A Quantitative Study of Firewall Configuration Errors

Avishai Wool

Yash@acm.org

Computer 37:6, 62-67, June 2004

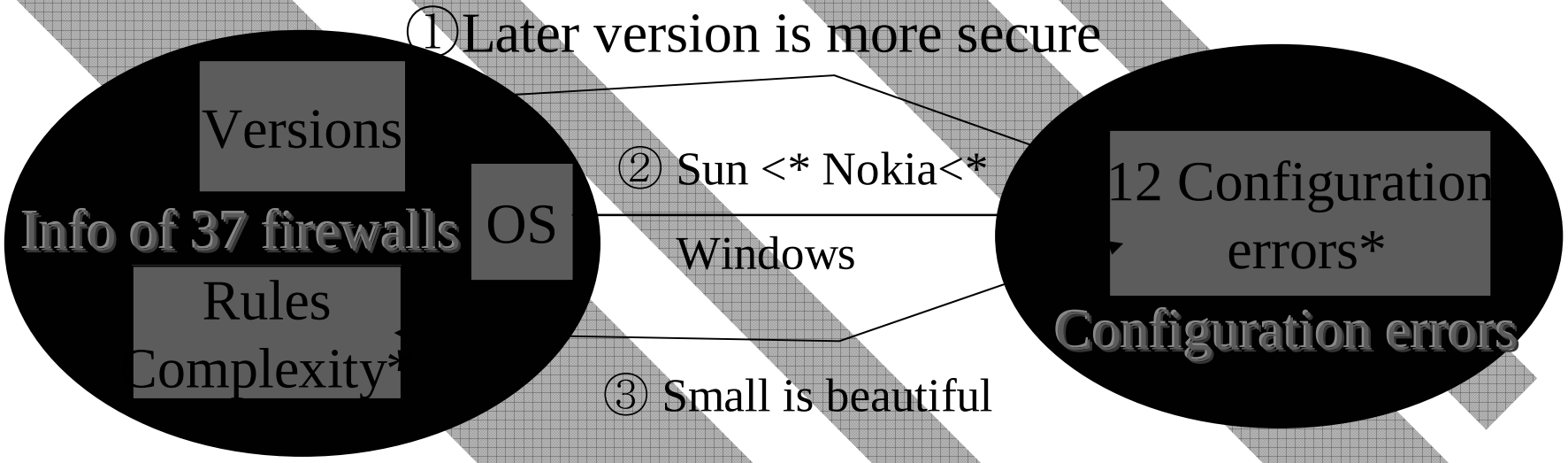
Presented by *Lei WANG*

One sentence summary

Through analyzing the different rule sets gathered from the configuration files of 37 Check Point* firewalls, the article gives out three quantitative relationships between the information in the rule sets and the firewall configuration errors.

“Check Point” is the brand of the firewall

Show the summary by graph.



* ”<” means “less secure”.

* Rules complexity = rules+objects+interfaces(interfaces-1)/2

* 12 configuration errors: they are “only those configurations that represented violations of well-established industry practices and guidelines”.(Said the author)

Example: Error[6.] “Allowing management sessions from more than five machines was counted as a configuration error.”

Appreciative comment

This article is well structured.

There are four parts in this article:

1.Data collection →
→ 2.Give Measurement Methods→
→ 3.Apply those methods→
→ 4.Get the results.

Critical comment 1

Unconvincing arguments are used when proving “small is beautiful”.

How did the author get the three beelines from so dispersed points?

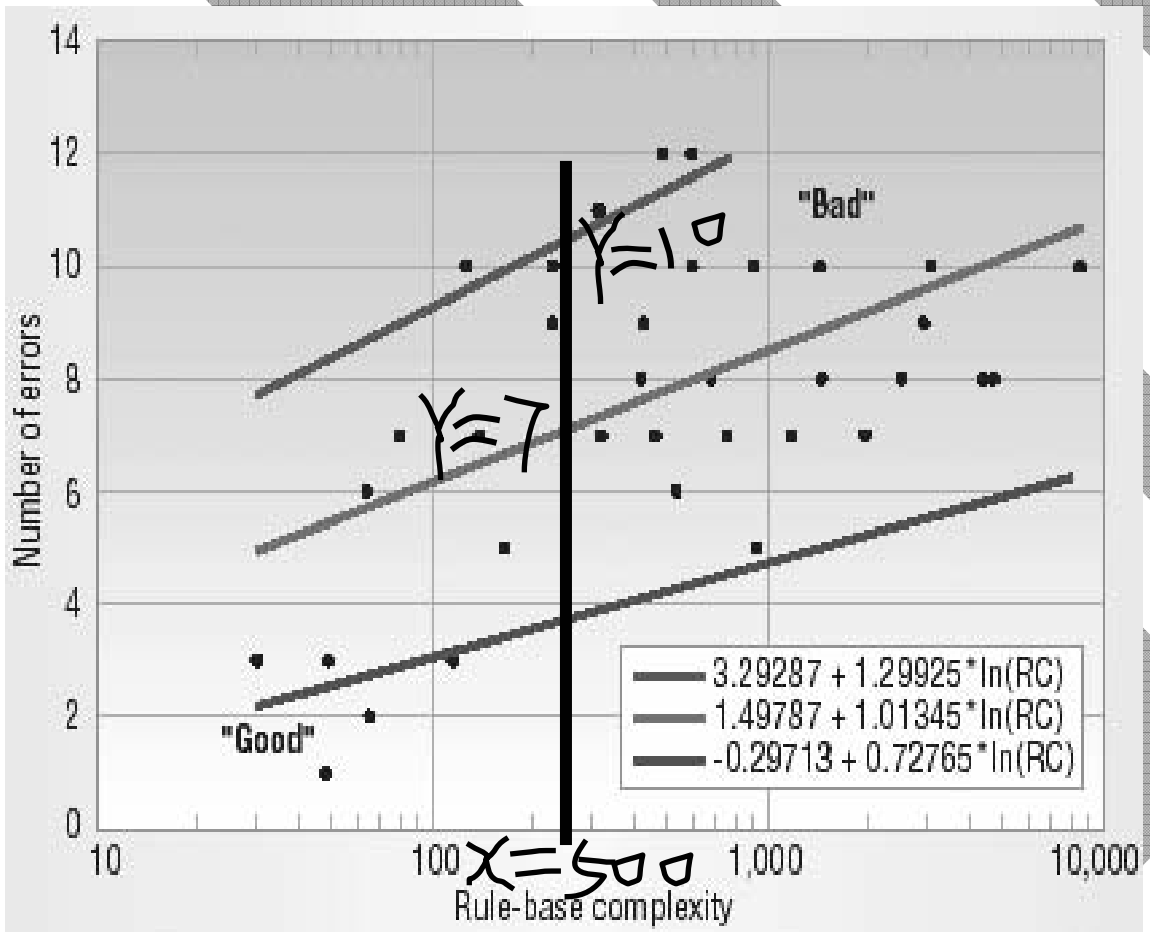


Figure 4. Number of errors VS complexity

He said “A linear regression shows that a rule set of complexity RC is predicted to have about ln(RC)+1.5 errors. This is the formula for the central green line in Figure 4.”

In fact, We can not predict anything by using that formula because there are lots of points far away from the green line.

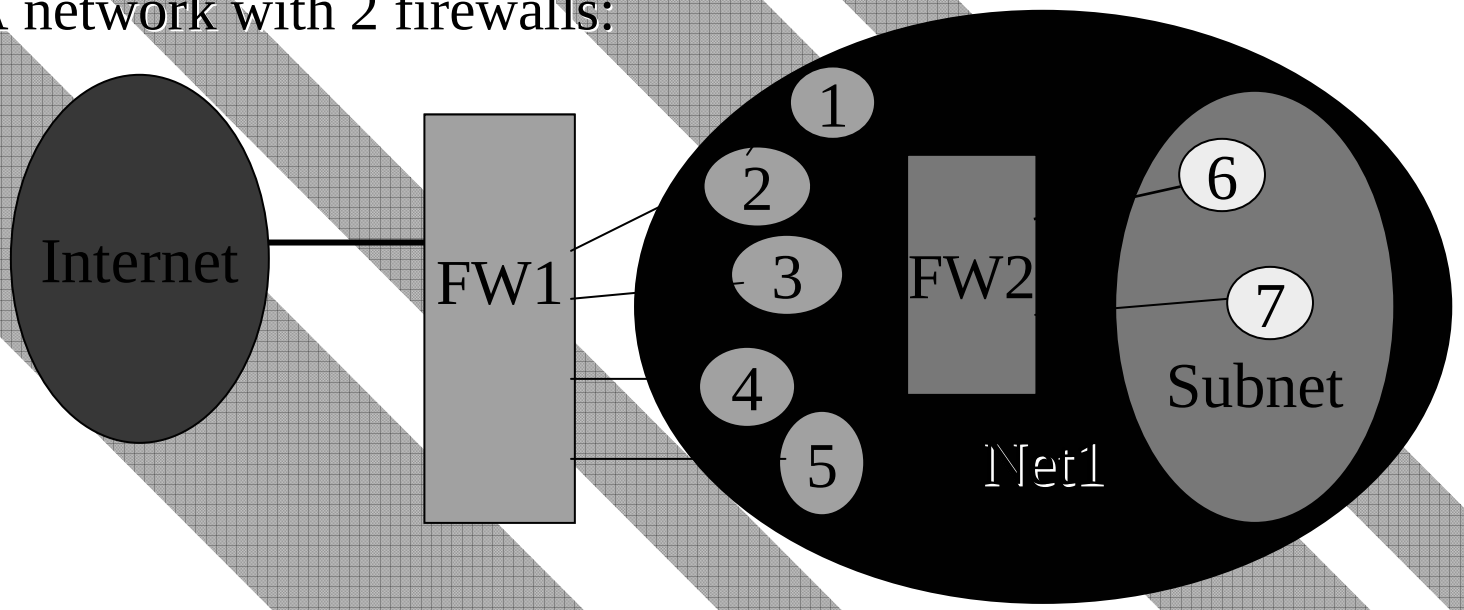
Critical comment 2

One problem is not mentioned about the rule set complexity:

> When multiple firewalls are used, how to calculate their complexity? (Asked by pro. Thomborson)

If we simply sum all the firewalls' complexities up as the whole system's complexity, then how to calculate the number of the corresponding configuration errors?

A network with 2 firewalls:



When FW1 allows all the 7 hosts in Net1 to be the manage machines while FW2 does not let the hosts in the subnet(no.6,7) access FW1, if treat FW1 and FW2 separately, FW1 does violate error no.6(#management machines should be less than5). However, it does not when we take the effect of FW2 into account(only 5 management hosts).

In conclusion, the author should say something more about how to map the complexity to the 12 configuration errors when more than one FWs are being used.

Question

What can WE learn from this article?

Here “we” refers to “students in class 725”.

- Option1: the 3 relationships .
- Option2: 12 configuration errors
- Option3: the way the author processes the data.

My Opinion

- I pick the third one.

1. 37 rule sets is too small as a real sample and check point firewall-1 is just a particular FW→ we can not apply any of the three results.

2. It is useful but when we apply them to analyze firewalls we have to take the concrete environment into account.

3. It focuses on 3 aspects rather than all the information.
   and structures the whole article in logically clear parts.
   So, I think, as postgraduate students, we can get some inspirations from that part of this article on how to find a way to analyze complex data and structure a report which would be good for our study.