

شماره : ۱۴۰۵۰۶۳۰۰۱

تاریخ : ۱۴۰۵/۰۶/۳۰

پیوست :

برنام خد



شرکت فناوری ارتباطات

آشیانه امن

شماره ثبت : ۲۴۰۶۳۲

مقایسه فنی معماری PT NGFW با فایروال های مبتنی بر شتاب دهنده سخت افزاری

مقایسه قابلیت های فایروال های مبتنی بر سخت افزارهای خاص و افلودر و فایروال های معماری نرم افزاری با انعطاف بالای سخت افزاری

Specialized Hardware NGFWs vs. Software-Defined NGFWs
Different Approaches. Different Trade-offs. A Smarter Choice for Your Needs.

Fortinet (Hardware-Accelerated Security)	Positive Technologies (Software-Defined NGFW)
ASIC / SPU Acceleration	Standard x86 Hardware
Proprietary Hardware	Software-Based Data Plane (DPDK)
Vendor Lock-in	Flexible Hardware Options
Limited Flexibility	Easier Upgrade & Scaling
Hardware Upgrade Depends on Vendor	Greater Control & Visibility
Supply Chain Risks	No Dependency on Specialized ASIC

High Performance (Per Appliance) | Closed Ecosystem | Hardware Dependent

High Flexibility | Software-Driven Innovation | Cost-Effective | Resilient Supply Chain

LIMITED OPTIONS | SUPPLY RISKS

FLEXIBILITY | SCALABILITY | FREEDOM

YOUR SECURE FUTURE

SAME GOAL | DIFFERENT ARCHITECTURES | A MORE SECURE TOMORROW

نگارش ۱.۴ - شهریور ۱۴۰۵



مقدمه

در طراحی تجهیزات مدرن امنیت شبکه، دستیابی همزمان به دو هدف «بازرسی عمیق ترافیک یا DPI» و «پردازش با نرخ چند ده یا چند صد گیگابیت بر ثانیه» یکی از چالش‌های اصلی معماری است. قابلیت‌هایی مانند NAT, Stateful Firewall, Application Control, Deep Packet Inspection, IPS, Anti-Malware و به خصوص TLS Inspection به منابع پردازشی قابل توجهی نیاز دارند. به همین دلیل بسیاری از سازندگان تجهیزات امنیتی طی سال‌های گذشته بخشی از پردازش ترافیک را از CPU عمومی به پردازنده‌های اختصاصی مانند ASIC, NPU, FPGA یا Crypto Processor منتقل کرده‌اند.

Fortinet یکی از نمونه‌های شناخته شده این رویکرد است. این شرکت در بسیاری از FortiGate‌ها از Security Processing Unit یا SPU استفاده می‌کند. Network Processor یا NPها برای Offload کردن پردازش حجیم ترافیک و Content Processor یا CPها برای شتاب‌دهی برخی عملیات امنیتی مانند رمزنگاری، رمزگشایی، تشخیص حملات و پردازش محتوا به کار می‌روند. مستندات رسمی Fortinet نیز تصریح می‌کنند که هدف این پردازنده‌ها برداشتن بخشی از بار پردازشی از CPU اصلی است.

PT NGFW محصول Positive Technologies رویکرد متفاوتی را انتخاب کرده است. معماری این محصول بر پردازنده‌های عمومی X۸۶، پردازش ترافیک در User Space، بهینه‌سازی TCP/IP Stack و استفاده از تکنیک‌هایی مانند DPDK بنا شده است. Positive Technologies در معرفی رسمی PT NGFW اعلام می‌کند که این محصول برای رسیدن به Performance بالا نیازمند ASIC یا FPGA اختصاصی نیست و نسخه‌های رده بالای آن می‌توانند روی معماری X۸۶ به صدها گیگابیت بر ثانیه ظرفیت پردازش برسند.

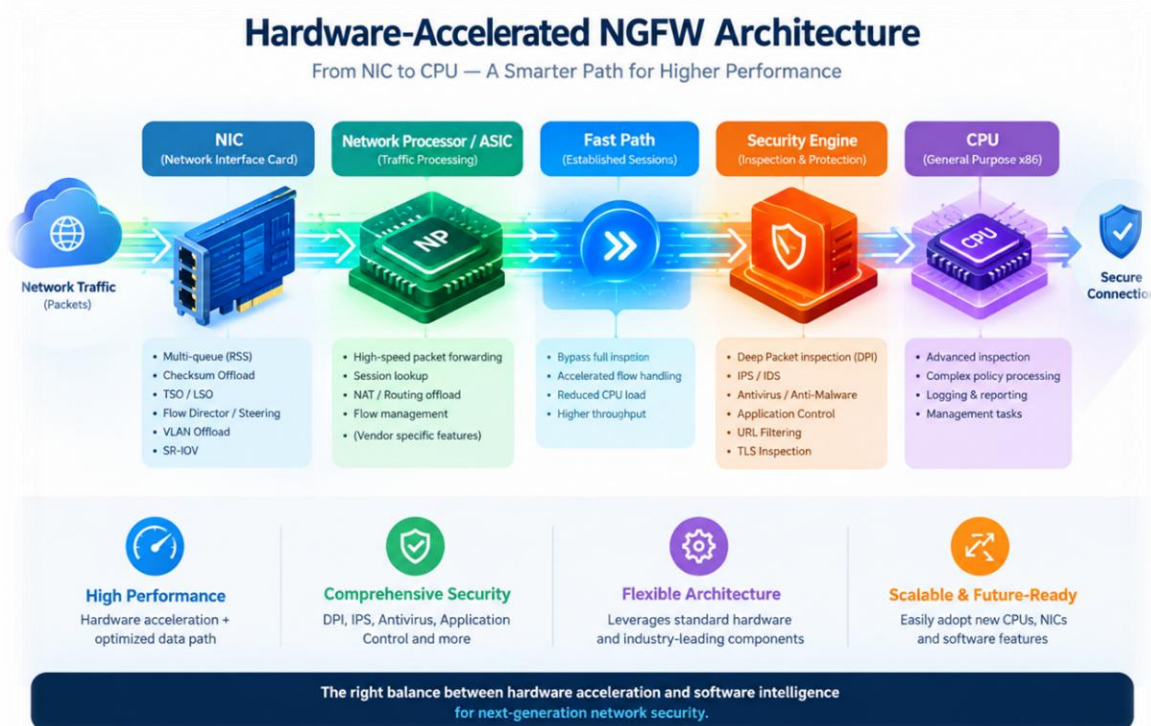
بنابراین تفاوت اساسی میان PT NGFW و بسیاری از Appliance‌های سنتی را می‌توان در دو فلسفه طراحی خلاصه کرد: در یک طرف «انتقال عملیات به سخت‌افزار تخصصی» و در طرف دیگر «بهینه‌سازی شدید پردازش نرم‌افزاری روی پردازنده‌های عمومی و NICهای استاندارد».

معماری Hardware Offload در فایروال‌های سنتی

در یک سیستم عامل شبکه معمولی مانند بسیاری از فایروال‌های بومی که مبتنی بر لینوکس و معماری امنیتی iptables بنا شده اند ، بسته پس از دریافت توسط کارت شبکه وارد Kernel Network Stack شده و مراحل مختلفی مانند Interrupt Processing، ایجاد Buffer، عبور از TCP/IP Stack، Policy Processing و نهایتاً انتقال به Application را پشت سر می‌گذارد. هر یک از این مراحل مقداری CPU Cycle و Memory Access مصرف می‌کند.

در تجهیزات امنیتی که از ASIC یا NPU استفاده می‌کنند، تلاش می‌شود بخشی از این مسیر از CPU عمومی جدا شود. پس از شناسایی و ایجاد یک Session، ممکن است اطلاعات Flow در جدول سخت‌افزاری ثبت شود و بسیاری از Packet‌های بعدی مستقیماً توسط Network Processor پردازش شوند. این مفهوم معمولاً با اصطلاحاتی مانند Hardware Offload، Fast Path یا Accelerated Session شناخته می‌شود.

معماری مفهومی چنین سامانه‌ای را می‌توان به صورت زیر نمایش داد:





در این حالت الزاماً تمام Packet ها یا تمام قابلیت های امنیتی Offload نمی شوند. برای مثال ممکن است NAT، Routing، Identification یا بازرسی پیچیده یک Payload همچنان نیازمند پردازش نرم افزاری باشد.

مزیت این معماری، Performance بالا با مصرف نسبتاً کمتر CPU در عملیات تکرارشونده است. در مقابل، توسعه قابلیت جدید ممکن است تا حدی به امکانات تراشه وابسته شود و Vendor برای هر نسل محصول مجبور به طراحی یا استفاده از نسل جدیدی از شتاب دهنده سخت افزاری باشد که هنوز محصولات بومی در ایران دارای این قابلیت ها نیستند و همچنین تکنولوژی ساخت این قطعات سخت افزاری در انحصار چندین شرکت غربی می باشد که قطعاً با توجه به تحریم های بین المللی امکان تولید مشترک فراهم نیست برای همین نه تنها شرکتهای تولید کننده فایروال ایرانی بلکه شرکتهای چینی و روسی نیز تلاشی برای وابستگی بیشتر به صنایع زیرساختی امریکا و اروپا برای بهبود کیفیت محصولات خود نمیکند برای همین دنبال راهکارهای هوشمندانه دیگری رفته اند.



رویکرد متفاوت PT NGFW

Positive Technologies برای PT NGFW معماری مبتنی بر X86 را انتخاب کرده است یعنی بهره برداری از پردازنده های عمومی که همه جا و انواع مختلف در دسترس می باشد. در مستندات جدید محصول به صراحت به « High-performance architecture » اشاره شده و اعلام می شود که پردازش بسته ها از Kernel Linux به User Space منتقل شده است. همچنین Standard Linux TCP/IP Stack برای Data Plane اصلی مورد استفاده قرار نمی گیرد ، این موضوع از نظر Performance اهمیت زیادی دارد.

در معماری سنتی Linux و بیشتر محصولات بومی در ایران مسیر Packet ممکن است به شکل ساده شده زیر باشد:

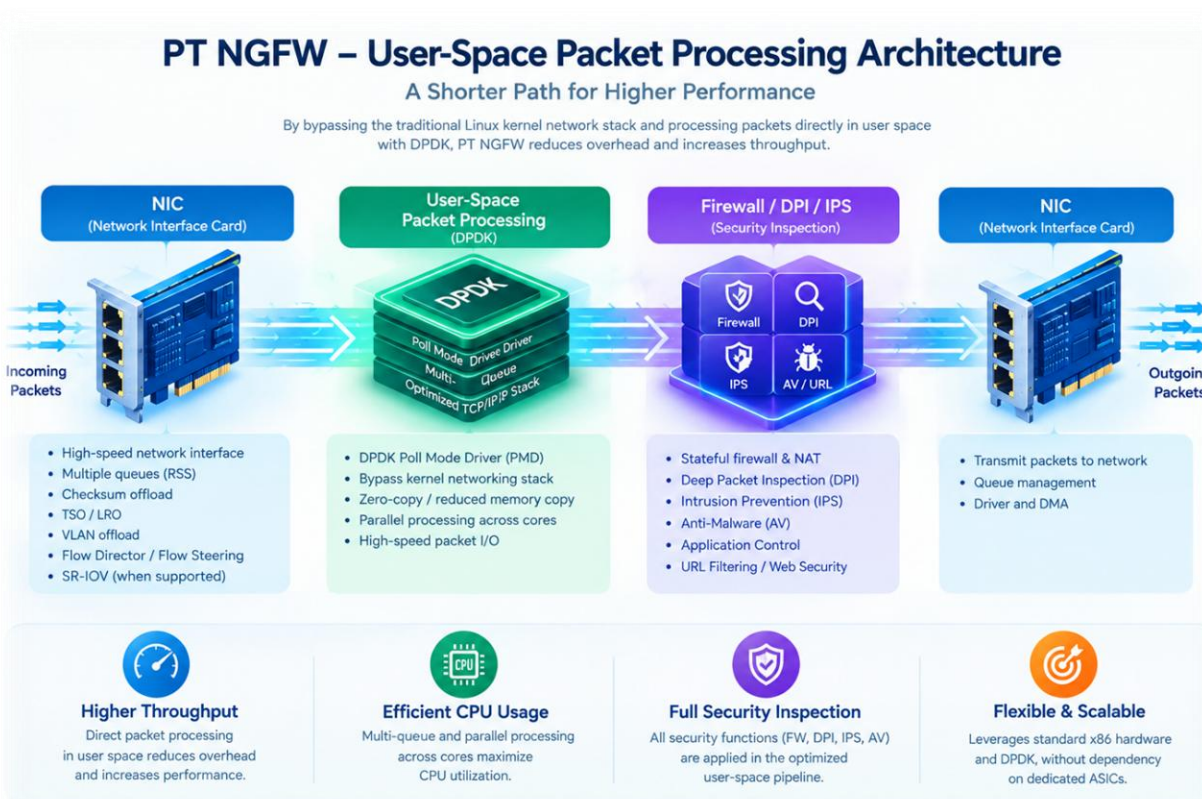
Traditional Linux Firewall Architecture

Packet Flow Through the Linux Kernel

In a traditional Linux-based firewall, each packet passes through multiple layers of the kernel, which increases processing overhead and CPU usage.



اما معماری User-Space Packet Processing اجازه می‌دهد مسیر کوتاه‌تری ایجاد شود:



با حذف یا کاهش عبورهای متعدد میان Kernel Space و User Space، تعداد Memory Copy ها، Context Switch ها و Interrupt های مورد نیاز کاهش پیدا می‌کند. در نتیجه CPU می‌تواند درصد بیشتری از توان خود را مستقیماً صرف پردازش Packet و موتورهای امنیتی کند.

یکی از فناوری‌های مهم در این معماری DPDK یا Data Plane Development Kit است. Positive Technologies منابع رسمی مرتبط با PT NGFW این محصول را یک Enterprise Solution مبتنی بر DPDK توصیف کرده است و حتی برای PT NGFW راهنمای اتصال به DPDK Telemetry منتشر کرده است.

همچنین PT در تشریح فناوری DPI خود توضیح می‌دهد که DPDK امکان Packet Processing با کارت‌های شبکه معمولی Intel، Broadcom و Mellanox (به دلیل اینکه شرکت مادر در اسرائیل فعالیت میکند و بعداً توسط NVIDIA بخش مهمی از سهامش خریداری شده است در زیر ساخت‌های حیاتی کشور توصیه به استفاده نمیشود) را فراهم کرده و نیاز به برخی کارت‌های تخصصی Capture را کاهش داده است. نسخه‌هایی از همین PT DPI در PT NGFW استفاده می‌شوند و پایه بخشی از قابلیت‌های Application Identification و IPS را تشکیل می‌دهند.



آیا DPDK جایگزین Hardware Offloader است؟

این نقطه نیازمند تفکیک دقیق مفاهیم است. DPDK خود یک ASIC یا Hardware Offloader نیست.

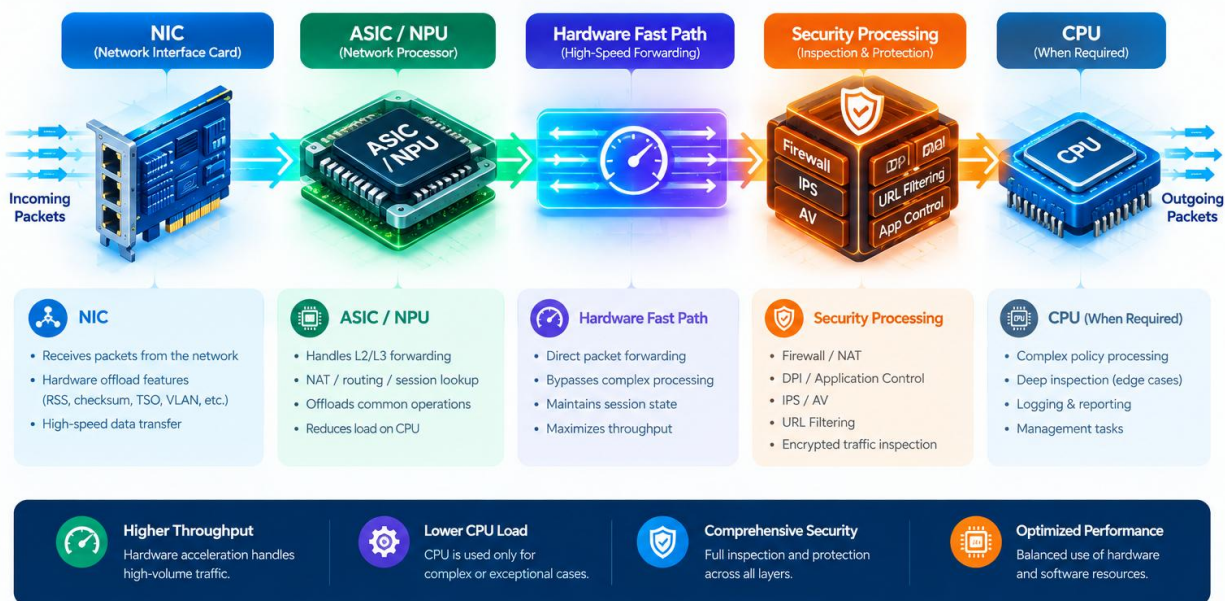
DPDK مجموعه‌ای از Library ها و Driver های بهینه برای پردازش سریع Packet در User Space است. یکی از مهم‌ترین قابلیت‌های آن استفاده از Poll Mode Driver یا PMD است. در این روش به جای وابستگی شدید به Interrupt برای هر مجموعه Packet، Core های مشخص CPU می‌توانند Queue های کارت شبکه را با سرعت بالا Poll کنند.

بنابراین در PT NGFW به جای اینکه یک NPU بخش بزرگی از Data Plane را مستقل از CPU پردازش کند، معماری نرم‌افزاری تلاش می‌کند بیشترین Performance ممکن را از CPU های X86 و NIC استخراج کند. می‌توان تفاوت دو معماری را به صورت مفهومی چنین نشان داد:

Hardware-Accelerated NGFW Architecture

From NIC to CPU when Required — A Dedicated Path for High Performance

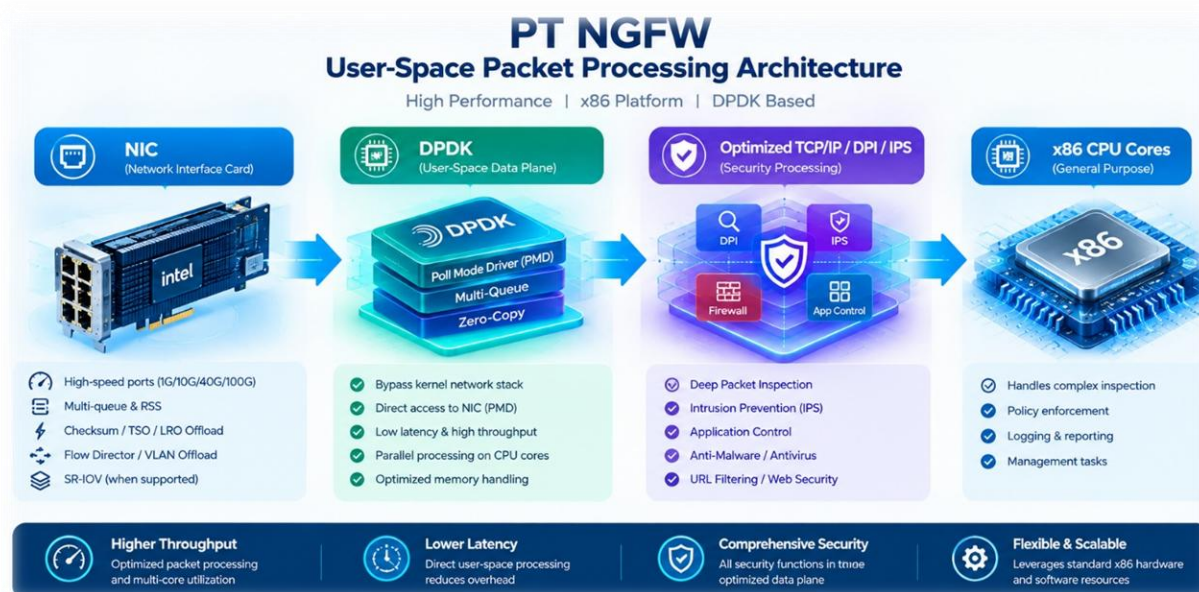
In advanced NGFW platforms, a specialized hardware accelerator (ASIC/NPU) handles high-volume traffic and common security functions, while the CPU is engaged only when necessary.



SMARTER ACCELERATION • STRONGER SECURITY • HIGHER PERFORMANCE



در نتیجه عبارت «PT از DPDK به عنوان Hardware Offloader استفاده می‌کند» صحیح نیست. بیان دقیق‌تر این است که PT با استفاده از User-Space Processing، DPDK، پردازش Parallel روی Core های X86 و الگوریتم‌های اختصاصی، نیاز به Security ASIC اختصاصی را کاهش یا حذف کرده است.



Positive Technologies نیز در صفحه رسمی PT NGFW اعلام می‌کند که معماری X86 با Performance بالا باعث شده نیازی به ASIC یا FPGA اختصاصی وجود نداشته باشد.



مزایای کاهش وابستگی به سخت افزار اختصاصی در معماری NGFW

یکی از مزایای مهم معماری مبتنی بر سخت افزار استاندارد ۸۶X، کاهش وابستگی سامانه امنیتی به تجهیزات اختصاصی یک تولیدکننده مشخص است. این موضوع در کشورهایی که با محدودیت های تجاری، تحریم، مشکلات واردات، تأخیر در تأمین تجهیزات و محدودیت خدمات رسمی Vendor مواجه هستند، اهمیت بیشتری پیدا می کند. در معماری های مبتنی بر ASIC یا NPU اختصاصی، بخش قابل توجهی از ظرفیت پردازشی محصول به تراشه ها و معماری سخت افزاری اختصاصی سازنده وابسته است و در صورت توقف تولید، عدم امکان تأمین یا پایان پشتیبانی یک Appliance، ارتقای سامانه ممکن است مستلزم جایگزینی کامل سخت افزار باشد.

در مقابل، استفاده از معماری X۸۶ و کارت های شبکه استاندارد صنعتی این امکان را فراهم می کند که بخش بیشتری از چرخه عمر سامانه از چرخه عمر یک Appliance اختصاصی مستقل شود. پردازنده، حافظه، Storage و NIC را می توان از خانواده های متداول و قابل تأمین انتخاب کرد و با پیشرفت نسل های پردازنده و کارت شبکه، بستر سخت افزاری را بدون وابستگی مطلق به طراحی اختصاصی یک Vendor توسعه داد. البته این مزیت زمانی کامل می شود که نرم افزار نیز از مجموعه مناسبی از سخت افزارهای استاندارد پشتیبانی کند.

موضوع مهم دیگر، قابلیت ارزیابی و مدیریت ریسک زنجیره تأمین است. تجهیزات امنیتی تجاری معمولاً از مجموعه بزرگی از Firmware، Bootloader، سیستم عامل، Driver، کتابخانه های Third-party و در برخی موارد ASIC/NPU یا اجزای اختصاصی تشکیل شده اند. سازمان مصرف کننده معمولاً به طراحی داخلی تمام این اجزا دسترسی ندارد و بنابراین نمی تواند همه لایه های محصول را مستقلاً تحلیل و ممیزی کند. این مسئله نباید به عنوان اثبات وجود Backdoor در محصولات تجاری تفسیر شود، اما سطحی از اعتماد به Vendor و زنجیره تأمین آن را اجتناب ناپذیر می کند.

وجود تراشه اختصاصی نیز به خودی خود به معنای ناامن بودن محصول نیست؛ همان طور که استفاده از X۸۶ نیز امنیت را تضمین نمی کند. تفاوت اصلی در میزان وابستگی و امکان جایگزینی اجزاست. هرچه معماری بر استانداردهای عمومی تر و قطعات قابل جایگزینی بیشتری متکی باشد، سازمان در طراحی راهبرد تأمین، ایجاد موجودی Spare، انتخاب تأمین کننده جایگزین و ارتقای نسل سخت افزار آزادی بیشتری خواهد داشت.

از طرف دیگر، تجربه سال های اخیر نشان داده است که حتی تجهیزات امنیتی شناخته شده می توانند دارای آسیب پذیری های بسیار جدی در Firmware و Software Stack خود باشند. برای مثال، چندین آسیب پذیری Fortinet با امتیاز CVSS برابر ۹.۸ منتشر شده اند که بعضی از آنها امکان Authentication Bypass یا اجرای کد و فرمان از راه دور را فراهم می کردند. در برخی موارد، این آسیب پذیری ها در فهرست Known Exploited Vulnerabilities نیز قرار گرفته اند؛ یعنی بهره برداری واقعی از آنها مشاهده شده است.

شماره : ۱۴۰۵۰۶۳۰۰۱

تاریخ : ۱۴۰۵/۰۶/۳۰

پیوست :

برنام خدا



شرکت فناوری ارتباطات

آشیانه امن

شماره ثبت : ۲۴۰۶۳۲

نمونه‌های زیر اهمیت این موضوع را نشان می‌دهند:



نمونه‌ای از آسیب‌پذیری‌های بحرانی Fortinet در سال‌های اخیر

این موارد نشان می‌دهند که حتی محصولات شناخته شده امنیتی نیز ممکن است دارای آسیب‌پذیری‌های بسیار جدی باشند و وابستگی کامل به یک Vendor می‌تواند ریسک عملیاتی قابل توجهی ایجاد کند.

CVE	Product / Component	Vulnerability Type	CVSS Score	Impact / Description
 CVE-2022-40684	FortiOS / FortiProxy / FortiSwitchManager	Authentication Bypass	9.8 Critical	Allows unauthenticated attackers to perform administrative operations on vulnerable devices.
 CVE-2023-27997	FortiOS / FortiProxy (SSL-VPN)	Heap-based Buffer Overflow	9.8 Critical	Allows remote code execution via specially crafted requests.
 CVE-2024-21762	FortiOS / FortiProxy	Out-of-Bounds Write	9.8 Critical	Allows remote code execution or command execution through crafted requests.
 CVE-2024-47575	FortiManager	Missing Authentication (FGFM)	9.8 Critical	Allows unauthorized code or command execution. Actively exploited in the wild.
 CVE-2024-55591	FortiOS / FortiProxy	Authentication Bypass	9.8 Critical	Allows remote attackers to gain super-admin access through crafted requests.



این نمونه‌ها نشان می‌دهند که حتی یک تجهیز امنیتی در لبه شبکه باید خود به‌عنوان یک دارایی حساس با سطح حمله بالا در نظر گرفته شود. به همین دلیل، کاهش وابستگی به یک Vendor خاص و استفاده از معماری مبتنی بر سخت‌افزارهای استاندارد می‌تواند ریسک‌های عملیاتی و زنجیره تأمین را به شکل قابل توجهی کاهش دهد.

- ✓ کاهش ریسک Vendor Lock-in
- ✓ افزایش امکان جایگزینی سخت‌افزار
- ✓ مدیریت بهتر ریسک زنجیره تأمین



REDUCE DEPENDENCY | INCREASE RESILIENCE | STRONGER SECURITY POSTURE | MORE CONTROL | A MORE SECURE TOMORROW

این نمونه‌ها نشان نمی‌دهند که یک Vendor خاص الزاماً ناامن است؛ آسیب‌پذیری بحرانی در محصولات بسیاری از تولیدکنندگان بزرگ کشف می‌شود. نکته معماری این است که هرچه سازمان به یک اکوسیستم بسته، Firmware اختصاصی، Appliance خاص و زنجیره تأمین واحد وابستگی بیشتری داشته باشد، یک آسیب‌پذیری بحرانی یا اختلال در تأمین آن Vendor می‌تواند دامنه عملیاتی وسیع‌تری ایجاد کند.

برای نمونه، CVE-۲۰۲۲-۴۰۶۸۴ یک Authentication Bypass با امتیاز ۹.۸ بود که امکان دسترسی غیرمجاز به عملیات مدیریتی را فراهم می‌کرد. CVE-۲۰۲۴-۲۱۷۶۲ نیز با امتیاز ۹.۸ می‌توانست از طریق درخواست‌های خاص به اجرای کد یا فرمان غیرمجاز منجر شود. CVE-۲۰۲۴-۵۵۵۹۱ نیز یک Authentication Bypass بحرانی بود که امکان دسترسی Remote به سطح Super-Admin را ایجاد می‌کرد. این موارد نشان می‌دهند که حتی یک Appliance امنیتی در لبه شبکه باید خود به‌عنوان یک دارایی دارای Attack Surface در نظر گرفته شود.

بنابراین، یکی از مزایای راهبردی معماری‌هایی مانند X86 + Standard NIC + Software-based Data Plane، امکان کاهش Vendor Lock-in در لایه سخت‌افزار است. سازمان می‌تواند Hardware Lifecycle را تا حد بیشتری مستقل از Software Lifecycle مدیریت کرده و برای CPU، RAM، Storage، NIC و حتی Appliance Server گزینه‌های جایگزین در نظر بگیرد.



در شرایط محدودیت تأمین نیز این ویژگی اهمیت دوچندان پیدا می‌کند. اگر یک Appliance اختصاصی قابل تهیه نباشد، تعمیر آن دشوار شود یا قطعات یدکی آن در دسترس نباشد، ممکن است کل ظرفیت امنیتی وابسته به همان خانواده سخت‌افزاری تحت تأثیر قرار گیرد. در مقابل، استفاده از سرور یا Network Appliance استاندارد X۸۶ امکان طراحی چند پیکربندی سخت‌افزاری تأییدشده، نگهداری قطعات Spare و مهاجرت به نسل جدیدتر CPU/NIC را فراهم می‌کند.

البته معماری X۸۶ نیز ریسک زنجیره تأمین را حذف نمی‌کند. CPU، BIOS/UEFI، BMC، NIC Firmware، Driver و سایر Firmwareها همچنان باید در فرآیند Hardening، Vulnerability Management و Supply-Chain Risk Management قرار گیرند. مزیت اصلی، حذف ریسک نیست؛ بلکه کاهش تمرکز ریسک و افزایش قابلیت جایگزینی و کنترل عملیاتی است.

در نتیجه، برای سازمان‌هایی که علاوه بر Performance، موضوعاتی مانند تحریم، پایداری تأمین، امکان نگهداری بلندمدت، استقلال از یک Vendor و قابلیت ارتقای سخت‌افزار برای آنها اهمیت دارد، معماری مبتنی بر سخت‌افزار استاندارد می‌تواند یک مزیت راهبردی محسوب شود. در چنین مدلی، انتخاب چند پلتفرم X۸۶ و NIC تأییدشده و انجام Benchmark و Hardening روی آنها می‌تواند تعادل مناسبی میان Security، Performance و Supply-Chain Resilience ایجاد کند.

نقش NIC Hardware Offload در معماری PT

نیبود Security ASIC به این معنی نیست که هیچ Hardware Acceleration در سیستم وجود ندارد. کارت‌های شبکه Enterprise امروزی خود دارای قابلیت‌های پردازشی متعددی هستند.

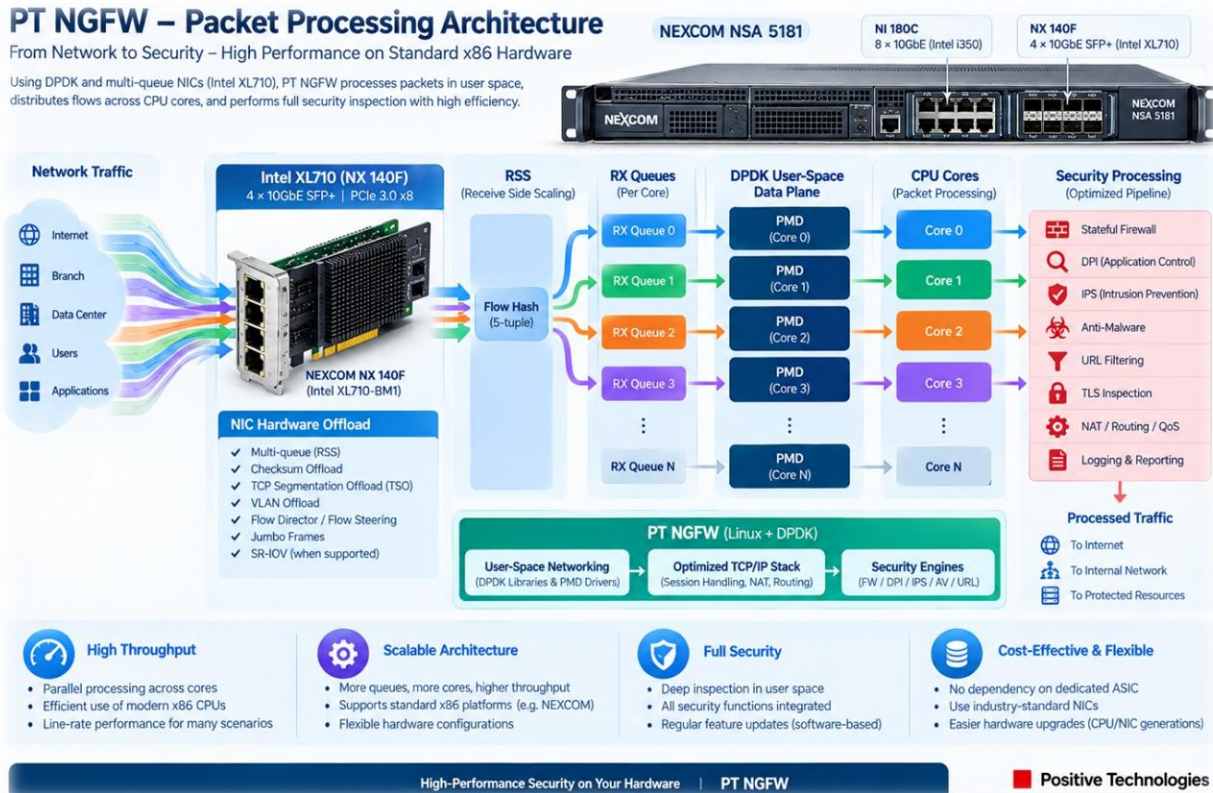
برای مثال Intel XLV۱۰ که در مازول F۱۴۰NX استفاده می‌شود، توسط DPDK i۴۰e Poll Mode Driver پشتیبانی می‌شود. DPDK برای خانواده Intel XLV۱۰ قابلیت‌هایی مانند Multiple RX/TX Queues، Receive Side Scaling، RSS، Flow Director، Checksum Offload، VLAN Offload، TSO، Jumbo Frame و SR-IOV را مستند کرده است. بنابراین بخشی از پردازش پایه Packet همچنان می‌تواند در NIC انجام شود.

برای مثال RSS می‌تواند Flowهای مختلف را بین چند RX Queue توزیع کند و هر Queue توسط Core متفاوتی پردازش شود:

PT NGFW – Packet Processing Architecture

From Network to Security – High Performance on Standard x86 Hardware

Using DPDK and multi-queue NICs (Intel XL710), PT NGFW processes packets in user space, distributes flows across CPU cores, and performs full security inspection with high efficiency.



این قابلیت برای یک NGFW نرم‌افزار-محور بسیار مهم است، زیرا اجازه می‌دهد تعداد زیادی Flow بین Coreهای فیزیکی پردازنده توزیع شوند و Bottleneck ناشی از یک Thread یا یک Queue کاهش پیدا کند.



Flow Director نیز در سطح NIC امکان هدایت هدفمند Flow ها به Queue های مختلف را فراهم می کند. Checksum Offload و TSO نیز برخی عملیات پایه Packet را از CPU خارج می کنند.

با این حال باید یک نکته مهم در ارزیابی PT رعایت شود: پشتیبانی DPDK و Intel XLV۱۰ از این قابلیت ها الزاماً به معنای فعال بودن تمام آنها در تمام نسخه های PT NGFW نیست. برای مشخص شدن اینکه PT دقیقاً از کدام Offload ها استفاده می کند، تأیید مستقیم تیم فنی سازنده ضروری است که بر اساس جدول نسخه های مورد استفاده و سخت افزارهای آن و همچنین قابلیت های مد نظر در نسخه تعیین می گردد :

PT NGFW 1005	PT NGFW 1010	PT NGFW 1020	PT NGFW 1050	PT NGFW 2010	PT NGFW 2020	PT NGFW 2050	PT NGFW 3010	PT NGFW 3040
Mode: L4 filtering + application-layer inspection								
1 Gbps	4 Gbps	8 Gbps	10 Gbps	80 Gbps	100 Gbps	140 Gbps	190 Gbps	300 Gbps
Mode: IPS + application-layer inspection								
120 Mbps	600 Mbps	1.4 Gbps	4.5 Gbps	12 Gbps	23 Gbps	32 Gbps	40 Gbps	60 Gbps
Mode: IPS + AV + URL filtering + NAT								
100 Mbps	480 Mbps	1 Gbps	3.3 Gbps	10 Gbps	18 Gbps	25 Gbps	32 Gbps	47 Gbps
1.3 Mpps	1.3 Mpps	2 Mpps	3.2 Mpps	7 Mpps	8.5 Mpps	12 Mpps	15 Mpps	20 Mpps
Full TLS/SSL inspection of all encrypted traffic, with all FW modules enabled								
85 Mbps	100 Mbps	800 Mbps	1 Gbps	8 Gbps	15 Gbps	15 Gbps	20 Gbps	25 Gbps

به عبارت دیگر، وجود Intel XLV۱۰ ظرفیت Hardware Offload را فراهم می کند، اما Policy نرم افزار PT مشخص می کند کدام قابلیت ها واقعاً در Data Plane مورد استفاده قرار می گیرند.



تفاوت NIC Offload با Security Offload

این تفاوت از مهم ترین نکات در مقایسه PT با محصولی مانند FortiGate است.

NIC Offload معمولاً فعالیت هایی مانند RSS، Checksum، Segmentation، Queue Distribution یا Flow Steering را تسريع می کند. اما یک Network Security ASIC ممکن است وظایف گسترده تری مانند Stateful Flow Processing، IPsec، Encryption، Pattern Matching یا برخی مراحل Content Inspection را برعهده بگیرد. بنابراین دو سیستم ممکن است هر دو از عبارت Hardware Acceleration استفاده کنند، اما سطح شتاب دهی آنها کاملاً متفاوت باشد.

جدول زیر تفاوت مفهومی این دو رویکرد را نشان می دهد:

ویژگی معماری	NGFW مبتنی بر ASIC/NPU	PT NGFW مبتنی بر x86/DPDK
اصلی Data Plane	Hardware + Software	Software/User Space
CPU	پردازنده تخصصی + CPU	عنصر اصلی پردازش
Kernel Bypass	بسته به Vendor	بخش مهم معماری
DPDK	الزاماً نیاز نیست	در معماری PT استفاده می شود
NIC Offload	قابل استفاده	قابل استفاده
Security ASIC	در بسیاری از محصولات وجود دارد	طبق PT مورد نیاز نیست
توسعه قابلیت جدید	ممکن است به قابلیت ASIC نیز وابسته باشد	عمدتاً نرم افزاری
مقیاس Performance	ASIC/NPU ظرفیت + CPU	بسیار مهم NIC و Memory، Clock، Core
DPI/IPS	ترکیبی از CPU و acceleration بسته به Vendor	عمدتاً Software-optimized
ارتقای Hardware	معمولاً نیازمند نسل جدید Appliance/ASIC	امکان استفاده از نسل های قوی تر x86

- Fortinet به طور رسمی اعلام می کند که NP ها وظیفه Offload ترافیک حجیم شبکه را برعهده دارند و CP ها قابلیت هایی مانند Encryption، Decryption، Virus Scanning و Attack Detection را شتاب می دهند.
- PT در مقابل اعلام می کند که Performance محصول روی پردازنده های x86 General-Purpose و بدون Dedicated ASIC یا FPGA حاصل می شود.

بنابراین مقایسه مستقیم فقط بر اساس تعداد Core یا فرکانس CPU میان یک FortiGate و یک PT Appliance می تواند گمراه کننده باشد.



اثر معماری PT بر انتخاب سخت افزار

این معماری اهمیت انتخاب CPU، Memory Architecture، PCIe و NIC را در PT بسیار بیشتر می کند. برای نمونه، یکی از پیکربندی های مورد بررسی برای اجرای PT NGFW روی تجهیزات رایج در بازار ایران شامل NSA۵۱۸۱، پردازنده Xeon E-۲۲۷۶، مقدار ۶۴GB RAM، ماژول F۱۴۰NX و C۱۸۰NI است.

NSA۵۱۸۱ چهار Slot برای LAN Module در اختیار قرار می دهد و از پردازنده های Xeon/Core خانواده Coffee Lake و DDR۴-۲۶۶۶ پشتیبانی می کند. NEXCOM همچنین استفاده از F۱۴۰NX مبتنی بر Intel XLV۱۰ و C۱۸۰NI مبتنی بر Intel I ۳۵۰ را روی این پلتفرم مستند کرده است.

F۱۴۰NX دارای چهار Interface ده گیگابیتی SFP+، کنترلر Intel XL-BM۷۱۰-۱ و رابط PCIe ۳.۰x۸ است.

این مشخصات از دید DPDK مطلوب هستند، زیرا Intel XLV۱۰ دارای پشتیبانی مناسب برای Multi-Queue و RSS است. در این معماری احتمالاً محدودیت اصلی سیستم قبل از ظرفیت فیزیکی NIC در CPU ظاهر می شود. چهار Interface ده گیگابیتی به معنای توان واقعی ۴۰Gbps در حالت IPS، DPI و TLS Inspection نیست.

پردازنده Xeon E-۲۲۷۶G دارای شش Core فیزیکی، دوازده Thread، فرکانس پایه ۳.۸GHz، Turbo تا ۴.۹GHz، ۲AVX و AES-NI است. فرکانس بالا برای Packet Processing مزیت محسوب می شود، اما تعداد شش Core فیزیکی برای بارهای سنگین Full Security می تواند عامل محدودکننده باشد. Hyper-Threading نیز نباید معادل دو برابر شدن تعداد Core های واقعی در محاسبات Capacity تلقی شود.

برای PT NGFW، افزایش تعداد Core، Memory Bandwidth، Cache، تعداد Memory Channel ها و نحوه اتصال NIC ها به PCIe/NUMA می تواند تأثیر مستقیم تری نسبت به تجهیزاتی داشته باشد که بخش بزرگی از Data Plane آنها توسط ASIC پردازش می شود.



مقایسه Performance اسمی و واقعی

Positive Technologies در حال حاضر برای خانواده PT NGFW ارقام متفاوتی را بر اساس نوع پردازش اعلام می کند.

برای مثال در وبسایت رسمی، PT NGFW ۲۰۲۰ دارای ظرفیت ۱۰۰G در ۴L Application Control +، حدود ۲۳G در IPS + Application Control و حدود ۱۸G در حالت IPS + Antivirus + URL Filtering معرفی شده است. مدل های بالاتر مانند PT NGFW ۳۰۵۰ تا ۴۰۰Gbps در ۴L Application Control + و ۸۶G در حالت ترکیبی IPS + AV + URL Filtering اعلام شده اند. PT همچنین اعلام می کند Performance محصولات را بر اساس روش های Benchmark مرتبط با RFC۹۴۱۱ ارزیابی می کند.

این اختلاف قابل توجه بین Throughput پایه و Full Security نکته مهمی را نشان می دهد: حتی در معماری بسیار بهینه X۸۶، فعال شدن موتورهای امنیتی عمیق بار پردازشی قابل توجهی ایجاد می کند. این موضوع مختص PT نیست و در تمام NGFW ها بومی و محصولات مشابه ایرانی به شدت مشاهده می شود، اما در معماری نرم افزار محور اهمیت Sizing صحیح CPU بیشتر می شود.

بنابراین هنگام طراحی یک Appliance سفارشی، معیار مناسب نباید فقط مجموع ظرفیت Port ها باشد. تجهیز دارای چهار پورت ۱۰GbE الزاماً یک NGFW با Full Security Throughput برابر ۴۰Gbps نیست.



مزایا و محدودیت‌های معماری x86/DPDK

مهم‌ترین مزیت معماری PT انعطاف‌پذیری آن است. قابلیت‌های جدید می‌توانند بیشتر در سطح Software توسعه پیدا کنند و Product Roadmap کمتر به طراحی نسل جدید ASIC وابسته باشد. همچنین استفاده از Processor و NIC استاندارد Enterprise می‌تواند امکان ایجاد مدل‌های متنوع Appliance و حتی نسخه Virtual را فراهم کند؛ PT NGFW نیز علاوه بر Hardware Appliance به شکل Virtual قابل استقرار است.

مزیت دیگر، استفاده سریع‌تر از پیشرفت نسل‌های جدید CPU است. افزایش تعداد Core، Cache، Memory Bandwidth و Instruction Set های جدید می‌تواند بدون طراحی یک Security ASIC جدید مستقیماً به Performance بیشتر منجر شود. در مقابل، این معماری نسبت به انتخاب Hardware حساس‌تر است. CPU ضعیف، تعداد Core ناکافی، NUMA Configuration نامناسب، Memory Bandwidth محدود یا NIC نامتناسب می‌تواند Performance را به شدت کاهش دهد.

در معماری ASIC محور، بخشی از این حساسیت توسط شتاب‌دهنده اختصاصی جذب می‌شود.

از طرف دیگر، نمی‌توان فرض کرد که DPDK به تنهایی معادل یک NPU است. DPDK مسیر رساندن Packet به CPU را بسیار کارآمد می‌کند، اما در نهایت بسیاری از عملیات DPI، IPS، Application Analysis و Inspection پیچیده همچنان باید جایی اجرا شوند و در معماری PT بخش عمده این توان از پردازنده‌های عمومی و الگوریتم‌های نرم‌افزاری تأمین می‌شود.



نتیجه گیری

PT NGFW نمونه‌ای از تغییر مهم در معماری نسل جدید تجهیزات امنیت شبکه است. در گذشته دستیابی به Throughput بسیار بالا تقریباً همواره با استفاده گسترده از ASIC، FPGA و پردازنده‌های امنیتی اختصاصی همراه بود. افزایش توان پردازنده‌های چند هسته‌ای X۸۶، توسعه DPDK، NICهای Multi-Queue و الگوریتم‌های بهینه User-Space Packet Processing باعث شده است رویکرد دیگری نیز امکان پذیر شود.

PT NGFW بر اساس اطلاعات رسمی موجود، از پردازنده‌های X۸۶، پردازش Packet در User Space، TCP/IP Stack، بهینه شده، فناوری DPDK و موتورهای اختصاصی DPI و IPS استفاده می‌کند و Positive Technologies اعلام می‌کند که برای دستیابی به Performance محصول نیازی به Dedicated ASIC یا FPGA ندارد.

این به معنی نبود کامل Hardware Acceleration نیست. NICهایی مانند Intel XLV۱۰ خود قابلیت‌هایی نظیر RSS، Multi-Queue، Flow Director، Checksum Offload و TSO دارند و DPDK امکان بهره‌برداری از چنین امکاناتی را فراهم می‌کند. اما این سطح از Offload باید از Security Processing Offload موجود در محصولاتی که دارای CP، NP یا ASIC اختصاصی هستند تفکیک شود.

از دید طراحی Appliance، نتیجه بسیار مهم است: در PT NGFW، انتخاب CPU و معماری Platform بخشی اساسی از طراحی امنیتی محسوب می‌شود. تعداد Coreهای فیزیکی، فرکانس، Cache، Memory Bandwidth، PCIe Topology، NUMA و نوع NIC همگی می‌توانند مستقیماً روی Throughput واقعی اثر بگذارند.

در مورد تجهیزات سخت افزاری، استفاده از کارت‌هایی مانند F۱۴۰NX مبتنی بر Intel XLV۱۰ از نظر DPDK و High-Speed Packet I/O انتخاب مناسبی است. اما در یک سیستم مانند ۵۱۸۱ با Xeon E-۲۲۷۱G شش هسته‌ای، در سناریوهای سنگین IPS، DPI و TLS Inspection احتمال ایجاد Bottleneck در CPU بسیار بیشتر از ظرفیت فیزیکی پورت‌های شبکه است. برای رسیدن به کلاس‌های Performance بالاتر PT NGFW، حرکت به سمت پلتفرم‌های Xeon Scalable با Core Count و Memory Bandwidth بیشتر منطقی‌تر خواهد بود.

در نهایت، مقایسه PT NGFW با FortiGate یا سایر NGFWهای Hardware-Accelerated نباید صرفاً بر اساس CPU، RAM یا تعداد پورت انجام شود. معیار صحیح، مقایسه End-to-End Performance در شرایط یکسان شامل Application Control، IPS، Antivirus، URL Filtering، TLS Inspection، تعداد Concurrent Session، Connection Rate، Packet Size و Logging است.

شماره : ۱۴۰۵۰۶۳۰۰۱

تاریخ : ۱۴۰۵/۰۶/۳۰

پیوست :

برنام‌خدا



شرکت فناوری ارتباطات

آشیانه امن

شماره ثبت : ۲۴۰۶۳۲

به همین دلیل، مهم‌ترین موضوعی که باید مستقیماً از تیم فنی Positive Technologies شفاف شود این است که در PT به NGFW دقیقاً کدام قابلیت‌های NIC Hardware Offload فعال هستند، نحوه تخصیص CPU Core ها در Data Plane چگونه است، آیا مکانیزمی مشابه Fast Path برای Established Session ها وجود دارد و کدام عملیات امنیتی در تمام شرایط همچنان توسط X86 CPU پردازش می‌شوند. پاسخ به این موارد امکان مقایسه دقیق و مهندسی‌شده PT NGFW با معماری‌های ASIC/NPU محور و همچنین Sizing صحیح پلتفرم‌های سخت افزاری را فراهم خواهد کرد.