S8500交换机 SSH终端服务的配置

罗淳榕 2006-08-28 发表

S8500交换机 SSH终端服务的配置

一、简单介绍

SSH是Secure Shell（安全外壳）的简称。当用户通过一个不能保证安全的网络环境远程登录到交换机时，SSH特性可以提供安全的信息保障和强大的认证功能，以保护交换机不受诸如IP地址欺诈、明文密码截取等攻击。

交换机作为SSH Server，可以接受多个SSH客户的连接，目前支持的版本是SSH2.0；SSH客户端的功能是允许用户与支持SSH Server的交换机、UNIX主机等建立SSH连接。

客户端与服务器端建立SSH通道有两种方式：

？ 通过本地局域网连接

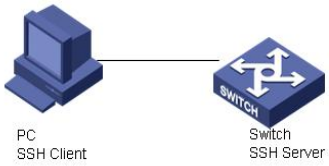
？ 通过广域网连接

二、S8500设备配置实例

1．组网需求

如下图所示，PC终端（SSH Client）上运行支持SSH2.0的客户端软件，与交换机（SSH Server）建立本地连接，更大限度地保证数据信息交换的安全。

2．组网图



SSH Server配置组网图

3. 配置步骤

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]rsa local-key-pair create
The key name will be: H3C_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 1024]:
Generating keys...
......++++++
.....................................++++++
...++++++++
.........++++++++
H3C]user-interface vty 0 4
[H3C-ui-vty0-4]authentication-mode scheme
 Notice: Telnet or SSH user must be added , otherwise operator can't login!
[H3C-ui-vty0-4]protocol inbound ssh
[H3C-ui-vty0-4]local-user lcr
New local user added.
[H3C-luser-lcr]password simple 8500
Updating the password file, please wait...
```

[H3C-luser-lcr]service-type ssh
[H3C-luser-lcr]qu
[H3C]ssh user lcr authentication-type password
三、正确配置状态显示
[H3C]dis ssh server status
SSH version : 1.99
SSH connection timeout : 60 seconds
SSH server key generating interval : 0 hours
SSH Authentication retries : 3 times
SFTP Server: Disable
[H3C]dis ssh server session
Conn Ver Encry State Retry SerType Username
[H3C]dis ssh user-information lcr
Username Authentication-type User-public-key-name Service-type
lcr password null stelnet

[H3C]qu
<H3C>debugging ssh server all
<H3C>t d
Current terminal debugging is on

<H3C>t m
Current terminal monitor is on
*0.8651680 H3C SSH/8/debugging_msg_send:SSH_VERSION_SEND message sen
t on VTY 0
*0.8651897 H3C SSH/8/SSH2 debug:debug info:The server's ssh version sent SSH-
1.9
9-VRP-3.3

*0.8652337 H3C SSH/8/msg_rcv_vty:SSH_VERSION_RECEIVE message received
on VTY 0
*0.8652436 H3C SSH/8/SSH2 debug:debug info:Now the server version is ssh2
*0.8652526 H3C SSH/8/SSH2 debug:debug info: The algorithm negotiation begins
*0.8652617 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_KEXINIT
sent
*0.8652697 H3C SSH/8/SSH2 debug:debug info: SSH2_MSG_KEXINIT received

*0.8652788 H3C SSH/8/SSH2 debug:debug info:kex: client->server aes128-cbc hma
c-s
ha1
*0.8652889 H3C SSH/8/SSH2 debug:debug info:kex: server->client aes128-cbc hma
c-s
ha1
*0.8652991 H3C SSH/8/SSH2 debug:debug info:The key exchange algorithm is
diffie-
hellman-group-exchange-sha1
*0.8653122 H3C SSH/8/SSH2 debug:debug info: The algorithm choose is done
*0.8653213 H3C SSH/8/SSH2 debug:debug info:The key exchange begins
*0.8653294 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_KEX_DH_GEX_REQ
UEST_OLD recei
ved
*0.8653395 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_KEX_DH_GEX_GRO
UP sent
*0.8653485 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_KEX_DH_GEX_REPL
Y sent
*0.8653576 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_NEWKEYS sent

*0.8653657 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_NEWKEYS received

*0.8653749 H3C SSH/8/SSH2 debug:debug info:The key exchange is done
*0.8653829 H3C SSH/8/SSH2 debug:debug info:User authentication begins
*0.8653910 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_SERVICE_REQUEST
received
*0.8654012 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_SERVICE_ACCEPT s

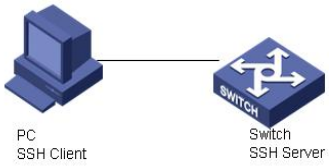
ent
*0.8654223 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_USERAUTH_REQUE
ST received wi
th user:lcr,service:ssh-connection,method:
none
*0.8654385 H3C SSH/8/SSH2 debug:debug info:None method authentication begins

*0.8654475 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_USERAUTH_FAILUR
E sent in pas
sword
*0.8656286 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_USERAUTH_REQUE
ST received wi
th user:lcr,service:ssh-connection,method:
password
*0.8656445 H3C SSH/8/SSH2 debug:debug info:Password authentication begins
*0.8656536 H3C SSH/8/SSH2 debug:debug info:Password: ********** received
*0.8656627 H3C
SSH/8/debugging_msg_send:SSH2_MSG_USERAUTH_SUCCESS message sent o
n VTY 0
*0.8656738 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_USERAUTH_SUCCE
SS sent
*0.8656829 H3C SSH/8/SSH2 debug:debug info:User authentication is done
*0.8656920 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_CHANNEL_OPEN re
ceived
*0.8657011 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_CHANNEL_OPEN_C
ONFIRMATION
sent
*0.8657122 H3C SSH/8/SSH2 debug:debug info:Channel is opened
*0.8657193 H3C SSH/8/msg_rcv_vty:SSH_SMSG_PUBLIC_KEY message received
on VTY 0
*0.8657294 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_CHANNEL_SUCCES
S sent
*0.8657386 H3C SSH/8/msg_rcv_vty:SSH_MSG_DISCONNECT message received
on VTY 0
*0.8657475 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_CHANNEL_SUCCES
S sent
%Aug 11 16:50:51 2006 H3C SHELL/5/LOGIN: lcr login from 192.168.0.2
*0.8657830 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8658042 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8658426 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8658659 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8658801 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8659527 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8661204 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8661529 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8663123 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8663356 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8663447 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8663669 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8663760 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
*0.8663911 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT

Y 0
*0.8664780 H3C SSH/8/msg_rcv_vty:SSH_CMSG_USER message received on VT
Y 0
<H3C>
%Aug 11 17:01:05 2006 H3C SHELL/5/LOGOUT: lcr logout from 192.168.0.2
*0.9271733 H3C SSH/8/SSH2 debug:debug info:SSH2_MSG_DISCONNECT sent.

四、客户端登陆

运行putty.exe，出现如下界面，在Host Name一栏中输入交换机IP地址



点击Open后出现登陆界面，输入用户名和密码即可登陆。SSH登陆默认的操作权限是最低级0级，因此可以用super命令并输入密码提高自己操作权限级别。Super权限级别及密码事先应在交换机上设置好，不然SSH登陆后只能是0级观看权限。