

FortiGate MAC+Portal 认证 测试介绍

版本	1.0
时间	2018 年 8 月
支持的版本	FortiGate-51E v6.0.2,build0163,180725 (GA) FAP221C FP221C-v5.6-build0499 Ningdun:6.7.3.3
作者	夏苗青
状态	待审核
反馈	support_cn@fortinet.com

目录

简介.....	3
测试网络拓扑.....	4
1. 配置防火墙.....	5
1.1. 配置防火墙接管 AP.....	5
1.2 授权 AP.....	5
1.3 配置无线 SSID.....	6
1.4 配置无线 WTP profile.....	8
1.5 配置无线用户上网的策略.....	9
2. 测试终端无线接入及 debug.....	9
2.1 无线用户首次接入.....	9
2.2 用户离开无线网络一段时间后再次接入无线网络.....	11
3. 测试中的 radius 认证抓包.....	13

简介

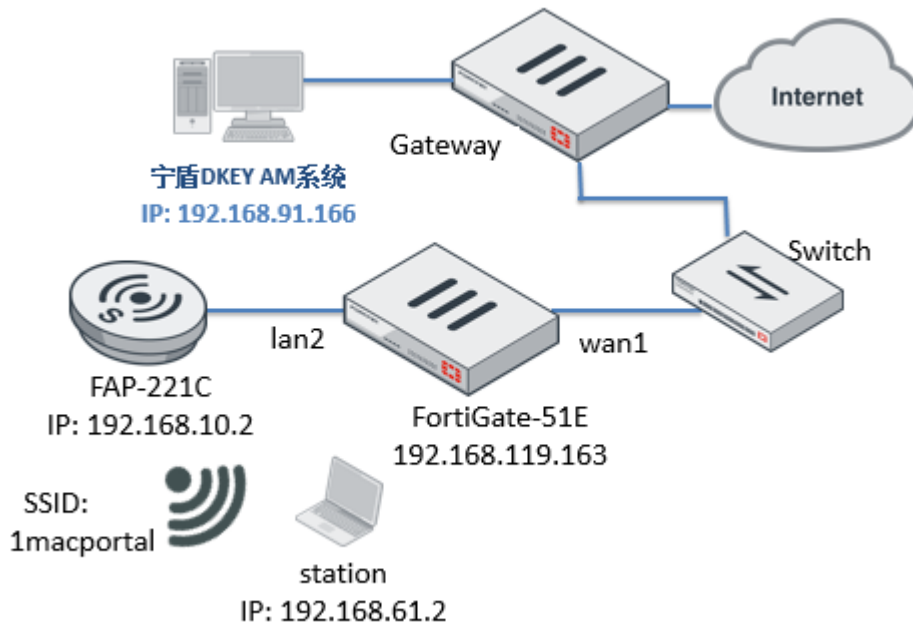
Portal 认证是无线网络部署时经常用到的一种认证方式,主要用于访客对于无线网络的访问,在实际使用过程中,经常会遇到的一种情况,就是用户通过 Portal 认证后,离开无线网络一段时间后,又再次接入无线网络时,需要重新做 Portal 认证,这样造成无线用户不方便的使用体验.

针对无线用户的这种使用情况,我们可以配置无线 MAC+Portal 认证,通过后台的 MAC 无感知认证来代替 Portal 认证,提高用户无线使用体验.

MAC+Portal 认证的过程为:

- ✓ 用户首次接入无线网络时,首先先做 MAC 认证,因为是新用户,Radius server 后台没有记录此用户的 MAC 地址,所以 MAC 认证失败,引导用户做 Portal 认证; Portal 认证成功后,后台 Radius server 记录用户的 MAC 地址信息,以便后续的 MAC 认证
- ✓ 当用户离开无线网络后,再次接入无线网路时,首先还是先对用户做无感知的 MAC 认证,由于用户 MAC 地址已经记录在 Radius server 上,所以用户 MAC 认证成功后,用户就可以直接上网了,无需再做 Portal 认证,提高用户体验.

测试网络拓扑



相关组件:

FGT51E:

lan2 口开启 CAPWAP, 管理 FAP, IP: 192.168.10.1/24

无线接口 1macportal: 开启 mac+portal 认证, IP: 192.168.61.1/24

wan1: 192.168.119.163

宁盾 AM 系统:

IP: 192.168.91.166, Radius/Portal 服务器, 支持 MAC+Portal 认证.

FAP221C:

AP221C 被 FGT51E 接管, 无线 SSID: 1macportal

1. 配置防火墙

1.1. 配置防火墙接管 AP

The screenshot shows the 'Edit Interface' configuration page for interface 'lan2'. The 'Administrative Access' section is expanded, and the 'CAPWAP' checkbox is checked and highlighted with a red box. Other checked options include HTTPS, HTTP, PING, and RADIUS Accounting. Unchecked options include FMG-Access, SNMP, and FortiTelemetry.

Below the interface configuration, the 'DHCP Server' section is visible, showing an 'Address Range' table with 'Starting IP' 192.168.10.2 and 'End IP' 192.168.10.254. The 'Netmask' is 255.255.255.0, and the 'DNS Server' is set to 'Specify' with the value 114.114.114.114.

1.2 授权 AP

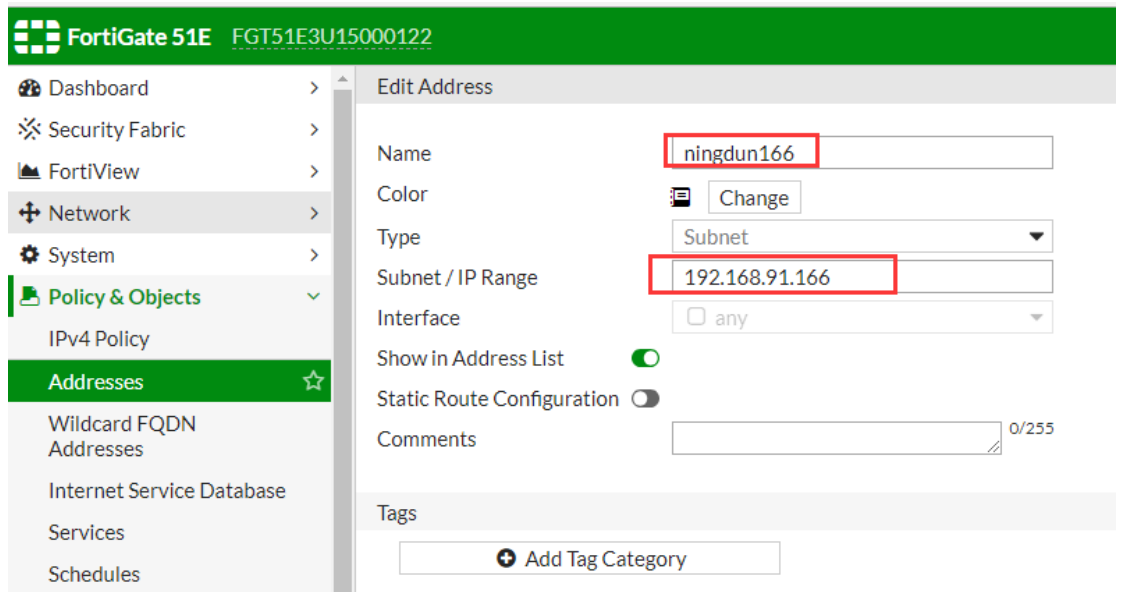
The screenshot shows the 'Managed FortiAPs' page in the FortiGate GUI. A table lists managed FortiAPs, with the first entry highlighted in yellow. The 'Authorize' button in the table is highlighted with a red box. A context menu is open over the 'Authorize' button, showing options like 'Edit', 'Deauthorize', 'Restart', and 'Upgrade'.

1.3 配置无线 SSID

由于 GUI 不支持配置 MAC+Portal 认证, 所以相关在命令行下配置.

1.3.1 配置无线 Portal 认证的例外

即认证成功之前,可以访问的相关地址, 一般为 Portal server IP 地址, 本例中为 192.168.91.166



配置例外:

```
FGT51E3U15000122 (security-exempt-list) # show
config user security-exempt-list
edit "1macportal-exempt-list"
config rule
edit ?
set dstaddr "ningdun166"
next
end
next
end
```

1.3.2 配置 radius 服务器和 user group

Edit RADIUS Server

Name:

Authentication method: Default Specify

NAS IP:

Include in every user group:

Primary Server

IP/Name:

Secret:

Connection status: ✓ Successful

Secondary Server

IP/Name:

Secret:

配置 user group

Edit User Group

Name:

Type: Firewall

Members: +

Remote Groups

Remote Server	
<input type="checkbox"/> Ningdun-91166	Am

1.4.1 无线接口配置

先配置一个集中转发的无线接口，配置为 open 认证，后续在命令行配置为 MAC+Portal 认证

The screenshot shows the 'Edit Interface' configuration page in the Fortinet GUI. The left sidebar is expanded to 'WiFi & Switch Controller' > 'SSID'. The main content area shows the following settings:

- Interface Name: 1macportal
- Alias: (empty)
- Type: WiFi SSID
- Traffic Mode: Tunnel
- Tags: Add Tag Category
- Address: IP/Network Mask: 192.168.61.1/255.255.255.0
- Administrative Access:
 - IPv4: HTTPS, HTTP, PING, FMG-Access
 - SSH, SNMP, FTM
 - RADIUS Accounting, FortiTelemetry

The screenshot shows the 'Edit Interface' configuration page in the Fortinet GUI. The left sidebar is expanded to 'WiFi & Switch Controller' > 'SSID'. The main content area shows the following settings:

- DHCP Server:
- Address Range:

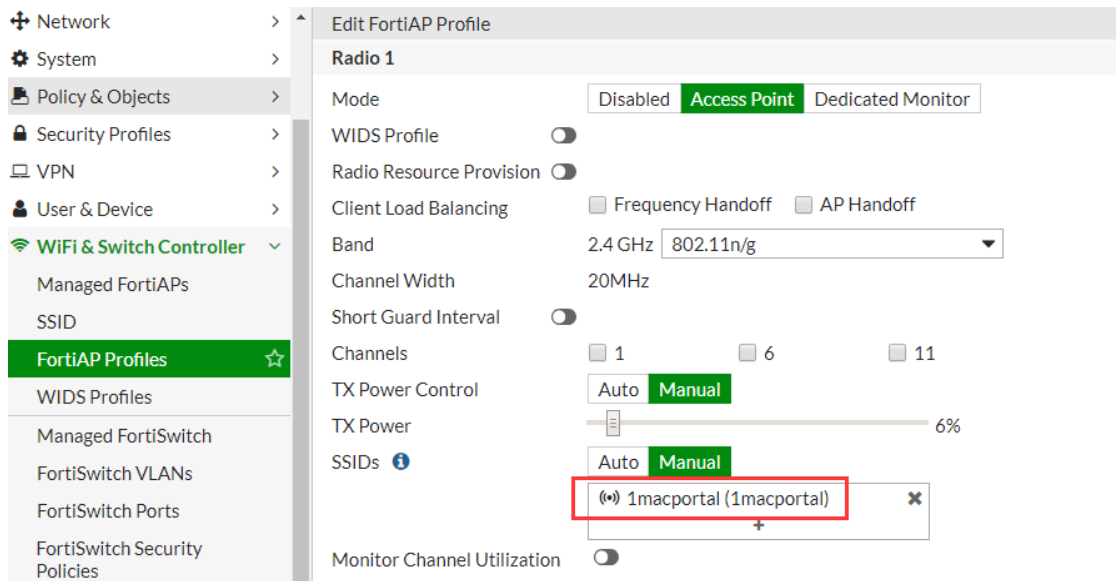
Starting IP	End IP
192.168.61.2	192.168.61.254
- Netmask: 255.255.255.0
- Default Gateway: Same as Interface IP
- DNS Server: Same as System DNS, Same as Interface IP, Specify: 114.114.114.114
- Advanced... (expanded)
- Networked Devices: Device Detection:
- WiFi Settings:
 - SSID: 1macportal
 - Security Mode: Open

命令行下配置此 SSID 为 MAC+Portal 认证:

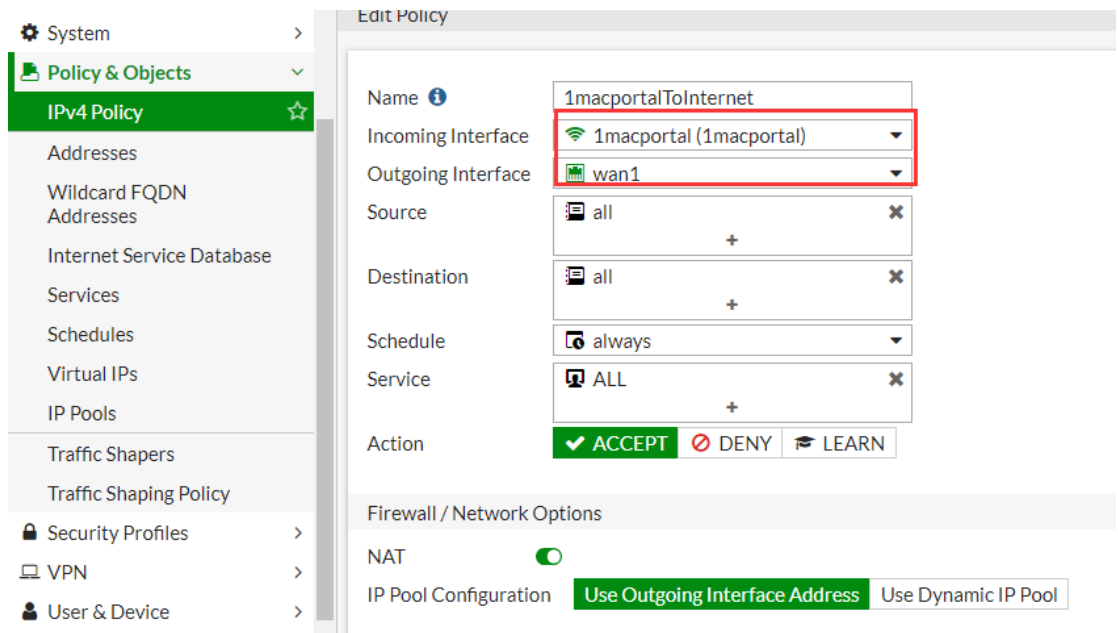
```
FGT51E3U15000122 #
FGT51E3U15000122 # config wireless-controller vap
FGT51E3U15000122 (vap) # edit 1macportal
FGT51E3U15000122 (1macportal) # show
config wireless-controller vap
  edit "1macportal"
    set vdom "root"
    set ssid "1macportal"
    set security captive-portal
    set mac-auth-bypass enable
    set selected-usergroups "Ningdun-91166"
    set security-exempt-list "1macportal-exempt-list"
    set schedule "always"
    set external-web "http://192.168.91.166:8080/am/portal/serviceId/SN180814214524/ac/FGT51E"
  next
end
```

1.4 配置无线 WTP profile

设置 AP 发出 SSID 为 1macportal 的无线信号



1.5 配置无线用户上网的策略



2. 测试终端无线接入及 debug

2.1 无线用户首次接入

无线用户首次接入时，会 MAC 认证失败:

FGT 上 debug 日志(FGT51E3U15000122 # diagnose debug application fnbamd 255):

```
[2224] handle_req-rcvd auth req 1838071636 for e0-06-e6-ce-50-9f in opt=00000500 prot=10
[394] __compose_group_list_from_req-group 4
[614] fnbamd_pop3_start-e0-06-e6-ce-50-9f
[605] fnbamd_cfg_get_radius_list_by_group-Loading RADIUS server 'Ningdun-91166' for usergroup 'Ningdun-91166' (4)
[305] fnbamd_create_radius_socket-Opened radius socket 13
[305] fnbamd_create_radius_socket-Opened radius socket 14
[1338] fnbamd_radius_auth_send-Compose RADIUS request
[1305] fnbamd_rad_dns_cb-192.168.91.166->192.168.91.166
[1280] fnbamd_rad_send-sent radius req to server 'Ningdun-91166': fd=13, IP=192.168.91.166(192.168.91.166:1812) code=1 id=115 1
en=211 user="e0-06-e6-ce-50-9f" using CHAP
[282] radius_server_auth-timer of rad 'Ningdun-91166' is added
[718] auth_tac_plus_start-Didn't find tac_plus servers (0)
[439] ldap_start-Didn't find ldap servers (0)
[556] create_auth_session-Total 1 server(s) to try
[2502] fnbamd_auth_handle_radius_result-timer of rad 'Ningdun-91166' is deleted
[1746] fnbamd_radius_auth_validate_pkt-RADIUS resp code 3
[2528] fnbamd_auth_handle_radius_result-->Result for radius svr 'Ningdun-91166' 192.168.91.166(1) is 1
[182] fnbamd_comm_send_result-Sending result 1 (error 0, nid 0) for req 1838071636
[708] destroy_auth_session-delete session 1838071636
```

Radius resp code 3 即 radius access reject.

下面是 radius server 侧的抓包:

No.	Time	Source	Destination	Protocol	Length	Info
→	346 12.608068	192.168.91.254	192.168.91.166	RADIUS	253	Access-Request(1) (id=115, l=211)
←	347 12.640805	192.168.91.166	192.168.91.254	RADIUS	78	Access-Reject(3) (id=115, l=36)

Frame 346: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits) on interface 0
 Ethernet II, Src: Fortinet_bc:e5:97 (08:5b:0e:bc:e5:97), Dst: Vmware_b6:12:00 (00:0c:29:b6:12:00)
 Internet Protocol Version 4, Src: 192.168.91.254, Dst: 192.168.91.166
 User Datagram Protocol, Src Port: 61883, Dst Port: 1812
 RADIUS Protocol

```

Code: Access-Request (1)
Packet identifier: 0x73 (115)
Length: 211
Authenticator: 3fea2e2df1c04af48bd8e699dc94b9e9
[The response to this request is in frame 347]
Attribute Value Pairs
  AVP: l=18 t=NAS-Identifier(32): FGT51E3U15000122
  AVP: l=19 t=User-Name(1): e0-06-e6-ce-50-9f
  AVP: l=19 t=CHAP-Password(3): b02672cd967e5b498e31582417780b9c99
  AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
  AVP: l=30 t=Called-Station-Id(30): 90-6C-AC-5D-C6-2D:1macportal
  AVP: l=19 t=Calling-Station-Id(31): E0-06-E6-CE-50-9F
  AVP: l=18 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
  AVP: l=24 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
  AVP: l=10 t=Acct-Session-Id(44): 6d8ebf54
  AVP: l=10 t=Connect-Info(77): web-auth
  AVP: l=12 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
  AVP: l=6 t=Service-Type(6): Login(1)
  
```

MAC 认证失败后, 转 Portal 认证, 用户在 Portal 登录页面输入正确的用户名和密码后:

FGT 上的 debug 日志:

```
[1338] fnbamd_radius_auth_send-Compose RADIUS request
[1305] fnbamd_rad_dns_cb-192.168.91.166->192.168.91.166
[1280] fnbamd_rad_send-sent radius req to server 'Ningdun-91166': fd=13, IP=192.168.91.166(192.168.91.166:1812) code=1 id=117 1
en=210 user="111-S-Z822ERQJCC" using CHAP
[282] radius_server_auth-timer of rad 'Ningdun-91166' is added
[718] auth_tac_plus_start-Didn't find tac_plus servers (0)
[439] ldap_start-Didn't find ldap servers (0)
[556] create_auth_session-Total 1 server(s) to try
[2502] fnbamd_auth_handle_radius_result-timer of rad 'Ningdun-91166' is deleted
[1746] fnbamd_radius_auth_validate_pkt-RADIUS resp code 2
[2528] fnbamd_auth_handle_radius_result-->Result for radius svr 'Ningdun-91166' 192.168.91.166(1) is 0
```

Radius resp code 2 即 radius access accept

Radius server 侧的抓包:

1025	36.305559	192.168.91.254	192.168.91.166	RADIUS	253	Access-Request(1) (id=116, l=211)
1027	36.331294	192.168.91.166	192.168.91.254	RADIUS	78	Access-Request(3) (id=116, l=36)
1244	39.681949	192.168.91.254	192.168.91.166	RADIUS	252	Access-Request(1) (id=117, l=210)
1245	39.714038	192.168.91.166	192.168.91.254	RADIUS	74	Access-Accept(2) (id=117, l=32)

Frame 1244: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface 0
 Ethernet II, Src: Fortinet_bc:e5:97 (08:5b:0e:bc:e5:97), Dst: Vmware_b6:12:00 (00:0c:29:b6:12:00)
 Internet Protocol Version 4, Src: 192.168.91.254, Dst: 192.168.91.166
 User Datagram Protocol, Src Port: 5971, Dst Port: 1812
 RADIUS Protocol

- Code: Access-Request (1)
 - Packet identifier: 0x75 (117)
 - Length: 210
 - Authenticator: 8d90aa45bd7647e4dd17ec89bd4628d0
 - [The response to this request is in frame 1245]
- Attribute Value Pairs
 - AVP: l=18 t=NAS-Identifier(32): FGT51E3U15000122
 - AVP: l=18 t=User-Name(1): 111-S-Z822ERQJCC
 - AVP: l=19 t=CHAP-Password(3): c63055266e32854de768fab631c2b978da
 - AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
 - AVP: l=30 t=Called-Station-Id(30): 90-6C-AC-5D-C6-2D:1macportal
 - AVP: l=19 t=Calling-Station-Id(31): E0-06-E6-CE-50-9F
 - AVP: l=18 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
 - AVP: l=24 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
 - AVP: l=10 t=Acct-Session-Id(44): 6d8ebf56
 - AVP: l=10 t=Connect-Info(77): web-auth
 - AVP: l=12 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
 - AVP: l=6 t=Service-Type(6): Login(1)

防火墙上认证状态查询:

GUI:

User Name	User Group	Duration	IP Address	Traffic Volume	Method
111-S-Z822ERQJCC	Ningdun-91166	5 minute(s) and 18 second(s)	192.168.61.2	104.25 kB	Firewall

命令行下:

```

FGT51E3U15000122 #
FGT51E3U15000122 # diagnose firewall auth list
192.168.61.2, 111-S-Z822ERQJCC
src_mac: e0:06:e6:ce:50:9f
type: fw, id: 0, duration: 370, idled: 0
expire: 300, allow-idle: 300
flag(130): radius idle wssso
server: Ningdun-91166
packets: in 330 out 401, bytes: in 72556 out 33076
group_id: 4
group_name: Ningdun-91166

----- 1 listed, 0 filtered -----
  
```

2.2 用户离开无线网络一段时间后再次接入无线网络

首先用户会进行 MAC 认证, 由于之前此 MAC 的 Portal 认证成功过, radius

server 上已经记录了此 MAC,所以 MAC 认证会显示成功.

FGT 上的 debug 日志:

```
[1338] fnbamd_radius_auth_send-Compose RADIUS request
[1305] fnbamd_rad_dns_cb-192.168.91.166->192.168.91.166
[1280] fnbamd_rad_send_send_radius_req to server 'Ningdun-91166': fd=13, IP=192.168.91.166(192.168.91.166:1812) code=1 id=120 l
en=211 user="e0-06-e6-ce-50-9f" using CHAP
[282] radius_server_auth-timer of rad 'Ningdun-91166' is added
[718] auth_tac_plus_start-Didn't find tac_plus servers (0)
[439] ldap_start-Didn't find ldap servers (0)
[556] create_auth_session-Total 1 server(s) to try
[2502] fnbamd_auth_handle_radius_result-timer of rad 'Ningdun-91166' is deleted
[1746] fnbamd_radius_auth_validate_pkt-RADIUS resp code 2
[2528] fnbamd_auth_handle_radius_result-->Result for radius svr 'Ningdun-91166' 192.168.91.166(1) is 0
```

Radius server 侧的抓包:

3744	141.892064	192.168.91.254	192.168.91.166	RADIUS	253	Access-Request(1) (id=120, l=211)
3746	141.926175	192.168.91.166	192.168.91.254	RADIUS	62	Access-Accept(2) (id=120, l=20)

Frame 3744: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits) on interface 0

Ethernet II, Src: Fortinet_bc:e5:97 (08:5b:0e:bc:e5:97), Dst: Vmware_b6:12:00 (00:0c:29:b6:12:00)

Internet Protocol Version 4, Src: 192.168.91.254, Dst: 192.168.91.166

User Datagram Protocol, Src Port: 24791, Dst Port: 1812

RADIUS Protocol

- Code: Access-Request (1)
 - Packet identifier: 0x78 (120)
 - Length: 211
 - Authenticator: 0adfe5d50f9dfe34f76ed761ef777dfb
 - [The response to this request is in frame 3746]
 - Attribute Value Pairs
 - AVP: l=18 t=NAS-Identifier(32): FGT51E3U15000122
 - AVP: l=19 t=User-Name(1): e0-06-e6-ce-50-9f
 - AVP: l=19 t=CHAP-Password(3): 54037bfee532bad5c10dbafc424876579a
 - AVP: l=6 t=NAS-Port-Type(61): Virtual(5)
 - AVP: l=30 t=Called-Station-Id(30): 90-6C-AC-5D-C6-2D:1macportal
 - AVP: l=19 t=Calling-Station-Id(31): E0-06-E6-CE-50-9F
 - AVP: l=18 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
 - AVP: l=24 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
 - AVP: l=10 t=Acct-Session-Id(44): 6d8ebf57
 - AVP: l=10 t=Connect-Info(77): web-auth
 - AVP: l=12 t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
 - AVP: l=6 t=Service-Type(6): Login(1)

防火墙上认证状态查询:

GUI:

User Name	User Group	Duration	IP Address	Traffic Volume	Method
e0-06-e6-ce-50-9f	Ningdun-91166	3 minute(s) and 18 second(s)	192.168.61.2	12.09 MB	Firewall

命令行显示:

```
FGT51E3U15000122 # diagnose firewall auth list
192.168.61.2, e0-06-e6-ce-50-9f
src_mac: e0:06:e6:ce:50:9f
type: fw, id: 0, duration: 249, idled: 0
expire: 300, allow-idle: 300
flag(130): radius idle wssso
server: Ningdun-91166
packets: in 10693 out 7149, bytes: in 11354487 out 757819
group_id: 4
group_name: Ningdun-91166

----- 1 listed, 0 filtered -----
```

3. 测试中的 radius 认证抓包

首次 MAC 认证失败,转 Portal 认证, Portal 认证成功:



fgt_mac_portal_ra
dius-portal.pcapn

用户再次接入无线网络时, MAC 认证成功:



fgt_mac_portal_ra
dius-mac.pcapng

测试使用的 FortiGate 配置:



FGT_Wireless_Ma
cPortal_Tunnel_FG