Scaling Forcepoint IPS solutions for high-performance networks

Summary

High-performance requirements in core networks, data centers, and large enterprises demand speed, scalability, and security without compromise from their Intrusion Prevention Systems (IPS). Forcepoint IPS solutions provide scalable, future-proof performance for demanding networks with the highest-rated security efficacy on the market today, all at a very low TCO-to-protected-throughput ratio.

Our example implementation using Forcepoint NGFWs (Next Generation Firewalls) as IPS engines and a Niagara™ Network Packet Broker (NPB) demonstrates how you can achieve performance and security at scale without compromise. The example implementation under test attains an IPS inspection throughput of 186 Gbps across a 100 Gigabit Ethernet link with bidirectional traffic.

The example implementation is very simple and highly flexible. By following our configuration overview, you'll learn key aspects of implementing a high-performance Forcepoint IPS solution for any environment and how to easily alter our example implementation to suit the specific requirements of your network and infrastructure.

Forcepoint IPS solutions provide the following key benefits for demanding deployments:

- High performance: Capable of inspection throughput easily exceeding 100 Gbps and close to line-rate speeds
- Scalability: Easy to deploy, configure, and update from a single centralized management system
- Unmatched security: Consistently rated highest in overall security effectiveness in independent testing
- Lower TCO: Cuts IT staff time in half with one of the lowest TCO-to-inspected-throughput ratios in the industry

Security, scalability, and speed without compromise

High-performance IPS solutions should be future-proof

As bandwidth growth continues to drive demand for higher performance in core networks, data centers, and large enterprises, more customers than ever require scalability and speed beyond the capabilities of any single IPS appliance.

A single modular IPS appliance may scale to satisfy demand in the short term, but the maximum number of modules and interfaces it can support will always be limited. When adding new appliances is inevitable, scalability can become a challenge.

For an IPS solution to be truly future-proof, it should support the addition of new appliances according to changing demands and accelerated performance requirements, and it should scale in a manageable and cost-effective way.

Unfortunately, it's dangerously easy to emphasize scalability and inspection throughput at the expense of security and inspection efficacy. If the impact of a breach could mean the future of your business, the only "right balance" between security and performance is one where neither is compromised.

One solution for security, scalability, and speed

For customers who cannot compromise, Forcepoint IPS solutions offer the security, scalability, and speed required by even the most demanding networks.

Forcepoint NGFW stands alone as the most secure IPS solution on the market today. Independent testing by NSS Labs[1] granted Forcepoint NGFW IPS the highest overall security effectiveness rating of all products tested, including a 99.9% exploit block rate, a 100% anti-evasion rating, and zero false positives.

Forcepoint NGFW IPS solutions are also highly scalable and cost-efficient, with the capability to achieve inspection throughput close to line-rate speeds and one of the lowest TCO-to-inspected-throughput ratios in the industry[1]. Centralized management using Forcepoint NGFW Security Management Center (SMC) also makes it easy to reconfigure, update, and scale according to your organization's needs, further lowering TCO by requiring an average of 53% less IT staff time[2] to manage your IPS appliances and respond to events.

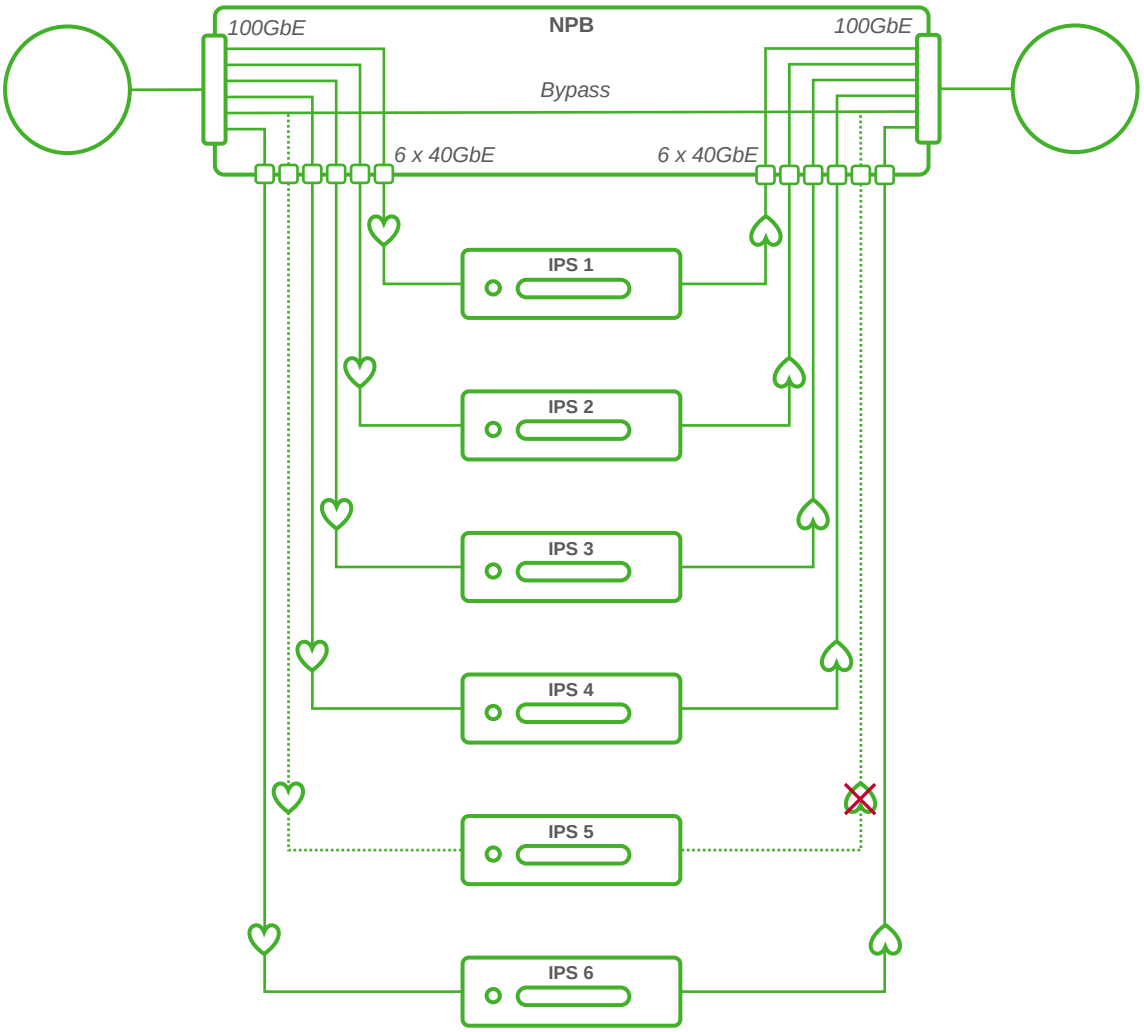
An example implementation and configuration overview are provided below to provide proof of performance and assist in implementing your own high-throughput IPS solution using Forcepoint NGFW appliances.

Example implementation

To illustrate the scalability and performance capabilities of Forcepoint IPS solutions, an example high-throughput implementation using multiple Forcepoint IPS appliances was created and validated. This example implementation is designed to be simple and flexible so that it can easily be altered to suit the specific requirements of your network and infrastructure.

A simplified diagram of the example implementation is provided below. The NPB device is connected inline to the main network link over two 100 Gigabit Ethernet (GbE) interfaces. The 6 IPS engines are connected in parallel to the NPB over 40GbE interfaces.

Figure: Hardware configuration diagram of high-throughput IPS implementation



The example implementation uses 6 Forcepoint NGFW appliances as IPS engines and a Niagara Networks™ 2847 modular Network Packet Broker (NPB) for balancing traffic across them. The Niagara NPB also acts as a fail-open bypass in the event of multiple IPS appliance failures or a failure of the NPB itself. For more information on the Niagara 2847, contact Niagara Networks.

The IPS engines are configured to use Forcepoint NGFW's "Customized High-Security Inspection Policy" with unconditional inspection coverage and evasion protection. Maximum inspection throughputs achieved with this implementation under test are as follows:

HTTP payload size	IP version	Inspection throughput
21 kB	IPv4	75 Gbps
21 kB	IPv6	105 Gbps
100 kB	IPv4	170 Gbps
100 kB	IPv6	185 Gbps

The following guide describes how to configure a similar high-throughput IPS solution using multiple Forcepoint NGFW IPS engines and an NPB to achieve performance and scale according to your organization's needs. Configurations specific to the example above are provided where appropriate.

Configuration overview

Provisioning NPB and IPS engines

Some general guidelines for choosing the right NPB and IPS engines are as follows:

- Ensure that the NPB is capable of load balancing traffic across IPS engines in a suitable manner according to the engines' capabilities and your network traffic's characteristics. More information on this topic is provided in the *Load balancing* section below.
- Ensure that the NPB includes the proper bypass functionality to divert traffic around the IPS engines in the case of failure or scheduled maintenance. More information on this topic is provided in the *Bypass* section below.
- Redundant NPB devices and external bypass switches may also be added for further system resiliency.
- Provision enough IPS engines to handle peak traffic loads even when one or more engines are unavailable. This allows continuity of service in case of an engine failure or maintenance break.

NPB configuration

Load balancing

It is important that traffic is distributed across the IPS engines proportionately according to each engine's capabilities. For example, if traffic is unevenly distributed across identical IPS engines, one or more engines will become overloaded while resources lay idle on other engines and the group's maximum performance will be limited. Likewise, if traffic evenly distributed across IPS engines with very different capabilities, the lowest performing engine will dictate the performance ceiling for the group.

Furthermore, multiple load balancing policies may be available depending on the NPB device chosen, each with its own suitable use cases. For example, load balancing based on MAC addresses may outperform balancing based on 5-tuples, but the former can more easily lead to asymmetrical traffic distribution across IPS engines.

Thus, the optimal load balancing policy for your implementation will depend on the IPS engines used as well as the typical traffic characteristics of your network. Our example implementation employed a load balancing policy using source and destination IP addresses and ports.

Bypass

In addition to load balancing, the NPB should also provide bypass functionality for high availability of IPS services. This enables IPS engine software upgrades with no downtime as well as fast failover recovery in the event of IPS engine failure. It is recommended to provision enough IPS engines and

configure bypass thresholds so that a single engine failure will not disrupt traffic, since a software upgrade will take an engine out of service for short period of time.

The NPB monitors IPS engine availability and health in order to determine when a bypass should occur by sending a heartbeat packet through IPS engines at a set interval. If a certain number of these packets is not received by the NPB within a timeout period, the NPB will consider the IPS engine or group as unresponsive and activate its bypass functionality for that engine or group.

Our example implementation is set to redistribute traffic across healthy IPS engines in the event of a single IPS engine failure, and to bypass the entire engine group if more than one engine fails. The Niagara NPB is also configured to fail open in case of power failure to the NPB. Ethernet heartbeat packets were transmitted every 250 ms.

IPS configuration

Connection tracking

Deep packet inspection requires connection tracking to be enabled in Normal, Strict, or Loose mode. Our example implementation uses Loose connection tracking, which is the default and recommended setting for IPS engines. Loose connection tracking is required when packets belonging to the same connection do not always pass through the same IPS engine.

Access rules

Access rules for IPS engines must allow heartbeat packets from the NPB without delay. More detailed instructions on access rule configuration for IPS engines are available from your Forcepoint NGFW Product Guide.

About Forcepoint

Forcepoint is transforming cybersecurity with systems that understand people's intent as they interact with critical data and IP, enabling companies to empower employees with unobstructed access to confidential data. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. Visit https://www.forcepoint.com and follow us on Twitter at @ForcepointSec.

[1] NSS Labs, *Next Generation Intrusion Prevention System Comparative Report*, 2017-11-17

[2] IDC, *Quantifying the Operational and Security Results of Switching to Forcepoint NGFW*, 2017-05