Firewall Security: Policies, Testing and Performance Evaluation

Michael R. Lyu and Lorrien K. Y. Lau
Department of Computer Science and Engineering
The Chinese University of Hong Kong, Shatin, HK
lyu@cse.cuhk.edu.hk, lorrienlau@ctimail3.com

Abstract

This paper explores the firewall security and performance relationship for distributed systems. Experiments are conducted to set firewall security into seven different levels and to quantify their performance impacts. These firewall security levels are formulated, designed, implemented, and tested phase by phase under an experimental environment in which all performed tests are evaluated and compared. Based on the test results, the impacts of the various firewall security levels on system performance with respect to transaction time and latency are measured and analyzed. It is interesting to note that the intuitive belief about security to performance, i.e. the more security would result in less performance, does not always hold in the firewall testing. The results reveal that the significant impact from enhanced security on performance could only be observed under some particular scenarios and thus their relationships are not necessarily inversely related. We also discuss the tradeoff between security and performance.

1. Introduction

Nowadays, large and small companies are seeking ways of doing business on the Internet for global business. Meanwhile, Internet security issues become a hot topic. Companies accessing the Internet are seeking methods of protecting their network sites against external attacks and intrusion. Firewall is one of the best solutions. Setting up a firewall for private network sites in organizations and at home is no longer a too fancy thing. On the other aspect, performance impact may cause major concerns: Is there a significant performance loss while incorporating a secure environment using a firewall for the Internet connection? To what level of security should we expect without sacrificing the network performance? These are the basic questions asked when addressing the design of a secure network. Little research effort is made on this area before. This paper addresses the above queries by performing some security and performance testing on firewall of different security levels.

The network security problems may be company security and network access policy problems. To create a real-world environment, a secured firewall system is set up by using the Linux TIS firewall packages with a router, and the objective is to compare the performance impact that a firewall system experiences when it is configured with different security policies and controls. Security and performance tests are designed for security verification and performance measurement under qualitatively different security levels. The firewall is configured into seven different security levels, phase by phase with their corresponding design and implementation. Experiments are conducted for firewall testing on the dedicated LAN, and empirical results are obtained regarding how the firewall performs under different policies of different security levels. Interesting observations about the tradeoff between security and performance are also described.

2. Methodology

The experiments are performed in a security testing LAN in which a firewall is set up as the entry point for all the traffic going in and out of the LAN. Security and performance tests are conducted on the firewall. The firewall is configured with different security levels by using a router and several proxy servers. The details are described as follows.

2.1. Setting up Firewall Policies of Different Security Levels

In order to determine the impact from different security controls on network performance, seven different firewall security policies are specified, so as to set up the firewall system for a project qualitative evaluation. The security levels defined in the paper are not based on any published class of security evaluation criteria such as the orange book [1]. However, lower security levels are theoretically and practically less secured than higher security levels.

There are four basic components in building a firewall [1]: policy, advanced authentication, packet filtering, and application gateway. We specify a total of seven configurations and security levels of firewall, according to the requirements stated in the corresponding security

0-7695-0792-1/00 $10.00 © 2000 IEEE

policies we defined theoretically. Security is considered higher for a higher level. The seven security policies are briefly described in Table 1.

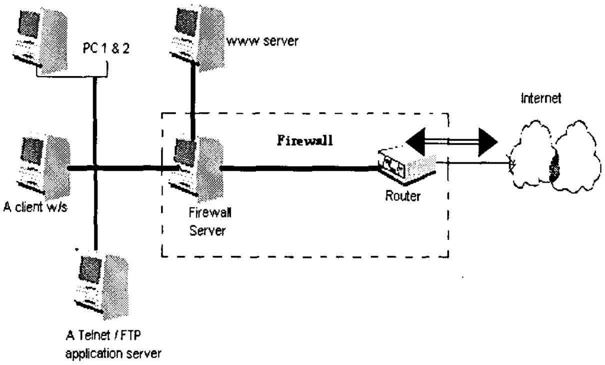
Table 1: Summary of the seven firewall security policies

Security Policy and Level	Main context of policy	Proxy services installed?	Other control	No. of screening rules set in the router
1	Permit any service unless it is explicitly denied	No	None	0
2	Permit any service unless it is explicitly denied	No	Disallow some problem service accesses from outside	6
3	Permit any service unless it is explicitly denied	Yes	Ditto	6
4	Permit any service unless it is explicitly denied	Yes	Ditto + Deny unauthorized and bad host accesses from outside	26
5	Deny any service unless it is explicitly permitted	Yes	Ditto	29
6	Deny any service unless it is explicitly permitted	Yes	Ditto + Restrict outside access to certain port number range only	37
7	Deny any service unless it is explicitly permitted	Yes	Ditto + Restrict internal access to some Internet services at outside hosts + deny access from hosts identified as intruder	43

2.2. The Test Bed

To test the performance and security for the firewall policies, we establish a security test bed as shown in Figure 1 below. The test bed is consisted of a protected testing LAN of 10Mb throughput with a firewall connected to the Internet through a Cisco router. The firewall server is a Pentium-Based PC with 32M RAM installed with Linux operating system and FWTK (Firewall Toolkit) package. The workstations used for the experiments are also running Linux. Users working at the PC communicate with the Internet through the firewall. Note that it is fairly common today to set up a firewall with a Linux box and a router for the protection of an internal network.

Figure 1: Test bed configuration for firewall testing



2.3. Security Testing

Some security checkups and penetration testing are applied in testing the security of the firewall. Penetration test uses techniques designed to defeat and bypass security mechanisms in order to determine the effectiveness of such mechanisms for the network. As a matter of fact, it is difficult to simulate the real attackers' behavior to the experimental LAN. However, the vulnerability of a specified firewall setup to certain intrusion or attacks could be checked with network scanning tools or some techniques which the intruders may use for hacking and attacking the firewall. Some scanning tools are used to simulate real network attacks and intrusions on the target system. When a security hole or warning was found in a particular test phase, it would be rectified or eliminated in the next test phase by adding some security controls such as screening rules to discard any questionable traffic. The 7 security levels are progressively defined and tested. The firewall in Level 7 is expected to be the most secured one.

2.4. Performance Testing

Performance tests are done on the firewall to measure the relative performance degradation of two types of service, i.e. 'HTTP' and 'FTP' of the firewall. It simulates the real usage of the firewall by directing various loads of FTP and HTTP traffic through the firewall. The data transfer requests would be initiated inside the private network to an outside network server.

The firewall performance is evaluated by the performance indicators of latency and total transaction time. Latency is the time required by a system to complete a single transaction from start to finish [4,5]. The data inspection at the firewall would lengthen the time required for data communication, as well as network or transaction latency. Experimentally, this indicator is measured by executing a bunch of transactions sequentially in a single thread and the result is obtained by the taking the elapsed time used for processing each transaction [5]. The total transaction time, on the other hand, refers to the amount of time it takes to open one or more connections in a transaction from the client to the server and to request and download data from the server. Also it is assumed that the variables such as the available network bandwidth and stray noise on the network are consistent and would not create too much variance for most of the results.

2.5. Measurement Procedure

FTP and HTTP test scenarios are designed for testing the firewall performance. During the experiments, the clients data download requests issued are passed to the firewall, which is responsible for communicating with outside and processing of data downloading requests. If no proxy service is adopted, the clients bypass the firewall and go directly to the outside network through Network Address Translation (NAT) done by IP Masquerader. Also FTP and HTTP requests could be initiated from clients to outside servers. This is the case when the firewall system is implemented with policies 1 and 2. On the other hand, if the firewall is incorporated with proxy services for data transfer, the FTP and HTTP requests are handled with additional traffic screening. This is the case with the firewall policies 3,4,5,6 and 7.

The clients pass the FTP data transfer requests to the FTP proxy gateway running at the firewall and wait for the proxy server to pass the result back to them. As the proxy server becomes the middleman or agent between the service clients and the outside server, extra overhead for traffic handling occurs. Likewise, for HTTP data retrieval requests, the firewall server would act as the HTTP proxy server for all of the clients inside the firewall under the firewall policies 3 to 7. At least 10 trials for each test scenario are executed and 3 or more valid sets of data for each scenario are used for analysis. The starting and ending time in seconds are jotted down right before the data transfer is executed and after it finishes. The total average and minimum values of each transaction were used to calculate the final result of network latency under every firewall security level.

2.6. Experimental Design for HTTP and FTP Session Test

Tests are carried out to transfer different amounts of data using HTTP and FTP protocols to see how the firewall performs under different policies. Some simple HTTP session scripts are written to perform HTTP GET protocol requests. The HTTP tests examine the environment of high volume but relatively small data size in a transaction. For FTP session test, bulk data of 5Mb data is attempted in scenario A. Scenario B involves a smaller data size of 1Mb. Besides, we examine the scenarios of low volume of data download and high volume of connections in test scenario C

2.7. Tools Description

We employ SAINT [2] and Nessus [3,6] for host attack and scanning. For system security checking and monitoring, COPS [7] and BSB Monitor [8] are adopted. During the performance testing, a tool called "workload" [1,9] together with some shell scripts doing HTTP and FTP data transfers are adopted in synthesizing the desired traffic workload.

3. Analysis of Results

3.1. Security Testing

The security testing are summarized in Table 2 below.

Table 2: Security testing result in summary

Security Level and Policy X	No. of warning and vulnerability count(s)
1	10
2	9
3	8
4	6
5	6
6	3
7	0

As expected that the security level (x + 1) is no less secured than the security level x based on the above results. The firewall setup for policies 4 and 5 is expected to be more or less the same with regards to the extent of security. But as policy 5 would deny everything by default whereas policy 4 would accept anything by default, so policy 5 is supposedly more secure than policy 4 even though the numbers of vulnerabilities found for them are similar. The testing is an attempt to quantify the difference of security between one security level and another. Furthermore, it helps in building up a secured firewall system from one level to another.

3.2. Performance Testing

The average total transaction time and latency are found in different test scenarios under the 7 firewall security policies. The HTTP average total transaction time versus the number of connection is shown in Table 3 for tabular results and Figure 2 for graphical display. The latency with the average total HTTP transaction time is shown in Table 4 and Figure 3. For the FTP performance testing, the latency calculated versus the number of connection in test scenario A is shown in Figure 4. Moreover, Figure 5 illustrates the performance test results with respect to the latency found in FTP test scenario B, while Figure 6 shows the performance test results derived in FTP test scenario C. Latency is calculated by the division of the "Total transaction time" with the "number of sequential transaction".

Table 3: The average total HTTP transaction times in second

A: No. of transaction B: No. of sequential connection

A	1	10	20	30	.	90	100
B	1x3	10x3	20x3	..	.	90x3	100x3
Cfg 1	0.94	10.40	22.20	....	.	111.00	143.40
Cfg 2	1.00	13.00	30.14	...	.	125.00	150.33
Cfg 3	1.50	63.88	304.38	...	.	1558.86	1710.71
Cfg 4	1.25	65.33	313.60	...	.	1538.00	1716.33
Cfg 5	2.86	70.88	316.38	...	.	1552.43	1743.00
Cfg 6	1.33	63.33	302.00	...	.	1536.00	1674.33
Cfg 7	2.75	63.25	304.50	...	.	1526.25	1737.25

Note: Cfg x refers to firewall configuration x with security level defined as Level x.

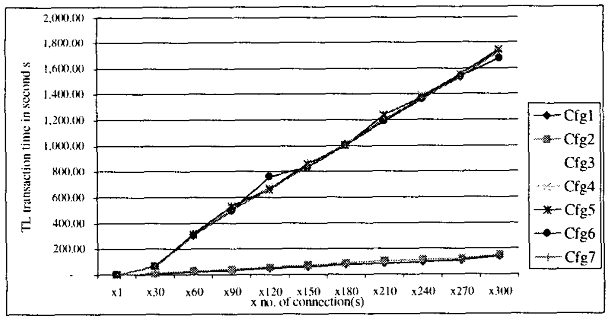


Figure 2: The HTTP total average transactions time vs the no. of connection

Table 4: Latency calculated with average total HTTP transaction time in second

Cfg	X1	X10	X20	X 30	X 40	X 50	X 60	X70	X80	X90	X100	Total
1	0.94	1.04	1.11	...	..	..	..	1.23	1.23	1.23	1.43	13.08
2	1.00	1.30	1.51	...	..	..	..	1.50	1.47	1.39	1.50	15.46
3	1.50	6.39	15.22	...	..	..	..	17.16	16.89	17.32	17.11	158.69
4	1.25	6.53	15.68	...	..	..	..	17.43	17.33	17.09	17.16	160.10
5	2.86	7.09	15.82	...	..	..	..	17.65	17.21	17.25	17.43	163.60
6	1.33	6.33	15.10	...	..	..	..	16.94	17.02	17.07	16.74	159.40
7	2.75	6.33	15.23	...	..	..	..	17.12	17.15	16.96	17.37	159.90

Note: x1 means 1 transaction and 3x 1 connections; x20 means 3x20 connections and so on.

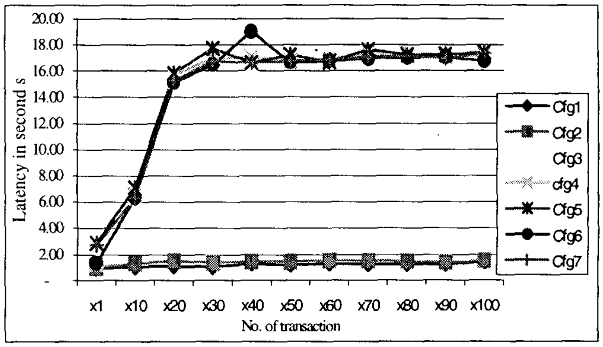


Figure 3: The average HTTP latency vs the no. of connection under different firewall security levels

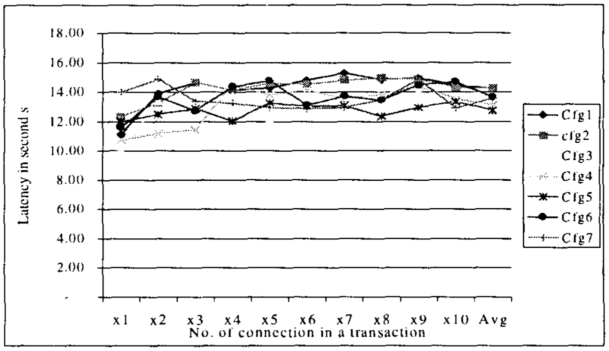


Figure 4: Average latency (calculated with the average total transactions times) vs no. of connection for FTP 5Mb data transfer

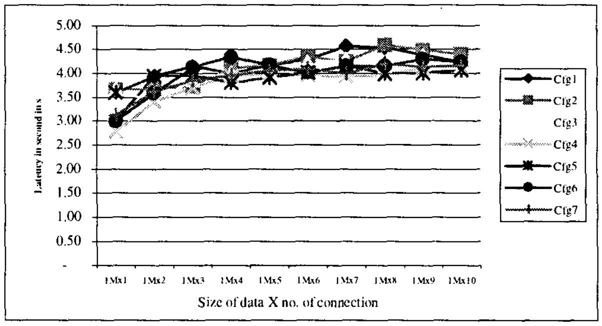


Figure 5: Average latency vs the no. of connection in a transaction for FTP 1Mb data

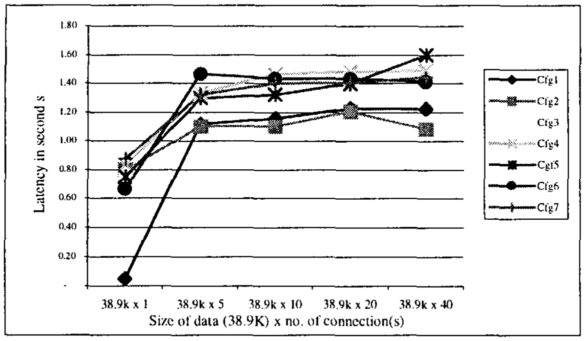


Figure 6: Average latency vs no. of connection request for FTP 38.9Kb data transfer

3.3. Analysis and Discussion

As shown above, the performance result obtained from HTTP session test is somewhat similar to that from test scenario C of FTP testing. The results from scenario A and B of FTP testing on firewall are more or less the same with respect to the overall firewall performance. Moreover, the firewall behaves very differently under particular security levels when comparing the results of FTP test scenarios A and B with that of test scenario C and the HTTP test. These interesting results provoke some thoughts on data traffic performance with different sizes and connection requests under different security policies.

(a) HTTP session test

In the testing of the high-volume connection and small data size file retrieval by using HTTP protocol, the data transfer times for the firewall policies 1, 2 and 3 differ significantly. When comparing the results of firewall security Level 2 with that of Level 3 in Figures 2 and 3, a remarkable increase of latency and processing time with security Level 3 is observed. But when proceeding from Level 3 to 4 or above, no obvious and consistent performance changes are concluded. Some key experimental observations are described below.

- **Observation 1 – Slight performance loss, but better security with security Level 2**

As expected the firewall of the basic configuration (i.e. the lowest security Level 1) performs the best as shown in Figure 2. It is because no packet-filtering rule is set into the router and the router does very little work outside of routing traffic, so low overhead occurs for the security Level 1. Moreover, the tests show that security Level 2 performs slightly poorer than Level 1 in data transfer by using http protocol. This can be explained by the enhanced security control in Level 2.

- **Observation 2 - Significant Performance Degradation with Security Level 3**

Furthermore, Figures 2 and 3 show a significant increase of processing time with security Level 3. In security Level 3, the proxy server imposes an overhead, which is comparatively significant to the total processing time and latency. The proxy process running at the firewall analyzes application commands inside data packets and keeps logs. Thus it incurs higher overhead than a simple packet filtering firewall, such as that in security Level 2. Moreover, for each new connection to the Internet, overhead from the proxy process happens. Thus if the number of connection is high the accumulated overhead would be enormous. Consequently, the time for HTTP transfer adds up quickly when the connection number is increased from 1 to 30 in security Level 3.

- **Observation 3 – Insignificant the performance impact among security Level 3 to 7**

Interestingly, the curves of security Levels 3, 4, 5, 6 and 7 seem to be overlapped with each others, so whether there is a performance gain or loss among them is difficult to conclude. In fact, the firewall security Levels 3 to 7 are mainly implemented by a firewall technology of packet filtering, which is controlled by configuring different screening rules in the router. There is clearly a performance loss when security level proceeds from 1 to 2 and the number of screening rule is increased from 0 to 7. However, when further rules are added to the router, the performance difference is not obvious, even though when the number of screening rule is increased from 17 (Level 3) to 43 (Level 7). This phenomenon could be explained by the way the router parses the screening rules. Normally the router parses the rules in sequential order for a match. The speed of traffic going through the router depends very much on the sequence of rules set in the router. In other words, if the traffic is matched in the sequence of rules earlier, the faster the traffic goes through the router. When we look at the details of screening rules set in the router, the numbers of rule the router parses for FTP traffic under the implementation of firewall policies 3 to 7 are similar. As a result, the overall performance of policies 3 to 7 is very close to each other. Besides, the irregular shape of the performance curves for firewall policies 3 to 7 also suggests that their performance is easily affected by environmental interference.

(b) FTP session test

As seen in the test results of scenarios A and B in Figures 4 and 5, the latencies of the 7 security levels do not differ from one another much in value. Similar to the HTTP testing, the latencies in scenario C are increased remarkably since the connection number is 5 or larger, and the latency of firewall configuration 3 is higher. Major observations are described as follows.

- **Observation 1 – Low volume connection testing vs high volume connection testing**

As implemented in the experiment, 'low-volume connection' means 1 to 10 connections, whereas 'high-volume connection' means 10 to 40 connection requests involved in data transfer. When considering the low-volume connection testing, i.e., the scenario A and B in Figures 4 and 5, the difference of latencies among different security levels is not significant no matter whether the file size is 5M or 1M. For the high-volume connection testing with small data size, i.e., the test scenario C in Figure 6, the performance degrades when the firewall security level proceeds from 1, 2 to 3. Also the latency values found under the firewall Levels 3 to 7 are clearly larger than those under Level 1 and 2.

This interesting result found in FTP test scenario C is similar to that found with HTTP protocol tests described previously. To sum up, if the number of connections to the Internet is high and the data size is small, the total accumulated overhead due to the proxy process becomes significant enough when it is compared with the total processing time without overhead. The usage of proxy servers for higher security at the firewall, as implemented in the firewall policies 3 to 7 in FTP test scenario C, would reduce the network performance. On the other hand, if the data size is large and the connection number to the Internet is small, the impact will be small, as seen in security policies 4 to 7. When the transaction time for each connection is comparatively longer, the time overhead added by proxy servers at the firewall becomes comparatively insignificant and unnoticeable.

- **Observation 2 – Insignificant performance difference among firewall policies 3 to 7**

It is also clear that the performance difference among the firewall policies 3 to 7 is not large in the three FTP test scenarios. Just like the results obtained from HTTP tests, the fluctuations in their performance result curves appear very often in testing the three scenarios of data transfer with FTP protocol. The results imply that the performance difference among security levels due to the overhead of packet filtering for more security is negligible when compared with the outside traffic interference.

4. Conclusion

In order to explore the security to performance relationship at firewall, we perform some experiments on a firewall system implemented with 7 proposed firewall policies. The performance of the firewall policies has been quantified and analyzed. In the security testing, the security levels are not only built up qualitatively with different security policies, but also tested and validated by using some network scanning tools. In the performance testing, for the scenarios of data transfer of small data size and high volume of HTTP or FTP connection requests, the firewall shows some performance difference under the implementation of different firewall policies.

As seen from the overall testing results, the firewall performance is affected only if the overhead incurred by the enhanced security control is significant when compared with the normal transaction time without the enhanced security control. Performance degradation would not result unless the accumulated overhead incurred from the additional security mechanisms at the firewall outweighs the interference from outside traffic. Besides, it could be concluded that the intuitive belief about the security and performance relationship does not always hold. In other words, the same level of security at firewall could be achieved with different firewall technologies and resulted in different network performance. Therefore, the firewall technology is a major factor for performance evaluation. If frequent connections with data of small size are required in communication, enhanced firewall security would be very likely to bring out some significant performance degradation to the private network. This study enables us to design an optimal firewall technology that could implement a high security control in defending a private network, without incurring a significant performance loss.

Acknowledgement

The work described in this paper was supported by a grant from the Research Grant Council of the Hong Kong Special Administrative Region (Project No. CUHK4432/99E).

References

[1] M. Goncalves, "Firewalls", McGraw-Hill, 1998.

[2] SAINT at the World Wide Digital Security Inc. http://www.wwdsi.com/saint/

[3] The Nessus Project, Renaud Deraison. http://www.nessus.org/.

[4] A. Molitor, "Measuring Firewall Performance", Network System Corporation.

[5] C. Kostick and M. Mancuso, "Firewall Performance Analysis Report", August 1995. Computer Science Corporation CSC.

[6] Vulnerabilities families of the Nessus Project. http://www.nessus.org/plugins/.

[7] COPS. http://www.fish.com/cops/.

[8] BSB Monitor. http://www.bsb-software.com/download/bsb-monitor/.

[9] WORKLOAD in the archives of the firewall-performance mailing list. ftp.greatcircle.com in /pub/firewalls-performance/digest/v01.n011.Z.