Mist 設定マニュアル

- Policy -

WxLAN(アクセス制御ポリシー)の設定

ジュニパーネットワークス株式会社
2021年7月 Ver 1.0

JUNIPer driven by Mist AI

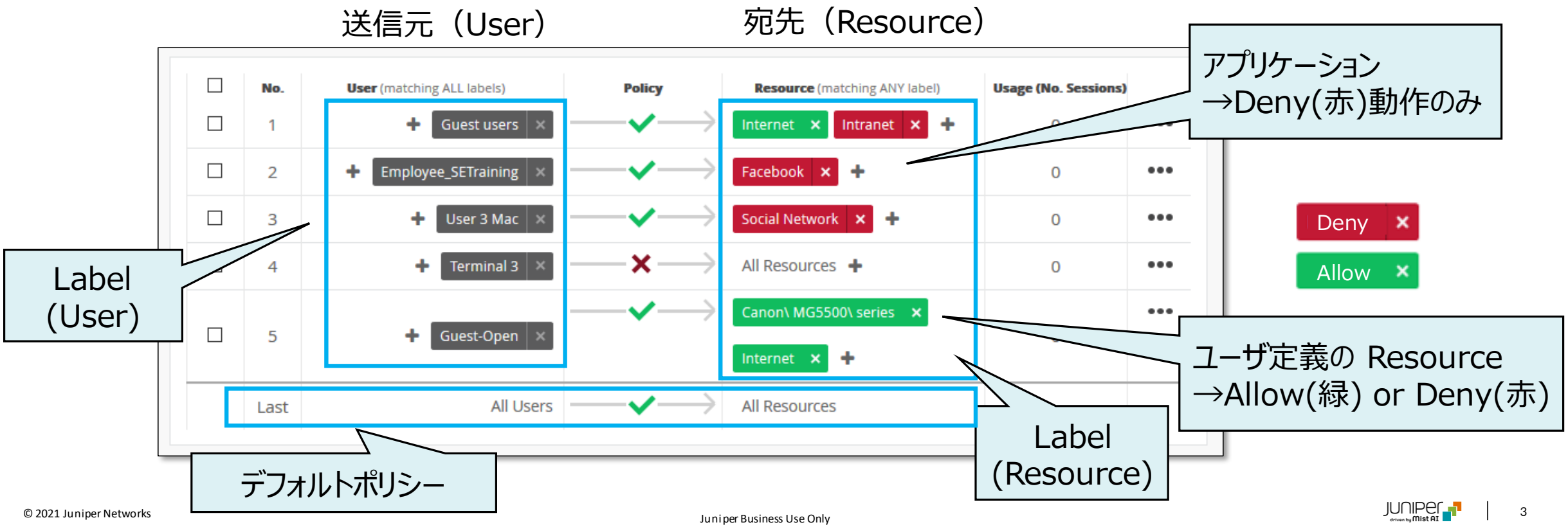
はじめに

- 本マニュアルは、『WxLAN(アクセス制御ポリシー)の設定』について説明します
- 手順内容は 2021年7月 時点の Mist Cloud にて確認を実施しております
  実際の画面と表示が異なる場合は以下のアップデート情報をご確認下さい
  https://www.mist.com/documentation/category/product-updates/
- 設定内容やパラメータは導入する環境や構成によって異なります
  各種設定内容の詳細は下記リンクよりご確認ください
  https://www.mist.com/documentation/
- 他にも多数の Mist 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております
  https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html

WxLAN(アクセス制御ポリシー)の概要

WxLAN(アクセス制御ポリシー)で、ユーザの通信を制御することが可能です

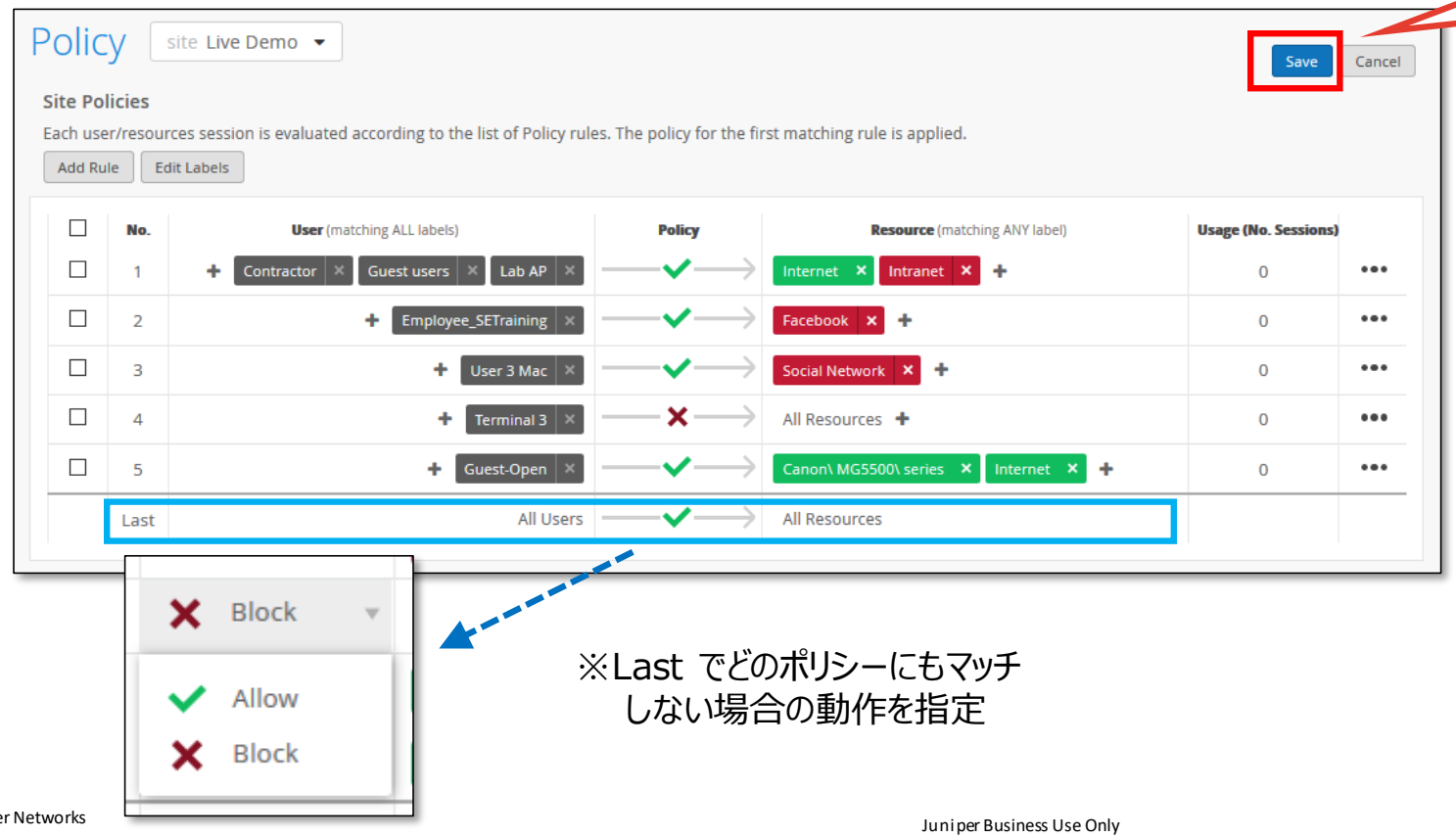
- 送信元(User)に対して宛先(Resource)を指定して、Allow/Deny で通信の可否を制御
- Resource はシステム定義のアプリーション(Deny動作のみ)を選択可能、User とその他の Resource は Label の作成(「Network」 >「Labels」)が必要(IPアドレスの直打ちは不可)
- デフォルトポリシー(Last)で、すべての通信を許可(拒否も設定可)



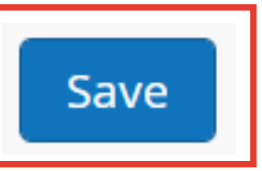
ポリシーの評価

ポリシーの適用ルールは以下の通りです

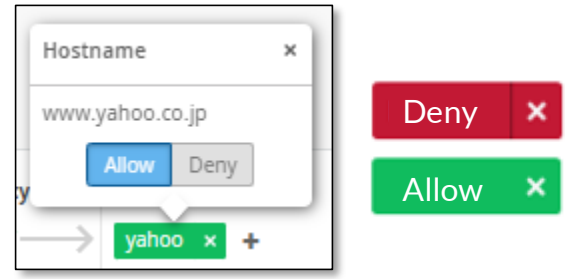
1. 上から順に評価
2. User に設定された**全てのラベルにマッチ**した場合にポリシーが実行
3. 一度ポリシーが適用されると以降のポリシーは評価されない(First Match)
4. ポリシーにマッチしない通信は、Last で全て許可または拒否される



※Last でどのポリシーにもマッチしない場合の動作を指定



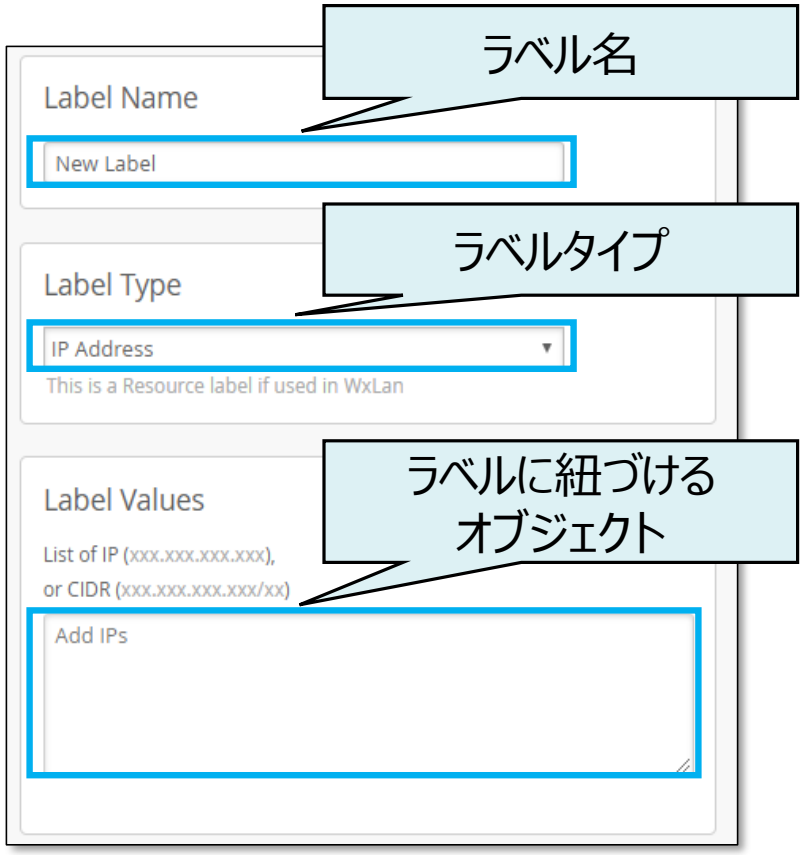
※ Save で設定を保存



※ 定義した Resource のラベルは、Allow/Deny の選択が可能

ラベルの概要

- ラベルには Label Name, Label Type, Label Values を設定します
- WxLAN(アクセス制御ポリシー)への設定が可能な Label Type は 8 項目（右表）
- Label Type 毎にポリシーの適用可能な箇所（User/Resource）が決まっている（右表）

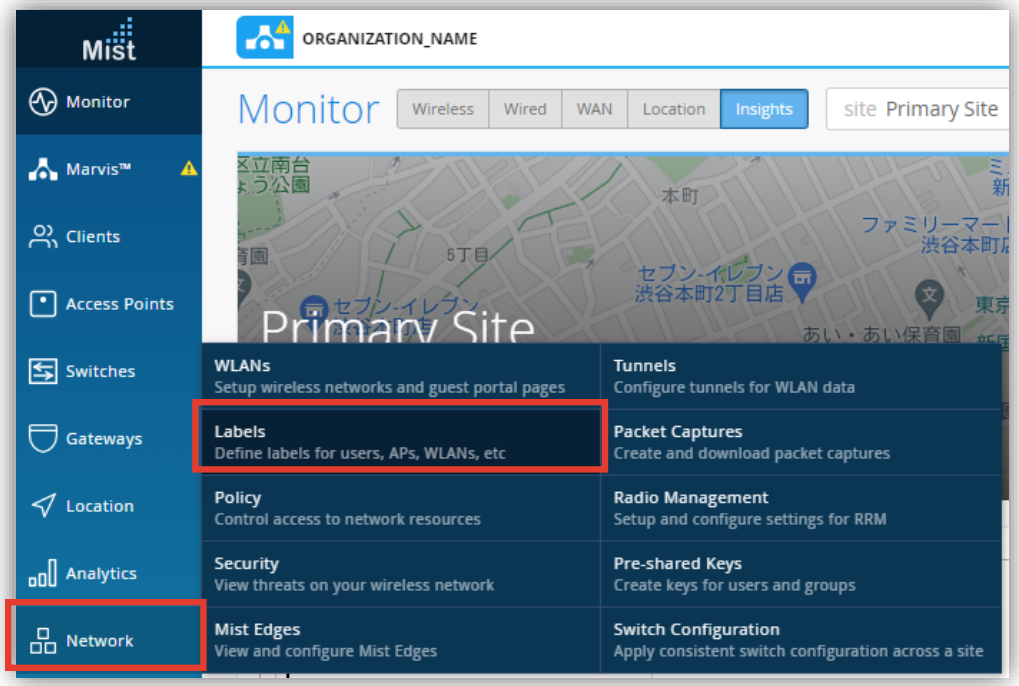


Label Type	Label Values	Policyへの設定
AAA Attribute	Radius Username（認証サーバに設定されたユーザー名）	User
WiFi Client	Wi-Fi クライアントの MAC アドレス	User
WLAN	作成済みの WLAN（SSID） 一覧から選択	User
Access Point	登録済みの AP 一覧から選択	User
IP Address	IP アドレス、またはレンジ（CIDR方式で入力）を指定	Resource
Hostname	URL で指定（例：xxx.org, xxx.com:8080）	Resource
Application	Mist で定義されているアプリケーション 一覧から選択	Resource
Port	TCP/UDP のポート番号	Resource
IP/Protocol/Port	IPアドレス、Protocol、Port を指定	Resource

※ WiFi Client Name, BLE Asset, App Client は Policy に適用不可

ラベルの作成

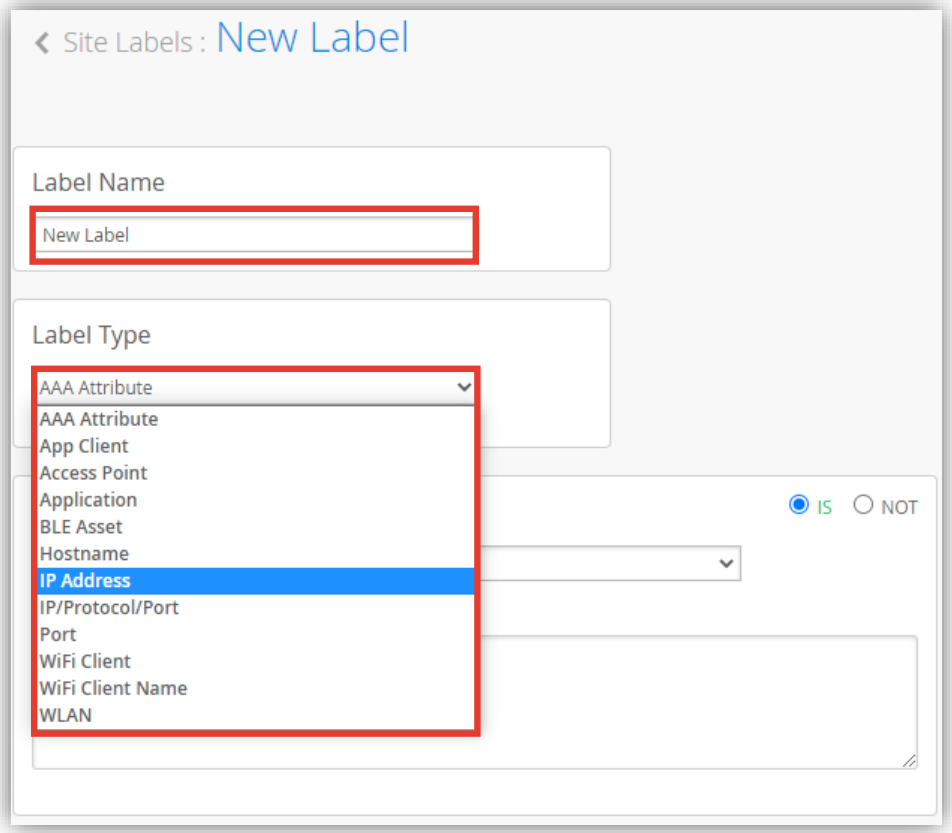
1．[Network] から [Labels] を選択します



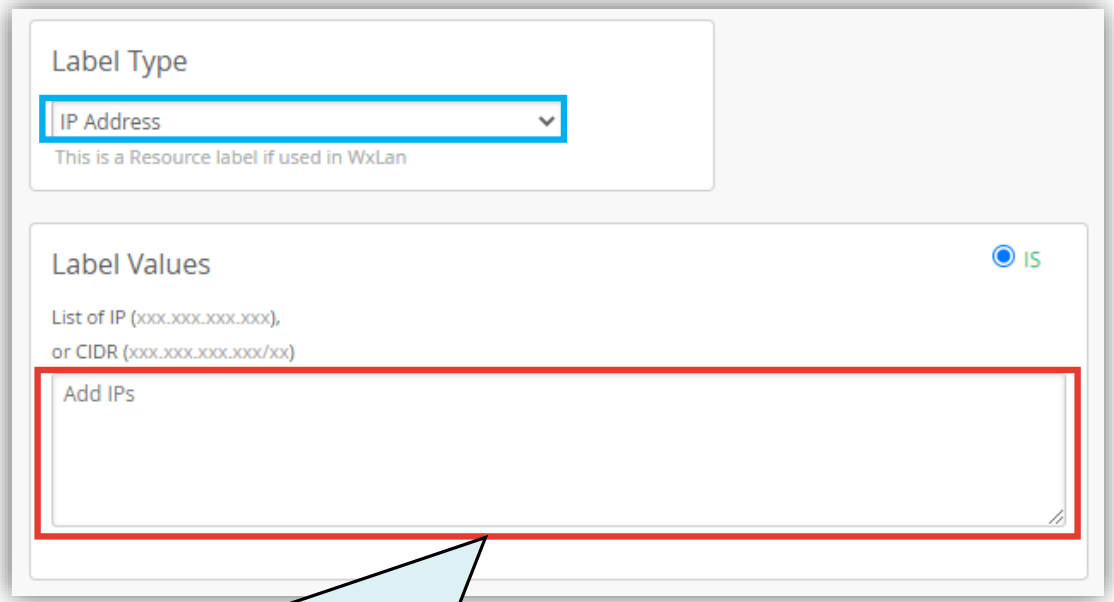
2．[Add Label] をクリックします

ラベルの作成

3. 任意の [Label Name] を入力し、
[Label Type] を選択します



4. [Label Values] を入力します
例) [Label Type] に [IP Address] を選択した場合



IP アドレスを登録
- コンマ区切りで複数登録
- CIDR の指定可能

WxLAN(アクセス制御ポリシー)の設定

0. 設定するポリシーに必要なラベルを作成します

詳細は、「Mist設定マニュアル ラベルの作成」を参照してください

ポリシー設定例

User	Resource	備考
WLANs	Youtube / Facebook	Youtube / Facebookへのアクセスをブロック
Guest	Private Address (RFC1918)	プライベートアドレスへの通信をブロック
All Users	All Resources	デフォルトポリシー(Last)で通信をブロック

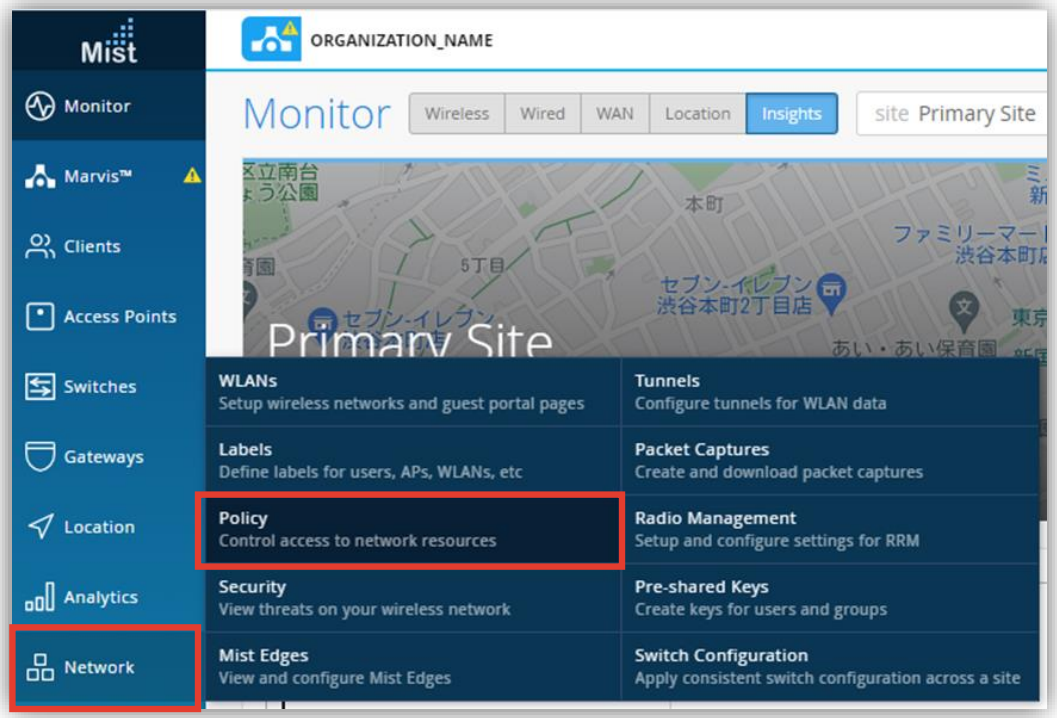
作成が必要なラベル

作成するラベル

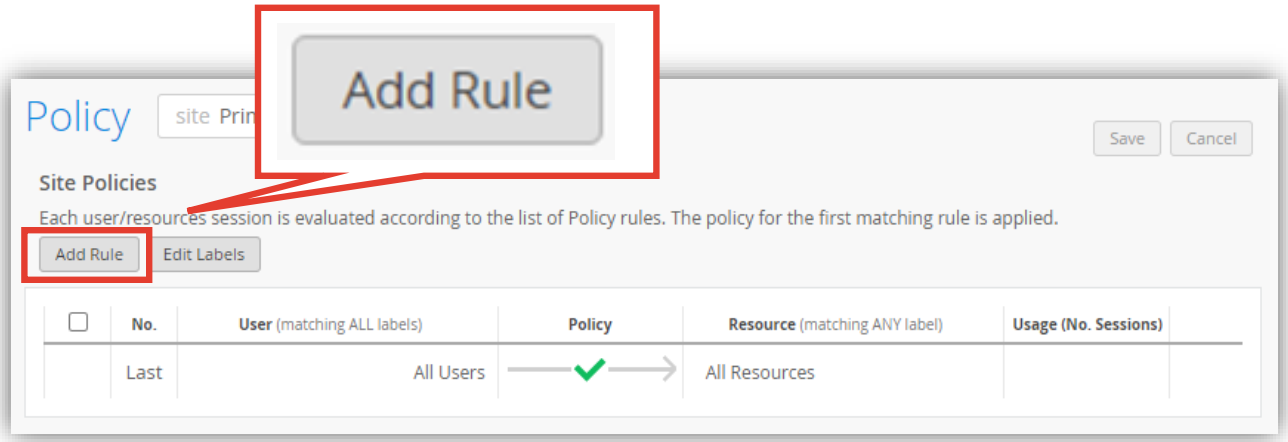
Name	Type	Values
Private Address (RFC1918)	IP Address	10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
WLANs	WLAN	WLAN_01,WLAN_02
Guest	WLAN	Guest

WxLAN(アクセス制御ポリシー)の設定

1．[Network] から [Policy] を選択します

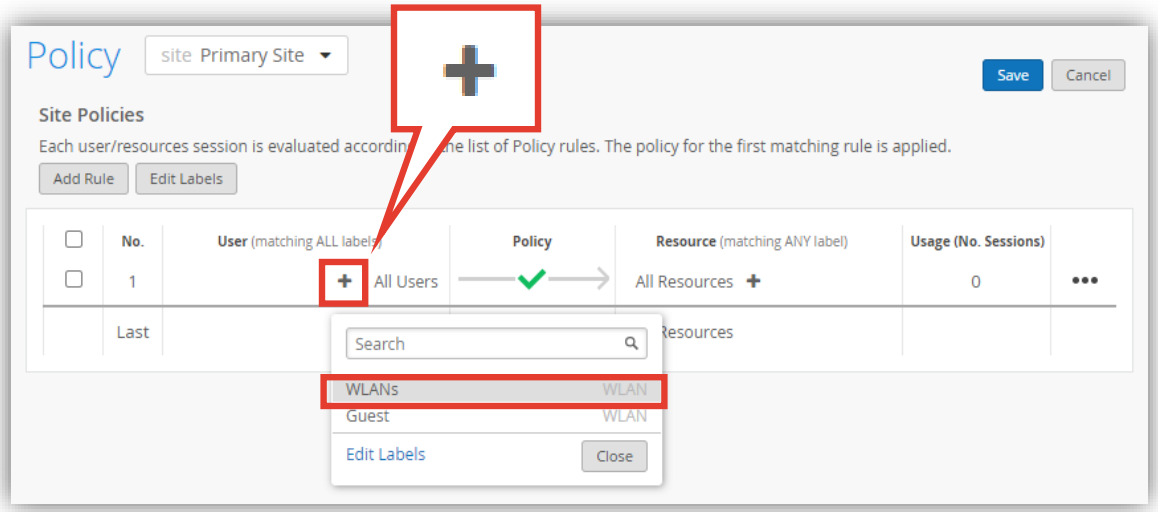


2．[Add Rule] をクリックします

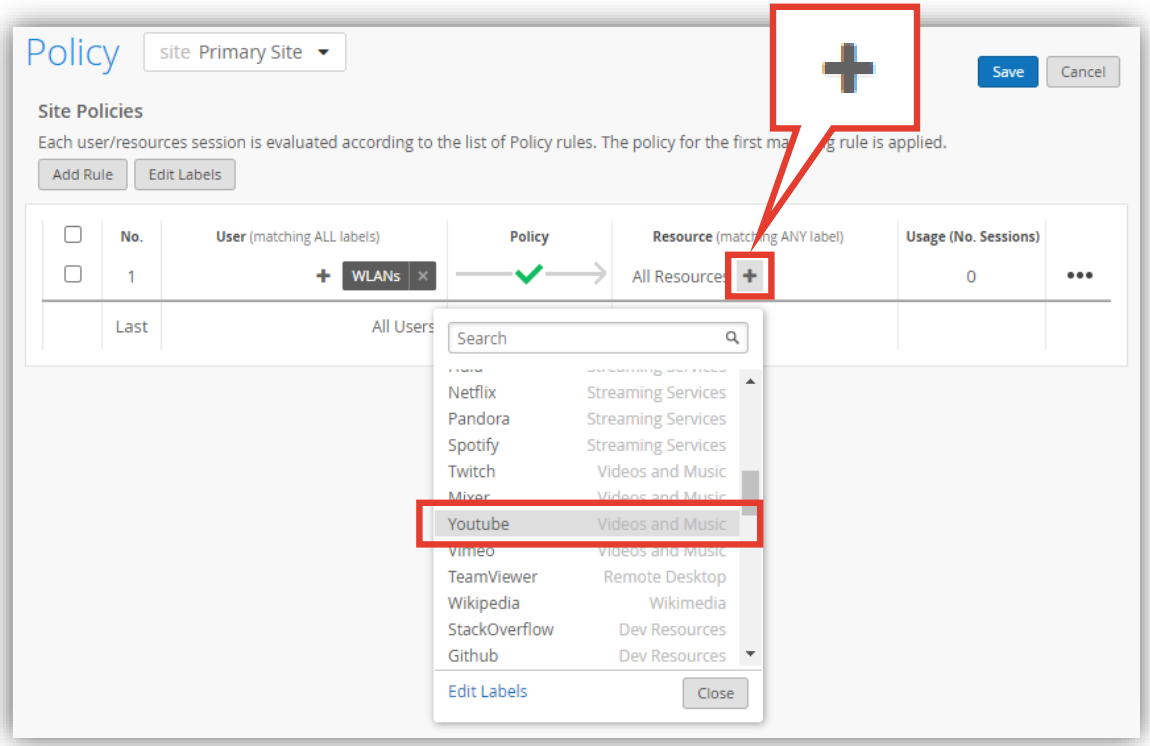


WxLAN(アクセス制御ポリシー)の設定

3. User のラベルを選択します
   [+] から WLANs を選択

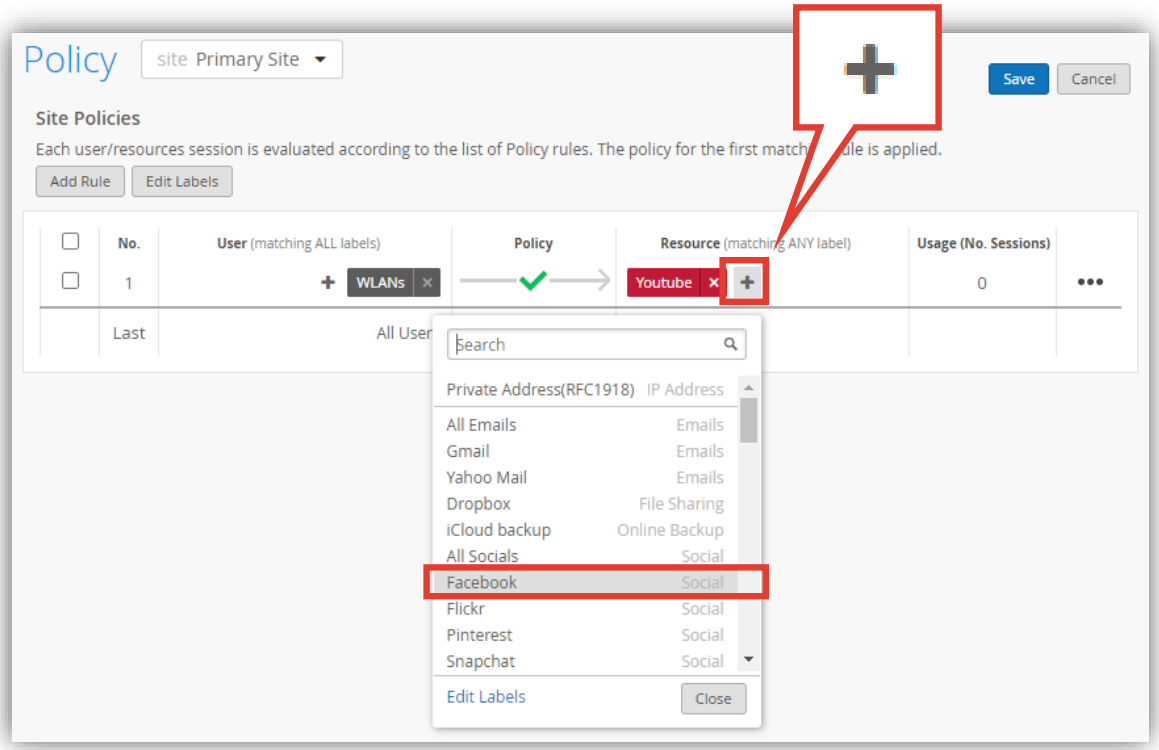


4. Resource のラベルを選択します
   [+] から Youtube を選択

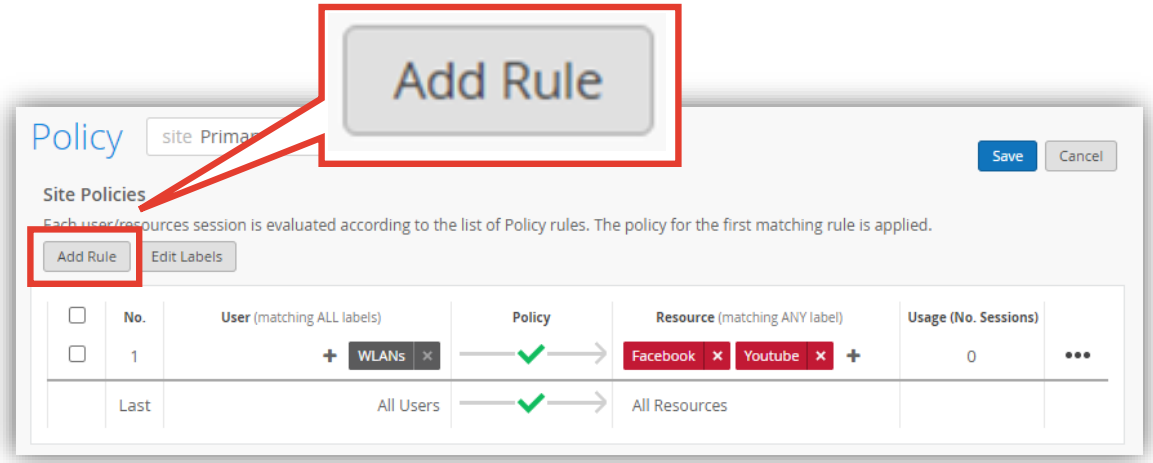


WxLAN(アクセス制御ポリシー)の設定

5. 同様に、Facebook を Resource に追加

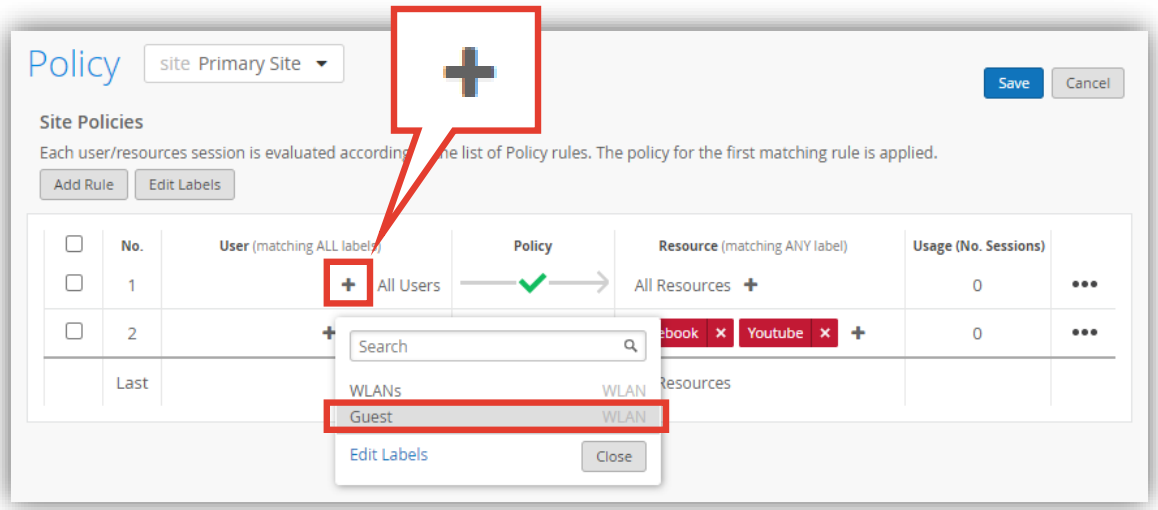


6. [Add Rule] でポリシーを追加します

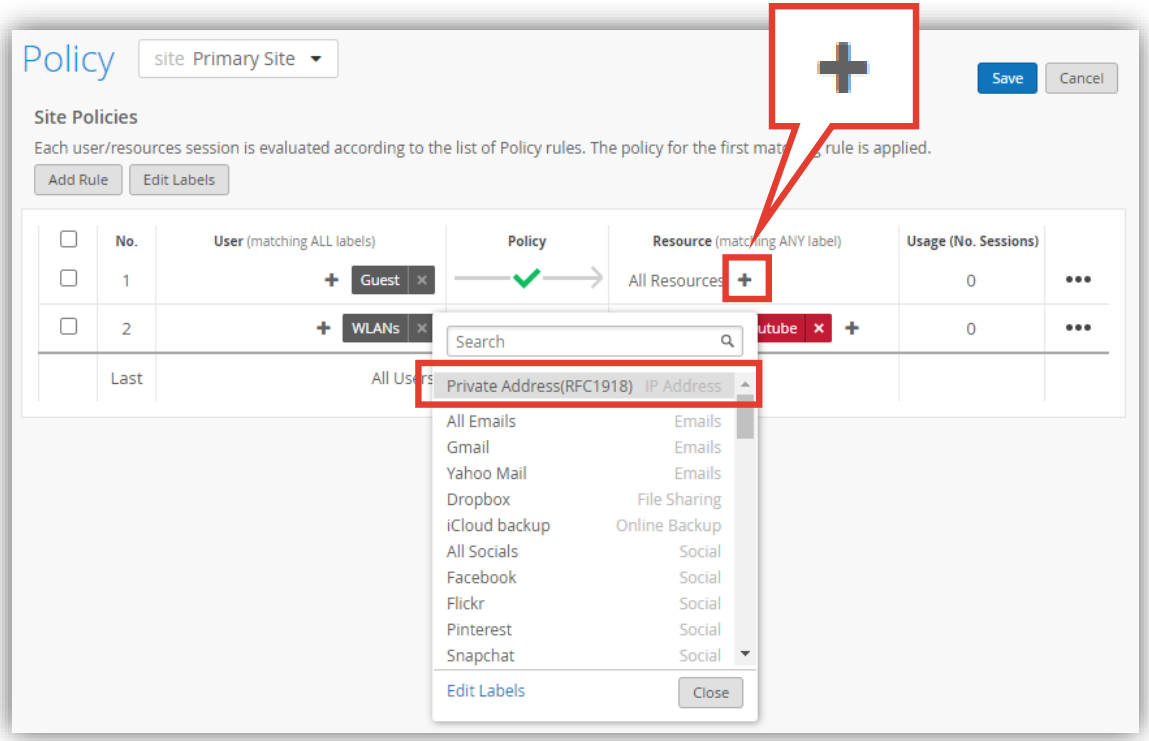


WxLAN(アクセス制御ポリシー)の設定

7. User のラベルを選択します
   [+] から Guest を選択

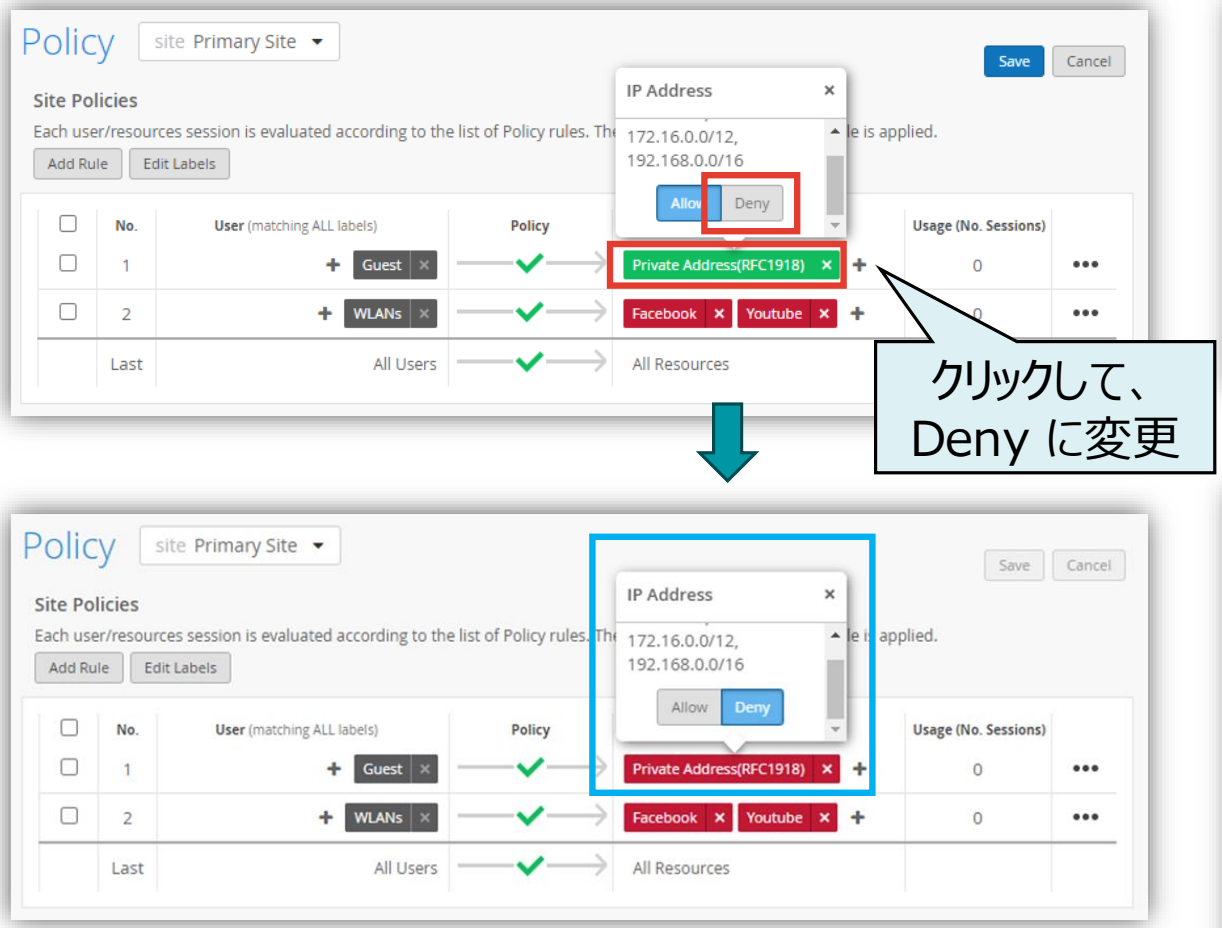


8. Resource のラベルを選択します
   [+] から Private Address(RFC1918) を選択

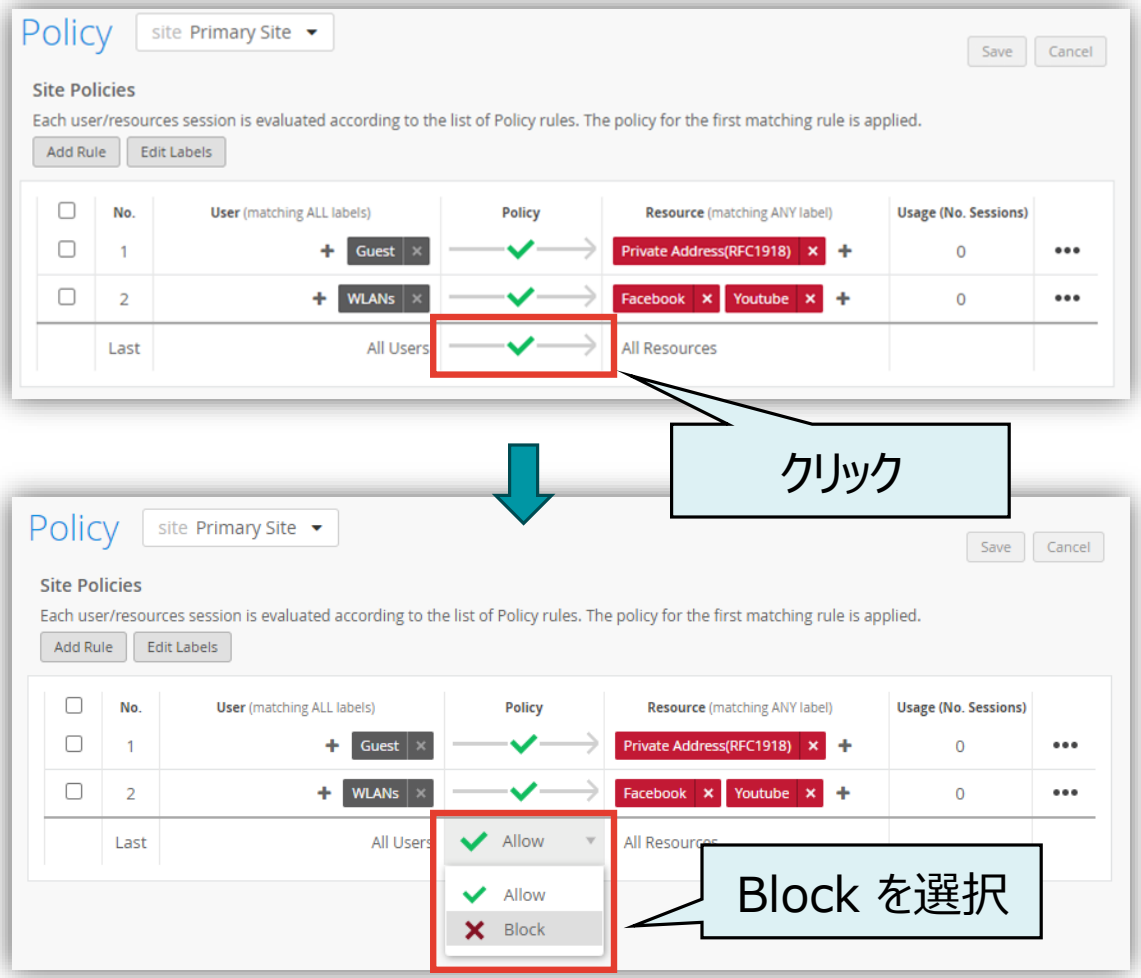


WxLAN(アクセス制御ポリシー)の設定

9. Resource のポリシーを Deny に変更します

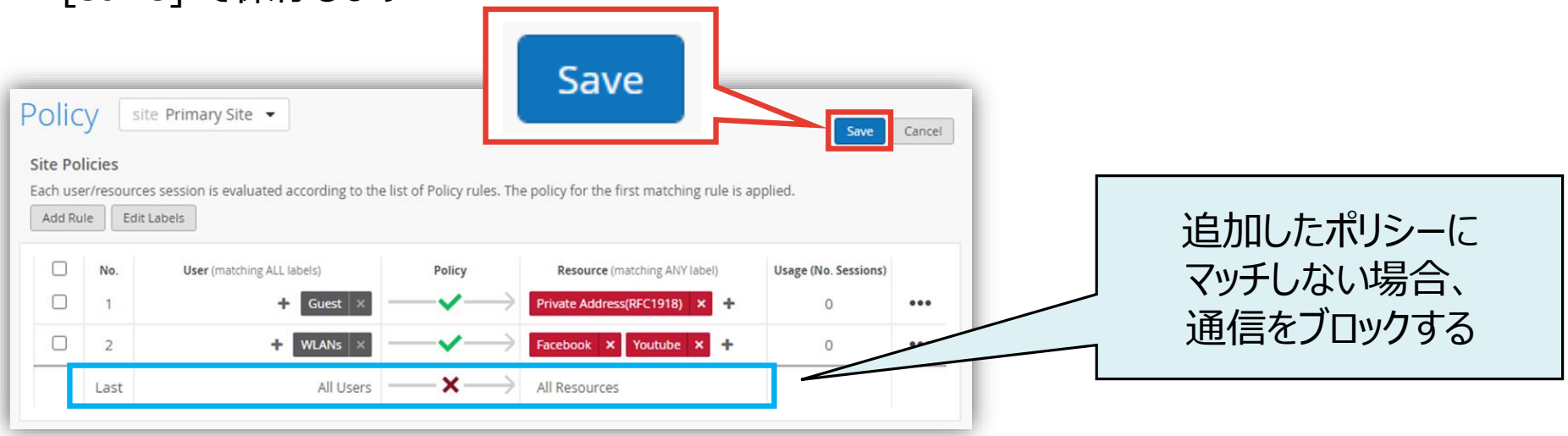


10.デフォルトポリシー(Last)を Block に変更します



WxLAN(アクセス制御ポリシー)の設定

11.[save] で保存します



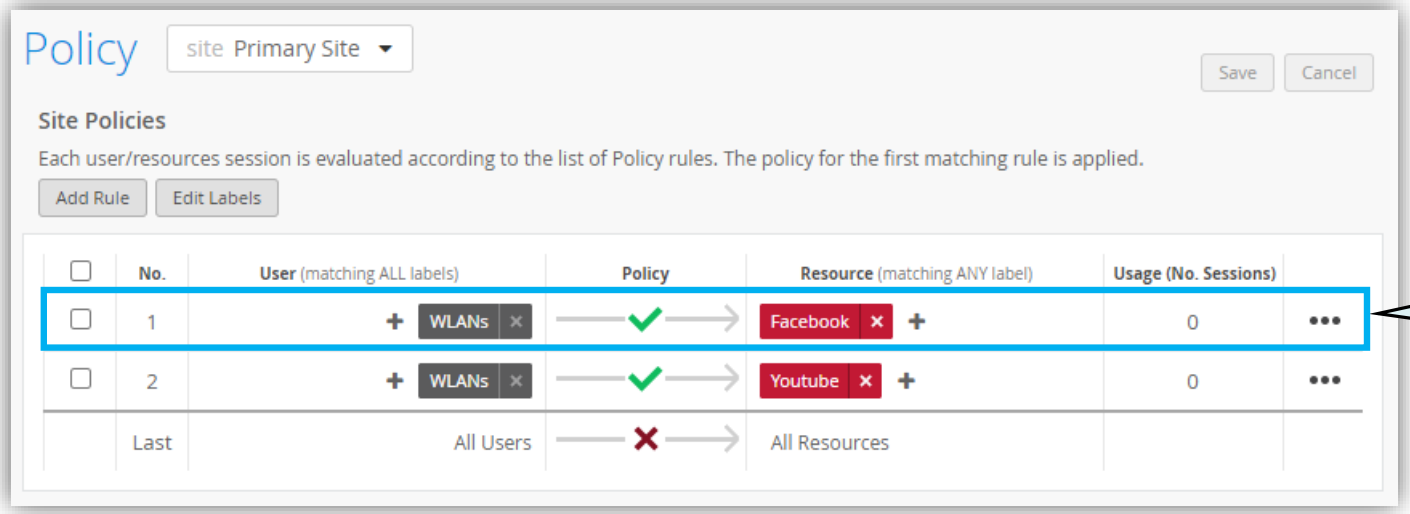
ポリシー設定例(再掲)

User	Resource	備考
WLANs	Youtube / Facebook	Youtube / Facebookへのアクセスをブロック
Guest	Private Address (RFC1918)	プライベートアドレスへの通信をブロック
All Users	All Resources	デフォルトポリシー(Last)で通信をブロック

WxLAN(アクセス制御ポリシー)の設定の注意点!!

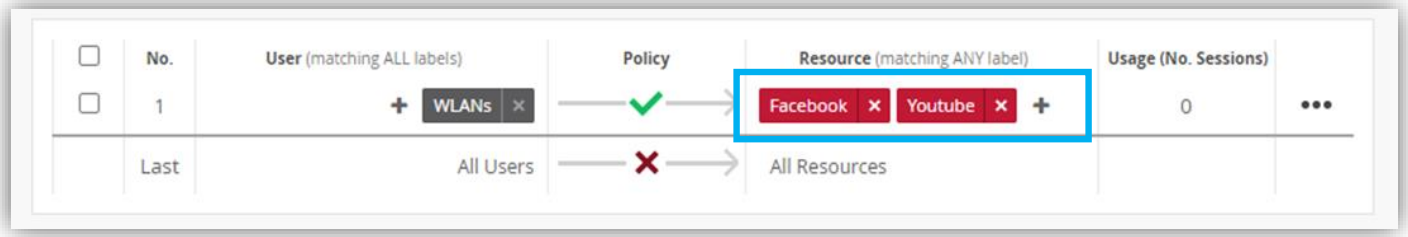
最初にマッチしたポリシーにより処理されます

下記のような場合、WLANs に対する **No.2 のポリシーは評価されず、**
WLANs は Youtube へのアクセスが可能です



First Match により
No.2は評価されない
→ WLANs は Youtube
へアクセスできる

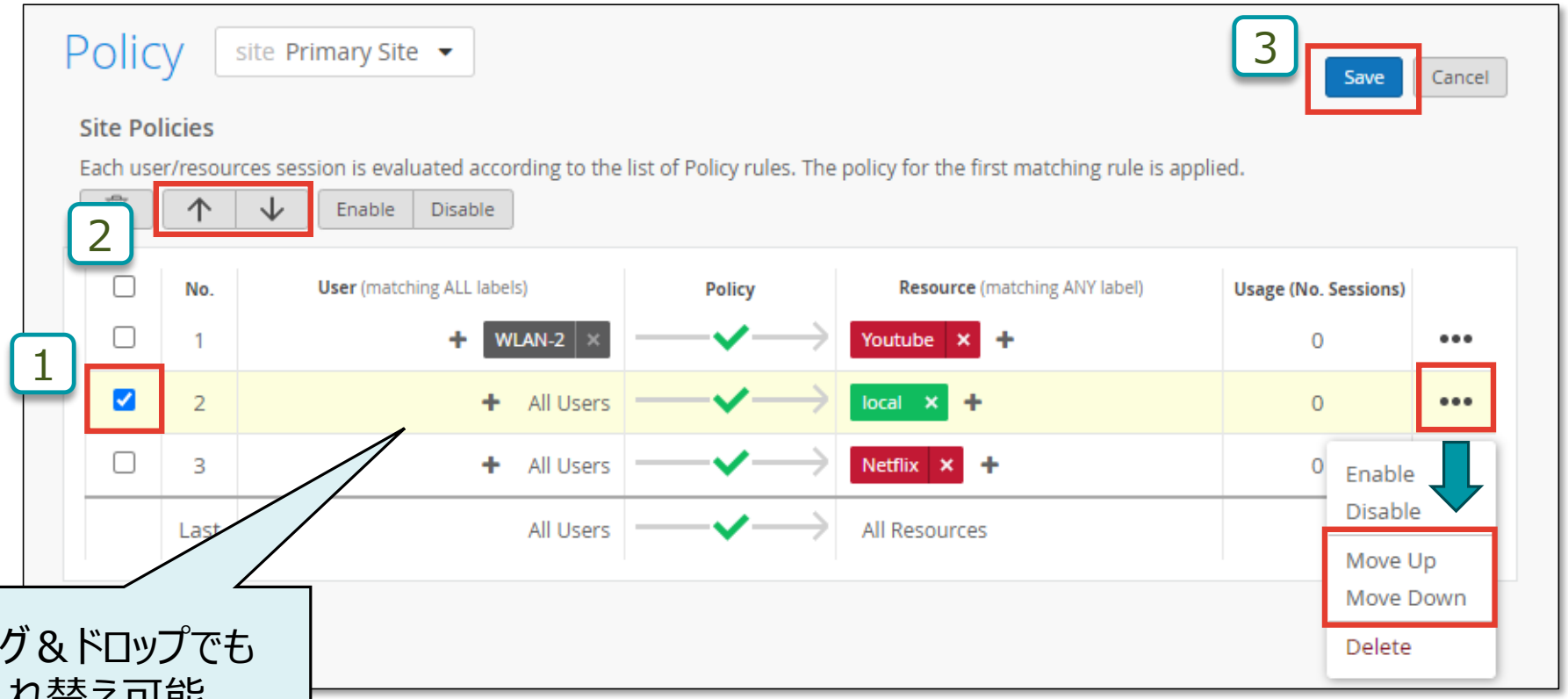
Facebook と Youtube 両方へのアクセスを制限する場合は、同一ポリシーの Resource に並べて設定します



ポリシーの順番の入れ替え

ポリシーの順番入れ替え

1. ポリシーを選択
2. 順番を入れ替え(Move Up/Move Down、または、↑ ↓ で移動)
3. Save をクリックして設定を保存



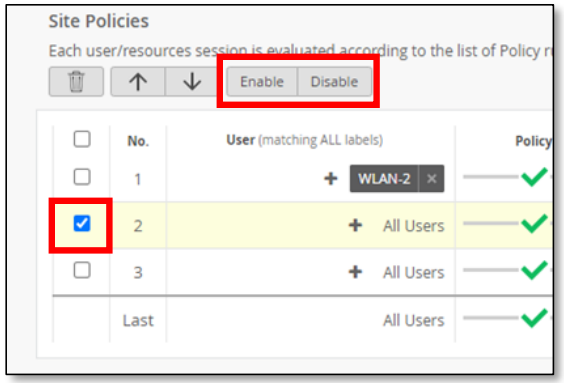
※ (・・・)からも入替可能。

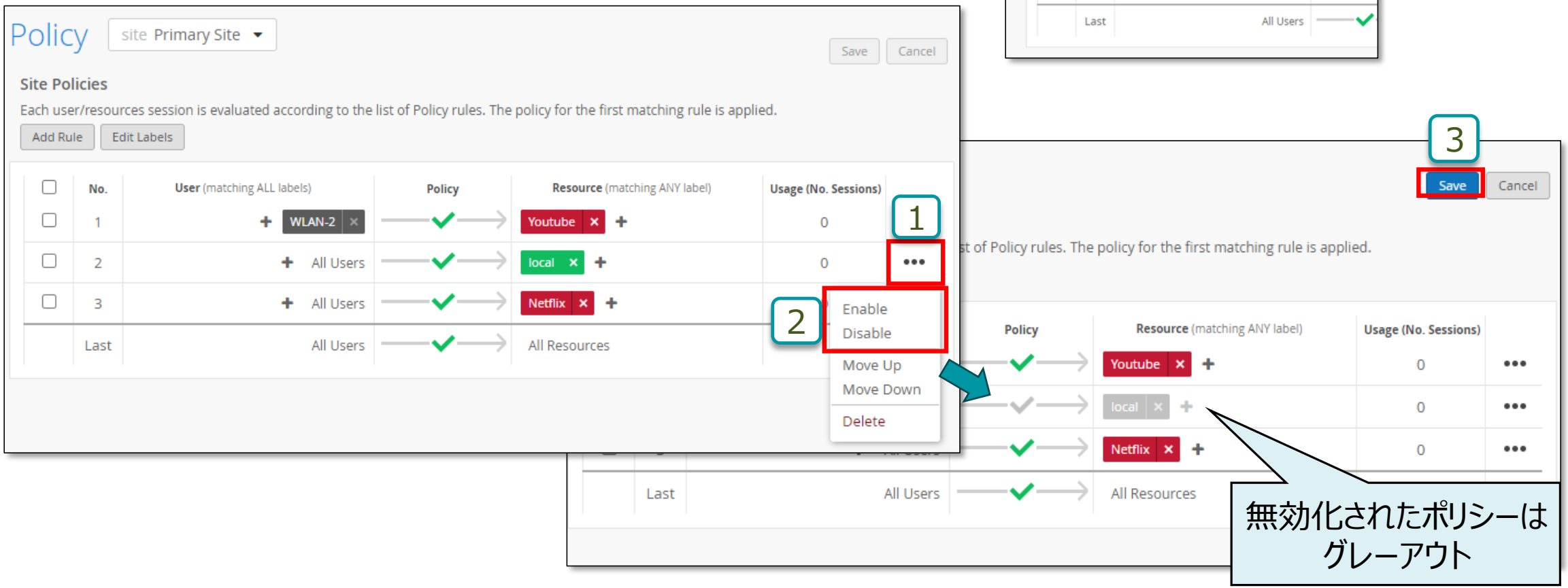
ポリシーの有効化・無効化

※ ポリシー選択、上部の Enable/Disable ボタンでも変更可能

ポリシーの有効化/無効化

1. Policy の右側の(・・・)をクリック
2. Enable/Disable を選択
3. Save をクリックして設定を保存

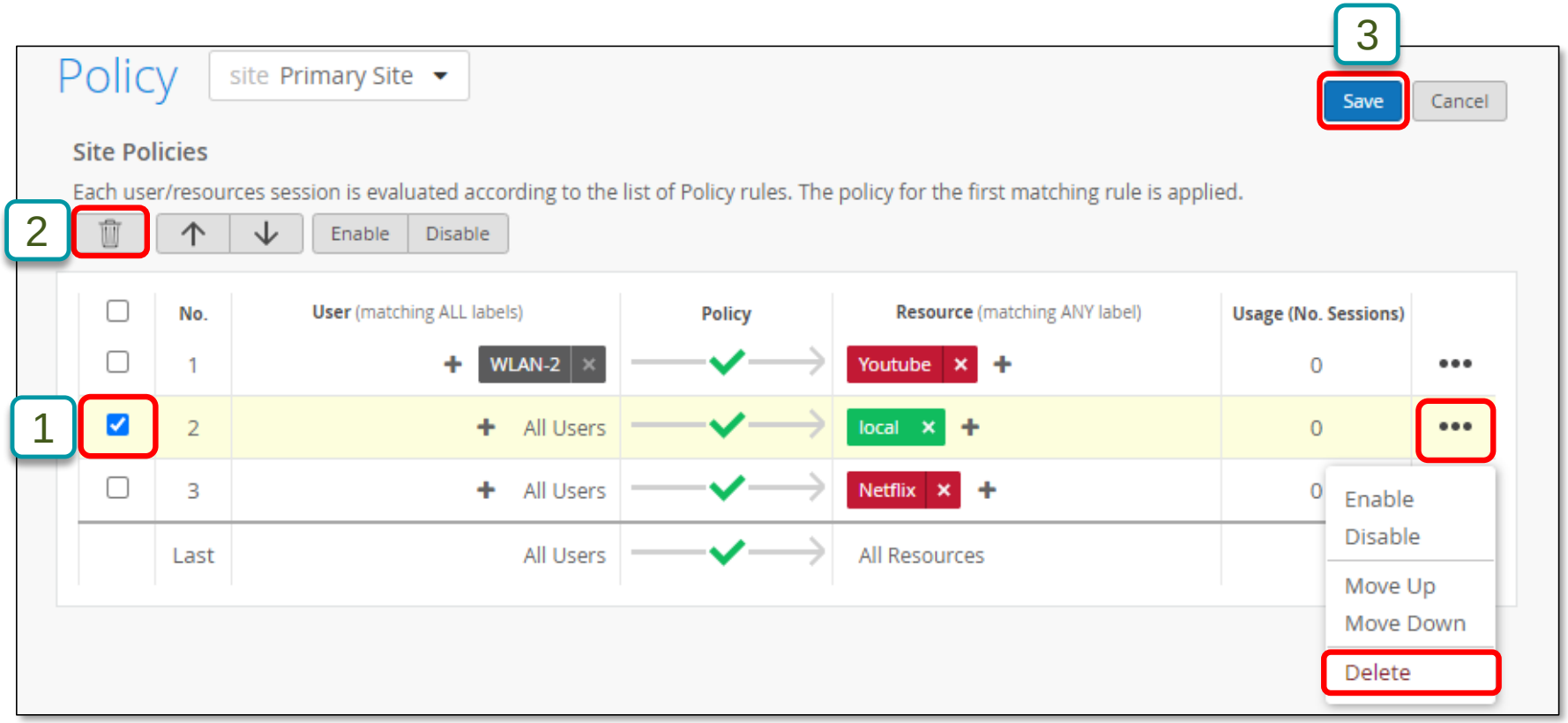




ポリシーの削除

ポリシーの削除

1. ポリシーを選択
2. ごみ箱アイコンをクリック
3. Save をクリックして設定を保存



※ (･･･)からも削除可能。