

V7防火墙和思科ACS 实现radius认证

AAA 李超 2018-09-17 发表

组网及说明

ACS版本为5.3

配置步骤

防火墙侧关键配置如下：

```
#  
radius scheme radius  
primary authentication xx.xx.xx.xx  
primary accounting xx.xx.xx.xx  
key authentication cipher $c$3$kd0dGV7u/GaWnAClib940/kGLgJdmbCbeg==  
key accounting cipher $c$3$YzwlejGtgqKC1vI0cyH2ePj+aehv5Tkx7Q==  
user-name-format without-domain  
#  
domain radius  
authentication login radius-scheme radius local  
authorization login radius-scheme radius local  
accounting login none  
#  
domain default enable radius  
#
```

ACS服务器侧配置：

System Administration>Configuration>Dictionaries>Protocols>RADIUS>RADIUS VSA页签下面创建h3c。

The screenshot shows the 'Vendor Specific Dictionary' list in the Cisco ACS configuration interface. The 'h3c' vendor is selected and highlighted with a red underline. Other vendors listed include Ascend, Cisco, Cisco Airespace, Cisco Aironet, Cisco BBSM, Cisco VPN 3000/ASA/PIX 7.x, Cisco VPN 5000, hillstone, Juniper, Microsoft, Nortel (Bay), RedCreek, and US Robotics.

Vendor	Vendor ID	Description
Ascend	529	
Cisco	9	
Cisco Airespace	14179	
Cisco Aironet	5842	
Cisco BBSM	5263	
Cisco VPN 3000/ASA/PIX 7.x	3076	
Cisco VPN 5000	255	
<u>h3c</u>	25506	
hillstone	28557	
Juniper	2636	
Microsoft	311	
Nortel (Bay)	1584	
RedCreek	1958	
US Robotics	429	

Vendor ID为25506。

The screenshot shows the configuration form for the 'h3c' vendor. The 'Name' field is set to 'h3c'. The 'Description' field has the placeholder text '必填'. The 'Vendor ID' field is set to '25506'. The 'Attribute Prefix' field is also set to '必填'. A checkbox labeled 'Use Advanced Vendor Options' is checked. A note at the bottom indicates that '必填' means 'Required'.

Name: h3c
Description: 必填
Vendor ID: 25506
Attribute Prefix: 必填
Use Advanced Vendor Options
必填 = 必需字段

System Administration>Configuration>Dictionaries>Protocols>RADIUS>RADIUS VSA>h3c下面增加属性User-Roles

ID为155, Type为String:

Network Resources>Network Devices and AAA Clients添加设备:

Users and Identity Stores>Internal Identity Stores>Users增加用户ahnx

Policy Elements>Authorization and Permissions>Network Access>Authorization Profiles增加一个Profile

Name

General	Common Tasks	RADIUS Attributes
<input checked="" type="radio"/> Name: <input type="text" value="h3c-role"/>		
Description:		
● = 必需字段		

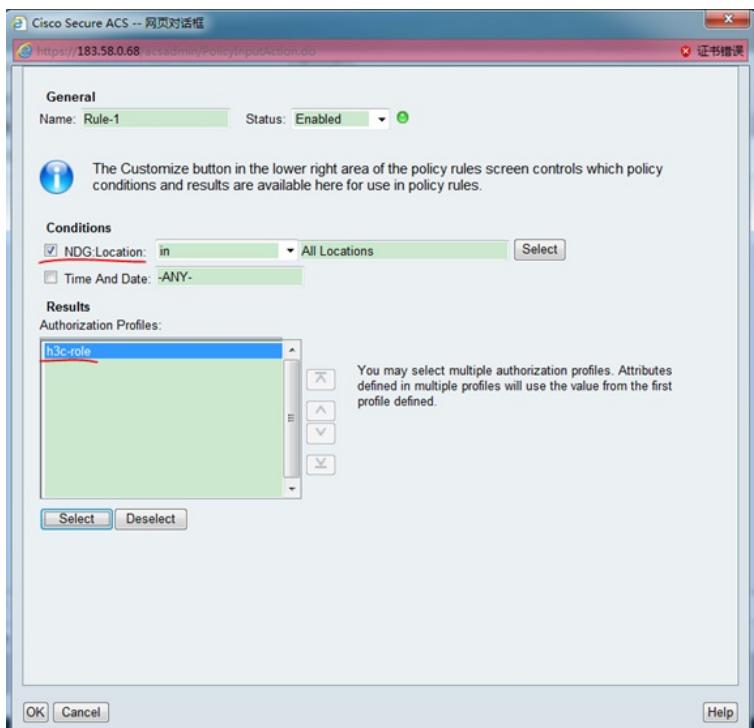
Attributes选择之前创建的User-Roles：

Attribute	Type	Value
User-Roles	String	shell:roles=network-admin

shell:roles=network-admin

Access Policies>Access Services>Default Network Access>Authorization , Policy下面增加一个rule

配置location , Profile选择之前创建的h3c-role。



Save Changes

ACS配置完成。

配置关键点

无