Performance Impacts of Firewall Policy Complexity

Study: Impact of Policy Size and Rule Order on Firewall Performance
Overview

▪ Jody Brazil, President & CTO, FireMon

▪ Agenda

▪ Issues of Complexity

▪ Impacts of Complexity

▪ Results of Research: “Impact of Firewall Policy Complexity on Firewall Performance”

▪ Recommendations
Overview

What is Complexity?

- Many devices
  - Eroded perimeter – more connection points
  - Increased segmentation
  - More layers of defense (internal firewalls)
- Large policies with many rules
  - More applications to protect
  - Additional network segmentation
  - More granular control
- Regulation
  - Results in more segmentation
- Application security controls
Complexity

How Big is the Problem?

- Many devices
  - More than 50% of companies with more than 15,000 employees reported having more than 100 firewalls.¹
  - 20% of companies with more than 15,000 employees reported having more than 500 firewalls¹
  - 20% of companies with less than 5,000 employees reported having more than 100 firewalls¹

¹ “Survey on Firewall Policy Management”, Secure Passage Report, Spring 2009
Complexity

How Big is the Problem?

- **Large Policies**
  - 73% of all respondents reported their policies were “complex” to “out of control”\(^1\)
  - 15% of large companies (those with more than 100 firewalls) reported averaging more than 1,000 rule per firewall\(^1\)
  - 86% of large companies reported averaging more than 100 rules per firewall\(^1\)
  - 76% of all companies reported averaging more than 100 rules per firewall\(^1\)
  - Our customers indicate on average 30% - 50% of all rules are unused
Complexity

What Causes Complexity?

- Complex environments / complex problems
  - 78% of large company respondents indicated complex environment caused policy complexity
  - Over 40% indicated compliance mandates

- Poor visibility of policy behavior
  - An HP Labs study of firewall management effectiveness found that complexity led to more “ineffective” rules.
  - Nearly 60% of all companies identified a lack of analysis tools in the change process results in complexity

- Unnecessary rules
  - Over 60% of all companies identified unused / obsolete rules responsible for complexity
  - Fear of business impact
  - Extensive creation processes, no removal process

---

1. [Source](#)
Impact of Complexity

Security Impacts

- Poor visibility / understanding results in mistakes
  - 65% of respondents identified security gaps caused by complexity as one of their biggest concerns\(^1\)
  - HP Labs indentified that as policy complexity increases mistakes increase\(^2\)
- Unnecessary complexity is often unnecessary security risk
- Lack of understanding is likely an indication of lack of security
  - 70% of respondents recognized that unused rules make it difficult to manage their firewalls\(^1\)
- Gartner Analysts Report:
  - 99% of firewall breaches are caused by firewall misconfigurations, not firewall flaws
  - Debugging errors in firewall rules or a new application can be cumbersome and time-consuming
Impact of Complexity

Performance Impacts

- Management Performance
  - Complexity results in more effort to manage the firewall
  - 70% of respondents identified unneeded complexity causing increased time to identify if and where to create new rules\(^1\)
  - HP Labs Study concluded that less confusing rule sets are easier to manage as validated by a measure of effectiveness over time\(^2\)
Thesis: Increased complexity results in decreased performance and increased system utilization, specifically CPU utilization.
   - Reducing unnecessary complexity will improve the performance of the device and increase the productive life of the firewall.

Device Performance
- CPU
- Connection Latency
- Impacts
  - What is the impact of policy size on device performance?
  - What is the impact of application security setting on device performance?
Impact of Complexity

Performance Impacts

• Test Plan:
  – IXIA IxLoad
  – Objectives
    • 5,000 HTTP conn./sec
    • 50 SMTP conn./sec
    • 10 DNS conn./sec
  – Crossbeam X80
    • Firewall-1 NGX R65
    • Quad processor
Impact of Complexity

Performance Impacts

- **System CPU Impact**
  - 5 rules: 27% load
  - 187 rules: 44% load
  - 264 rules: 48% load

- **Process CPU**
  - 12% down to 9%

- **SoftIRQ**
  - CPU spent waiting

![System CPU Diagram](chart.png)

- **CPU Usage** vs. **Number of Rule**
  - Red line: CPU
  - Blue line: Process CPU
Impact of Complexity

Performance Impacts

- **Connection Latency**
  - 5 rules: 600 µs
  - 187 rules: 1800 µs
  - 264 rules: 2600 µs

![HTTP Connection Latency Graph](image)
**Impact of Complexity**

*Performance Impacts*

- **Rule Location**
  - Same size policy
  - Active rules moved closer to top
  - Average location from rule 5 to rule 276
- **Size is not the issue!**
  - Location of used rule affects performance

![Graph showing CPU usage vs. average rule location](image)
Impact of Complexity

Performance Impacts

- **Interesting results:**
  - Combining 60 rules into one rule had a drastic performance impact on both CPU and Connection Latency dropping CPU usage significantly
    - Check Point appears to short circuit packet evaluation on Service, Source then Destination
  - Using 254 host objects versus a single network object has no visible impact on performance
  - Noisy traffic rule close to top is an effective performance enhancement
  - SmartDefense is efficient, but does have significant performance impact on system:
    - 42% - 60% by adding HTTP Web Intelligence checks
    - 42% - 62% by adding SMTP Application Intelligence checks
    - 35% - 40% by adding SYN Attack checks
Summary

Solution Recommendation: FireMon

- Understand what you have
  - Rule report detailing each rule
  - Breakdown group members

- Perform a clean-up process
  - Identify unused rules
  - Make it a continuous process
  - Understand usage over time
  - Make sure you can keep significant history

- Sort rules based on usage
  - Focus on top 10% of rules
  - 5% often takes up 90%
  - Maintaining usable, understandable policy is still a priority

- Improve rule creation process
  - Identify if a rule is needed using analysis tools
  - Identify rule consolidation opportunities
Summary

Solution Recommendation: Rule Usage Analysis

- Identify Unused Rules
  - Establish a process to review unused rules and remove as part of routine maintenance
  - Verify accuracy of results. Inaccurate or incomplete data is worthless.

- Identify Most Used Rules
  - Identify highly-utilized rules placed low in the rulebase. Focus only on top most used rules.
  - If the drop rule is one of you top three rules, identify if it is possible to drop some expected traffic (noisy protocols) early in the policy.

- Identify Unused Objects
  - Focus on most used rules and remove unnecessary unused network objects
Solution Recommendation: Policy Analysis

- Pre-change evaluation
  - If a rule is needed
  - Where a rule must go
  - Possible consolidation options

- Troubleshoot connectivity issues
  - Identify which rule will act on traffic

- Business Continuity Reporting