モード設定③　DHCPモード

DHCPモード

1.DHCP モードの概要

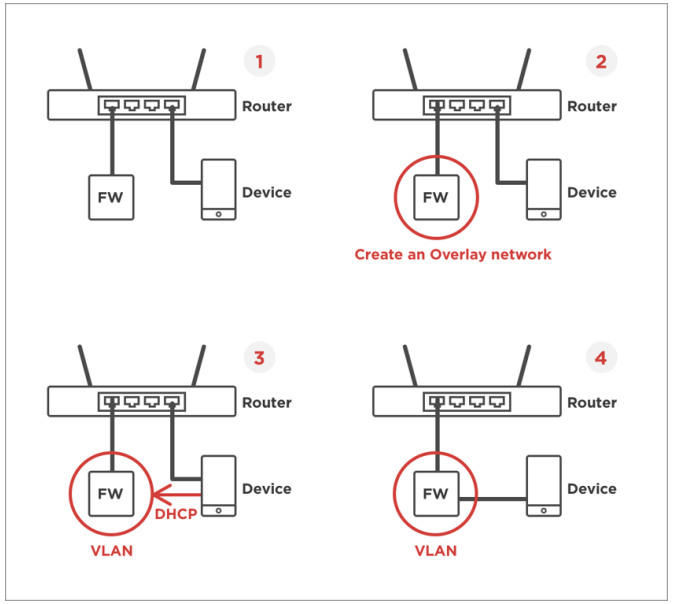
ルータの DHCP サーバーを無効化しFirewallaがDCHPサーバとなることで、トラフィックを監視します。
DHCP モードはルータからパケットを取得するためのARPスプーフィングに応答しないため、シンプル モードよりも安定し、高速になります。また、ほとんどのルータと互換性があります。

2.DHCP モードの動作

DHCP方式では、Firewallaが既存のネットワーク上に更にネットワークを追加します。
新しいネットワークは、ホーム ネットワークの物理層の上に静的にオーバーレイします。
デバイスをこのオーバーレイ ネットワークに静的にポイントすることも、メイン ルーター上の既存のDHCPサービスを無効化または変更して、FirewallaにDHCP要求を処理させることもできます。
Firewallaは、同じネットワーク内のすべてのデバイスからのDHCP要求に応答し、オーバーレイ ネットワークからIPを割り当てます。

3.Firewalla のオーバーレイ ネットワーク

オーバーレイ ネットワークはFirewalla によってランダムに作成されます。
Firewallaアプリでオーバーレイ ネットワークを確認するには、[Box 設定] ⇒ [詳細設定] ⇒ [ネットワーク設定] ⇒ [オーバーレイ ネットワーク] をタップします。
ネットワークを他のサブネットに変更することもできます。また、DHCPサーバーを使用するか、そのブロックでデバイスの静的IPアドレスを手動で構成することで、ネットワークを使用できます。



注:現在、Firewalla DHCPモードはIPv4トラフィックのみを監視可能です。

4.DHCPモードのセットアップ

初めてFirewallaを起動すると、デフォルトでシンプル モードで実行されます。
ホーム ルーターの一部は、Firewallaのシンプル モードと互換性がない可能性があります。

ステップ 1: DHCP モードで Firewalla をセットアップする

インストール中: Firewallaがメイン ルーターがシンプル モードと互換性がないことを検出した場合は、代わりにDHCPモードを使用するようにアドバイスします。[DHCP モードでセットアップ] をタップして続行します。

インストール後: DHCPモードに手動で切り替えるには、「詳細」→「Mode」ボタンをタップし、「現在設定しているモード」を選択し、一覧の中から「DHCP モード」を選択します。Firewallaボックスは、すべてのデバイスに新しいIPアドレスを割り当てます。

ステップ 2: ルータの DHCP サーバーをオフにする

重要

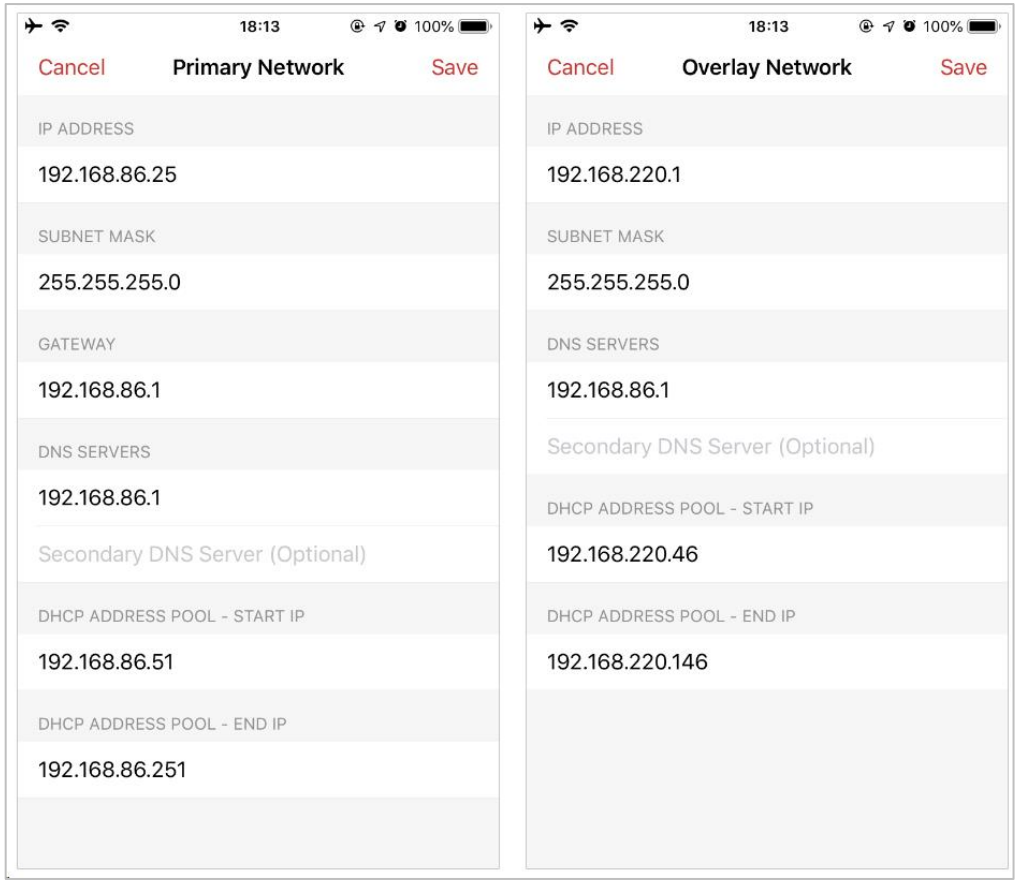
1. DHCPサーバーをオフにする前に、ルータのIPアドレス (通常は 192.168.x.1 または 10.xx1) をメモしてください。
   何か問題が発生した場合は、スマートフォン/PCで静的IPを手動で設定し、ルータのIPをネットワーク ゲートウェイとして設定して、
   ルータへのアクセスできるようにしておく必要があります。
2. DNSサーバーがルータ自体である場合は、DNSサーバーを 1.1.1.1 や 8.8.8.8 などのパブリックなものに変更します。
   DHCPがオフの場合、ルータ上のDNSサーバーをオフにするルータがいくつかあります。以下はSynology Routerを使用した例です。

ステップ 3. ネットワークに再接続する

Firewalla DHCPサービスから新しい IP アドレスを取得するために、すべてのデバイスをホーム ルーターに接続し、ネットワークに再度接続させます。
(モバイル デバイスの機内モードをオフ/オンにするか、単にデバイスを再起動することができます)

5.DHCP の IP 範囲を設定するには

DHCPモードでは、オーバーレイ ネットワークはすべての監視対象デバイスが接続するネットワークであり、プライマリ ネットワークはすべての監視対象デバイスが接続するネットワークです。
Firewalla DHCPサービスは、監視設定に基づいてデバイスをこれら2つのネットワークに自動的に割り当てます。
*注意: DHCPモードのGold Plusはこれらのオプションを提供せず、常にオーバーレイネットワークをプライマリ ネットワークと同じネットワークとして構成します。



プライマリネットワーク

プライマリ ネットワークは、すべての監視されていないデバイスのネットワーク設定を構成します。
Firewalla DHCPサービスがデバイスのDHCP要求に応答すると、ネットワーク設定がデバイスに渡されます。デフォルトでは、ルーターから設定を継承します。

オーバーレイネットワーク

オーバーレイ ネットワークは、すべての監視対象デバイスのネットワーク設定を構成します。
Firewalla DHCPサービスがデバイスの DHCP 要求に応答すると、ネットワーク設定がデバイスに渡されます。

デフォルトでは、オーバーレイ ネットワークはFirewallaによってランダムに作成されますが、他のネットワーク サブネットに変更することもできます。
モニタリングのためにオーバーレイ ネットワーク内でデバイスのIPアドレスを変更しないようにしたい場合は、オーバーレイ ネットワークでプライマリ ネットワークと同じサブネットを使用するようにできます。

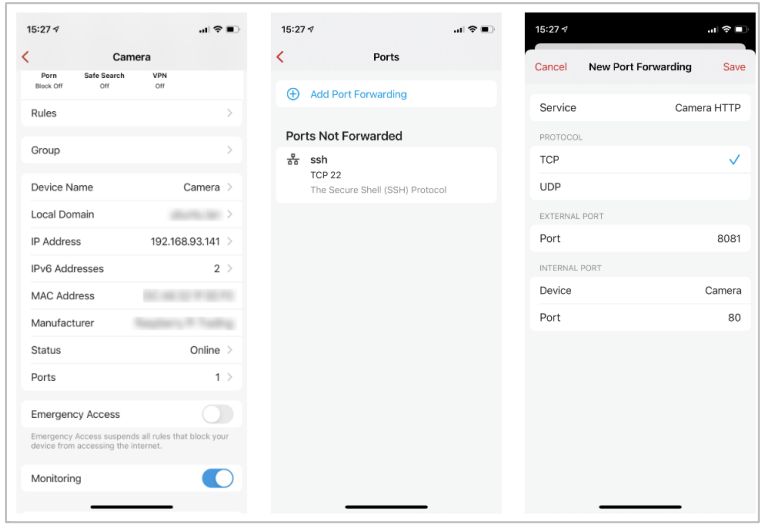
デバイスがFirewallaから新しいDHCP設定を取得するには、古い設定の有効期限が切れるまで待つか (通常は24時間以内にかかります)、
デバイスをネットワークに再参加させるか (IoTデバイスの場合は再起動します) する必要があることに注意してください。仕事をする）。

VPN サーバー ネットワーク

VPNサーバー ネットワークは、Firewalla VPNサーバーに接続する場合のVPNクライアントのサブネットです。
各クライアントは、このサブネットに割り当てられたIPアドレスを取得します。サブネットはFirewallaによってランダムに生成され、構成することはできません。

6.DHCP モードでデバイスのポート転送を設定する

Firewalla DHCPモードはメイン ネットワーク上にオーバーレイ ネットワークを作成するため、自宅の外のNASやカメラにアクセスするなど、デバイスのポート転送を作成する場合は、Firewallaでポート マッピングを作成する追加の手順を実行する必要があります。さらに、ルーター上でポート転送を作成します。
注: この設定により、外出先からNASデバイスまたはカメラにリモートでアクセスできますが、これは最も安全な方法ではありません。
この記事では、セキュリティ保護で同じ機能を実現するために、代わりにFirewalla VPN サービスを使用することをお勧めします。
例:ホームカメラのWebサイト (HTTP、TCP ポート 80) にリモートでアクセスしたい場合は、ルーターだけでなくポート転送 (例: TCP 8081 ⇒ 8080) も設定する必要があります。)
Firewallaでも同様です。
これで、 http://<Firewalla_DDNS>:8080からカメラ Web サイトにアクセスできるようになります。



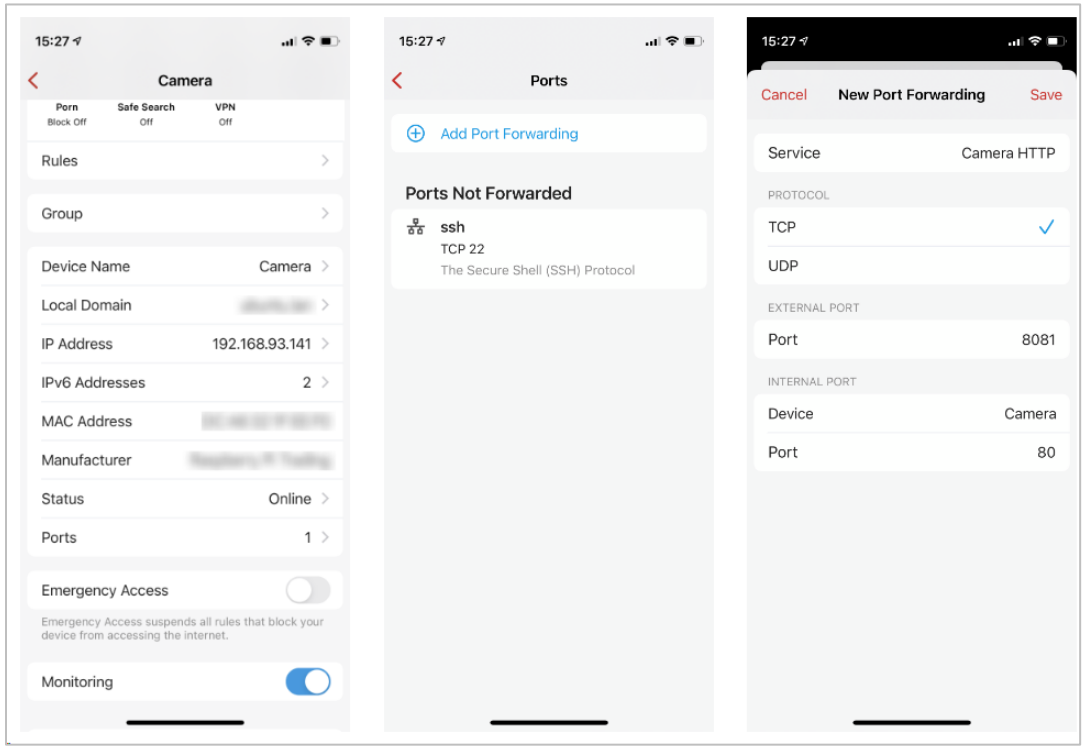
*注意: ポート 8080 と 8081 については、ルーターとFirewallaの間で一貫性がある限り、独自のポートを選択できます。
ルーター上のウェルノウン ポート (22、80、443 など) を開くことは、攻撃される可能性が非常に高くなるため、お勧めできません。

ステップ 1

ルーター上で、TCPポート 8080 をFirewallaのポート、たとえばポート 8081 に転送するポート転送を作成します。
詳細な手順は、各ルーターのインターフェイスによって異なります。

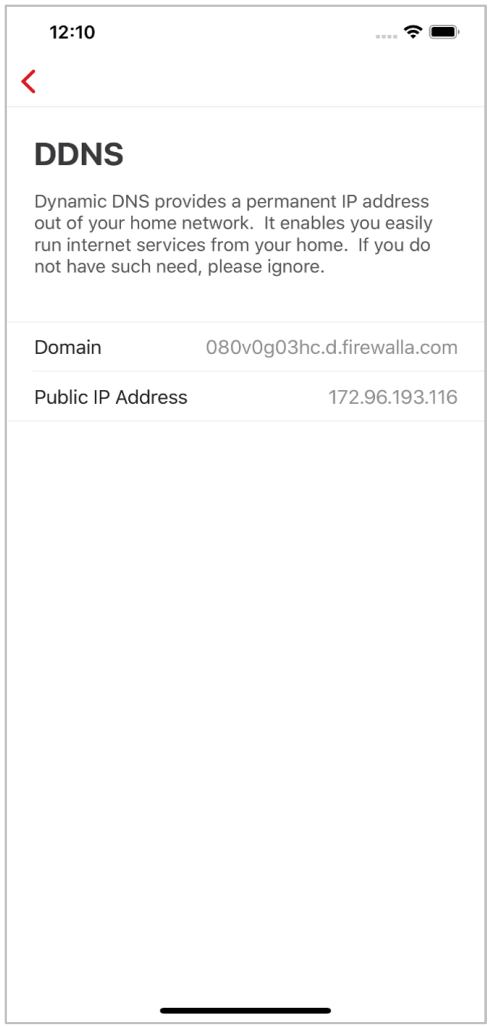
ステップ 2

Firewallaで、[デバイス]でアクセスしたいカメラを見つけ 、 [ポート] ⇒ [ポート転送の追加] をタップして 新しいポート転送を作成します。
外部ポートをFirewallaのポートとして 8081 に設定します。内部ポートをカメラのポートとして 80 にします。
「保存」をタップして設定を保存します。



ポートにアクセスするには

たとえば、ブラウザを使用して http://<Firewalla_DDNS>:8080にアクセスします。
DDNS情報は「DDNS」機能で見つけることができ、Firewalla DDNSは自動的にパブリックIPを指します。



7.DHCP モードでデバイスの IP アドレスを予約する

Firewalla DHCPモードでは、次の3つのオプション間でIP割り当て方法を切り替えることができます。

動的

この設定では、Firewallaはネットワークの IP範囲に基づいてランダムなIPアドレスをこのデバイスに割り当てます。

- ダイナミックには追加の設定はありません。

予約済み

この設定では、Firewallaは指定した特定のIPアドレスをこのデバイスに割り当てます。

IPを予約するには:

- デバイスリストでデバイスを開き、セクション >情報までスクロールし、デバイスのIPアドレスをタップし、予約済み をタップすると、IP アドレスフィールドを編集してデバイス用に予約できます。
  デバイスを再起動するか、IPリースの有効期限が切れるまで (通常は 24 時間)、IPは予約されたアドレスに切り替わらないことに注意してください。
  現在の IP と予約済みのIPが表示され、現在の状態が明確になります。

割り当てない

この設定では、FirewallaはこのデバイスにIPアドレスをまったく割り当てません。
例えば、プリンタなどのデバイスに手動で IP を割り当てる場合、このデバイスに対してFirewallaが何もしないようにすることができます。

- このオプションを使用すると、#3に示すような警告が表示されます。