How capture the packet on the firewall

Limitation: a.Currently, this function can only use in the CLI, WebUI is not supported.

b. Not all the firmware version were supported this function.

Purpose: To capture the packet on the firewall, we should use the ***pcapdump*** command

```
DFL-860:/> pcapdump
 Valid options: -cleanup, -show, -start, -status, -stop, -wipe, -write, <enter>
```

Procedure:

1. To start capture the packet on the lan interface we can do the following command:

DFL-860:/> pcapdump -start lan

Starting packet capture on: lan

```
DFL-860:/> pcapdump -start lan
Starting packet capture on: lan
```

You can also capture the other interface

2. Type the following for stop capturing the packet on the lan:

DFL-860:/> pcapdump -stop lan

Stopping packet capture on: lan

```
DFL-860:/> pcapdump -stop lan
Stopping packet capture on: lan
```

3. Put the capturing packet in a file(Test.cap) by typing the following command:

DFL-860:/> pcapdump -write -filename=Test.cap lan

```
DFL-860:/> pcapdump -write -filename=Test.cap lan
Dumping capture for lan to "Test.cap"
```

4. Check the Test.cap file is created in the root directory by the following command:

DFL-860:/> ls

```
DFL-860:/> pcapdump -write -filename=Test.cap lan
Dumping capture for lan to "Test.cap"
DFL-860:/> ls
HTTPALGBanners/
HTTPAuthBanners/
Test.cap
certificate/
config.bak
full.bak
script/
selftest.txt
sshclientkey/
```

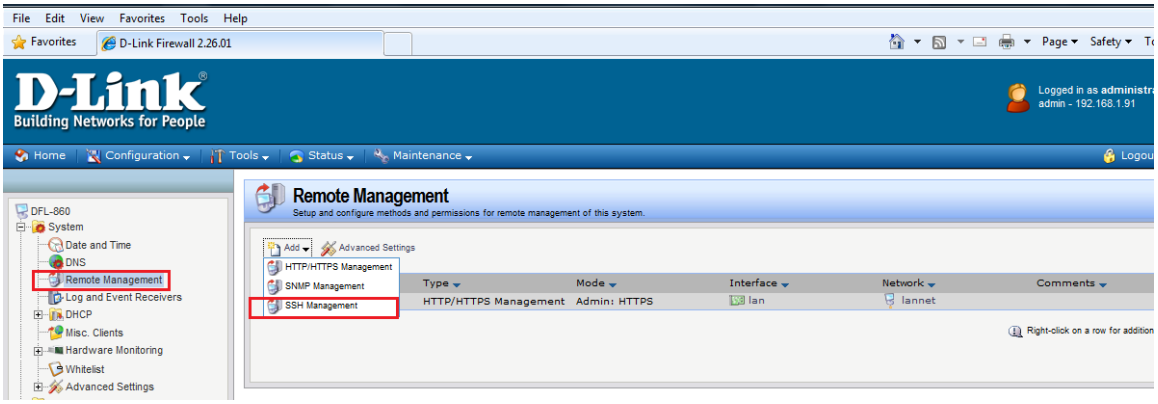
How to get the file from the firewall to local PC

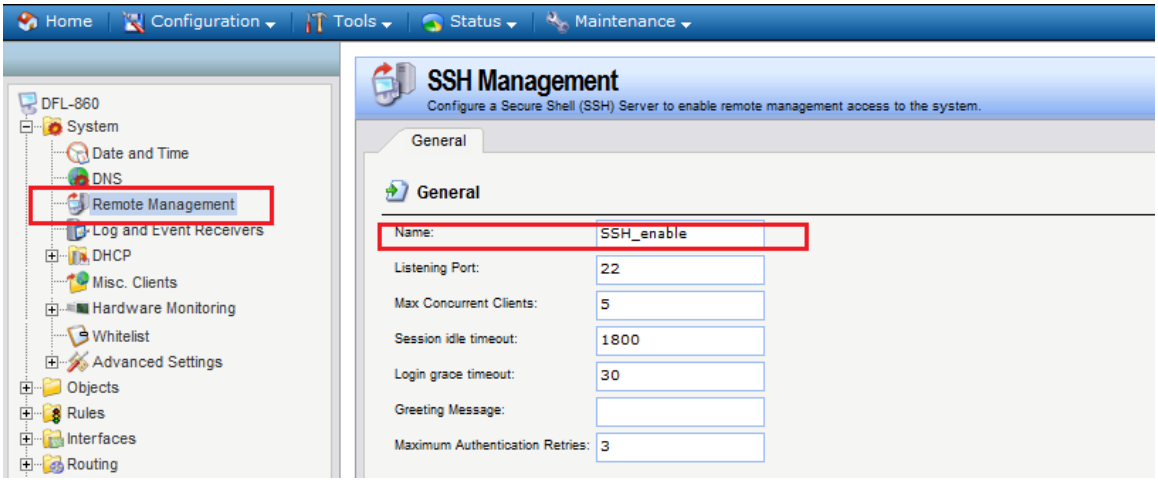
[Topology]:

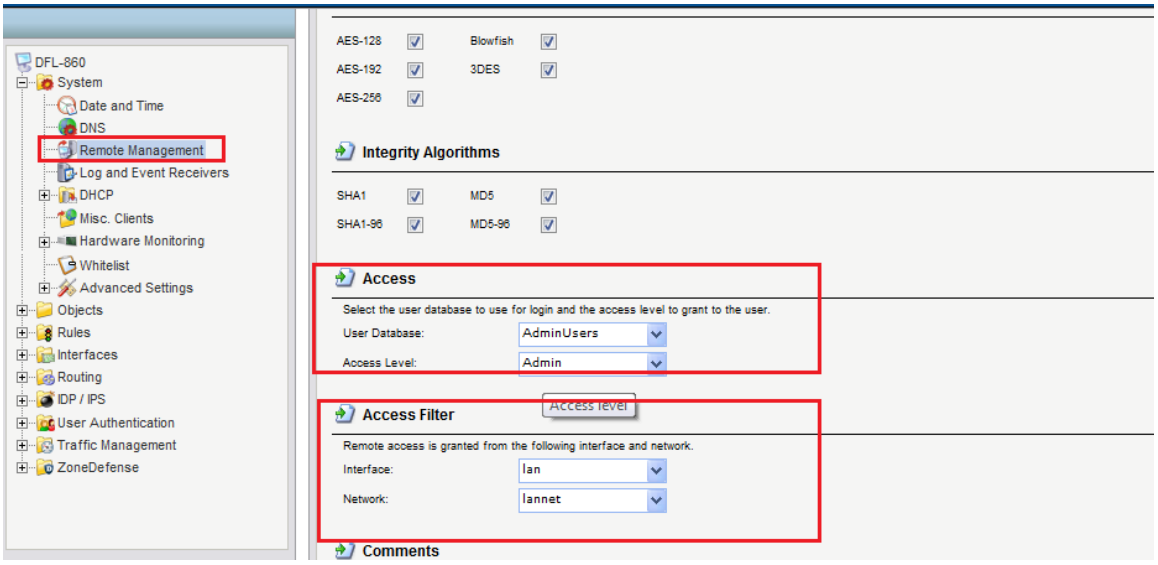
PC(192.168.1.91/24)----------LAN(192.168.1.1/24)DFL-860

[Procedure]:

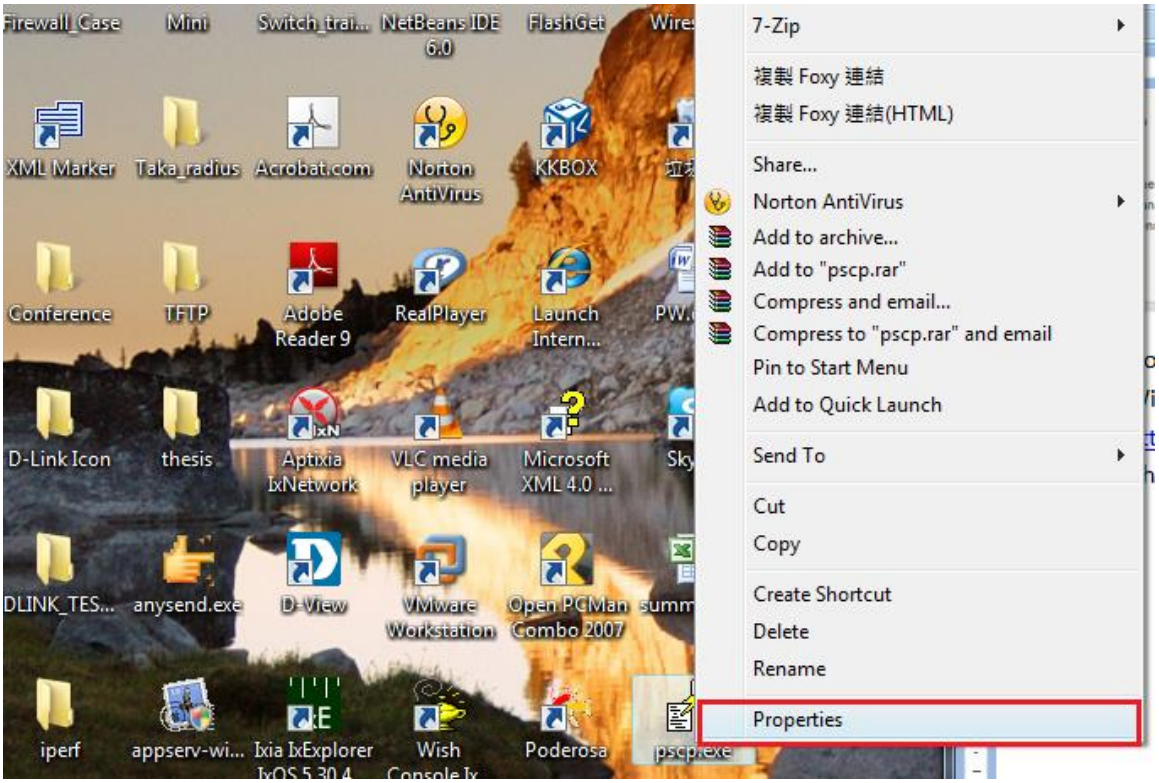
1. Check the firewall has open the ssh function via the following:

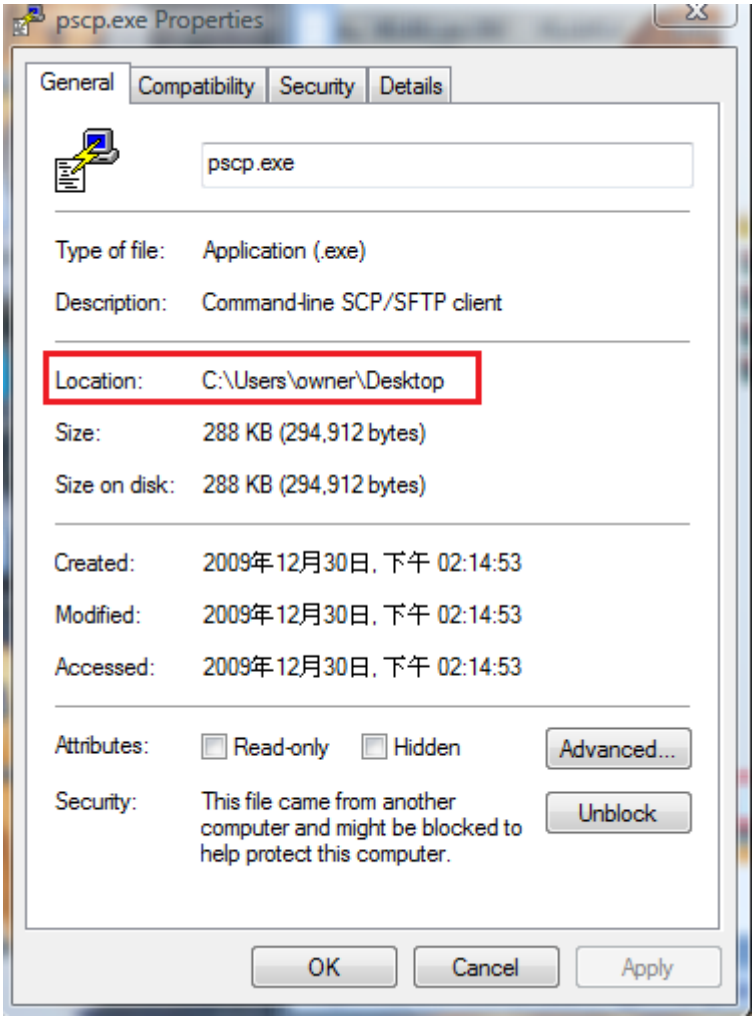




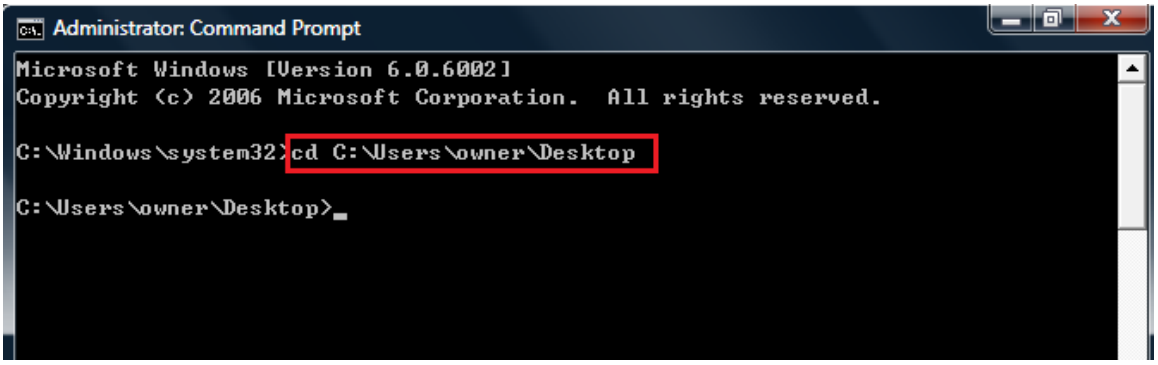


2. Download the software PSCP software from the following website since we are using Windows system on the PC: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
3. Check the path of pscp.exe file via the following steps:

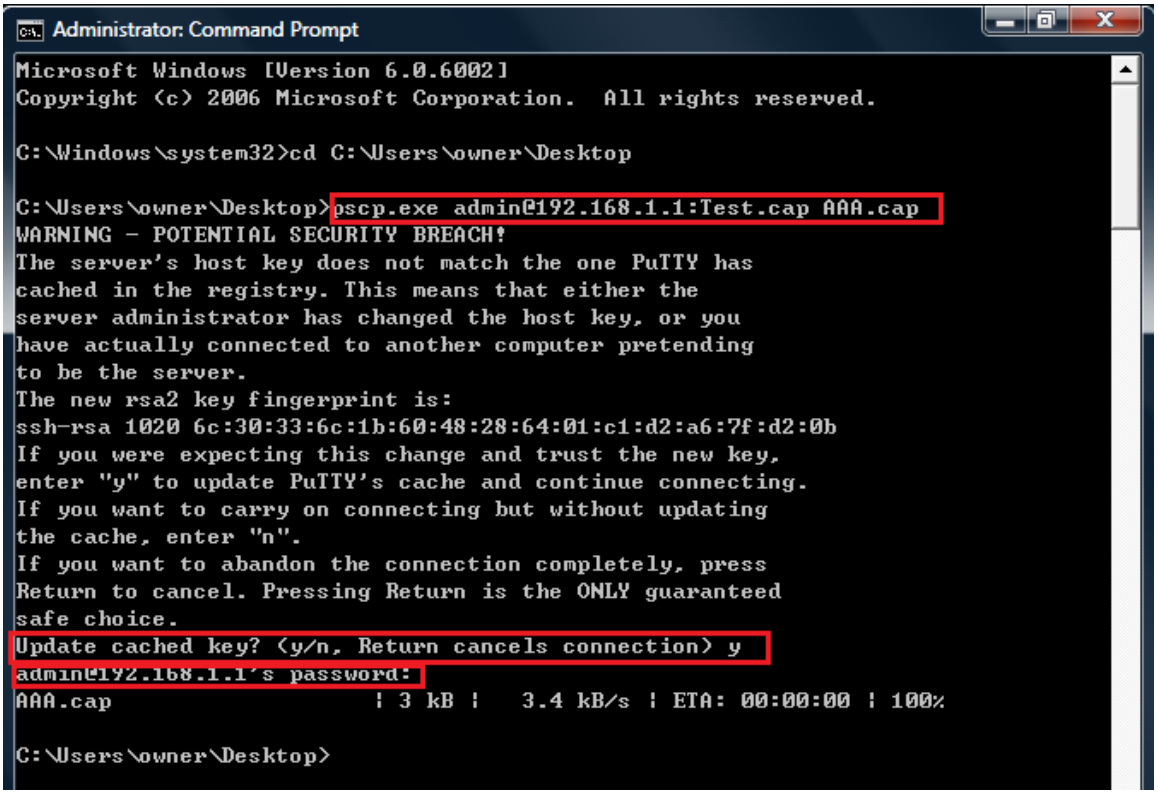

Firewall_Case
Mini
Switch_trai...
NetBeans IDE 6.0
FlashGet
XML Marker
Taka_radius
Acrobat.com
Norton AntiVirus
KKBOX
Conference
TFTP
Adobe Reader 9
RealPlayer
Launch Intern...
D-Link Icon
thesis
Aptixia IxNetwork
VLC media player
Microsoft XML 4.0 ...
DLINK_TES...
anysend.exe
D-View
VMware Workstation
Open PCMan Combo 2007
iperf
appserv-wi...
Ixia IxExplorer
Wish
Poderosa
pscp.exe
7-Zip
複製 Foxy 連結
複製 Foxy 連結(HTML)
Share...
Norton AntiVirus
Add to archive...
Add to "pscp.rar"
Compress and email...
Compress to "pscp.rar" and email
Pin to Start Menu
Add to Quick Launch
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties



4. Copy the location of this software part and open the **command prompt, then change it** to this location like the following:



5. Download the file via the following command:



The syntax is **pscp.exe** ***admin_account@Firewall_IP:filename_onfirewall local_PC_filename***

6. After you checked the file is downloaded to local PC, you can type the following command to erase the file on the firewall:

```
DFL-860:/> pcapdump -cleanup
PCAPDump cleaned up.
```