无线动态 vlan 分配配置方法

版本	1.0
时间	2014 年 4 月
支持的版本	FortiOS v5.0.4 及更高版本，FortiAP v 5.0.7 及更高版本
审核	已通过
反馈	support_cn@fortinet.com

目录

环境介绍

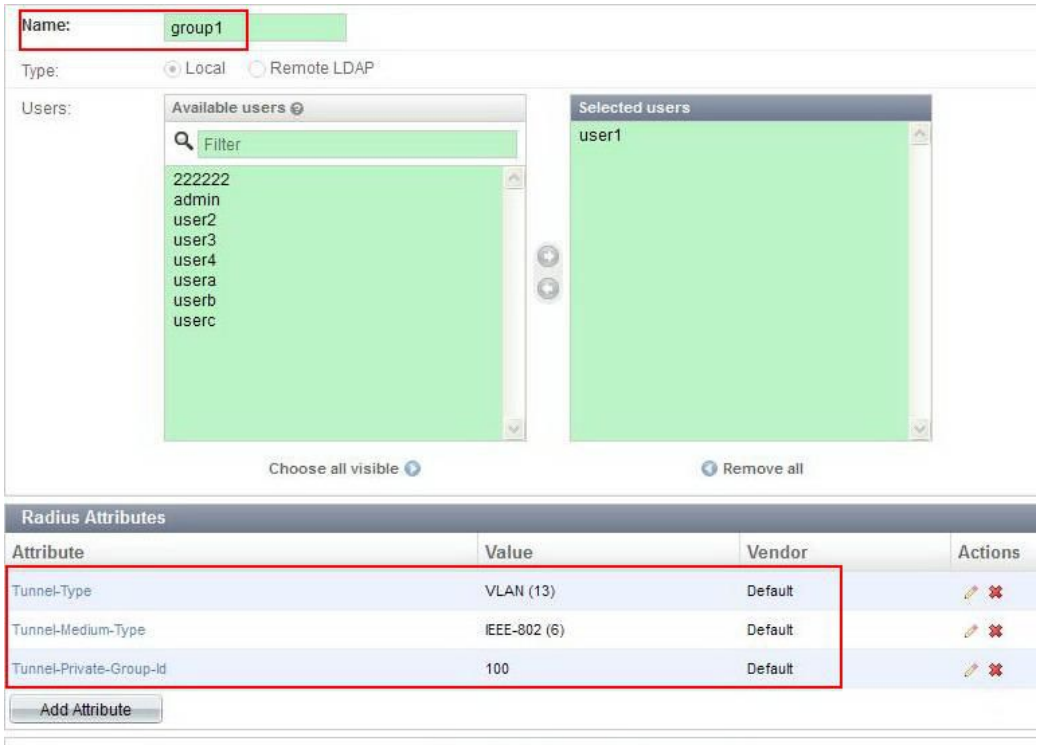
从 5.0.4 开始 FortiGate 支持动态 vlan 功能，它可以实现在同一个 SSID 内划分多个 vlan 的功能。例如，

用户组	vlan id
group1	100
group2	200
…	…

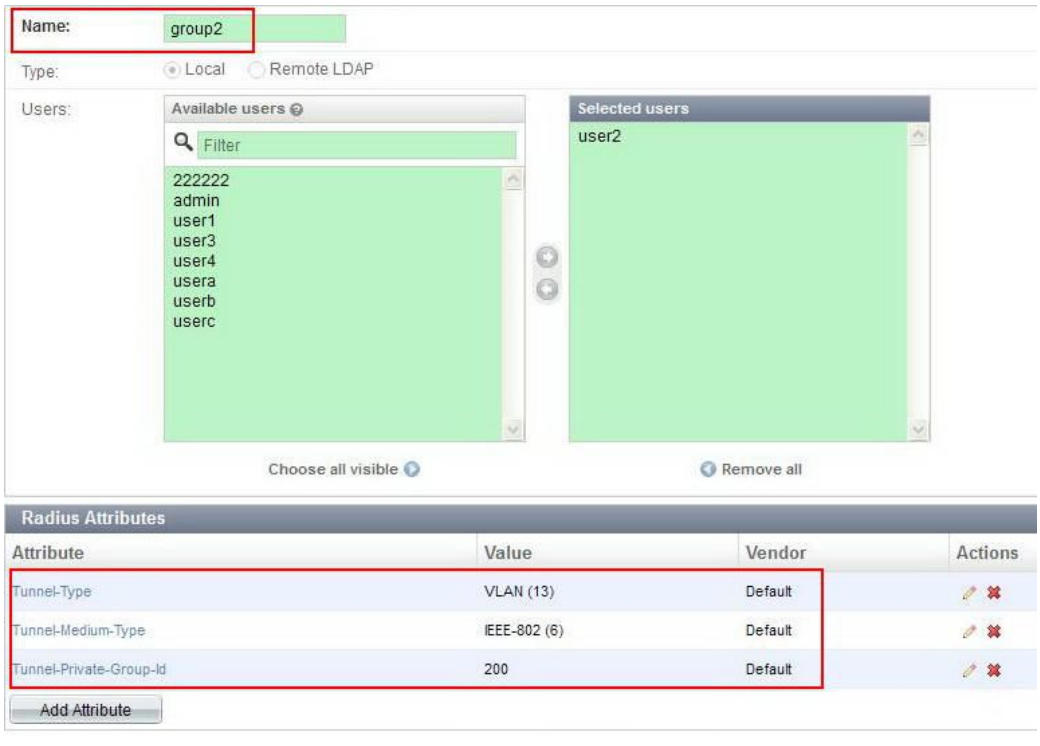
要实现该需求之前的做法需要两个 SSID（或更多），使用动态 vlan 只需要一个 SSID 即可完成。它的原理是使用 radius 认证，给每个用户组在 radius 上分配不同的 vlan 属性。认证后 radius 将用户组的 vlan 属性传递给 AC， AC 再告知 AP 该用户所在的 vlan。
Radius 上需要配置的 vlan 属性公有三个
IETF64 (TunnelType)——VLAN
IETF65 (Tunnel Medium Type)——802
IETF81 (Tunnel Private Group ID)——VLAN ID（填写具体 ID 号）
本例使用 FAC 作为 radius 认证服务器。版本是 v3.0 bulid007

步骤一：FAC 配置 RADIUS 用户组属性

登录到 FAC web 管理页面，在菜单 Authentication—>User Management—>User Groups 中添加 vlan 属性，如下图，



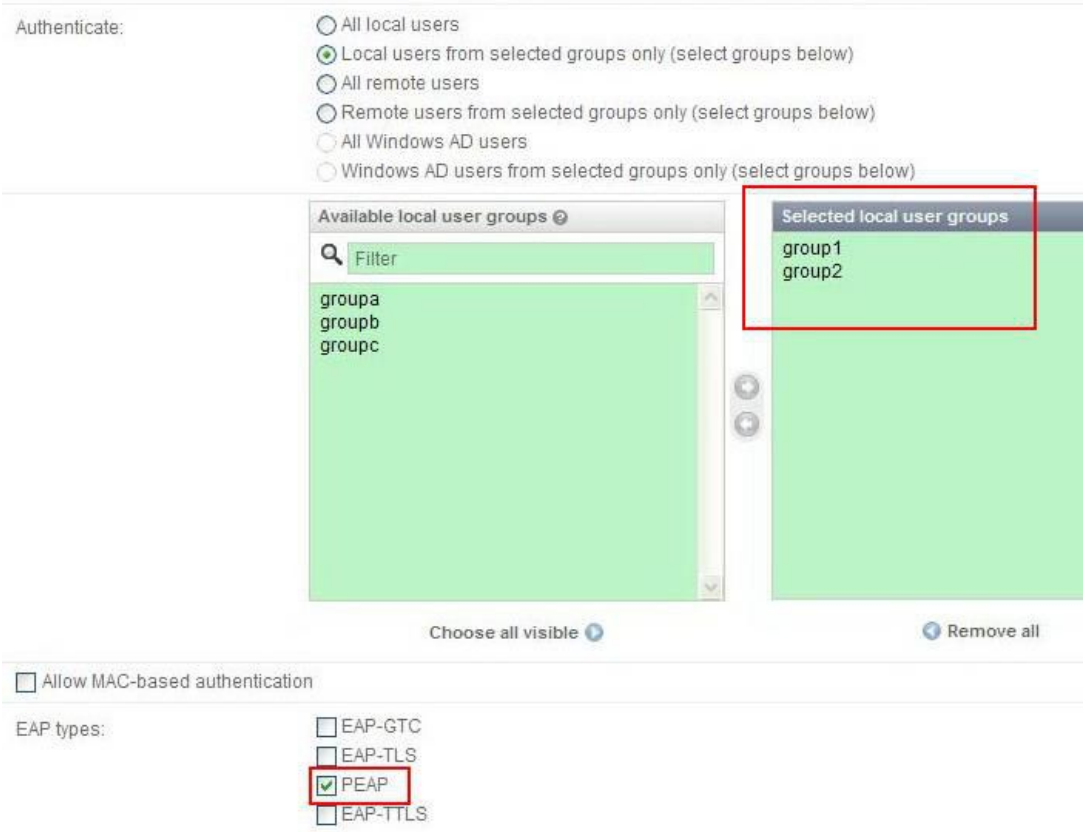
group1 对应的 vlan ID 是 100



group2 对应的 vlan ID 是 200

步骤二：FAC 配置 RADIUS 服务器

在 Authentication—>RADIUS Service—>Clients 菜单中新建客户端，如下图



注意选择 PEAP 认证方法

步骤三：FGT 配置 RADIUS 服务器

登录到 FGT 在菜单 用户&设备—>认证—>RADIUS 中创建服务器，如下图

步骤四：FGT 配置 AP 属性

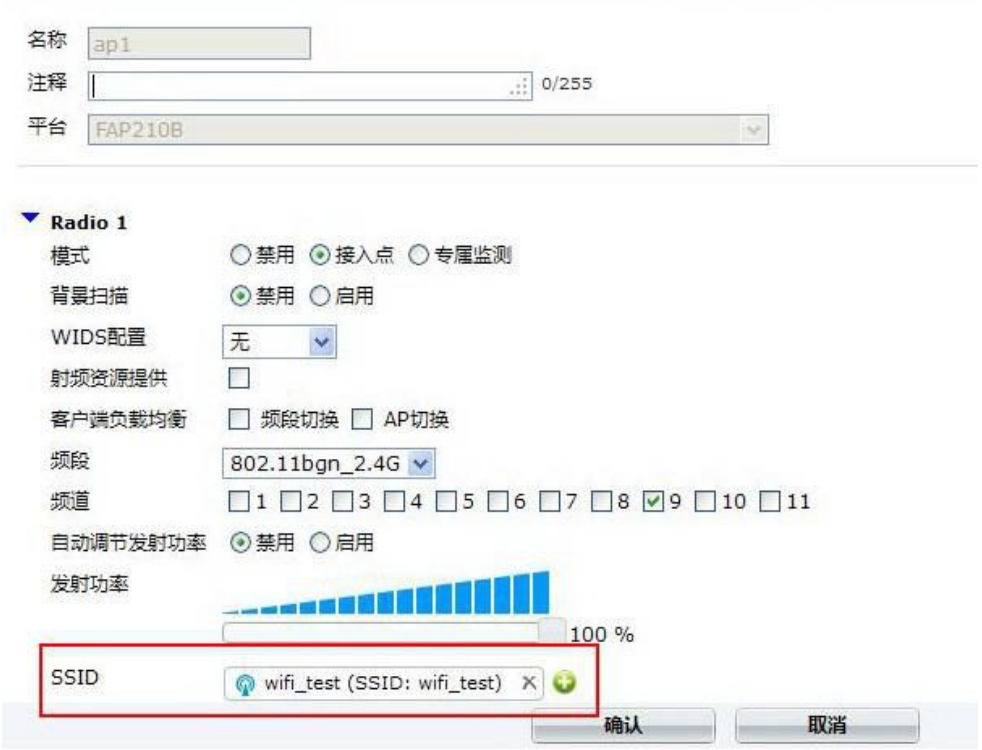
在 WiFi 与交换控制器—>无线网络—>SSID 菜单中创建新的 SSID，如下图

注意选择步骤三中的 RADIUS 服务器

在 CLI 中启用动态 vlan，如下图

```
config wireless-controller vap
    edit "wifi_test"
        set vdom "root"
        set ssid "wifi_test"
        set security wpa-enterprise
        set auth radius
        set radius-server "fac"
        set dynamic-vlan enable
    next
end
```

在 WiFi 与交换控制器—>无线网络—>自定义 AP 配置菜单中创建新配置，如下图



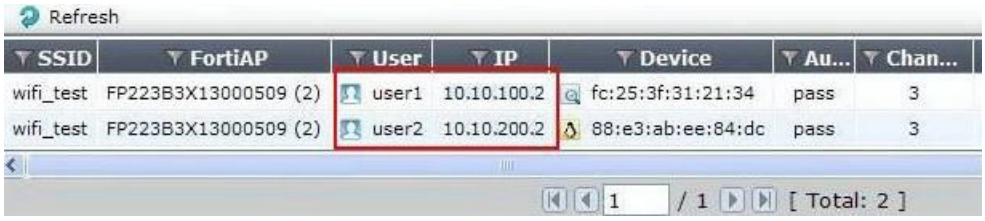
步骤五：FGT 配置 vlan 接口

在系统管理—>网络—>接口菜单中新建 vlan 接口，如下图

注意接口要选择对应的无线接口名称，这里的 vlan ID 要和步骤一中 FAC 配置的用户组属性 vlan ID 保持一致

步骤六：FG 查看连接到 AP 的用户

在 WiFi 与交换控制器—>监视器—>客户端检测菜单中查看连接的客户端，如下图



在日志与报告—>事件日志—>WiFi 菜单中查看相关日志，如下图