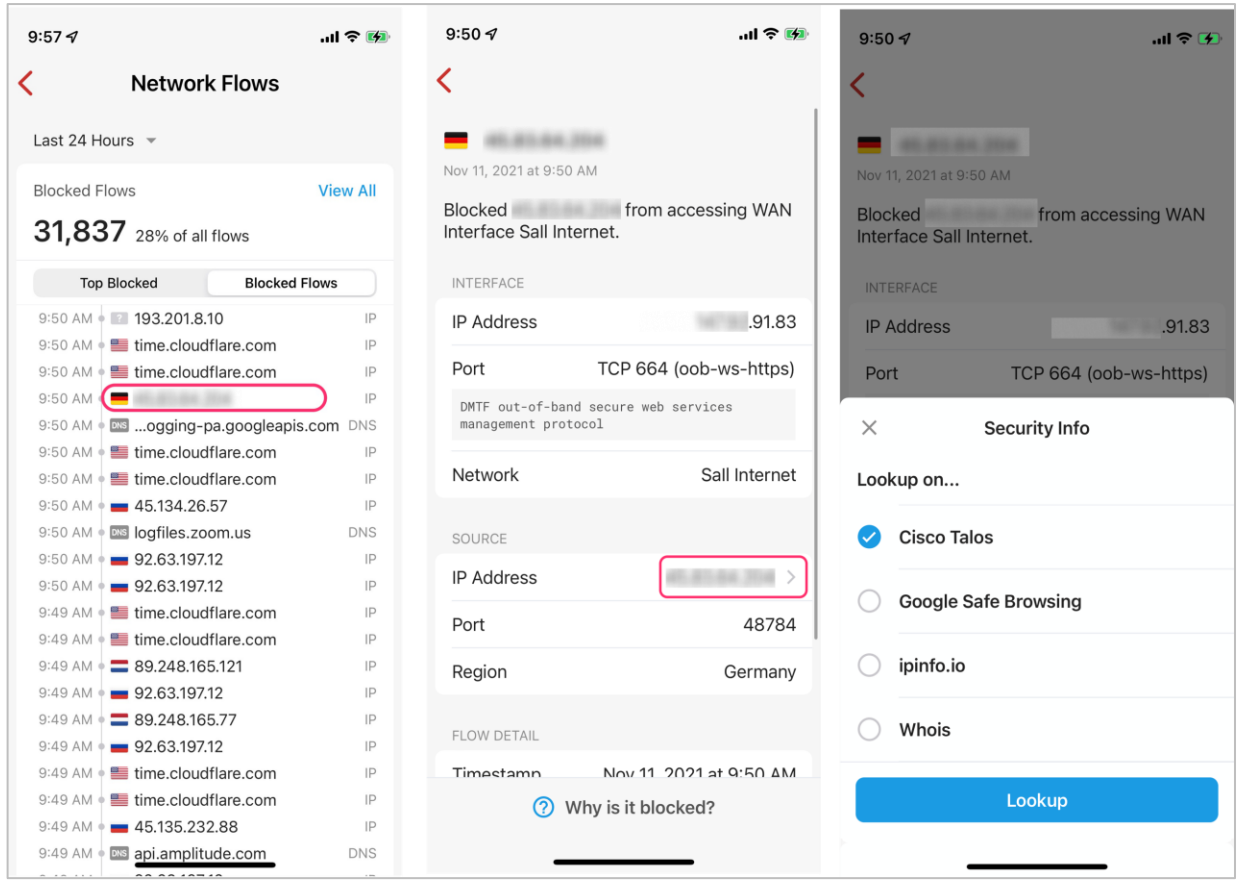
1. ブロック数:特定のドメインまたはIPが何回ブロックされたか
2. インバウンドとアウトバウンド:ネットワークの外から入った通信か、それともネットワークの内部から外への通信か
3. ブロックの理由: Firewallaが接続をブロックしたのはなぜか
4. ポート:どのポート番号がアクセスされていたか



また、ブロックされたフローのエントリのいずれかをクリックすると、トラフィックの発信元または宛先であるサーバーの場所、使用された WAN 接続、使用されたポート、およびブロックされた理由の詳細を確認することもできます。

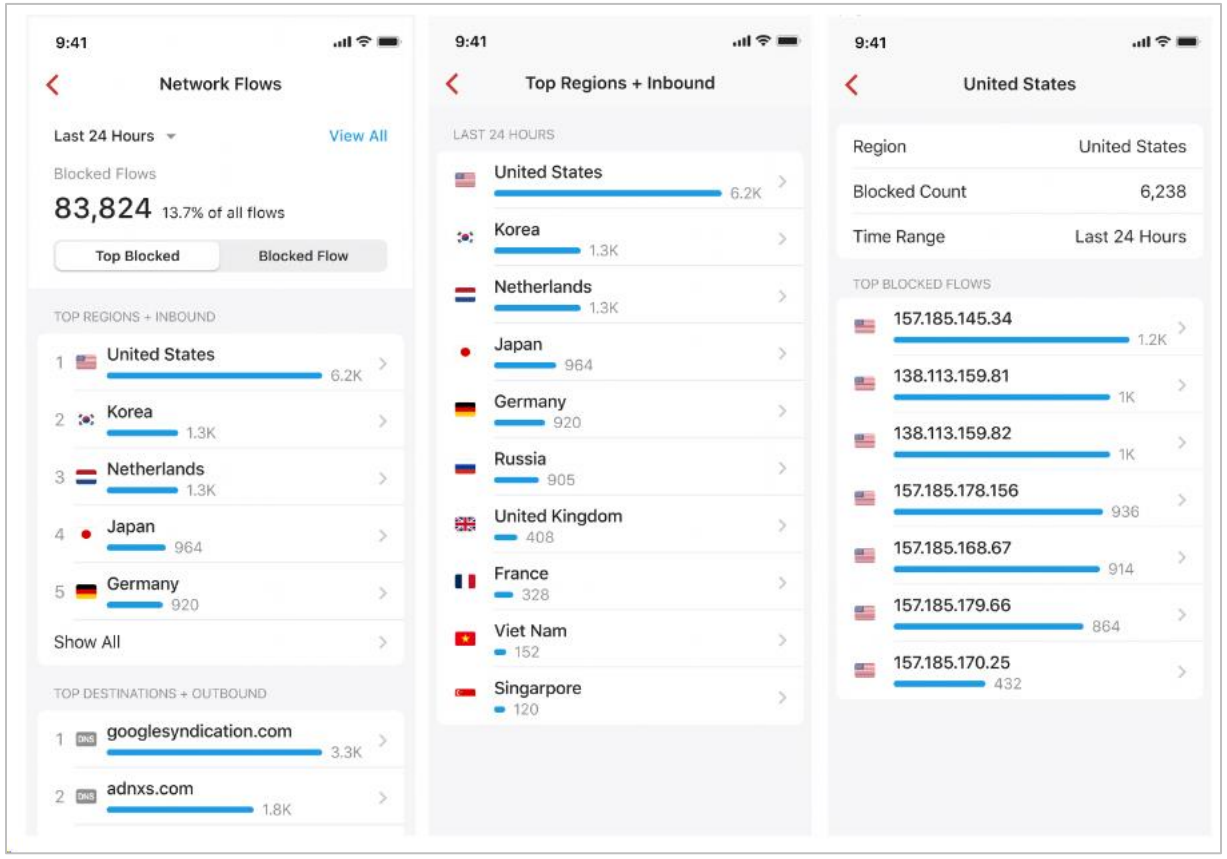


特定のIPアドレスまたはドメインについてさらに詳しく調べることもできます。これにより、そのサーバーに接続するリスクを確認することができます。



Firewallaは、地域と宛先ごとにブロックされた上位フローの 2 つのリストを表示します。

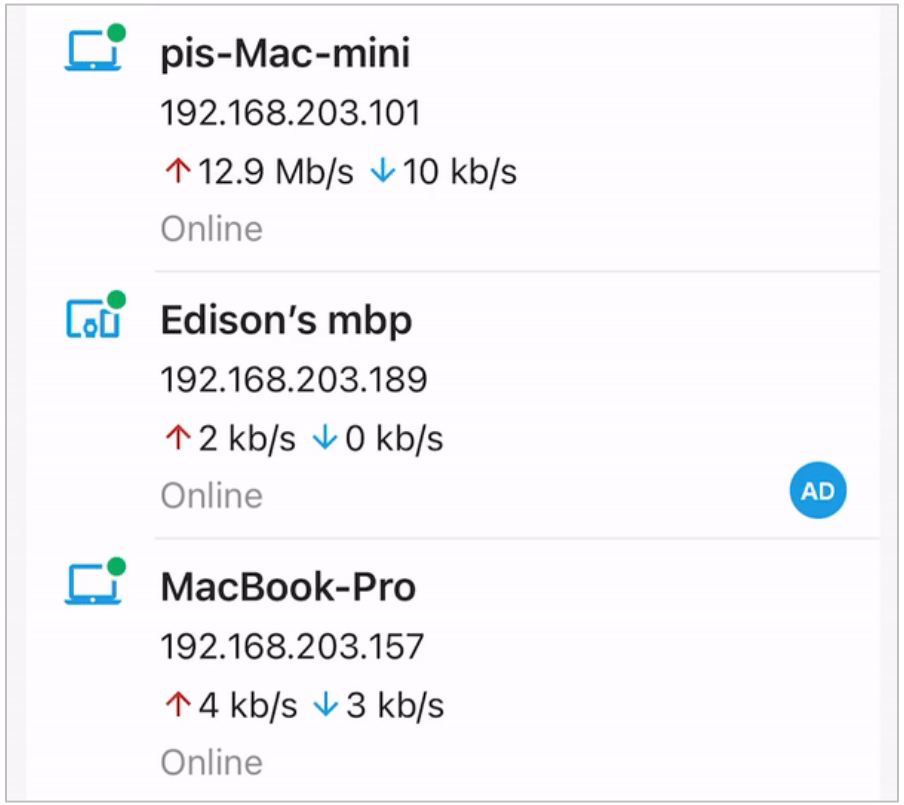
- **トップ リージョン + インバウンド:**
  外部からの誰かがネットワークに接続しようとすると、
  ほとんどの接続は**FirewallaのIngress Firewall**によってブロックされます。
  これらのフローを地域に基づいて集計します。
- **上位の宛先 + 送信:**これらは、デバイスが接続しようとしている宛先です。



3. ライブスループット

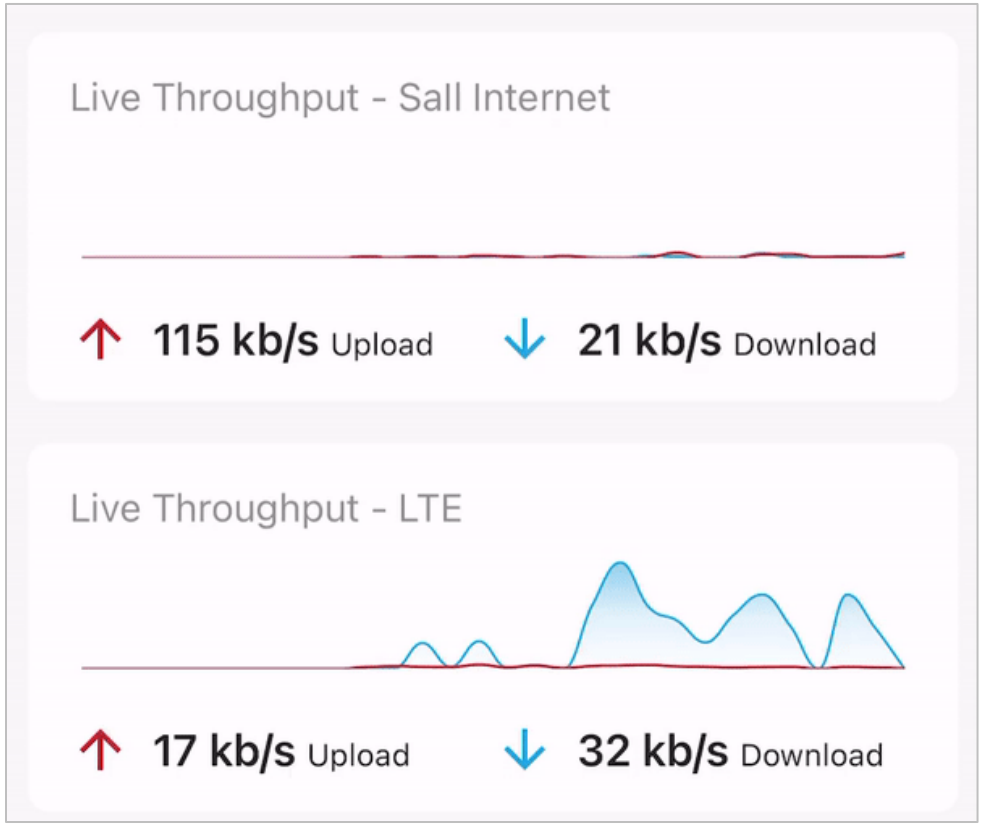
ライブ スループットはアップロードとダウンロードのアクティビティをリアルタイムで測定します。
注: iOSを使用している場合は、Firewallaアプリがローカル ネットワークにアクセスできることを確認してください。

[設定] で、**[プライバシー] > [ローカル ネットワーク]**に移動し、Firewallaアプリへのアクセスを許可します。
ライブ スループットは個々のデバイス単位で確認できます。

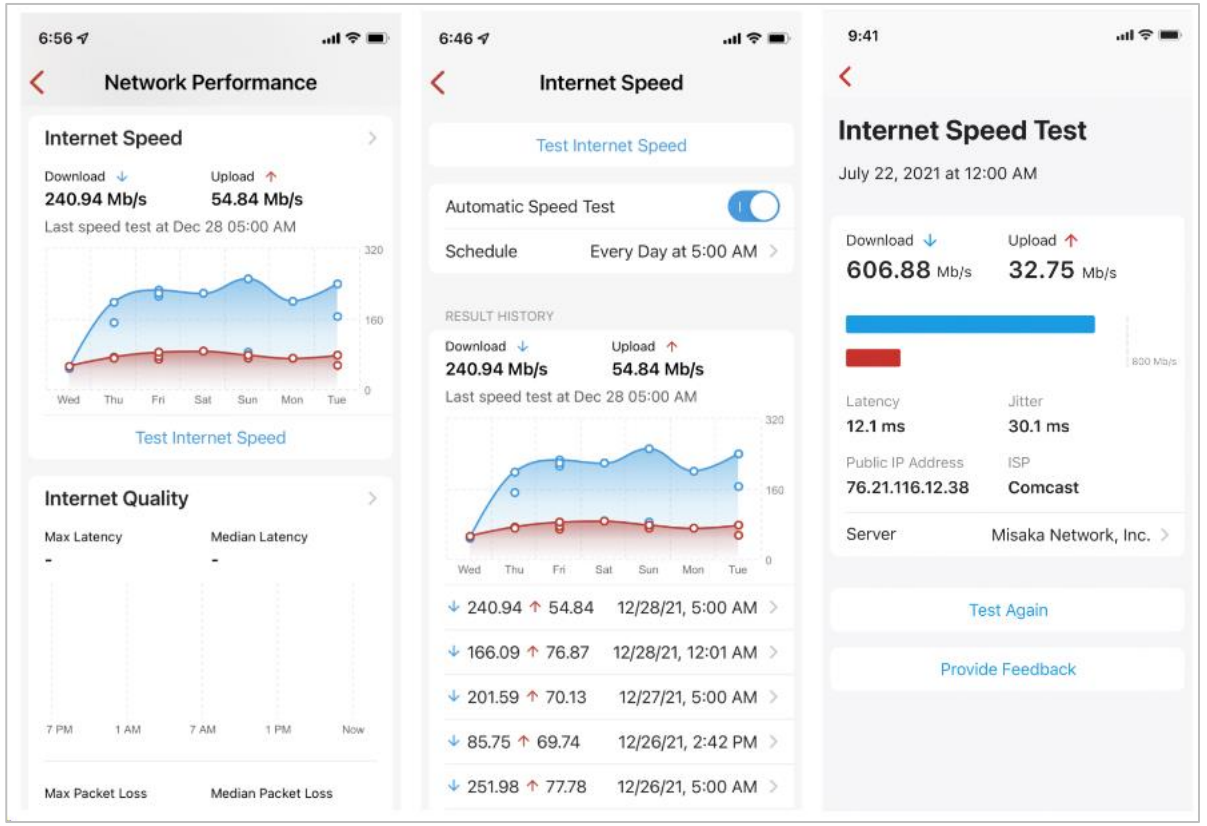


ネットワークを理解する

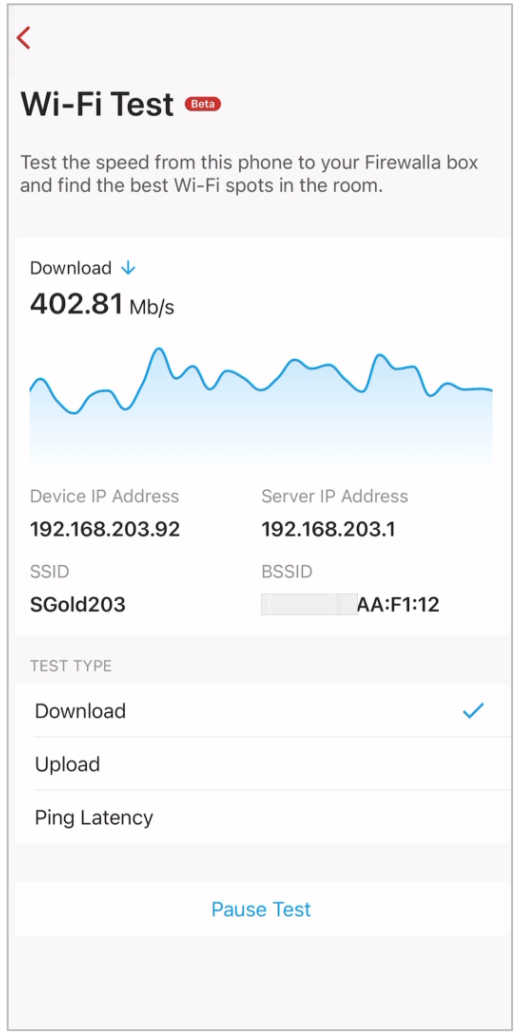
さらに、1.53 アプリ リリースの一部として、ローカル ネットワークに接続している間、デバイス リストに個々のライブ スループットが表示されるようになりました。
ビデオ チュートリアルを参照するか、 Firewallaアプリ リリース 1.53 ノートでこの機能の詳細を参照してください。



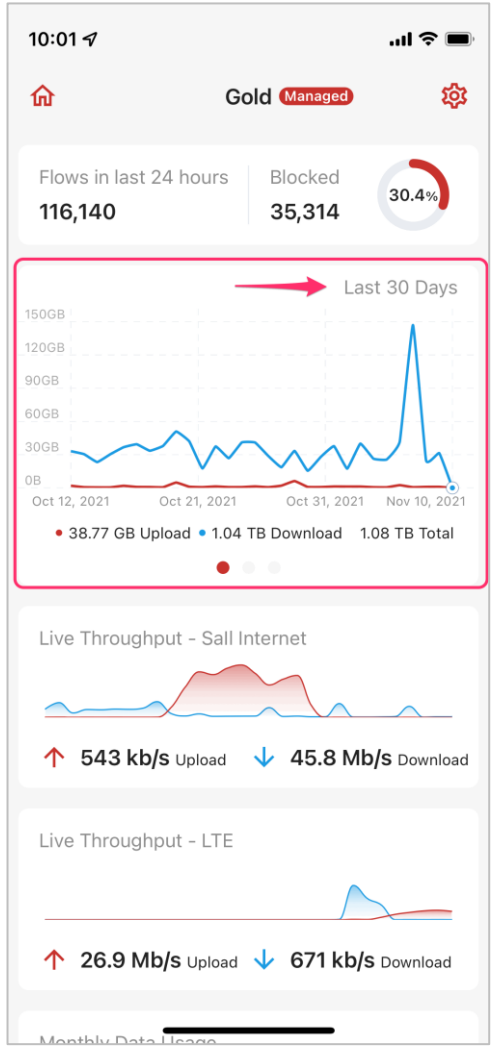
Firewallaには、ネットワーク パフォーマンスの監視と向上に役立つツールが用意されています。
Firewallaは、LAN/Wi-FiネットワークとWANの両方でインターネット速度、ネットワーク遅延、ネットワーク パケット損失を測定できます。



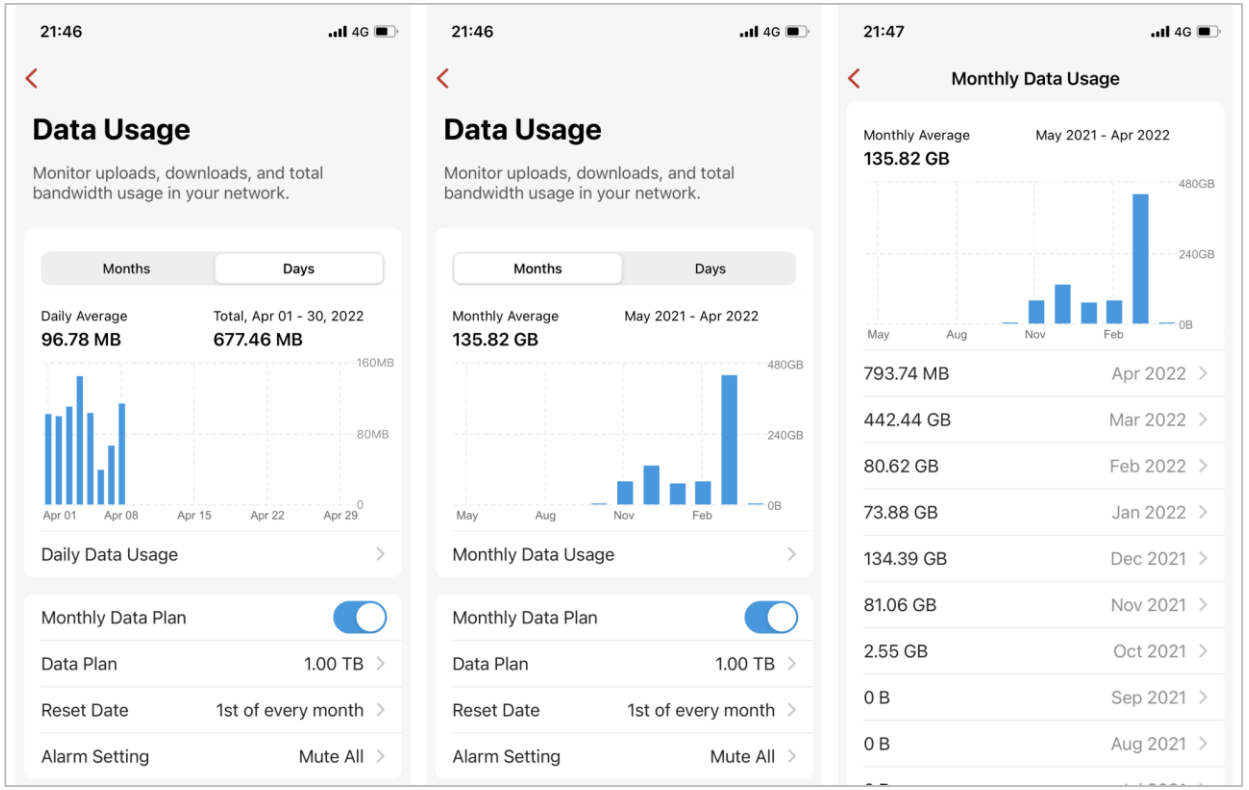
Firewallaは、Wi-Fi接続をリアルタイムでテストおよび調整するのに役立つWi-Fiテスト機能も提供します。
この機能を使用するには、ボックスのローカルWi-Fiに接続していることを確認し、[Wi-Fiテスト] をタップします。
接続のダウンロード速度、アップロード速度、ping遅延、Wi-Fiローミングに関する情報を確認できます。



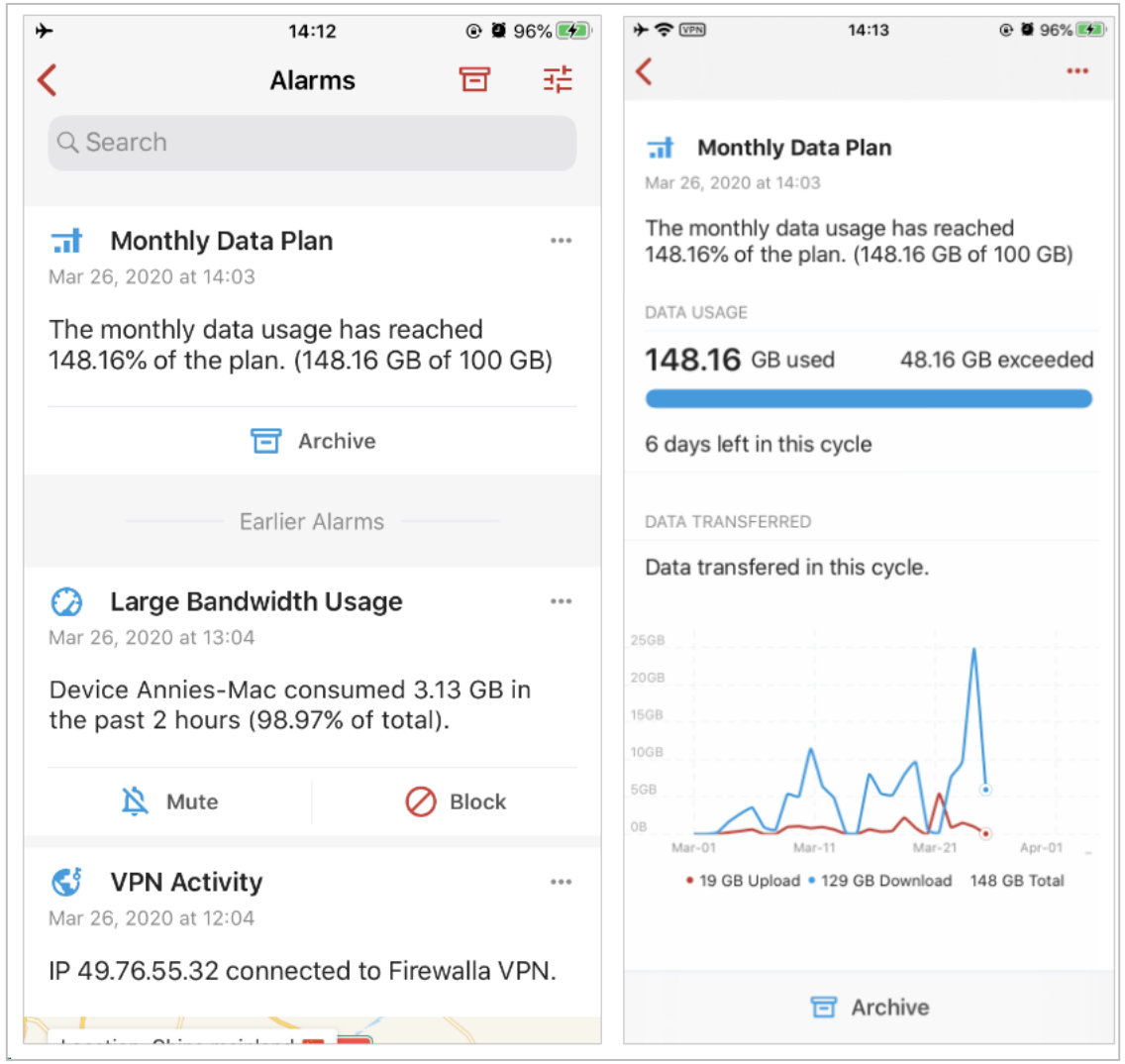
Firewallaでは、過去30日、24時間、および60分間のアップロードおよびダウンロードの合計データ消費量を表示できます。
これにより、月の中で最も活動的な日、1日の時間、または1時間の分を観察できます。
これは、異常なアクティビティを見つけたり、ネットワークのボトルネックを特定したりするのに役立ちます。



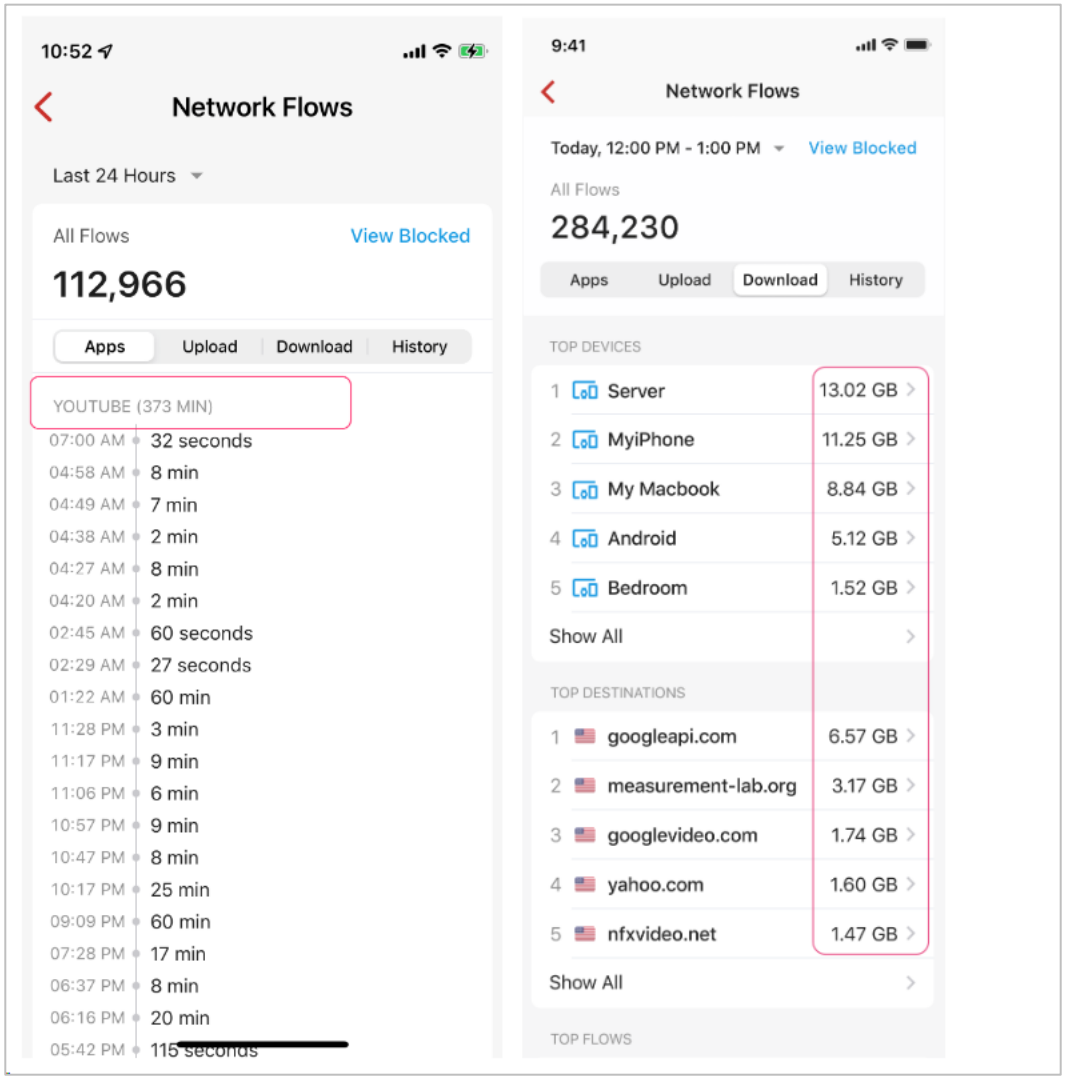
過去のデータ使用量を調べたい場合は、ボックスのメイン ページの一番下までスクロールし、[**詳細**] > [**データ使用量**]機能をタップします。
この機能では、月ごとのデータ使用量グラフと日ごとのデータ使用量グラフが表示されます。各グラフをタップすると詳細が表示され、月間のデータ消費量を比較できます。



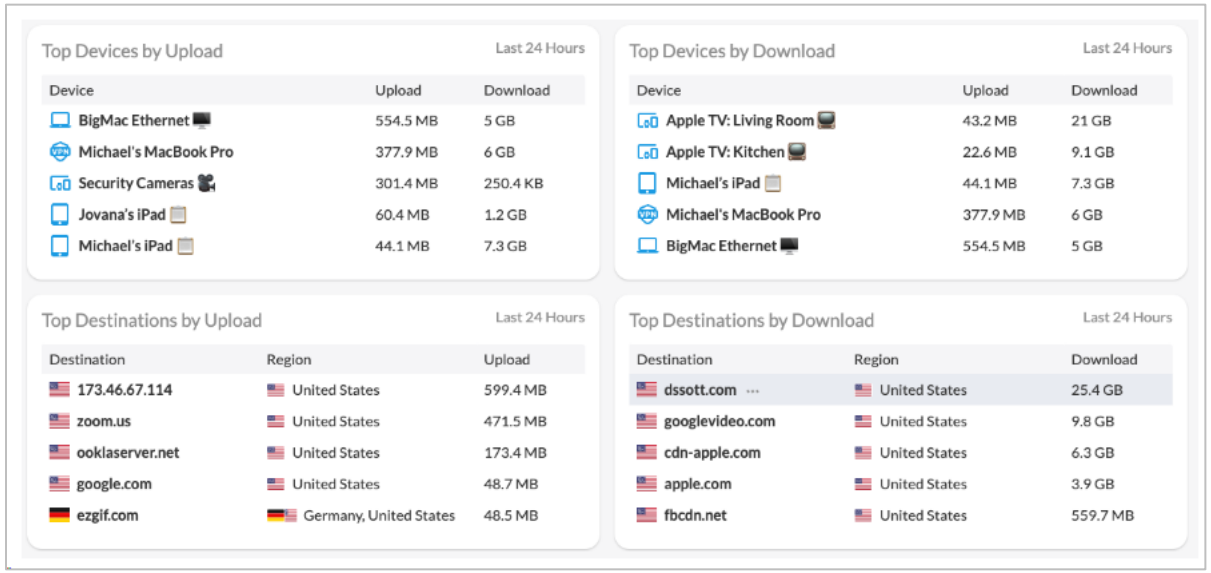
インターネット接続にデータ制限がある場合、Firewallaは消費したデータ量と請求サイクルの残り日数を監視できます。
また、ISPからのペナルティを避けるために、データの上限に達しそうになったときに通知するアラームを設定することもできます。



[ネットワーク フロー]の**[アプリ]**ビューを使用すると、ネットワーク、グループ、またはデバイスがアプリ/ドメインごとに費やしているおおよその時間を確認できます。**アップロード**と**ダウンロード**を使用して、データ使用量の上位を確認してください。



Webインターフェイスには、アップロードとダウンロードの上位デバイスと宛先が表示されます。

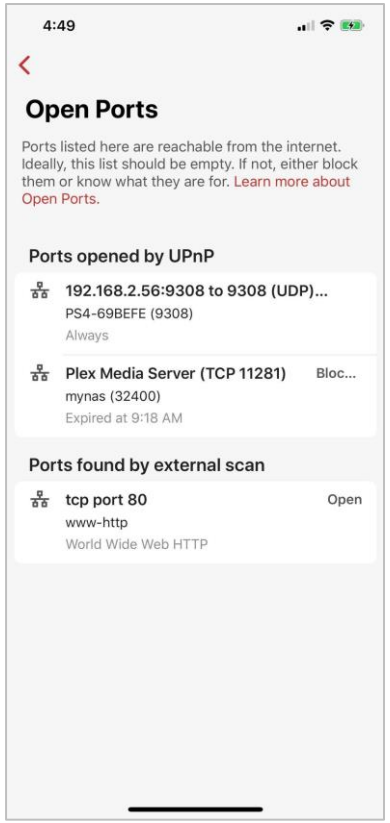


開いているポートを調べる

Firewallaは、次の開いているポートを検出できます。

- 外部スキャンされたポート: 外部スキャンによって検出されたポート。
- UPnP ポート: UPnPプロトコルを使用して検出されたポート。これらのポートは、UPnP経由で他のデバイス/サービスによって開かれます。

「ポートを開く」ボタンをタップすると、これらのポートが表示されます。
それぞれのポートが開いている理由を必ず理解してください。
ルーターでポートを開く必要がある場合は、Firewalla VPNサーバーを使用してそのデバイスにアクセスする方が良い解決策と考えられます。

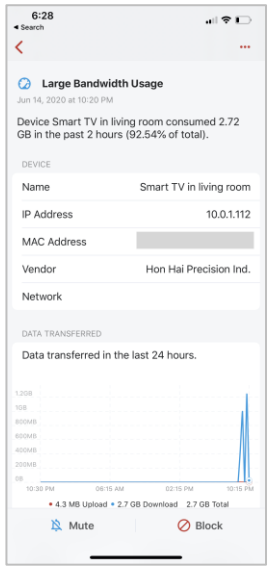


アラームの確認と管理

Firewallaは、不審なアクティビティが発生した場合にアラームと通知で警告します。
アラートには次のようなものが含まれます。

1. ポルノ活動
2. ゲーム活動
3. 警備活動
4. WAN接続の問題
   (Wi-Fiに問題があるのか、ISPがダウンしているのかを推測する必要はありません)
5. VPN接続と接続の喪失
6. デバイスがオン/オフラインになる
7. ネットワーク イベント、ISPダウンタイム、および接続テストの結果
8. 大量の帯域幅の使用量
9. 新しいデバイスの接続
10. ポートを開く

これらのアラートは、ネットワークを管理するのに役立ちます。
アラームが通常の操作または信頼できるサービスに関連付けられている場合は、アラームを無視またはミュートできます。
ただし、デバイスのアクティビティが予期しないものである場合は、調査するかブロックする必要があります。



Webインターフェイスを使用すると、アラーム検索をフィルタリングできます。
たとえば、ハートビート攻撃のセキュリティ アクティビティは次のようになります。