Firewalla ユーザマニュアル

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]  $\Rightarrow$  [詳細設 定]  $\Rightarrow$  [ネットワーク設定]  $\Rightarrow$  [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

- 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。

-	18:13	@ 🔊 🖉 100% 🗩)	→    →    18:13	@ 🔊 Ö 100% 🕅
Cancel	Primary Network	save	Cancel Overlay Network	Save
IP ADDRESS			IP ADDRESS	
192.168.86	.25		192.168.220.1	
SUBNET MAS	ĸ		SUBNET MASK	
255.255.25	55.0		255.255.255.0	
GATEWAY			DNS SERVERS	
192.168.86	.1		192.168.86.1	
DNS SERVERS	3		Secondary DNS Server (Option	al)
192.168.86	.1		DHCP ADDRESS POOL - START IP	
Secondary	DNS Server (Optior	nal)	192.168.220.46	
DHCP ADDRE	SS POOL - START IP		DHCP ADDRESS POOL - END IP	
192.168.86	.51		192.168.220.146	
DHCP ADDRE	SS POOL - END IP			
192 168 86	.251			



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  $\Rightarrow$  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。

< Came	ra	<	Ports			
Porn Safe Search	VPN		10110		Cancel N	ew Port Forwarding
Block Off Off	Off	Đ	Add Port Forwarding			
Rules	>				Service	Camer
		Port	ts Not Forwarded		PROTOCOL	
Group	>		ssh		TCP	
Device Name	Camera >		TCP 22 The Secure Shell (SSH) Proto	col	UDP	
Local Domain					EXTERNAL POI	RT
IP Address	192.168.93.141 >				Port	
IPv6 Addresses	2 >				INTERNAL POP	rr
MAC Address	10.46.007.007				Device	
Manufacturer	agent 7 palling				Port	
Status	Online >					
Ports	1 >					
Emergency Access						
Emergency Access suspends device from accessing the int	all rules that block your ernet.					
Monitoring						

\*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。



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。



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。

Dynamic DNS provides a permanent IP address out of your home network. It enables you easily run internet services from your home. If you do not have such need, please ignore.	DDNS	
Domain 080v0g03hc.d.firewalla.co	Dynamic DNS proviout of your home nerrun internet service not have such need	des a permanent IP address atwork. It enables you easily s from your home. If you do , please ignore.
	Domain	080v0g03hc.d.firewalla.cor
Public IP Address 172.96.193.1	Public IP Address	172.96.193.11

## 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。



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。

								9									
1:11 🕇			11:	:11 🕇	,						.∥ 奈	88	11:11 -	,			🗢 🛙
IP Addr	ess		<			IF	P Ad	dres	SS		Doi	ne	<		IP Ad	ldress	
IP ALLOCATION			19	92.1	68.23	1.19					e		IP ALL	OCATION			
Dynamic		$\checkmark$				1							Dyna	imic			$\checkmark$
Reserved													Rese	rved			
Do Not Allocate													Do N	ot Alloca	ite		
Dynamics a the durines of plotting advnamic IP address. If you w always have the same IP addres Reserved - If you want your de same IP address, select Reser Do Not Allocate - If you don't IP Address for this device, sele Current IP Address	rant your devic ess, select Res evice to always ved. want Firewalla ect Do Not Allo 192.168	e to erved. have the to assign cate. 3.231.19											a dyna alway Rese same Do N IP Ac <b>Cur</b>	This getting	Do not IP Ad device of IP addr Firev	allocate Idress can no longer ess assigned b walla.	e to d. sigr by 1.1!
														Carr	Cei	Committee	
			1	2	3	4	5	6	7	8	9	0					
			-	1	:	;	(	)	\$	&	@	"					
			#+=		•	,		?	!	'		$\bigotimes$					
			ļ	ABC			spa	ace			don	е					
											-						