

ClearPass 对接 FortiGate 实现 FortiGate RSSO 功能 测试文档

fox210317@sina.com

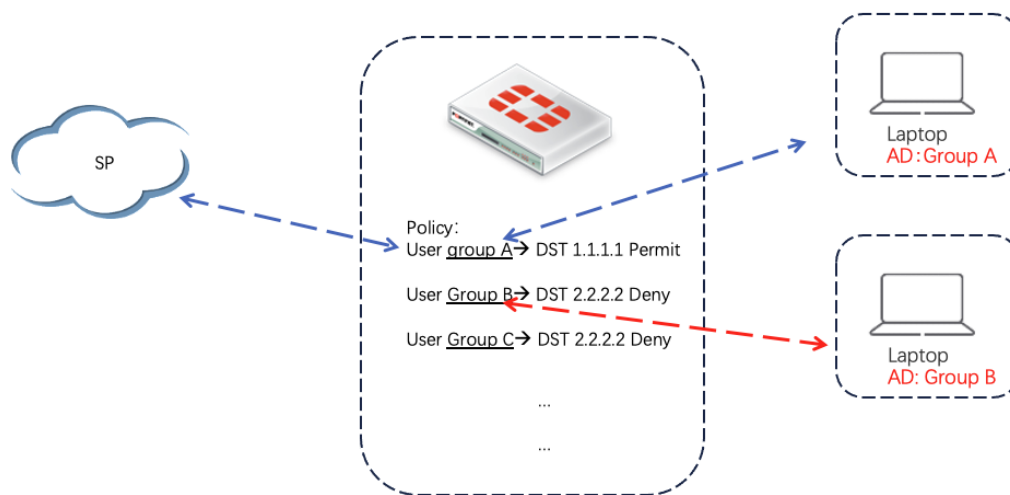
gaoyuan@xinyuming.com.cn

2026-04-15

一、使用需求分析

(一) 使用需求

部署在网络边界的 FortiGate 防火墙通过设置“用户（域账号）在 AD 中组的信息”策略实现域账号的访问权限，相比传统的 IPv4 策略更具有灵活性，方便日常网络运维。如下图所示：



(二) 功能实现的分析

1. 防火墙在整体网络架构中的角色

因为防火墙部署在网络出口区域，而且在较大的网络规模中，不承担用户网关的角色，仅作一些安全防护、策略管控等功能。因此防火墙不会作为 NAD 设备与 AAA 服务器交互 RADIUS 报文，便无法通过 RADIUS Authentication 流程获取用户的域账号组属性信息。

2. 如何将组属性传送到防火墙

在使用需求中，防火墙又必须使用域账号的组属性，我们可以通过 AAA 服务器将 RADIUS Accounting 报文传递防火墙。

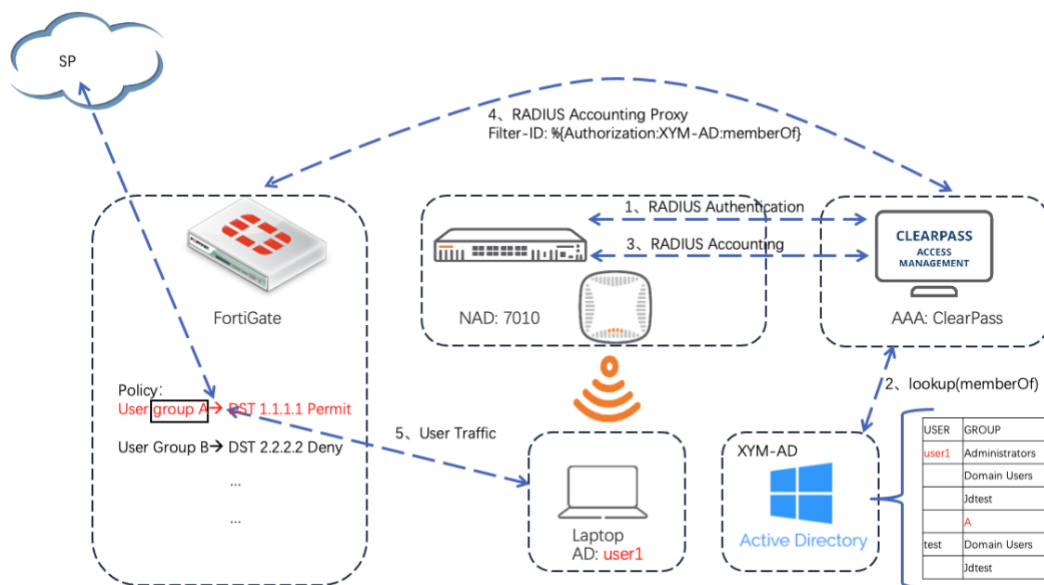
3. 用户的组成

包含有线用户、无线用户

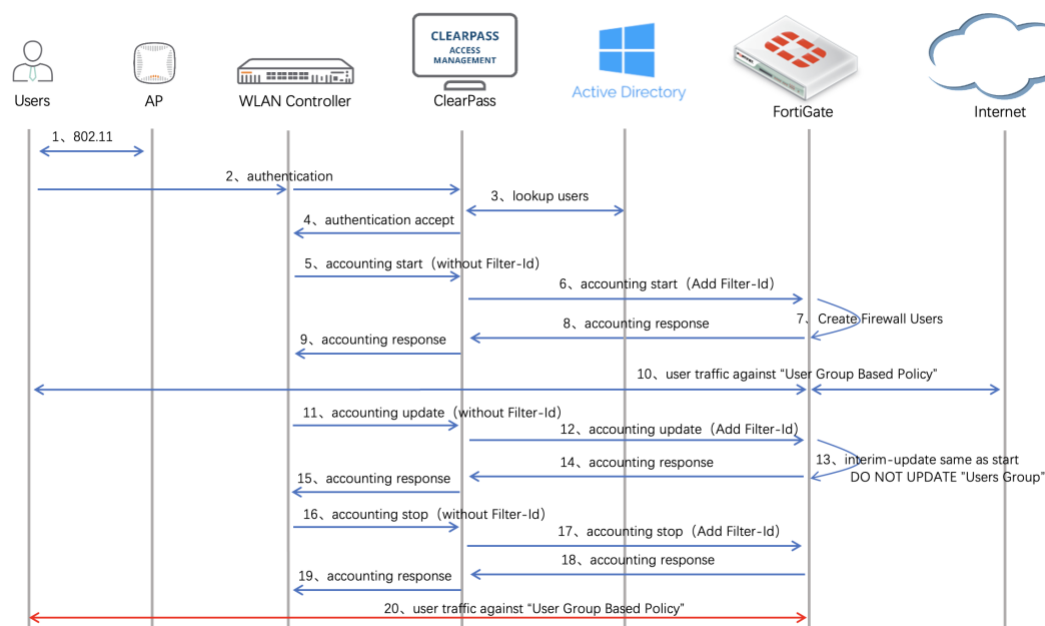
文档中仅测试了无线用户

4. 整体流程

(1) 流程图：



(2) 报文交互过程:



(三) 测试过程

1. 测试设备清单

设备类别	设备型号	软件版本	数量
AAA 服务器	ClearPass	6.9.0.130064	1
NAD	ARUBA 7010	8.6.0.23	1
AP	325	8.6.0.23	1
防火墙	FortiGate60F	7.4.11	1
AD	Win Server	2016 10.0.14393.1737	1
DNS	Win Server	2016 10.0.14393.1737	1
测试终端	手机		3

2. 设备的配置

(3) IP 信息

设备类别	设备型号	IP address
AAA 服务器	ClearPass	192.168.1.150
NAD	ARUBA 7010	192.168.1.100
AP	325	192.168.1.32
防火墙	FortiGate60F	192.168.1.253
AD	Win Server	192.168.1.251
DNS	Win Server	192.168.1.251
测试终端	手机	

(4) ClearPass 的配置

a) 添加 NAD

Configuration - Network - Device - Add

Edit Device Details

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name:

IP or Subnet Address:
(e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)

Description:

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name:

Enable RADIUS Dynamic Authorization: ☒ Port:

Enable RadSec: ☐

b) 添加 Proxy Targets

Configuration - Network - Proxy Targets - Add

A proxy target represents a RADIUS server (ClearPass or third party) that is the target of a proxied RADIUS request.

Filter: Name contains Go Clear Filter

#	Name	Hostname	Protocol
1.	fortigw	192.168.1.253	RADIUS

Showing 1-1 of 1

Edit Proxy Target

Name: fortigw

Description: send user group & username to fortigw

Hostname: 192.168.1.253

Protocol: RADIUS

Shared Secret: *****

Verify Shared Secret: *****

RADIUS Authentication Port: 1812 (Default is 1812)

RADIUS Accounting Port: 1813 (Default is 1813)

Copy Save Cancel

c) 添加 Authentication Sources

Configuration - Authentication - Sources—Add

- cache timeout 1s
- 因为测试环境，在 AD 参数中使用的都是配置模板

Monitoring

Configuration

- Service Templates & Wizards
- Services
- Authentication
 - Methods
 - Sources
- Identity
 - Single Sign-On (SSO)
 - Local Users
 - Endpoints
 - Static Host Lists
 - Roles
 - Role Mappings
- Posture
 - Posture Policies
 - Audit Servers
 - Agentless OnGuard
- Enforcement
 - Policies
 - Profiles
- Network
 - Devices
 - Device Groups
 - Proxy Targets
 - Event Sources
- Network Scan
- Policy Simulation

Authentication Sources - XYM-AD

Summary General Primary Attributes

General:

Name: XYM-AD

Description:

Type: AD

Use for Authorization: Enabled

Authorization Sources: -

Primary:

Hostname: example.com

Connection Security: None

Port: 389

Bind DN: gaoyuan@example.com

Bind Password: *****

Base DN: dc=example,dc=com

Search Scope: SubTree Search

Bind User: true

User Certificate: userCertificate

Attributes:

Filters :

1. (&(sAMAccountName=%(Authentication:Username))(objectClass=user))
2. (distinguishedName=%(memberOf))
3. (&(sAMAccountName=%(Host:Name))(objectClass=computer))
4. (&(sAMAccountName=%(Onboard:Owner))(objectClass=user))
5. (distinguishedName=%(Onboard memberOf))

启用 memberOf 作为属性

Authentication Sources - XYM-AD

Summary General Primary Attributes			
Specify filter queries used to fetch authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	Attribute
	department	Department	Attribute
	title	Title	Attribute
	company	company	Attribute
	memberOf	memberOf	Attribute
	telephoneNumber	Phone	-
	mail	Email	Attribute
	displayName	Name	-
	accountExpires	Account Expires	-
2. Group	cn	Groups	-
3. Machine	dnsHostName	HostName	-
	operatingSystem	OperatingSystem	-
	operatingSystemServicePack	OSServicePack	-
4. Onboard Device Owner	memberOf	Onboard memberOf	-
5. Onboard Device Owner Group	cn	Onboard Groups	-

d) ClearPass 加入 AD

- Clearpass 配置的 DNS 是 Win Server 中启用的服务；
- FQDN 需要在 DNS 可解析

Administration » Server Manager » Server Configuration - CLEARPASS

Server Configuration - CLEARPASS (192.168.1.150)

System Services Control Service Parameters System Monitoring Network FIPS

Hostname: CLEARPASS

FQDN:

Policy Manager Zone: default

Enable Performance Monitoring Display: ☒ Enable this server for performance monitoring display

Insight Setting: ☐ Enable Insight

Enable Ingress Events Processing: ☐ Enable Ingress Events processing on this server

Master Server in Zone: Primary master

Span Port: -- None --

	IPv4	IPv6	Action
Management Port	IP Address: 192.168.1.150		
	Subnet Mask: 255.255.254.0		
	Default Gateway: 192.168.1.253		Configure
Data/External Port	IP Address: 192.168.0.150		
	Subnet Mask: 255.255.255.0		
	Default Gateway: 192.168.0.253		Configure
DNS Settings	Primary: 192.168.1.251		
	Secondary: 8.8.8.8		
	Tertiary:		Configure
	DNS Caching: Disabled		

AD Domains:

Domain Controller	Action
1. EXAMPLE.COM	Join AD Domain Leave AD Domain

Join AD Domain

Enter the FQDN of the controller and the short (NetBIOS) name for the domain:

Domain Controller: WIN-GESK41RNE0.example.com

NetBIOS Name: EXAMPLE

In case of a controller name conflict:

☒ Use specified Domain Controller

☐ Use Domain Controller returned by DNS query

☐ Fail on conflict

☐ Use default domain admin user (Administrator)

Username: 123123

Password: *****

管理员账号

Save Cancel

Back to Server Configuration Save Cancel

e) 创建 Profiles

Configuration - Enforcement - Profiles

Enforcement Profiles - [Allow Access Profile]

Summary Profile Attributes

Profile:

Name:	[Allow Access Profile]
Description:	System-defined profile to allow network access
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name
------	------

f) 创建 Policies

Configuration - Enforcement - Policies

Configuration » Enforcement » Policies » Edit - AD[Allow Access Policy]

Enforcement Policies - AD[Allow Access Policy]

Summary Enforcement Rules

Enforcement:

Name:	AD[Allow Access Policy]
Description:	Sample policy to allow network access
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: Evaluate all

Conditions	Actions
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	[Allow Access Profile]

g) 创建 Services

- 启用 Authorization、Accounting Proxy
- Authentication Sources: XYM-AD
- Authorization Sources: XYM-AD、[Local User Repository]
- Enforcement, 选择 f) 创建的模板

- Accounting Proxy: 选择 b) 创建的模板
- 额外添加的 RADIUS Accounting 属性, Filter-Id: %{Authorization:XYM-AD:memberOf}

ClearPass Policy Manager

Configuration » Services » Edit - FortiGate-RSSO-WLAN

Services - FortiGate-RSSO-WLAN

Summary Service Authentication Authorization Roles Enforcement Accounting Proxy

Service:

Name: FortiGate-RSSO-WLAN
Description: 802.1X WLAN Access Service
Type: 802.1X Wireless
Status: Enabled
Monitor Mode: Disabled
More Options: 1. Authorization
2. Accounting Proxy

Service Rule

Match ANY of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Connection	NAD-IP-Address	BEGINS_WITH	192.168

Authentication:

Authentication Methods: 1. [EAP PEAP]
2. [EAP TLS]
3. [EAP MSCHAPv2]
4. [CHAP]
5. [PAP]
Authentication Sources: XYM-AD [Active Directory]
Strip Username Rules: -
Service Certificate: -

Authorization:

Authorization Details: 1. XYM-AD [Active Directory]
2. [Local User Repository] [Local SQL DB]

Roles:

Role Mapping Policy: -

Enforcement:

Use Cached Results: Disabled
Enforcement Policy: AD[Allow Access Policy]

Accounting Proxy:

Accounting Proxy Targets: fortigw

RADIUS attributes to be deleted for Accounting proxy

Type	Name	Operator	Value
------	------	----------	-------

RADIUS attributes to be added for Accounting proxy

Type	Name	Operator	Value
1. Radius:IETF	Filter-Id	=	%{Authorization:XYM-AD:memberOf}

Back to Services Disable Copy Save Cancel

Apr 22, 2026 14:59:35 CST ClearPass Policy Manager 6.9.0.130064 [FIPS] on C1000V (Trial Version) platform

(5) 控制器的配置

因测试环境为 7010 standalone 工作模式, 此文档配置层级均为 mynode (既 7010 层级); 其他 ARUAB 控制器组网架构按照网络逻辑关系自定义

a) 添加认证服务器、服务器组

- 先创建认证服务器, 类型 RADIUS, 填写 HOST、Key

- 再创建认证服务器组，将创建的认证服务器加入组

Mobility Controller > 7010

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication**
- Services
- Interfaces
- System
- Tasks
- Redundancy

Diagnostics

Maintenance

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Groups 4

NAME	SERVICES	FAIL THROUGH
default	1	--
internal	1	--
clearpass-sg	1	--
fortigw	2	--

Server Group > clearpass-sg Servers Options Server Rules

NAME	TYPE	IP ADDRESS
clearpass	RADIUS	192.168.1.150

Server Group > clearpass-sg > clearpass Server Options Server Group Trim FQDN Server Gro

Name: clearpass

IP address / hostname: 192.168.1.150

Auth port: 1812

Acct port: 1813

Shared key:

Retype key:

b) 创建 L2 Authentication

选择 802.1X Authentication，点+创建，配置参数保持默认

Auth Servers AAA Profiles **L2 Authentication** L3 Authentication User Rules Advanced

L2 Authentication

- 802.1X Authentication
- Hzz-Test_dot1_aut
- XYM-1X-AUTH-Pro
- default
- default-psk
- fortigw**
- MAC Authentication
- Stateful 802.1X Authentication

802.1X Authentication Profile: fortigw

Max authentication failures:

Enforce Machine Authentication:

Machine Authentication: Default Machine Role:

Machine Authentication Cache Timeout:

Blacklist on Machine Authentication Failure:

Machine Authentication: Default User Role:

Interval between Identity Requests:

Quiet Period after Failed Authentication:

c) 创建 AAA Profiles

- 802.1X Authentication 调用步骤 b) 模板
- 802.1X Authentication 调用步骤 a) 模板
- RADIUS Accounting Server Group 调用步骤 a) 模板
- AAA Profile 开启 RADIUS Interim Accounting

Auth Servers **AAA Profiles** L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- default-mac-auth
- default-open
- default-tunneled-use...
- default-xml-api
- fortigw**
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server
- portal
- xym

AAA Profile: fortigw

Initial role: logon

MAC Authentication Default Role: guest

802.1X Authentication Default Role: authenticated

Download Role from CPPM: ☐

Set username from dhcp option 12: ☐

L2 Authentication Fail Through: ☐

Multiple Server Accounting: ☐

User idle timeout: seconds

Max IPv4 for wireless user: 2

RADIUS Roaming Accounting: ☐

RADIUS Interim Accounting: ☒

RADIUS Acct-Session-Id In Access-Request: ☒

User derivation rules: -None-

Wired to Wireless Roaming: ☒

Reauthenticate wired user on VLAN change: ☐

Device Type Classification: ☒

Enforce DHCP: ☐

PAN Firewall Integration: ☐

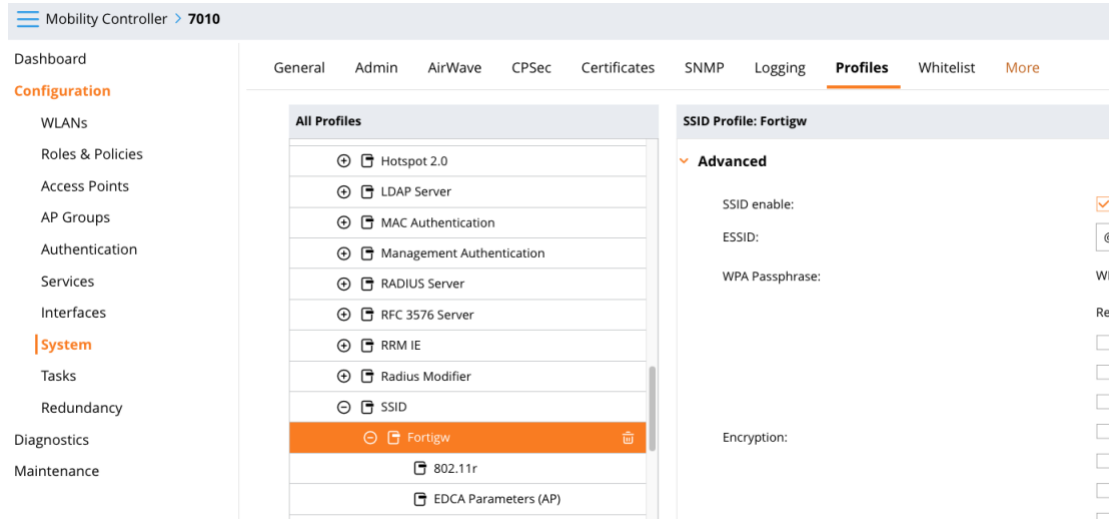
Open SSID radius accounting: ☐

Apply ageout mechanism on bridge mode wireless clients: ☐

d) 创建 SSID Profiles

配置路径： Configuration-System-Profiles-展开 Wireless LAN-SSID

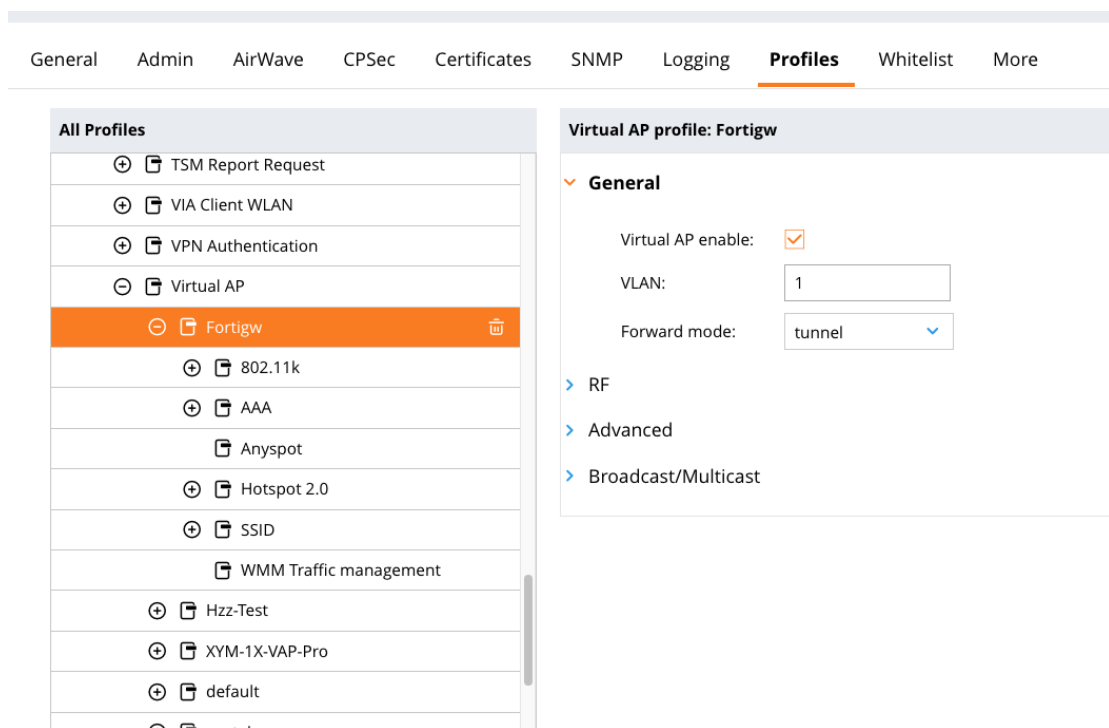
写入 ESSID 名称、Encryption 选择 wpa2-aes，其他参数保持默认



e) 创建 Virtual-ap Profiles

配置路径： Configuration-System-Profiles-展开 Wireless LAN-Virtual AP

- 关联步骤 c) 创建的 AAA Profiles 模板
- 关联步骤 d) 创建的 SSID Profiles 模板
- 写入 VLAN (用户获取 IP 的 VLAN ID)



f) AP Group 关联 Virtual-AP

配置路径：Configuration-AP Groups-default-WLANs-加号-选择步骤 e) 创建的模板，点击 submit，右上角 Pending Changes、Deploy

The screenshot shows the Aruba Mobility Controller configuration interface. On the left, the navigation menu has 'Configuration' and 'AP Groups' highlighted with red boxes. The main content area shows 'AP Groups' with a list of groups: 'NAME', '123', and 'default' (highlighted with a red box). Below this, there is a '+ NoAuthApGroup' link. A modal window titled 'Select WLAN' is open, showing 'Virtual-ap:' with a dropdown menu set to 'Fortigw' (highlighted with a red box). A red arrow points to the 'Submit' button in the modal. Below the modal, there is a table with tabs: 'AP Groups > default', 'APs', 'WLANs' (highlighted with a red box), 'Radio', 'Mesh', 'LMS', and 'MultiZone'. The table has columns: 'NAME', 'AP GROUP', 'AIRTIME LIMIT (%)', and 'PER-USER LIMIT (KBPS)'. It contains two rows: 'xym' with 'default' and 'XYM-1X-VAP-Pro' with 'default'.

NAME	AP GROUP	AIRTIME LIMIT (%)	PER-USER LIMIT (KBPS)
xym	default	--	--
XYM-1X-VAP-Pro	default	--	--

(6) 防火墙的配置

a) 创建 RADIUS Servers

FortiGate60F

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition

User Groups

Guest Management

LDAP Servers

RADIUS Servers

TACACS+ Servers

Single Sign-On

Authentication Settings

FortiTokens

WiFi & Switch Controller

System

Security Fabric

Log & Report

New RADIUS Server

Name

Authentication method

Default Specify

NAS IP

Include in every user group ☒

Primary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

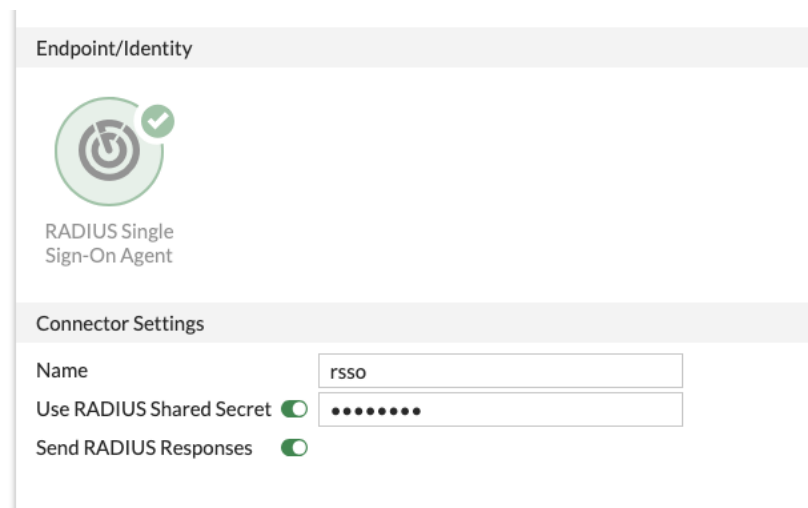
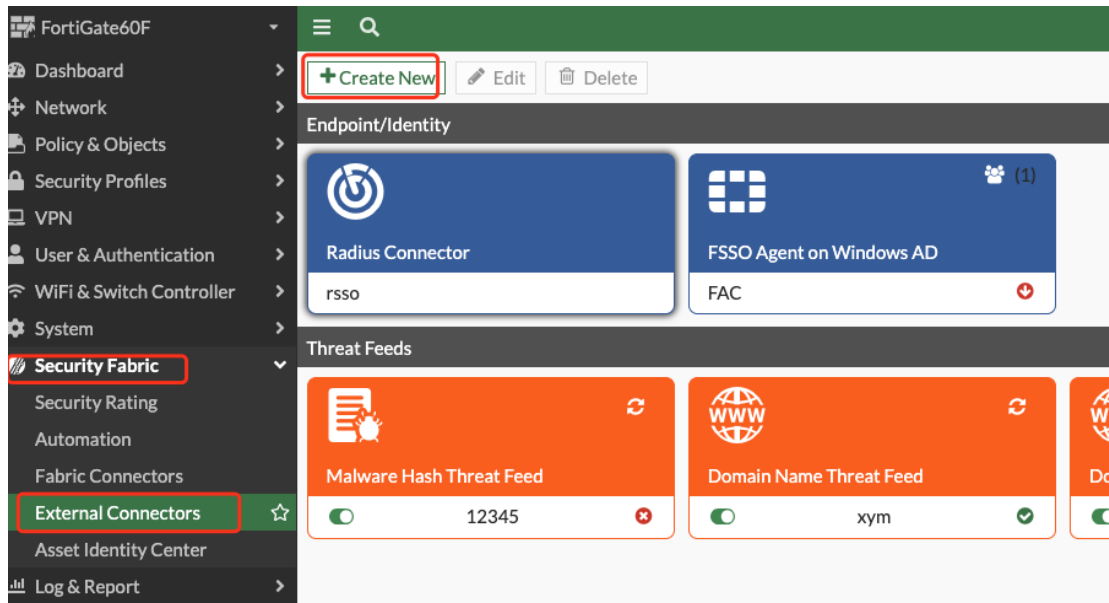
Test User Credentials

b) 创建 External Connectors

飞塔防火墙需要网页+命令行配置

网页配置：

配置路径：System - Security Fabric - External Connectors - Create New, 选择 RADIUS Connector (RSS0)



命令行配置：

此处 `set sso-attribute Filter-Id` 只能通过命令行配置，目的是与 ClearPass 返回的属性对应。

```
edit "rssl"
  set acct-all-servers enable
  set rssl enable
  set rssl-radius-response enable
  set rssl-validate-request-secret enable
  set rssl-secret ENC TIHxfxIw3buBGmAb9KmnsL2e7x0021LYEmiSe
kXC3soP1NfKEtKV3wPZyz1wMWFpQy/Nwzcvo+D50+wDU/y1lmMjY3dkVA
  set rssl-endpoint-attribute User-Name
  set sso-attribute Filter-Id
next
end
FortiGate60F #
```

c) 创建 User Groups

- 选择 User & Authentication -User Groups -Create New
- Name: 方便识别的名称
- Type: RADIUS Single Sign-On(RSSO)
- RADIUS Attribute Value:CN=Administrators,CN=Builtin,DC=example,DC=com 此处添加的是对应用户在 AD 中的组信息

注：如果域账号只属于一个组，则在 FortiGate 配置属性值写一个，如果域账号属于多个组，则需要在 FortiGate 配置属性值写全部。

在 FortiGate 中创建的 user group 与 ClearPass Accounting 报文中 Filter-ID 形成一个映射关系表，如下表所示：

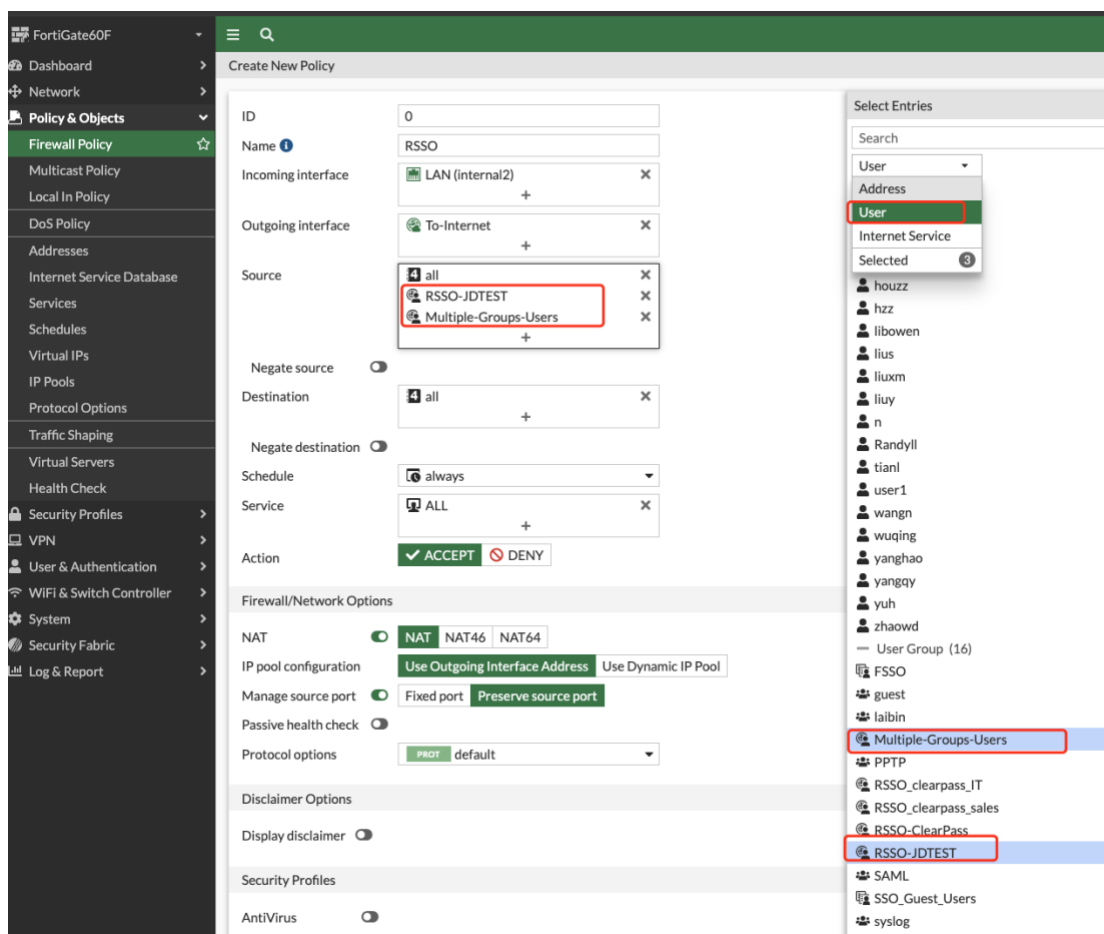
FortiGate Group Name	FortiGate RADIUS Attribute	ClearPass Accounting 报文中的 Filter-ID 内容	AD User
RSSO-JDTEST	CN=Administrators,CN=Builtin,DC=example,DC=com	CN=Administrators,CN=Builtin,DC=example,DC=com	gaoyuan
Multiple-Groups-Users	CN=Administrators,CN=Builtin,DC=example,DC=com, CN=JDtest,CN=Users,DC=example,DC=com, CN=PPPPP,CN=Users,DC=example,DC=com	CN=Administrators,CN=Builtin,DC=example,DC=com, CN=JDtest,CN=Users,DC=example,DC=com, CN=PPPPP,CN=Users,DC=example,DC=com	yanghao
			zhangsan

映射关系表

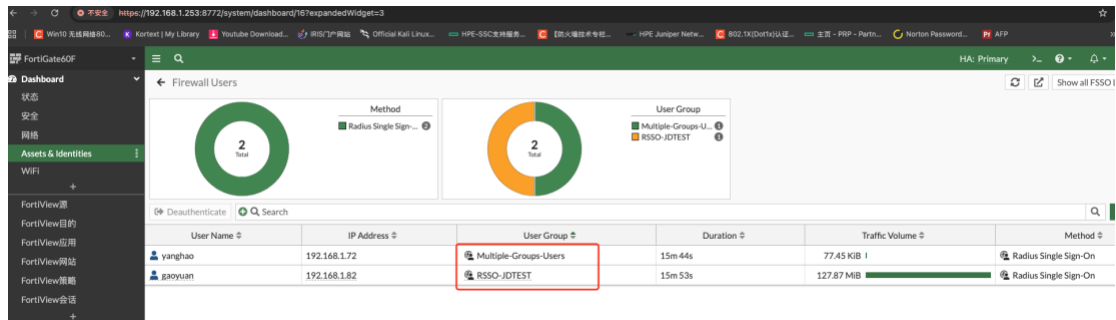
d) 创建 Policy

选择 Policy & Objects -Firewall Policy -Create New

- 流入接入、流出接口对应选择
- Source 需要选择 2 个内容，一个是 Address（可以选择 any 或自定义）、二是需要选择 User（选择定义的 User Group Name）
- 此处需要注意的是在 Destination 中无法选择 User Group



e) 仪表盘中显示用户组信息



(7) 测试结果验证

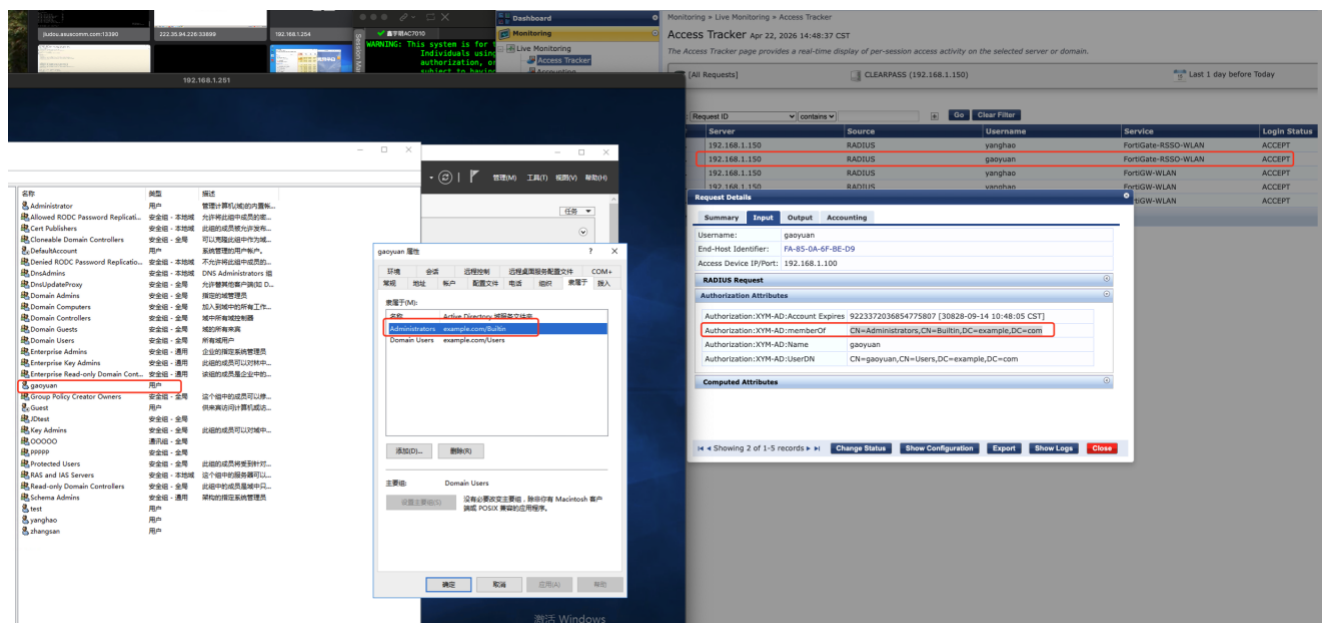
a) 测试域账号 gaoyuan 的结果

- 测试手机连接 ESSID: @@Fortigw

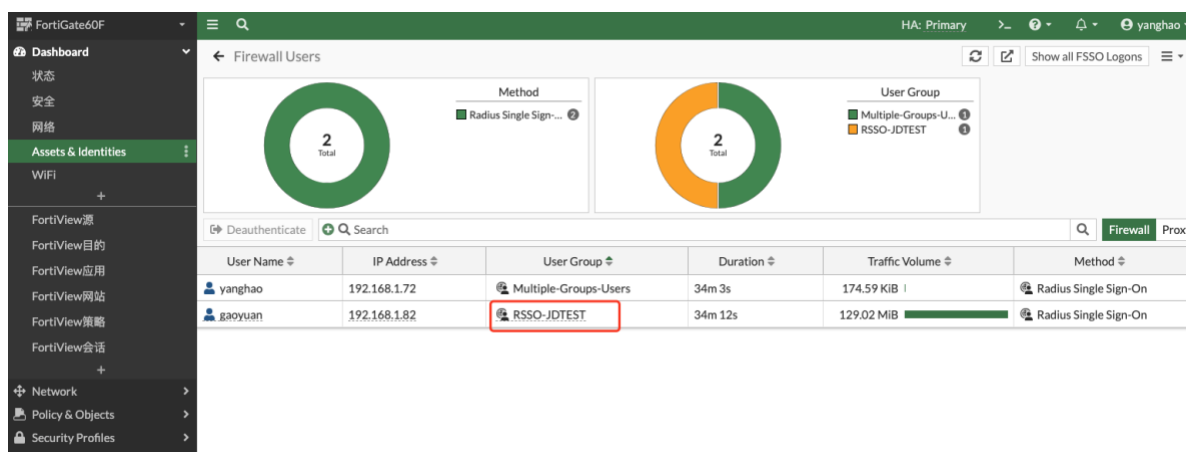


注：AD 域账号 gaoyuan 仅加入了一个组

- 在 AD 中 gaoyuan 账号关联了一个 Administrators 组，ClearPass 中查询到授权信息 “CN=Administrators,CN=Builtin,DC=example,DC=com”，如下图所示：



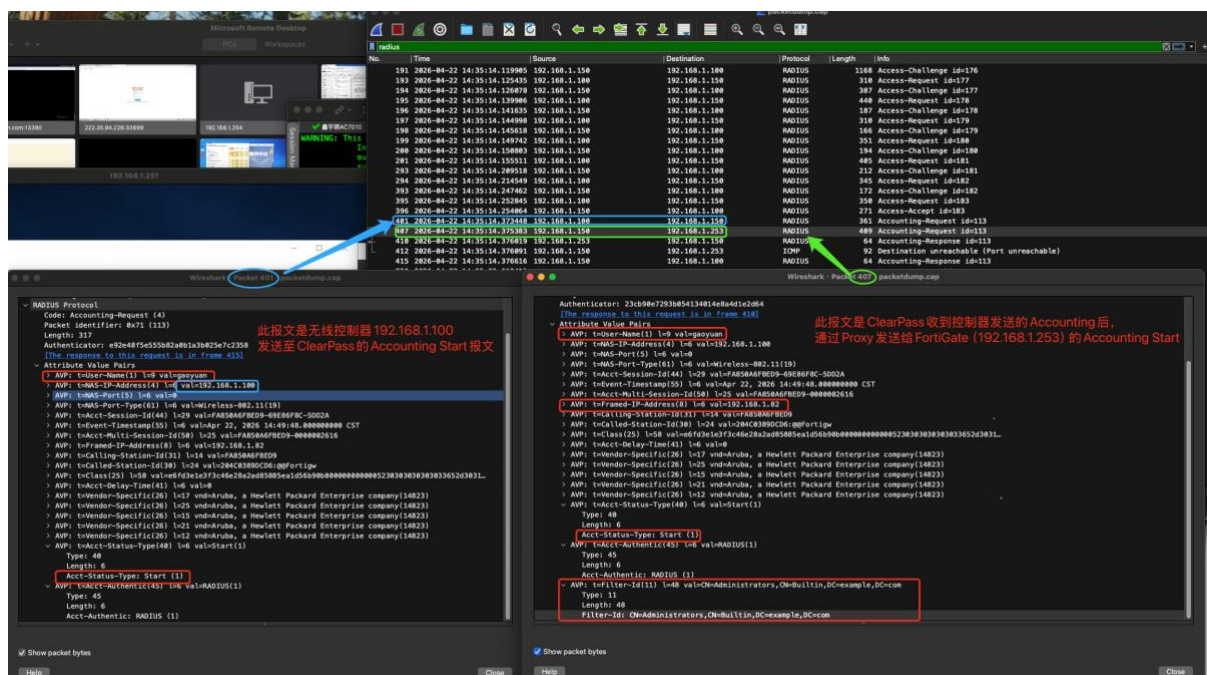
- 防火墙中可以查看到该用户 gaoyuan 的用户组信息
对应关系见（三）-（6）-b)小节《映射关系表》



- 控制器中关于账号 gaoyuan 的上线信息

```
(7010) [mynode] #show user-table name gaoyuan
Wed Apr 22 15:20:40.127 2026
Users
-----
pe IP MAC Name Role Age(d:h:m) Auth VPN link AP name Roaming Essid/Bssid/Phy Profile
-----
192.168.1.82 fa:85:0a:6f:be:d9 gaoyuan authenticated 00:00:30 802.1x 80:8d:b7:cf:3a:d0 Wireless @@Fortigw/80:8d:b7:73:ad:12/a-VHT fortigw
User Entries: 1/0
Curr/Cum Alloc:24/1987 Free:13/1963 Dyn:37 AllocErr:0 FreeErr:0
```

- 在通过 ClearPass 抓包文件中可以查看到关于账号 gaoyuan 的 accounting 相关信息。



- 在后续的无线控制器出的 Accounting update 报文中, ClearPass 仍然会额外添加 Filter-ID 属性内容, 并与其发送的 accounting start 报文中 Filter-Id 字段内容保持一致。

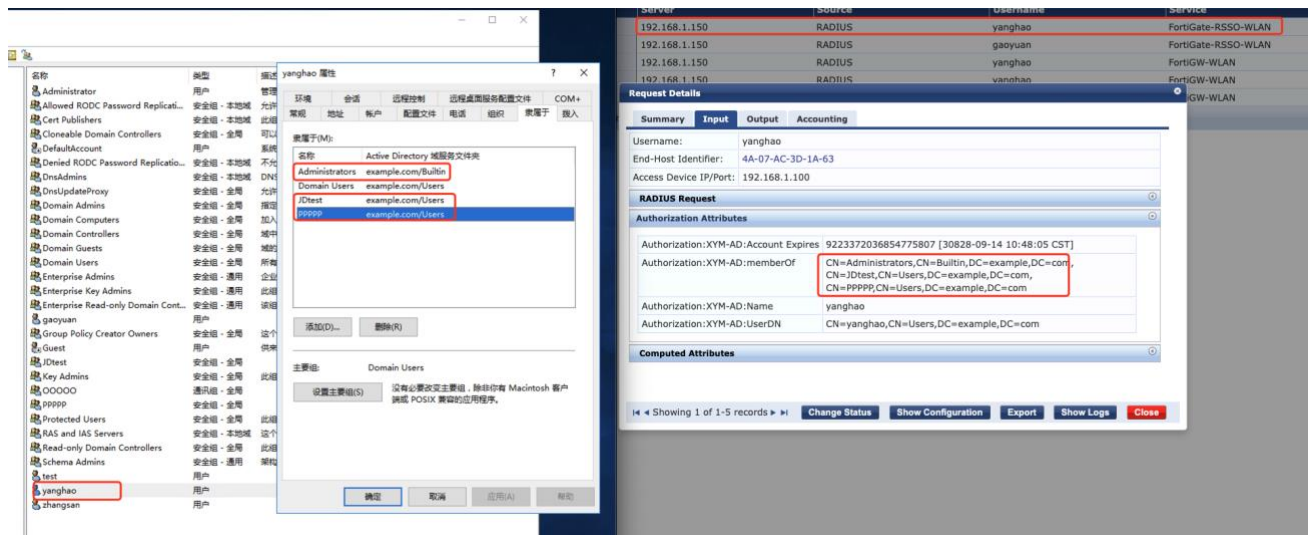
b) 测试域账号 yanghao 的结果

- 测试手机连接 ESSID: @@Fortigw

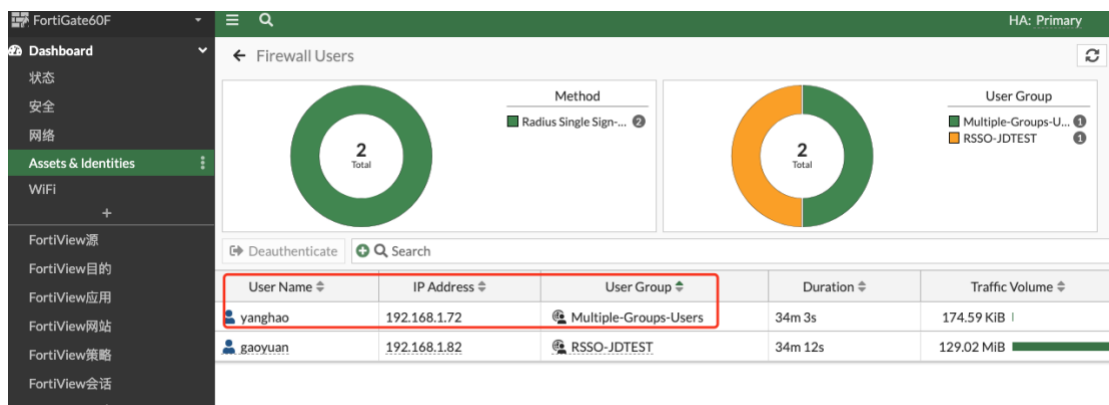


注：AD 域账号 yanghao 加入了三个组

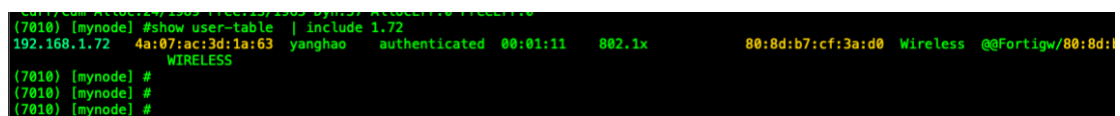
- 在 AD 中 gaoyuan 账号关联了三个组，Administrators、Jdtest、PPPPP；ClearPass 中查询到授权信息“CN=Administrators,CN=Builtin,DC=example,DC=com, CN=Jdtest,CN=Users,DC=example,DC=com, CN=PPPPP,CN=Users,DC=example,DC=com”，如下图所示：



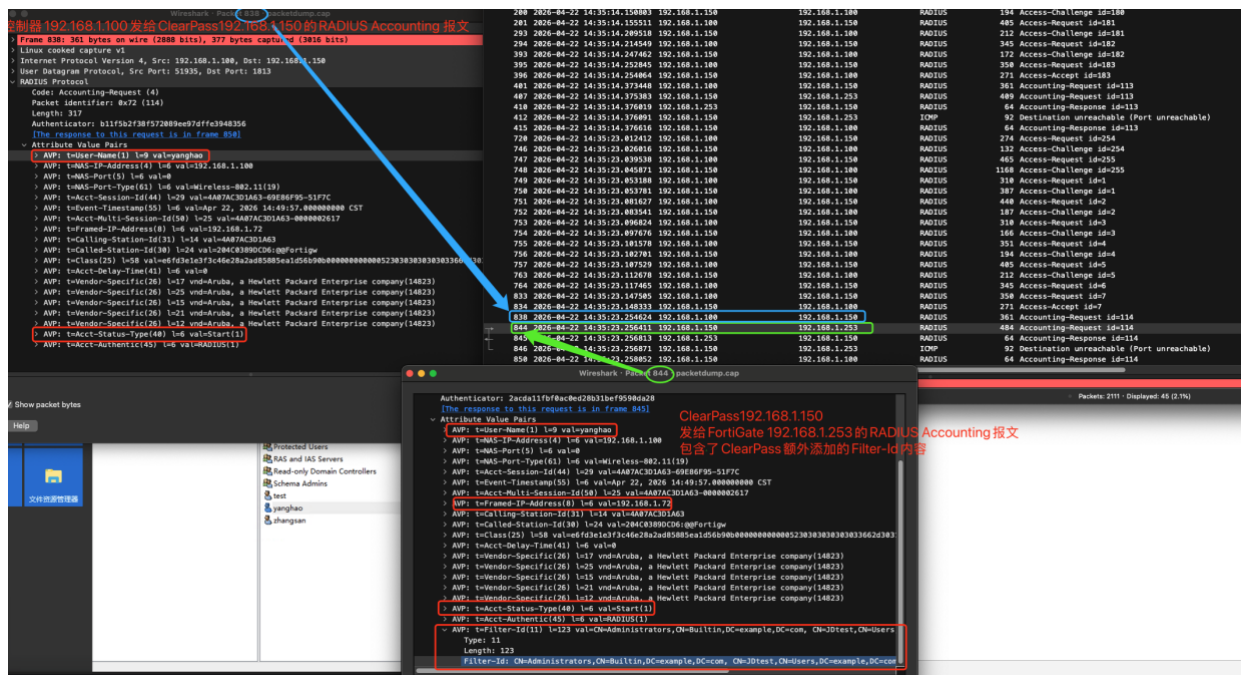
- 防火墙中可以查看到该用户 yanghao 的用户组信息



- 控制器中关于账号 yanghao 的上线信息



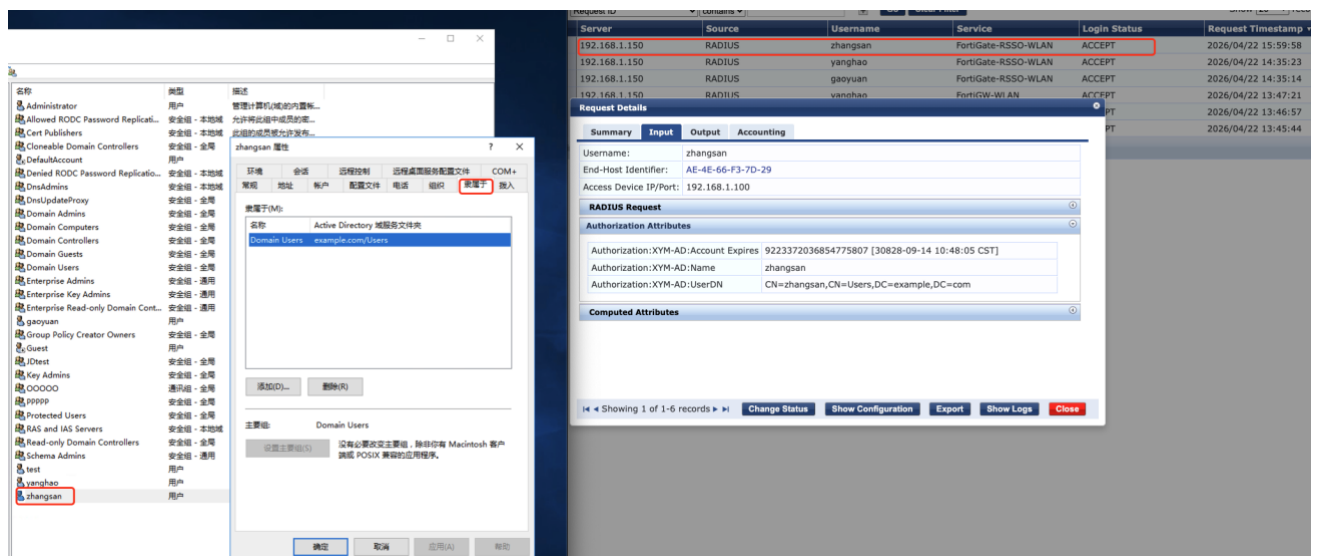
- 在通过 ClearPass 抓包文件中可以查看到关于账号 yanghao 的 accounting 相关信息。



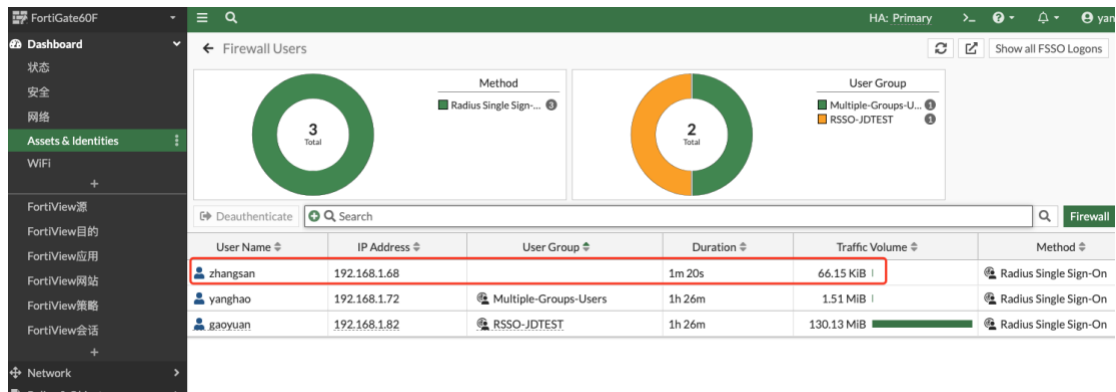
c) 测试域账号 zhangsan 结果

注：AD 域账号 zhangsan 未加入任何 AD 组

在 ClearPass Tracker 中也可以没有关于 memberOf 的授权属性



在 FortiGate 中也没有关于 zhangsan 的 User Group 属性



(四) 其他测试场景

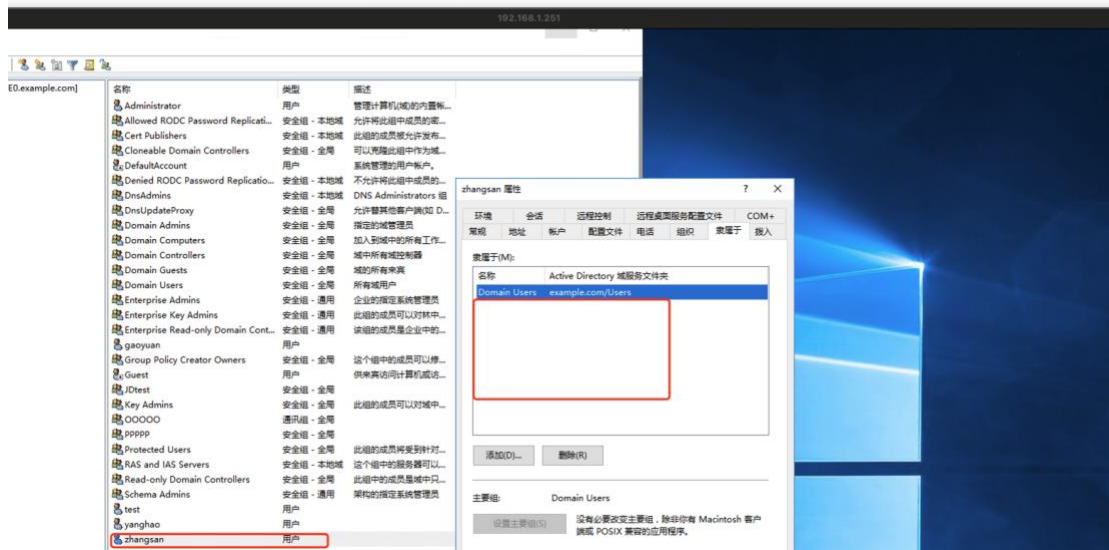
(1) 测试一

a) 测试条件:

- AD 中 zhangsan 账号未加入任何组
- iPhone12 先通过 zhangsan 连入 WLAN
- iPhone13 在通过 zhangsan 连入 WLAN

终端	MAC	IP
iPhone12	7e:61:2f:ab:96:0c	192.168.1.71
iPhone13	12:5d:92:9a:f8:8d	192.168.1.70

User Name ⇅	IP Address ⇅	User Group ⇅	Duration ⇅	Traffic Volume ⇅	
zhangsan	192.168.1.70		5s	57.53 KIB	Radius Single S
zhangsan	192.168.1.71		36s	56.53 MIB	Radius Single S



b) 变更动作:

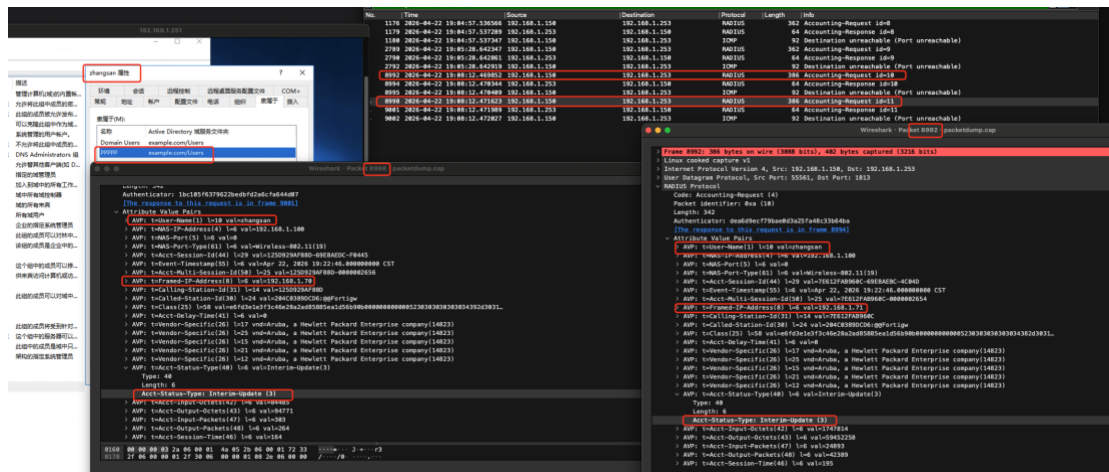
将域账号 zhangsan 加入 PPPPP 组, 19:07:40

观察是否会通过 RADIUS Accounting Update 更新 Firewall User Group, ClearPass 抓包。

c) 测试结果:

发现在 ClearPass 发至 Fortigate 报文中, 并未携带已经变更了 zhangsan 域账号信息的 Filter-Id 字段;

ClearPass 关于 AD 的 Cache Timeout:1s



(五) 测试中的常见问题 FAQ

问: FortiGate 是通过什么机制将用户表象加载到 Firewall Users 中的?

答: 根据 FortiGate 配置的 RSSO 参数(包括 key、attribute、port 等), 收到匹配的 Accounting Start 报文, 即添加至 Firewall Users;

问: 在 FortiGate Firewall Users 用户表象存活周期是多久?

答: 取决于 AAA 服务器(本文中是 ClearPass)发送的 Accounting Start 报文与 Accounting Stop 报文, 一旦 FortiGate 收到 stop 即刻删除 Firewall Users 中对应的用户条目。

问: 域账号在线时, “User Group” 是如何更新的?

答: 不更新, FortiGate 只通过识别 Accounting start 报文中的属性更新, 不参考 Accounting update 报文内容。只有重新触发

Accounting start 会更新。

问：如果 FortiGate 持续收不到 Accounting Stop 报文，用户表象会维持多久？

答：默认情况下 8 小时超时，可以根据配置参数调整；配置参数如下：

```
config user radius
  edit "RSSO"
    set timeout 5
    set rso enable
    set rso-radius-server-port 1813
    set rso-radius-response enable
    set rso-validate-request-secret enable
    set rso-secret 12345678
    set rso-endpoint-attribute User-Name
    unset rso-endpoint-block-attribute
    set sso-attribute Filter-Id //此文档中使用了该属性
    set rso-context-timeout 28800 //RSSO 超时，默认 8 个小时，范围<0>
to <4294967295>，最大约 49710 天
    set rso-flush-ip-session enable// accounting stop 报文发送时清除
会话。
    set rso-ep-one-ip-only disable
  next
end
```

问：域账号的 memberOf 属性信息在什么报文中存在？

答：此文档是 ClearPass 在 RADIUS Accounting Request 报文（类型包含 start、interim-update、stop）中将域账号在 AD 中的 memberOf 信息填充在 RADIUS Attribute: Filter-Id 字段；

问：多个终端使用同一账号时，并保持在线状态。期间在 AD 调整了域账号的组信息，ClearPass 会如何发送 Accounting update？

答：根据测试过程抓取的 RADIUS 报文分析，ClearPass 会在后续的

interim-update 报文，保持与 start 报文 Filter-Id 内容一致，不会再次查询 AD 中域账号的 memberOf 信息；每个终端仍然有对应 Accounting 报文。