Probabilistic Policy Violation Detection with IPFWD

Abstract

When using a firewall system like IPFW to detect threats, we can end up doing a lot of packet processing. This can negatively impact performance-sensitive systems such as storage nodes. This presentation describes a practical solution to this problem using a load-weighted probabilistic mechanism that allows a trade-off between perfect visibility of incoming packets and reduced impact to system load.

IPFWD

IPFWD is a daemon for FreeBSD that updates an early rule in IPFW that has a chance to accept any packet. The probability of acceptance is updated over time and dependent on the current system load. To account for this, IPFWD extends IPFW logs to include the likelihood an undetected policy violation occurred.

This approach is based on the premise that firewall performance can be improved by reducing the number of rules applied to each packet. Supposing a whitelist policy, a firewall has to apply every rule to each packet before it's denied. With IPFWD, we have a chance to accept any packet early and skip any further computation. Test results shows this reduces the system resources required to handle the same amount of traffic.

This is a shift in mindset from typical firewalls. Instead of enforcing every part of a security policy all 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 often repeated and the goal is detection and not immediate prevention. Preventative action may be taken later when resource requirements are lower.

As an example, under heavy load IPFWD may immediately accept 40% of packets. Supposing a port scan was initiated during this time and rules exist to block it, 60% of the port scan would still be rejected and logged. Since the probability will fluctuate over time, IPFWD provides information in the IPFW logs to show the chance undetected violations occurred for each detected violation. IPFWD allows administrators to keep extensive rule sets that fully implement their security policy. Instead of having to simplify 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.