White Paper

NSFOCUS and Intel Achieve High-Performance Encrypted Traffic Detection Through Fastjoy and AI Acceleration

"The performance and intelligence level of traffic feature analysis tools are critical to the cybersecurity defence system. While the open-source Joy library has laid a solid foundation for capturing and analysing network data, it still faces multiple bottlenecks when handling complex network traffic, creating an urgent need for technological innovation. NSFOCUS has deeply integrated Intel's Fastjoy framework, with Intel's advanced hardware acceleration capabilities and AI development acceleration toolkits. This integration significantly enhances the intelligence and efficiency of network-security defence systems, setting a new benchmark for the cybersecurity industry."

- Ye Xiaohu, CTO of NSFOCUS

Authors

Liyan Wang
Dong Wang
Xuekun Hu
Hongjun Ni
David Lu
Intel Corporation

Hongliang Zhao
Tian Peng
NSFOCUS

Table of Contents

1. Encrypted Traffic Detection Emerges as a Critical Requirement for Network Supervision

The rising frequency of cyber threats—including network intrusions, telecom fraud, and the spread of violent or extremist multimedia—has reinforced the importance of network traffic analysis as a core component of network supervision. The ongoing strengthening of global cybersecurity regulations, together with heightened user awareness, has accelerated the widespread adoption of encryption technologies across the internet. As encrypted traffic rises—reaching over 90% in certain contexts[1]—the cumulative impact of these trends presents substantial challenges to traditional network supervision approaches.

Today, encrypted traffic detection typically relies on three categories of technologies. First, traditional Deep Packet Inspection (DPI) is the most technically mature approach, but its effectiveness diminishes sharply in encrypted environments. Encryption protocols designed to evade scrutiny deliberately avoid exposing fixed, detectable features, making DPI unsuitable for such scenarios. Second, fingerprint-based techniques—such as JA3, JA3S, and JA4+—are widely applied in TLS encrypted-traffic detection and can achieve reasonable results. However, they require detailed analysis and ongoing validation of traffic fingerprints, resulting in high maintenance overhead. Also, when facing encrypted network tools that disguise themselves as normal TLS traffic, the detection effectiveness is declined. Third, AI model-based encrypted traffic detection avoids dependency on predefined rules or deep protocol parsing. AI models can adapt to complex encryption protocols, offer self-evolving detection capabilities, and significantly reduce manual maintenance. As a result, AI-driven approaches are gaining momentum in encrypted-traffic detection. Nonetheless, AI-based traffic detection approaches are facing cyberthreat challenges, including substantial computational and memory demands. These resource requirements can place considerable pressure on edge-deployment devices, potentially affecting overall detection performance.

NSFOCUS's network-traffic detection products are designed to address these challenges. The NSFOCUS Unified Threat Sensor (UTS) series integrates all three detection technologies, delivering comprehensive and robust detection capabilities. The NSFOCUS UTS has successfully identified encrypted attack activities across numerous real-world customer environments. To further enhance product performance, NSFOCUS continues to explore optimization strategies for AI-based encrypted-traffic detection.

2. NSFOCUS Utilizes Fastjoy Optimized by Intel to Enhance AI-Based Encrypted Traffic Detection Solution

The NSFOCUS UTS is an industry-wide, full-traffic threat detection probe that integrates NSFOCUS's extensive expertise in security research and threat detection accumulated over many years. Leveraging technologies such as rule engines, virtual sandboxes, threat intelligence, and machine learning, UTS delivers wide-ranging threat visibility, high detection accuracy, and strong interoperability. It can conduct advanced threats detection and analysis across diverse scenarios and supports comprehensive event tracing and investigation.

The product offers a rich set of capabilities through multiple built-in detection engines, covering intrusion detection, web security detection, encrypted traffic detection, malicious file detection, dynamic malware analysis, 5G security inspection, anomaly behaviour detection, and threat intelligence integration. These engines enable precise identification of advanced threats across various environments. UTS also provides comprehensive threat traceability and forensic capabilities. In addition to storing full network traffic and alert logs, it supports session-level full-traffic storage and malicious traffic archiving. Attack events can be accurately reconstructed through logs and raw PCAP packets, enabling timely and effective forensic investigation. Furthermore, the system supports flexible and customizable log plug-ins and is compatible with mainstream industry interface protocols. This enhances customers' capabilities in full-traffic detection, analysis, and operational integration.

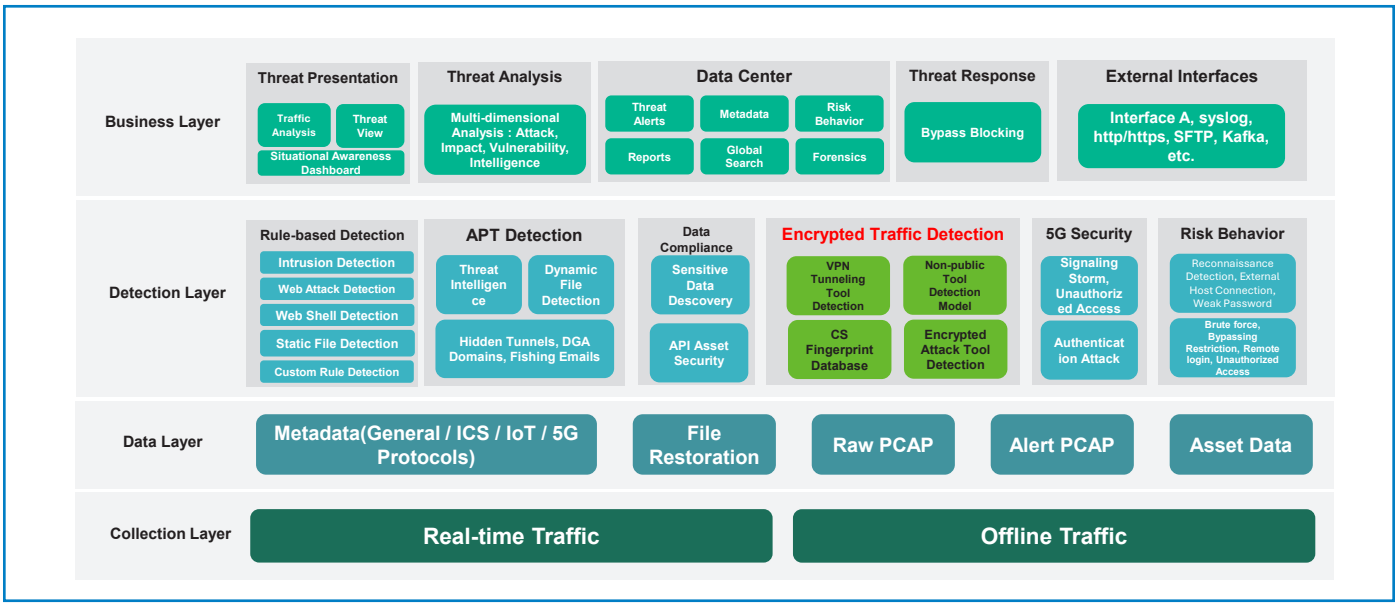

Figure 1. NSFOCUS UTS Architecture

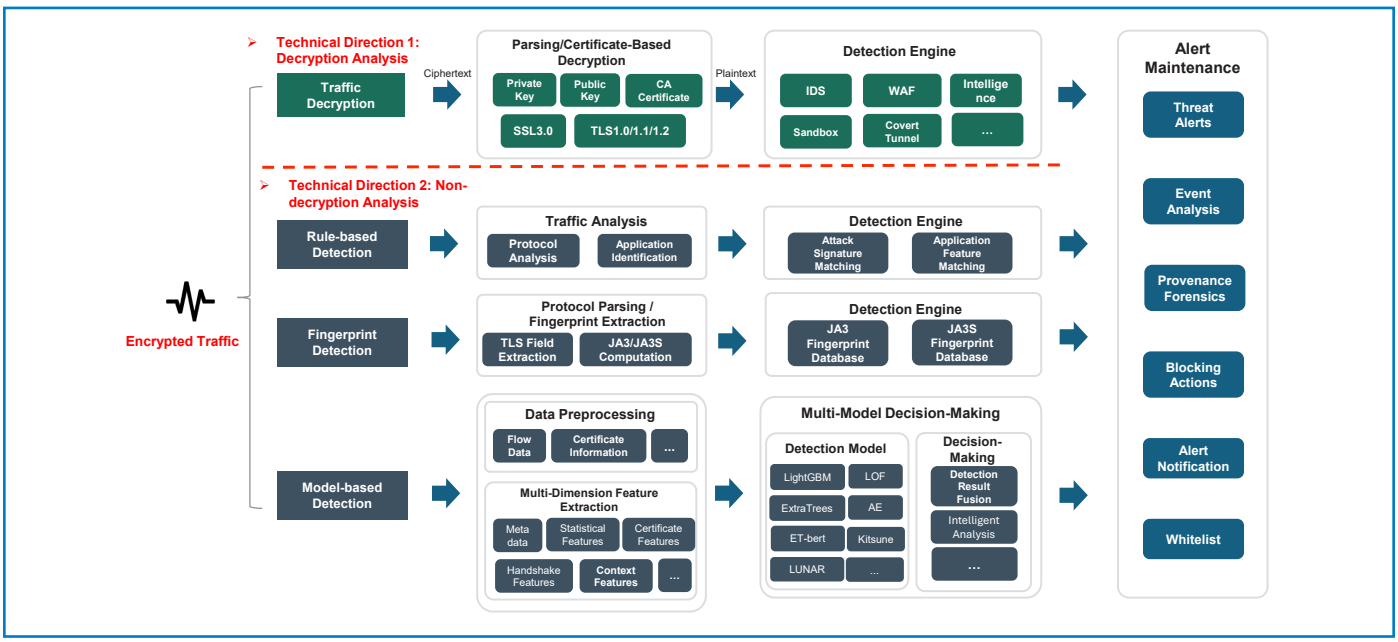

Figure 2. NSFOCUS Encrypted Traffic Detection Technology Architecture

NSFOCUS UTS incorporates a diverse set of encrypted traffic detection technologies. Through continuous research and optimization efforts in fingerprint features and AI-based detection conducted in collaboration with NSFOCUS's security research team. NSFOCUS UTS has yielded strong results in real-world deployments, demonstrating the viability and value of AI-driven encrypted traffic detection. NSFOCUS continues to refine its technical approach to strengthen performance and product competitiveness.

To address challenges commonly encountered when applying AI models in encrypted traffic detection—such as limited performance and high memory consumption—NSFOCUS and Intel jointly introduced Fastjoy, a next-generation, open-source traffic feature analysis framework. Fastjoy is optimized with Intel's advanced hardware acceleration capabilities, the high-performance VPP (Vector Packet Processor) data-processing engine, and Intel® oneAPI Toolkit, delivering a comprehensive upgrade over the open-source Joy library. Fastjoy uses a full-stack acceleration approach. At the hardware layer, Intel® processors with Intel® Advanced Vector Extensions 512 (Intel® AVX-512) and Intel® Deep Learning Boost (Intel® DL Boost) instruction sets, enabling real-time extraction of traffic features and efficient online inference of complex AI models. At the software layer, Fastjoy seamlessly connects with AI frameworks, tools, and libraries optimized for Intel platforms, including Intel® oneDNN and Intel® oneDAL, significantly improving algorithm performance. This integrated pipeline—spanning hardware acceleration, framework optimization, and model deployment—optimizes platform resource utilizations from memory overhead to processing efficiency, and supports AI models for different domain.

With Fastjoy integrated, NSFOCUS UTS achieves notable gains in encrypted traffic detection throughput, delivering true real-time detection while reducing system memory pressure and device cost. Furthermore, Fastjoy-enhanced AI detection capabilities can be extended across NSFOCUS's broader portfolio of gateway security products, strengthening the overall market competitiveness of the solution.

3. Test Configuration and Reference Performance Results

3.1 Intel® Xeon® 6 SoC

Intel Xeon 6 SoC, with up to 72 Performance-cores (P-cores) in a single-socket configuration, offers strong compute density and excellent performance-per-watt. Designed for edge and network-centric workloads, the SoC provides PCIe 5.0 support and integrates a comprehensive suite of accelerators and interfaces—including Intel® QuickAssist Technology (Intel® QAT), Intel® Media Transcode accelerator, Intel® vRAN accelerator, and Intel® Ethernet. The processor also incorporates Intel® Advanced Matrix Extensions for high-efficiency matrix operations and supports the expanded Intel AVX-512 instruction set.

Compared with previous generations, Intel Xeon 6 SoC delivers DDR5 with higher memory bandwidth and significantly enhanced on-chip acceleration engines, enabling optimized performance for applications such as virtualized RAN (vRAN),

Figure 3. Intel® Xeon® 6 SoC Delivering High Performance and Connectivity

media processing, and AI inference. These improvements make Intel Xeon 6 SoC a strong fit for high-throughput, latency-sensitive security and networking scenarios.

3.2 Fastjoy vs. Joy Software Performance and Connectivity

The test was conducted to compare the performance of Fastjoy and Joy on the Intel Xeon 6 SoC-based platform[2]. The test topology is shown in Figure 4 and Figure 5. The test system is directly connected to the device under test (DUT) through a network interface card, with a link bandwidth of 25 Gbps. Network packets are transmitted from the test machine, pass through the DUT, and are then returned to the test machine.

During this process, Fastjoy, built on VPP, receives and processes the packets through VPP and forwards the processed packet to achieve inline processing. In contrast, Joy reads packets using the Linux kernel's AF_PACKET socket interface, without affecting packet forwarding within the kernel, operating instead in an out-of-band (bypass) processing mode.

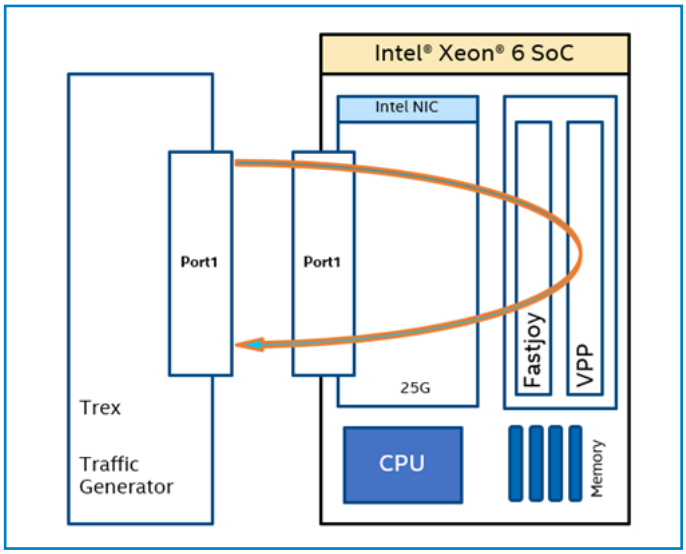

Figure 4. Fastjoy Test Topology

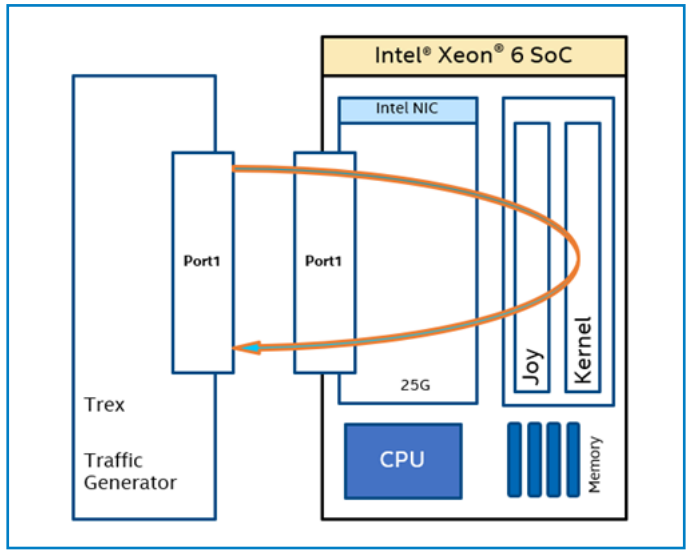

Figure 5. Joy Test Topology

The VPN-nonVPN dataset (ISCXVPN2016)[3] is used in this evaluation. This dataset includes traffic generated by multiple categories of applications operating over various protocols, such as email, web browsing, file transfer, and video calling. Each application category contains both normal session traffic and VPN-based session traffic, providing two distinct traffic modalities. With tens of millions of packets in total, the dataset offers sufficient scale and diversity to support research in network traffic analysis and detection.

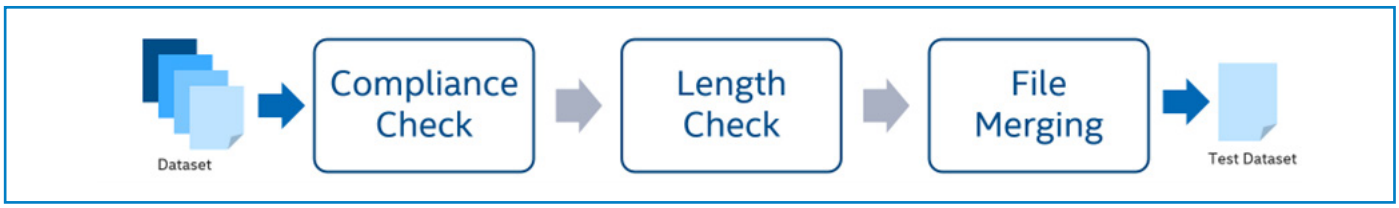

Figure 6. Data Preprocessing Workflow

To ensure consistent and reliable testing, the dataset was systematically pre-processed. Packets failing to meet format requirements were removed, and excessively long packets were truncated to avoid skewing results. All remaining packets were then consolidated into a single PCAP file for easier use. The final dataset is 17 GB, containing 21.94 million packets ranging from 64 to 8,900 bytes, providing a stable and standardized basis for subsequent evaluation.

From Figure 7, Fastjoy achieves a 23 times performance improvement over Joy on the Intel Xeon 6 SoC platform. In the 8-core configuration, Fastjoy has not yet reached its maximum potential, as the Trex traffic generator has already hit its packet-generation limit. Compared with Joy, Fastjoy incorporates multiple architectural optimizations—including packet-receiving mechanisms, flow-aging algorithms, packet scheduling, and memory management. Detailed comparisons are provided in Table 1.

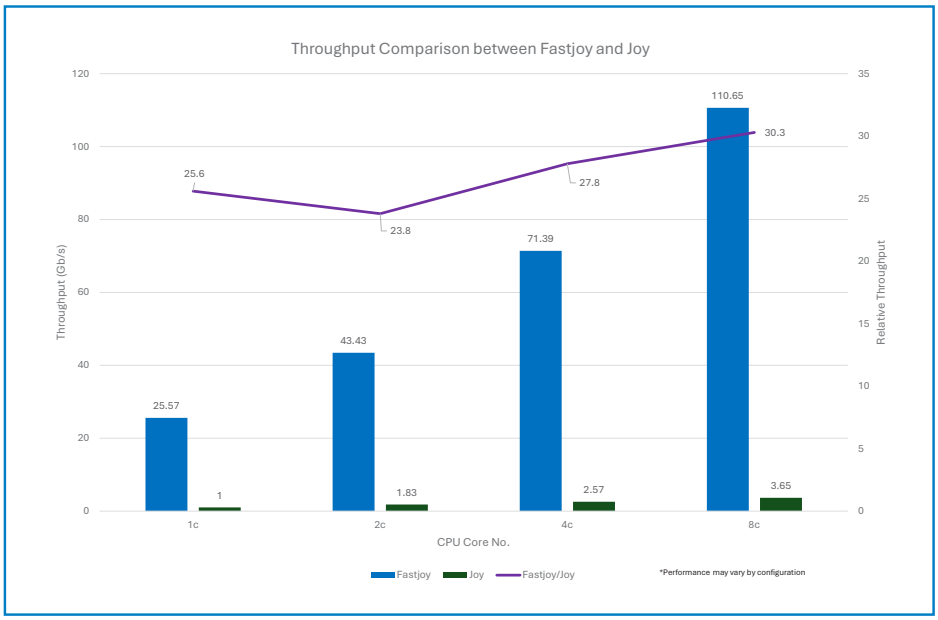

Figure 7. Fastjoy vs. Joy Throughput Comparison

	Fastjoy	Joy
Packet Reception Method	VPP	AF_PACKET
Flow Aging Algorithm	Three-Level Timing Wheel	Sequential Traversal
Packet Scheduling	Hardware-Assisted RSS	AF FANOUT
Memory Management	Memory Management Optimized for Network Workloads	Generic Linux Memory Management

Table 1. Key Technical Differences Between Fastjoy and Joy.

The test results show that Fastjoy delivers a major performance leap in traffic-analysis workloads through a combination of software-level optimizations and effective use of hardware acceleration features, while maintaining full functional compatibility with Joy.

This demonstrates Fastjoy's ability to help users upgrade their traffic-analysis solutions, achieving substantial performance improvements without requiring significant redevelopment effort.

3.3 Performance Comparison and Analysis of Fastjoy vs. Joy in Real-World Scenarios

NSFOCUS carried out a performance comparison between its original Joy-based traffic detection solution and the updated solution incorporating Fastjoy. Both solutions provide equivalent functionality. The evaluation used approximately 400,000 real-world flows collected from a production environment and was executed on a commercially released hardware platform equipped with an Intel® Core™ i7 processor.

The test results show a performance advantage for Fastjoy in real-world scenarios. On the Intel Core processor, Fastjoy achieves a 4.5× throughput increase and a 37.5× reduction in memory usage compared to Joy. These gains stem from Fastjoy's deep integration with Intel's acceleration technologies, enabling more efficient traffic-feature processing and minimizing intermediate data buffering.

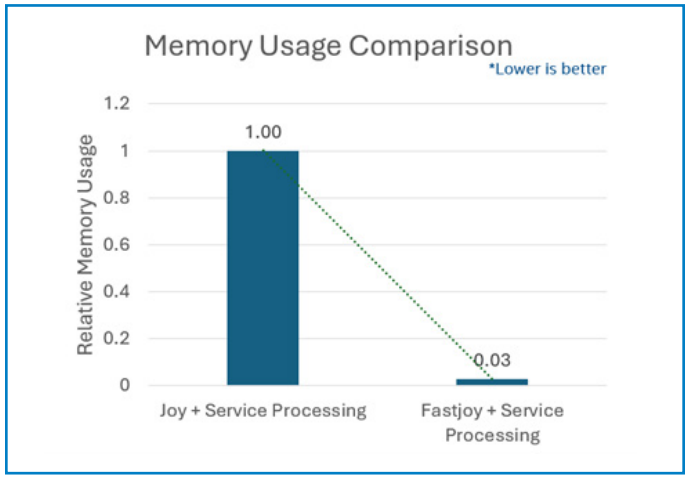

Figure 8. Memory Usage Comparison Between Joy and Fastjoy in Real-World Scenarios

4. Outlook

As a full-traffic threat detection solution built for real-world operations, the NSFOCUS UTS demands both high detection accuracy and strong performance. With Intel's continued advancements in hardware–software optimization, it gives both parties broad prospects for cooperation in performance upgrades and scenario expanding.

Leveraging the Intel Xeon 6 SoC's advanced instruction sets and series of acceleration technologies, along with high-performance software components such as Fastjoy, OpenVINO, and oneDAL, NSFOCUS UTS not only significantly improves the performance of encrypted traffic detection, but also is poised to enhance the accuracy and response speed of other detection capabilities, deepen threat backtracking capabilities, accelerate PCAP package storage and analysis efficiency, strengthen threat forensics. Together, these innovations enable NSFOCUS to offer more efficient, lower-power, and higher-precision advanced threat-defence solutions across the industry.

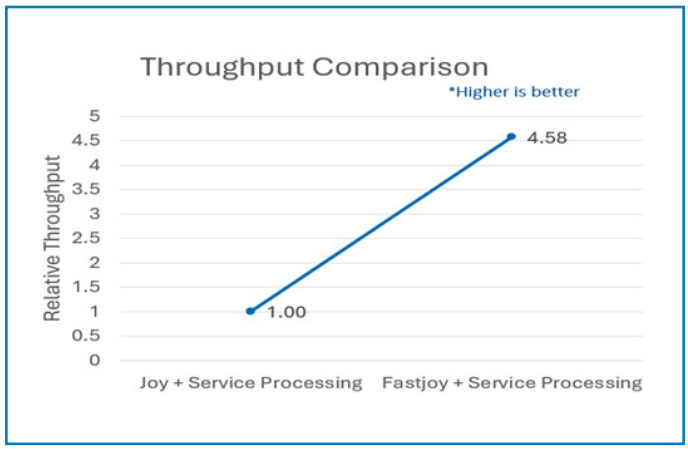

Figure 9. Throughput Comparison Between Joy and Fastjoy in Real-World Scenarios

References

1 https://www.sciencedirect.com/science/article/pii/S2352864821000699#bib1

2 Test configuration: Single Intel® Xeon® 6543P-B processor @ 2.0 GHz, 32 cores, 128 GB total memory (4x32 GB DDR5 5600 MT/s), Hugepage Size 1GB, Ubuntu 22.04.1 LTS, Linux 5.15.0-27-generic, Fastjoy v25.04, Joy v4.5.0, Trex v3.00.

3 Gerard Drapper Gil, Arash Habibi Lashkari, Mohammad Mamun, Ali A. Ghorbani, "Characterization of Encrypted and VPN Traffic Using Time-Related Features", In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), pages 407-414, Rome, Italy.

Learn More

NSFOCUS

Intel® Industry Solution Builders

0426/KF-DP/PDF 368870-001US