SOLUTION BRIEF

Scaling Forcepoint IPS

Solutions for High-Performance Networks

SUMMARY

Core networks, data centers, and large enterprises demand speed, scalability, and security without compromise. Forcepoint Intrusion Prevention System (IPS) solutions provide scalable, future-proof performance with the highest-rated security efficacy on the market today, at a very low total cost of ownership (TCO).

The example implementation referenced in this document uses Forcepoint NGFWs (Next Generation Firewalls) as IPS engines and a Niagara Networks™ N2 series device as a network packet broker (NPB) to demonstrate how to attain performance and security at scale. Under test conditions, this implementation achieved an impressive IPS inspection throughput of 186 Gbps across a 100 Gigabit Ethernet link with bidirectional traffic.

The example implementation is 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 to suit the specific requirements of your network and infrastructure.

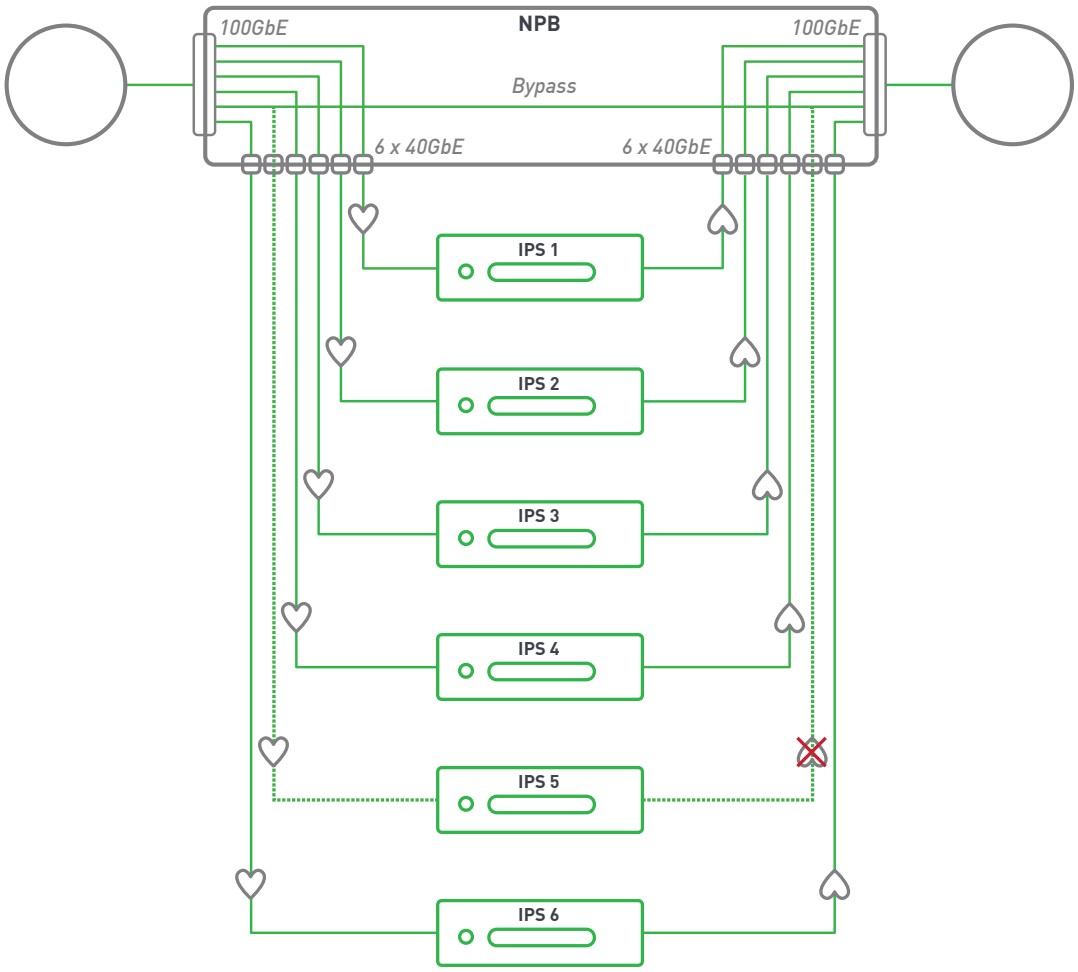
Forcepoint IPS solutions provide the following key benefits for demanding deployments:

- **High performance:** Capable of inspection throughput in excess of 100 Gbps and near line-rate speeds
- **Scalability:** Deploy, configure, and update up to 2,000 Forcepoint IPS, NGFW, or layer two firewalls from a single, centralized management system
- **Unrivaled security:** Consistently rated highest for overall security effectiveness in independent tests
- **Reduced TCO:** Cuts IT staff time in half with one of the lowest TCO-to-inspected-throughput ratios in the industry

EXAMPLE IMPLEMENTATION

An high-throughput example implementation was designed and validated to illustrate the scalability and performance capabilities of Forcepoint IPS solutions. This can easily be altered to suit the specific requirements of any network or infrastructure.

A simplified diagram of the example implementation is provided below. The NPB device is populated with a 100Gb bypass module and three 40Gb packet broker modules, and connected inline to the main network link over two 100GbE interfaces. The six IPS engines are connected in parallel to the NPB over 40GbE interfaces.



Hardware configuration diagram of the example implementation (Appliance IPS 5 is bypassed due to heartbeat loss)

The example implementation uses Forcepoint NGFW appliances as IPS engines and a Niagara Networks N2 2847 modular multi-purpose Network Packet Broker (NPB) for balancing traffic across them. The Niagara Networks modular NPB uses double protection bypass technology and supports fail-open bypass in the event of multiple IPS appliance failures or failure of the NPB itself. For more information on the Niagara Networks N2 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 throughout
21 kB	IPv4	75 Gbps
21 kB	IPv6	105 Gbps
100 kB	IPv4	170 Gbps
100 kB	IPv6	185 Gbps

Maximum inspection throughputs achieved by the example implementation under test

The following section 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

- Ensure that the NPB is capable of load balancing traffic across IPS engines in a manner suitable for the engines' capabilities as well as the mix and volume of network traffic
- Verify that the NPB includes bypass functionality to divert traffic around the IPS engines in the event of failure or scheduled maintenance
- 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
- Deploy additional NPB devices and external bypass switches if further system resiliency is required

NPB CONFIGURATION

LOAD BALANCING

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

Multiple load balancing policies may be available depending on the NPB device chosen, each with its own use cases. For example, load balancing based on MAC addresses may outperform balancing based on quintuples, but the former is more likely to cause asymmetrical traffic distribution across IPS engines.

The example implementation assumed a load balancing policy based on source/destination IP addresses and ports but the optimal load balancing policy for your implementation will depend on the IPS engines used as well as the typical traffic of your network.

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 to be completed without network 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 or offline maintenance period will not cause disruption to network functionality.

The NPB monitors IPS engine availability and health by sending a heartbeat packet at designated intervals. If a certain number of these packets is not returned to the NPB within the timeout period, the NPB will consider the IPS engine or group as unresponsive and activate the bypass function.

Ethernet heartbeat packets are transmitted every 250ms in the example implementation. In the event of a single IPS engine failure, traffic is redistributed across healthy IPS engines. If more than one engine fails, traffic will bypass the entire engine group. The Niagara Networks NPD is also configured to fail open in the case of a power failure.

IPS CONFIGURATION

CONNECTION TRACKING

Deep packet inspection requires connection tracking to be enabled in normal, strict, or loose mode. The 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 www.forcepoint.com and follow us on Twitter at @ForcepointSec.

ABOUT NIAGARA NETWORKS

Niagara Networks provides all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb. Based in San Jose, California, Niagara Networks are agile in responding to market trends and in meeting the customized needs of customers worldwide. Visit https://www.niagaranetworks.com

CONTACT
www.forcepoint.com/contact