Probabilistic Policy Violation Detection with IPFWD

IPFWD is a system load monitoring daemon for FreeBSD that updates an early rule in IPFW that has a chance to accept any packet. This provides a graceful tradeoff between performance and security policy enforcement. The probability of acceptance is dependent on the current system load. IPFWD also extends IPFW logs to include information about the probability of undetected rule violations when the accept any packet rule is in effect.

Abstract

By allowing a probabilistic chance for allowing any packet through the firewall, IPFWD can provide a graceful transition between performance and security that dynamically follows current system load.

Firewall performance can be improved by reducing the number of rules applied to each packet. Supposing a white list policy, the firewall has to apply every rule to each packet before it's denied. Instead of applying each rule to every packet that will be denied, we have a chance to immediately accept it without any further computation. Testing shows this reduces the system resources required to handle the same amount of traffic.

IPFWD has the most potential for usefulness in high bandwidth environments, such as data centers, where it's not feasible to apply an extensive rule set, or any rule set at all, to each packet but it’s important to be notified of security policy violations. The balance between security information and performance is tuned by IPFWD based on current system load.

IPFWD

This is a shift in mindset from typical firewalls. Instead of enforcing every part of a security policy all of the time, IPFWD enforces the policy some of the time and extrapolates from the violations it encounters. This provides insight into the violations that weren't detected. For this cost, you gain increased firewall performance and network throughput in resource bound systems. It's acceptable to allow a percentage of policy violations given that network traffic patterns are typically repeated and administrative goal is detection and not immediate prevention. Preventative action may be taken later when resource requirements are lower.

For example, under heavy load IPFWD may immediately accept 40% of packets. Supposing a port scan was initiated during this time, 60% of the port scan would still be rejected and logged. Since the percentage chance will fluctuate over time, IPFWD provides additional information in the IPFW logs to show the chance additional undetected violations occurred for detected violation. This also allows administrators to retain extensive rule sets that fully implement their security policy. Instead of having to simplifying rule sets to increase performance, IPFWD balances policy enforcement and performance automatically. Under normal or light load, IPFWD will enforce the entire security policy 100% of the time.