Enhancing HPC Administration Security with Port Knocking Technique

Irfan Syamsuddin

CAIR Center for Applied ICT Research
Politeknik Negeri Ujung Pandang Makassar INDONESIA

Introduction

Problem Statement

Basically in order to provide users with ease of access High Performance Computing (HPC) systems gives unrestricted use of its internal network [1]. Although adequate access control (without encryption) always be applied, HPC systems does not provide a method to authenticate administrative access by network administrator, thus opening possible cyber threats in the future [2].

Purpose

This study proposes the utilization of Port Knocking technique [3] in order to hide administrative access of Firewall external attackers. Our experiments show an improved security mechanism by HPC admin both for SSH and FTP services.

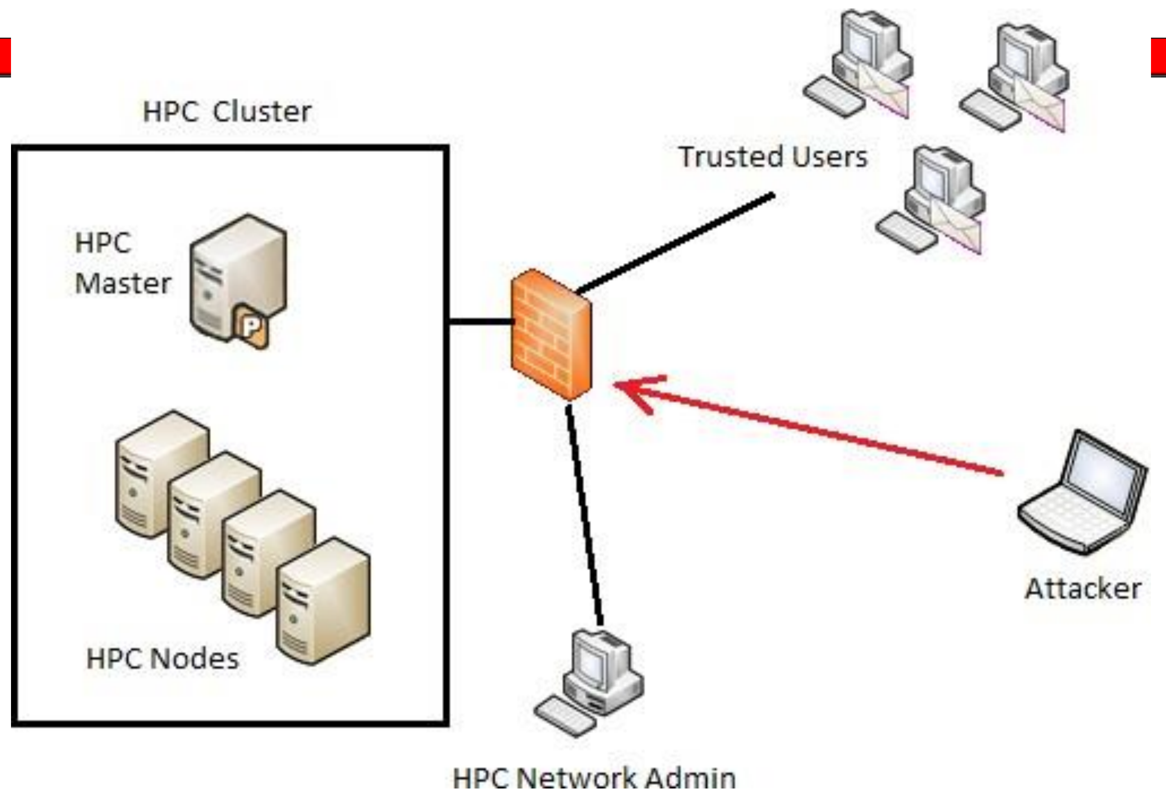
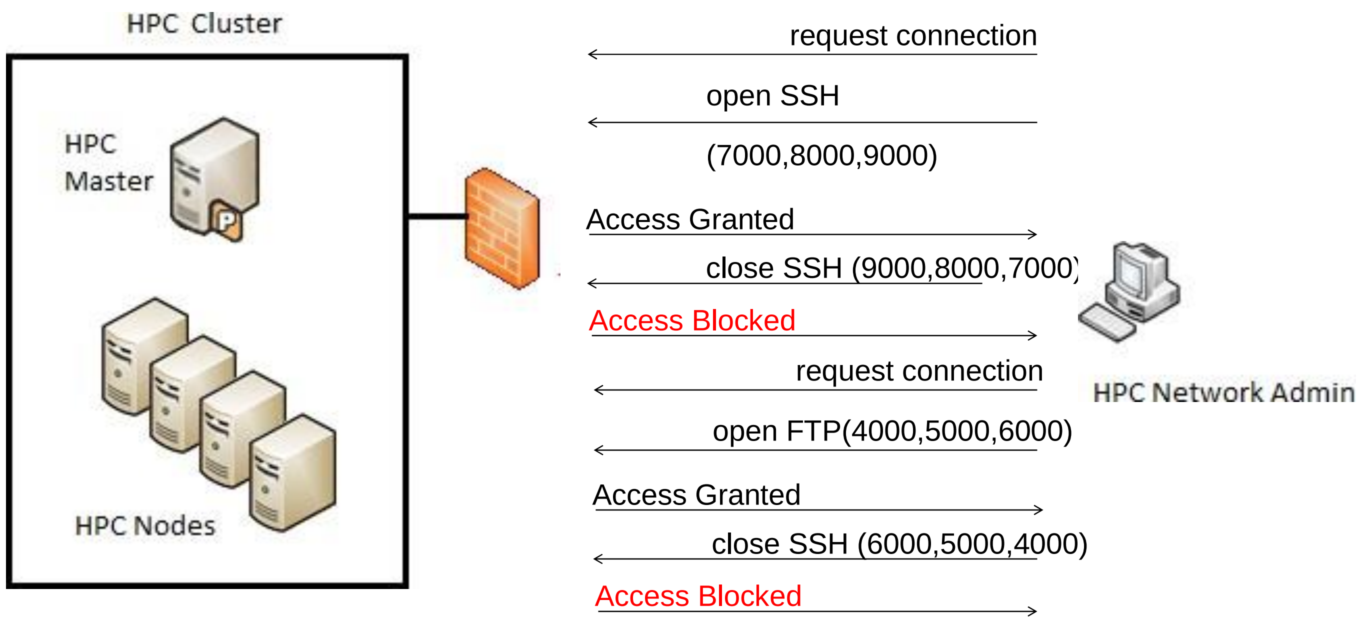


Fig. 1. Firewall to secure HPC Systems from attack



request connection

open SSH

(7000,8000,9000)

Access Granted

close SSH (9000,8000,7000)

Access Blocked

request connection

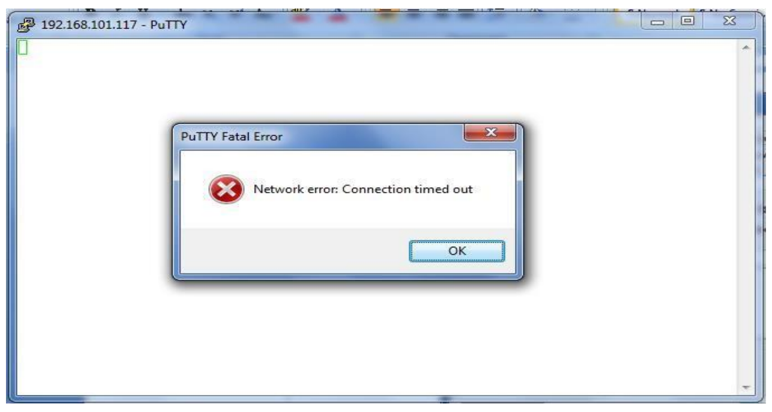
open FTP(4000,5000,6000)

Access Granted

close SSH (6000,5000,4000)

Access Blocked

Fig. 2. Mechanism of Port Knocking technique



Network error: Connection timed out

Fig. 3. Port scanning attack failed

System Design

Firewall for HPC Systems

In order to apply access control from outside into internal network, Firewall offers the solution. Practically, Firewall defines security rules of allowing or dropping packets from particular sources by IPTables [3].
Considering role of HPC systems, it is strongly advised that Firewall with appropriate IPTables configuration should be deployed with regular maintenance by administrator. However, it is possible that during configuring the Firewall remotely, administrator may leave a security hole on the firewall which could be exploited by external attackers. If so, IPTables configuration including open ports will be obtained by the attacker to perform cyber attack on HPC systems [1].

Port Knocking

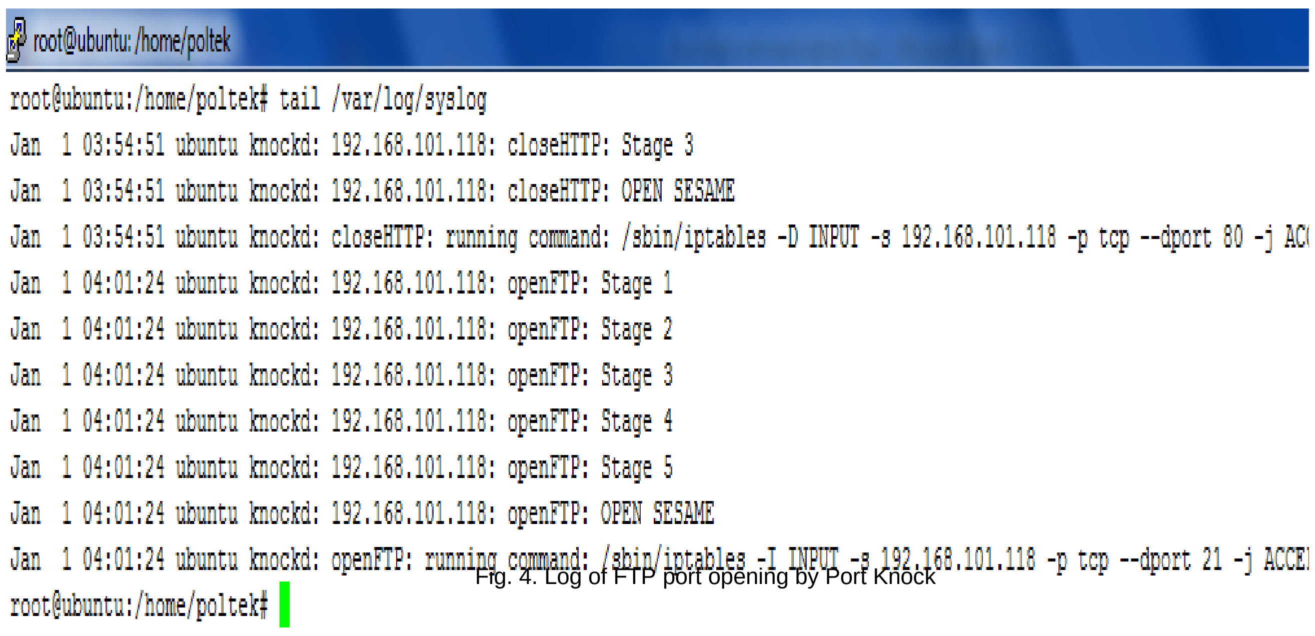
Port Knocking is a method of externally hiding open ports on a firewall by generating a connection attempt (KNOCK) on a set of predefined closed ports [3]. IPTables on firewall will be dynamically modified only if the correct sequence of connection attempts is received. Port Knocking prevents any port scan attacks because all ports will appear closed from attacker side. Administrator of HPC systems will gain benefits in securing its maintenance of the network even from distance.

Summary

The implementation of Port Knocking technique will significantly reduce risk of port scanning attack performed by attacker from external HPC systems.
Through this study, we have shown how opening or closing SSH and FTP services of HPC systems might be invisible by attackers.
In addition, the knock combinations might be easily changed by administrator periodically which in turn will give less chances for cyber attacks in the future.

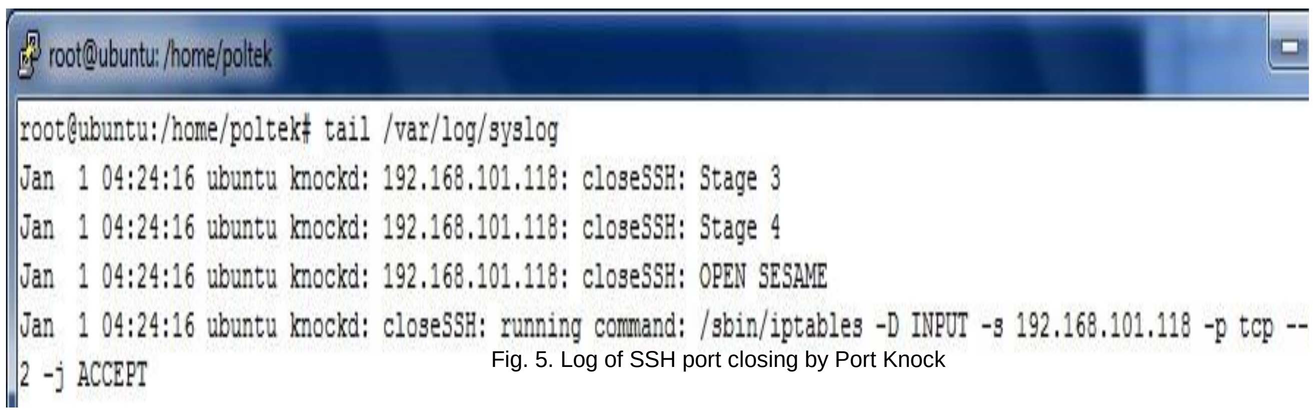
References

1. Malin, A., & Van Heule, G. (2013). “Continuous monitoring and cyber security for high performance computing” In *Proceedings of the first workshop on Changing landscapes in HPC security* (pp. 9-14). ACM.
2. Merlo, Alessio (2017) "From HPC to Security: How to Change Research Focus and Survive–A Career Perspective." *IEEE International Conference on High Performance Computing & Simulation (HPCS 2017).* IEEE
3. KrzywinskiM. (2003). „*PortKnocking*". Linux Journal, June 2003. Available at http://www.linuxjournal.com/article/6811 (Accessed Februari 2018)



```
root@ubuntu:/home/poltek# tail /var/log/syslog
Jan  1 03:54:51 ubuntu knockd: 192.168.101.118: closeHTTP: Stage 3
Jan  1 03:54:51 ubuntu knockd: 192.168.101.118: closeHTTP: OPEN SESAME
Jan  1 03:54:51 ubuntu knockd: closeHTTP: running command: /sbin/iptables -D INPUT -s 192.168.101.118 -p tcp --dport 80 -j AC
Jan  1 04:01:24 ubuntu knockd: 192.168.101.118: openFTP: Stage 1
Jan  1 04:01:24 ubuntu knockd: 192.168.101.118: openFTP: Stage 2
Jan  1 04:01:24 ubuntu knockd: 192.168.101.118: openFTP: Stage 3
Jan  1 04:01:24 ubuntu knockd: 192.168.101.118: openFTP: Stage 4
Jan  1 04:01:24 ubuntu knockd: 192.168.101.118: openFTP: Stage 5
Jan  1 04:01:24 ubuntu knockd: 192.168.101.118: openFTP: OPEN SESAME
Jan  1 04:01:24 ubuntu knockd: openFTP: running command: /sbin/iptables -I INPUT -s 192.168.101.118 -p tcp --dport 21 -j ACCE
root@ubuntu:/home/poltek#
```

Fig. 4. Log of FTP port opening by Port Knock



```
root@ubuntu:/home/poltek# tail /var/log/syslog
Jan  1 04:24:16 ubuntu knockd: 192.168.101.118: closeSSH: Stage 3
Jan  1 04:24:16 ubuntu knockd: 192.168.101.118: closeSSH: Stage 4
Jan  1 04:24:16 ubuntu knockd: 192.168.101.118: closeSSH: OPEN SESAME
Jan  1 04:24:16 ubuntu knockd: closeSSH: running command: /sbin/iptables -D INPUT -s 192.168.101.118 -p tcp --
2 -j ACCEPT
```

Fig. 5. Log of SSH port closing by Port Knock

High Performance Computing Saudi Arabia (HPC Saudi 2018)