H3Cアクセスコントローラ

Microsoft NPSサーバーによるアクセス認証の構成例

Copyright©2022 New H3C Technologies Co.,Ltd.無断転載を禁ず。

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の承諾なく、いかなる形式または手段によっても複製または譲渡することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の商標または登録商標です。

このドキュメントの情報は、予告なしに変更されることがあります。

内容

はじめに	3
使用されているソフトウェアバージョン	3
例:NPS認証サーバーを使用したポータル認証の構成	3
ネットワーク構成	
制約事項とガイドライン	4
手順	
設定の確認	
構成ファイル	

はじめに

次の情報では、Microsoft NPSの認証サーバーソフトウェアを使用してワイヤレスクライアントを認証す るようにH3Cアクセスコントローラーを構成する例を示します。この例には、Microsoft NPSベースのポ ータル認証および承認ACL割り当ての構成が含まれます。

使用されているソフトウェアバージョン

次の設定例は、次のハードウェアおよびソフトウェアバージョンで作成および確認されたものです。

- AC:R5435P03を実行するvAC。
- NPS認証サーバー:Windows Server 2016 NPSコンポーネント。
- iMCサーバー:iMC PLAT 7.3(E0706P03)およびiMC 7.3(E0620)を実行するサーバー。

例:NPS認証サーバーを使用したポータル認証 の構成

ネットワーク構成

図1に示すように、APはスイッチを介してACに接続され、クライアントはAPを介してワイヤレスネットワークにアクセスします。

直接ポータル認証を構成して、クライアントのネットワークリソースへのアクセスを制御します。NPSサーバーをRADIUSサーバーとして使用し、IMCサーバーをポータルサーバーとして使用します。

図1 ネットワーク図



制約事項とガイドライン

APの背面パネルに表示されているシリアルIDを使用して、APを指定します。



ACの設定

RADIUSスキームを構成します。 1. #RADIUSスキームnpsを作成します。 <AC> system-view [AC] radius scheme nps #NPSサーバーをプライマリ認証およびアカウンティングサーバーとして指定し、サーバーとの安全 な通信のための共有キーを指定します。共有キーが、NPSサーバーで構成されている共有シーク レットと同じであることを確認してください。 [AC-radius-nps] primary authentication 8.72.1.7 key simple 12345678 [AC-radius-nps] primary accounting 8.72.1.7 key simple 12345678 #NPSサーバーに送信されるユーザー名からドメイン名を除外します。 [AC-radius-nps] user-name-format without-domain [AC-radius-nps] quit ISPドメインを構成します。 2. #ISPドメインポータルを作成します。 [AC] domain portal #ユーザー認証、承認、およびアカウンティングの既定の方法としてRADIUSスキームnpsを使用す るようにISPドメインを構成します。 [AC-isp-portal] authentication portal radius-scheme nps

[AC-isp-portal] authorization portal radius-scheme nps

[AC-isp-portal] accounting portal radius-scheme nps

[AC-isp-portal] quit

3. ポータル認証を設定します。

#ポータル認証サーバー名をimc、IPアドレスをIMCサーバーのIPアドレス、キーをプレーンテキストのポータルとして設定します。

[AC] portal server imc

[AC-portal-server-imc] ip 8.1.1.231 key simple portal

[AC-portal-server-imc] quit

#ポータルWebサーバーのURLをhttp://8.1.1.231:8080/portal/として構成します。(実際のポータ

ルWebサーバーのURLを指定してください。)

[AC] portal web-server imc

[AC-portal-websvr-imc] url http://8.1.1.231:8080/portal/

[AC-portal-websvr-imc] quit

#サービステンプレートポータルを作成します。

[AC] wlan service-template portal

#サービステンプレートのSSIDを指定します。

[AC-wlan-st-portal] ssid portal_nps

#サービステンプレートで直接ポータル認証を有効にします。

[AC-wlan-st-portal] portal enable method direct

#サービステンプレートでポータルWebサーバーimcを指定します。

[AC-wlan-st-portal] portal apply web-server imc

#サービステンプレートで認証ドメインポータルを指定します。

[AC-wlan-st-portal] portal domain portal

#サービステンプレートを有効にします。

[AC-wlan-st-portal] service-template enable

[AC-wlan-st-portal] quit

#ap1という名前の手動APを設定し、そのモデルとシリアルIDを指定します。

[AC] wlan ap ap1 model WA6638-JP

[AC-wlan-ap-ap1] serial-id 219801A24F8198E0001G

[AC-wlan-ap-ap1] quit

#radio 1を有効にし、サービステンプレートポータルとVLAN 80を無線にバインドします。

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] service-template portal vlan 80

[AC-wlan-ap-ap1-radio-1] radio enable

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

4. ACL 3999を設定します(必要に応じてACLを設定します)。

[AC] acl advanced 3999

[AC-acl-ipv4-adv-3999] rule 0 permit ip

[AC-acl-ipv4-adv-3999] quit

5. ACでDHCPサービスをイネーブルにし、DHCPアドレスプールを作成してクライアントにIPアドレ スを割り当てます。

#VLAN 80とVLAN-interface 80を作成します。VLANインターフェイスにIPアドレス72.205.1.1とサ ブネットマスク255.255.0.0を割り当てます。

[AC] vlan 80

[AC-vlan80] quit

[AC] interface Vlan-interface 80

[AC-Vlan-interface80] ip address 72.205.1.1 255.255.0.0

[AC-Vlan-interface80] quit
#DHCPサービスを有効にします。
[AC] dhcp enable
#80という名前のDHCPアドレスプールを作成します。
[AC] dhcp server ip-pool 80
[AC-dhcp-pool-80] quit
#DHCPアドレスプールで、動的割り当てのサブネットを72.205.0.0/16に指定します。
[AC-dhcp-pool-80] network 72.205.0.0 mask 255.255.0.0
#DHCPアドレスプールでゲートウェイアドレスを72.205.1.1として指定します。
[AC-dhcp-pool-80] gateway-list 72.205.1.1
#DHCPアドレスプールでDNSサーバードレスを72.205.1.1として指定します。
[AC-dhcp-pool-80] dns-list 72.205.1.1
[AC-dhcp-pool-80] quit

IMCサーバー(ポータルサーバー)の設定

- 1. ポータルサーバーを構成します。
 - a. IMCにログインし、Userタブをクリックします。
 - b. 図2に示すように、ナビゲーションツリーからUser Access Policy > Portal Service > Serverを選択して、ポータルサーバー構成ページを開きます。
 - c. 必要に応じてポータルサーバーのパラメーターを構成します。
 - d. OKをクリックします。

図2ポータルサーバーの構成

🕲 User > User Access Policy > Portal Service > Server	E. P. S					
Portal Server						
Basic Information						
Log Level *	Info					
Bind IP Group to Port Groups	Deny					
Portal Server	Portal Server					
Request Timeout (Seconds) *			Server Heartbeat Interval (Seconds) *			
User Heartbeat Interval (Minutes) *			LB Device Address			
Portal Web						
Request Timeout (Seconds) *				бвк		
Verify Endpoint Requests						
HTTP Heartbeat Display	New Page 👘		HTTPS Heartbeat Display	New Page 🚽		
Authentication Success Page Display Duration (Seconds) *						
	http://192.168.100.2 https://192.168.100	241:8080/portal/ .241:8443/portal/				
Portal Page						

- 2. IPアドレスグループを設定します。
 - a. ナビゲーションツリーからUser Access Policy > Portal Service > IP Groupを選択して、 ポータルIPアドレスグループの設定ページを開きます。
 - b. Addをクリックすると、図3のようなページが開きます。
 - c. IPグループの開始IPアドレスと終了IPアドレスを入力します。クライアントIPアドレスがIPグルー プ内にあることを確認します。

- d. サービスグループを選択します。この例では、既定のグループUngroupedを使用します。
- e. ActionリストからNormalを選択します。
- f. OKをクリックします。

図3 IPアドレスグループの追加

び User > User Access Policy > Portal S	service > IP Group > Add IP Group
Add IP Group	
IP Group Name *	72.205.0.0
Start IP *	72.205.0.0
End IP *	72.205.255.255
Service Group	Ungrouped 🔷
Action *	Normal
	OK Cancel

- 3. ポータルデバイスを追加します。
 - a. ナビゲーションツリーからUser Access Policy > Portal Service > Deviceを選択して、 ポータルデバイス設定ページを開きます。
 - b. Addをクリックすると、図4のようなページが開きます。
 - c. デバイス名(ACの名前)を入力します。
 - d. ポータルサーバーと情報を交換するACのインターフェイスのIPアドレスを入力します。
 - e. キーを入力します。このキーは、ACに設定されているキーと同じである必要があります。この例では、Portalです。
 - f. Access Methodリストから Directly Connectedを選択します。
 - g. 他のパラメータには既定の設定を使用します。
 - h. OKをクリックします。

図4 ポータルデバイスの追加

Device Information			
Device Name *	8.72.1.202	IP Address *	8.72.1.202
		Confirm Key *	
Advanced Information			
Listening Port *	2000	Local Challenge *	
Authentication Retries *		Logout Retries *	
Support Server Heartbeat *	No	Support User Heartbeat *	
Version *	Portal 2.0	Service Group *	Ungrouped
Access Method *	Directly Connected		
Device Description			

- 4. ポータルデバイスをIPアドレスグループに関連付けます。
 - a. 図5に示すように、デバイスのPort Group Information Managementアイコンをクリック

して、ポートグループ設定ページを開きます。

- b. 図6に示すように、Addをクリックしてページを開きます。
- **c.** ポートグループ名を入力します。
- d. 設定されたIPアドレスグループを選択します。
 ユーザーがネットワークにアクセスするために使用するIPアドレスは、このIPアドレスグループ
 内にある必要があります。
- e. 他のパラメータには既定の設定を使用します。
- f. OKをクリックします。

⊠5 Devicelist

閁	User > User Access Policy > Po	ortal Service > Device	1 - B. J. A. J.	1			
0							
	Deploy Result						
	Device IP Address Range From						
A	10						
	Device Name 🗣	Version ©	Service Group 👂	IP Address	Last Deployed at 🗢	Deploy Result	Operation
							19 5 17 11

図6 ポートグループの追加

asic Information				
	72.205.0.0	Authentication Type *	PAP	
ransparent Authentication	Not Supported			Ť
age Push Policy		Default Authentication Page		
Advanced Information				
Auvanceu mormation				
		QuickAuthentication *		
NAT or Not *			Yes	
.anguage *	English	Client Protection Against Cracks *		
leartbeat Interval (Minutes) *		Heartbeat Timeout (Minutes) *		
		Port Group Description		

NPSサーバー(RADIUSサーバー)を構成する

- 1. RADIUSクライアントを設定します。
 - a. ネットワークポリシーサーバー(NPS)コンポーネントを開きます。左側のナビゲーションペインで RADIUS Client and Servers > RADIUS Clientsを選択します。
 - b. 新しいRADIUSクライアントの追加: Address(IP or DNS)フィールドにACのIPアドレスを入力します。共有秘密を入力します。共有秘密は、プライマリ認証およびアカウンティングサーバーに設定されている共有キーと同じである必要があります。この例では、共有秘密は12345678です。

図7 RADIUSクライアントの作成

NPS (Local)	RADIUS Clients		
RADIUS Clients and Servers	RADIUS	S clients allow you to s	bedfy the network access servers, that provide access to your network.
 Epolicies Connection Request Policies Network Policies Accounting Templates Management 	Friendly Name	IP Address Devic	INTERN RADIUS Client e M Settings Advanced Enable this RADIUS client Select an existing template: Name and Address Friendly name: VAC Address (IP or DNS): 8,72.1.202 Verify Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret: Shared secret: Confirm shared secret: Confirm shared secret: OK

- 2. ユーザーの作成:
 - a. Active Directory Users and Computersコンポーネントを開きます。Usersディレクトリを選択して右クリックし、新しいユーザーを追加します。
 - b. ユーザー名をmyに設定し、Nextをクリックします。

図8ユーザーの作成

	0 🗟 🖬 📑 🦷	58837	2 · 82			
Active Directory Users and Com	Name Type	e	Description			
test.com	Administrator Use	r	Ruilt-in acco	unt for ad	~	
> 🚞 Builtin	New Object - User				~	
Computers Domain Controllers ForeignSecurityPrincipal:	Create in	: test.com/U	iers			
Users	First name:	my		Initials:		
1	Last name:					
Ł	64					
4	rui name:	iny				
1	User logon name:					
	my		@test.com		~	
8	User logon name (pr	e-Windows 200	0):			
	TEST\		my			
4	-					
4			e Oraște	Marka	Cound	
4			C DBOK	iveod >	Cancel	

c. ユーザーパスワードを構成し、Password never expiresを選択します。

Nextをクリックします。

図9ユーザーパスワードの構成

Active Directory Users and Com Saved Queries	Name Type Description	
test.com	New Object - User X	
Computers Domain Controllers ForeignSecurityPrincipal:	Create in: test.com/Users	
Managed Service Accour Users	Password:	
	Confirm password:	
	a User must change password at next logon	
	User cannot change password	
	Password never expires	
	4	
	Back Next > Cancel	

- 3. 接続要求ポリシーを構成します。
 - a. 新しい接続要求ポリシーを追加します。 #NPSコンポーネントを開きます。ナビゲーションペインで、Policies > Connection Request Policieを選択します。

#request policyを追加します。ポリシー名を設定し、他のオプションにはデフォルト設定を使用して、Nextをリックします。

図10 接続要求ポリシーの作成

🚯 NPS (Local)	Connection Reque	est Policies
 RADIUS Clients and Servers RADIUS Clients 	Connection	request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.
Remote RADIUS Server Groups		New Connection Request Policy X
Connection Request Policies Network Policies Accounting Templates Management	Policy Name	Specify Connection Request Policy Name and Connection Type You can specify a name for your connection request policy and the type of connections to which the policy is applied
		Policy name:
		example
	Conditions - If the Condition	Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specified. Type of network access server: Unspecified Vendor specific: 10 0
	Settings - Then the	-
		Brevious Next Enish Cancel

b. Add a user name: Specify ConditionsページでUser Nameを選択し、Addをクリックして、 前の手順で追加したRADIUSユーザーを接続リクエストポリシーに追加します。OKをクリック します。

図11	ユーザー名の追加	
-----	----------	--

New Connecti	on Reques	Policy		×
	Specify the minimum	y Conditions e conditions that determine whether this connection request po of one condition is required.	olicy is evaluated	for a connection request.
Select conditio	n on, and the	click Add.		×
User Name				^
User I The us typical	N ame ser name ti ly contains	User Name	×	r string that
Connection Pro	operties ss Client I ccess Clier e RADIUS ss Client I	Specify the user name of the access request message. You can matching syntax.	use pattem	uesting access
from the Arrange Frame	e RADIUS	OK	Cancel	ol for incoming
packet	is, such as f	PP or SLIP.		Add Cancel
		A	vdd	jdit <u>R</u> emove
		Previous	Vext Fir	rish Cancel

c. NASポートタイプを構成します。

Specify Conditionsページの下部で、NAS Port Typeを選択し選択したタイプを接続要求 ポリシーに追加します。

#Common 8021.X connection tunnel types領域で、Wireless IEEE-802.11を選択します。Others領域で、Wireless-Otherを選択します。

#**OK**をクリックします。

図12 NASポートタイプの構成

Specify th minimum	e conditions that determine whether this connection request policy is evaluate of one condition is required. NAS Port Type X	d for a connection request. A
Select a condition, and the NAS Identifier The NAS Identifier Can use pattern r NAS IPv4Addr The NAS IP v4Addr The NAS IP v6Addr The NAS IPv6Addr The NAS IPv6Addr	Specify the access media types required to match this policy. Common dial-up and VPN tunnel types Async (Modem) Sync (Sync Sync (T1 Line) Virtual (VPN) Common 802.1X connection tunnel types Ethemet FDDI Token Ring Virtual sectors Sync (T1 Line) Virtual (VPN)	er (NAS). You
	OK Cancel Add Previous Next E	Add Cancel

#Nextをクリックして、Connection Request Forwardingページを開きます。

d. ID認証の場所を設定します。

Connection Request Forwardingページで、Authenticationを選択し、Authenticate requests on this serverを選択します。

図13 ID認証ロケーションの構成

the policy conditions mat	h the connection request, these settings are a	pplied.	
ettings: Forwarding Connectio Request Authentication	Specify whether connection requered in the provided in the pr	uests are processed locally on, or are accepted without server wing remote RADIUS serve ng credentials	/, are forwarded to remote .t authentication. er group for authentication:

#Nextをクリックして、Authentication Methodsページを開きます。

e. 認証方式を指定します。

#EAP Typesボックスで、Protected EAP(PEAP)とSecured password(EAP-MSCHAP v2)を追加します。

#Less secure authentication methods領域で、Microsoft Encrypted Authentication version 2(MS-CHAP-v2)、Microsoft Encrypted Authentication(MS-CHAP)、Encrypted Authentication(CHAP)、Unencrypted Authentication(PAP.SPAP)、およびAllow clients to connect without negotiating an authentication methodを選択します。

図14 認証方式の指定

ew Connecti	ion Request Polic	у				
	Specify Au	uthentication	Methods re	ls equired for the c	onnection request	t to match this policy. For EAP
Override r	network policy auth ntication settings an	entication settings e used rather than the c	constraints a	nd authentication	settings in network	k policy.
EAP types ar	re negotiated betwe s:	een NPS and the client i	in the order i	in which they are	listed.	
Microsoft: 1 Microsoft: 3	Protected EAP (PE/ Secured password	AP) (EAP-MSCHAP v2)				Move <u>Up</u> Move Do <u>w</u> n
Add	Edit	Remove				
Less secur Microsoft	re authentication Encrypted Authent can change passwo Encrypted Authent	n methods : tication version 2 (MS-C ord after it has expired tication (MS-CHAP)	HAP- <u>v</u> 2)			
User of Engrypter	can change passwo d authentication (Cl	ord after it has expired HAP)				
Unencryp Allow clie	oted authentication ints to connect with	(PAP, <u>S</u> PAP) nout negotiating an auth	entication m	ethod.		
				Previous	Next	Enish Cancel

#Nextをクリックします。

#開いたウィンドウで、NoをクリックしてConfigure Settingsページを開きます。

f. ポリシーアトリビュートを設定します。AttributeリストからCalled-Station-Idを選択します。

図15 ポリシー属性の構成

figure the settings for this netv	work policy.			
nditions match the connection tings:	n request and the p	iolicy grants access, settings are applied.		
pecify a Realm Name Attribute	Select the the order the	attributes to which the following rules will be ney appear in the list.	e applied. Rules	are processed in
ADIUS Attributes	Attribute:	Called-Station-Id	~	
🧊 Stanuaru 711 Vendor Specific	Rules:			
	Find	Replace With		Add
				Edit
				Remove
				Move Up
				Move Down

g. 標準のRADIUSアトリビュートを追加します。

#RADIUS AttributesでStandardを選択します。

#Attributes列で属性名を選択し、Addをクリックします。Attribute Informationダイアログボ ックスが表示されます。

図16 標準RADIUSアトリビュートの追加

To add an attribute to the settings, select the attribute, and then click Add. To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add. Access type: Attributes: Name Acct-Interim-Interval Callback-Id Callback-Id Callback-Number Class Fiter-Id Framed-AppleTalk-Link		Add Standard RADIUS Attribute	×	y ar
To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add. Access type: All Attributes: Name Acct-Interim-Interval Callback-Id Callback-Id Callback-Id Filter-Id Firamed-AppleTalk-Link		To add an attribute to the settings, select the attribute, and then click Add.		
Access type: All Attributes: Name Acct-Interim-Interval Callback-Id Callback-Id Callback-Number Class Fiter-Id Framed-AppleTalk-Link	ig	To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add		
Attrigutes: Attrigutes: Name Acct-Interim-Interval Callback-Id Callback-Id Callback-Vumber Class Filter-Id Framed-AppleTalk-Link		Annese time -		
Attributes: Name Acct-Interim-Interval Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link	I			⊢
Attributes: Name Acct-Interim-Interval Callback-Id Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link	C			
Name Acct-Interim-Interval Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link <		Atributes:	_	
Acct-Interim-Interval Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link		Name	^	
Callback-Id Callback-Number Class Filter-Id Framed-AppleTalk-Link		Acct-Interim-Interval		
Callback-Number Class Filter-Id Framed-AppleTalk-Link		Callback-Id		
Class Filter-Id Framed-AppleTalk-Link		Callback-Number		
Fritter-Jd Framed-AppleTalk-Link		Class		
		Filter-IO Ersmad Appla Talk J ink		
S		riameu-appie raik-unk	×	
		· · · · · · · · · · · · · · · · · · ·	_	
		Specifies the length of the interval (in seconds) between each interim update that the NAS sends.		1
Specifies the length of the interval (in seconds) between each interim update that the NAS sends.				
Specifies the length of the interval (in seconds) between each interim update that the NAS sends.		Add Char	2	
Specifies the length of the interval (in seconds) between each interim update that the NAS sends.		Add Lose		

#表示されるAttribute Informationダイアログボックスで、属性値を設定します。

#属性の既定の選択を保持し、ドロップダウンリストから属性値を選択して、OKをクリックします。

たとえば、Framed-Protocol属性では、デフォルトでDial-UpまたはVPNに一般的に使用されるオプションが選択されています。このデフォルトの選択をそのまま使用して、ドロップダウンリストからPPPを選択し、OKをクリックします。属性値PPPはFramed-Protocol属性で設定されています。

図17 属性値の構成

To add an attribute to the settings, select the attribute, and then cick Add. To add a oustom or predefined Vendor Specific attribute, close this dialog and, add. Attribute information Access type: Attribute name: Framed-Protocol Attribute number	select Vendor Specific, and then click
Config To add a custom or predefined Vendor Specific attribute, close this dialog and f cond Add. Attribute Information Settian Access type: All Framed-Protocol Attribute number	select Vendor Specific, and then click
Setian Access type: All Framed-Protocol Altibute name: Framed-Protocol Attribute name:	
P Attribute number	
RAD Attributes: 7	
Name Attribute format: Enumerator Image: Protocol Framed-Protocol Framed-Route Attribute Value: Attribute Value: Framed-Route Framed-Routing © Commonly used for Dial-Up or VPN	
Ide-Timeout ppp	~
< Others	
Description: Specifies the proto	Cancel

#前の手順を繰り返して、値FramedのService-Typeアトリビュート、値802のTunnel-Media-Typeアトリビュート(すべての802メディアとEthernet...を含む)、および値3999のFilter-Id(ACL)を追加します。設定されたアトリビュートは次のとおりです。

図18 標準のRADIUS属性

lew Connection Request Policy		2
NPS applies sett matched.	Settings	if all of the connection request policy conditions for the policy are
Configure the settings for this netw If conditions match the connection Settings:	ork policy. request and the policy grants ac	ccess, settings are applied.
Specify a Realm Name Attribute RADIUS Attributes	To send additional attribut then click Edit. If you do r your RADIUS client docu	tes to RADIUS clients, select a RADIUS standard attribute, and not configure an attribute, it is not sent to RADIUS clients. See mentation for required attributes.
😝 Standard		
🗾 Vendor Specific	Attributes:	
	Name Filter-Id Framed-Protocol Service-Type Tunnel-Medium-Type	Value 3999 PPP Framed 802 (includes all 802 media plus Ethernet canonical for
	Add Ed	itBemove
		Previous Next Finish Cancel

h. 接続要求ポリシーを表示または編集します。

#NPSの左側のナビゲーションペインで、**Policies > Connection Request Policies**の順 に選択します。

Policy Name列で、接続要求ポリシーを表示できます。 #ポリシーの構成を編集するには、ポリシー名を右クリックしてPropertiesを選択します。

図19 接続要求ポリシー

🚯 NPS (Local)	Connection Request Policies			
ADIUS Clients and Servers ADIUS Clients Remote RADIUS Server Groups If Policies	Connection request policies allow you t	to designate whether conne	ction requests are processed locally or forwarded to remote RADIUS servers.	
Connection Request Policies	Policy Name	Status Processing On	er Source	
Network Policies		Enabled 1	Unspecified	
Accounting Templates Management	Use Windows authentication for all users	Enabled 999999	Unspecified	
	je example			
	Conditions - If the following conditions are me	t:		
	Condition Value			
	NAS Port Type Wireless - IEEE 802.11 OF	Wireless - Other		
	User Name my			
	Settings - Then the following settings are app	lied:		
	Setting	Value		
	Authentication Provider	Local Computer		
	Override Authentication Authentication Method Extensible Authentication Protocol Method	Enabled EAP OR Unencrypted auti Microsoft: Protected EAP	entication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 OF PEAP) OR Microsoft: Secured password (EAP-MSCHAP v2)	NS-CHAP v2 OR Allow Unauthenticated Access
	Fiter-Id	3999		
	Framed-Protocol Service-Type	Framed		A
	Tunnel-Medium-Type	802 (includes all 802 media	plus Ethernet canonical format)	Activate Windo

設定の確認

- クライアントで、ワイヤレスネットワークに接続します。ブラウザを使用してWebサイトにアクセス します。ポータル認証ページが開きます。構成されたユーザー名myとパスワードを入力します。 ユーザーは認証を正常に通過できます。
- **2.** ACで、次のコマンドを使用して、ユーザーがオンラインになり、サーバーが認可ACLをユーザーに 割り当てたことを確認します。

[AC] display portal user all verbose Total portal users: 1 Basic:

AP name: ap1

Radio ID: 1

SSID: portal_nps

Current IP address: 72.205.0.1

Original IP address: 72.205.0.1

Username: my

User ID: 0x1000002b

Access interface: WLAN-BSS0/4

Service-VLAN/Customer-VLAN: 80/-

MAC address: d4bb-c8a1-8a55

Authentication type: Normal

Domain name: portal

VPN instance: N/A

Status: Online

Portal server: imc

Vendor: VIVO Portal authentication method: Direct AAA: Realtime accounting interval: 720s, retry times: 5 Idle cut: N/A Session duration: 0 sec, remaining: 0 sec Remaining traffic: N/A Login time: 2021-12-3 18:57:44 UTC Online time(hh:mm:ss): 00:00:05 DHCP IP pool: N/A Web URL: N/A ACL&QoS&Multicast: Inbound CAR: N/A Outbound CAR: N/A ACL number: 3999 (active, AAA) User profile: N/A Session group profile: N/A Max multicast addresses: 4 Flow statistic: Uplinkpackets/bytes: 7/540 Downlink packets/bytes: 0/0

構成ファイル

radius scheme nps primary authentication 8.72.1.7 key simple 12345678 primary accounting 8.72.1.7 key simple12345678 user-name-format without-domain # domain portal authentication portal radius-scheme nps authorization portal radius-scheme nps accounting portal radius-scheme nps # portal server imc ip 8.1.1.231 key simple portal # portal web-server imc url http://8.1.1.231:8080/portal/ #

wlan service-template portal ssid portal_nps portal enable method direct portal domain portal portal apply web-server imc service-template enable # wlan ap ap1 model WA6638-JP serial-id 219801A24F8198E0001G radio 1 radio enable service-template portal vlan 80 # Acl advanced 3999 rule 0 permit ip # vlan 80 # interface Vlan-interface 80 ip address 72.205.1.1 255.255.0.0 # dhcp server ip-pool 80 gateway-list 72.205.1.1 network 72.205.0.0 mask 255.255.0.0 dns-list 72.205.1.1 # return