A Quantitative Study of Firewall Configuration Errors
Avishai Wool, Tel Aviv Univ

Presented by
Saurabh Jain
Introduction

- The protection that firewalls provide is only as good as the policy they are configured to implement.
- Corporate firewalls are often enforcing rule sets that violate well established security guidelines.
Methodology

- Data collection – 37 Check point FireWall-1 Rule sets. (out of hundreds of thousands)
- Could be biased towards badly configured.

| Table 1. Statistical properties of the collected rule sets. |
|------------------------|------|--------|--------|
| Property description   | Minimum | Maximum | Average |
| Number of rules\(^1\)  | 5     | 2,671   | 144.0  |
| Number of objects\(^2\) | 24    | 5,847   | 968.0  |
| Number of interfaces\(^3\) | 2     | 13      | 4.1    |
Rule-set Complexity

- RC = Rules + Objects + Interfaces(Interfaces – 1)/2
  - Rules:- No of rules implementing the policy. (contains sources, destinations, service objects)
  - Can have more than one interfaces in one network.
Configuration Errors

- No stealth rule – *From anywhere to the firewall, with any service, DROP.*
- *Insecure firewall management.* Access to the firewall over insecure, unencrypted, and poorly authenticated protocols—such as telnet, ftp, or x11—counted as error
Configuration Errors..

- **Too many management machines** - Allowing management sessions from more than five machines was counted as a configuration error.

- **External management machines.** An error was counted if machines outside the network’s perimeter could manage the firewall.

- Allowing any NetBIOS service to cross the firewall in any direction counted as
Configuration Errors..

- RPCs include the Network File System protocol, which potentially exposes all the organization’s file system.

- **Zone-spanning objects**

- “Any” service on **inbound rules**.

- “Any” destination on
Figure 1. Distribution of configuration errors. Numbers on bar descriptions correspond to the configuration error descriptions in the text.
Figure 2. Number of errors as a function of the firewall’s operating system. The bar widths are proportional to the number of configurations. The red squares mark the average number of errors per operating system.
Results and Analysis

Figure 3. Number of errors as a function of firewall version. The bar widths are proportional to the number of configurations. The red squares mark the average number of errors in each version.
Take Away:- Small is beautiful

Figure 4. Number of errors as a function of rule-set complexity. The green line represents the least-squares fit; the red and blue lines represent one standard deviation above and below the least-squares fit.
THANK YOU