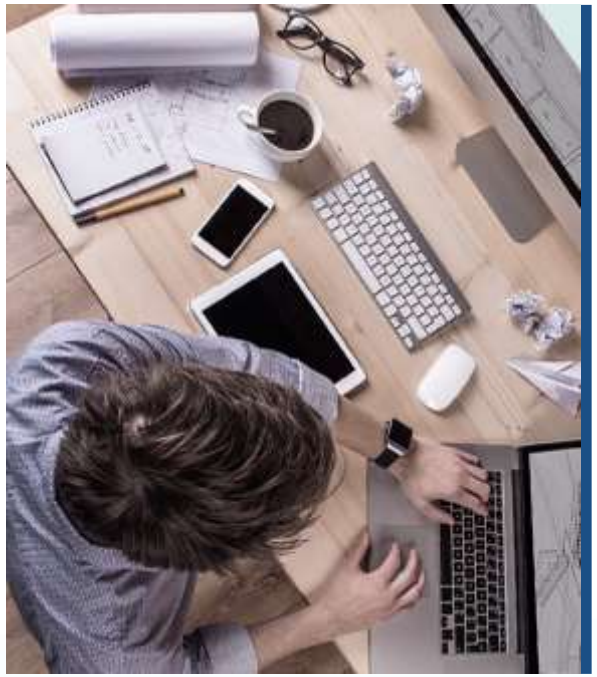
SANGFOR

04 Authentication

IAG 13.0.80 - Associate



Background of the Authentication Function

The authentication function is mainly used to verify the identity of users who have accessed the Internet through IAG devices. The authentication function can identify the identity of the intranet users and provide a basis for subsequent traffic management, user access rights policies, and application auditing.

PART 1

Authentication Method Introduction

Authentication Introduction

Users shown in IAG device are end users who access the Internet through IAG device. Therefore, users are basic units allocated with network access privileges. The administrators can manage users and their access privileges through [Group/User] page.

SANGFOR IAG authentication types:

1. Open authentication，Authentication based on IP, MAC, Hostname
2. Username/Password based authentication
3. SSO Authentication
4. DKEY Authentication
5. SMS Authentication
6. Social media account authentication
7. QR code authentication
8. User self-registration

Authentication Introduction

1. Open authentication，Authentication based on IP, MAC, Hostname

This authentication identifies users according to source IP address, MAC address or computer name.

The advantage of this authentication is the authentication dialogue will not appear to require users to type username and password. Therefore, users will not perceive the existence of the IAG device.

The disadvantage of this authentication is it cannot identify specific name for user, thus it cannot locate specific user of network behaviors, especially in an environment where addresses are dynamically allocated. In this situation, inaccurate access controls might be implemented on user.

Authentication Introduction

2. Username/Password based authentication

For username/password based authentication, user will be redirected to IAG's identity authentication system page in web browser before they can access to the Internet. There are two types of password based authentication, namely password authenticated on local computer and on external authentication server.

After user enters his username and password, IAG will check if the username is correct according to the local user list. If it fails to find the user in local user list, device will check its username and password on the external authentication server.

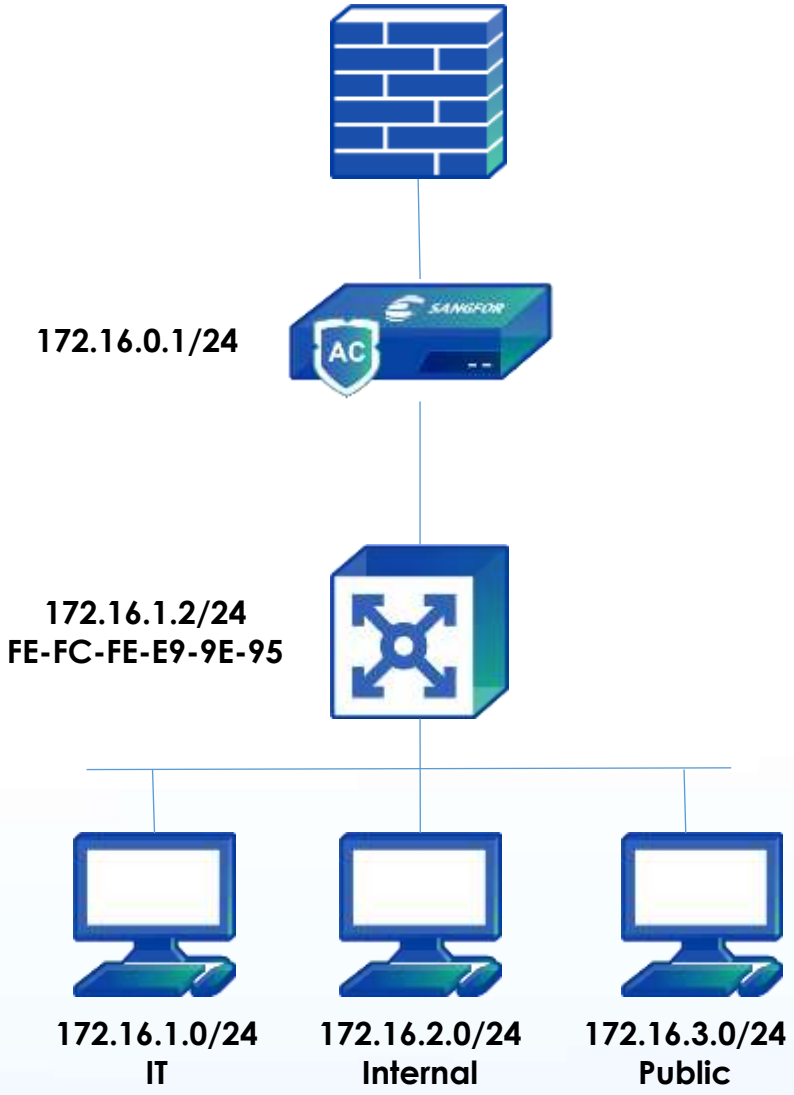
You can manually create users on IAG or use a user account that is available in external authentication server.

**SANGFOR IAG supports LDAP, RADIUS, POP3, Database, H3C CAMS, H3C IMC

Requirement Background

Requirement 3：

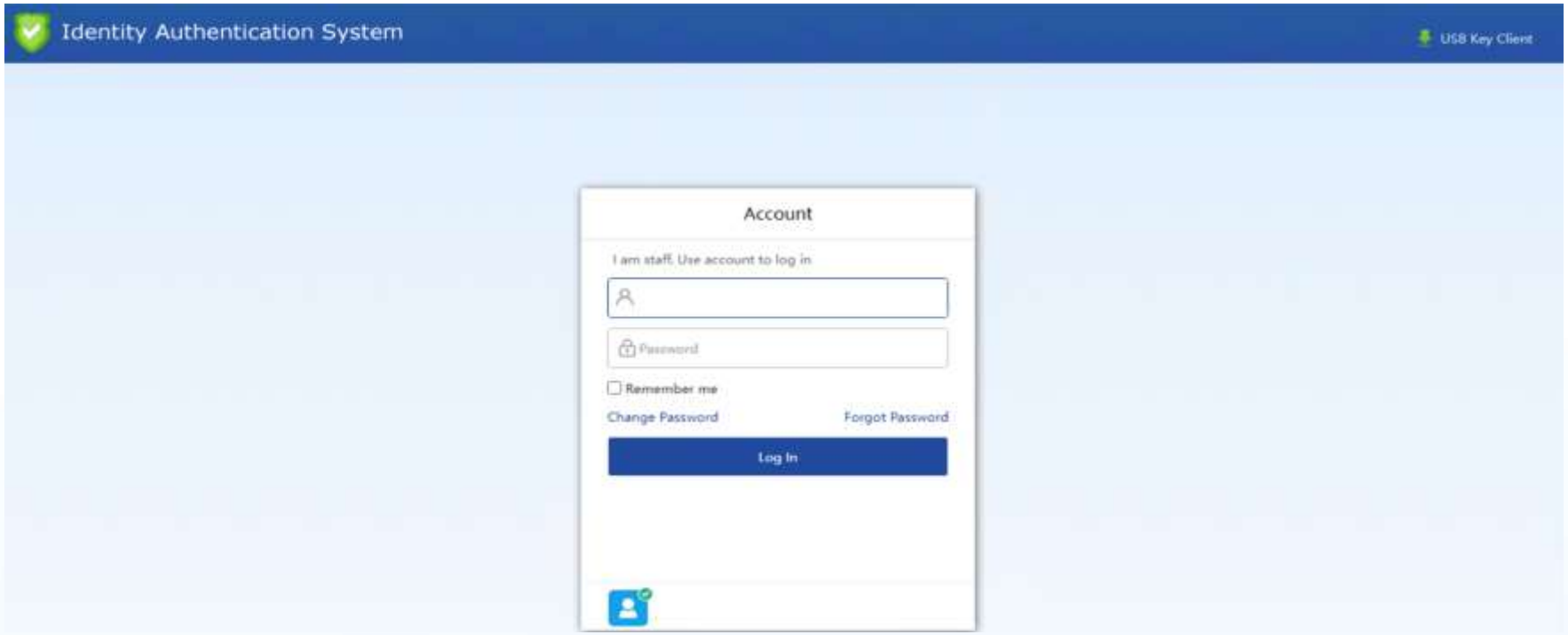
In the public Internet area, you need to enter an account number and password to access the Internet to ensure that network behavior can be tracked.



Requirement Background

When the user surfs the Internet for the first time, the user will be required to submit the username and password information. If the username and password information submitted by the user is consistent with the local (or third-party server) the authentication will be passed.

Generally, it is suitable for scenarios that require strict authentication requirements, wish to record specific accounts in the Internet log, or wish to combine authentication with the customer's existing third-party server.

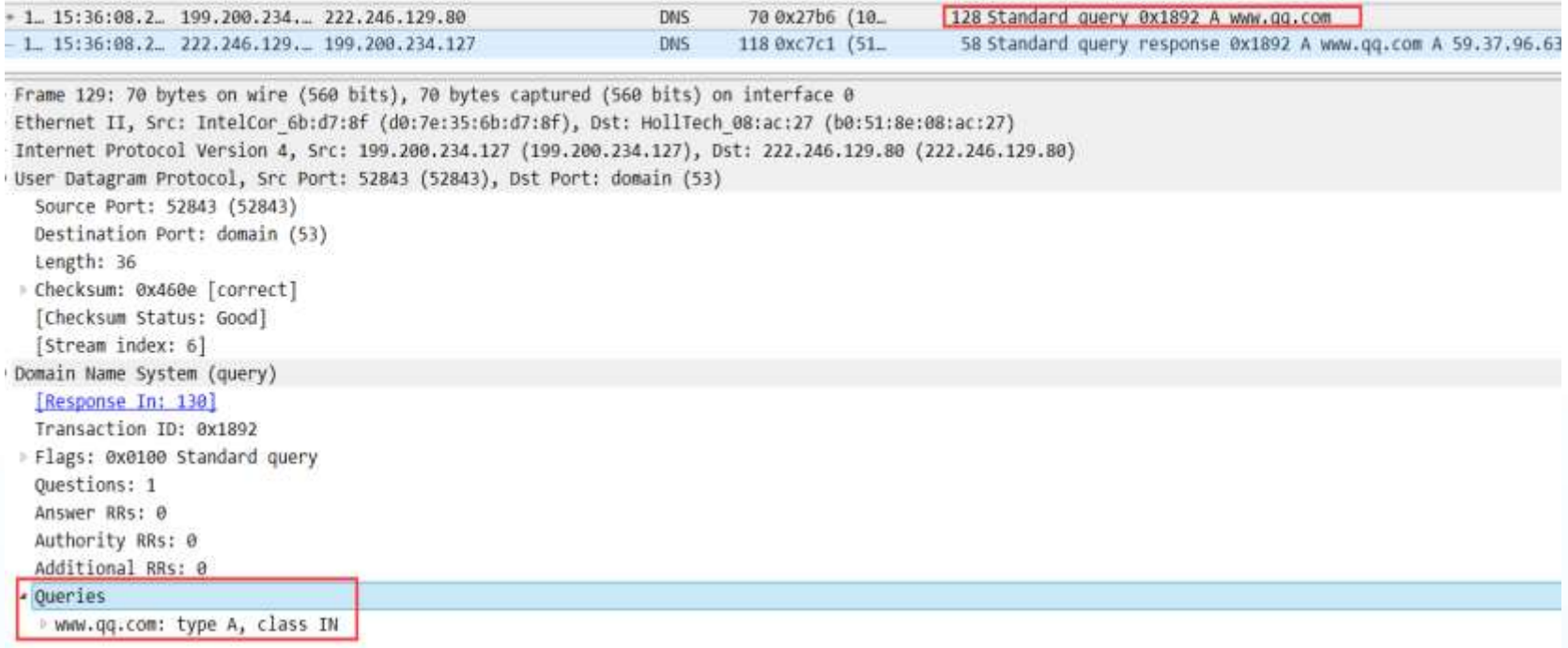


Visit Website Analytics

Step 1: Browser analysis of URLs in hyperlinks

Step 2: DNS request

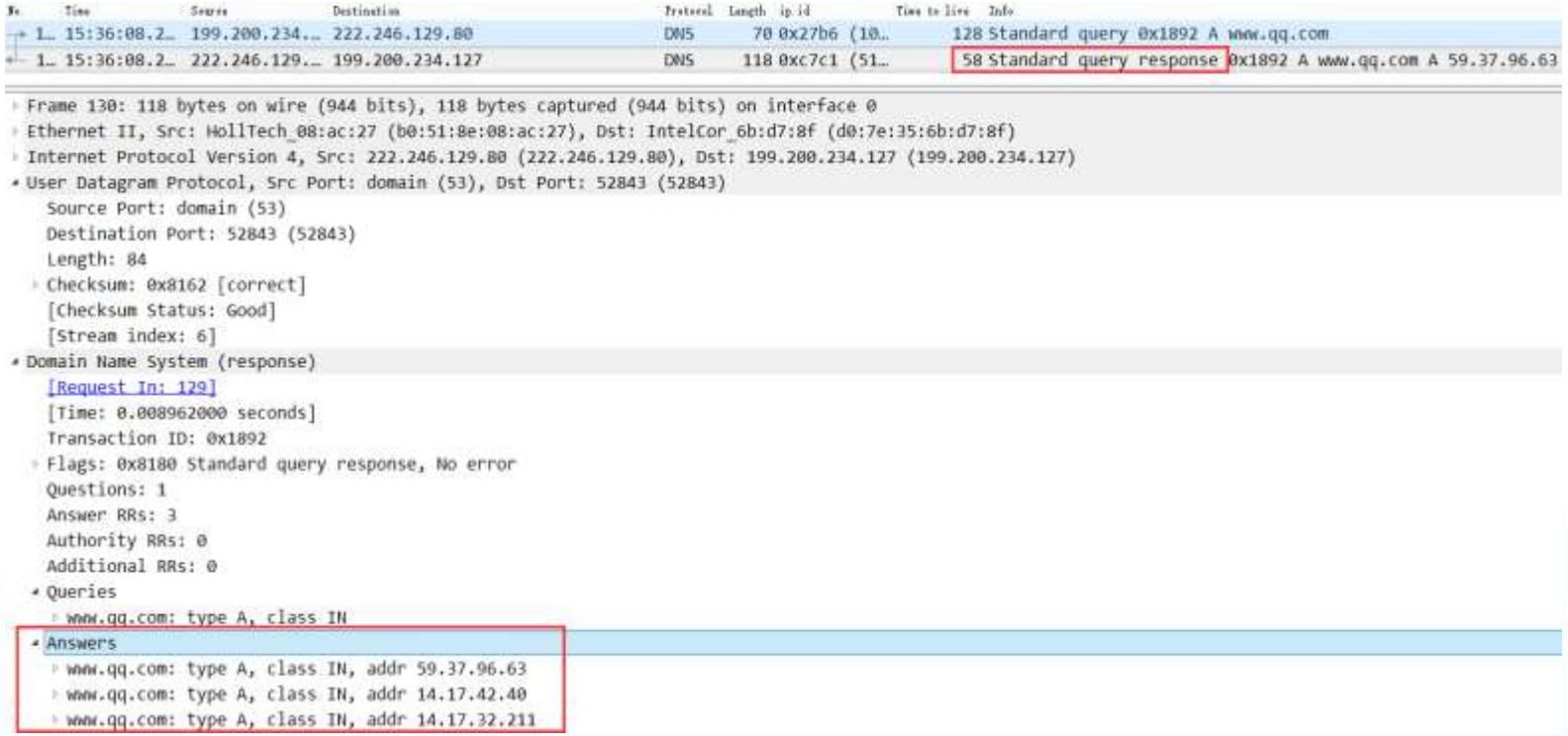
The PC sends a DNS QUERY request to the DNS server 222.246.129.80, requesting the A record of www.qq.com.



Visit Website Analytics

Step 3: DNS response

The DNS server 222.246.129.80 replies to the DNS response, and resolves the three A records 59.37.96.63, 14.17.42.40/14.17.32.211 corresponding to the domain name www.qq.com



DNS A record: resolves the hostname to the corresponding IP

Visit Website Analytics

Step 4: The PC initiates a tcp three-way handshake to the resolved www.qq.com server address

Source	Destination	Protocol	Length	ip.id	Time to live	Info
199.200.234.127	59.37.96.63	TCP	74	0x102a (41…	128	52897→80 [SYN] Seq=2090988732 Win=65535 Len=0 MSS=1460 W
59.37.96.63	199.200.234.127	TCP	74	0x0000 (0)	54	80→52897 [SYN, ACK] Seq=1952991786 Ack=2090988733 Win=14
199.200.234.127	59.37.96.63	TCP	66	0x102b (41…	128	52897→80 [ACK] Seq=2090988733 Ack=1952991787 Win=262144

Step 5: The PC sends a GET request to the www.qq.com server to request the homepage

```
1… 15:36:08.2… 199.200.234.127  59.37.96.63       TCP    74 0x102a (41…  128 52897→80 [SYN] Seq=2090988732 Win=65535 Len=0
1… 15:36:08.3… 59.37.96.63      199.200.234.127  TCP    74 0x0000 (0)    54 80→52897 [SYN, ACK] Seq=1952991786 Ack=209098
1… 15:36:08.3… 199.200.234.127  59.37.96.63       TCP    66 0x102b (41…  128 52897→80 [ACK] Seq=2090988733 Ack=1952991787
1… 15:36:08.3… 199.200.234.127  59.37.96.63       HTTP  419 0x102c (41…  128 GET / HTTP/1.1

Frame 135: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface 0
Ethernet II, Src: IntelCor_6b:d7:8f (d0:7e:35:6b:d7:8f), Dst: HollTech_08:ac:27 (b0:51:8e:08:ac:27)
Internet Protocol Version 4, Src: 199.200.234.127, Dst: 59.37.96.63
Transmission Control Protocol, Src Port: 52897, Dst Port: 80, Seq: 2090988733, Ack: 1952991787, Len: 353
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Accept: text/html, application/xhtml+xml, */*\r\n
  Accept-Language: zh-CN\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; .NET CLR 3.5.30729; .NET C
  Accept-Encoding: gzip, deflate\r\n
  Host: www.qq.com\r\n
  DNT: 1\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://www.qq.com/]
  [HTTP request 1/3]
  [Response in frame: 354]
  [Next request in frame: 2275]
```

Visit Website Analytics

Step 6: The www.qq.com server responds with HTTP/1.1 200 OK and returns the home page packet

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: zh-CN
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; .NET CLR
3.5.30729; .NET CLR 2.0.50727; .NET CLR 3.0.30729; max-meeting-user)
Accept-Encoding: gzip, deflate
Host: www.qq.com
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: squid/3.5.20
Date: Fri, 11 Nov 2016 07:36:06 GMT
Content-Type: text/html; charset=GB2312
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Expires: Fri, 11 Nov 2016 07:37:06 GMT
Cache-Control: max-age=60
Vary: Accept-Encoding
Content-Encoding: gzip
Vary: Accept-Encoding
X-Cache: MISS from shenzhen.qq.com

faa
............yw.G.(.7>..!.8..^..K.....ns......~}t.2.TiJUE-BB.......q.....B...M !..........^1..B.>/.......*
...A.T..q....7n.....1{v...=.]*6.K.....H%.<..;X...;..Y.      ..Z
]2*..Un....p.......^.[.....)j..jT...M{.7.....;R.b.....t.`K...`Uo.....Z....2.P...(Y.o.uwb....M......F..
6...N0zI...SP...;`....D.b...r.Q......u....5.1a.S..U...&z..z.;.R..~....R..}b
....Z-Y?...17..vU.v....
..XW.....Q.%.u..e. .^:tHZ..k.........z..=.v?..;....e.........?.
{..C{..<.....J..v........w..V.V.C.=.c.....zf.../...}../>{h..{.......C{*...5...
+.C{vl.:.e.b.......q[.~T....?.....mb..D}...$...Y....?.&e.V..C?D...s.J.:t..........E_I7..Y..H....5kD... .1...>...?
```

Step 7: Complete the data interaction process, 4-way handshake to disconnect

HTTP Request Method

Request message method

Method is the operation performed on the requested object, that is, some commands. The operations in the request message are:

Method(Operation)	Meaning	Method(Operation)	Meaning
GET	Request to read a web page	HEAD	Request to read the header of a web page
POST	Attach a named resource (such as a web page)	PUT	Request to store a web page
DELETE	Delete web page	TRACE	For testing, asking the server to send back the received request
CONNECT	For proxy server	OPTION	Query specific options

POST Request Method

POST - Submit data to be processed to the specified resource

```
1Y.|....6sU..;.-.....*.?......f...POST /member.php?mod=logging&action=login&loginsubmit=yes&handlekey=post&loginhash=LlmjM&inajax=1 HTTP/1.1
Host: bbs.sangfor.com.cn
Connection: keep-alive
Content-Length: 159
Cache-Control: max-age=0
Origin: http://bbs.sangfor.com.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://bbs.sangfor.com.cn/plugin.php?id=info:index
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: gr_user_id=53345538-f240-4178-bceb-84de4f25f881; UM_distinctid=15be598ebc618f-09af4d91a3bb63-62101a75-144000-15be598ebc7436;
Hm_lvt_0e8161ac4f393ecc79c975079cc5fcc8=1494207748,1494209478,1494323977,1494385739; Udvb_2132_rid=25065765422567599; Df1w_2132_saltkey=k828uVJ8;
Df1w_2132_lastvisit=1494911132; CNZZDATA1254045219=394365775-1494203502-%7C1494912229; Df1w_2132_lastact=1494914734%09member.php%09logging;
Df1w_2132_sid=LZo1Id

formhash=1b50e104&referer=http%3A%2F%2Fbbs.sangfor.com.cn%2Fplugin.php%3Fid%3Dinfo
%3Aindex&username=179369652%40qq.com&password=[redacted]ookietime=2592000HTTP/1.1 200 OK
Date: Tue, 16 May 2017 06:05:46 GMT
Server: Apache
Expires: -1
Cache-Control: no-store, private, post-check=0, pre-check=0, max-age=0
Pragma: no-cache
Set-Cookie: Df1w_2132_lastact=1494914746%09member.php%09logging; expires=Wed, 17-May-2017 06:05:46 GMT; path=/
Set-Cookie: Df1w_2132_ulastactivity=a5f5nW2K18RISctEuwWLrD%2FaiGvCAZTklrc90tAtIqLUfz6pgSC%2B; expires=Wed, 16-May-2018 06:05:46 GMT; path=/
Set-Cookie: Df1w_2132_sid=LZo1Id; expires=Wed, 17-May-2017 06:05:46 GMT; path=/
Set-Cookie: Df1w_2132_auth=d6e8MuNBHtemHQeaFpkQb5H1kxlW45cY2fvHOWLMbARUtW5WCJew3vyMRADaE4P1gVgL2DyBlHQ9UWP19JNXk94; expires=Thu, 15-Jun-2017 06:05:46
GMT; path=/; httponly
Set-Cookie: Df1w_2132_loginuser=deleted; expires=Mon, 16-May-2016 06:05:46 GMT; path=/
Set-Cookie: Df1w_2132_activationauth=deleted; expires=Mon, 16-May-2016 06:05:46 GMT; path=/
Set-Cookie: Df1w_2132_pmnum=deleted; expires=Mon, 16-May-2016 06:05:46 GMT; path=/
Set-Cookie: Df1w_2132_lastcheckfeed=142%7C1494914746; expires=Wed, 16-May-2018 06:05:46 GMT; path=/
Set-Cookie: Df1w_2132_checkfollow=1; expires=Tue, 16-May-2017 06:06:16 GMT; path=/
Set-Cookie: Df1w_2132_lip=175.11.88.173%2C1494914725; path=/
Cache-Control: no-store, private, post-check=0, pre-check=0, max-age=0
```

HTTP Response

Response message status-code

Status-Code is a 3-digit number included in the status line of the response message, indicating whether a particular request was fulfilled, and if not, why. Status codes are divided into the following five categories :

Status code	Meaning	Example
1xx	Notification information	100=Server is processing client request
2xx	Success	200=The request was successful (OK)
3xx	Redirect	301=Page changed position
4xx	Client error	403=Forbidden page; 404=page not found
5xx	Server error	500=internal server error; 503=try again later

HTTP Header

header field or message header

header	Type	Illustrate
User- Agent	request	Information about the browser and its platform, such as Mozilla 5.0
Accept	request	The type of page the client can handle, e.g. text/html
Accept-Charset	request	A character set acceptable to the client, such as Unicode-1-1
Accept-Encoding	request	A page encoding method that the client can handle, such as gzip
Accept-Language	request	Natural languages that customers can handle, such as en (English), zh-cn (Simplified Chinese)
Host	request	DNS name of the server. Extracted from URL, required.
Referer	request	The user accesses the currently requested page from the page represented by the URL.
Cookie	request	Send the previously set cookie back to the server, which can be used as session information.
Date	both	Date and time when the message was sent
Server	response	Information about the server, such as Microsoft-IIS/6.0
Content-Encoding	response	how the content was encoded (eg gzip)
Content-Language	response	The natural language used by the page
Content-Length	response	page length in bytes
Content-Type	response	MIME type of the page
Last-Modified	response	Web page last modified date and time, it is meaningful for the cache
Location	response	Redirect to other URL
Set-Cookie	response	Server need client store a cookie

UA Field

User-Agent: Browser type (OS ID; Encryption Level ID; Browser Language) rendering Engine ID Version Information.

```
GET / HTTP/1.1
Host: www.qq.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
58.0.3029.110 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: RK=SBGymg0uZp; pgv_pvi=2504480768; pac_uid=1_179369652;
rv2=80FFB6BC0109F0A27719A952C3227E1DFF4C09B4823C87F5FC;
property20=1306C920DFB75EC8636B8F6CF8B0FF8538092D9D29AD7D80E53606D9CA7DB866FB4802BDD0DB9C4E;
qz_gdt=zfpruwlhaaacur3rd5ma; ts_uid=5261623201; qv_als=GHau2mU1t77B0rSJA11494914934R020Pw==;
tvfe_boss_uuid=51702bfe7bd72710; o_cookie=179369652; pgv_info=ssid=s3581387376; pgv_pvid=8621361160;
pgv_si=s9327318016; _qpsvr_localtk=0.9080250126742624; ptisp=ctc;
ptcz=fb14567159e1591c7a42bba8105964b9e998545c780ac2920eaeb6ceabb43170; pt2gguin=o0179369652;
uin=o0179369652; skey=@71x944TDP
```

Server Field

Server: The response header contains software information about the origin server that handled the request

```
GET /c/guojixinwen.js HTTP/1.1
Host: www.qq.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like
Accept: */*
Referer: http://www.qq.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: RK=SBGymg0uZp; pgv_pvi=2504480768; pac_uid=1_179369652; rv2=80FFB6BC01C
property20=1306C920DFB75EC8636B8F6CF8B0FF8538092D9D29AD7D80E53606D9CA7DB866FB48
qv_als=GHau2mUlt77BOrSJA11494914934RO2OPw==; tvfe_boss_uuid=51702bfe7bd72710; p
_qpsvr_localtk=0.9080250126742624; ptisp=ctc; ptcz=fb14567159e1591c7a42bba81059
pt2gguin=o0179369652; uin=o0179369652; skey=@71x944TDP; pgv_info=ssid=s35813873
pgv_pvid=8621361160; o_cookie=179369652; ts_uid=5261623201; ad_play_index=18

HTTP/1.1 200 OK
Server: squid/3.5.20
Date: Thu, 18 May 2017 03:13:37 GMT
Content-Type: application/javascript; charset=GB2312
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Expires: Thu, 25 May 2017 03:13:37 GMT
Cache-Control: max-age=604800
Vary: Accept-Encoding
Content-Encoding: gzip
Vary: Accept-Encoding
X-Cache: HIT from shenzhen.qq.com
```

Referrer Field

Referrer: The browser indicates to the WEB server from which page/URL it got/clicked the URL/URL in the current request.

```
GET / HTTP/1.1
Host: health.qq.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
Referer: http://www.qq.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: RK=SBGymg0uZp; pgv_pvi=2504480768; pac_uid=1_179369652; pt2gguin=o01
ptisp=ctc; ptcz=fb14567159e1591c7a42bba8105964b9e998545c780ac2920eaeb6ceabb4
rv2=80FFB6BC0109F0A27719A952C3227E1DFF4C09B4823C87F5FC;
property20=1306C920DFB75EC8636B8F6CF8B0FF8538092D9D29AD7D80E53606D9CA7DB866F
pgv_info=ssid=s3581387376; pgv_pvid=8621361160; o_cookie=179369652
```

HTTP Redirection

Location: The WEB server tells the browser that the object you are trying to access has been moved to another location and go to the location specified by the header to retrieve it.

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.baidu.com
DNT: 1
Connection: Keep-Alive
Cookie: BD_UPN=1126314551; ispeed_lsm=6; BAIDUID=06DEF25F8520F5F32889DF58B1BA2E5C:FG=1;
BIDUPSID=06DEF25F8520F5F32889DF58B1BA2E5C; PSTM=1494141005;
__cfduid=db940c72a3a66834ba1eae62432e14ea31494141011

HTTP/1.1 302 Moved Temporarily
Date: Tue, 16 May 2017 06:12:34 GMT
Content-Type: text/html
Content-Length: 215
Connection: Keep-Alive
Location: https://www.baidu.com/
Server: BWS/1.1
X-UA-Compatible: IE=Edge,chrome=1
Set-Cookie: BD_LAST_QID=15871331934698220647; path=/; Max-Age=1
```

Password Authentication Case Study

First, we take the visit www.qq.com as an example to review the data flow process of password authentication

Step 1: The PC first performs the DNS resolution process of www.qq.com
Step 2: The PC initiates a tcp three-way handshake to the resolved www.qq.com server address

Step 3: The PC sends a GET request to the www.qq.com server to request the homepage
Step 4: IAG intercepts the PC's GET request, and disguises the IAG as a server (using the Tencent server's IP to send packets to the PC), replies to the PC with HTTP 302 Moved Temporarily, and asks the PC to redirect the request to the following URL
http://10.1.3.4:80/ac_portal/proxy.html?template=default&tabs=pwd&vlanid=0&url=http://www.qq.com%2f
10.1.3.4 is the LAN IP, bridge IP or virtual IP of the IAG device

Step 5: The PC is automatically redirected to access the authentication interface of the AC, enter the correct account and password, and the login is successful.

Password Authentication Case Study

SANGFOR

```
GET / HTTP/1.1
Host: www.qq.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/52.0.2743.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
ts_refer=10.1.3.4/ac_portal/disclaimer_noad/pc.html%3Ftemplate%3Ddisclaimer_noad%26tabs%3Dany%26
vlanid%3D0%26url%3Dhttp%3A//www.qq.com%252f; pac_uid=1_774148569;
ptcz=e4269a5a85053a1eaf0309388433e92ca9694f193772dc92ddc78875ddf409ad; pt2gguin=o0774148569;
ptui_loginuin=774148569; pgv_pvi=3078745088; pgv_pvid=5687473024; o_cookie=774148569;
ts_uid=8334306400
HTTP/1.0 302 Moved Temporarily
Location:
http://10.1.3.4:80/ac_portal/proxy.html?template=default&tabs=pwd&vlanid=0&url=http://www.qq.com%2
f
Content-Type: text/html;
Content-Length: 14
<h2>Moved</h2>
```

Password Authentication Configuration

1. First, create a user group for users in the office area. In [Users] - [Users] - [Local Users], click Add, select [Group], and define the group name: public area

2. Create user, set local password

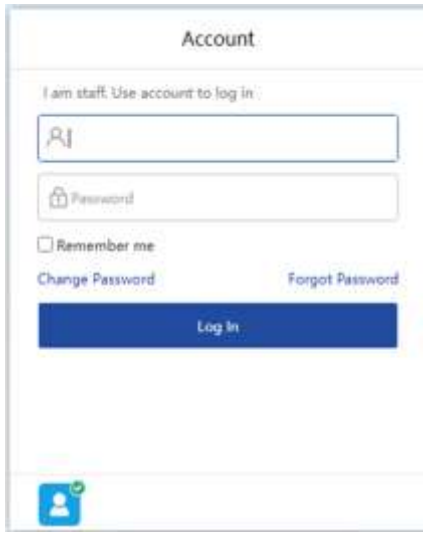
3. Add [Authentication policy], select password-based authentication

4. [Advanced]-[Other option], select [DNS service is available even user is not authenticated of is locked]

What will happen if no select [DNS service is available even user is not authenticated of is locked] ?

Password Authentication Effect Display

1. When the user goes to the Internet, open the website and redirect to the authentication interface



2. Enter the username and password. After the user authentication is completed, you can see that the user has been successfully online in the online user list.

Members

No.	Username(Alias)	Group	IP Address	Endpoint Type	Auth Method	Ingress Client	Check Result	Time Logged In...	Online Duration
1	test	/	10.10.10.10	PC(Windows PC)	User Account	Installed	-	2022-03-14 11...	24 seconds

Summary of Password Authentication

If “authentication page” not showing，how to troubleshoot?

First confirm the network environment, and manually open whether it can be opened

1、 Whether the virtual address deployed by the bridge conflicts with the intranet, and whether the PC browser acts as an Internet proxy.

2、 Are there any restrictions on the devices connected to the IAG?

3、Need to enable option “DNS service is available even user is not authenticated of is locked”

4、If the website you visit is https, you need to enable [Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated]

5、 HTTP applications and dns applications cannot be rejected according to the associated Internet policy.

6、Firewall rules cannot deny ports 80 and 53 [System]-[Firewall rules]-[LAN-WAN]

Summary of Password Authentication

If deployed in device bridge mode in an environment with a 30-bit mask, will the redirect page still pop up?

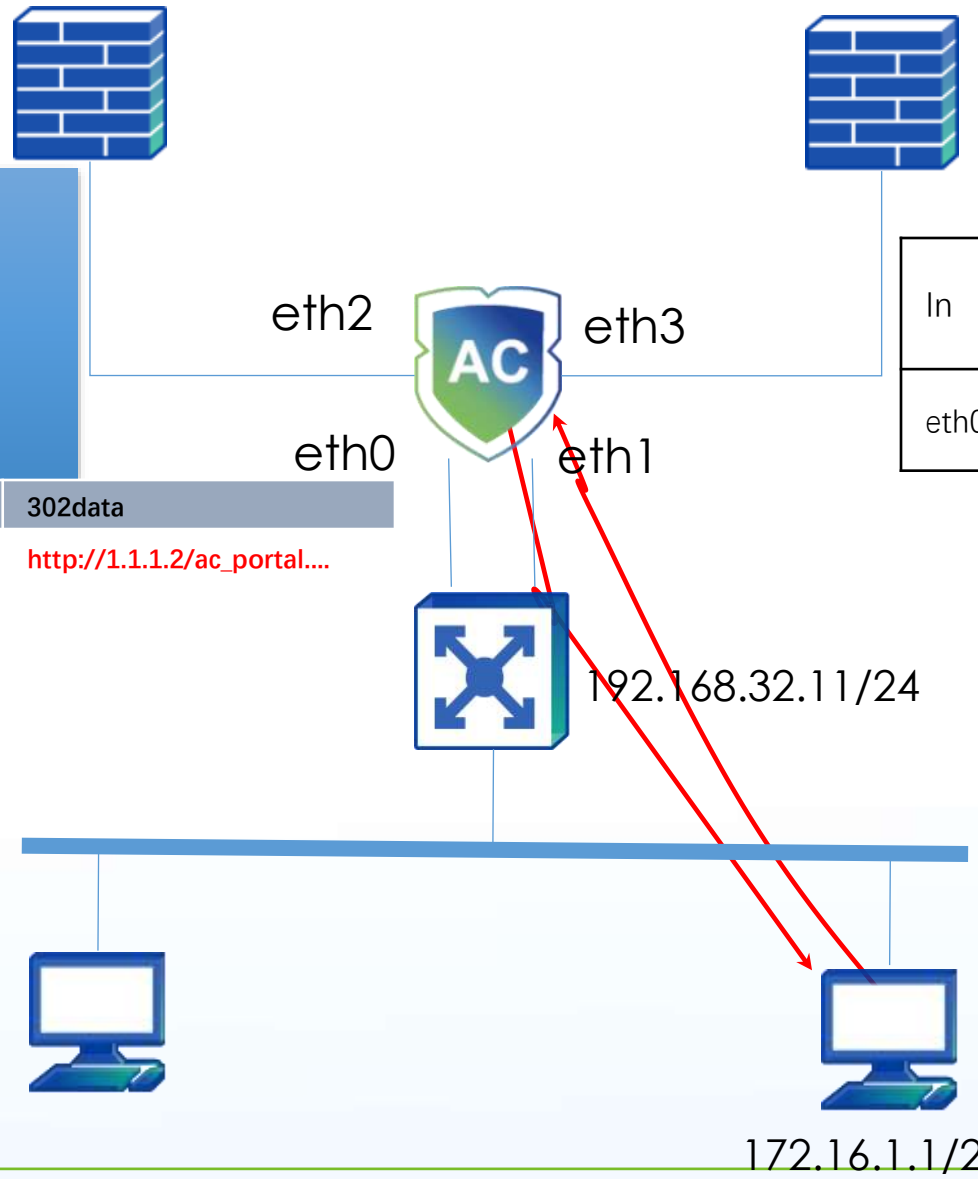
Redirection

Virtual IP redirection：When the HTTP Internet access data before the authentication of the intranet PC passes through the IAG, the IAG intercepts and records the source, destination IP, encapsulation type of the data packet, and the interface when the data packet enters the IAG. When IAG bounces the redirection authentication page of the portal, it will reverse the source and destination IP of the recorded data packet, and then send it directly from the interface where the data packet entered, and the data field in the data packet will be replaced with the IAG virtual IP. The redirect URL address. (IAG only has virtual IP redirection in bridge mode)

DMZ redirection：When the HTTP Internet access data before the authentication of the intranet PC passes through the IAG, the IAG intercepts the data packets. The IAG searches the routing table of its own DMZ port and sends the redirected authentication page of the portal from the DMZ port. The data fields in the data packets are replaced with the redirect URL address of the DMZ port IP of the IAG. (It is generally used to redirect from the DMZ port when there is no available bridge IP.)

The redirect page does not check the IAG routing table and directly returns packets from the network port eth0 where the data comes in to the intranet

out	Sip	Dip	302data
eth0	121.14.85.198	172.16.1.1	http://1.1.1.2/ac_portal....



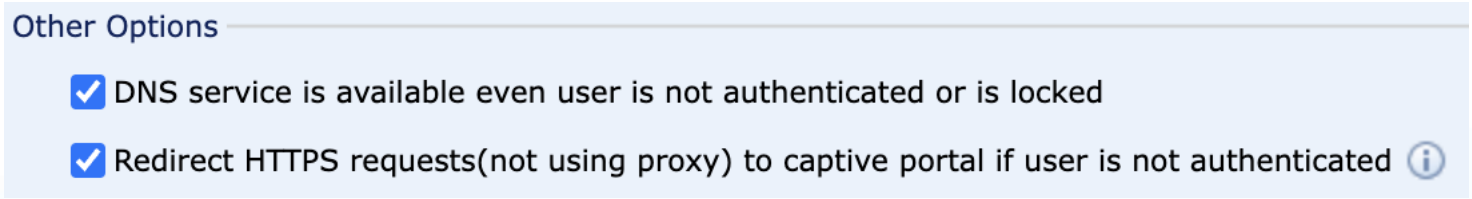
In	Out	SIP	DIP
eth0	eth2	172.16.1.1	121.14.85.198

Password Authentication Precautions

1、 If the post-authentication process requires the user to bind a mac address, it is necessary to pay attention to whether the intranet is a Layer 3 environment, and if so, enable cross-layer 3 mac address recognition.

2、 If the intranet is a DHCP scenario, do not check the bind IP address.

3、 If users open the HTTPS website to be able to redirect to the authentication page, they need to check the following options in [Authentication Options]



Authentication Introduction

3. Single Sign On (SSO)

SSO indicates that if the network has already deployed an authentication system, IAG device will combine the authentication system to identify users corresponding to a certain IP address. For example, if you log in to Gmail, you can directly access your Google Drive without having to authenticate again.

If user is found, he can access to the Internet, and he does not have to enter his username/password again.

At this moment, the following SSO types are supported:
Active Directory Domain SSO
Script SSO
IWA SSO
Radius SSO
SANGFOR Appliance SSO

Authentication Introduction

4. DKEY Authentication

Users adopting DKEY authentication has to submit their user information for records which will be saved in DKEY (SANGFOR DKEY pendrive). The DKEY will then identify user according to DKEY authentication information. Among the four authentication, DKEY authentication, DKEY authentication has the highest priority.

If you insert a DKEY into a computer that has already been authenticated using other method, the identity of the computer will be changed to DKEY user automatically with its corresponding privileges.

There are two types of DKEY. One is authentication DKEY and the other is audit-free DKEY. The audit-free DKEY has not only authentication function, but also the privilege to exempt from being audited by IAG. The device will not monitor nor record user behaviors with audit-free DKEY.

Authentication Introduction

Green: For DKEY authentication

Purple: Can be supported without policy control or audit-free.

Brown: For Data Center query

Authentication Introduction

5. SMS Authentication

For some organization, it is a requirement to use genuine identity to authenticate online users within their environment. Besides, their marketing team would like to keep track of these users and their information for marketing purposes.

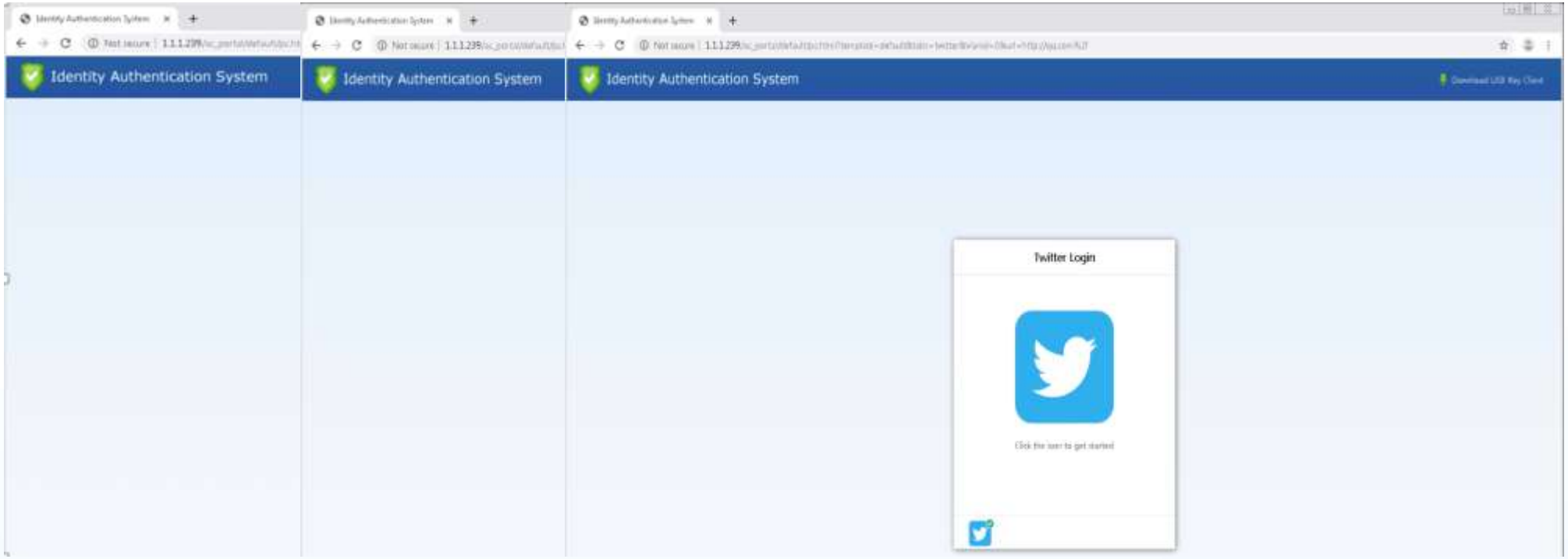
When using SMS authentication, guest users will have to fill in their handphone numbers to obtain a code generated by our IAG and it will be sent via SMS through courier service provider

Guest is required to key in the code received in order to access Internet

Authentication Introduction

6. Social media account authentication

With the development of the Internet, users have demanded rich authentication scenarios. Starting from the IAM 12.0.25 version, it supports authentication by combining four social accounts: Facebook, Gmail, Line, and Twitter.



Authentication Introduction

7. QR code authentication

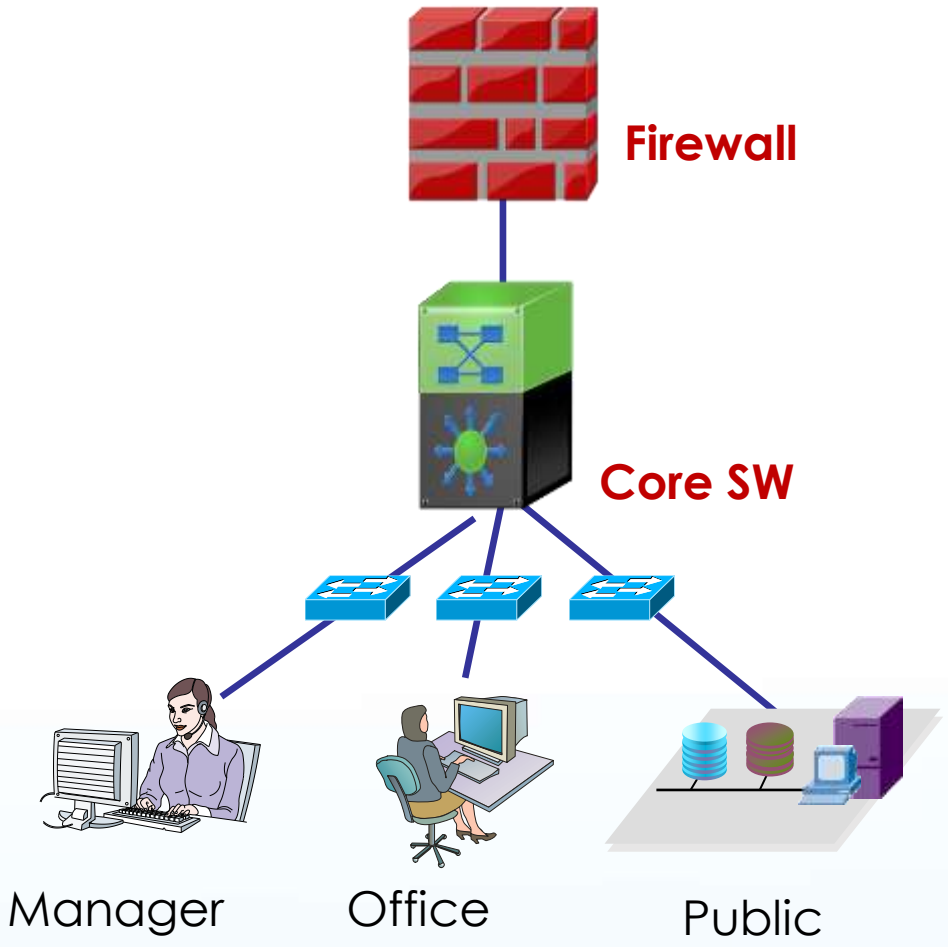
In the place of external visitors, visitors can normally access the Internet only after they have been approved by internal employees. While bringing a good experience to the visitors, the internal can also effectively manage external visitors. It is recommended to use a QR Code Based Approved Login method for internal The employee scans the QR code of each visitor to meet this scenario.

For the meeting room meeting online experience, or a small-scale online experience private experience, it is expected to achieve the meeting room or a small area, access the Internet to access the Internet, and outsiders will not be informed of the Internet access method, and introduced a conference QR Code Registered Login method

PART 2

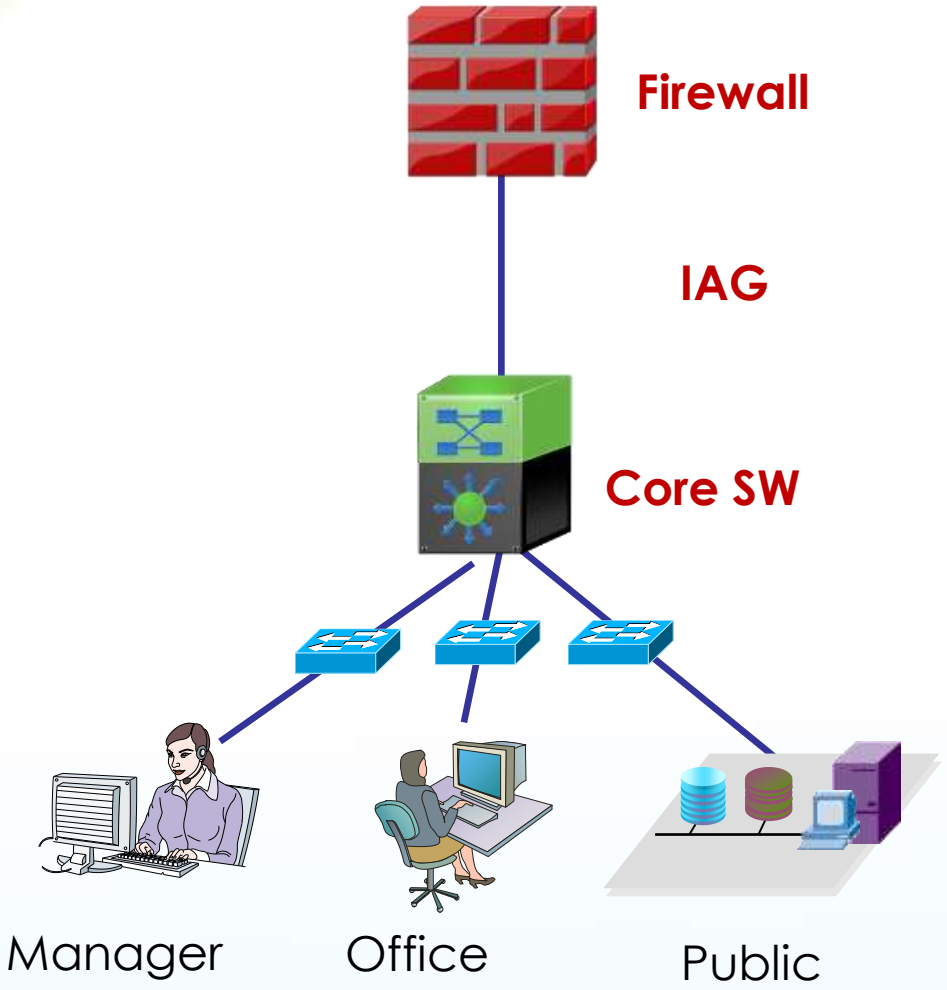
Authentication Configuration

Scenario



A company has an office area and public area. 192.168.1.0/24 IP segment cannot modify IP and MAC addresses while public access areas in 192.168.2.0/24 needs username/password. In addition, do not audit manager's Internet activities, do not audit manager's Internet activities.

Scenario



According to customer's demand, we can deploy IAG between firewall and core switch with the following requirements:

Office users use IP/MAC binding authentication method

Public users use password-based authentication.

Manager uses audit-free KEY

Configuration Steps

1. Add authentication policy

IAG device will determine user's authentication according to configured IP or MAC address.

2. Manually/automatically add new users

New users can be edited manually, you can define specific user's authentication information include username/password, enable IP/MAC binding, enable DKEY and IP/MAC binding

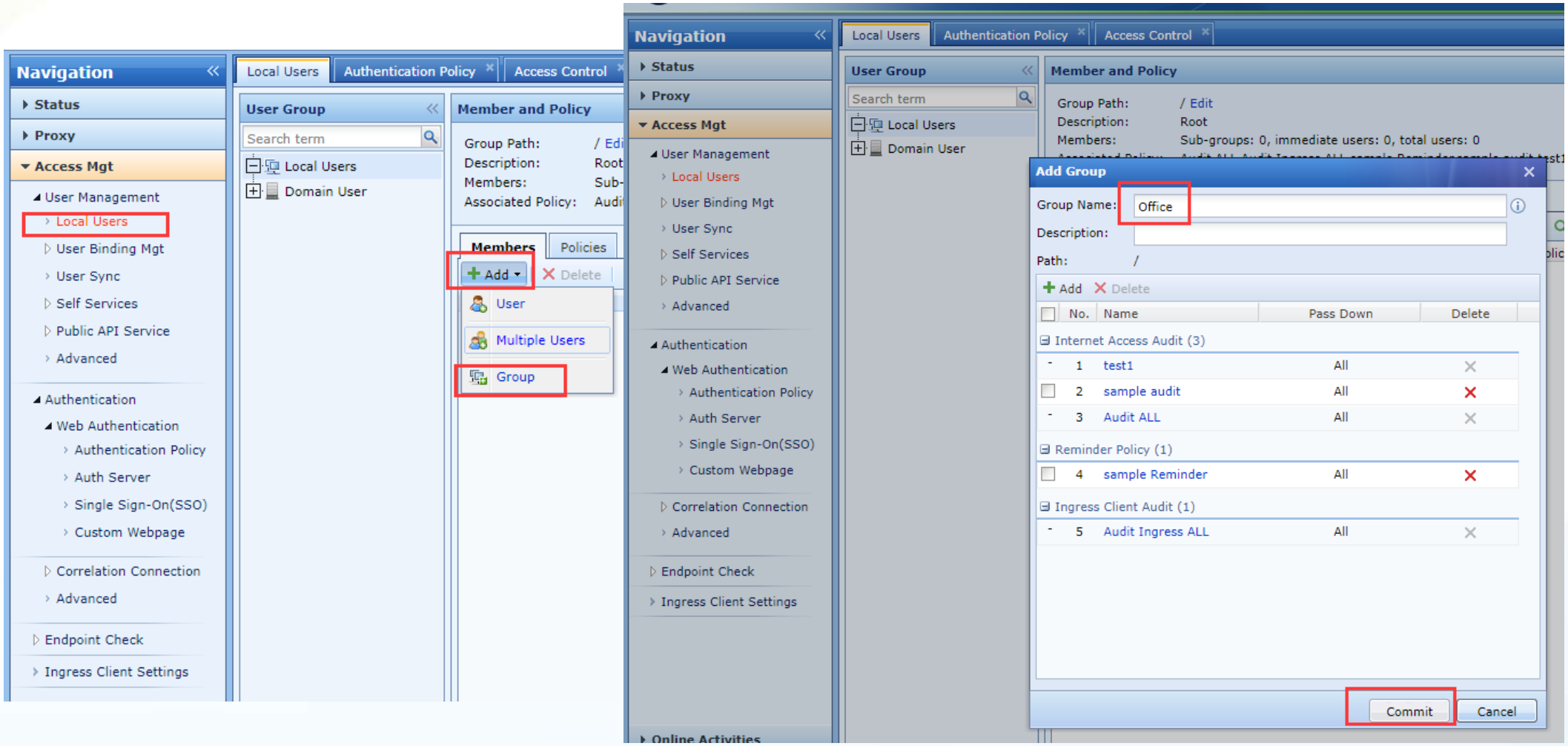
By configuring authentication policy to automatically add users.

Note：
DKEY authentication has the highest priority and do not need to enable in authentication policy.

None, Username/Password, SSO need to enable in authentication policy.

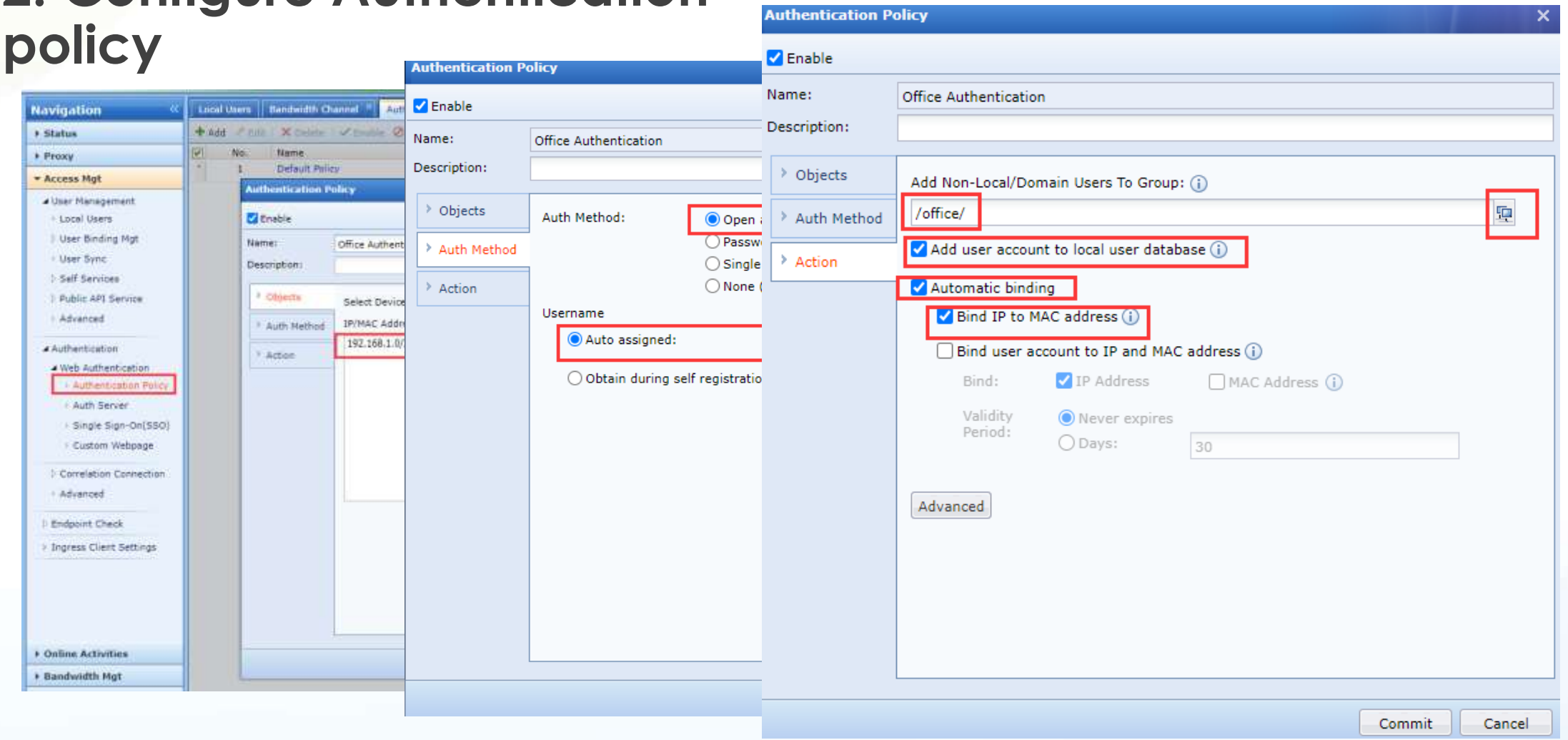
Configuration - Step 1

1. Add a group named “Office”



Configuration - Step 1

- 2. Configure Authentication policy

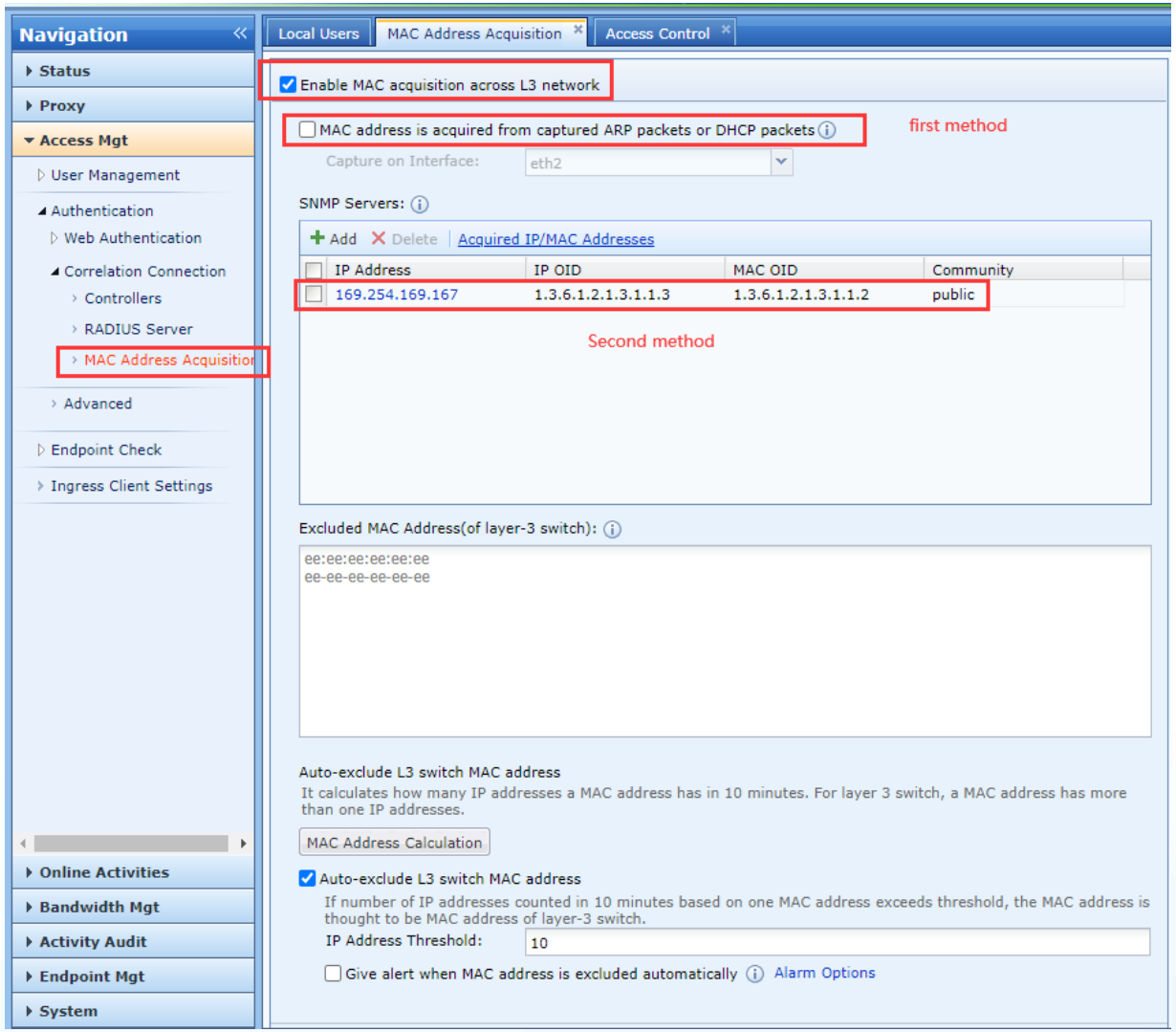


Configuration - Step 1

In addtion：if there are layer 3 core switch enviroment，we must enable “MAC Acquisition Across L3 Switch".

Why do we need enable the “MAC Acquisition Across L3 Switch”?

The data stream of the computer is transmitted to the IAG through the core switch. The source MAC address of the data packet is modified to the MAC address of the core switch interface. The IAG cannot obtain the real MAC address of the terminal from the data packet.



Demand Analysis

Problem 1:

Will the source MAC address of the data packet change after the data packet is forwarded by the Layer 2 switch?

Problem 2:

After a data packet is forwarded by a Layer 3 switch, will the source MAC address of the data packet change?

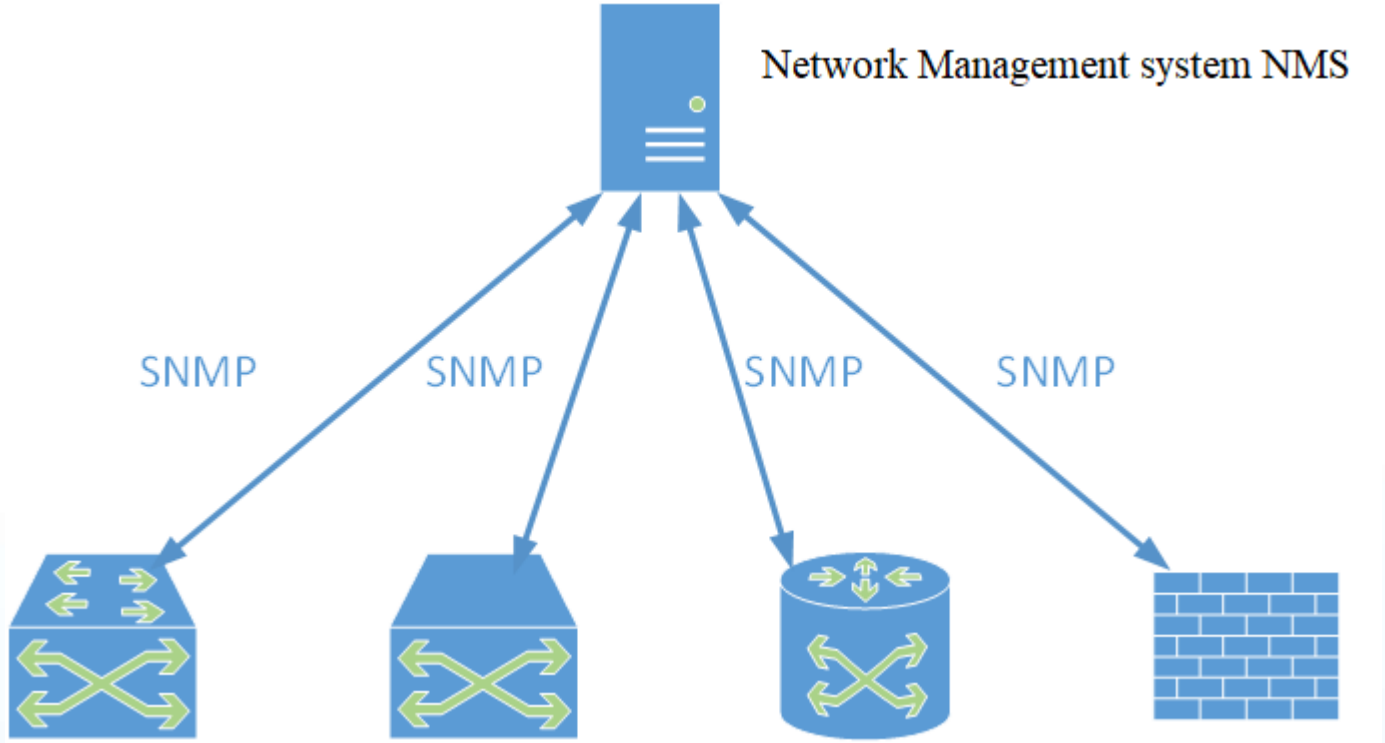
Problem 3:

How can we get the real IP/MAC entry of the terminal?

Little Knowledge for SNMP Protocol

SANGFOR

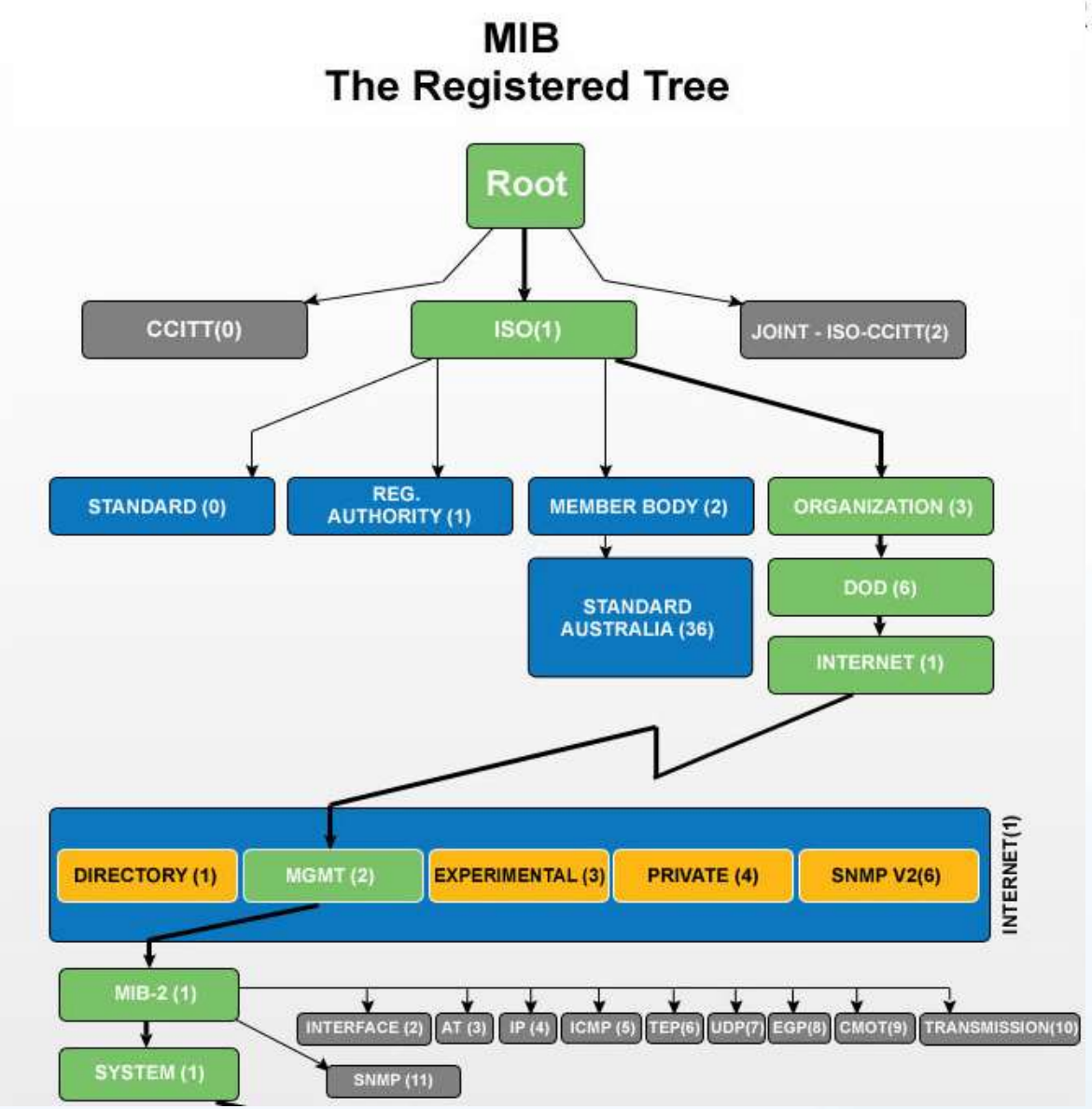
SNMP is a network management standard based on the TCP/IP protocol suite and is a standard protocol for managing network nodes (such as servers, workstations, routers, switches, etc.) in an IP network.



MIB Library

MIB library： Any managed resource is represented as an object, called a managed object.

Every OID (Object IDentification) corresponds to a unique object.



OID Value

RFC1213-MIB	atPhysAddress.1.10.1.2.1	1.3.6.1.2.1.3.1.1.2	1.10.1.2.1	String	10:0D:0E:A5:01:C2
RFC1213-MIB	atPhysAddress.1.10.1.3.102	1.3.6.1.2.1.3.1.1.2	1.10.1.3.102	String	FE:FC:FE:2F:0D:79
RFC1213-MIB	atPhysAddress.1.10.1.3.103	1.3.6.1.2.1.3.1.1.2	1.10.1.3.103	String	FE:FC:FE:8C:C3:D9
RFC1213-MIB	atPhysAddress.1.10.1.3.104	1.3.6.1.2.1.3.1.1.2	1.10.1.3.104	String	12:34:56:78:12:34
RFC1213-MIB	atPhysAddress.1.10.1.3.105	1.3.6.1.2.1.3.1.1.2	1.10.1.3.105	String	FE:FC:FE:27:B0:38
RFC1213-MIB	atPhysAddress.1.10.1.3.106	1.3.6.1.2.1.3.1.1.2	1.10.1.3.106	String	FE:FC:FE:77:81:39
RFC1213-MIB	atPhysAddress.1.10.1.3.110	1.3.6.1.2.1.3.1.1.2	1.10.1.3.110	String	FE:FC:FE:02:BF:4A
RFC1213-MIB	atPhysAddress.1.10.1.3.121	1.3.6.1.2.1.3.1.1.2	1.10.1.3.121	String	FE:FC:FE:B7:E7:96
RFC1213-MIB	atPhysAddress.1.10.1.3.123	1.3.6.1.2.1.3.1.1.2	1.10.1.3.123	String	FE:FC:FE:2F:C2:0C
RFC1213-MIB	atPhysAddress.1.10.1.3.124	1.3.6.1.2.1.3.1.1.2	1.10.1.3.124	String	FE:FC:FE:47:E1:44
RFC1213-MIB	atPhysAddress.1.10.1.3.200	1.3.6.1.2.1.3.1.1.2	1.10.1.3.200	String	FE:FD:FE:FD:4C:DC
RFC1213-MIB	atNetAddress.1.10.1.2.1	1.3.6.1.2.1.3.1.1.3	1.10.1.2.1	IpAddress	10.1.2.1
RFC1213-MIB	atNetAddress.1.10.1.3.102	1.3.6.1.2.1.3.1.1.3	1.10.1.3.102	IpAddress	10.1.3.102
RFC1213-MIB	atNetAddress.1.10.1.3.103	1.3.6.1.2.1.3.1.1.3	1.10.1.3.103	IpAddress	10.1.3.103
RFC1213-MIB	atNetAddress.1.10.1.3.104	1.3.6.1.2.1.3.1.1.3	1.10.1.3.104	IpAddress	10.1.3.104
RFC1213-MIB	atNetAddress.1.10.1.3.105	1.3.6.1.2.1.3.1.1.3	1.10.1.3.105	IpAddress	10.1.3.105
RFC1213-MIB	atNetAddress.1.10.1.3.106	1.3.6.1.2.1.3.1.1.3	1.10.1.3.106	IpAddress	10.1.3.106
RFC1213-MIB	atNetAddress.1.10.1.3.110	1.3.6.1.2.1.3.1.1.3	1.10.1.3.110	IpAddress	10.1.3.110
RFC1213-MIB	atNetAddress.1.10.1.3.121	1.3.6.1.2.1.3.1.1.3	1.10.1.3.121	IpAddress	10.1.3.121
RFC1213-MIB	atNetAddress.1.10.1.3.123	1.3.6.1.2.1.3.1.1.3	1.10.1.3.123	IpAddress	10.1.3.123
RFC1213-MIB	atNetAddress.1.10.1.3.124	1.3.6.1.2.1.3.1.1.3	1.10.1.3.124	IpAddress	10.1.3.124
RFC1213-MIB	atNetAddress.1.10.1.3.200	1.3.6.1.2.1.3.1.1.3	1.10.1.3.200	IpAddress	10.1.3.200

SNMP Protocol Data Unit

SNMP specifies five protocol data unit PDUs (that is, SNMP messages) for exchange between management processes and agents.

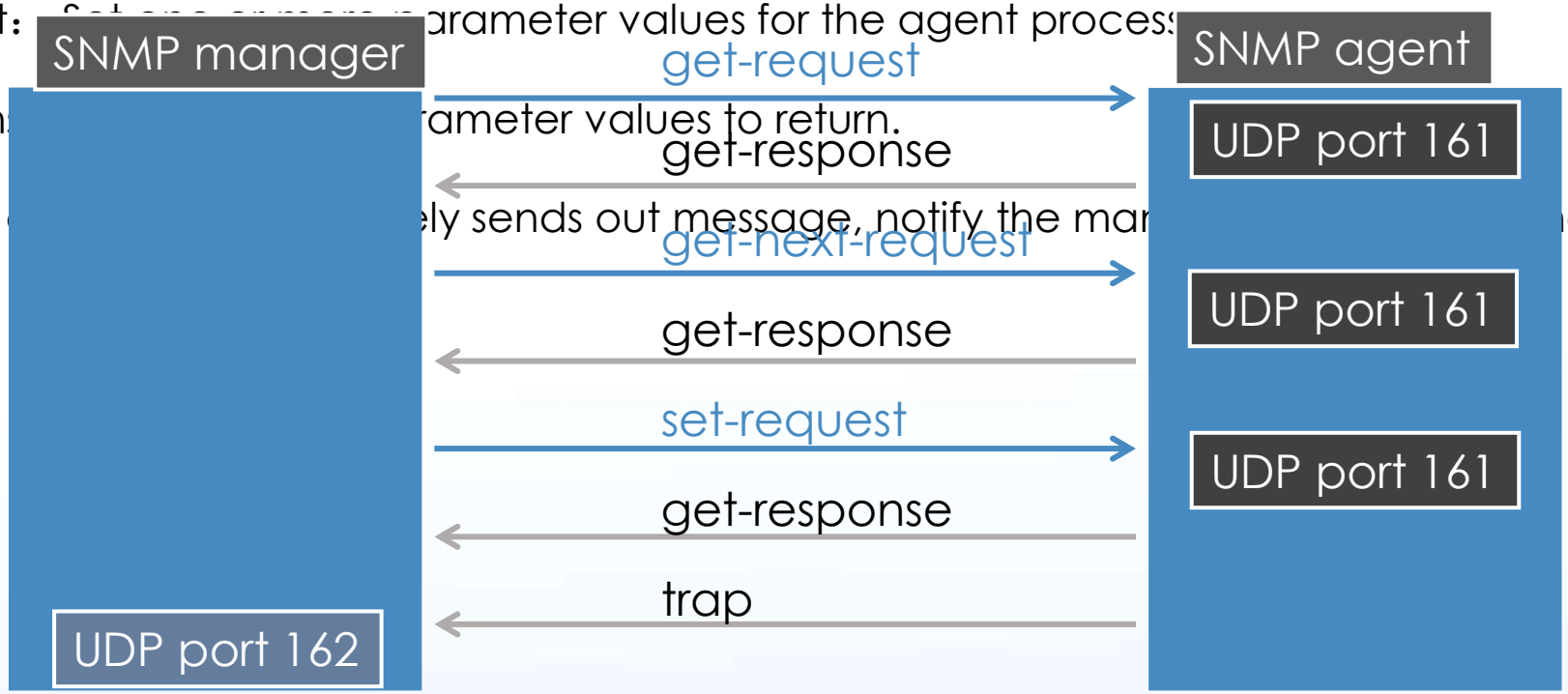
get-request： Extract one or more parameter values from the agent process.

get-next-request： Extract the next parameter value immediately following the current parameter value from the agent process.

set-request： arameter values for the agent proces

get-respon ameter values to return.

trap： The ly sends out message, notify the mar at something



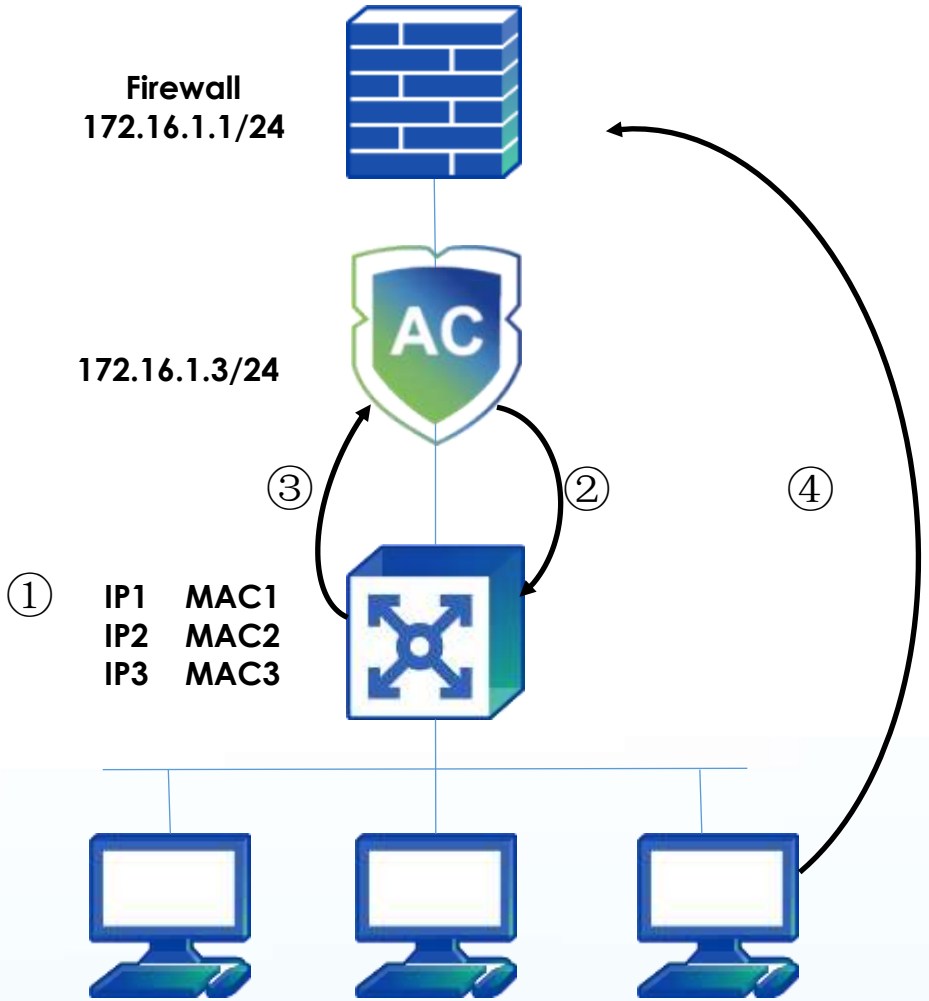
SNMP Protocol Packet

Capture SNMP interactions via Wirehsark

29	0.115843	199.200.233.197	10.1.3.4	SNMP	89	get-next-request 1.3.6.1.2.1.3.1.1.2.1.10.1.3.102
30	0.121616	10.1.3.4	199.200.233.197	SNMP	103	get-response 1.3.6.1.2.1.3.1.1.2.1.10.1.3.103
31	0.125026	199.200.233.197	10.1.3.4	SNMP	89	get-next-request 1.3.6.1.2.1.3.1.1.2.1.10.1.3.103
32	0.130612	10.1.3.4	199.200.233.197	SNMP	103	get-response 1.3.6.1.2.1.3.1.1.2.1.10.1.3.104
33	0.133459	199.200.233.197	10.1.3.4	SNMP	89	get-next-request 1.3.6.1.2.1.3.1.1.2.1.10.1.3.104
34	0.138537	10.1.3.4	199.200.233.197	SNMP	103	get-response 1.3.6.1.2.1.3.1.1.2.1.10.1.3.105
35	0.141946	199.200.233.197	10.1.3.4	SNMP	89	get-next-request 1.3.6.1.2.1.3.1.1.2.1.10.1.3.105
36	0.147405	10.1.3.4	199.200.233.197	SNMP	103	get-response 1.3.6.1.2.1.3.1.1.2.1.10.1.3.106
37	0.150358	199.200.233.197	10.1.3.4	SNMP	89	get-next-request 1.3.6.1.2.1.3.1.1.2.1.10.1.3.106
38	0.155466	10.1.3.4	199.200.233.197	SNMP	103	get-response 1.3.6.1.2.1.3.1.1.2.1.10.1.3.110

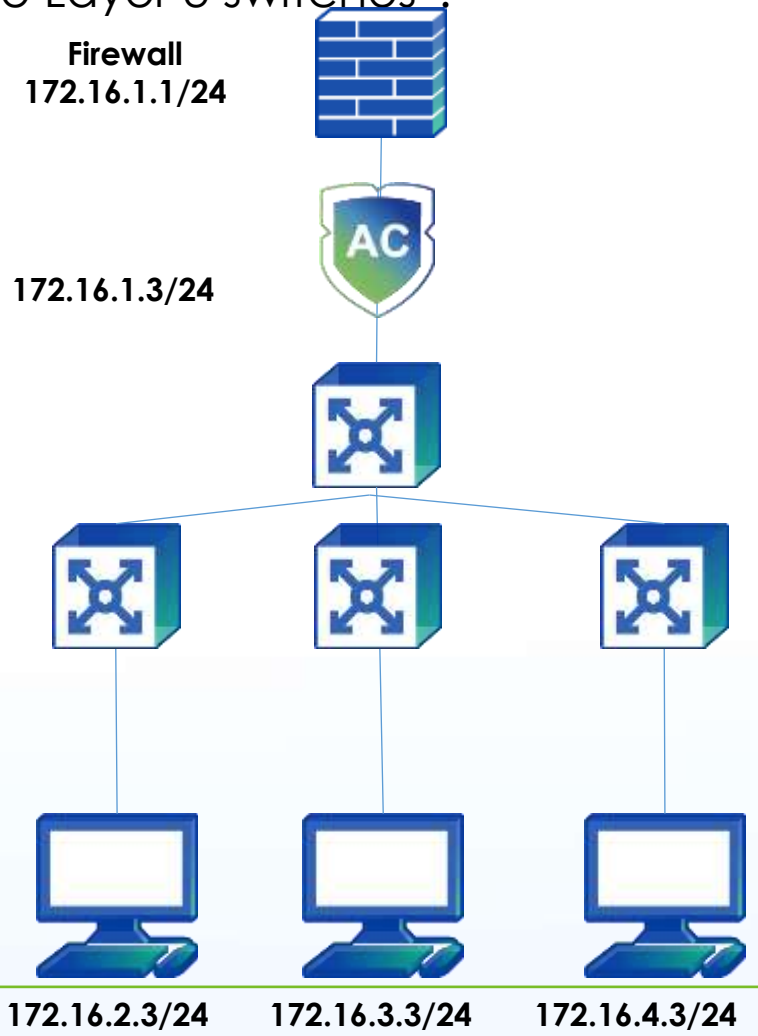
```
▷ Frame 30: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
▷ Ethernet II, Src: HollTech_08:ac:27 (b0:51:8e:08:ac:27), Dst: IntelCor_6b:d7:8f (d0:7e:35:6b:d7:8f)
▷ Internet Protocol Version 4, Src: 10.1.3.4, Dst: 199.200.233.197
▷ User Datagram Protocol, Src Port: 161, Dst Port: 57586
◢ Simple Network Management Protocol
    version: version-1 (0)
    community: sangfor
  ◢ data: get-response (2)
    ◢ get-response
        request-id: 0
        error-status: noError (0)
        error-index: 0
      ◢ variable-bindings: 1 item
        ▷ 1.3.6.1.2.1.3.1.1.2.1.10.1.3.103: fefcfe8cc3d9
```

Theory


Firewall
172.16.1.1/24
AC
172.16.1.3/24
③
②
④
①
IP1 MAC1
IP2 MAC2
IP3 MAC3

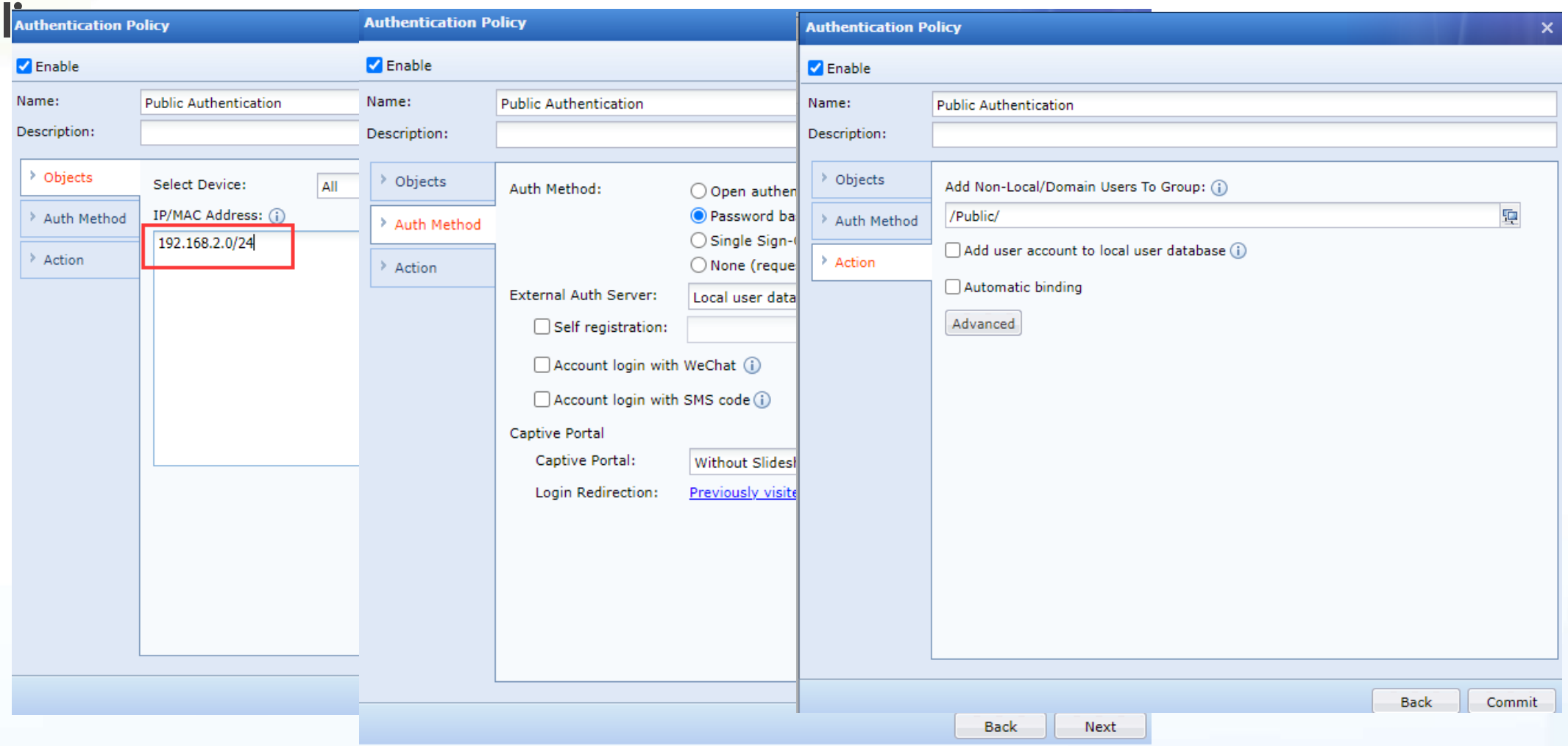
Theory

Think： How to obtain in the case of multiple Layer 3 switches ?



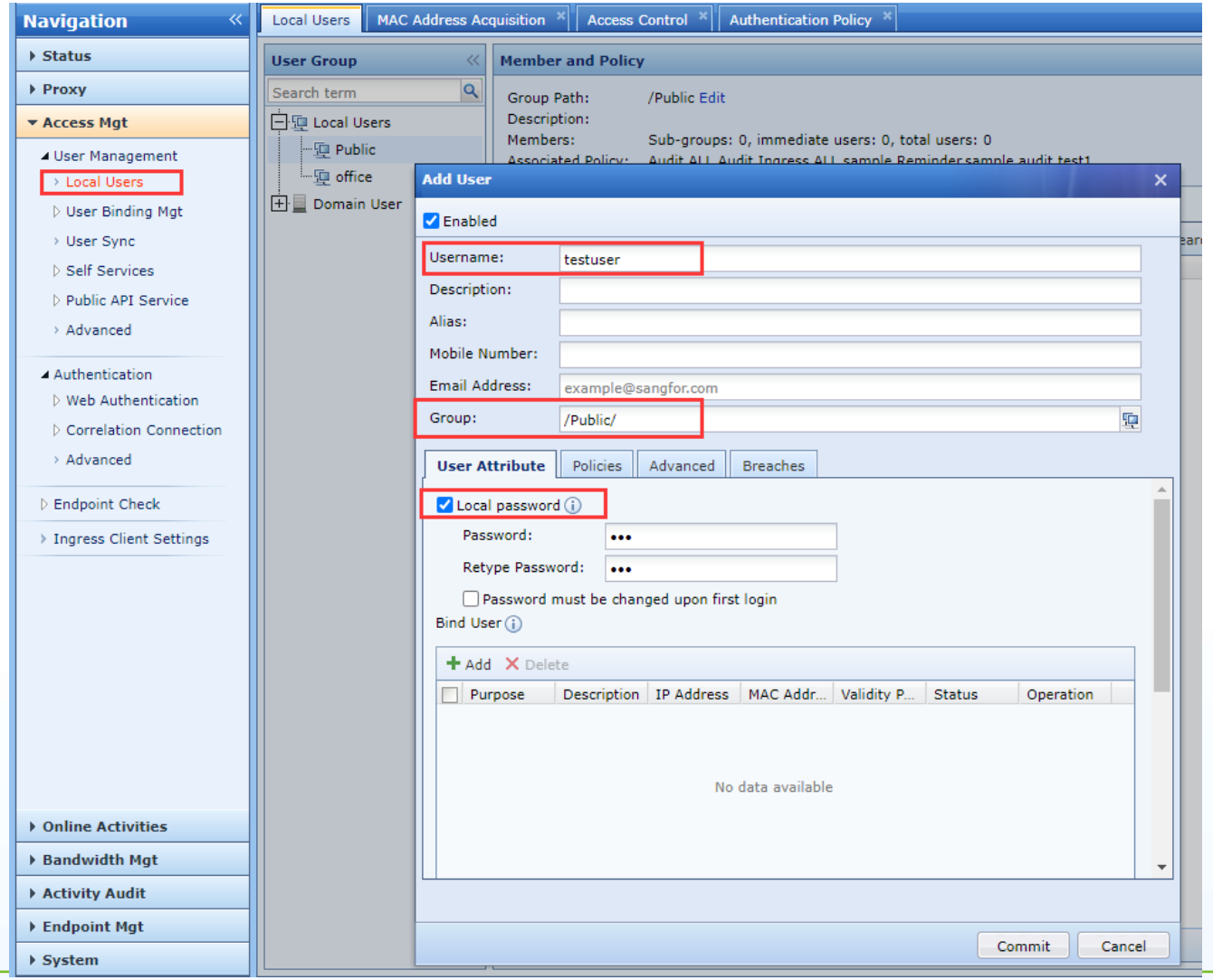
Configuration - Step 2

1. Add a group name "PUBLIC" and an authentication poli



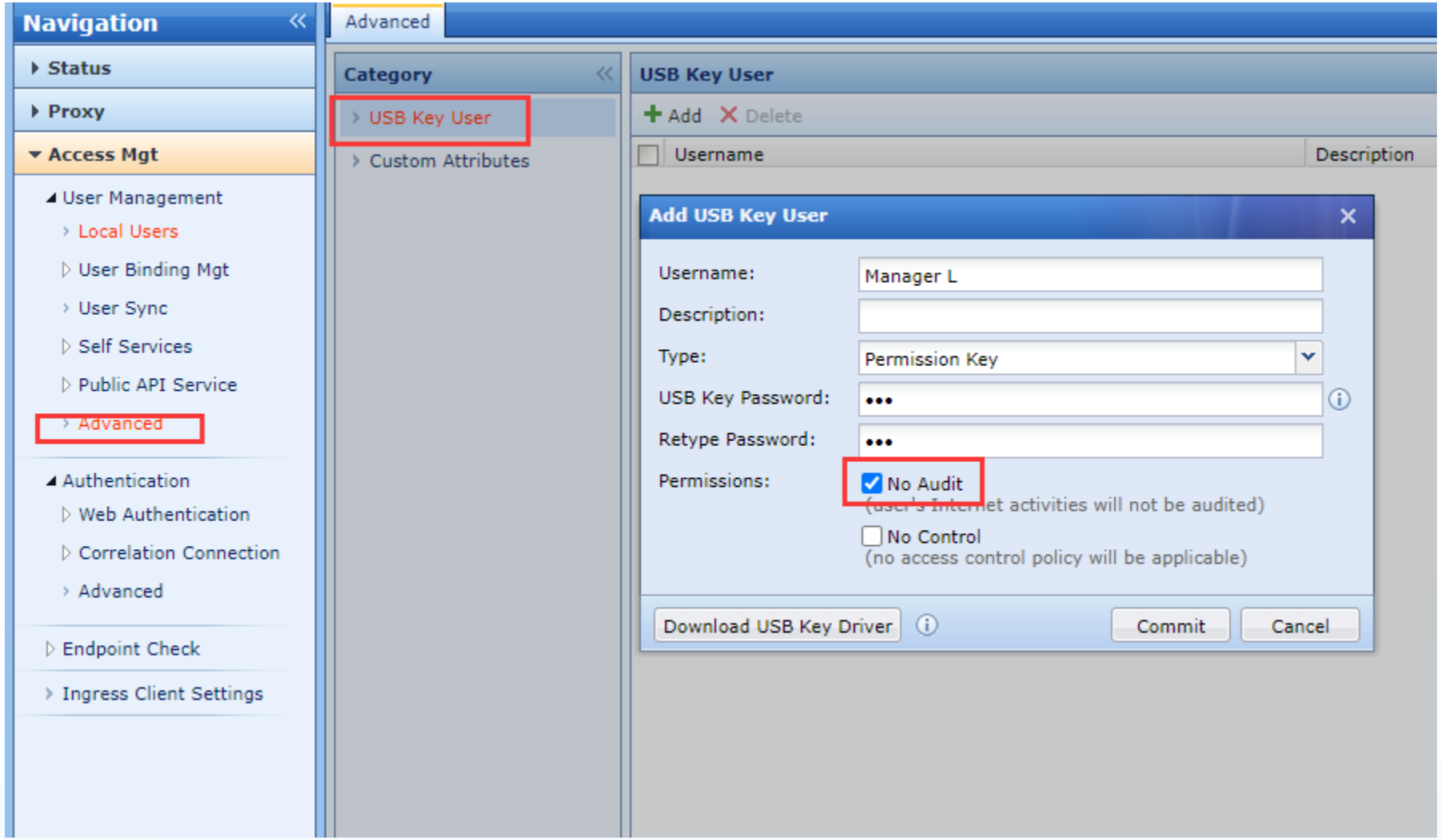
Configuration - Step 2

2. Add new username and password



Configuration - Step 3

1. Add a DKEY user.



Summary

IP/MAC binding failed?

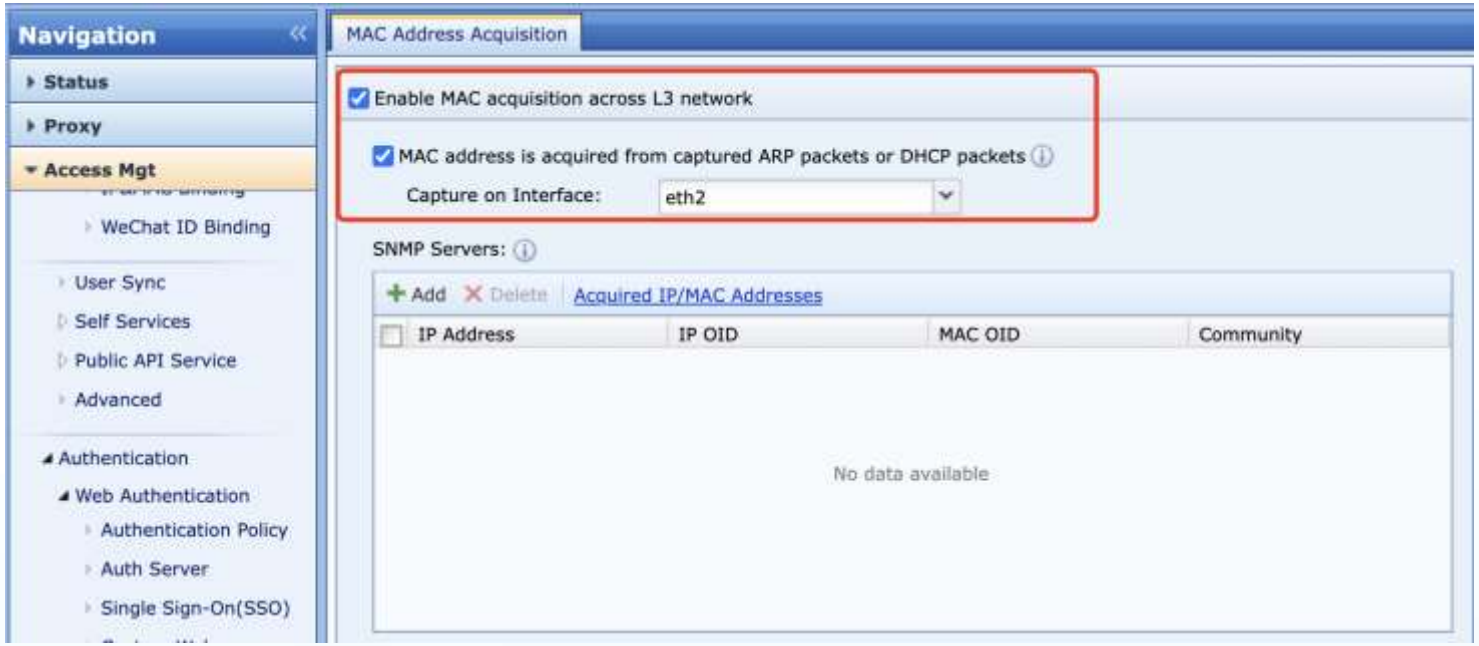
1、 Check whether the MAC address of the Layer 3 device is not excluded in [Mac acquisition across layer 3 network]

2、In [IP/MAC binding], Check whether the IP or MAC of the PC has be er the MAC of the

SANGFOR

Cross-three-layer identification method 2

Capture arp packet or dhcp packet to obtain MAC



Obtain the user's mac address by mirroring the switch arp or dhcp data to the idle port of the device (as a mirror port).

Implementation method 1: Add a trunk port on the core switch, allow all VLANs, and connect this trunk port to the AC idle network port. In this way, all broadcast packets can be copied to the IAG, including ARP packets and DHCP packets.

Cross-three-layer identification method 2

Capture arp packet or dhcp packet to obtain MAC

Are there any flaws in this scheme?

1. The gateway devices are all in the aggregation switch, and the aggregation switch and Internet behavior management are not in the same computer room. The two computer rooms are interconnected by optical fibers and cannot be implemented using this solution

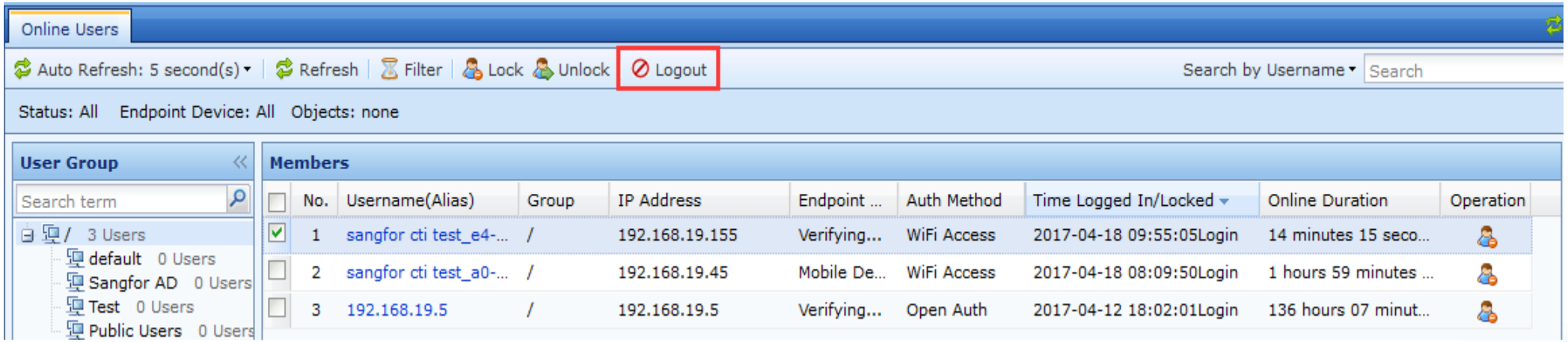
2. Or multiple core switches need to be identified across Layer 3, and this solution cannot be implemented because currently only one device mirror port can be set.

PART 3 User Logout

Force Logout Online Users

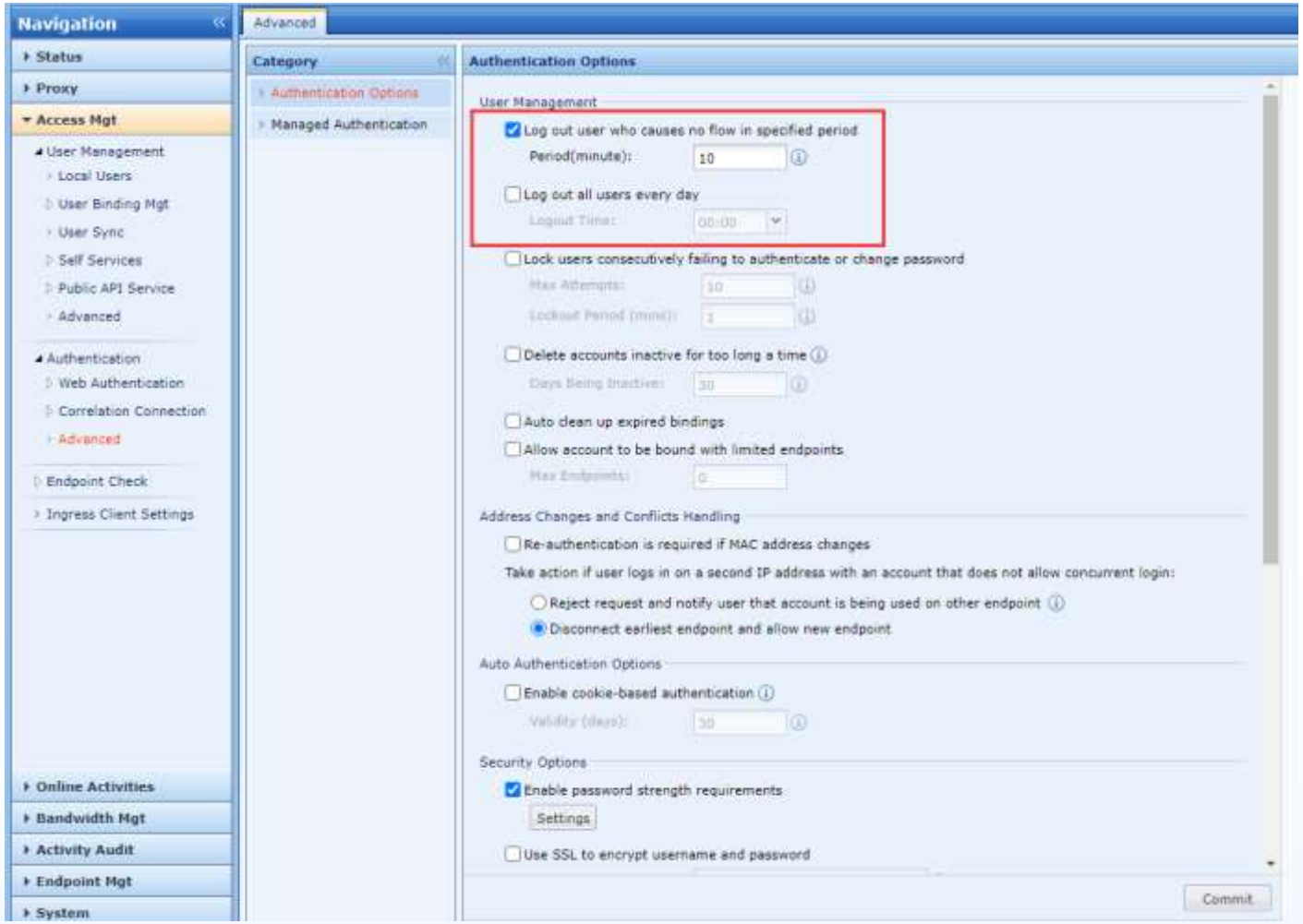
Web console

1. Force to Logout (DKEY users, temporary users and users that are free from authentication cannot be logged out!)



Force Logout Online Users

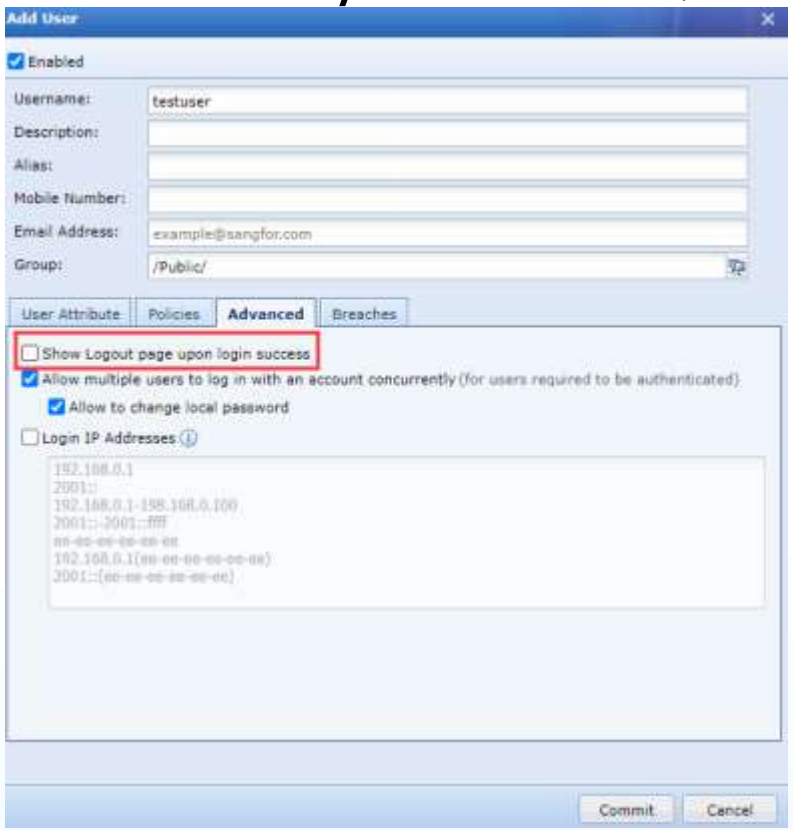
2. Log out user who cases no flow in specified period; Log out all users every day (working for all kinds of user authentication)



Force Logout Online Users

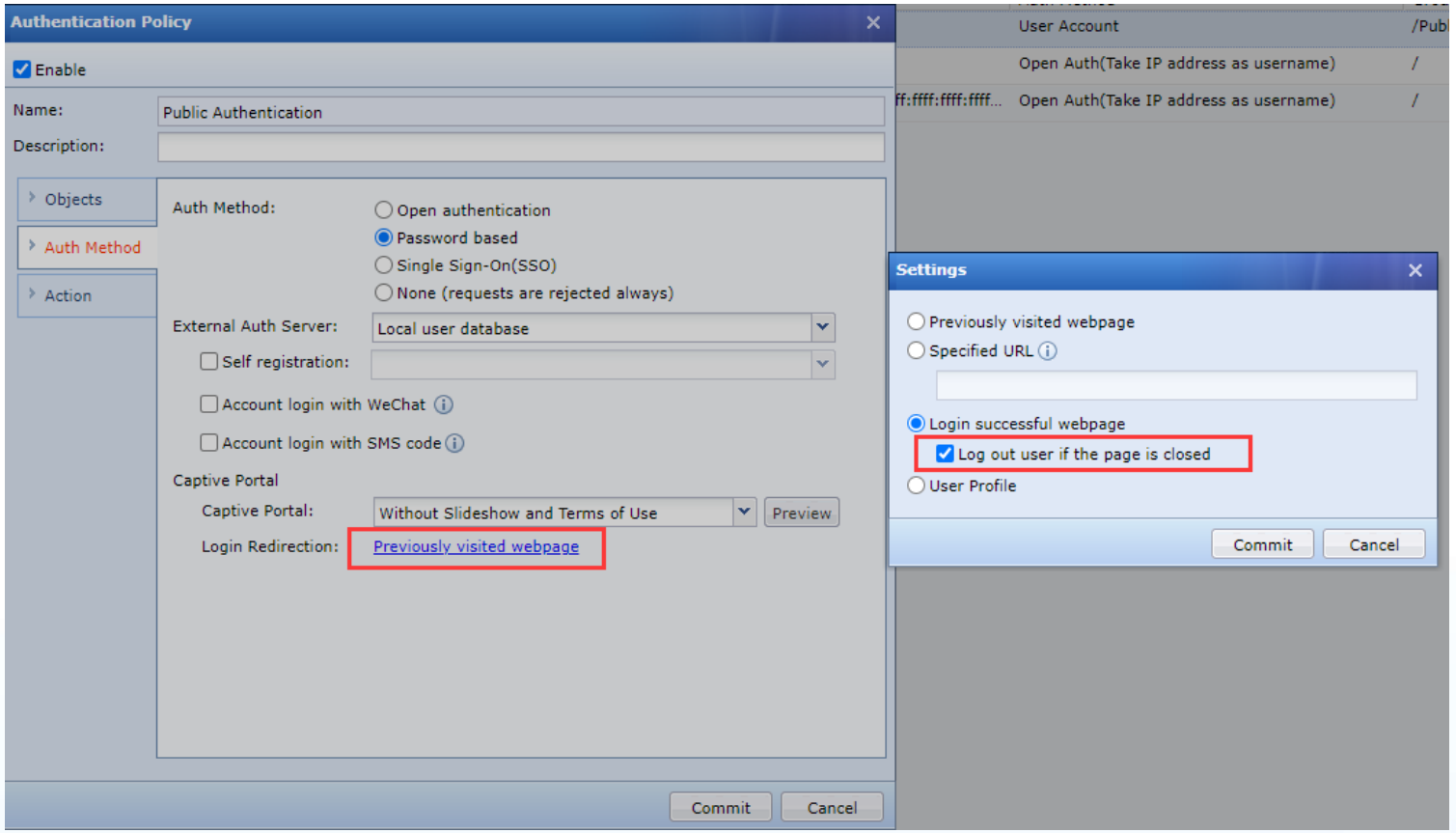
3. Display Logout page upon login success

（only worked for Username/Password ）



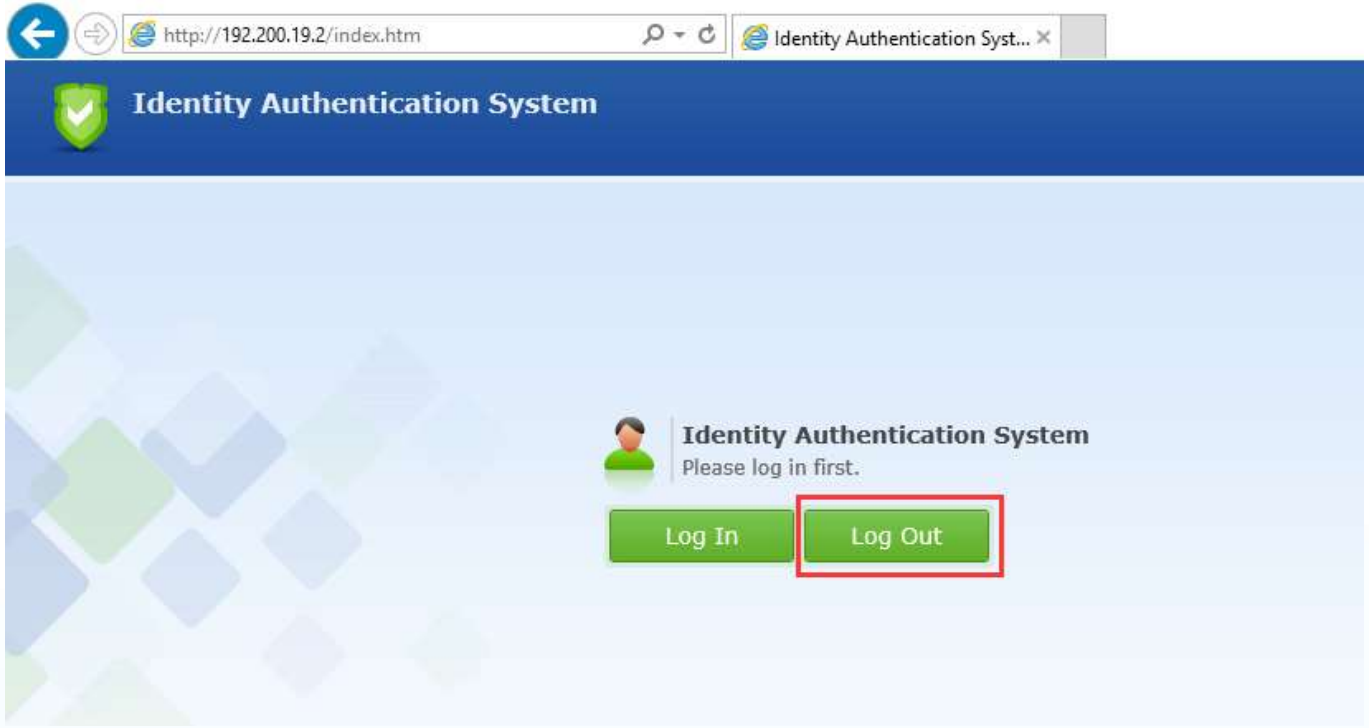
Force Logout Online Users

4. After user passes the authentication, page will be redirected to "Logout page" and click the logout button.



Force Logout Online Users

5. Client logout manually by entering http://IAGIP to open the logout page and click the logout button (only worked for Username/Password or SSO authentication users)



Practice

A hotel has a Layer 2 network (192.168.1.0/24), each computer is assigned a fixed IP address and staff can only use their own computer to surf the Internet in order to make sure the network behaviors can be traced. Customer room area users should use username/password authentication.

Advice：

Employee's computer use IP/MAC binding

Others use Username/Password

Question

1.What are the authentication modes can IAG support?

2.Why we should enable SNMP when customer want to bind ip/mac over layer 3 core switch?

3. In what conditions, user password policy will not take effect?

THANK YOU

Technical Support Service

Email: tech.support@sangfor.com

Community: community.sangfor.com