

---

Semester thesis for Beat Strasser

# Firewall Testing

An extension to fwtest to handle UDP and ICMP

Supervisor: Diana Senn  
Professor: Prof. D. Basin  
Issue Date: August 2005  
Submission Date: February 2006

---

## 1 Introduction

We live in a world where all the company networks are connected to the Internet. Nobody can control the Internet, therefore a company has to protect their data from unauthorised access through the Internet. This is done by firewalls whose analogon in the physical world are locks. Everybody understands that doors need to be locked to prevent unauthorised access. It is the same in the digital world: unauthorised access to a companies network should be prevented, and this can be done by one or several firewalls.

Using the analogon of the door lock again, everybody understands that it is not enough to have a door lock. Only if the lock is locked properly and only authorised people have got a key to unlock it, we have what we want. It is the same in the digital world. It is not enough to have a firewall. We can only be satisfied if the firewall is doing what we expect from it. And to find out if a firewall satisfies our expectations (stated by a policy) we need to test it.

## 2 Motivation

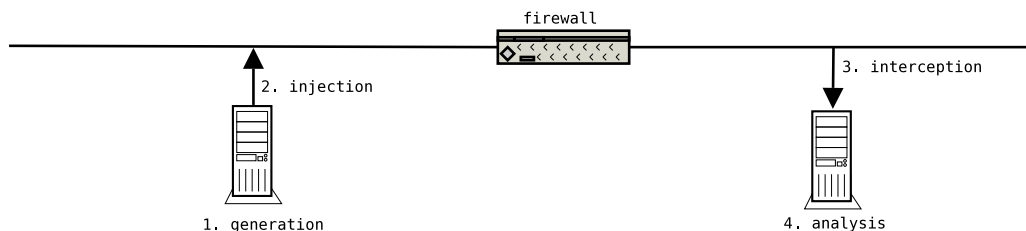


Figure 1: Flow of the Test Packets

Firewall Testing consists of two parts: the theoretical part of finding adequate test cases, and the practical part of running these test cases on the real system. The aim of this thesis is to cover the second part.

Running test cases on a real system consists of four steps as shown in figure 1. The first step is the generation of the network packets. According to a given test case the corresponding network packets have to be built. The second step consists of injecting the packets generated in step one into the network. The third and the fourth step are then to intercept the packets which were injected in step two behind the firewall, comparing them to the expectations, and logging the result.

## 3 Assignment

### 3.1 Objectives

During his diploma thesis [1], Gerhard Zaugg has written a simple tool – named fwtest – which can do the above for TCP packets in a bidirectional way. As there are also other interesting low-level protocols passing the firewall, the goal of this semester thesis is to extend fwtest to being able to generate UDP and ICMP packets as well.

### 3.2 Tasks

- Understanding fwtest
- Designing a format for UDP and ICMP tp-files
- Adding generation methods for UDP packets to fwtest
- Adding generation methods for ICMP packets to fwtest
- Conducting tests to show the correct behaviour of the implementation

As there will be another student (Adrian Schüpbach) working on fwtest in an overlapping time frame, some synchronisation between the two students is expected. This will mainly consist in determining a new format for the tp-files together and working on the same subversion repository.

### 3.3 Deliverables

- At the beginning of the semester thesis an agreement must be signed which allows the supervisor of this thesis, his project partners and ETH Zurich to use and distribute the software written during the thesis.
- At the end of the second week, a detailed time schedule of the semester thesis must be given and discussed with the supervisor.
- At the end of the semester thesis a presentation of 20 minutes must be given during an Infsec group seminar. It should give an overview as well as the most important details of the work.
- The final report may be written in English or German. It must contain an abstract written in both English and German, this assignment and the schedule. It should include an introduction, an analysis of related work, and a complete documentation of all used software tools. Three copies of the final report must be delivered to the supervisor.

- Software and configuration scripts developed during the thesis must be delivered to the supervisor on a CD-ROM.

## References

[1] Gerry Zaugg. Firewall testing. [http://www.infsec.ethz.ch/people/dsenn/DA\\_GerryZaugg\\_05.pdf](http://www.infsec.ethz.ch/people/dsenn/DA_GerryZaugg_05.pdf).

16th August 2005

Prof. D. Basin