

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.....	3
步骤一：FAC 配置 RADIUS 用户组属性.....	3
步骤二：FAC 配置 RADIUS 服务器.....	5
步骤三：FGT 配置 RADIUS 服务器.....	5
步骤四：FGT 配置 AP 属性.....	6
步骤五：FGT 配置 vlan 接口.....	7
步骤六：FG 查看连接到 AP 的用户.....	8

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 属性共有三个

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，

Name:

Type: Local Remote LDAP

Users:

Available users

Filter

- 222222
- admin
- user2
- user3
- user4
- usera
- userb
- userc

Choose all visible

Selected users

- user1

Remove all

Radius Attributes

Attribute	Value	Vendor	Actions
Tunnel-Type	VLAN (13)	Default	
Tunnel-Medium-Type	IEEE-802 (6)	Default	
Tunnel-Private-Group-Id	100	Default	

Add Attribute

group1 对应的 vlan ID 是 100

Name:

Type: Local Remote LDAP

Users:

Available users

Filter

- 222222
- admin
- user1
- user3
- user4
- usera
- userb
- userc

Choose all visible

Selected users

- user2

Remove all

Radius Attributes

Attribute	Value	Vendor	Actions
Tunnel-Type	VLAN (13)	Default	
Tunnel-Medium-Type	IEEE-802 (6)	Default	
Tunnel-Private-Group-Id	200	Default	

Add Attribute

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

Authenticate:

- All local users
- Local users from selected groups only (select groups below)
- All remote users
- Remote users from selected groups only (select groups below)
- All Windows AD users
- Windows AD users from selected groups only (select groups below)

Available local user groups

Filter

groupa
groupb
groupc

Selected local user groups

group1
group2

Choose all visible Remove all

Allow MAC-based authentication

EAP types:

- EAP-GTC
- EAP-TLS
- PEAP
- EAP-TTLS

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

编辑RADIUS服务器

名称 fac

主服务器名称/IP 10.20.1.3

主服务器密钥 测试

从服务器名称/IP

从服务器密钥 测试

验证方案

- 用户默认验证方案
- 指定验证协议

PAP

NAS IP/呼叫站点ID

包含进所有用户组 启用

确认 取消

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

编辑接口

接口名称: wifi_test
类型: WiFi SSID
流量模式: 通过隧道连接至无线控制器

IP地址/网络掩码: 10.10.60.1/255.255.255.0

管理访问: HTTPS PING HTTP FMG-访问
 SSH SNMP TELNET FCT-访问

DHCP Server: 启用

地址范围:

起始IP	终止IP
10.10.60.2	10.10.60.254

掩码: 255.255.255.0

缺省网关: 与接口IP相同 Specify 设定

DNS服务器: 与系统DNS相同 Specify 设定

高级...

无线设置

SSID: wifi_test
安全模式: WPA/WPA2-Enterprise
数据加密: AES TKIP TKIP-AES
认证: RADIUS服务器 用户组
fac
屏蔽SSID内部流量:

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

名称

注释 0/255

平台

Radio 1

模式 禁用 接入点 专属监测

背景扫描 禁用 启用

WIDS配置

射频资源提供

客户端负载均衡 频段切换 AP切换

频段

频道 1 2 3 4 5 6 7 8 9 10 11

自动调节发射功率 禁用 启用

发射功率

SSID

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

编辑接口

接口名称

类型

接口

VLAN ID

地址模式 自定义 DHCP PPPoE

IP地址/网络掩码

管理访问 HTTPS PING HTTP FMG-访问 CAPWAP
 SSH SNMP TELNET FCT-访问

DHCP Server 启用

地址范围

起始IP	终止IP
10.10.100.2	10.10.100.254

掩码

缺省网关 与接口IP相同 Specify 设定

DNS服务器 与系统DNS相同 Specify 设定

高级...

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

编辑接口

接口名称	vlan200
类型	VLAN
接口	wifi_test
VLAN ID	200

地址模式 自定义 DHCP PPPoE

IP地址/网络掩码

管理访问 HTTPS PING HTTP FMG-访问 CAPWAP
 SSH SNMP TELNET FCT-访问

DHCP Server 启用

地址范围

+ Create New <input type="button" value="Edit"/> <input type="button" value="Delete"/>	
起始IP	终止IP
10.10.200.2	10.10.200.254

掩码

缺省网关 与接口IP相同 Specify 设定

DNS服务器 与系统DNS相同 Specify 设定

[高级...](#)

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

SSID	FortiAP	User	IP	Device	Au...	Chan...
wifi_test	FP223B3X13000509 (2)	user1	10.10.100.2	fc:25:3f:31:21:34	pass	3
wifi_test	FP223B3X13000509 (2)	user2	10.10.200.2	88:e3:ab:ee:84:dc	pass	3

/ 1

在日志与报告—>事件日志—>WiFi 菜单中查看相关日志，如下图

Refresh Download Raw Log Log loca

#	Date/Time	Level	Action	Message	SSID
1	11:01:12	notice	client-ip-detected	Client fc:25:3f:31:21:34 assigned an IP address.	wifi_test
2	11:01:10	notice	client-authentication	Client fc:25:3f:31:21:34 authenticated.	wifi_test

1 / 2 [Total: 74]

Action	client-ip-detected	Band	802.11n
Channel	3	Date/Time	11:01:12 (1395399672)
Group	r1	IP Address	10.10.100.2
Level	notice	Log ID	43524
MAC	fc:25:3f:31:21:34	Message	Client fc:25:3f:31:21:34 assigned an IP
Physical AP	N/A	Reason	N/A
SSID	wifi_test	Security	wpa2-auto
Serial Number	FP223B3X13000509	Sub Type	wireless
Timestamp	2014年3月21日 11:01:12	User	user1
Virtual AP	wifi_test	Virtual Domain	root

Refresh Download Raw Log Log loca

#	Date/Time	Level	Action	Message	SSID
1	11:03:23	notice	client-ip-detected	Client 88:e3:ab:ee:84:dc assigned an IP address.	wifi_test
2	11:03:21	notice	client-authentication	Client 88:e3:ab:ee:84:dc authenticated.	wifi_test

1 / 2 [Total: 77]

Action	client-ip-detected	Band	802.11n
Channel	3	Date/Time	11:03:23 (1395399803)
Group	r1	IP Address	10.10.200.2
Level	notice	Log ID	43524
MAC	88:e3:ab:ee:84:dc	Message	Client 88:e3:ab:ee:84:dc assigned an IP
Physical AP	N/A	Reason	N/A
SSID	wifi_test	Security	wpa2-auto
Serial Number	FP223B3X13000509	Sub Type	wireless
Timestamp	2014年3月21日 11:03:23	User	user2
Virtual AP	wifi_test	Virtual Domain	root