SANGFOR

IAG
RST redirection authentication function

Version 13.0.15

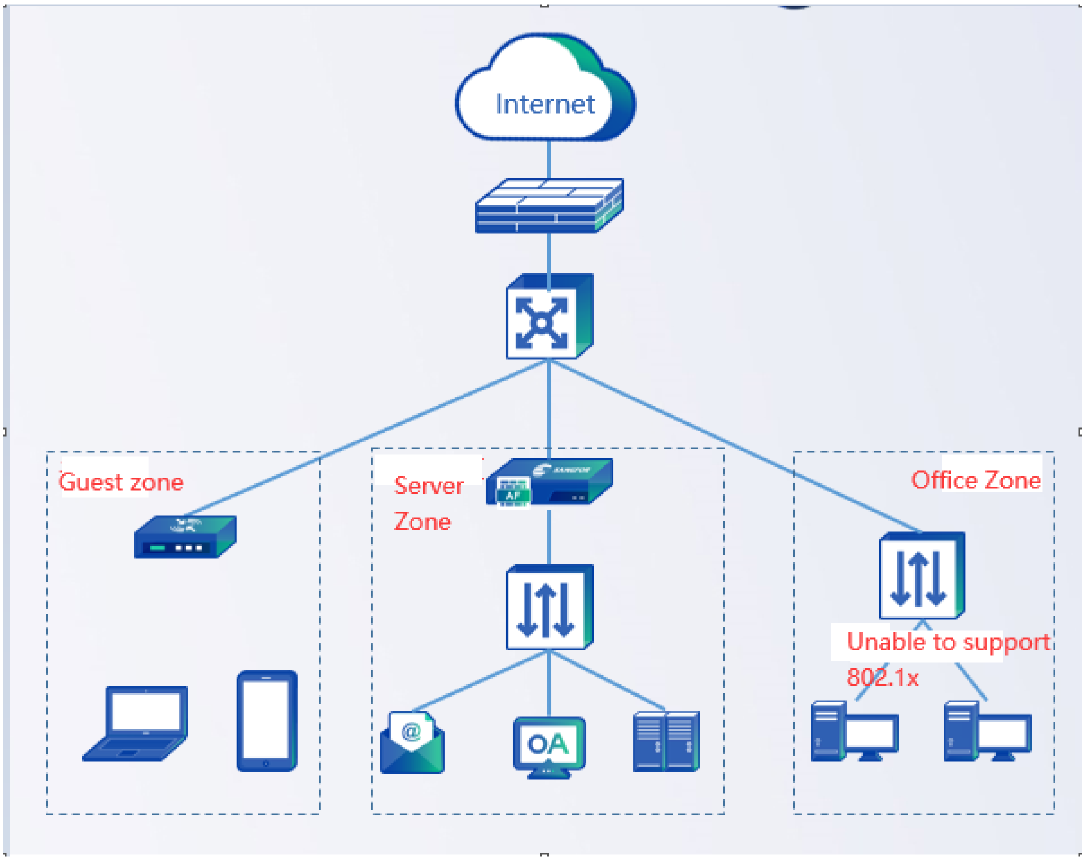
Change Log

Date	Change Description
Sep 23, 2020	Version 13.0.15 Release

CONTENT

Chapter 1 Background

1. Switch not support to configure 802.1x authentication, and unable to use level 2 method to done authentication.
2. User access to server packet unable to be controlled.
3. User access to Internet packet unable to be controlled.



Chapter 2 RST redirection authentication Solution

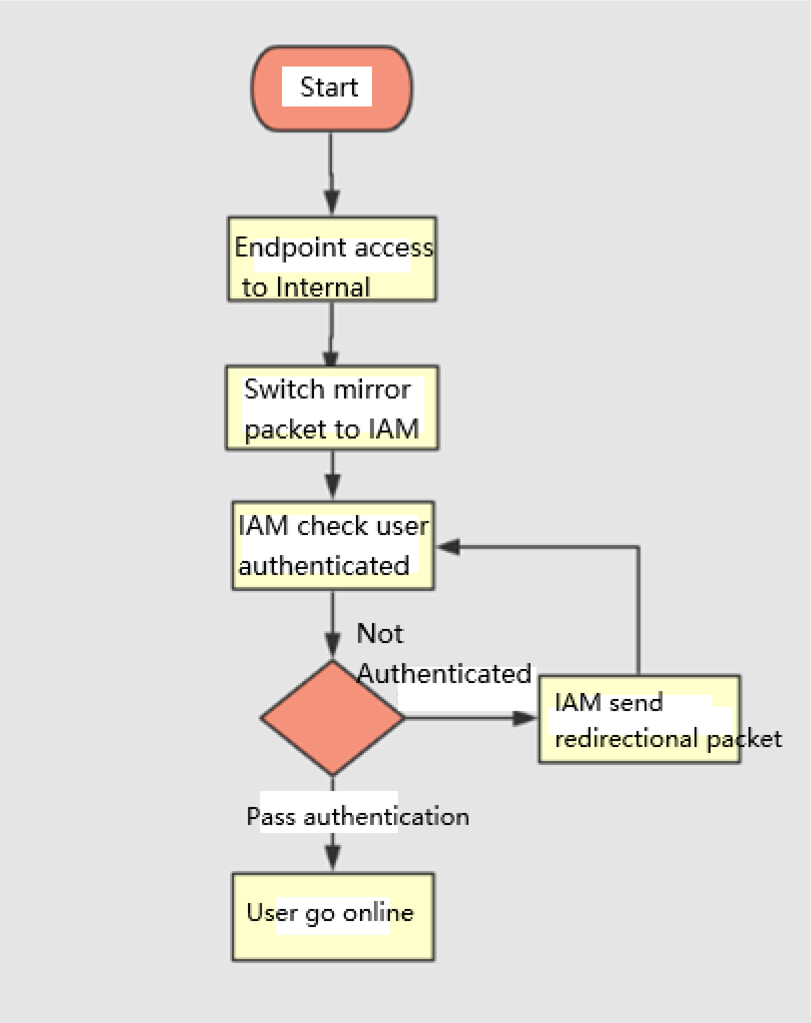
1. IAG set as bypass at core switch, it will set reset packet reject the non-authenticated request; for the required authentication will send 302 redirection to redirect the traffic to authentication page.
2. For unable to access to the Internal business before authenticated, and this method doesn't need to go through the core switch, this solution is simply, it just required to mirror the traffic from IAG and the switch doesn't need to do any configuration.

Chapter 2.1 Comparison between RST redirection authentication and 802.1x authentication

	Client software	Convenience	Security	Mirror	Authentication process	Scenario
RST redirection authentication	Not required	High	Middle	Required	User get the IP address, when access to specific URL, it will redirect to the portal authentication page, after that enter username and password to	Layer 3 authentication, for the switch unable to support 802.1x function or doesn't required to docking with switch. The device is the 3rd layer environment and packet access will go through core switch
802.1x authentication	Required	Middle	High	Not required	When user access to the layer 2 network required to do authentication, it required to use client software to done the authentication, after done the authentication then can access to the internal resources.	For scenarios where access to the internal network is strictly controlled, 802.1x authentication is used, and the internal network (including the Layer 2 network cannot be accessed) cannot be accessed without authentication, that is, it cannot pass through the Layer 2 switch.

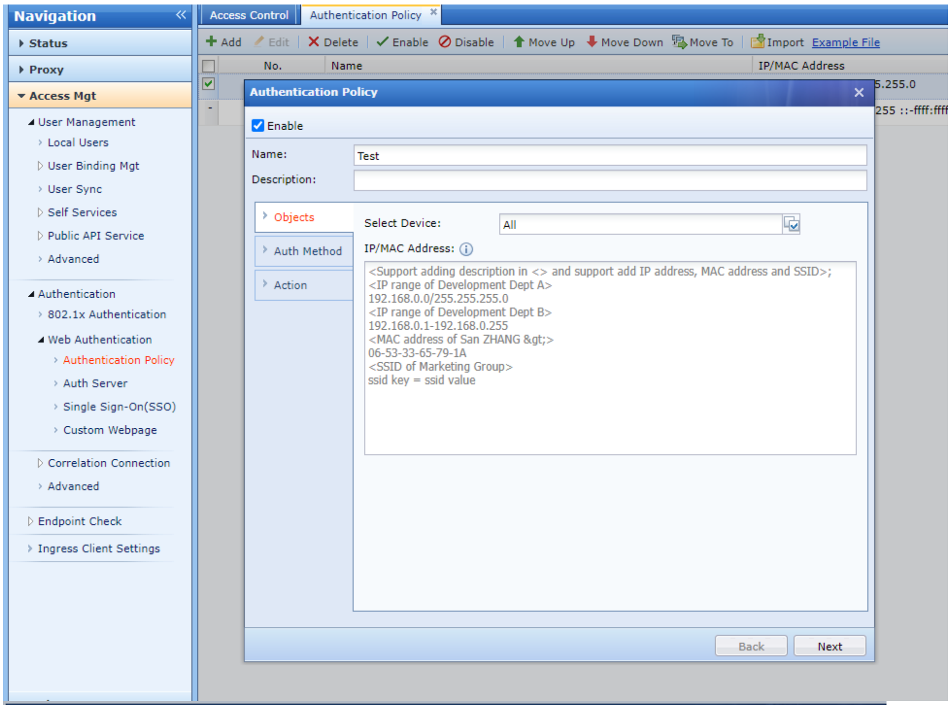
1. Chapter 2.2 RST Redirection authentication function description

1. Endpoint access to business or the internet data go through switch, switch mirror the traffic to IAG, IAG will check the endpoint has been authenticated or not, if not authenticated, it will send the 302 redirection packet.
2. When the endpoint received the 302 redirection packet, it will do the authentication on IAG.
3. After endpoint authenticated, it will not send the redirection packet again and allow the traffic, if the authentication is not passed, it will send the reset packet to reject user access to the internal network resources.
4. Except from the authentication, it also required to check the endpoint does it fullfill the rule before connect to the network, after authenticated and check all the rule, then it allow to access to the Internal network resources.


Start
Endpoint access to Internal
Switch mirror packet to IAM
IAM check user authenticated
Not Authenticated
IAM send redirectional packet
Pass authentication
User go online

Chapter 2.3 Configuration Guide

1. Switch configure the mirror port and connect to the IAG's mirror port
2. Configure a new authentication policy, navigate to Authentication -> Web Authentication -> Authentication policy and create new, Insert the IP range, authentication method can choose password based, SSO and None.



Authentication Policy

☑ Enable

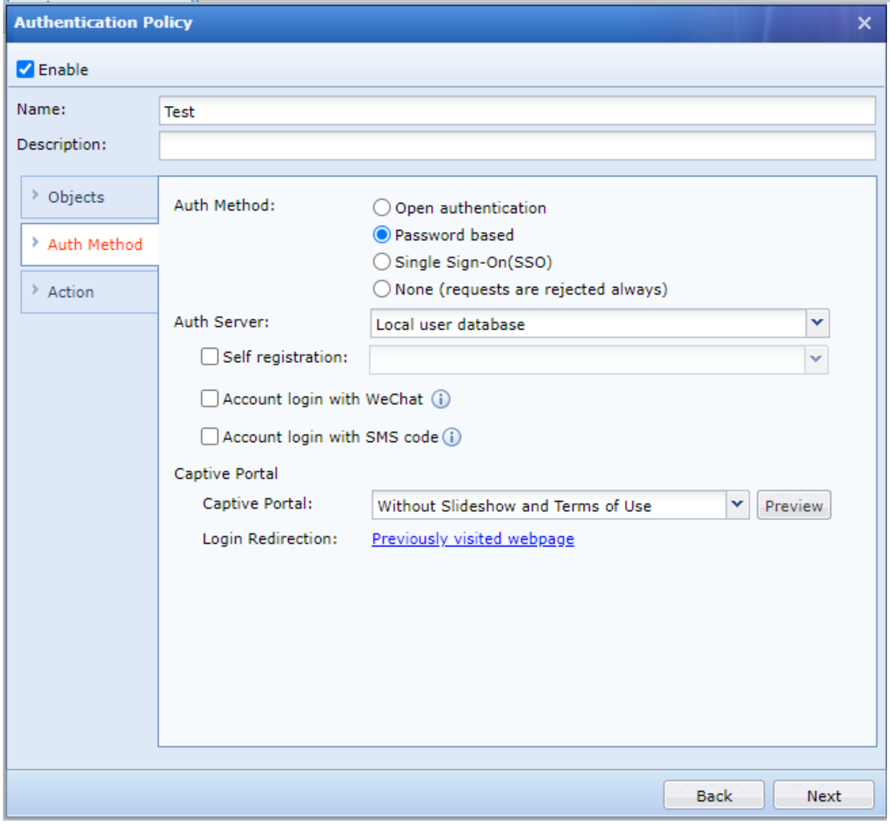
Name: Test

Description:

Select Device: All

IP/MAC Address:

<Support adding description in <> and support add IP address, MAC address and SSID>;
<IP range of Development Dept A>
192.168.0.0/255.255.255.0
<IP range of Development Dept B>
192.168.0.1-192.168.0.255
<MAC address of San ZHANG &gt;>
06-53-33-65-79-1A
<SSID of Marketing Group>
ssid key = ssid value



Authentication Policy

☑ Enable

Name: Test

Description:

Auth Method:
○ Open authentication
● Password based
○ Single Sign-On(SSO)
○ None (requests are rejected always)

Auth Server: Local user database

□ Self registration:

□ Account login with WeChat

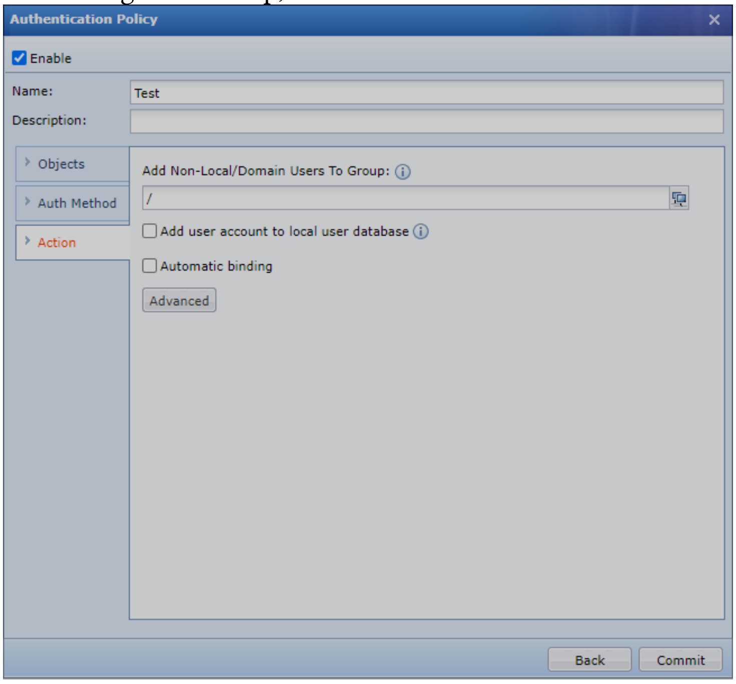
□ Account login with SMS code

Captive Portal

Captive Portal: Without Slideshow and Terms of Use

Login Redirection: Previously visited webpage

3. Action can select online to the certain group, also can Add user into local user group and set the binding relationship, as below:



Authentication Policy

☑ Enable

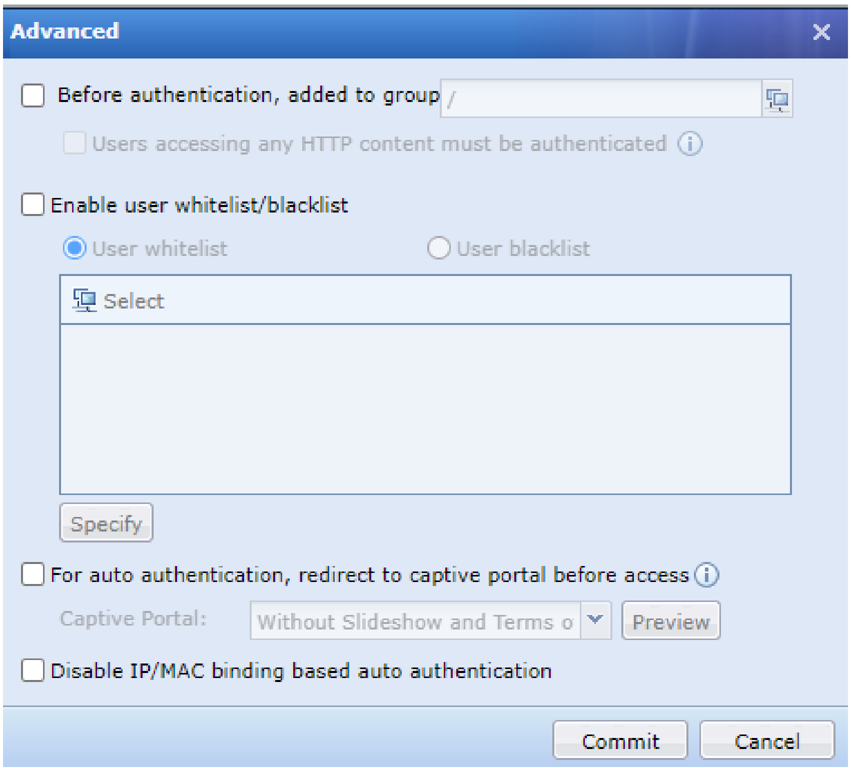
Name: Test

Description:

Add Non-Local/Domain Users To Group: /

☐ Add user account to local user database

☐ Automatic binding



Advanced

☐ Before authentication, added to group /

☐ Users accessing any HTTP content must be authenticated

☐ Enable user whitelist/blacklist

● User whitelist ○ User blacklist

☐ For auto authentication, redirect to captive portal before access

Captive Portal: Without Slideshow and Terms o

☐ Disable IP/MAC binding based auto authentication

Precaution:

1. The RST redirection only support bypass deployment mode.

2. The reset packet only can support TCP request, UDP request is not supported, if the authentication page cannot redirect required to do packet capture on IAG to check whether the endpoint has sent the packet and the IAG has sent the RST packet.

3. For the https traffic can take effect, the success rate of https redirection is depend on the speed of reply packet from Website, if the packet is more than 10ms then the success rate will be higher.

1.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc