Trend Micro

DEDICATED INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

Why enterprises should consider a dedicated IDPS as part of their network security stack

There's been a lot of confusion sown in the security markets around the validity of a dedicated Next Generation Intrusion Prevention Systems (NGIPS) versus the IPS functionality in a Next Generation Firewall (NGFW). It's a nuanced topic that often gets lost in big marketing spend and within the noise of the industry. We will look at some answers—including that often-ignored nuance—to some of the assertions and questions enterprises ask about NGFW vs. dedicated NGIPS.

NGFW HAS IPS IN IT, SO IT IS THE SAME AS DEDICATED NGIPS?

Not all NGIPS are created equal. Since the NGFW was introduced, dedicated NGIPS has consistently been much better than the IPS in NGFW. Next Generation Firewall emerged only when "good enough IPS" was available in it. Therefore, if an enterprise wants best protection, the dedicated ones are better. It's a result of focus. Focus is real.

SO IS THE NGFW AND IPS GAP CLOSING?

We don't believe that the those two are equal. NGFW purchases are primarily based on firewall features. Once the NGFW had "good enough IPS" there wasn't great incentive to keep improving on the IPS capability in those NGFWs. On the other hand, dedicated NGIPS vendors devote all their efforts to advance their NGIPS because dedicated selections are usually made on comparing IPS features and the depth and breadth of their security effectiveness.

HOW ARE NGFW AND IPS DIFFERENT?

- Firewalls are a control safeguard (allow A to connect to B based on our policy which is likely unique to us) and IPS is threat-facing (stop all attacks that are common to most organizations).
- Firewalls are "default deny" (if there is no rule, don't allow it) and IPS are "default allow" (if it isn't triggering a signature, it goes through).
- Firewalls are set to "fail closed" (stop all traffic if there's an issue) and IPS are defaulted to "fail open" (if there's an issue the packets keep flowing).
- Most firewall inspection happens at layers 3 and 4, and most IPS inspection happens at layer 2. The short answer on why this is important is visibility—layer 2 devices are less visible and intrusive.

FIVE EXAMPLES WHERE AN ENTERPRISE-GRADE DEDICATED NGIPS IS REQUIRED:

1. When the customer is looking for a best-of-breed security efficacy.
2. In certain deployment scenarios—where consistent performance around critical metrics such as latency and throughput are required—a dedicated NGIPS is often the best solution that offers the breadth of security features with the bump in the wire, high throughput, and low latency.
3. A dedicated NGIPS offers an additional layer of defense to inspect north-south traffic.
4. Another typical scenario for the dedicated NGIPS is to inspect traffic between load balancers or WAFs and web applications and offer protection against threats to internal assets where agent-based protection is cumbersome or impractical, such as between IT and IoT and between LAN segments and BYOD networks.
5. Dedicated NGIPS also is increasingly being used to protect network segmentation by monitoring internal network for lateral movement and compliance mandates.

WHEN IS A DEDICATED NGIPS BEST PRACTICE?

Short answer; when security is important. If the security required is more than good-enough, then this is the classic IPS buying scenario. Even if the same team manages the firewall, it is the quality of the IPS that matters and shouldn't be secondary in that scenario. When a different group manages the IPS from that of the firewalls, stand-alone IPS is usually selected—notwithstanding the IPS quality requirements.

If there is any noteworthy amount of compliance tracking in the firewalls, having IPS in the same platform can in some cases be a barrier. Compliance tracking can discourage access by non-firewall staff in order to limit the events that need to be within the compliance scope. So even if the product has good role separation, auditors may not always see it that way and treat every NGFW management action as an "in scope with compliance" event.

SUMMARY

NGFW's promise of consolidated management and functionality are certainly appealing. When they first arrived a few years ago, many enterprise CISOs jumped at the chance to aggregate multiple network security services into a single appliance as a means of reaping numerous financial and operational benefits.

While many enterprises explored this strategy, few pursued it because NGFW convenience came with many security, organizational limitations, and compromises. For those that did pursue NGFWs, many are reversing their decisions and returning to a layered network security infrastructure that includes perimeter-based NGFWs and dedicated NGIPS deployed behind the firewall and at various other locations on internal networks.

Key Findings

- **IDPS offers the best detection efficacy and performance network security**, but firewalls are absorbing IDPS on the perimeter. Security and risk management leaders should seek innovation in advanced analytics, augmenting vulnerability management and internal segmentation from their IDPS solution.
- **Advanced Threat Detection and IDPSs continue to combine into products**, offering both capabilities, broadening potential use cases.
- **Intrusion detection and prevention systems (IDPS) remain a popular use case for threat detection (IDS mode)**, while blocking threats and protecting IaaS instances continue to drive adoption (IPS mode) for new deployments.
- **Enterprise network firewalls continue to replace IDPS for perimeter edge use cases and some internal ones**, for which high throughput is not a requirement.
- **Advanced threat intelligence feeds continue to improve IDPS effectiveness**, by augmenting capabilities, and threat intelligence appliances will not replace them.
- **Not enough solutions support native integrations**, with vulnerability assessment (VA) and threat and vulnerability management (TVM) to facilitate better execution of risk-based vulnerability management processes.

For details about what personal information we collect and why, please see our Privacy Notice on our website at:
https://www.trendmicro.com/privacy

TREND MICRO™

Securing Your Connected World

[TPR00_Dedicated_NGIPS_Technology_Primer_200114US] trendmicro.com