ネットワーク防御③　IDS/IPS(侵入検知サービス/侵入防止サービス)

アクティブプロテクト

Firewallaは、ネットワークを可視化し、ネットワークを制御するために必要な機能を提供するだけでなく、バックグラウンドで動作し、ネットワークを悪意のある活動から継続的かつ積極的に保護します。
Firewallaは、侵入検知システム (IDS) として、ネットワークを監視し、悪意のあるアクティビティや脆弱性を検出すると警告を発します。
また、Firewallaは侵入防止システム(IPS)として、危険な接続を自動的に識別してブロックします。
Firewallaは、デバイスを可能な限り安全に保つため、いくつかの保護モードを使用しています。

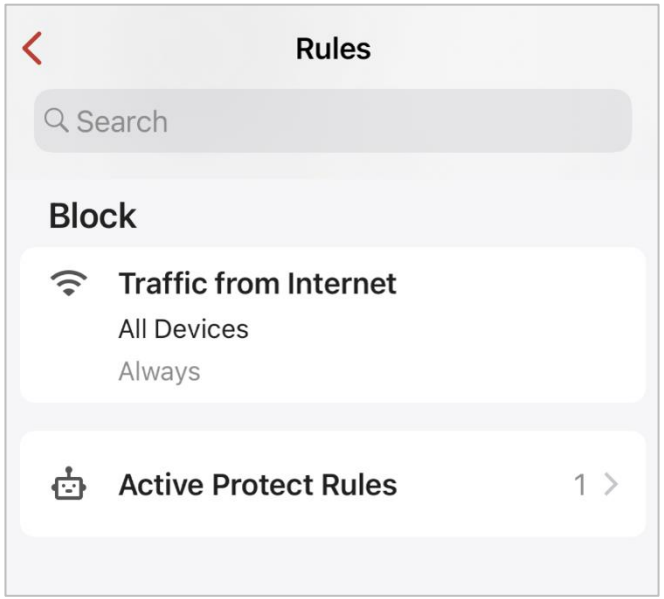
1. ファイアウォール
2. アクティブプロテクト
   2.1. 動作検出
   2.2. シグネチャベースの検出
      - ターゲット リスト
      - ユーザーフィードバック
3. 外出先でのセキュリティ
4. FAQ: 既定のブロックとドメインのみのブロック

Firewallaはネットワークを理解、評価しネットワーク エクスペリエンスを向上させることができます。
Firewallaを使用し、ネットワークを可能な限りベストの状態を維持するための方法をご覧ください。

1. ファイアウォール

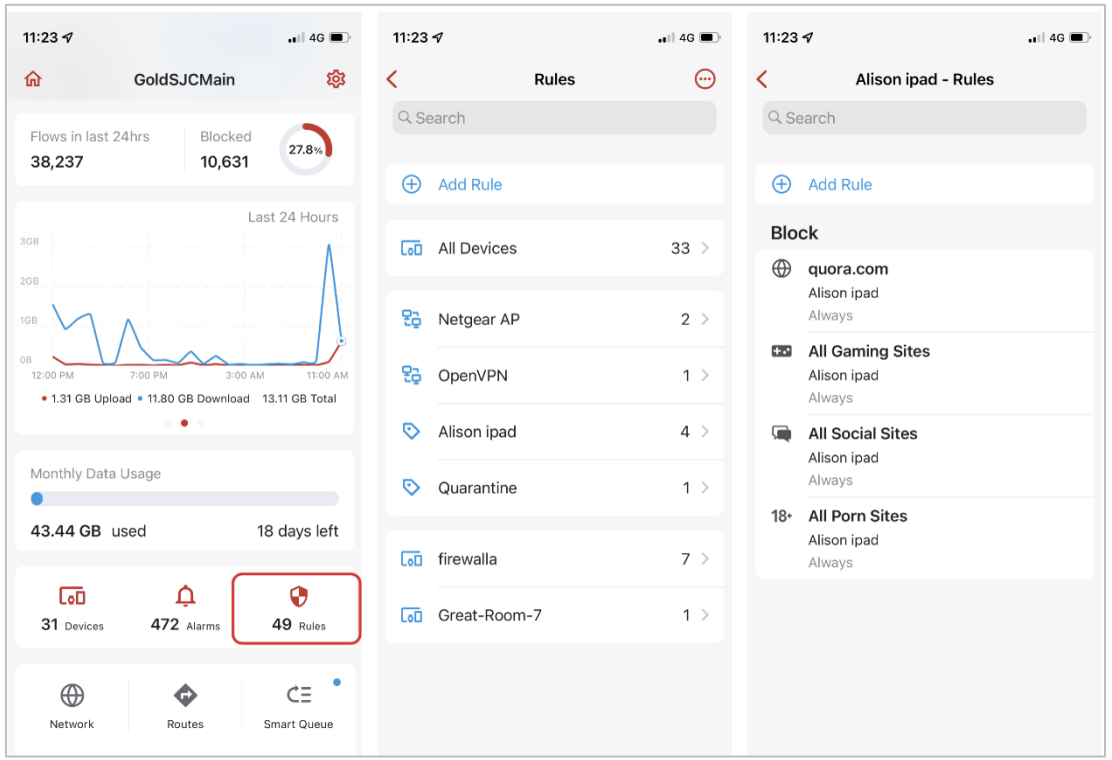
1.1.イングレス ファイアウォール

ルーターモードで実行している場合、すべてのFirewallaボックスにはステートフルイングレスファイアウォール(外部からのネットワークトラフィックがネットワークの内部に受信する)があります。これは「インターネットからのトラフィックをブロックする」ルールです。このルールは、ネットワークに侵入しようとするものをすべてブロックすると同時に、通常のトラフィックに影響を与えません。



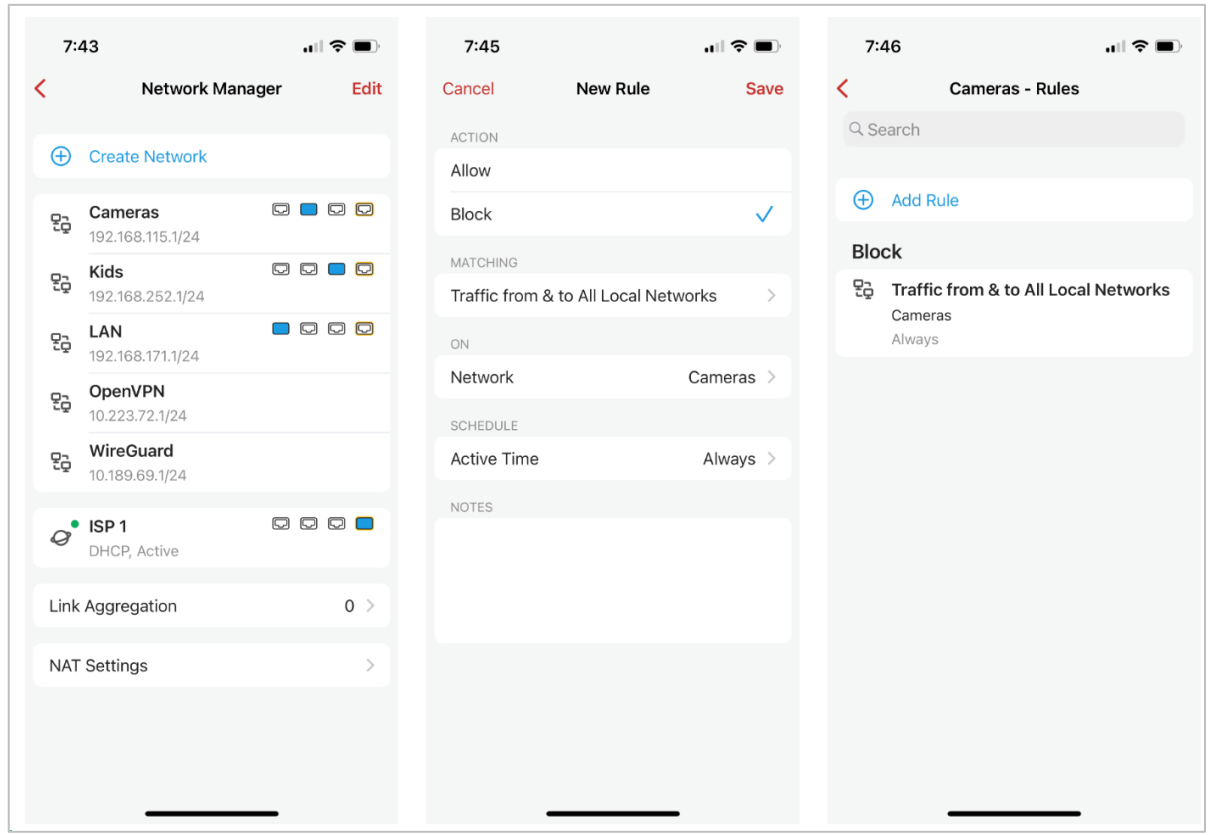
1.2.エグレスファイアウォール

Firewallaは、内側から外側への送信パケットに対しフィルタリングするファイアウォールでもあります。
デバイスにルールを設定することで、出力ファイアウォールを構成できます。ルール設定については、**「ネットワークの防御②　ルール設定 」**を参照してください。



1.3.セグメントファイアウォール

ルーターモードを使用するとFirewallaに接続されたネットワークセグメントにも適用できます。
イングレスファイアウォールとエグレスファイアウォールを使用して、セグメントへの出入りを制御できます。

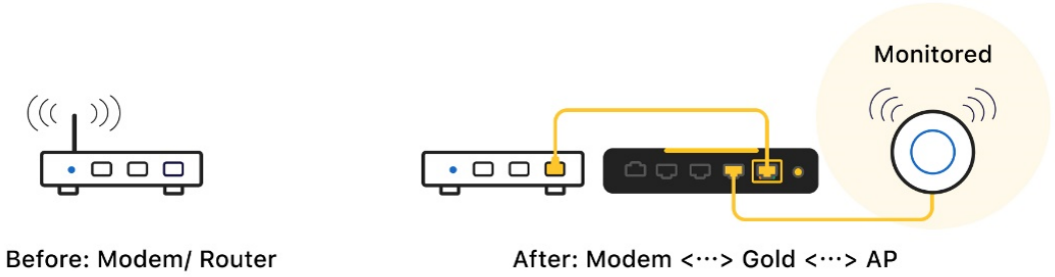


2. アクティブプロテクト

アクティブプロテクトは、Firewalla が提供するIDS/IPS(侵入検知サービス/侵入防止サービス)です。
次の手順でアクティブプロテクトを設定できます。**[Firewallaアプリ下部の詳細] > [アクティブプロテクト]**
アクティブプロテクトを有効にすると、自動的に次のことが行われます。

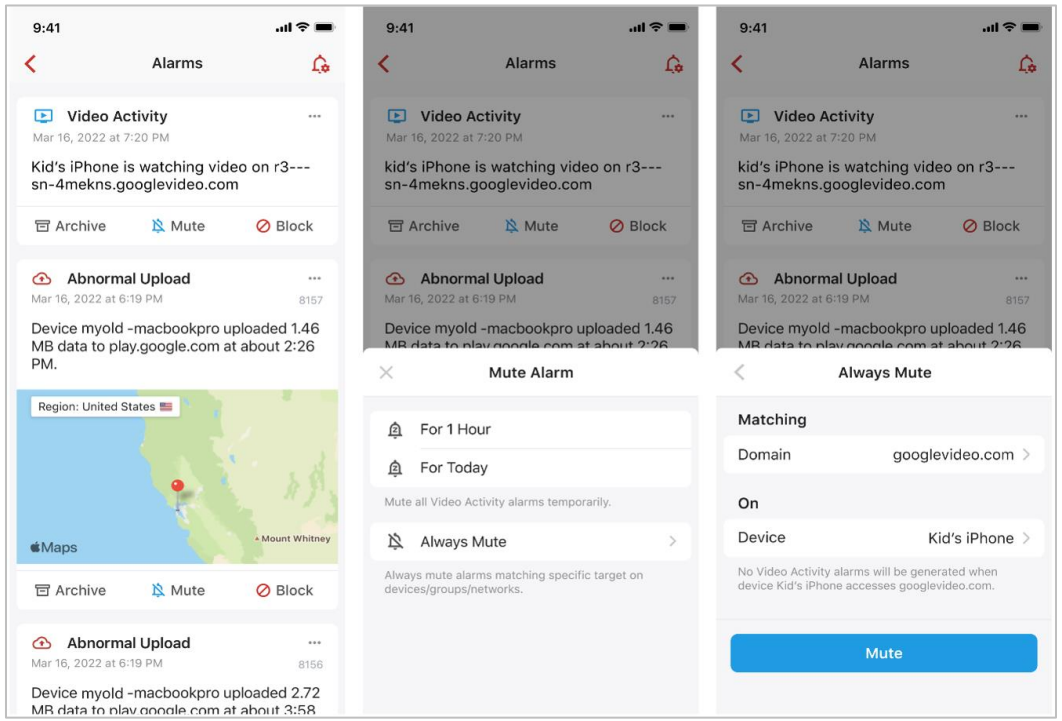
- ネットワークに出入りするトラフィックを分析し疑わしいアクティビティを検出
- 危険度の高い接続をブロック
- 異常なアクティビティを検出すると、アラームと通知で警告

Purple SEとGold Plusは、通常は物理的にインラインでもあるマルチポートデバイスであるため、すべてのデータエグレス(アウトバウンド)またはイングレス(インバウンド)はFirewallaによって監視、評価、および管理されます。



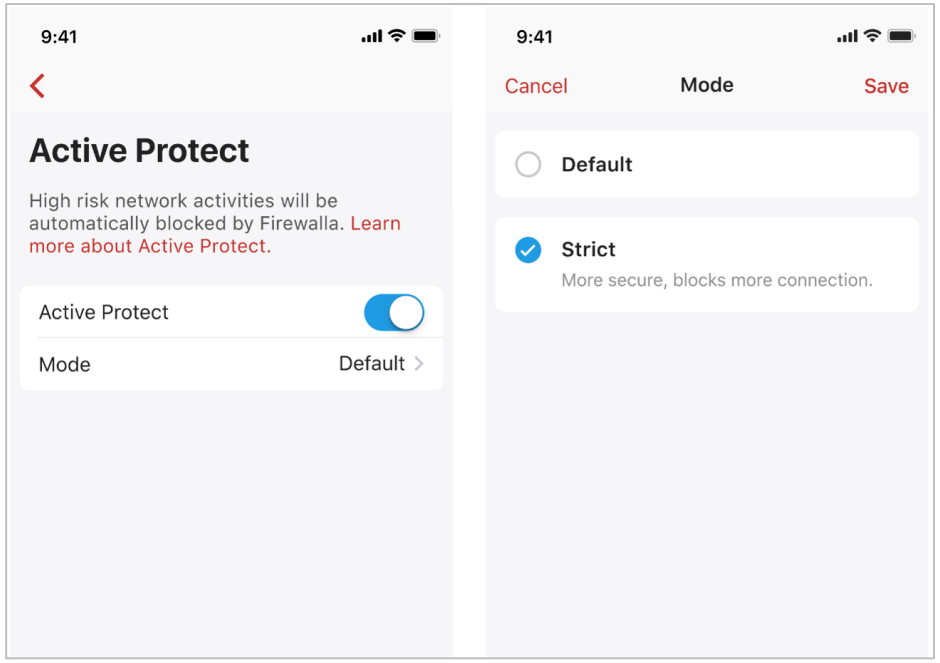
2.1.ネットワークベースの保護

ネットワークを内部的に保護するために、アクティブプロテクトには、すべてのデータフローが比較される複数の保護レイヤーがあります。これらはすべて連携して、どのトラフィックが危険であるかを判断します。
「悪意ある通信」であることが確実な接続の場合、Firewallaはそれらを自動的にブロックできます。
疑わしいが正当な接続の場合、アラームが発生し、接続をブロックするオプションが表示されます。
アクティブプロテクトは、シグネチャベースのアルゴリズムと動的分析の両方を使用し、危険な接続を検出します。
たとえば、「異常な」アップロードアクティビティが発生した場合、アクティブプロテクトは「異常なアップロード」アラームを生成します。
そこから、アラームを無視したり、アクティビティを許可またはブロックしたりできます。



2.2 行動検出

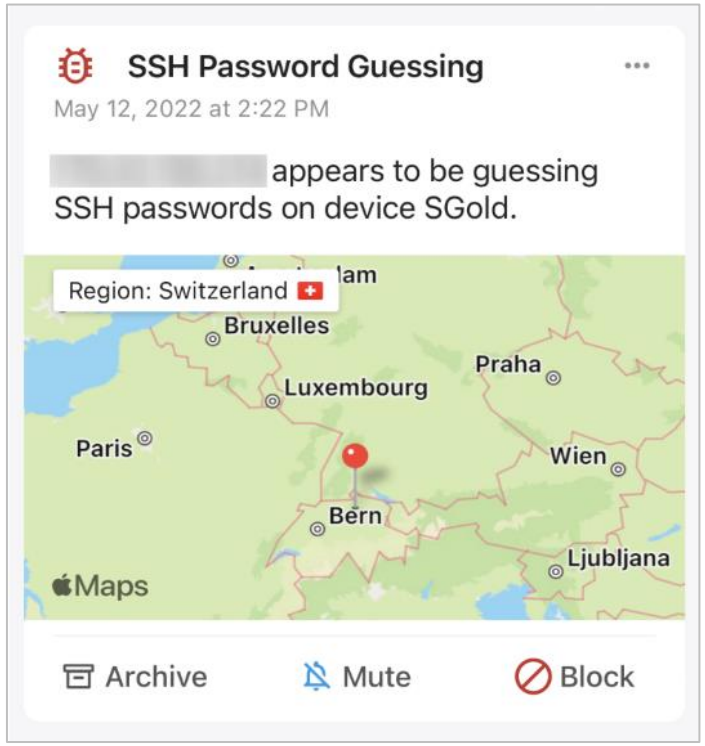
Firewallaのシステムはレピュテーション（評判）に基づいており、アクティビティやサイトのレピュテーションは時間とともに変化します。
変化によっては、常時ブロックポリシーが誤検知を引き起こし、インターネットエクスペリエンスを妨げる可能性があります。
このため、Firewallaはアクティブプロテクトに対してデフォルトモードとストリクトモードの 2つの異なる構成を提供しています。
●ストリクトモードは、Firewallaのセキュリティインテリジェンスのクラウドデータベースをより頻繁にチェックします。
●ストリクトモードでは、アラームを発生させる代わりにフローをブロックする可能性が高くなります。
●ストリクトモードでは、ブロック確率が高いため、誤検知が増える可能性があります。



アクティブプロテクト は、この機能または監視を手動でオフにした場合にのみ一時停止できます。

FirewallaのIDSおよびIPSシステムは、攻撃者(またはユーザー)の意図に基づいて、アラームを生成したり、アクセスをブロックします。シグネチャベースの検出とは異なり、このタイプの検出はマッチングを超えて、何が起こっているのかを深く掘り下げます。
この検出の一部は、ネットワーク上の従来のIDS/IPSを介して行われます。動作検出では、次のことができます。

- SSH ログイン失敗の試行を検出し、アラームを生成する
- ハートブリード攻撃の検出/ブロックする
- データの異常なアップロードまたは転送を検出する



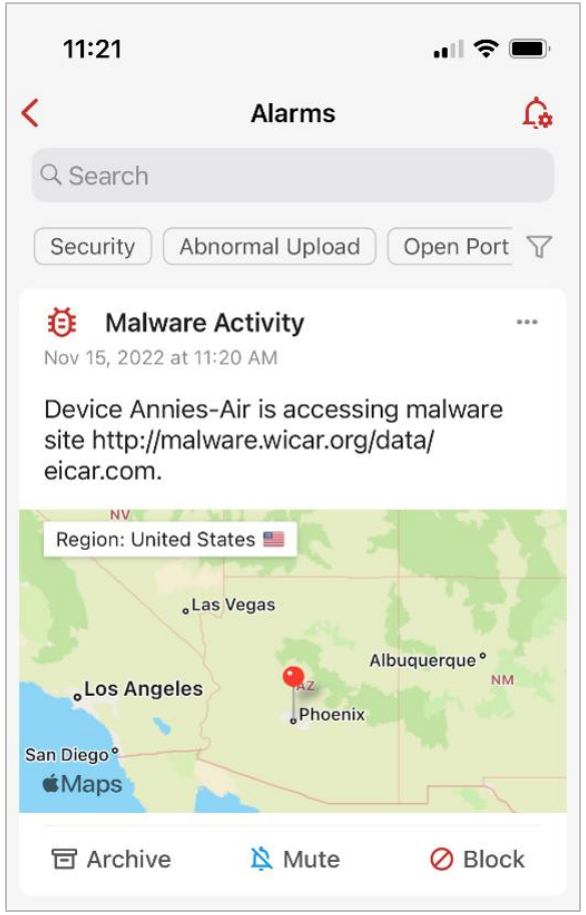
Firewallaの行動検出は、機械学習によって通知されます。
これらの IDS/IPS の一部もシグネチャベースでもあります。
これは、異常ベースの検出と呼ばれる場合があります。

2.3 シグネチャベースの検出

Firewallaは、広範なセキュリティ インテリジェンスにアクセスできます。
これらのフィードは非常に大きく(一般的な小型コンピュータが処理できるよりもはるかに多い)、動的です(サイトの評判は頻繁に更新されます)。
ネットワーク フローが生成されたとき、または生成されようとしているとき、Firewallaは Firewalla ボックスから 2 段階のルックアップ システムを使用します。
パフォーマンス上の理由から、最も頻繁に使用される情報は常にFirewallaボックスに定期的に同期されます。

シグネチャベースの検出は、次の方法で機能します。

1. DNS および TLS ヘッダー スニッフィングを使用してフロー (送信元と宛先) を識別します。
2. IPアドレス/ポートをチェックして、発信元と宛先を確認します。
3. ローカルのファイアウォールインテリジェンスをチェックして、フローをブロックする必要があるかどうかを確認します。
4. このフローが危険度の高い可能性があるかどうかを確認し、必要に応じて二次チェックのためにクラウドを参照します。
5. ユーザー定義のターゲット リストとの照合します。(シグネチャベースの検出を機能させるために独自のリストを持ち込む必要はありません)。

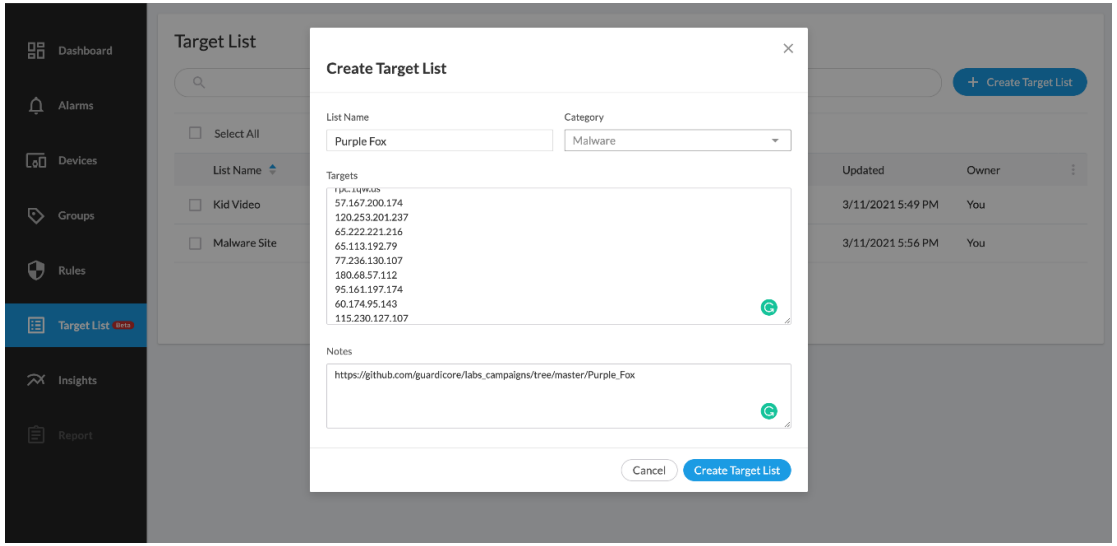


Firewallaは何百万ものサイトを追跡する必要があるため、作業を簡単にするために、各サイトにレピュテーションスコアを付けています。
このレピュテーションスコアは、良いか悪いかの二項評価ではなく、良いと悪いの間のスコアです。
時間の経過とともに、サイトの評判は多くの要因によって変化する可能性があります。
サイトの評判が悪くはないがそれほど良くない場合は、アラームを受け取る可能性があります。不良の場合、ブロックとアラームが発生する可能性があります。

2.4.ターゲット リスト

Firewallaにはすでに動的セキュリティ情報の非常に大きなデータベースがあるため、必要な場合を除いて、独自のリストをインポートする理由はありません。ただし、独自のターゲットを選択したい場合に備えて、ターゲットリスト機能を提供しています。

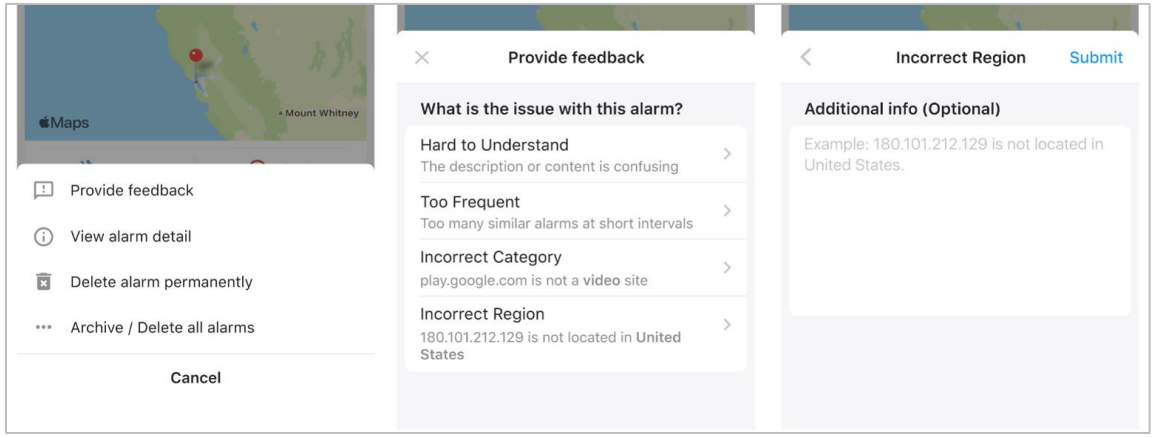
- ユーザー定義のターゲット リストを使用して、ドメインと IP をグループ化できます。このリストの長さには制限があります。
- また、Firewallaは、より一般的なリスト(OISDやlog4j攻撃サイトなど)の一部を自動的に同期します。Firewallaは、これらを自動的に管理します。



アクティブプロテクトは動的でレピュテーションベースであるため、レピュテーションが良好なサイトをブロックしない可能性があります。ターゲット リストをブロックするルールを作成すると、サイトのレピュテーションに関係なく、ターゲット リストのエントリは常にブロックされます。
Firewallaのシグネチャは、合法的なサイトをブロックする可能性がないことを確認するために、システムによって常にチェックされています。
さらに、Firewallaの情報は動的に管理されるため、Firewallaはターゲットリストを手動で同期するよりもはるかに速く情報を削除および追加できる場合があります。
Firewallaの特殊なシグネチャリストの合計サイズは、6000万エントリ以上です（2022/1/1時点）

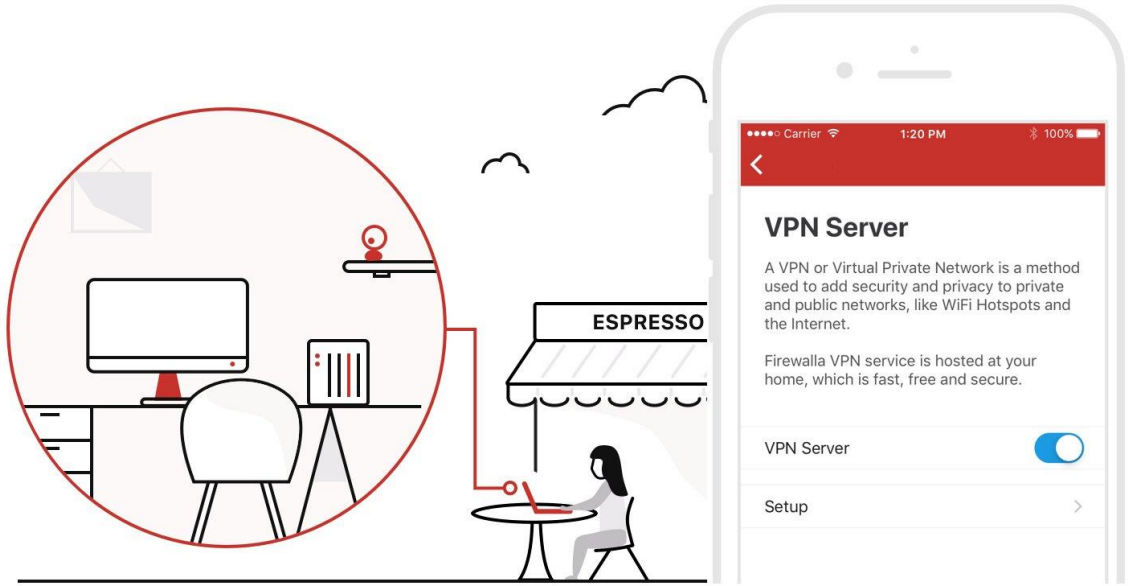
2.5.ユーザーフィードバック

アラームが表示され、ミュート/無視、アーカイブ、またはブロックしてそれに対処することで、Firewallaシステムに貴重なフィードバックを提供します。
十分なフィードバックがあれば、システムはあなたの習慣を学習し、あなたの習慣に合わせて行動を調整し始めます。
ただし、時々間違いを犯す可能性はあります。このような場合は、アプリから直接フィードバックを送信できます。
たとえば、ファイルをクラウドにバックアップするのに数時間を費やすと、Firewallaはこれを異常なアップロード動作として登録し、アラームを送信する可能性があります。
アップロードする頻度とデータの量に応じて、Firewalla はこのアクションにフラグを立て続け、より多くのアラームを送信する場合があります。
Firewallaの学習を改善するために、異常なアップロードアラームが「頻繁すぎる」というフィードバックをアプリのアラーム通知から直接提供できます。



3.外出先でのセキュリティ

Firewallaは、自宅でデバイスを保護するだけではありません。
外出先やお気に入りのコーヒーショップにいるときは、Firewallaの組み込みVPNサーバーに接続して、自宅にいるかのように同じレベルの保護でインターネットを閲覧できます。
Firewallaが外出中にユーザーを保護する方法の詳細をご覧ください。



参考

デフォルトブロックとドメインのみのブロック

ドメインをブロックするファイアウォールを設定するときは、デフォルトモードとドメインのみモードのどちらかを選択できます。
デフォルトモードでは、2つの異なるドメインが同じIPアドレスにマッピングされている場合、一方のドメインをブロックするともう一方のドメインもブロックされます。
ドメインのみモードは、同じIPでホストされている他のドメインをブロックしない、制限の少ないオプションです。
ただし、一部のアプリケーションはドメインではなく IP アドレスでサーバーにアクセスするため、ドメインのみのルールが意図したとおりに機能しない場合があります。