Пример настройки межсетевых экранов D-Link NetDefend

Как захватить пакеты на межсетевом экране

Ограничения:

a. На данный момент данная возможность доступна только через командную строку.

В веб интерфейсе она не доступна.

b. Не все версии программного обеспечения поддерживают эту возможность.

Цель: Для захвата пакетов на межсетевом экране необходимо использовать команду ***pcapdump***

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

Процедура:

1. Для того, что бы начать захватывать пакеты на lan интерфейсе, необходимо выполнить следующую команду:

DFL-860:/> pcapdump -start lan

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

Так как размер буфера межсетевого экрана, выделенный для захвата пакетов ограничен (по умолчанию – 512К), то рекомендуется задать фильтр для захватываемых пакетов, что бы межсетвой экран захватывал только те пакеты, которые необходимы. При захвате всех пакетов буфер может очень быстро заполниться, и в него могут не попасть необходимые пакеты. Фильтр указывается в команде start.

```
pcapdump -start [<interface(s)>] [-size=<value>] [-snaplen=<value>]
         [-count=<value>] [-out] [-out-nocap] [-eth=<Ethernet Address>]
         [-ethsrc=<Ethernet Address>] [-ethdest=<Ethernet Address>] [-ip=<IP4
         Address>] [-ipsrc=<IP4 Address>] [-ipdest=<IP4 Address>]
         [-port=<0...65535>] [-srcport=<0...65535>] [-destport=<0...65535>]
         [-proto=<0...255>] [-icmp] [-tcp] [-udp] [-promisc]
         [-ipversion=<1...15>]
```

Например, нам необходимо захватить пакеты telnet сессии:

```
 DFL-860:/> pcapdump -start lan -destport=23
Starting packet capture (port 23) on: lan
```

2. Для того, что остановить захват пакетов на lan порту необходимо дать следующую команду:

DFL-860:/> pcapdump -stop lan

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

3. Что бы поместить, захваченные пакеты в файл (Test.cap), необходимо ввести следующую команду:

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

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

4. Проверить наличие созданного файла Test.cap в root директории можно следующей командой:

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/
```

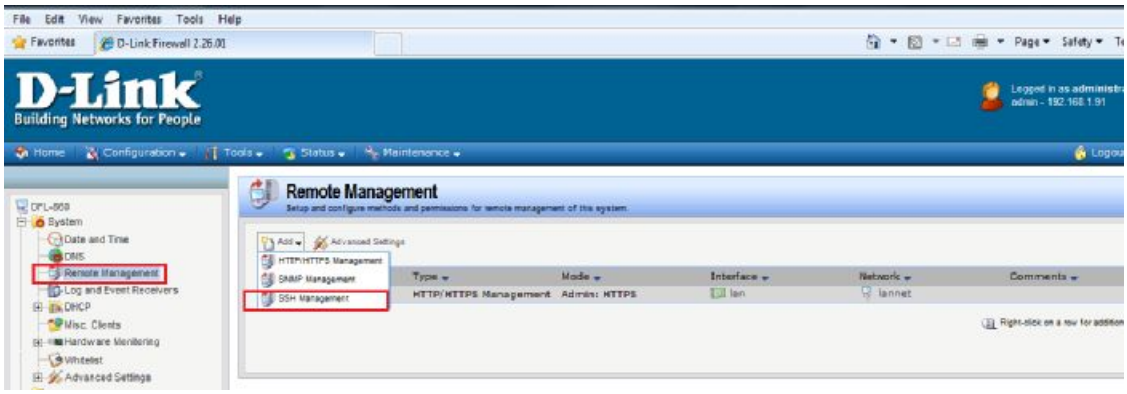
Как загрузить файл с межсетевого экрана на локальный компьютер

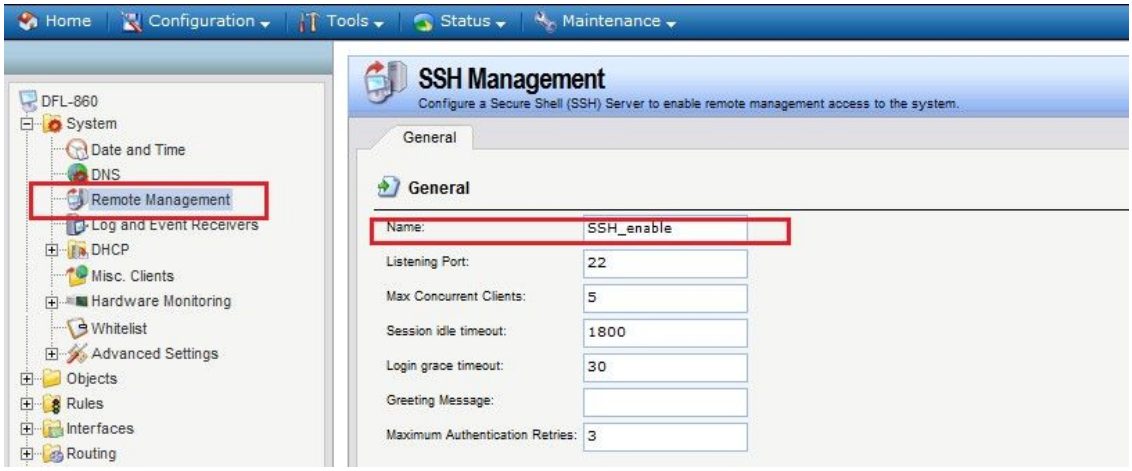
[Топология]:

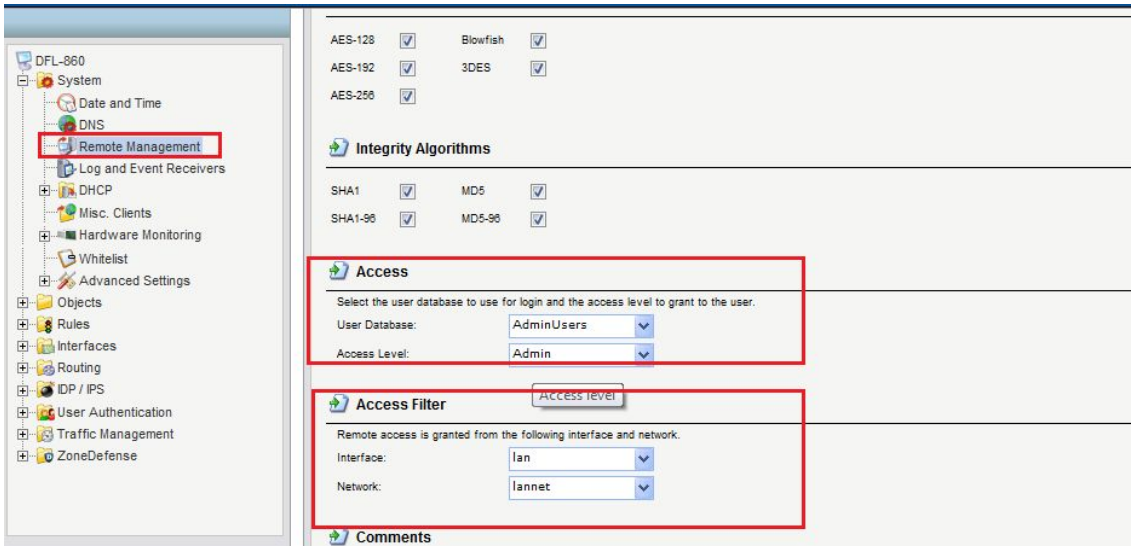

PC(192.168.1.91/24)----------LAN(192.168.1.1/24)DFL-860

[Процедура]:

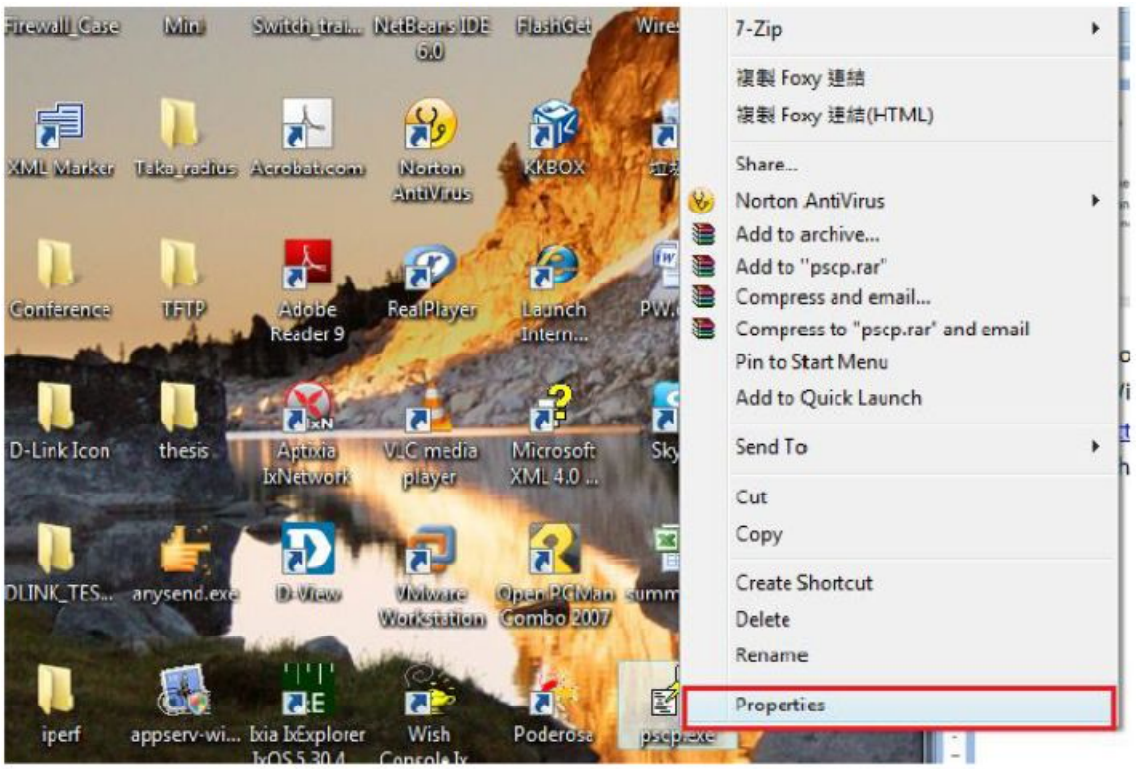
1. Проверьте что бы на межсетевом экране было разрешено удалённое управление по ssh:

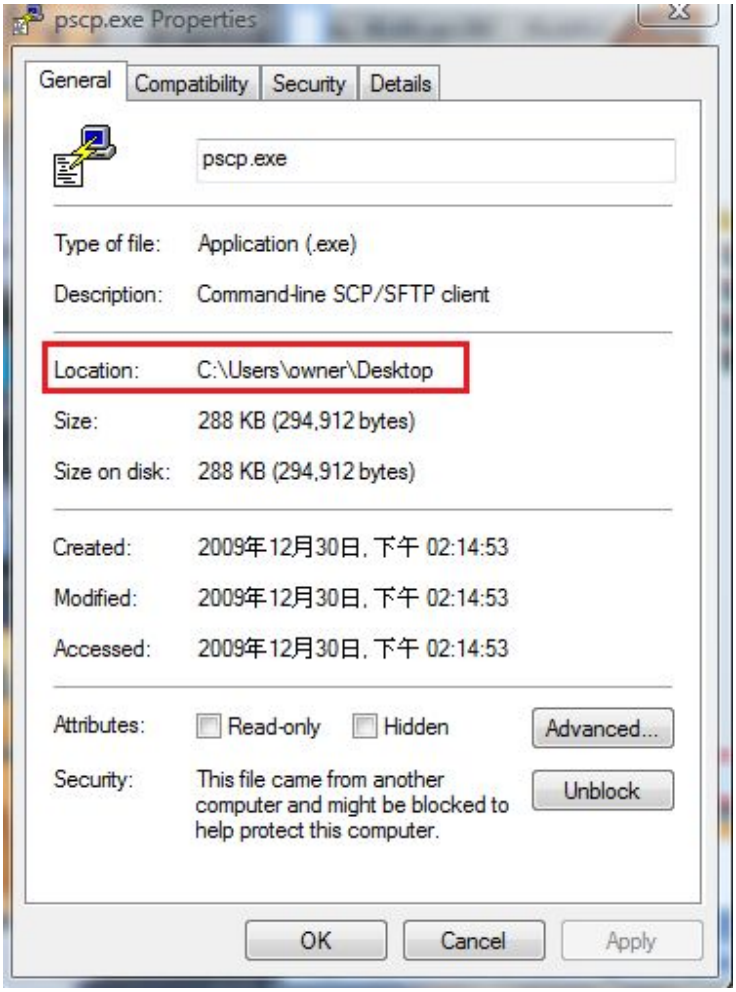




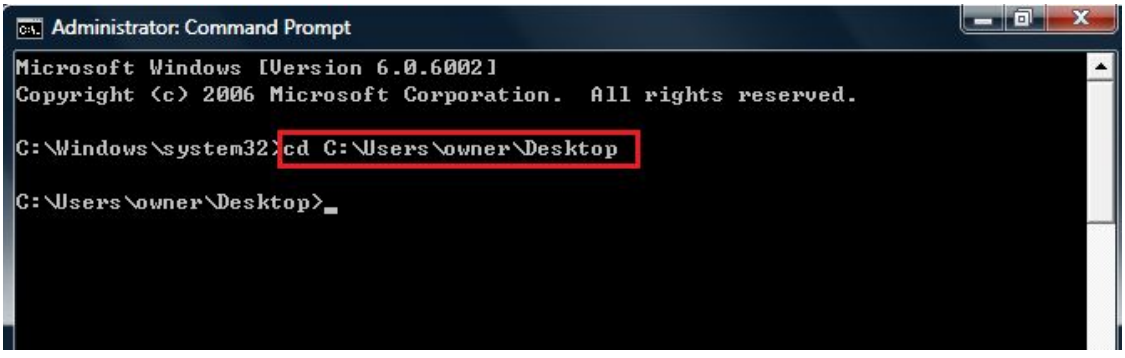


2. Если вы используете Windows OS, то вам необходимо загрузить PSCP ПО со следующего сайта: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
3. Проверьте, где находится ваш файл pscp.exe:

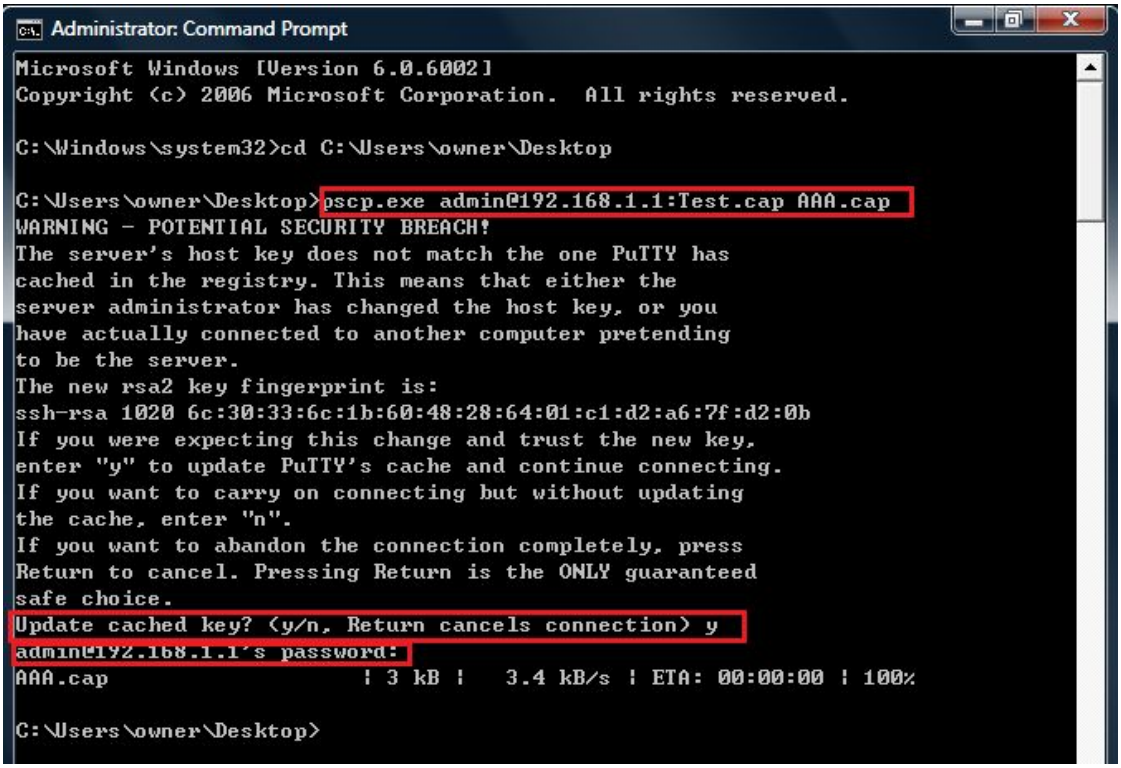

Firewall_Case
Min
Switch_trai...
NetBeans IDE 6.0
FlashGet
XML Marker
Teka_radius
Acrobat.com
Norton AntiVirus
KKBOX
Conference
TFTP
Adobe Reader 9
RealPlayer
Launch Intern...
D-Link Icon
thesis
Aptixia IxNetwork
VLC media player
Microsoft XML 4.0 ...
DLINK_TES...
arysend.exe
D-View
VMware Workstation
Open PGMan Combo 2007
iperf
appserv-wi...
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. Скопируйте местонахождение вашего файла, затем **перейдите в режим командной строки и измените своё местоположение** на директорию, в которой находится файл pscp.exe :



5. Загрузите файл захваченных пакетов Test.cap при помощи следующей команды:



Синтаксис: **pscp.exe** ***admin_account@Firwall_IP:filename_onfirewall local_PC_filename***
Если будет запрошено обновление закешированного ключа, то ответьте "y" (yes). После запроса пароля введите пароль**.**

6. После того, как вы проверите, что файл Test.cap загружен на локальный компьютер, его можно будет удалить на межсетевом экране при помощи следующей команды:

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

Юникс пользователи для загрузки файла с межсетевого экрана могут воспользоваться аналогичной утилитой - SCP:

owner@owner-desktop:~$ scp admin@192.168.1.1:Test.cap owner@192.168.1.91:/home/owner/AAA.cap

Просмотреть файл захваченных пакетов можно любым сетевым анализатором, поддерживающим формат pcap, например, при помощи wireshark http://www.wireshark.org/.