

معرفی سامانه CGNAT شرکت ایمن پردیس

فهرست

۲ معرفی شرکت ایمن پردیس
۵ معرفی راهکار ipCGN
۱۱ معرفی سیستم عامل NetOS



ایمن پردیس

معرفی شرکت ایمن پردیس

شرکت «فناوری ارتباطات ایمن پردیس» توسط گروهی از متخصصین حوزه امنیت اطلاعات، شبکه و سیستم‌های مبتنی بر یونیکس فعالیت خود را با هدف ارایه خدمات تخصصی در زمینه پژوهش، مشاوره، طراحی و پیاده‌سازی خدمات مدیریت شده امنیت اطلاعات و توسعه سیستم‌های پربازده مبتنی بر شبکه آغاز نمود. این شرکت در حال حاضر مشغول به ارایه خدمات و تولید محصولات مورد نیاز شبکه‌های NGN به سازمان‌ها و شرکت‌های فعال در این حوزه‌ها می‌باشد.

رسالت شرکت، توسعه دانش بومی و انتقال دانش و تکنولوژی در حوزه‌های امنیت اطلاعات و زیرساخت‌های حساس، رفع نیاز کشور به متخصصین خارجی در حوزه امنیت از طریق تولید محصولات داخلی بوده و مأموریت‌های زیربرای شرکت در نظر گرفته شده است:

۱. انجام فعالیت‌های تخصصی در حوزه امنیت اطلاعات و زیرساخت‌های امن

۲. پژوهش و تولید محصولات مرتبط با حوزه تخصصی شرکت

۳. انتقال دانش تخصصی و نهادینه سازی دانش در سازمان‌ها

با توجه به رسالت شرکت، خدمات ارایه شده توسط این مجموعه دارای مزایای زیر در مقایسه با نمونه‌های خارجی می‌باشد:

- پشتیبانی تخصصی در محل به صورت ۲۴ ساعته در سه سطح مختلف
- همکاری و ارایه مشاوره به مشتریان در زمینه یکپارچه‌سازی محصولات شرکت با راهکارهای موجود
- امکان توسعه و اعمال تغییرات در محصولات مطابق نیازمندی مشتریان
- ارایه مزایای اقتصادی و کیفی رقابتی با محصولات خارجی

از خدمات شرکت ایمن پردیس می‌توان به موارد زیر اشاره نمود:

- طراح و مجری موفق‌ترین پیام رسان مبتنی بر موبایل ایرانی (بیسفن) با بیش از دو میلیون کاربر. این پیام رسان با دیدگاه رفع نگرانی‌های امنیتی و حریم خصوصی در کشور طراحی و پیاده‌سازی شد. طی مدت انجام این پروژه، بیش از بیست نفر متخصص داخلی در حوزه پیاده سازی نرم‌افزارهای مبتنی بر تلفن همراه آموختند.
- طراح و مجری سیستم NAT ipCGN با نام تجاری Carrier Grade NAT در سال ۱۳۹۲ به عنوان اولین نمونه در کشور، مورد استفاده در اپراتورهای اینترنت و موبایل کشور - این سامانه علاوه بر رفع مشکل کمبود آدرس‌های

IPv4، راهکاری جهت ثبت داده‌های ترافیک اینترنت و هویت کاربران جهت ارایه خدمات به قوه قضاییه و پلیس ارایه نموده است. همچنین با پیاده‌سازی استاندارد NAT64 در این محصول، بستر مناسب برای مهاجرت اپراتورها به IPv6 فراهم گردیده است.

- توسعه سیستم عامل NetOS مبتنی بر یونیکس به عنوان پایه محصولات و Appliances های تولید شده - این سیستم عامل علاوه بر ملاحظات امنیتی، مقیاس پذیری افقی و عمودی با ضریب بالا را فراهم می‌نماید. از مهمترین قابلیت‌های این سیستم عامل امکان پردازش ترافیک در مقیاس چند ده گیگابیت در ثانیه است که آن را برای پیاده سازی در شبکه‌های Carrier مناسب می‌سازد.
- توسعه سامانه ipDNS به عنوان DNS Resolver با پشتیبانی کامل از DNSSEC و بازدهی بالا (۴۰۰ هزار درخواست در ثانیه) برای اپراتورهای اینترنت. همچنین با توجه به پیاده سازی استاندارد DNS64 در این محصول و امکان یکپارچگی آن با ipCGN، امکان مهاجرت ساده‌تر به پروتکل IPv6 در شبکه اپراتورها فراهم شده است.
- ارایه خدمات تخصصی پیاده سازی، انتقال دانش و مهاجرت به پروتکل IPv6
- توسعه نرم افزارهای خاص منظوره در زمینه NSM و امنیت شبکه در سطح Enterprise و Carrier
- طراحی و پیاده سازی حسگرها و پویشگرهای شبکه با ظرفیت‌های 1G و 10G
- طراحی و پیاده سازی حسگرها و کیفی شبکه و سیستم‌های جمع آوری و تقارن داده‌های حسگرها
- طراحی و پیاده سازی مدیریت شبکه در سطح Carrier Grade به صورت توزیع شده و با مدیریت یکپارچه مرکزی
- ارایه خدمات مهاجرت به سیستم‌های باز متن و بهینه سازی سیستم‌های موجود مبتنی بر سیستم عامل‌های Solaris و HP-UX و انواع مختلف سیستم‌های UNIX در سطوح Enterprise و Carrier
- ارایه خدمات تخصصی و راهکارهای ذخیره سازی اطلاعات با فایل سیستم ZFS
- طراحی و پیاده سازی سیستم‌های خاص منظوره (Embedded) با قابلیت پردازش بالا در سطح Grade
- طراحی و پیاده سازی سیستم‌های (ipOSINT) جمع آوری اطلاعات، مرتبط سازی و داده کاوی اطلاعات شبکه در سطح SOC و CSIRT/CERT و IP, Port, AS Number, Domain Name
- طراحی و پیاده سازی سیستم ipSpectator (Passive Network Forensics) جهت انجام (پردازش داده‌های ضبط شده شبکه و استخراج داده‌های کارآگاهی) - مورد استفاده در مراکز CERT/CSIRT و مراجع قضایی
- ارایه راهکارهای Content Distribution و Load Balancing

• ارایه راهکارهای Cloud Computing با استفاده از تکنولوژی های BSD BHyve و VMWare، Oracle Solaris و

- طراحی و پیاده سازی مرکز عملیات امنیت شبکه (SOC) و مرکز پاسخگویی به رخدادهای امنیتی رایانه ای (CSIRT)

مشتریان

شرکت ایمن پردیس از بدو تاسیس خدمات تخصصی خود را به چندین سازمان و شرکت فعال در زمینه های مختلف شامل سازمان های دولتی، شرکت های خصوصی و ارایه دهندهای خدمات اینترنت ارایه نموده است.

اسامی تعدادی از مشتریان شرکت به شرح زیر است:

- سازمان تنظیم مقررات و ارتباطات رادیویی
- ارتباطات کوهکشان
- بزرگ نت آریا
- شرکت گیلاس کامپیوتر
- شرکت تالیا
- شرکت زعیم
- شرکت نوین مهر
- توسعه فناوری اطلاعات خوارزمی
- شرکت تراشه سبز تهران (بیستاک)
- U2Telecom
- گلوبال پتروتک کیش
- شرکت تجارت الکترونیک صبا (آپارات و کلوپ)

معرفی راهکار ipCGN

مقدمه

رشد بی‌سابقه تلفن‌های همراه هوشمند و افزایش تعداد کاربران اینترنت در سالهای اخیر، ارایه دهنده‌گان خدمات اینترنت را مجبور به سرمایه‌گذاری قابل توجهی در بخش زیرساخت، به منظور ارایه و پشتیبانی از ترافیک رو به رشد و همچنین ارایه سرویسهای نوین نموده است. این موضوع سبب استفاده بسیار زیاد از IPv4 شده و در نتیجه معضل کمبود IPv4 از مشکلات و چالشهای حال حاضر می‌باشد.

در سوم ماه فوریه سال ۲۰۱۱، سازمان IANA آخرين پنج آدرس /8 را به ثبت کنندگان محلی اینترنت Regional Internet Registries (RIR) اختصاص داد. از ماه آوریل سال ۲۰۱۴ طرح تخصیص IP سازمان ARIN وارد فاز نهایی خود گردید و این سازمان قادر به پاسخگویی به درخواستهای جدید نمی‌باشد.

از طرف دیگر محتوای دیجیتال و ترافیک اینترنت در حال رشد تصاعدی می‌باشد و تمایل روزافزون به استفاده از اینترنت در تمامی بخشها و ایجاد شدن مباحثی همچون Internet of Things سبب گردیده تعداد تجهیزات متصل به اینترنت تا پایان این دهه میلادی به ۲۰ میلیارد دستگاه برسد و این خود به معنای تقاضای بیشتر برای آدرس‌های IP است.

به منظور پیشبرد وضعیت کنونی و آماده شدن برای توسعه طولانی مدت، مهاجرت به IPv6 به امری اجتناب ناپذیر برای ارایه دهنده‌گان خدمات بدل گشته است.

از آنجاییکه پروتکل IPv6 به طوری ذاتی با IPv4 سازگار نیست، سرویس دهنده‌گان مجبور به ارایه طرحی برای پیاده سازی توامًا IPv4 و IPv6 در کنار هم به منظور ادامه فعالیت کنونی و همچنین آماده سازی برای توسعه در آینده می‌باشد.

شرکت ایمن پردیس با ارایه راهکار جامع مهاجرت از IPv4 به IPv6، این امکان را برای ارایه دهنده‌گان خدمات به وجود آورده است تا با تکیه بر زیرساخت کنونی مبتنی بر IPv4 خود، زمان بیشتری به منظور آمادگی انتقال به زیرساخت جدید IPv6 داشته باشد. این راهکار علاوه بر رفع مشکل کمبود آدرس‌های IPv4 با استفاده از NAT44، مسیر مهاجرت به پروتکل IPv6 را از طریق NAT64 امکان‌پذیر می‌سازد.

لازم به ذکر است به جهت حفظ زیرساخت‌های موجود و کاهش هزینه‌های سربار اپراتورها، این سیستم به گونه‌ای طراحی شده است که در طی پروسه Integration نیاز به اعمال تغییر در زیرساخت‌های شبکه اپراتور و همچنین نرم افزارهای موجود (مانند نرم افزار Billing) نباشد.

چالشهای سرویس دهنده‌گان

سازمان IANA مسئولیت هماهنگی جهانی آدرس دهی و پروتکلهای اینترنتی را بر عهده دارد. نقش این سازمان اختصاص آدرس‌های استفاده نشده به ثبت کنندگان محلی اینترنت (RIR) با توجه به نیازشان می‌باشد. در حال حاضر آدرس‌های موجود در IANA رو به کاهش است و ثبت کنندگان محلی اینترنت نیز به سرعت IP‌های خود را مصرف می‌کنند.

افزایش سریع تعداد تجهیزات متصل به اینترنت موجب کاهش فضای آدرس دهی IPv4 گردیده است و در عین حال

ارایه دهنده‌گان خدمات با تقاضاهای زیادی جهت اتصال به اینترنت مواجه هستند. با اینکه مهاجرت به IPv6 به خدمات دهنده‌گان در جهت توسعه زیرساخت کمک می‌نماید اما مهاجرت ناگهانی و یکباره نیز راه حل منطقی نبوده و در عمل امکان‌پذیر نمی‌باشد. به علاوه، با توجه به ناسازگاری پروتکل‌های IPv6 و IPv4، فرایند ترجمه آدرس نیز باعث ایجاد اختلال در بعضی پروتکل‌ها و برنامه‌ها می‌شود.

پایداری ارتباط، از جمله اولویتهای هر ارایه دهنده خدمات به حساب می‌آید و اپراتورها به دنبال اطمینان از صحت کارکرد برنامه‌های اجرا شده توسط کاربران خود می‌باشند. سرویس دهنده‌گان جهت ادامه فعالیت کنونی خود و آمادگی برای ایجاد توسعه و پاییندی به توافقنامه سطح خدمات (SLA)، با چالشهای زیر روبرو هستند:

- حفظ زیرساخت‌های موجود:** سرویس دهنده‌گان دارای زیرساخت‌های گستردۀ مبتنی بر IPv4 می‌باشند و تمایل دارند ضمن حفظ این زیرساخت موجود، بدون اعمال تغییرات پرهزینه و ایجاد اختلال در سرویس دهی، برای طرحهای توسعه‌ای آینده آماده شوند.

- آمادگی برای رشد آنی تعداد کاربران:** ارایه دهنده‌گان خدمات همچنین به دنبال راههای مشخصی جهت مواجهه با تقاضاهای رو به رشد متقارضیان اتصال به اینترنت می‌باشند. به علاوه مادامی که آنها جهت انتقال به بستر IPv6 آماده می‌شوند، تمایل دارند از انتقال بدون مشکل و بدون اختلال و نیز برطرف کردن مشکلات سازگاری با بستر IPv4 کنونی نیز مطمئن باشند.

- پاییندی به توافقنامه سطح خدمات (SLA):** فعالیت اقتصادی ارایه دهنده‌گان خدمات به میزان زیادی به پایداری و برقراری سرویس آنها بستگی دارد. قطعی سرویس برای خدمات دهنده‌گان قابل قبول نیست، چرا که موجب ضرر مالی، نارضایتی کاربران و کاهش اعتبار حرفه‌ای آنها می‌شود.

راه حل، ایجاد یک برنامه جایگزین با درنظر گرفتن فضای کلی IPv6 و استفاده از راهکارهای مهاجرت می‌باشد. با این وجود سیستم‌های مبتنی بر IPv4 تا سالها وجود خواهند داشت و ضروری است که زیرساخت‌های IPv4 و IPv6 در کنار یکدیگر وجود داشته باشند.

راهکارهای گوناگونی جهت توسعه شبکه‌های IPv4 و مهاجرت مرحله به مرحله به IPv6 وجود دارند. معروف‌ترین و معمول‌ترین این راهکارها شامل موارد زیر هستند:

تفصیل	راهکار
به منظور صرفه جویی IPv4 در مقیاس بالا و با استفاده از تکنولوژیهای NAT44/NAT444	CGNAT یا LSN
ایجاد دسترسی به IPv6 از طریق شبکه IPv4	DS-Lite (Dual-Stack Lite)
پیاده‌سازی IPv6 در یک شبکه مبتنی بر IPv4	6rd (IPv6 Rapid Deployment)

توضیح	راهکار
ایجاد ارتباط کاربران IPv6 به اینترنت مبتنی بر IPv4	DNS64 + NAT64

راهکار ipCGN

راهکار CGN ارایه شده توسط شرکت ایمن پردیس (ipCGN)، با انجام ترجمه آدرس و پورت (NAT/PAT) با راندمان بالا این امکان را برای ارایه دهندهای خدمات به وجود آورده است تا علاوه بر استفاده از شبکه IPv4، به طور همزمان آمادگی لازم مهاجرت به IPv6 را کسب نمایند. ipCGN بر پایه سیستم عامل NetOS طراحی شده که ویژگیهایی همچون راندمان بالا، توسعه پذیری، صرفه جویی در IPv4، مهاجرت به IPv6 و امنیت را فراهم می‌آورد. در این راهکار، نیازمندی‌های امنیتی و قانونی اپراتورها به منظور پاسخگویی به مراجع قضایی نیز به طور کامل در نظر گرفته شده است.

افزایش عمر زیرساخت‌های IPv4

محصول شرکت ایمن پردیس (ipCGN) مطابق با استانداردهای موجود در زمینه CGNAT ساخته شده است. CGNAT با استفاده از ترجمه آدرس و پورت در مقیاس بزرگ علاوه بر پایان دادن به مصرف بیش از حد IPv4، به افزایش عمر سرویس‌دهی شبکه‌های مبتنی بر IPv4 نیز کمک می‌کند.

اصلًاً تعداد آدرسهای Private در شبکه سرویس‌دهندهای بسیار زیاد بوده و انجام ترجمه آدرس، از نظر امکانات پردازشی، فرایندی بسیار پیچیده و پرهزینه می‌باشد. به همین منظور، ipCGN از ابتدا با هدف ارایه سرویس CGNAT با راندمان بالا و قابلیت توسعه پذیری، طراحی و ساخته شده است. به علاوه ipCGN از ویژگی نگهداری و پردازش Log پیشرفت‌هایی برخوردار است که ضمن نگهداری اطلاعات مربوط به فعالیت کاربران، پاسخگوی درخواست‌های مراجع قانونی مربوطه می‌باشد.

همانطورکه در تصویر ۱ نشان داده شده است، راهکار ipCGN، این امکان را برای ارایه دهندهای خدمات فراهم می‌آورد تا عمر زیرساخت‌های مبتنی بر IPv4 خود را افزایش داده و ضمن صرفه جویی در هزینه‌های مالی، فرصت کافی جهت اجرای برنامه مهاجرت به IPv6 را نیز پیدا کنند.

یکپارچگی با زیرساخت‌های موجود

ورود یک سامانه جدید به قلب شبکه اپراتورها امری حساس بوده و همواره با نگرانی‌های اپراتورها همراه است. یکپارچگی با توبیلوزی موجود و نیاز به حداقل تغییرات در طراحی فعلی شبکه، از اهداف شرکت ایمن پردیس در طراحی سیستم ipCGN بوده است. همچنین در صورت لزوم امکان اعمال تغییرات در محصول به منظور یکپارچگی آسانتر با شبکه اپراتور فراهم می‌باشد. برای مثال، امکان مسیریابی توسط پروتکل‌های BGP و OSPF درسیستم در نظر گرفته شده تا یکپارچگی سیستم با شبکه موجود با کمترین تغییرات در توبیلوزی شبکه اپراتور امکان‌پذیر گردد.

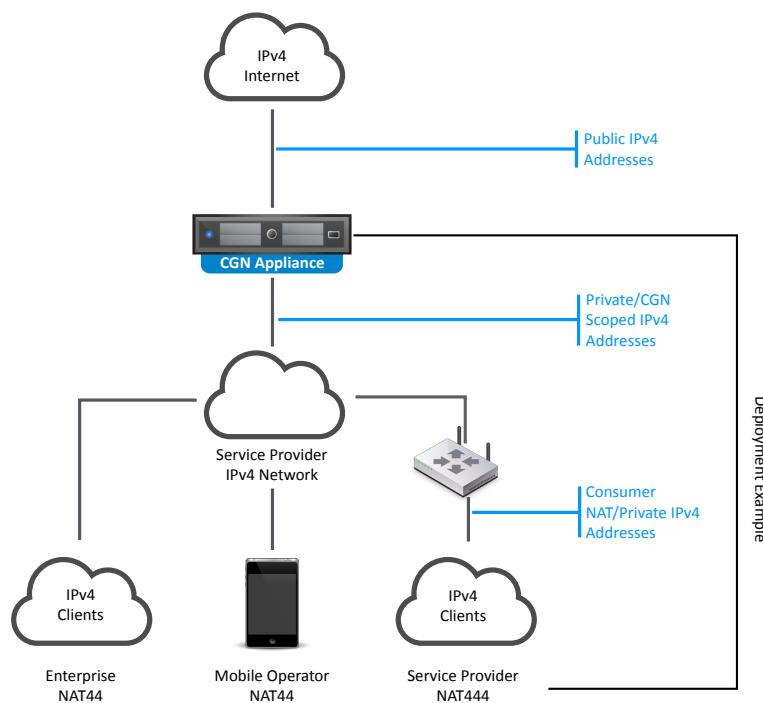
همچنین یکپارچگی با راهکارهای BSS موجود به منظور دریافت داده‌های هویتی کاربران (در صورت نیاز) به صورت Passive و با دریافت یک نسخه از پروتکل Radius موجود در شبکه امکان‌پذیر می‌باشد. بنابراین اپراتور نیازی به

تغییر راهکار Billing موجود یا استفاده از نرم افزارهای خاص را در این مورد نخواهد داشت.

ضریب اطمینان پروتکل های لایه Application

محصول CGN شرکت ایمن پردیس (ipCGN) با فراهم آوردن شرایط برقراری برنامه ها و پایداری ارتباط، این امکان را به وجود می آورد که سرویس ها در طول فرایند آدرس دهی، در دسترس بوده و بدون هیچ مشکلی به فعالیت خود ادامه دهند.

بسیاری از برنامه ها همچنان با تکیه بر اطلاعات لایه شبکه و اپلیکیشن (۳ تا ۷) فعالیت می کنند. برنامه هایی که اطلاعات مربوط به شبکه و سایر موارد را در Payload بسته های خود قرار می دهند با انجام فرایند NAT دچار وقفه می شوند. محصول ipCGN با فراهم آوردن قابلیت (ALG) Application Layer Gateway این امکان را فراهم کرده تا پروتکلهایی همچون ICMP، DNS، SIP، PPTP، RSTP، FTP و H.323 با انجام فرایند NAT نیز به کار خود ادامه دهند. به علاوه ویژگی های پیشرفته ای همچون Endpoint Independent Mapping (EIM) با قابل پیش بینی کردن رفتار NAT، باعث می شود کل فرایند تاثیری بر فعالیت اپراتور نداشته باشد.



تصویر ۱ - جایگزاري CGN در شبکه اپراتور

تنوع در روش های مهاجرت به IPv6

شبکه های سرویس دهنده کان از نظر انواع خدمات بسیار متنوع بوده و تکنولوژی های متفاوتی به طور همزمان در آنها پیاده سازی شده است. محصول ipCGN انتخاب گسترده ای از راهکارها را فراهم می آورد تا انتقال به IPv6 سادگی و سهولت انجام پذیرد. همچنین شرکت ایمن پردیس خود را موظف می داند همکاری های لازم در راستای

همفکری و ارایه راهکار به اپراتور به منظور اعمال حداقل تغییرات در شبکه موجود و یکپارچه سازی راهکار ipCGN در شبکه اپراتور ارایه نماید.

تکنولوژیهای IPv6 (6rd) این امکان را برای تجهیزات IPv6 فراهم می آورند تا از طریق یک شبکه مبتنی بر IPv4 به اینترنت متصل شوند.

تجهیزاتی که فقط با IPv6 کار می کنند احتیاج به راهی برای اتصال به اینترنت 6rd IPv4 دارند و راهکارهای NAT64/DNS64 این امکان را برای آنها فراهم می آورند. قابلیت ترجمه آدرس های IPv6 به IPv4 در نسل جدید ipCGN امکان مهاجرت قدم به قدم به پروتکل IPv6 را فراهم نموده است.

به علاوه، محصول ipCGN این اطمینان خاطر را برای مشتریان فراهم می سازد که آنها می توانند تکنولوژیهای مهاجرت را به طور همزمان پیاده سازی نمایند و در عین حال ipCGN نیز با همه آنها سازگار بوده و این امکان را برای ارایه دهنده ای خدمات فراهم می آورد تا به صورت مرحله به مرحله برای انتقال به IPv6 برنامه ریزی نمایند. به عنوان مثال ابتدا به منظور صرفه جویی در مصرف IPv4 از CGNAT استفاده نمایند و سپس اقدام به پیاده سازی NAT64/DNS64 نمایند تا کاربران IPv6 نیز بتوانند به اینترنت IPv4 متصل شوند.

با توجه به موارد گفته شده، محصول ایمن پردیس (ipCGN) ویژگیهای جامع و کاملی همچون CGNAT، ALG و تکنیکهای گوناگون مهاجرت به IPv6 را یکجا فراهم آورده است.



مزایای ipCGN

طراحی آدرس دهی شبکه و مهاجرت به IPv6 در هر سازمان و شبکه متفاوت است. سرویس دهنده ای کاری می باشند که بیشترین سازگاری و پشتیبانی را از ملزمومات استاندارد آدرس دهی و مهاجرت داشته باشند. شرکت ایمن پردیس با ارایه محصول ipCGN توانسته ویژگیهای پیشرفته ای را بطور یکجا ارایه داده است که سبب فراهم آمدن فواید گوناگونی شده است:

- **افزایش عمر زیرساختهای IPv4:** محصول ipCGN با فراهم آوردن امکان ترجمه آدرس و پورت با بازدهی بالا، این قابلیت را برای ارایه دهنده ای خدمات فراهم آورده است که مدت زمان بیشتری بتوانند از زیرساخت خود استفاده نمایند.

• ضریب بالای کارایی برنامه‌ها: محصول ipCGN برقراری برنامه‌ها و پایداری ارتباطات را فراهم می‌آورد. پشتیبانی ALG از پروتکلهای پرکاربرد موجود، باعث افزایش تداوم سرویس ارایه دهنده‌گان خدمات، ارایه SLA بهتر و افزایش رضایت کاربران می‌شود.

• ترجمه IPv6: محصول ipCGN از راهکارهای گوناگون مهاجرت به IPv6 پشتیبانی می‌کند و وجود همزمان این تکنولوژیها با همدیگر، امکان مهاجرت آسانتر را برای سرویس‌دهنده‌گان فراهم می‌آورد. سازگاری و هماهنگی بین CGNAT و تکنولوژیهای مهاجرت به IPv6، امکان انتقال مرحله به مرحله و همچنین وجود هردو نسخه IPv6 و IPv4 در شبکه را بدون احتیاج به تجهیزات مختلف می‌سازد.

معرفی سیستم عامل NetOS

تحولات تکنولوژی‌های Application Networking

با روی کار آمدن و فراگیر شدن روزافزون تکنولوژی‌های موبایل و رایانش ابری، دیتاسترها مدرن دائماً در حال تغییر شکل و ماهیت ناشی از نیازمندی‌های این تکنولوژی‌ها هستند. افزایش سریع ترافیک دیتاسترها به چالشی جدید برای سرویس دهنده‌گان و شبکه‌های بزرگ بدل شده است که آنها را به سمت توسعه و استفاده از زیرساخت‌های مقیاس پذیر با بازدهی بالا سوق می‌دهد. برای همسو شدن با این روند و به جهت بهبود بازدهی و امنیت معماری دیتاسترها، تکنولوژی‌های Application Networking نیز تغییرات زیادی را تجربه کرده‌اند.

برای مثال افزایش ناگهانی ترافیک شبکه‌ها که از اپلیکیشن‌های موبایل، کلان‌داده و ترافیک وب ناشی شده است، چالشهای جدی در مقیاس پذیری و بازدهی سیستم‌های Application Networking به وجود آورده است. به منظور انطباق با این رشد، سیستم‌های Application Networking مقیاس پذیر و با ضریب اطمینان بالا مورد نیاز است تا امکان ارایه خدمات با سطح کیفی مطلوب امکان‌پذیر گردد.

طی شش سال گذشته، معماری پردازنده‌های چند هسته‌ای که توسط سازندگان سیستم‌های Application Networking استفاده می‌شده است از پردازنده‌های تک هسته‌ای ۳۲ بیتی، به پردازنده‌های چند هسته‌ای ۶۴ بیتی تغییر پیدا کرده است. ولی با این وجود، معماری نرم‌افزارهای Application Networking به منظور سازگاری با این پردازنده‌های جدید بهینه سازی نشده و بعضی از سازندگان، در زمان کوتاه قادر به تطبیق محصولات خود برای مواجهه با افزایش ترافیک دیتاسترنبوده‌اند. به منظور رفع این مشکل، لازم است معماری سطح بالای این سیستم‌ها مورد بازنگری کلی قرار گرفته تا تغییرات مورد نیاز در کیفیت عملکرد سیستم‌های Application Networking انجام پذیرد. این معماری مجدد در پلتفرم NetOS شرکت «ایمن پردیس» انجام پذیرفته است.

دوران پردازنده‌های چند هسته‌ای

سیستم‌های سنتی شبکه (مانند سوئیچها و روترهای header) که فقط نیاز به پردازش بخش کوچکی از ترافیک شبکه را دارند، این عمل را با استفاده از پرداشگرهای ASIC و با بازدهی بالا انجام می‌دهند. طبیعی است که این سیستم‌ها قادر به ارائه و پیاده‌سازی پردازش‌های کاربردی تر و عمیق‌تر بروی ترافیک نمی‌باشند.

از سوی دیگر سیستم‌های Application Networking مانند ADC، با بررسی عمیق‌تر بسته‌ها و رفتار هوشمندانه تر نسبت به ترافیک، توانایی پیاده‌سازی پردازش‌های پیچیده روى ترافیک شبکه را دارند. به همین منظور، سیستم‌های Application Networking به حافظه و پرداشگرهای چند هسته‌ای منظوره وابسته هستند تا بتوانند هر گونه پردازش را بدون محدودیت‌های موجود در ASIC انجام دهند. صنعت ساخت پردازنده، نقش کلیدی را در چرخه توسعه Application Networking ایفا می‌کند. پیش از این، بازدهی پردازنده‌ها با افزایش سرعت clock آنها افزایش می‌یافتد. اما بالا بردن سرعت clock، از سوی دیگر منجر به افزایش مصرف انرژی می‌گردد. در سال ۲۰۰۵ به منظور رفع این مشکل، پردازنده‌های چند هسته‌ای با دو یا چند CPU برروی یک چیپ سیلیکونی، با هدف افزایش سرعت، کاهش مصرف، کاهش فضای کاهش هزینه تمام شده ارائه شدند. اما چندین پردازنده، الزاماً به معنی افزایش خطی راندمان پردازش نبوده و در حقیقت، افزایش بازدهی در یک سیستم چند هسته‌ای کاملاً به معماری

نرم افزار وابسته است.

در سطح سیستمی، دو برابر کردن تعداد پردازنده‌ها به طور خودکار باعث دو برابر شدن بازدهی نمی‌شود، بلکه تغییرات اساسی در طراحی نرم افزار لازم است و بدون این تغییرات، عملابخش عمدتی از توان این پردازنده‌های گرانقیمت چند هسته‌ای به هدر می‌رود.

در طراحی یک سیستم چند هسته‌ای، موضوع حائز اهمیت، عدم هماهنگی سرعت پردازنده و دیگر اجزای سیستم (مانند حافظه و I/O) است که معمولاً مهمترین دلیل بازدهی پایین سیستم می‌باشد. به علاوه سیستم‌های چند هسته‌ای بدون وجود معماری نرم افزاری که بتواند از پردازش موازی پشتیبانی کند، قادر به استفاده بهینه از پردازنده‌های چند هسته‌ای نمی‌باشند. خوب‌بختانه این محدودیتها قابل برطرف کردن بوده و با ترکیب درستی از معماری صحیح نرم افزار و طراحی بهینه در مدل دسترسی به حافظه می‌توان بازدهی این‌گونه سیستم‌ها را افزایش داد.

چالش‌های طراحی سیستم‌های چند هسته‌ای

پردازنده‌های چند هسته‌ای، در عین فراهم کردن امکانات و قابلیت‌های جدید به منظور افزایش بازدهی سیستم، چالش‌های جدیدی را نیز در زمینه طراحی سیستم‌های Application Networking به وجود آورده‌اند. در این راستا طراحان این سیستم‌ها با چالش‌های زیر در زمینه طراحی روبرخواهند شد:

۱. حافظه: با توجه به این موضوع که سرعت درگاه حافظه همیشه کمتر از سرعت پردازنده است، در صورت بهینه نبودن روش دسترسی به حافظه، این عدم هماهنگی باعث کاهش بازدهی سیستم می‌گردد. چراکه زمان پردازنده در حین دسترسی به حافظه به دلیل این ناهمانگی به هدر خواهد رفت. در یک سیستم چند هسته‌ای، دسترسی همزمان به بخشی از حافظه توسط چند پردازنده مختلف می‌تواند باعث ایجاد گلوبگاه در دسترسی به حافظه شده و تأثیر منفی روی بازدهی کلی سیستم داشته باشد.

۲. پردازش موازی: پردازش موازی می‌تواند با اجرا کردن instruction های متفاوت بر روی چند پردازنده، باعث افزایش راندمان شود. اما معماری‌های سنتی نرم افزار که به منظور استفاده از یک پردازنده به وجود آمده‌اند نمی‌توانند از این مزیت بهره‌مند شوند. معماری نرم افزار یک سیستم چند هسته‌ای باید به گونه‌ای طراحی شود تا بتواند به صورت بهینه، همزمانی (Concurrency) و دسترسی به منابع مشترک را مدیریت نماید. بدون همچین تغییری در معماری، مزایای پردازش موازی در پردازنده‌های چند هسته‌ای، قابل استفاده نخواهد بود.

۳. ارتباط بین پروسس‌ها (IPC²): پردازش موازی نیازمند ارتباط بین پردازنده‌ها به منظور تبادل اطلاعات مربوط به وضعیت سیستم می‌باشد تا تمامی هسته‌ها همزمان مشغول پردازش و انجام کارها شوند و همه کارها به شکل نامطلوبی روی یک هسته انجام نگیرد. در یک سیستم چند هسته‌ای با پردازش موازی، دشواری و هزینه تعویض و تخصیص حافظه در بین هسته‌ها، به صورت نمایی با افزایش تعداد هسته‌ها افزایش می‌یابد و باعث کاهش بازدهی کلی می‌شود.

طراحی سیستم‌های پردازش موازی به طور معمول به دو دسته³ SMP⁴ و MPP تقسیم‌بندی می‌شود. در سیستم‌های

2- Inter-Process Communications

3- Symmetric Multi-Processing

4- Massively Parallel Processing

مبنی بر SMP چندین پردازنده، سیستم عامل، حافظه و دیگر منابع O/I را بایکدیگر به اشتراک می‌گذارند. سیستم عامل، به منظور بهبود بازدهی، task‌ها را به طور مساوی بین پردازنده‌ها تقسیم می‌نماید. ولی به دلیل سربار نسبتاً زیاد ناشی از Locking منابع مورد استفاده مانند حافظه، این سیستم‌ها دارای محدودیت‌هایی در مقیاس پذیری می‌باشند.

از سوی دیگر، سیستمهای MPP منابع را در میان پردازنده‌ها به اشتراک نمی‌گذارند. هر پردازنده در MPP، مالک بخش مشخصی از منابع حافظه و سیستم عامل است و به هر پردازنده وظیفه متفاوت و مشخصی داده می‌شود تا بازدهی سیستم به شکل مناسبی افزایش پیدا کند. با وجود این، به دلیل عدم توزیع مناسب بار در سیستمهای MPP و هزینه بسیار بالای ارتباطات IPC، این سیستم‌ها مقیاس پذیری و افزایش بازدهی قابل قبولی را ارایه نمی‌دهند.

همچنانکه ضریب نفوذ و میزان به کار گیری پردازنده‌های چند هسته‌ای افزایش می‌یابد، طراحی‌های SMP و MPP به خاطر محدودیتهایی که بیان شد نمی‌توانند از قابلیتهای موجود در آن استفاده کنند. بدین منظور لازم است نرم‌افزارهای سیستمی که نیازمند به بازدهی بالا هستند، چالشهای مرتبط با معماری‌های چند هسته‌ای را بطرف نمایند. معماری‌های مورد استفاده در نرم‌افزار که به منظور استفاده از پردازنده‌های تک هسته‌ای به وجود آمدند، می‌باید با در نظر گرفتن پردازش موازی و به منظور کاهش هزینه‌های Locking و IPC بازطراحی شوند. همچنین به طور ویژه، معماری دسترسی به حافظه باید به طور جدی مورد بازبینی و طراحی مجدد قرار گیرد.

طراحی‌های سنتی سیستم معمولاً یکی از روش‌های زیر را به منظور به اشتراک گذاری حافظه، بین هسته‌های پردازنگر در یک سیستم چند هسته‌ای، به کار می‌گیرند:

۱. حافظه توزیع شده^۵: در این نوع از سیستم، هر پردازنده دارای فضای حافظه مختص به خود بوده و تبادل داده‌ها بین پردازنده‌ها به صورت داخلی صورت می‌گیرد. اینگونه طراحی به منظور تبادل داده‌ها نیاز به مکانیزم‌های IPC دارد. به همین منظور لازم است داده‌ها قبل از تبادل توسط IPC، آماده سازی شوند که این امردارای هزینه سربار بالایی می‌باشد. همچنین با توجه به اینکه هر پردازنده دارای حافظه مختص به خود است، لازم است بعضی از داده‌ها در قسمتهای مختلف کپی شوند که باعث بروز Data Duplication شده و در نتیجه منجر به استفاده ناکارآمد از حافظه و ایجاد محدودیت در مقیاس پذیری سیستم می‌شود.

۲. حافظه اشتراکی^۶: در این نوع از طراحی سیستم، تمامی پردازنده‌ها به یک حافظه مشترک دسترسی دارند و می‌توانند بدون در نظر گرفتن موقعیت فیزیکی خود، به آن حافظه دسترسی پیدا کنند. از آنجاییکه هر پردازنده بدون احتیاج به IPC می‌تواند به کل حافظه دسترسی داشته باشد، بنابراین بار اضافی روی بازدهی سیستم تحمیل نخواهد شد. با این وجود، در سیستمهای حافظه اشتراکی سنتی، به دلیل استفاده همزمان از بلوکهای حافظه توسط پردازنده‌ها، بین آنها تصادم به وجود می‌آید. در نتیجه منابع حافظه می‌بایستی در هر زمانی که هر کدام از پردازنده‌ها به آنها دسترسی پیدا می‌کند، برای بقیه پردازنده‌ها غیرقابل دسترس شوند. این مشکل که سیستمهای حافظه اشتراکی سنتی از آن رنج می‌برند، در سیستمهای چند هسته‌ای، چند برابر می‌شود.

بسیاری از سیستمهای Application Networking به منظور استفاده از معماری قدیمی، از روش اول استفاده نموده و نرم‌افزار را روی چند هسته اجرا می‌نمایند. اما این روش به دلیل هزینه سربار استفاده از IPC و استفاده نامناسب از حافظه، قابلیت توسعه پذیری لازم را ندارد.

5- Distributed Memory

6- Shared Memory

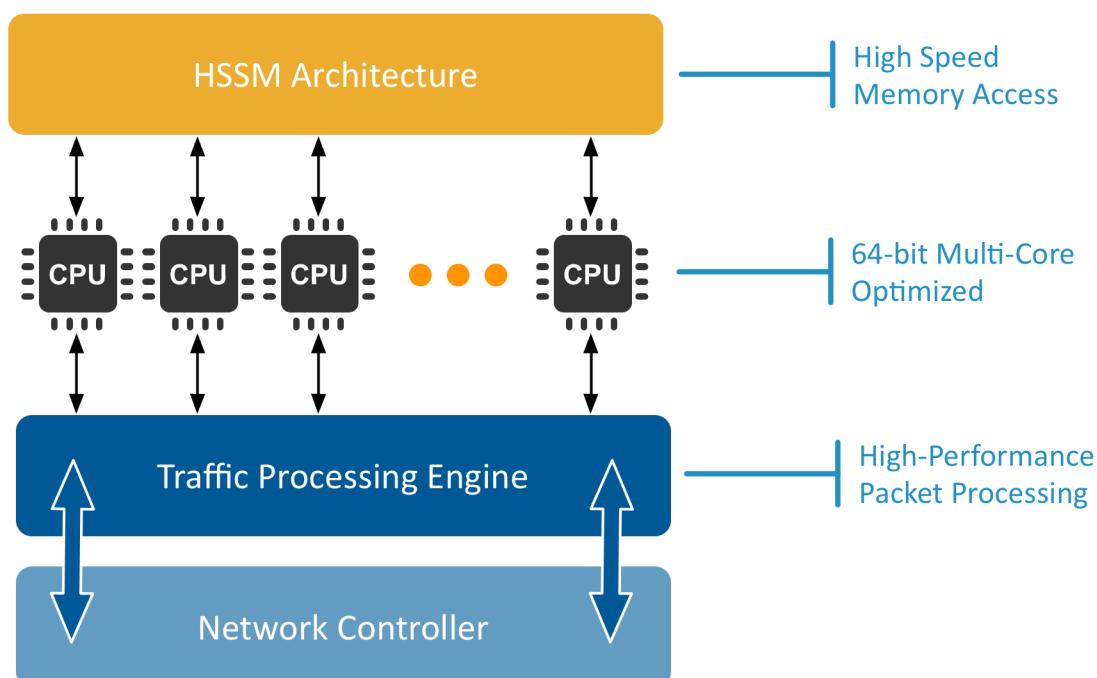
سیستمهای Application Networking مدرن می‌باید آمادگی لازم را به منظور پردازش ترافیک با سرعت‌های بالا را داشته باشند که این امر فقط با استفاده از نرم افزارهای بهینه شده برای سیستم‌های چند هسته‌ای که برای دسترسی سریع به حافظه بهینه‌سازی شده باشند امکان‌پذیر است.

معماری NetOS در HSSM

سیستم «NetOS»، از ابتدا به منظور مقیاس پذیری بر مبنای پردازنده‌های چند هسته‌ای بهینه‌سازی شده است. معماری NetOS، نقاط ضعف و محدودیت‌های هر دو مدل طراحی سنتی حافظه که پیشتر اشاره شد را برطرف ساخته و امکان استفاده از تکنولوژی پیشرفته در طراحی سیستم‌های پردازنده چند هسته‌ای را فراهم می‌آورد.

HSSM^۷ یا معماری حافظه اشتراکی با سرعت بالا، محدودیت‌های طراحی سنتی را زیان برده و بازدهی سیستم را به طور خطی و بر اساس معماری پردازنده چند هسته‌ای افزایش می‌دهد.

همچنین، معماری NetOS مسیر ترافیک عبوری را از مسیر ترافیک مدیریتی جدا می‌کند. برای ارسال ترافیک اصلی، چندین پردازنده اختصاصی به منظور پردازش موازی و با راندمان بالا در نظر گرفته شده‌اند. برای کاربری مدیریتی، NetOS یک یا چند پردازنده را متناسب نیاز، به این امر اختصاص می‌دهد. در نتیجه مدیر شبکه می‌تواند حتی در زمان اوج ترافیک، بدون نگرانی بازبینی‌های سیستمی خود را به منظور آگاهی از وضعیت و سلامت سیستم انجام دهد. جداسازی ترافیک اصلی و ترافیک مدیریتی بر روی هسته‌های جداگانه باعث افزایش انعطاف پذیری و پایداری کلی سیستم می‌شود.



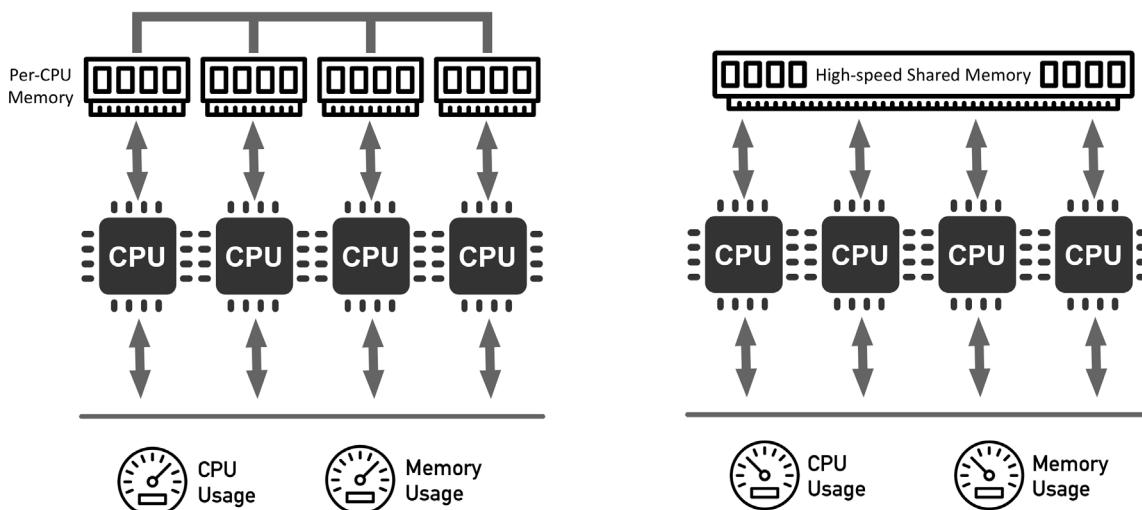
تصویر یک - معماری سطح بالای NetOS

معماری حافظه اشتراکی سرعت بالای NetOS، نیاز به ارتباطات IPC را از میان برده و دیگر نیازی به کپی کردن

7- High-Speed Shared Memory

محتوای حافظه نخواهد بود که این موضوع باعث می‌شود پردازنده‌ها با قدرت بیشتری، مهمترین وظایف خود را که پردازش ترافیک است انجام دهند. (مزایایی حافظه اشتراکی NetOS در تصویر دو نمایش داده شده است.)

معماری حافظه اشتراکی NetOS استفاده از پردازنده‌های چند هسته‌ای گرانقیمت و منابع حافظه را بهینه نموده و در مقایسه با سیستمهای رایج، اجزای سخت‌افزاری کمتری احتیاج دارد. اجزای کمتر، کارآیی عملیاتی و ضریب اطمینان کلی سیستم را افزایش می‌دهد.



تصویر دو - مقایسه معماری HSSM و Distributed Memory

مزایای NetOS

یکی از نتایج استفاده از معماری حافظه اشتراکی سرعت بالای NetOS، نیاز به سخت‌افزار (پردازنده و حافظه) کمتر است تا به توانایی و راندمان یکسان در حالت طراحی سنتی با معماری سنتی برسند.

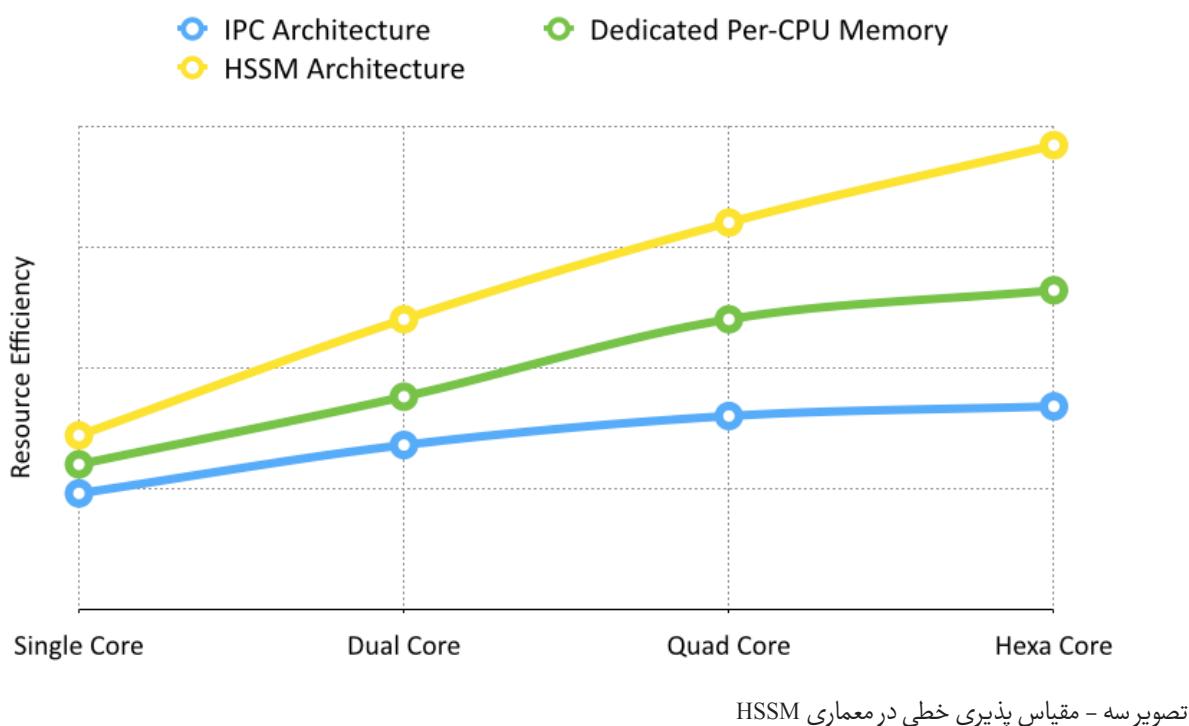
پلتفرم NetOS علاوه بر رشد بازدهی و مقیاس پذیری به صورت خطی، ویژگی‌های دیگری را نیز فراهم می‌آورد:

- **افزایش بازدهی نرم‌افزارها:** NetOS به مقدار قابل ملاحظه‌ای ضریب دسترسی برنامه‌ها را افزایش داده و همچنین باعث بهبود درسرعت پاسخگویی نرم‌افزارهای میانی می‌گردد که نتیجه آن، تجربه کاربری بهتر برای کاربرنهایی می‌باشد.
- **بازدهی قابل پیش‌بینی:** NetOS بازدهی را به طور خطی افزایش می‌دهد که باعث ارایه سطح کیفی مناسب حتی در صورت رشد ترافیک می‌گردد.
- **کاهش پیچیدگی:** بازدهی بالا و توسعه پذیری سیستم باعث عدم نیاز به اضافه نمودن سخت‌افزار پیچیده و شبکه را داشته و مدیریت سیستم را به سادگی امکان‌پذیر می‌نماید.
- **محافظت از سرمایه گذاری اپراتورها:** با افزایش ترافیک شبکه، سرویس دهنده‌گان می‌توانند خدمات خود

را توسعه دهنده و در عین حال با استفاده از زیربنای موجود، از سرمایه‌گذاری خود محافظت کنند.

- **کاهش هزینه‌های سرمایه‌گذاری:** راندمان و کارآیی بیشتر نسبت به تجهیزات مشابه، به سرویس دهنده‌گان این امکان را می‌دهد از هزینه اولیه خود بهره بیشتری ببرند.

- **کارآیی بیشتر دیتا سنتر و بازده اقتصادی بهتر:** کاهش میزان برق مصرفی، سرمایش و فضای موردنیاز کمتر باعث کاهش هزینه‌ها می‌شود.



جمع‌بندی

پلتفرم NetOS ابتدا برپایه اصول طراحی مدرن و حافظه اشتراکی سرعت بالا ساخته شده است تا بتواند پاسخگوی نیاز روزافزون Application Networking باشد. NetOS در سیستمهای پردازنده چند هسته‌ای، راندمان را به صورت خطی افزایش داده و در مقایسه با طراحی‌های سنتی مشابه، سخت افزار کمتری را برای رسیدن به نتایج مشابه نیاز دارد.

در نتیجه، سرویس دهنده‌گان می‌توانند سیستم کارآمدتری را در اختیار داشته باشند که می‌تواند بازدهی بیشتری را فراهم نماید و این به منزله فراهم کردن تجربه بهتر برای کاربران و بازده اقتصادی بهتر از نظر هزینه و بودجه می‌باشد.