router - Podrška #14062

kako kreirati ssh public key na openwrt-u ?

23.04.2008 12:52 - Ernad Husremović

Status:	Zatvoreno	**Početak:**	23.04.2008
Prioritet:	Normalan	**Završetak:**	
Odgovorna osoba:	Jasmin Beganović	**% završeno:**	100%
Kategorija:		**Procjena vremena:**	0.00 sat
Ciljna verzija:			

Opis

ovo nam treba za router-wan-rg-2 da može pristupiti passwordless archive.rama-glas.com

zaključak:

1. na ubuntu host-u instalirati dropbear
   - apg-get install dropbear
2. generisati standardni ssh ključ
3. dropbearconvert-om dobiti dropbear compatibilan private ključ
   - /usr/lib/dropbear/dropbearconvert openssh dropbar ~/.ssh/openwrt.key ~/.ssh/openwrt_dropbear.key
4. prebaciti public i private key na openwrt router
5. public key dodati u ~/.ssh/authorized_keys hosta kome želimo pristupiti passwordless

Historija

#1 - 23.04.2008 13:51 - Ernad Husremović

root@router-wan-sa-1:/# ipkg -d net install dropbearconvert

```
Installing dropbearconvert (0.50-3) to net...
Downloading http://openwrt.bring.out.ba/packages/brcm-2.4/./dropbearconvert_0.50-3_mipsel.ipk
Configuring dropbearconvert
Done.
```

root@router-wan-sa-1:/# ipkg files dropbearconvert

```
Package dropbearconvert (0.50-3) is installed on net and has the following files:
/mnt/1/usr/bin/dropbearconvert
```

root@router-wan-sa-1:/# /mnt/1/usr/bin/dropbearconvert

```
All arguments must be specified
Usage: /mnt/1/usr/bin/dropbearconvert <inputtype> <outputtype> <inputfile> <outputfile>

CAUTION: This program is for convenience only, and is not secure if used on
untrusted input files, ie it could allow arbitrary code execution.
All parameters must be specified in order.

The input and output types are one of:
openssh
dropbear

Example:
dropbearconvert openssh dropbear /etc/ssh/ssh_host_rsa_key /etc/dropbear_rsa_host_key
```

#2 - 23.04.2008 13:53 - Ernad Husremović

a da li taj convert mogu uraditi na ubuntu host-u ?

hernad@nmraka-1:~$ sudo apt-get install dropbear

```
..
Unpacking dropbear (from .../dropbear_0.50-2_amd64.deb) ...
Setting up dropbear (0.50-2) ...
```

```
Converting existing OpenSSH RSA host key to Dropbear format.
Key is a RSA key
Wrote key to '/etc/dropbear/dropbear_rsa_host_key'
Converting existing OpenSSH RSA host key to Dropbear format.
Key is a DSS key
Wrote key to '/etc/dropbear/dropbear_dss_host_key'
OpenSSH appears to be installed.  Setting /etc/default/dropbear so that
Dropbear will not start by default.  Edit this file to change this behaviour.

NO_START is not set to zero.
```

vidim da je postojeći rsa key konvertovan u dropbear format ... znači trebalo bi da može

#3 - 23.04.2008 13:54 - Ernad Husremović

evo ga: isti utility imamo i na ubuntu host-u

hernad@nmraka-1:~$ /usr/lib/dropbear/dropbearconvert

#4 - 23.04.2008 14:04 - Ernad Husremović

evo i konkretnog primjera, na ubuntu host-u

Enter file in which to save the key (/home/hernad/.ssh/id_rsa): /home/hernad/.ssh/openwrt.key

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/hernad/.ssh/openwrt.key.
Your public key has been saved in /home/hernad/.ssh/openwrt.key.pub.
The key fingerprint is:
77:23:7a:88:57:6d:1f:02:57:d7:e3:4a:33:e4:8b:60 hernad@nmraka-1
```

hernad@nmraka-1:~$ /usr/lib/dropbear/dropbearconvert openssh dropbar ~/.ssh/openwrt.key ~/.ssh/openwrt_dropbear.key

```
Key is a RSA key
Wrote key to '/home/hernad/.ssh/openwrt_dropbear.key'
```

na router (primjer router-wan-rg-2) kopiramo ključ:

- scp /home/hernad/.ssh/openwrt.key.pub root@router-wan-rg-2:/etc/dropbear/router-wan-rg-2.pub[1]
- scp /home/hernad/.ssh/openwrt_dropbear.key root@router-wan-rg-2:/etc/dropbear/router-wan-rg-2.key

također sadržaj javnog ključa dodamo na host kome želimo pristupiti passwordless - npr **archive.rama-glas.com:/root/.ssh/authorized_keys**

[1] držati se konvencije da taj set ključeva ima ime <hostname>.key, <hostname>.pub

#5 - 23.04.2008 17:29 - Ernad Husremović

- Status promijenjeno iz Dodijeljeno u Zatvoreno

#6 - 24.04.2008 09:40 - Ernad Husremović

- Status promijenjeno iz Zatvoreno u Dodijeljeno

- Odgovorna osoba promijenjeno iz Ernad Husremović u Jasmin Beganović

- % završeno promijenjeno iz 0 u 80

jasko sa ovim instrukcijama ipak nije uspo podesiti publickey konekciju, trebamo vidjeti šta još treba ovdje reći

#7 - 24.04.2008 09:43 - Ernad Husremović

pretpostavljam da je jasko testirao passwordless konekciju sa jednostavnim

$ ssh root@archive.rama-glas.com što je sa dropbear-om nedovojno, u mrežnoj skripti /mnt/1/etc/init.d/init-b-out-ba, i u /etc/refresh_ip.sh može se vidjeti kako to hoda - treba koristiti "-i" parametar

#8 - 24.04.2008 09:48 - Ernad Husremović

u /etc/refresh_ip imamo

```
ssh -y -i /etc/dropbear/${HOSTNAME}.key root@${NAMESERVER} service named restart ..
```

znači test passwordless pristupa na archive.rama-glas.com bi bio

```
ssh -y -i /etc/dropbear/router-wan-rg-2.rama-glas.com.key root@archive.rama-glas.com
```

#9 - 24.04.2008 11:35 - Ernad Husremović

- Status promijenjeno iz Dodijeljeno u Zatvoreno

- % završeno promijenjeno iz 80 u 100

jasko je provjerio, pubickey pristup radi sa navođenjem "-i" switch-a