

无线网络桥接有线网络

版本	1.0
时间	2014 年 9 月
支持的版本	FortiOS 5.0
作者	彭俊
状态	已审核
反馈	support_cn@fortinet.com

涉及平台

Fortigate 5.0/5.2

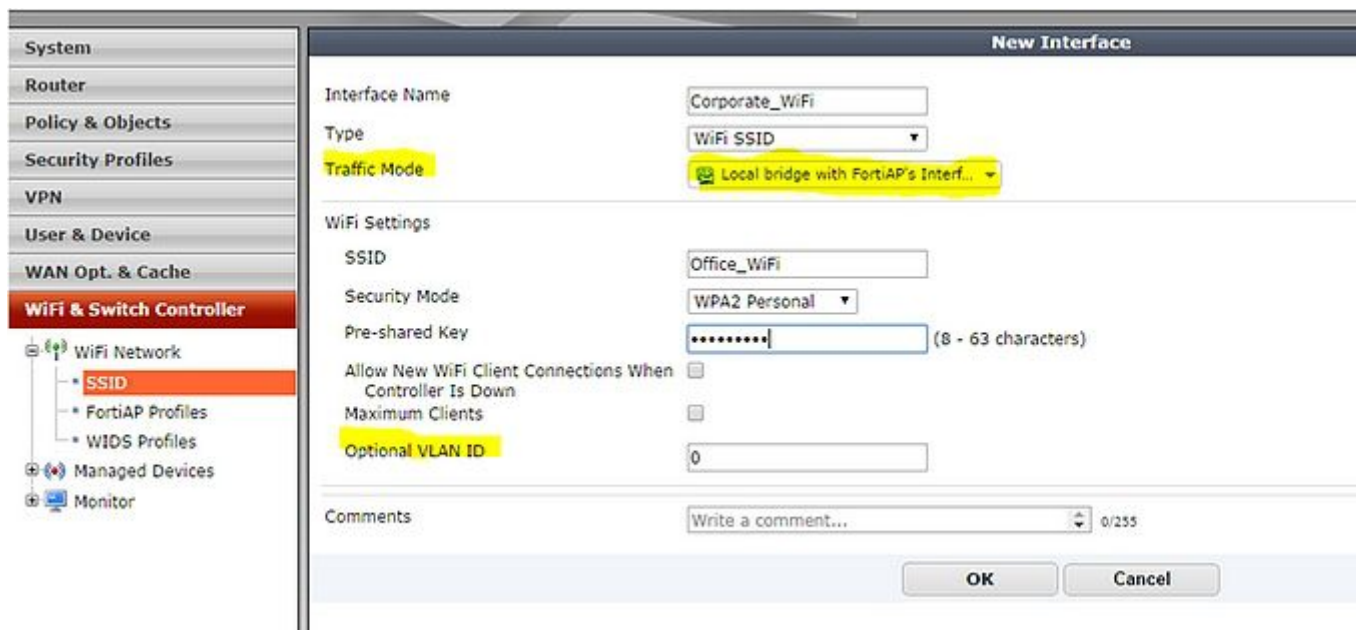
描述

该文档将介绍如何配置 fortigate，使得无线网络桥接入已存在的有线网络

步骤

桥接无线网络和有线网络需先创建 SSID，使得流量经由 FORTIAP 的接口至 FORTIGATE 防火墙，从而取代无线控制器

- 1.) 按需进入以下目录 WiFi Controller > WiFi Network > SSID 点击 创建新的。
- 2.) 使用以下流量模式 “Local bridge with FortiAP’s Interface”，配置 SSID。



- 3.) 进入以下目录 WiFi Controller > FortiAP profiles > 修改 FortiAP profile 并应用至对应的 SSID 下 a

同时可在 cli 界面下使用以下命令配置.

该例子为穿件了一个“Corporate_WiFi” , SSID 为“Office_WiFi” 使用 WPA 加密, 密钥为“Fortinet1”.

```
config                                wireless-controller                                vap
edit                                  Corporate_WiFi
set                                   vdom                                                  "root"
set                                   ssid                                                  "Office_WiFi"
set                                   local-bridging                                       enable
set                                   passphrase                                           Fortinet1
end

config                                wireless-controller                                wtp-profile
edit                                  FAP221C-default
config                                radio-1
set                                   vaps                                                  Corporate_WiFi
end
config                                radio-2
set                                   vaps                                                  Corporate_WiFi
end
end
```

在网络中使用 MAC 地址过滤会比使用 IP 地址过滤更安全和可靠, 因为 MAC 不会改变。

在无线环境中我们可以使用配置 access list 来禁止指定客户端的接入。

Step 1) 定义指定 mac 地址对象 :

```
config user device
edit mac-1
set mac 11:11:11:11:11:11 {---the MAC address you need filter
next
end
```

Step 2) 配置 devices access list:

```
config user device-access-list
edit Black-list
set default-action accept {---- This is set to allow all except the one in the list
config device-list
edit 1
set device "mac-1"
set action deny
next
end
next
end
```

Step 3) 在 开 启 了 wireless 的 接 口 下 调 用 access list:

```
config system interface
edit [name]
set device-identification enable
set device-access-list Black-list
next
end
```

在 fortigate 防火墙上开启相关功能

```
config user radius
edit [name]
config accounting-server
edit 1
set status enable
set server [IP]
set secret [secret]
end
set acct-interim-interval [duration] duration between each interim update[600 to 86400
seconds]
end
```

注意：radius server 需开启以下参数 “Acct-Interim-Interval=xxx” (seconds)

Example configuration on Windows NPS server:

Fortigate_Domain_Admins Properties

Overview | Conditions | Constraints | Settings

Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- Standard
- Vendor Specific
- Network Access Protection
- NAP Enforcement
- Extended State
- Routing and Remote Access
- Multilink and Bandwidth Allocation Protocol (BAP)

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Value
Acct-Interim-Interval	600

Buttons: Add, Edit, Remove

Buttons: OK, Cancel, Apply

Fortigate_Domain_Admins

Conditions - If the following conditions are met:

Condition	Value
User Groups	VISWA\Domain Users
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 0

Settings - Then the following settings are applied:

Setting	Value
Access Permission	Grant Access
Authentication Method	Unencrypted authentication (PAP, SPAP) OR Er
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Vendor-Specific	Domain Users
Acct-Interim-Interval	600

2	0.059067	0.059067	192.168.1.26	192.168.1.20	RADIUS	283	Access-Accept(2) (id=4, l=241)
3	0.061263	0.002196	192.168.1.20	192.168.1.26	RADIUS	183	Accounting-Request(4) (id=5, l=141)
4	0.061594	0.000331	192.168.1.26	192.168.1.20	RADIUS	62	Accounting-Response(5) (id=5, l=20)
5	605.600827	605.539233	192.168.1.20	192.168.1.26	RADIUS	201	Accounting-Request(4) (id=6, l=159)
6	605.601794	0.000967	192.168.1.26	192.168.1.20	RADIUS	62	Accounting-Response(5) (id=6, l=20)

```

Frame 2: 283 bytes on wire (2264 bits), 283 bytes captured (2264 bits)
Ethernet II, Src: Vmware_8e:17:5e (00:0c:29:8e:17:5e), Dst: Vmware_1e:8a:e8 (00:0c:29:1e:8a:e8)
Internet Protocol Version 4, Src: 192.168.1.26 (192.168.1.26), Dst: 192.168.1.20 (192.168.1.20)
User Datagram Protocol, Src Port: radius (1812), Dst Port: solid-mux (1029)
Radius Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x4 (4)
  Length: 241
  Authenticator: 429a88f23bbc205f658ddb1200c3c3b8
  [This is a response to a request in frame 1]
  [Time from request: 0.059067000 seconds]
  Attribute value Pairs
    AVP: l=6 t=Acct-Interim-Interval(85): 600
      Acct-Interim-Interval: 600
    AVP: l=20 t=vendor-specific(20) v=Fortinet, Inc. (12356)
  
```

