Knockd is a utility that can enhance security on your network. Until dd-wrt moves /etc to rw space there is going to be problems with a lot of ipkg installs. The following details a workaround but is not considered ideal. Knockd will perform whatever action you script only when a special knock sequence is given. A knock sequence is defined as a series of either TCP or UDP requests on defined ports. These ports do not even have to be open.

For example, a script could be written to forward the SSH port (port 22) to a specific LAN host for 20 seconds when the knock sequence is given. This knock sequence could be defined as connecting to port 22 twice with UDP, port 151 once with TCP, and then port 15 with UDP, for example.

Port Scanning the routers WAN interface would yield no ports open. If the port scan was run again within 20 seconds of sending the knock sequence, the scan would yeild that port 22 was open. This could enhance security as most attacks begin with port scans to determine what services you have open, and port 22 wouldn't show up unless the attacker both expected you to be running knockd *AND* took the time to deterime the knock sequence.

A knock sequence of connecting with either udp or tcp on port 1, followed by port 2, followed by port 3, followed by port 4, followed by port 5 could be used to launch a script that closes all ports on the router, or even disables the WAN port for 60 seconds before bringing it back up. In this way you are protecting yourself from attackers as soon as a port scan is detected.

It is recommended that you know how to:

... use the command line
... have the ability with SCP to copy files to and from your desktop setup
... have knowledge of using ipkg to install packages
... jffs configured if you don't want to install to ram

If you're running Windows on your desktop you need:

```
-Vim, Win32Pad, Crimson Editor or Notepad2
 (or other *nix friendly text editor. DO NOT USE NOTEPAD)
```

Contents

Installation

NB.
http://www.dd-wrt.com/phpBB2/viewtopic.php?t=5935&view=previous&sid=4e92151d09fa5d4a0a69f0294ce7eb32
tells of problems with these instructions, and an alternate solution.

Install the libpcap package

Knockd depends on libpcap's presence. If it isn't installed, install it

```
-telnet or ssh shell into the router
-run the command ipkg -d <dest_name> install libpcap

<dest_name> should be root to install to /jffs
<dest_name> should be ram to install to /tmp
    *Remember, /tmp is deleted on router reboot*
Ex: ipkg -d root install http://openwrt.alphacore.net/libpcap_0.8.3-1_mipsel.ipk

 The default is root so a simpler way of doing this is unless you want to
 install to /tmp space just do

 'ipkg install libpcap'
```

Install the knockd package

```
-Find the knockd package in the OpenWRT Package Tracker.
 You will need the URI of package to install it.

-telnet or ssh shell into the router
-run the command ipkg -d <dest_name> install <URI of package>

<dest_name> should be root to install to /jffs
<dest_name> should be ram to install to /tmp
    *Remember, /tmp is deleted on router reboot*
Ex: ipkg -d ram install http://openwrt.alphacore.net/knockd_0.4_mipsel.ipk
```

Adjust knockd.conf to DD-WRT

for the "open sesame" rule, replace "-A INPUT" by "-I INPUT" (the last rule is a generic DROP one, and control would never reach the appended rule)

Configure LD PATH

at the command prompt type the following

```
$ LD_LIBRARY_PATH=/lib:/usr/lib:/jffs/lib:/jffs/usr/lib
$ export LD_LIBRARY_PATH
```

You will need to set this every time the router reboots, or include it in your Startup Scripts

Usage & Troubleshooting

General Usage

You will need to pass a different config file at startup (again because of /etc not being writable) this is however quite easy. just type

knockd -d -c /jffs/etc/knockd.conf

or replace that path with wherever your conf file is.

Also note the default interface is eth0, if you are using ppp you will need to do something like this (adjust for you interface and conf file)

knockd -d -i ppp0 -c /jffs/etc/knockd.conf

See the knockd homepage

Troubleshooting

See the knockd homepage

If you get the error "knockd: can't load library 'libpcap.so.0.8" do the following:
Then you either haven't installed libpcap or you haven't updated your LD_LIBRARY_PATH env see above section.

Load on router startup

```
either point rc_startup at it or have rc_startup point to a general
startup script which includes starting knockd as above.
fwiw, my rc_startup points at a startup script say /jffs/.init
I then use that script to set up any aliases or env variables and
start programs such as knockd.
```

An example (to be included in your regular startup script)

```
#!/bin/sh
export LD_LIBRARY_PATH=/lib:/usr/lib:/jffs/lib:/jffs/usr/lib
knockd -d -i ppp0 -c /jffs/etc/knockd.conf

This will start knockd in daemon mode listening on initerface ppp0 using the config
```

```
from /jffs/etc/knockd.conf. If you have a different interface (ie eth0) or a different
config file you will obviously need to adjust this to suit.
```

Security

personal opinions on Security Port knocking is not a means of security and has been compromised in the past. First off, its only a means of authentication, not a means of protection. A sniffer sitting between the client and the router could easily pick up on the sequence and repeat it. Also, a few tools are out there that can be used to "brute force" this technique. In general, Port Knocking is not secure. A better solution is VPN tunnels, since they employ strong authentication and encryption. Furthermore, port knocking is also vulnerable to spoofing. If a hacker is able to spoof his/her IP, they could prevent a legitimat user from doing the sequence by interupting the pattern. Also mentioned was the fact that it protected the router from port scanning attacks. A better means of protection (Again VPN being ideal if the services are only meant for the outside world) is to ban the IP address attempting to port scan the router. So if the attacker where to scan TCP ports 1 2 3 4 in sequence, the router would add a iptables rule saying "If <IP Address> attempts to connect, drop." Also, the mention of knocking ports 1-5 and running a script to disable the WAN port or shutdown the router leaves open the possibility of DOS attacks. Since port knocking keeps track of the IP address of the knocker, it is entirely possible to use multiple IP addresses to port scan the router in order to prevent any pattern of arising. Also, tools like NMAP have time delays to prevent the firewall from knowing its being portscanned. If someone where to portscan the router using 3 different IP addresses with a 2 second delay between each port and random port numbers, port knocking (as a means of protection) would not work. In general, port knocking is a big No No.. If you want real security, secure the services behind the firewall and use a VPN connection when necessary..

== That's one users's opinion. I'd like to add, installing any VPN on the router will require port forwarding. If the port(s) are only forwarded when a user has properly authenticated using the correct knock sequence, well, that's sort of like adding an extra password to your VPN. The thing the person above forgets is that we are not talking about running port knocking on enterprise networks, but on home routers, and port knocking is still extremely obscure, so planned denial of service attacks like those described above will only happen if your friends know your running a port knocking daemon. Nobody else is even going to consider it...

== In fact, to agree with the second user, port knocking is an efficient way to protect against "scan and attack" methods. If the SSL daemon (or VPN server, whatever you like) that a relatively advanced home user is running is later found to have a security flaw, they are much better off hiding the fact that it even exists. Corporate networks are policed by paid professionals whose job it is to watch for vulnerabilities and keep software up to date. Home networks, even those run by competent professionals, simply cannot be updated as accurately as a part time job/hobby.

Another Perspective

The above arguments annoy me greatly, they are both misleading and contradictory. Port Knocking implemented incorrectly, like anything is a security risk. But lets be clear Port Knocking is nothing but a trigger, and it is what is triggered that can cause problems. The above author suggests VPN as an alternative to Port Knocking, these are two completely different things. Instead I would suggest using a knock daemon to add another level of security to a VPN. Any services you run on your LAN that you want to be able to access externally will need to have some sort of allowances (weakening) of your security. A great function of a knock daemon is that instead of say leaving a VPN or SSH port open 24/7 you can open it remotely as

required for as long as required. But what about replay attacks etc etc sure these are all possible exploits although you do have the option of using one time knock sequences from a pre-defined list which makes a replay attack useless. But that isn't even the point, the point is that at best if someone uses the correct knock sequence all they would achieve is to open say port 22 which would have otherwise been open anyway, and is still locked down by your ssh daemon.

And lastly I was completely baffled by the portscanning argument. First the author suggests that a better method is to simply ban the ip address of any ip thought to be doing a port scan of your router (most software firewalls can do this dynamically). But the author then explains some of the very reasons why this method is not very good and even suggests ways around having a portscan detected. None of which has any relevance to Port Knocking because unless in this portscan from multiple spoofed IP's the would be hacker magically got a knock sequence correct ALL ports would be stealthed. As opposed to without your knock daemon where the VPN ports the author seems to love so much would be revealed.

External links

- Linux Journal's General Discussion of Port Knocking
- knockd official wiki
- Slashdot "Port Knocking" For Added Security
- Port Knocking on Linux Journal
- PortKnocking.org