(m) Local Portal authentication configuration example (GUI)

Wireless 龚训杰 2020-10-09 Published



Configuration Step

1. Click the <Network> button at the bottom of the page, then click [Network Security/Authentication] in the left navigation bar, then click the "Portal" tab, and then click the button to add. The configuration steps are:

H ₃ C	WX	2510H-F			👤 admin
Actions		All Networks > Network Security > Authentication > ISP Domains			
Deshboard		ISP Domains RADIUS			
Quick Start	>	ISP Domain			0 0
Monitoring	>	C 0 4.		Search	Q. Q
Wireless Configuration	>	Domain 🔺	State		Operation III
Network Security 2.	•	local-domain	Active		2 8
Packet Filter	П	system	Active		
Traffic Policy					
Access Control					
Authentication 3.					
BYOD		Total 2 entries, 2 matched, 0 selected. Showing page 1 of 1.			14 04 80 81 Q
Here Management		Delete			
172.20.10.4/wnm/frame/in	dex.php	2xessionid=200001889e898fdcef0ff7655460e6d11	1. System View Network View	Access Points Clients	Event Logs

2. As shown in the figure, configure the domain name, service type, select "Local" for authentication, and click Apply.



3. Complete ISP domain configuration

ISP Do	mains RADIUS			
ISP Do	omain			0
C	\odot		Search	Q. Q
	Dormalin 🔺	State		Operation III
0	iocal-domain	Active		28
•	system	Active		

4.Click the <Network> button at the bottom of the page, then click [Network Security/Access Manage ment] on the left navigation bar, and click the "Portal" tab to enter the Portal configuration page.

PECKET PICK	1	All Networks > Network Security > Access Control.> Portal	
Traffic Policy		Port Security Portal 3.	
Access Control		Portal	
Authentication		Portal authentication, also called Web authentication, controls user access to networks authentication page.	by authenticating the username and password entered on a p
8100		Portal authentication server	>
User Management		Portal Nieb server	>
Guest Hanagement		Local portal Web server 💡	>
Access Control 2		Portal-free rule 🥊	>
ystem	>	Interface policy	>
pois	>	Online users	>
sporting	>		

5. "Click "Portal Web Server", and then click the button to add a Portal Web server

uthentication	Portal authentication, also called W authentication page.	Veb authentication, controls user acces	s to networks by authenticat	ing the username and	d password entered on a po	
WOD	Portal authentication server			,	•	
ser Management	Portal Web server			,	>	
uest Management	Local portal Web server 📍			,	>	
ccess Control	Portal-free rule 📍			,	•	
stem >	Interface policy			,	>	
is >	Online users			,	>	
porting >						
				Delete Cliev		
Networks≯Network Sec Server name ◆	web 1	System View Network View	Access	0% 0% 1	ts EventLogs 0 ○ 13 △ 27	
Networks > Network Sec Server name • URL VRF	web 1 http://172.20.10.4/portal	Spitren View Renwork View	Access 100% ((1-32 chars) (1-256 chars) (1-31 chars)	2 0% 0 0% 1	ts Event Logs	
Networks > Network Sec Server name * URL VRF URL parameters •	web 1 http://172.20.10.4/portal Parameter name	system View Retwork View	Access (1-32 chars) (1-256 chars) (1-31 chars)	1-32 chars)	ets Event Logs	
Networks > Network Ser Server name • URL VRF URL parameters •	web 1 http://172.20.10.4/portal Parameter name @ User IP Address \ User MAC	Spitten View Reheard View Portal Web Server 2 Address O Original URL O Self-d	Access > 100% ((1-32 chars) (1-256 chars) (1-31 chars) (1-31 chars) (1-31 chars)	1-32 chars)	ts Event Logs	
Networks > Network Ser Server name • URL VRF URL parameters •	urity>Access Control > Portal > Edit web 1 http://172.20.10.4/portal Parameter name 0 User IP Address \ User MAC Add Type	Spiten View Portal Web Server Address \ Original URL \ Self-d ParamNam	Access > 100% ((1-32 chars) (1-256 chars) (1-31 chars) (1-31 chars) (1-31 chars)	Value	ets Event Logs	
Networks > Network Ser Server name • URL VRF URL parameters •	eurity > Access Control > Portal > Edit web 1 http://172.20.10.4/portal Parameter name @ User IP Address \ User MAC Add Type Setf-defined	Spateen View Retwork Ver Portal Web Server 2 Address Original URL O Self-d ParamNam wlanacnam	Access 0 100% ((1-32 chars) (1-256 chars) (1-31 chars) (1-31 chars) (1-31 chars) (1-31 chars)	Volue AC	event Logs	
Networks > Network Ser Server name • URL VRF URL parameters •	eurity > Access Control > Portal > Edit web 1 http://172.20.10.4/portal Parameter name © User IP Address _) User MAC Add Type Self-defined	Spateen View Retwork Ver Portal Web Server 2 Address O Original URL O Self-d ParamNam wlanacnam	Access 0 100% ((1-32 chars) (1-256 chars) (1-31 chars) (1-31 chars) (1-31 chars) (1-31 chars) (1-31 chars)	I-32 chars)	erent Logs	

6. Click "Local Portal Web Server", and then click the button to add a local Portal Web server

Port Security Portal		
ortal		
rtal authentication, also called Web authentication, controls user access to	networks by authenticating the username and password entered on a portal aut	hentica
Portal authentication server	>	
Portal Web server	>	
Local portal Web server 📍	>	
Portal-free rule 💡	>	
Interface policy	>	
Online users	>	

MTTP		
Default logon page 🔸	defaultfile.zip	x * +
TCP port	80	(1-65535,80 by default)
Apply Cancel		

7. Click "Portal-free rule", and then click the button to add authentication-free rules

Portal authentication server	>
Portal Web server	>
Local portal Web server 💡	>
Portal-free rule 💡	>
Interface policy	>
Online users	>

Rule ID 🔹	99	(0-4294967295
IP-based		
Source IP		
Destination	IP	
IPv4	□ IPv6 ○ Any IPv4 ○ Any IPv6	
114.1	14.114.114 / 32	(Example:192.168.0.1/16)
TCP	ort 8.8.8.8	
UDP	port	
UDP Source-based	port	
UDP Source-based	port	

8.Click [Wireless Configuration/Wireless Network] in the left navigation bar to enter the wireless network configuration page, click the button to add a wireless service, the configuration steps:

Actions		All Networks > Wireless Con	figuration > Wireless Networks > W	ireless Networks > Adva	nced Settings(123)			
Dashboard		WLAN Authentic	ation Authorization Intrus	ion Prevention Key	Management Binding			
Quick Start	>							
Monitoring		Service template	123	(1-63 chars)	Maximum client quantity			(1-2007)
romoning	-	SSID +			Association location	• AC	OAP	
Wireless Configuration	~	3310	portal	(1-32 chars)	Quick association 💡	CEnable	 Disable 	
Miroloce Notworks		Service template	Enable O Disable		Fast transition 📍	⊖ Enable	 Disable 	
WILCIESS NELWOLKS		Default VLAN	1					
AP Management			(1-4094, 1 by default)					
Wireless QoS		Hide SSID 📍	🔿 Enable 💿 Disable					
	-	Forwarding type	Centralized forwarding					
Wireless Security	- 1		O Local forwarding					
			Policy-based forwarding					
Radio Management		Apply	Cancel					

9.Click [Wireless Configuration/Wireless Network] in the left navigation bar to enter the wireless network configuration page, Click "authentication", configuration is as follows:

Authenticati	Intrusion Prevention Key Management	Binding		
Basic Settings		Portal authentication	n	
Authentication type	O Open (no authentication) Static PSK	2 Domain name	local-domain	(1-255 chars)
	0 802.1X authentication	Portal fail-permit 📍	O Enable Disable	
	O 802.1X Authentication (Clear)	Portal Web Server 🔹	web	(1-32 chars)
	⊖ Static WEP			
	MAC authentication	Maximum number of		(1-4294967295
	With Portal Authentication 3	users		
Authenticator	Local AC	BAS-IP 🣍		(eg:1.1.1.1)
	OAP			
Security mode	○ WPA ● WPA2 ○ WPA or WPA2			
Cipher suite	○ TKIP ● CCMP ○ TKIP or CCMP			
Static PSK				
Key type	Passphrase Rawkey			

10. Click "AP Management', create a new AP, and select the wireless service binding service template.

Actions	All Networ	ks > Wireless Conf	iguration > AP Manageme	nt > AP				
Dashboard	AP	AP Groups	AP Global Settings	P Provisioning AP Grou	p Provisioning			
Quick Start >	0	③ 2					Search	
Monitoring >		AP Name 🔺	AP Type	AP Model	Serial ID	MAC Address	Radios	Status
Wireless Configuration 🗸	0	1	Manual AP	UAP300-SI	219801A1CT8176E0	1C-AB-34-84-80-A0	2,802.11ac(5GHz)(1)	2
Wireless Networks								
AP Management								
Wireless QoS								
All Networks > Wireless	s Configur	ation > AP Ma	anagement > AP > I	Edit AP (1)				
General AC E	Backup	WLAN Serv	vice					
Bind WLAN servic	ce to radi	o 5GHz(1)						
Bind VLAN					Bind WLAN Service			
					123			άī.
100					123		```	• 💿
Bind WLAN servic	ce to radi	o 2.4GHz(2)					
Bind VLAN					Bind WLAN Service			
100					123			άī
1 - 4094					123		```	•
Apply	Apply a	ind Save	Cancel					
	1.1.1							

1. 11.Create a new local-user and select the service-type as "portal".

Projects Configuration	Local Users				
etwork Security 1 👻	Local Users For the device to act as an AAA server to perform local a	authentication, authorization, and accounting, you must	configure user settings on the dev	Users //cs.	User groups 🕐
Packet Filter	0.0.3			Search	0 0
Traffic Policy	User Name Dec	within Autoria	ation User Group	Service Types	Action
Access Control	123214124	system			10.0
Authentication	12345	system		Portal	2 1
	125580	system		Portal	12 18
8400	30#914144c20	system			8.0
User Hanagement	876416474476	rotten		Landovarr	
Guest Management	Total 13 entries, 13 metched Page 1/1.				14 15 81 81 Q
				Access Points Client	s EventLogs
		System Wese Retwork New		O 3% O 97% O 0% 0	0 0 0 A 510 C
Vireless Configuration	Username .	nortal		(1.55 chard)	
Honitoring	>		1 *		
Wireless Configuration	Viser name	portal		(1-55 chars)	
Network Security	 Password 			(1-63 chars)	
Packet Filter	Confirm password				
				(1-63 chars)	
Traffic Policy	description			(1-127 chars)	
Access Control	1				
	-			(t)	
Authentication	Authorization user group 📍	Select			
RV00	Service types	ADVPN KE IPoE LAN acces	Server	vice-type=portal	
10 1 10 10	Max concurrent logins				
				(1-1024)	
User Management					
User Management	Authorization attributes	 Authorization ACL 			
User Management Guest Management	Authorization attributes	Authorization ACL		+ (2000-4999)	
User Management Guest Management	Authorization attributes	Authorization ACL			

The redirect page is a Chinese page by default. If you want to use an English page, please import the attachment file defaultfile_en.zip.

附件下载: defaultfile_en.zip WEB portal.pdf