Configuration of Launching SSH by RSA with HWtacacs authentication on S 3600

陈玉龙 2007-04-10 发表

Configuration of Launching SSH by RSA with HWtacacs authentication on S3600* 1 Network requirements:

Before launching SSH by RSA on S3600, user should pass HWtacacs authentication. The following is IP address allocation: **Server:** 192.168.0.15/24,

VLAN 1 on S3600 switch: 192.168.0.1/24 (All ports belong to VLAN 1) PC: 192.168.0.2/24

2 Network diagram:



3 Configuration procedure:

3.1 Enter system view:

<H3C>system-view

3.2 Configure HWtacacs policy:

[H3C]hwtacacs scheme 3com

[H3C-hwtacacs-3com]primary authentication 192.168.0.15

[H3C-hwtacacs-3com]primary authorization 192.168.0.15

[H3C-hwtacacs-3com]primary accounting 192.168.0.15

[H3C-hwtacacs-3com]key authentication expert

[H3C-hwtacacs-3com]key authorization expert

[H3C-hwtacacs-3com]key accouting expert

[H3C-hwtacacs-3com]user-name-format without-domain

3.3 Configure HWtacacs domain:

[H3C-hwtacacs-3com]quit

[H3C]domain 3com

3.4 Bind domain with policy:

[H3C-isp-3com] scheme hwtacacs-scheme 3com

[H3C-isp-3com]accounting optional

3.5 Set 3Com as its default domain:

[H3C-isp-3com]quit

[H3C]domain default enable 3com

3.6 Create a Vlan interface:

[H3C]inter vlan 1

[H3C-vlan-interface1]ip add 192.168.0.1 24

3.7 Configure SSH:

[H3C-vlan-interface1]quit

[H3C]user-interface vty 0 4

[H3C-ui-vty0-4]authentication-mode scheme

[H3C-ui-vty0-4]user privilege level 3

[H3C-ui-vty0-4]protocol inbound ssh

3.8 Configure username and RSA of SSH:

[H3C-ui-vty0-4]quit

[H3C] ssh user lelsw authentication-type rsa

3.9 Use software on client to generate stochastic RSA key and transit public ke y to server. Configure *client public key* on server. Here assign *abc* as public ke y for example:

[H3C] rsa peer-public-key abc

[H3C-rsa-public-key] public-key-code begin

[H3C-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463 [H3C-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913 [H3C-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4 [H3C-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC [H3C-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16 [H3C-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125 [H3C-rsa-key-code] public-key-code end [H3C-rsa-public-key] peer-public-key end

[H3C] ssh user lelsw assign rsa-key abc

4 Configuration Tips:

4.1 Please select new domain you create as the default domain.

4.2 Please add private key (user name and password are on ACS3.1 server) on putty and use it to launch.

*NOTICE: This case is also applicable to H3C S3610 / S5510 / S5500 / S5600 series switch.