Net-Gateway Appliance Series Microsoft Forefront Edge Security

Produced by Iron Networks

تهیه شده توسط: مهندس بهاره فاطمی جهرمی

معرفی Appliance های Microsoft Forefront Edge Security ارائه شده توسط Iron Networks

Iron Networks یکی از شرکتهای تابعه متعلق به Iron Systems است که در سال 1996 تأسیس شد. Iron Systems ارائه دهنده محصولاتی سفارشی، خلاقانه و مشتری محور در حوزه زیرساخت شبکه، مانند سرورها، storage ها و appliance ها می باشد. مرکز کار Iron Networks در San Jose کالیفرنیا است. ترکیب بیش از یک دهه تخصص نرم افزاری و سخت افزاری Iron Networks به همراه Iron Systems، به ارائه Appliance های قدرتمندی مبدل شده است که تنها یک شرکت مجرب در زمینه فناوری، قادر به تولید و ارائه آن می باشد. شرکای تجاری Iron Networks، شرکتهای Microsoft، RSA، Cavium، Intel، Websense و Sonasoft می باشند.

Iron Networks، Turnkey appliance های مبتنی بر ویندوز را برای زیرساختهای شبکه و امنیت شبکه، عرضه کرده است و یک خط تولید کاملا اختصاص یافته، هدف دار و آماده برای توسعه سرویسهای سخت افزاری جهت اجرای Forefront TMG 2010، را دارا می باشد. http://www.ironnetworks.com/

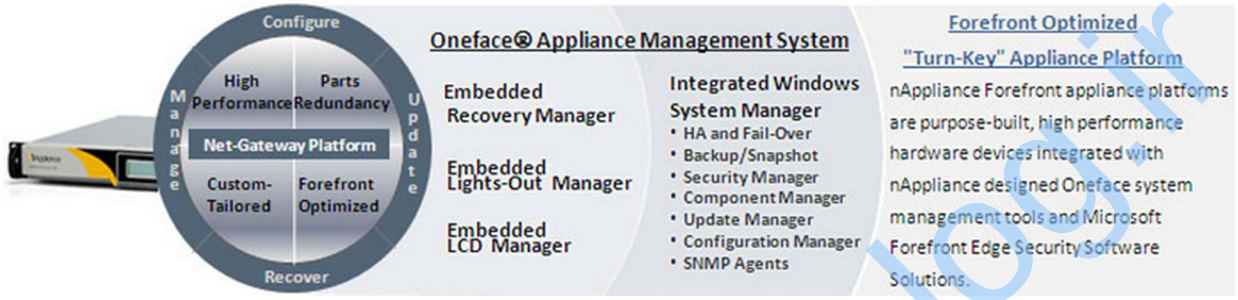
اصطلاح Turnkey، که اغلب در صنعت فن آوری استفاده می شود، بیشتر برای توصیف Package های کامپیوتری پیش ساخته می باشد که در آن، هرآنچه که برای اجرای نوع خاصی از وظایف، مورد نیاز است، توسط عرضه کننده آن در کنار یکدیگر قرار داده شده و به عنوان یک بسته نرم افزاری به فروش می رسد و معمولا شامل کامپیوتری، با یک نرم افزار از پیش نصب شده و انواع مختلفی از سخت افزارها و لوازم جانبی است. این نوع Package ها، معمولا appliance، نامیده می شوند.

خانواده nAppliance Net-Gateway appliance طیف گسترده ای از مدلها را پشتیبانی می کند. هریک از این مدلها، دقیقا متناسب با نیازهای منحصر به فرد مشتریان می باشد. این appliance ها، ویژگیهای performance (کارایی)، capacity (ظرفیت) و availability (در دسترس بودن) را که برای هر محیطی مورد نیاز می باشد، از کوچکترین branch office ها تا بزرگترین data center ها، تأمین می کند. امکان خرید این Appliance ها برای کشور ایران نیز، مقدور می باشد.

http://www.ironnetworks.com/purchase/contact-ironnetworks

Forefront Optimized "Turn-Key" Appliance Solution

nAppliance Forefront appliance ها، device های سخت افزاری با کارایی بالا و هدفمند می باشند، که با ابزارهای طراحی شده برای Oneface system management و راه کارهای Microsoft Forefront Edge Security Software، یکپارچه شده اند.



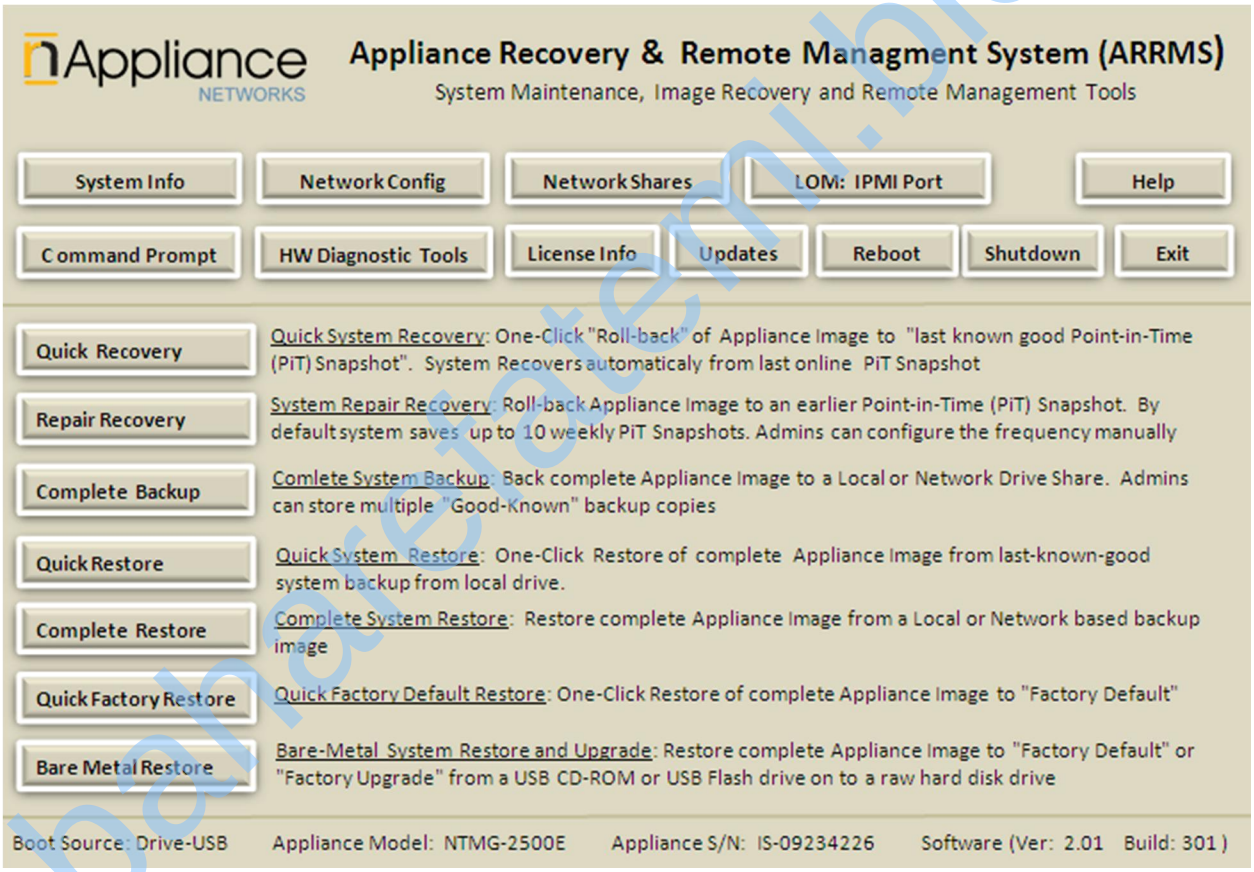
پلت فرم برقراری امنیت برروی شبکه، بر مبنای یکپارچه سازی با تکنولوژی Microsoft's Integrated Forefront Edge Security Gateway، بنا شده است.

Microsoft Forefront Threat Management Gateway 2010 یک پلت فرم edge security (ایجاد امنیت در لبه شبکه) جامع و یکپارچه است که ارائه دهنده راه کارهای محافظتی در برابر انواع تهدیدات مبتنی بر اینترنت، امکان برقراری اتصال امن و مدیریت ساده، هم برای datacenter ها و هم branch office ها می باشد. این ویژگیهای محافظتی و ارزشمند، به مدیران IT، مدیران شبکه و متخصصان امنیت اطلاعات که در خصوص امنیت، عملکرد، TCO (هزینه های مالیاتی) و یا مدیریت شبکه های سازمانی خود، نگران می باشند، ارائه شده است.

توصیف معماری nAppliance ها

Oneface Embedded Recovery Manager

- **Recovery Manager تعبیه شده – Appliance Recovery and Remote Management System (ARRMS)** : ARRMS، یک محیط عملیاتی تعبیه شده در تمامی سیستمهای nAppliance است و امکان مدیریت سیستم و نگهداری سخت افزار Appliance و software image را به صورت آفلاین برای Administrator، فراهم می کند. محیط عملیاتی ARRMS کاملا مستقل از سخت افزار اصلی appliance و محیط نرم افزاری آن، عمل می کند. appliance می تواند با استفاده از ARRMS و در حالت "maintenance mode" بوت شود، که در این حالت حتی با shutdown شدن سیستم عامل appliance یا power off شدن سخت افزار، Administrator دسترسی کاملی به محیط های نرم افزاری و سخت افزاری در سطح BIOS دارد.



ARRMS برای مدیران شبکه، یا برای پرسنل IT که در نقطه ای نزدیک به سخت افزار appliance، واقع شده اند، ویژگی maintenance و مدیریت کاملا کاربردی محیط را بدون نیاز به CD utility های بازیابی فراهم می کند. این ویژگی، مدیریتی قدرتمند برای انجام عملیات متمرکز IT و یا ارائه مدیریت ریموت "branch" office ها را بدون نیاز به پشتیبانی محلی IT، به بخشهای IT یک سازمان ارائه می دهد.

توصیف مزایا و ویژگیهای کلیدی

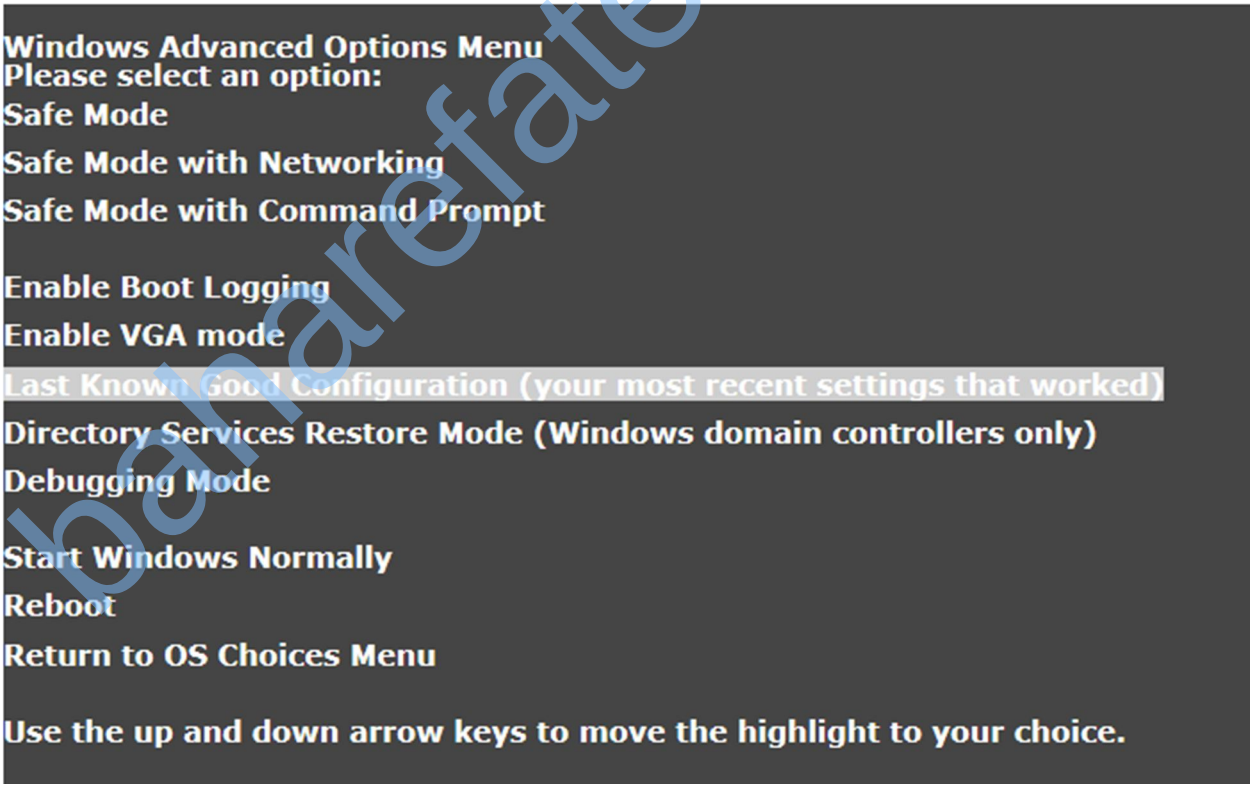
Online, Quick Point in Time (PiT) snapshot Backups and Recovery

- یک سیستم backup گیری تعبیه شده در ARRMS است که امکان backup گیری های آنلاین سازگار با VSS (Volume Shadow Copy Service) را ارائه می دهد. Backup ها می توانند برای هر دو rollback های **"Last Known Good Configuration"** که backup تعبیه شده سخت افزاری و ریموت شبکه توسط سرویسهای **Disaster Recovery** می باشد، زمان بندی شوند.

VSS یک رابط ویندوزی خاص را ارائه می دهد که امکان هماهنگی درخواست کنندگان back up گیری از داده ها، writer هایی که اطلاعات را برروی دیسک، به روز رسانی می کنند و Provider هایی که Storage ها را مدیریت می کنند، فراهم می سازد.

"Last Known Good Configuration"، ابتدا در Windows 2000 معرفی شد و در تمام نسخه های بعدی ویندوز از جمله Windows XP، در دسترس می باشد. این ویژگی کاربر را قادر می سازد که آخرین نسخه ویندوز را با کارکرد صحیح Load کند و این روشی به منظور تلاش برای برطرف کردن مشکلاتی در کامپیوتر است که مانع از Load ویندوز می شوند.

Disaster recovery (DR) به فرایندها، Policy ها و روشهایی گفته می شود که به ریکاوری سیستم یا استمرار زیرساختهای فن آوری مرتبط می باشد.



- **سازگاری با VSS**، امکان یکپارچه سازی snapshot جهت backup های آنلاین از File System های "in-motion" و SQL logging و مدیریت دیتابیسها را فراهم می کند.
- **Bare Metal Restore : جایگزینی سخت افزار سیستم یا Upgrade ها:** ARRMS، جایگزینی کامل سخت افزار یا migrate از محیط عملیاتی را به منظور "bare-metal-recovery" یا جایگزینی سیستمهای سخت افزاری، سهولت می بخشد. هر appliance می تواند به راحتی با یک کلیک ماوس توسط کارکنان IT، Image گیری دوباره شود.
- **ویژگی های مدیریتی و پیکربندی سیستم:**
  - **System Info :** نمایش استاتیک جزئیات پیکربندی و نسخه های نرم افزار و سخت افزار
  - **Network Config :** امکان پیکربندی کارت شبکه را با آدرسهای IP، rout ها و غیره
  - **Network Shares :** Administrator می تواند Share ها را به صورت ریموت Attach کرده و backup های موقت آفلاین ایجاد کند، و همچنین appliance را با Share Backup ها از طریق ریموت بازیابی کند.
  - **HW Diagnostics Tools:** ابزارهای داخلی برای عیب یابی و تعمیر سیستم
  - **License Info:** سیستم بازیابی لایسنس و اطلاعات پرداخت و همچنین نصب license key های نرم افزاری تعبیه شده Microsoft Server را، بازرسی می کند.
  - **Updates:** در صورتی که محیط عملیاتی اصلی با استفاده از این امکان، دچار مشکل شده باشد، دانلودهای نرم افزاری و Update ها می توانند اعمال شوند.
- **High Availability, Fail-Over Option (sold separately) :** ARRMS، اساس High Availability یا failover بلادرنگ را در حالت standby فراهم می کند. appliance ها دارای LAN port اختصاصی می باشند که برای مدلهایی که قابلیت HA/NLB محلی در ویندوز در دسترس نمی باشد، می توانند با استفاده از یک کابل به عنوان جفت failover دیگری مورد استفاده قرار گیرند.

Embedded system environment

ARRMS برروی یک flash drive تعبیه شده سخت افزاری، اجرا می شود که امکان نگهداری از تمامی عملیات انجام شده برروی Appliance، که شامل bare-metal-recovery با جایگزین کردن و فرمت مجدد hard درایوها و سایر اجزاء سخت افزاری می باشد، فراهم می کند.

- **WinPE 2.0 operating environment :** ARRMS از قابلیت اجرای Windows Vista Pre-Install Environment برخوردار می باشد که نسخه تعبیه شده سبک Windows Vista است. این وِیژگی یک محیط توانمند و انعطاف پذیر را ارائه می دهد، که Administrator می تواند سیستم را با استفاده از دستورات ویندوزی متداول مدیریت کند.
- **Full GUI interface with windows CLI support :** ARRMS یک محیط GUI ویندوزی را که محیطی توانمند و با قابلیت استفاده آسان می باشد، ارائه می دهد. ابزارهای اصلی مدیریت ویندوز که تقریبا هر ابزار

Command Line ویندوزی را شامل می شود، پشتیبانی می شوند. این دستورات می توانند به منظور انجام تنظیمات پیشرفته تر و بازرسی های سیستمی، توسط Administrator، مورد استفاده قرار گیرند.

Option های دسترسی به ARRMS : Local, Remote over internet and Headless via LCD

nAppliance ARRMS از چندین Option دسترسی جهت مدیریت موثر، کارامد و انعطاف پذیر سیستم Appliance ها پشتیبانی می کند. ARRMS، علاوه بر دسترسی محلی از طریق صفحه کلید، ویدئو و ماوس، از طریق ریموت و با استفاده از **Lights-Out management (LOM)** مبتنی بر iKVM (KVM over IPMI) یا با استفاده از صفحه نمایش LCD و keypad نیز قابل دسترسی می باشد.

Option های توسعه LCD based Headless : ARRMS از طریق یک LCD interface ساده، قابل دسترس است. به طوری که می توان Appliance را از طریق منوی ساده LCD interface، مدیریت، تعمیر و upgrade نمود. این ویژگی، یک محیط مدیریتی و مانیتورینگ ساده را بدون نیاز به اتصال مانیتور و کی بورد فراهم می کند و هدف از آن موارد زیر می باشد:

- **تسریع وظایف مدیریتی**
- **انجام عملیات ریموت بدون نیاز به پشتیبانی IT در محل**

توضیح برخی از اصطلاحات:

out-of-band management (گاهی اوقات، **lights-out management** یا **LOM** نیز خطاب می شود) استفاده از یک کانال مدیریتی اختصاصی برای تعمیر و نگهداری device را شامل می شود. این ویژگی به system administrator اجازه می دهد که صرف نظر از اینکه دستگاه powered on است و یا سیستم عامل نصب شده و در حال کار می باشد، سرورها و سایر تجهیزات شبکه را مانیتور با استفاده از ریموت کنترل، مانیتور و مدیریت کند.

در مقابل، **in-band management**، مانند VNC یا SSH، بر اساس نرم افزاری است که می بایست برروی سیستم ریموت نصب شده و تنها پس از بوت شدن سیستم عامل مدیریت می شود. این solution ممکن است ارزان تر باشد، اما امکان دسترسی به تنظیمات BIOS و یا نصب مجدد سیستم عامل را ممکن نمی سازد. و نمی تواند برای برطرف کردن مشکلاتی که مانع از بوت سیستم عامل می شود، مورد استفاده قرار گیرد.

معمولا هم **in-band management** و **out-of-band management** هردو از طریق اتصال شبکه انجام می شوند. اما out-of-band management card می تواند از یک network connector جداگانه فیزیکی استفاده کند. معمولا یک remote management card، حداقل یک power supply (منبع تغذیه) تا حدی مستقل را دارا بوده و می تواند از طریق شبکه، main دستگاه را Power on یا Power off کند.

IPMI (Intelligent Platform Management Interface)، یک system interface کامپیوتری استاندارد است که توسط system administrator (شخصی که وظیفه تعمیر و نگهداری، و عملکرد قابل اعتماد سیستمهای کامپیوتری به ویژه کامپیوترهای چند کاربره مانند سرورها را بر عهده دارد) به منظور مدیریت out-of-band و مانیتورینگ عملیات آنها، مورد استفاده قرار می گیرد. IPMI روشی برای مدیریت کامپیوتری است که ممکن است خاموش شده و یا با اتصال شبکه به یک سخت افزار به جای سیستم عامل یا login shell، پاسخ مناسبی نمی دهد.

KVM over IP (iKVM)

KVM over IP یک سوئیچ یا Device سخت افزاری است که این Device ها از یک میکروکنترلر اختصاصی و سخت افزار بالقوه تخصصی video capture برای ضبط سیگنالهای ویدئو، صفحه کلید و ماوس، و سپس فشرده سازی و تبدیل آنها به بسته های اطلاعاتی و ارسال آنها از روی یک Ethernet link به یک remote console application، استفاده کرده و یک تصویر گرافیکی پویا را unpack و بازسازی می کند. Device های KVM over IP معمولا به standby power plane متصل می شوند، به طوری که می توان تمامی مراحل بوت را مشاهده کرده، یا به BIOS دسترسی پیدا کرد. این Device ها اجازه می دهند چندین کامپیوتر در سرتاسر **wide area network**، **local area network** یا **telephone-line** با استفاده از پروتکل TCP/IP به صورت ریموت، کنترل شوند. می توان با استفاده از وب بروزر، یا یک client application مستقل، سرور را مدیریت نمود. KVM، امکان دسترسی به سرور را حتی اگر اتصال ریموت یک شبکه Public، down شده باشد، فراهم می کند.

موارد استفاده از KVM

- عیب یابی مشکلات
- نصب Linux / *BSD به صورت ریموت
- دسترسی به BIOS و تغییر تنظیمات به صورت ریموت
- دسترسی به سرور حتی اگر شبکه down شده باشد
- دسترسی به سرور حتی اگر سرور خیلی busy بوده و یا پاسخگویی به اتصالات شبکه، متوقف شده باشد
- ریست کردن root password
- اجرای fsck (**F**ile **S**ystem **C**hec**k**)، ابزار و کامندی جهت تعمیر file system های آسیب دیده) و بسیاری از موارد دیگر

با استفاده از این تکنولوژی، می توانید کل Server rack را از office خود یا از هر جایی کنترل کنید. امروزه می توان با اضافه کردن یک card (daughtercards)، ویژگی KVM Support را فعال نمود و دیگر مجبور به استفاده از external KVM device ها در پشت server rack نمی باشد.

قابلیتهای Forefront Appliance Platform

این قابلیتها مشتمل بر:

- **Multi-Core 64-bit architecture for high-performance network security**

طراحی پلت فرم nAppliance، شامل معماری multicore x86، کش پردازنده با سرعت بالا، بزرگترین حافظه و پهنای باند multi lane PCIe، بوده و جهت به حداکثر رساندن کارایی، مقیاس پذیری و کاهش یافتن مصرف برق، طراحی شده است. nAppliance ها، بازرسی عمیق بسته های اطلاعاتی و محافظت از محتویات بسته ها را در مقابل حملات پیچیده ای که دائما در حال تکامل می باشند، هم از داخل و هم خارج از شبکه، به صورت بلادرنگ، فراهم می کند.

- **Enterprise grade high availability**

راه کارهای nAppliance، قابلیت تحمل پذیری خطا و ویژگی failover را به شیوه ای جدید، برروی هسته Service appliance های امنیتی شبکه ارائه می دهد. ویژگیهای ارائه شده عبارتند از:

- **Hardware availability (در دسترس بودن سخت افزار) از طریق component level های ایجاد redundancy برروی دیسکها، power supply ها و fan ها**
- **Windows operating system availability (در دسترس بودن سیستم عامل ویندوز) از طریق system image redundancy و online PiT snapshot Recovery system (PITR)**
- **Network level system availability از طریق load balancing و fail-over**

High copper and fiber network port density

کارت شبکه های high port-density Gigabit Ethernet، کارایی، انعطاف پذیری عملیاتی و redundancy را که برای ایمن سازی high-availability در زیرساخت های شبکه ضروری می باشد، همراه با صرفه جویی در مقیاس، که برای سازمانهای بزرگ، Enterprise، data center ها و service provider ها لازم می باشد، فراهم می کند.

سخت افزار تعبیه شده SSL acceleration با کارایی بالا جهت 100% TCP/IP Offload (افزایش سرعت سیستمهای Ethernet با هدف بهینه سازی توان عملیاتی)

سخت افزار SSL acceleration co- processor شرکت Cavium حجم کاری CPU را کاهش داده و مزایای زیر را فراهم می کند (برای آشنایی بیشتر با شرکت Cavium، به لینک http://www.cavium.com/company.html مراجعه نمایید)

- **پاسخگویی با کمترین زمان تأخیر:** در نتیجه کاهش Load CPU، کاهش یافتن زمان تأخیر در پاسخگویی به هر کلاینت می باشد.

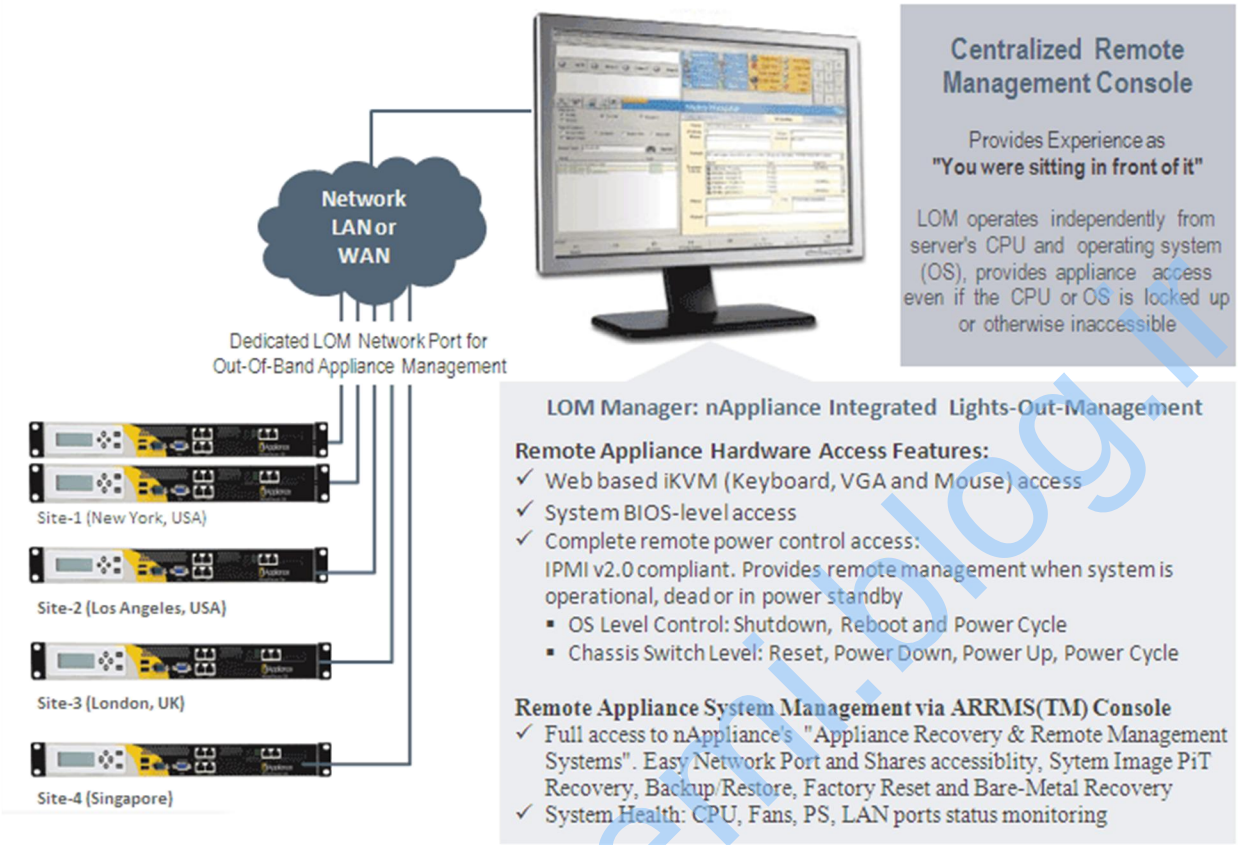
- **افزایش burst rate (حداکثر سرعت انتقال داده یا سرعتی که شبکه در یک time frame کوتاه دارا می باشد، که معمولا تحت عنوان سرعت در Mbps نامیده می شود)، از طریق SSL handshake سریعتر.** این ویژگی می تواند از 100 لاگین همزمان جدید، در هر ثانیه پشتیبانی می کند. این ویژگی افزایش عملکرد قابل ملاحظه burst rate و ثبات سیستم را برروی راهکارهای software-only، فراهم می کند.
- **افزایش عملکرد Peak Time:** کاهش حجم کاری CPU، تعداد پردازش transaction های هر appliance system که را افزایش می دهد.
- **افزایش امنیت:** private key های سرور به منظور جلوگیری از ذخیره شدن برروی hard disk drive ها، در flash device های Write-only ذخیره می شوند که در processor های Cavium تعبیه شده است، و این امر دسترسی های غیر مجاز را مشکل تر می سازد.

مدیریت HSM certificate : سخت افزار HSM، مخزن Certificate و سهولت ایجاد Certificate را فراهم می کند. اگر یک سیستم به خطر بیفتد، Certificate ها نیز در معرض خطر قرار می گیرند، مگر اینکه Certificate ها ایجاد شده و در این قطعات سخت افزاری خاص ذخیره شوند.

ممیزی های امنیتی جامع: سیستمهای appliance ای nAppliance با بهترین شیوه امنیتی متصور طراحی شده اند. نرم افزارهای مختلف افزوده شده، Component های سخت افزاری و تنظیمات سیستمی، system profile را تغییر خواهد داد. هریک از نسخه های Image، به صورت سیستماتیک بسته بندی شده و به منظور قابلیت اطمینان و دریافت ممیزی های امنیتی کامل، به صورت مداوم توسط کارشناسان سیستمهای امنیتی مورد آزمایش قرار می گیرد.

مدیریت Lights-Out-Management (LOM) – سیستم مدیریت سخت افزار Appliance به صورت ریموت

قابلیت LOM در بسیاری از پلت فرمهای nAppliance تعبیه شده است و همراه با شبکه و پورتهای سریال جهت ارائه قابلیتهای مدیریتی ریموت در سطح BIOS به صورت SSL امن "out of band" web-based تکمیل شده است. LOM ویژگی کامل "in-front-of-the-server" را که تجربه مدیریتی سرور به صورت ریموت و عملا از هر نقطه ای از جهان از طریق یک رابط گرافیکی وب می باشد فراهم می کند و دسترسی KVM (خلاصه شده "keyboard, video and mouse") به صورت ریموت، power on/off/reboot نمودن system، یکپارچه سازی کامل با مدیریت ARRMS´ و دسترسی به رسانه های ذخیره سازی، دسترسی به کنسول سیستم، health monitoring جامع، و اعلانهای user rights و پشتیبانی از مدیریت دسترسی های LDAP و RADIUS می باشد را شامل می شود.



LOM با iKVM/ IPMI v2.0 سازگار بوده و مزایای زیر را ارائه می دهد:

- **Out of Band management**

Administrator می تواند به Appliance دسترسی پیدا کرده و سیستم را Power off یا Power on نموده و سایر عملیات تعمیر و نگهداری سیستم را در سطح پیشرفته اجرا کند.

- **Remote Storage Media Support**

دسترسی ریموت به CD/DVD media را به صورت internal و External و appliance ISO image فراهم می کند.

- **Remote access to ARRMS manager interface**

ARRMS دسترسی ریموت به رابط مدیریتی ARRMS را به منظور مدیریت ساده پورتهای شبکه و تنظیمات Share ها، عیب یابی، image backups/recovery/restore/upgrade از سیستم Appliance و سایر عملیات پشتیبانی را فراهم می کند.

- **iKVM (Keyboard/VGA/Mouse support over IP) Support**

تغییر مسیر System console جهت دسترسی ریموت از طریق کنسول وب و دسترسی ریموت به keyboard، ویدئو و ماوس

- **Rich enterprise system standard support**

پشتیبانی از IPMI، SSL و SNMP trap ها به منظور یکپارچه سازی ساده تر سیستمهای سازمانی

- **User Rights and access management**

LDAP و RADIUS

- **Health Monitoring and Notification**

Health monitoring جامع برروی بیش از 100 پارامتر سیستمی و Email/SMTP notification alert ها جهت اطلاع از error ها و مشکلات سخت افزاری

LCD Manager – Headless Appliance Deployment System : سیستمهای Appliance شامل نرم افزار و سخت افزار LCD می باشند که امکان نصب آسان، بدون اتصال keyboard، ماوس و video monitor ها را فراهم می کند. این ویژگی تا حد زیادی امکانات نصب، از جمله نصب ریموت را بدون نیاز به پشتیبانی بخش IT ساده نموده است.

Oneface® Integrated Windows System Manager

nAppliance مدیریت MMC بر پایه UI (User Interface) را جهت اداره یک یا چند سیستم nAppliance از طریق یک Interface واحد، طراحی کرده است. این سیستم، مدیریت و توسعه سیستمهای نرم افزاری و سخت افزاری nAppliance را که شامل تنظیمات شبکه، ویزاردهای TMG rule، مدیریت clustering، و سایر package های امنیتی 3rd party می باشد به صورت ساده و متمرکز تبدیل نموده است. Component های کلیدی **Oneface Windows System Manager** شامل:

- **Hardware Failover Manager**

Onface، امکان پشتیبانی و مدیریت Microsoft Clustering، و تکنولوژی اختصاصی و کم هزینه Fault Tolerant "Warm Standby" را که مختص به nAppliance می باشد، فراهم می کند. این ویژگی قابلیت redundant و fault tolerant امن را، بدون نیاز به هزینه های خریداری چندین license و انجام تنظیمات active-active، فراهم می کند.

- **Backup Manager**

چندین Option جهت backup گیری و فراهم کردن snapshot backup های Point-in-Time از کل سیستم Appliance، و یا به صورت داخلی، و یا با استفاده از ریموت، در دسترس می باشد.

- **Security Manager**

هر Appliance، سیستم های مانیتورینگ داخلی را جهت remove کردن، آسیب پذیریهای امنیتی و سایر احتمالات منجر به آسیب پذیری، با توجه به تنظیمات و سایر تدابیر امنیتی در نظر گرفته شده، اجرا می کند.

- **Component Manager**

استفاده از نرم افزارهای 3rd party به منظور توسعه قابلیتهای Appliance شامل QOS، content management، WAN Optimization و سایر Component های دیگر

- **Update Manager**

مانیتورینگ مداوم Software patch های منتشر شده و فراهم کننده یک سیستم مدیریت یکپارچه Patch ها برای کل appliance از درایورها، تا سیستم عامل و تمامی Application System های نصب شده

- **Configuration Manager**

مدیریت تنظیمات Appliance، شامل، مدیریت شبکه، سیستم عامل و تنظیمات اختیاری با استفاده از کنسول مدیریت مرکزی

- **Alert Manager**

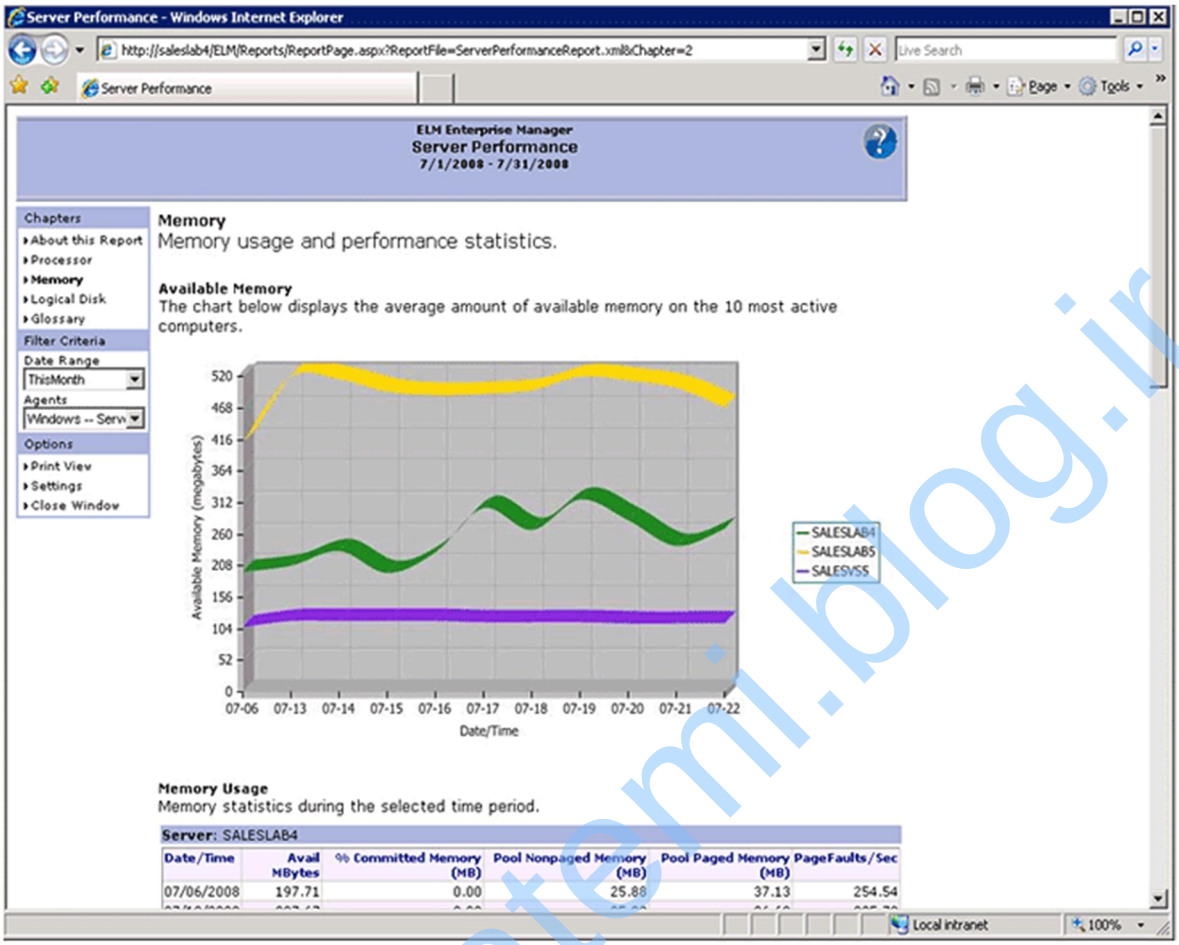
مدیریت Alert ها

- **SNMP Agents Support**

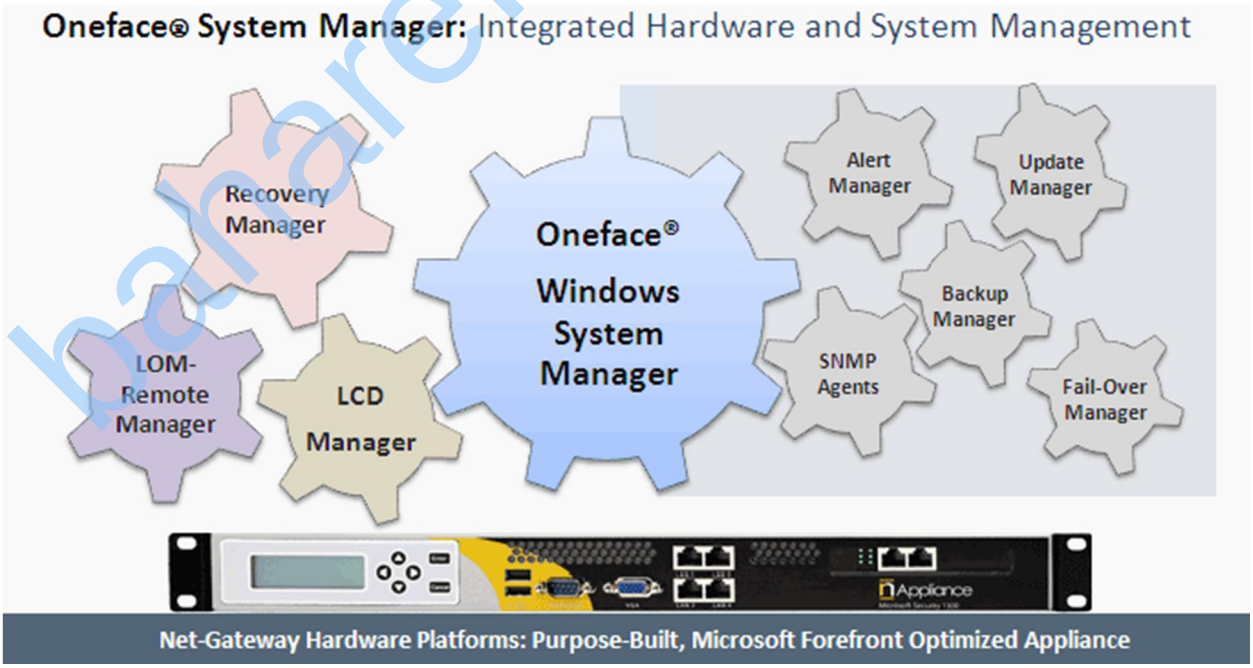
Simple Network Management Protocol (SNMP)، یکی از پروتکلهای شناخته شده برای مدیریت شبکه است که برای جمع آوری اطلاعات و پیکربندی Device های شبکه، مانند server ها، printer ها، hub ها، و router ها، با استفاده از پروتکل IP، برروی شبکه مورد استفاده قرار می گیرد. SNMP Agent یک Component اختیاری است که با فعال کردن آن برروی Device مورد نظر، و استفاده از نرم افزارهای مدیریت SNMP، می توان اطلاعات مربوط به آن Device را جمع آوری نمود.

- **Lightweight Enterprise Manager**

nAppliance یک سیستم مدیریت شبکه با استفاده از پروتکل SNMP را که با سخت افزار، سیستم عامل و Application ها یکپارچه شده است، فراهم می کند. این ویژگی یک dashboard مدیریتی کامل و مستقل را ارائه می دهد.

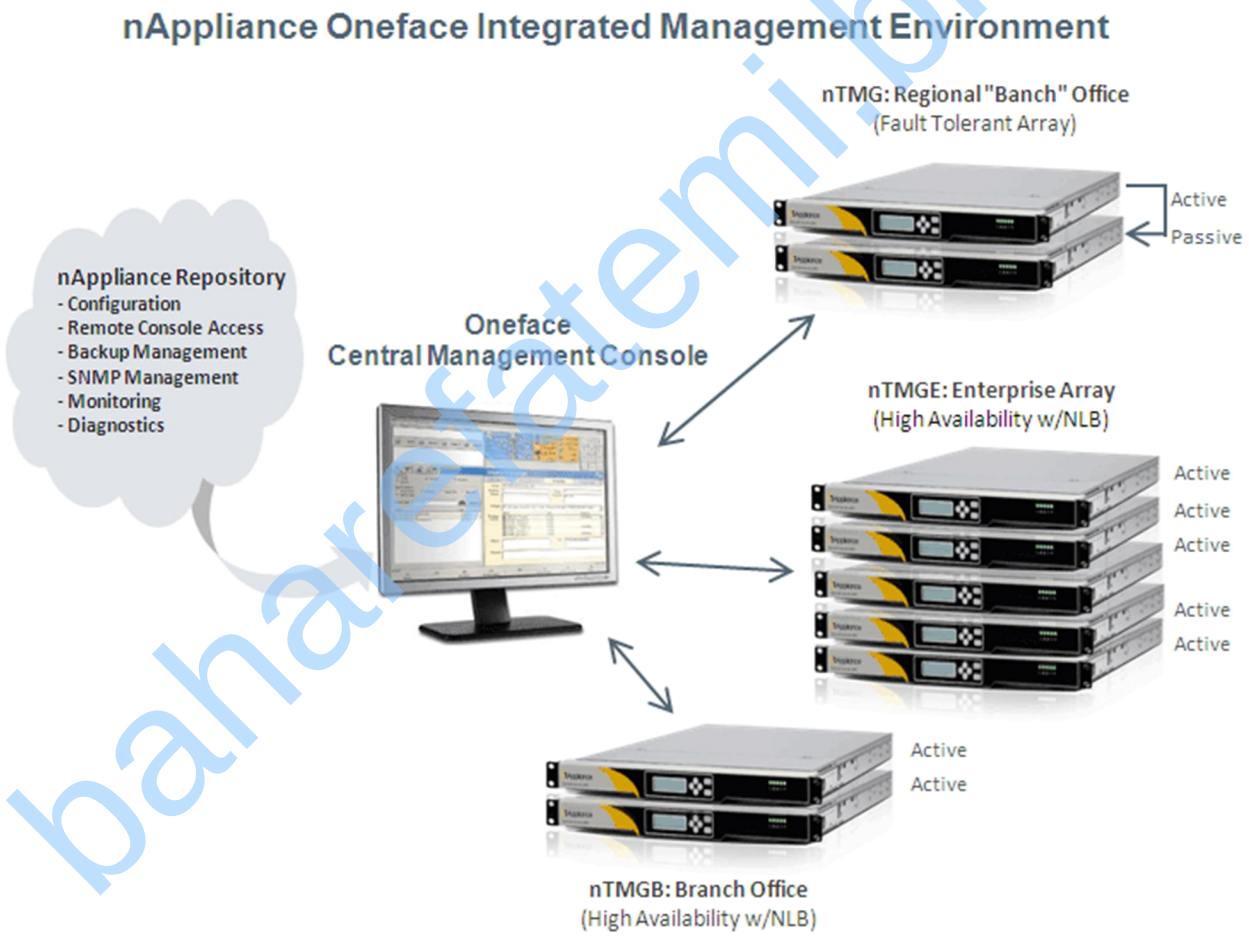


پلت فرم nAppliance Oneface® System Management،



Oneface® System Management یک سیستم مدیریتی از قبل یکپارچه شده را برای پیاده سازی appliance در هر تعداد، از نصب یک appliance تا توزیع چندین appliance را فراهم می کند. Oneface بر مبنای Microsoft Windows MMC 2.0 می باشد. این ویژگی Oneface را کاملا با زیرساختهای Microsoft Management سازگار ساخته و با سایر Microsoft MMC snap-in های مایکروسافت، توسعه پذیر می سازد.

کنسول مدیریت مرکزی nAppliance OneFace، یک داشبورد مدیریت متمرکز است که می تواند یک appliance یا تعداد بیشتری appliance را به صورت محلی یا با استفاده از ریموت مدیریت کند. این کنسول، پیکربندی، ارتقا، مانیتورینگ و مدیریت هر appliance را از یک محل مرکزی، فراهم می کند. همچنین Oneface می تواند به سیستمهای مدیریت Enterprise SNMP مانند HP Openview یا Microsoft Systems Center متصل شود.



سرویسهایی که ویژگی ARRMS ارائه می دهند، عبارتند از:

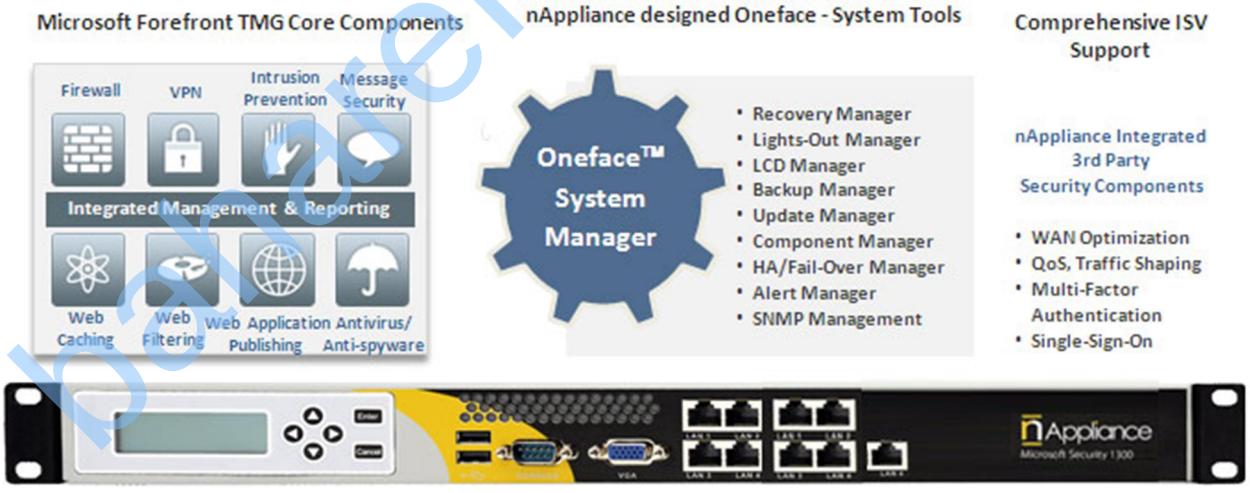
- Appliance System Configuration برای مدیریت server network port، lights-out management iKVM port، network share ها و hardware diagnostics service ها
- Appliance Image Management برای مدیریت آنلاین Point in Time (PiT) system OS recovery، multi image backup ها، restore ها، factory default reset و سرویسهای bare-metal appliance reset

Option های دسترسی ARRMS : به صورت Local، مدیریت ریموت از طریق شبکه و Headless با استفاده از LCD

nAppliance ARRMS، از چندین Option دسترسی جهت مدیریت پیشرفته، کارامد و انعطاف پذیر appliance system ها پشتیبانی می کند. علاوه بر دسترسی محلی با استفاده از صفحه کلید، ویدئو و ماوس، می تواند از طریق remote LOM بر مبنای iKVM (KVM over IPMI) یا از طریق صفحه نمایش LCD و keypad نیز در دسترس قرار گیرد.

پشتیبانی از Microsoft System Center و Enterprise Management System های مشابه: سیستمهای nAppliance، شامل پشتیبانی از پروتکل SNMP، همراه با تنظیمات Custom برای HP Openview و Microsoft Systems Center PAK ها می باشد. SNMP support، یکپارچه سازی مستقیم با Enterprise Management system ها را که تقریبا توسط تمامی بخشهای بزرگ IT سازمان مورد استفاده می باشد، فراهم می کند.

معرفی مدلهای nAppliance بر اساس Microsoft Forefront TMG Core Components



مدلهای nTMGB nAppliance Net-Gateway :

http://www.ironnetworks.com/products/nTMGB-branchoffice-products.asp

مدل nTMGB یک appliance با ساختار integrated **branch office security gateway**، و بر اساس نسخه Microsoft Forefront TMG 2010 Branch Offices، می باشد. دو nTMGB appliances، می تواند در حالت active/active array، و با استفاده از قابلیت NLB یکپارچه سازی شده با Forefront، برای ارائه قابلیت به اشتراک گذاری redundancy، پیکربندی شوند. nTMGB، نسل هوشمند بعدی **Branch Office Security Gateway**، را فراهم می کند.

- **Connect and Secure Branch Offices Network Infrastructure**
- **Simplified Branch Office Deployment and Efficient Management**
- **Intelligent Content Caching and Acceleration**

مدل nTMGB 1500B

NetGateway nTMGB-1500B 	• **مناسب برای Small-Sized Branch Office (Branch Ofiice های کوچک)** • **پشتیبانی تا 500 کامپیوتر و 2500 کاربر وب** • **Redundant Hotswap Disks** • **Dual Node High Availability NLB Support داخلی** برای مطالعه ویژگیهای این مدل به لینک زیر مراجعه کنید http://www.ironnetworks.com/products/nTMGB-1500B.asp

مدل nTMGB 2500B

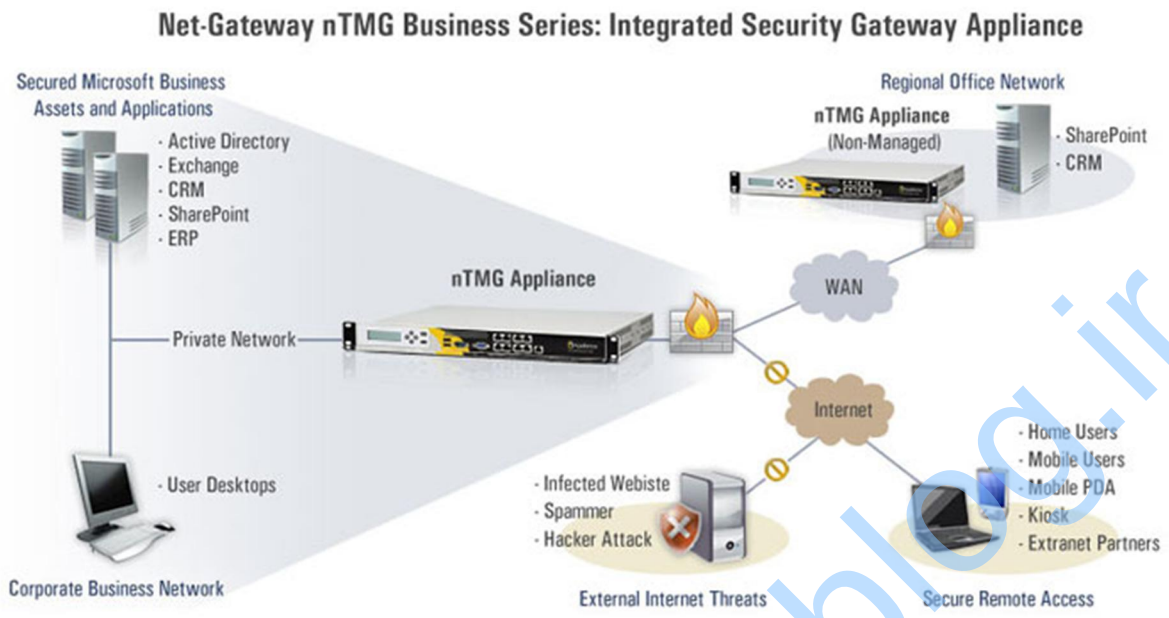
NetGateway nTMGB-2500B 	• **مناسب برای Mid-Sized Branch Office (Branch Ofiice های متوسط)** • **پشتیبانی تا 1000 کامپیوتر و 5000 کاربر وب** • **Redundant Hotswap Disks** • **Dual Node High Availability NLB Support داخلی** برای مطالعه ویژگیهای این مدل به لینک http://www.ironnetworks.com/products/nTMGB-2500B.asp مراجعه کنید

مدل nTMGB 3500B

NetGateway nTMGB-3500B 	• مناسب برای Mid-Sized Branch Office (Branch Ofiice های متوسط) • پشتیبانی تا 3000 کامپیوتر و 15000 کاربر وب • Redundant Hotswap Disks و Power Supply Modules • Dual Node High Availability NLB Support داخلی برای مطالعه ویژگیهای این مدل به لینک http://www.ironnetworks.com/products/nTMGB-3500B.asp مراجعه کنید

مدل nTMGB 5500B

NetGateway nTMGB-5500B 	• مناسب برای Large-Sized Branch Office (Branch Ofiice های بزرگ) • پشتیبانی تا 4000 کامپیوتر و 20000 کاربر وب • Redundant Hotswap Disks و Power Supply Modules • Dual Node High Availability NLB Support داخلی برای مطالعه ویژگیهای این مدل به لینک http://www.ironnetworks.com/products/nTMGB-5500B.asp مراجعه کنید



مدلهای nTMGE : nAppliance Net-Gateway nTMGE،

یک appliance با ساختار integrated **edge security gateway** بر مبنای Microsoft Forefront TMG 2010 نسخه Enterprise، و مناسب برای data center ها می باشد. چندین nTMGE appliance را می توان در حالت active/active array، و با استفاده از قابلیت NLB یکپارچه سازی شده با Forefront، و استفاده از ویژگی scalability (مقیاس پذیری) به صورت نامحدود، پیکربندی نمود. nTMGE می تواند در هریک از نقشهای (Role) زیر، توسعه داده شود:

- **Unified Threat Management (UTM) Gateway - "All-in-One" Integrated Security Solution**
- **Remote Access Gateway Solution**
  - Anywhere VPN Remote Access
  - Secure Web Application Publishing
- **Remote Branch Office Gateway - Highly Scalable Enterprise Management Solution**
- **Secure Web Gateway Solution**
- **Secure Messaging Email Gateway Solution for Exchange**

لیست محصولات nTMGE Datacenter

http://www.ironnetworks.com/products/nTMGB-5500B.asp

مدل nTMGE-1500E

nAppliance nTMGE-1500E ، یک Appliance در سطح Enterprise و یکپارچه سازی شده با TMG، بر مبنای Microsoft Forefront Threat Management Gateway 2010 — Enterprise Edition (Corporate Data Center) می باشد.

NetGateway nTMGE-1500E 	• مناسب برای Small Sized Enterprise • پشتیبانی تا 500 کامپیوتر و 2500 کاربر وب سازمانی • Redundant Hotswap Disks • پشتیبانی از مقیاس پذیری درونی بسیار بالا برروی NLB Array http://www.ironnetworks.com/products/nTMGE-1500E.asp

مدل nTMGE-2500E

nAppliance nTMGE-2500E ، یک Appliance در سطح Enterprise یکپارچه سازی شده با TMG و بر مبنای Microsoft Forefront Threat Management Gateway 2010 — Enterprise Edition (Corporate Data Center) می باشد.

NetGateway nTMGE-2500E 	• مناسب برای Small/Mid Sized Enterprise • پشتیبانی تا 1000 کامپیوتر و 5000 کاربر وب سازمانی • Redundant Hotswap Disks • پشتیبانی از مقیاس پذیری درونی بسیار بالا برروی NLB Array http://www.ironnetworks.com/products/nTMGE-2500E.asp

مدل nTMGE-3500E

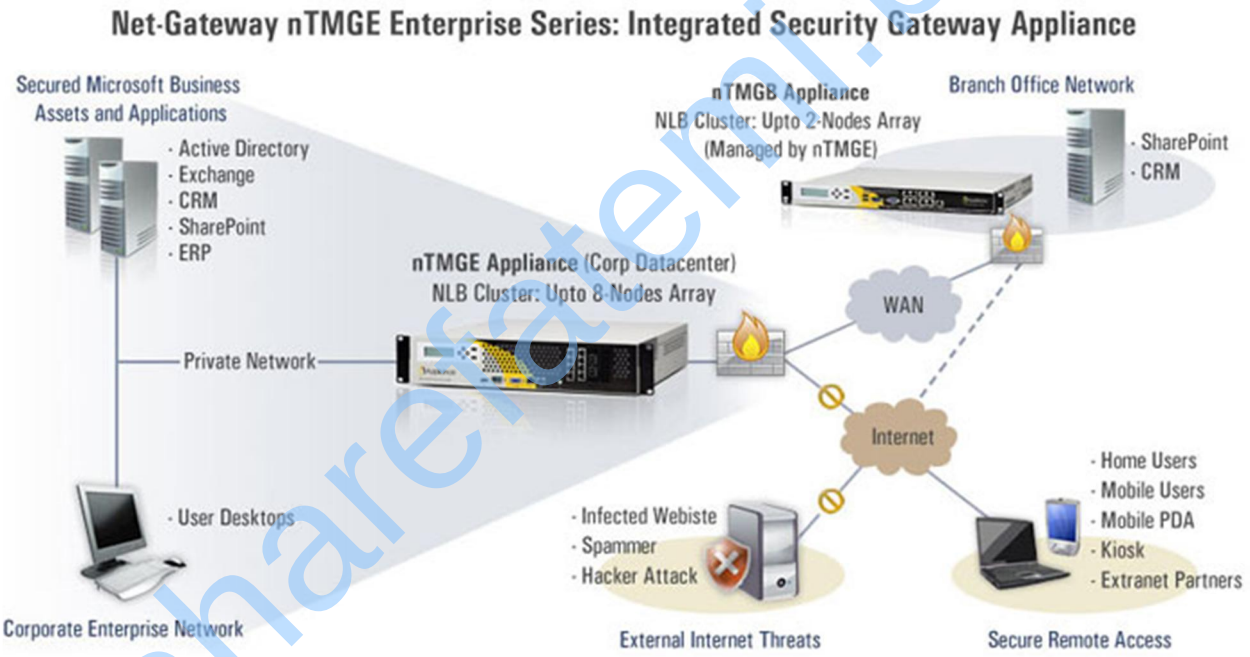
nAppliance nTMGE-3500E ، یک Appliance در سطح Enterprise و یکپارچه سازی شده با TMG بر مبنای Microsoft Forefront Threat Management Gateway 2010 — Enterprise Edition (Corporate Data Center) می باشد

NetGateway nTMGE-3500E 	• مناسب برای Mid Sized Enterprise • پشتیبانی تا 3000 کامپیوتر و 15000 کاربر وب سازمانی • Redundant Hotswap Disks • پشتیبانی از مقیاس پذیری درونی بسیار بالا برروی NLB Array http://www.ironnetworks.com/products/nTMGE-3500E.asp

مدل nTMGE-5500E

nAppliance nTMGE-5500E ، یک Appliance در سطح Enterprise و یکپارچه سازی شده با TMG بر مبنای Microsoft Forefront Threat Management Gateway 2010 — Enterprise Edition (Corporate Data Center) می باشد

NetGateway nTMGE-5500E	
	• مناسب برای Very Large Sized Enterprise • پشتیبانی تا 4000 کامپیوتر و 20000 کاربر وب سازمانی • Redundant Hotswap Disks و ماژولهای Power Supply • پشتیبانی از مقیاس پذیری درونی بسیار بالا برروی NLB Array http://www.ironnetworks.com/products/nTMGE-5500E.asp



لیست محصولات nTMG Gateway

http://www.ironnetworks.com/products/NetGateway-nTMG-products

مدل NetGateway nTMG 1500S

nAppliance nTMG 1500S، یک Appliance یکپارچه سازی شده مبتنی بر Microsoft Forefront Threat Management Gateway 2010 — Enterprise Edition (Corporate Data Center)، در سطح Enterprise می باشد

NetGateway nTMG-1500S 	• مناسب برای Small Sized Business • پشتیبانی تا 500 کامپیوتر متصل شده و 2500 کاربر وب سازمانی • Redundant Hotswap Disks • قابلیت پشتیبانی از Large Network Port Density & Remote KVM http://www.ironnetworks.com/products/nTMG-1500S

مدل NetGateway nTMG 2500S

nAppliance nTMG 2500S یک Appliance در سطح Enterprise و یکپارچه سازی شده با TMG بر مبنای Microsoft Forefront Threat Management Gateway 2010 — Enterprise Edition (Corporate Data Center) می باشد.

NetGateway nTMG-2500S 	• مناسب برای Mid Sized Business • پشتیبانی تا 1000 کامپیوتر و 5000 کاربر وب سازمانی • Redundant Hotswap Disks • قابلیت پشتیبانی از Large Network Port Density & Remote KVM http://www.ironnetworks.com/products/nTMG-2500S

مدل NetGateway nTMG 3500S

NetGateway nTMG-3500S 	• مناسب برای Large Business • پشتیبانی تا 3000 کامپیوتر و 15000 کاربر وب سازمانی • Redundant Hotswap Disks • قابلیت پشتیبانی از Large Network Port Density & Remote KVM http://www.ironnetworks.com/products/nTMG-3500S

مدل NetGateway nTMG-5500S

NetGateway nTMG-5500S 	• مناسب برای Very Large Business • پشتیبانی تا 4000 کامپیوتر و 20000 کاربر وب سازمانی • Redundant Hotswap Disks و ماژولهای Power Supply • قابلیت پشتیبانی از Large Network Port Density & Remote KVM http://www.ironnetworks.com/products/nTMG-5500S

سناریوهای قابل پیاده سازی با Appliance های Microsoft TMG Standard (nTMG), TMG Enterprise (nTMGE), TMG Branch Office (nTMGB)

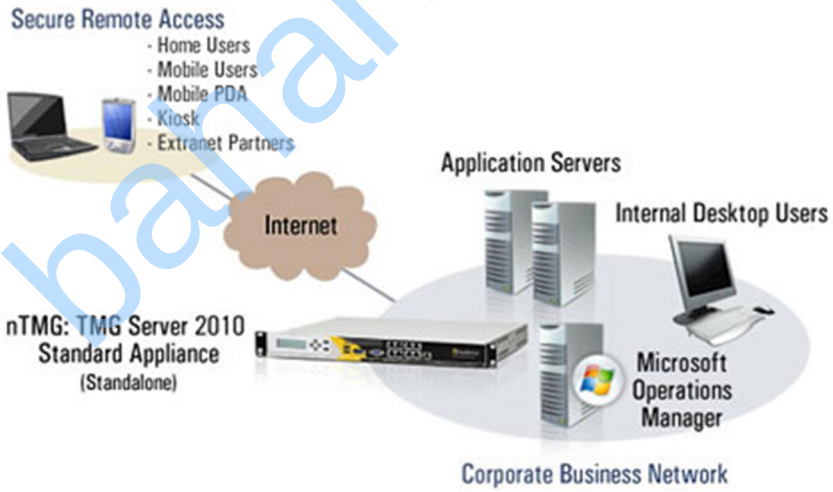
مروری بر قابلیتها

TMG Server 2010 Appliance (مدلهای nTMG یا nTMGE) ویژگیهایی را در جهت ایجاد، امنیت، کارایی، امکانات مدیریتی و کاهش هزینه های عملیاتی فراهم می سازد که از جمله مهمترین دغدغه های مدیران IT، مدیران شبکه و متخصصان امنیت اطلاعات محسوب میشوند. ویژگیهای TMG Server 2010 Appliance (مدلهای nTMG یا nTMGE) عبارتند از:

- دفاع در برابر تهدیدات داخلی و بیرونی تحت وب

TMG Server 2010 Appliance (مدلهای nTMG یا nTMGE) برای ارائه امنیت قویتر برای مدیریت و محافظت از شبکه های شما طراحی شده است.

Smaller Size Deployment (nTMG)



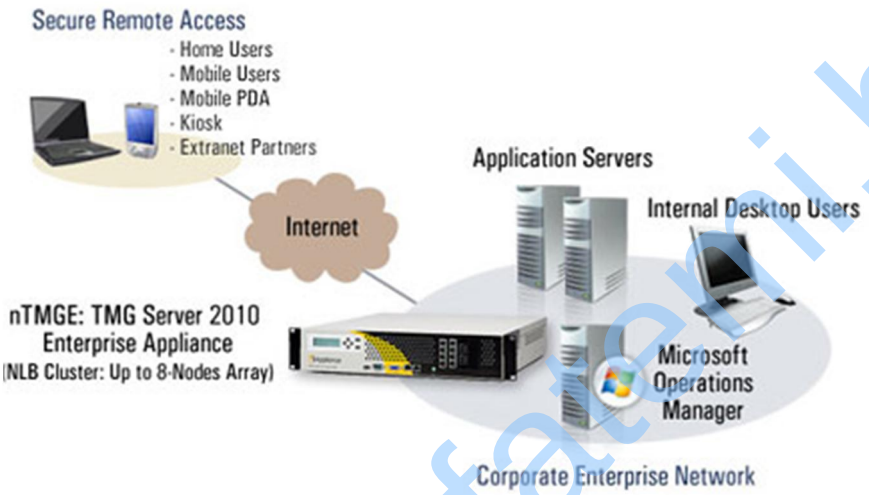
- نقطه ضعف (Fail-Over): از تنظیماتActive-Active Failover Appliance، برای ایجاد High Availability، پشتیبانی نمی کند.
- قیمت appliance: $4’000 برای یک مدل از سری 1500S
- مشخصات Performance

http://www.ironnetworks.com/products/nTMG-1500S

- نحوه پشتیبانی از Appliance های سری nTMG 1500S

http://www.ironnetworks.com/products/nTMG-1500S

Medium-Large Size Deployment (nTMGE)



- برمبنای TMG Server Appliance : مدلهای nTMGE
- مزایا (Fail-Over) : پشتیبانی از تنظیمات Active-Active Failover Appliance برای ایجاد High Availability، مقیاس پذیری نامحدود با استفاده از NLB Clustering
- قیمت appliance: $10’000 برای یک مدل از سری 1500E
- مشخصات Performance

http://www.ironnetworks.com/products/nTMGE-1500E.asp?quicktabs_4=1

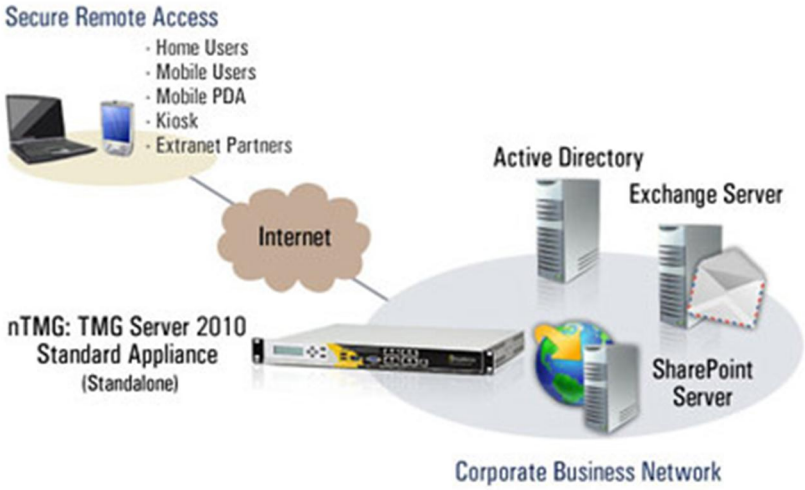
- نحوه پشتیبانی از Appliance های سری nTMGE

http://www.ironnetworks.com/products/nTMGE-1500E.asp?quicktabs_4=1

- **ایجاد امنیت کامل برروی محتوای Publish شده برای دسترسی ریموت**

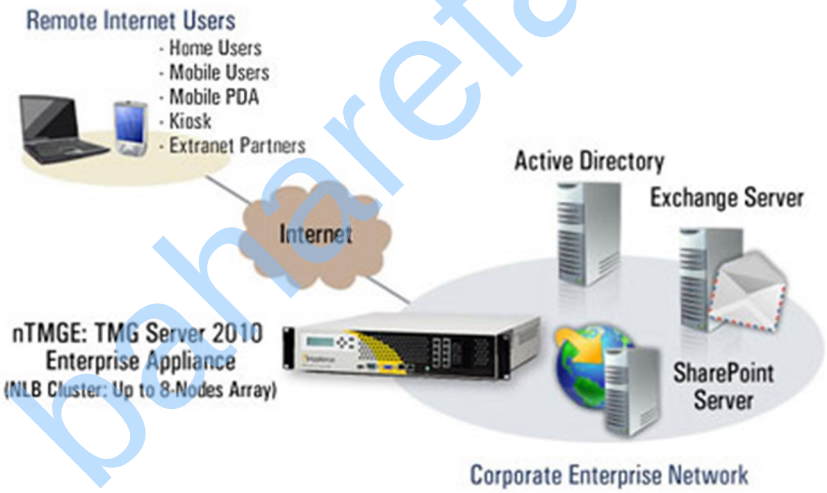
TMG Server 2010 Appliance (مدلهای nTMG یا nTMGE) ایجاد امنیت برروی Application های سازمان را که از طریق اینترنت، در دسترسی می باشند، ساده و موثر می سازد.

Smaller Size Deployment (nTMG)



- TMG Server Appliance Series : سری های nTMG
- نوع کلاینت: PPTP/L2TP /Windows VPN Client
- نقطه ضعف (SSL/VPN): No-SSL VPN, NAC (End-Point Security) or Granular Resource Access Built-In
- نقطه ضعف (Fail-Over): از تنظیمات Active-Active Failover Appliance برای ایجاد High Availability پشتیبانی نمی کند
- قیمت Appliance : $4’000 برای یک مدل از سری 1500S

Medium-Large Size Deployment (nTMGE)

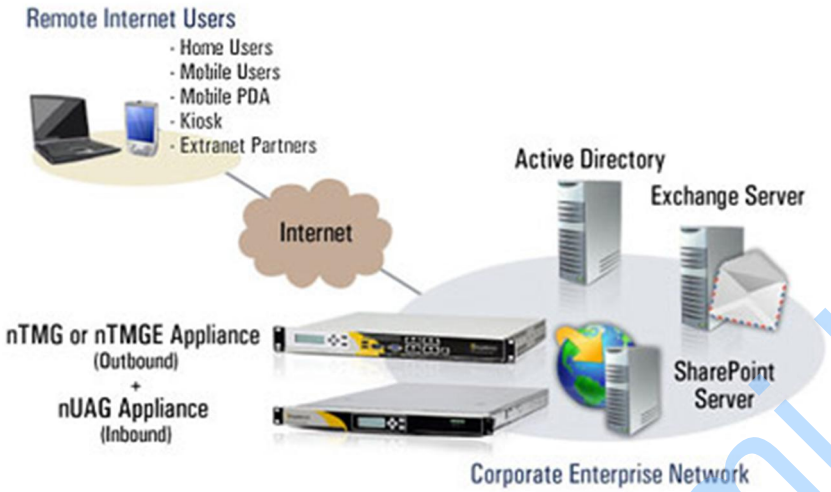


- **TMG Server Appliance Series :** سری های nTMGE
- **Client Type :** Windows VPN Client Built-In, PPTP/L2TP
- **معایب (SSL/VPN):**

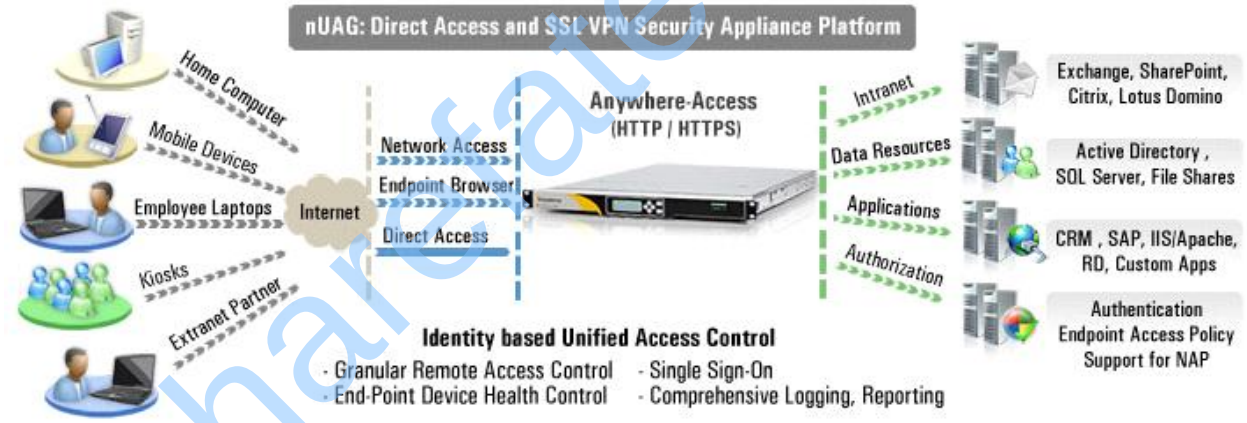
No-SSL VPN, NAC (End-Point Security) or Granular Resource Access Built-In

- **مزایای (Fail-Over):** پشتیبانی از تنظیمات Active-Active Failover Appliance برای ایجاد High Availability و مقیاس پذیری نامحدود از طریق NLB Clustering
- قیمت Appliance : $10’000 برای یک مدل از سری 1500E

Medium-Large Size Deployment (Additional nUAG Appliance)

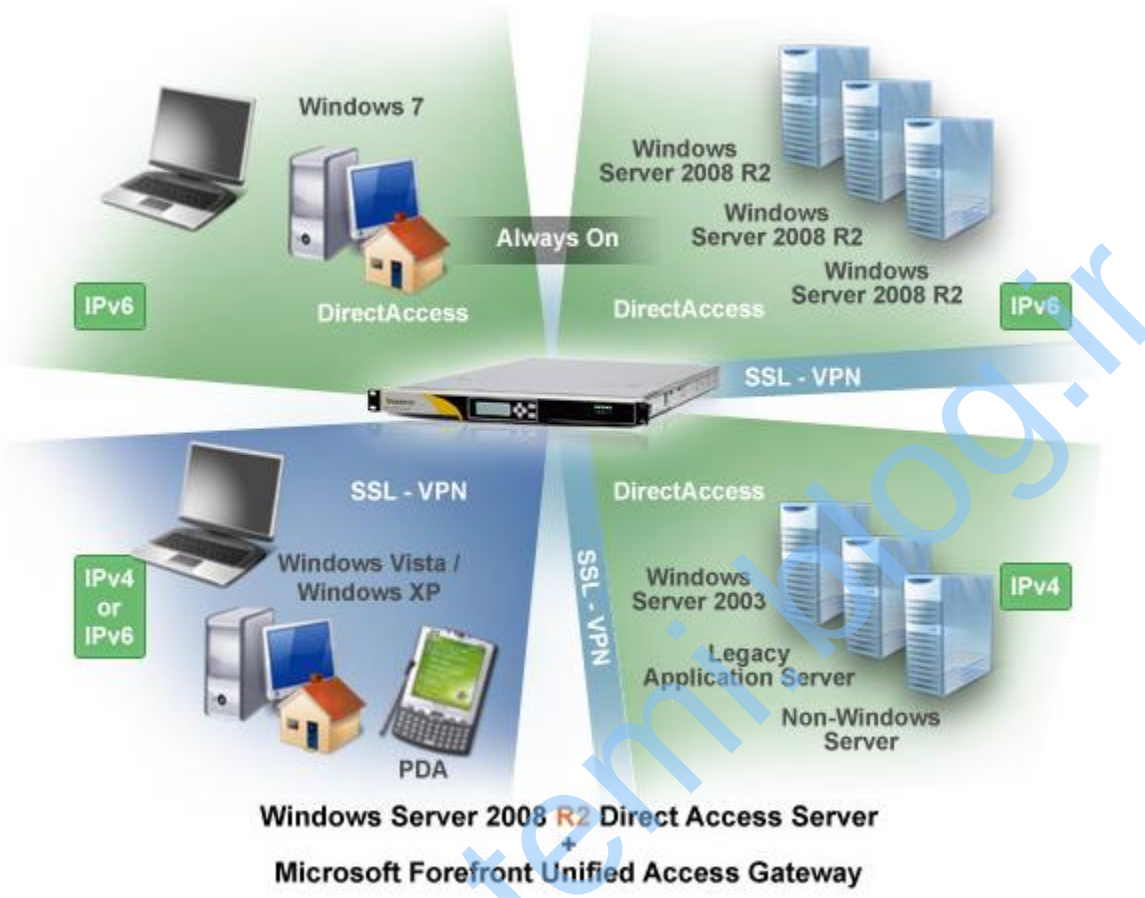


- **UAG Server Appliance Series :** سری های nUAG



- مزایای (SSL/VPN) : Clientless SSL VPN Access, NAC (End-Point Security) and Granular Resource Access Built-In
- مزایای (Fail-Over) : پشتیبانی از تنظیمات Active-Passive Failover Appliance، مقیاس پذیری نامحدود از طریق پشتیبانی از Clustering
- قیمت Appliance : نیاز به Appliance اختصاصی بیشتر، $5000 برای یک مدل از سری 1500U

توجه: UAG یک standalone appliance است و به عنوان یک option نرم افزاری افزوده شده به nTMG یا nTMGE که یک appliance package محسوب می شوند، موجود نمی باشد.



- برای مطالعه ویژگیهای سری Net-Gateway nUAG Remote Access Gateway به لینک زیر مراجعه کنید

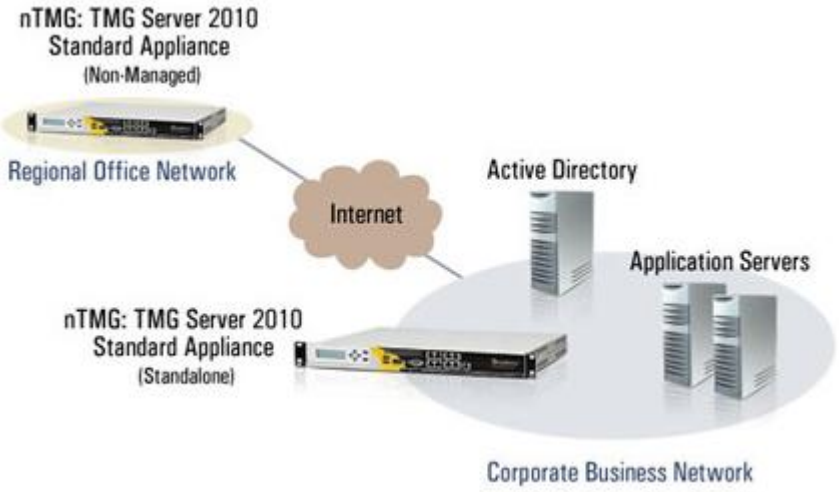
http://www.ironnetworks.com/products/NetGateway-nUAG

- **اتصال امن به Branch Office ها**

TMG Server 2010 Appliance (مدلهای nTMG یا nTMGE) یک شیوه قوی برای ایمن سازی شبکه های سازمان و کاهش هزینه های سازمانی را توسط اعمال نفوذ برروی اتصالات موجود، ارائه می دهد.

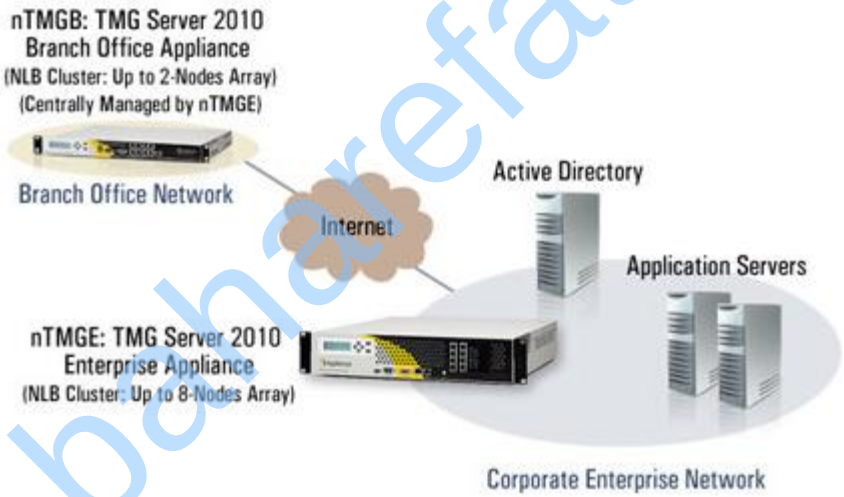
سازمانها می توانند از TMG Server 2010 Appliance (مدلهای nTMG یا nTMGE)، برای اتصال امن به Branch Office ها استفاده کنند در حالی که از پهنای باند شبکه نیز به صورت موثری استفاده می شود. ارائه ویژگیهای HTTP compression، caching of content (شامل software update ها) و قابلیتهای site-to-site virtual private network (VPN/IPSec) که با application-layer filtering یکپارچه شده اند، توسعه امن شبکه های سازمانی را ساده تر می سازد.

Smaller Size Deployment (nTMG)



- **نقطه ضعف (Policy-Management)**: بدون مدیریت متمرکز، مجموعه تنظیمات به صورت لوکالی برروی هر appliance ذخیره می شود و از طریق Export و Import کردن Policy ها به صورت دستی، مدیریت می شوند
- **نقطه ضعف (Fail-Over)**: از تنظیمات Active-Active Failover Appliance برای ایجاد High Availability پشتیبانی نمی کند.
- **قیمت appliance**: قیمت 2 appliance باهم : $8000 (4’000$x2) برای یک مدل از سری 1500S

Medium-Large Size Deployment (nTMGE)



- **مزایا (Policy-Management)** : مدیریت متمرکز Policy ها و توسعه آسان برروی تعداد زیادی branch office
- **مزایا (Fail-Over)**: پشتیبانی از تنظیمات Active-Active Failover Appliance برای ایجاد High Availability، Scalability نامحدود از طریق ایجاد NLB Clustering برروی هردو appliance های (Branch) nTMGE/B و nTMGE (Enterprise) appliance

- **قیمت Appliance:** به دو appliance نیاز می باشد. $10’000 برای یک مدل از هر سری 1500E (Corporate Data Center) و $5000 برای یک مدل از هر سری 1500B (Branch Office)، جمعا $15’000

جدول مقایسه ویژگی مدلهای TMG Server 2010 Standard Edition (nTMG Series), TMG Server 2010 Enterprise Edition (nTMGE Series) and TMG Server 2010 Branch Office Edition (nTMGB Series).

	Business Standalone	Corporate Datacenter	Corporate Branch Office
Microsoft Forefront Threat Management Gateway 2010	TMG Standard Edition	TMG Enterprise Edition	TMG Branch-Office Edition
Deployment Type:			
Business Type	SMB	Enterprise	Branch Office
nAppliance Net-Gateway Platform Series	nTMG Series	nTMGE Series	nTMGB Series
Supported deployment scenarios	Standalone	Server in a standalone array or an array managed by EMS*	Server in a standalone array or an array managed by EMS*
High Availability:			
NLB Arrays for Load Balancing & Failover	No	√	√
Scale Out: Number of Supported TMG Server in Array	1	Unlimited	2
Non-domain joined gateway	√	√	√
ISP Link redundancy	√	√	√

	Business Standalone	Corporate Datacenter	Corporate Branch Office
Unified Threat Management Functionalities:			
Firewall - Stateful	√	√	√
Firewall - Application Layer			
Network IPS (NIS)	√	√	√
VPN (site-to-site and remote access)	√	√	√
Web Proxy	√	√	√
Web Publishing	√	√	√
HTTPS inspection	√	√	√
Caching , Cache Compression	√	√	√
NLB Arrays for CARP Support		√	
Web Anti-Malware Protection**	√	√	√
E-mail Protection***	√	√	√
Configuration Storage Server (CSS)			
Local Management of Firewall Policies and Config Settings	√	√	√
Remote Management of Firewall Policies and Config Settings		√	

	Business Standalone	Corporate Datacenter	Corporate Branch Office
Enterprise Management: EMS for Centralized Management			
Management of Enterprise (nTMGE) Edition Gateways		√	
Management of Branch (nTMGB) Edition Gateways*			√
Management of Branch Standard (nTMG) Edition Gateway*	√		
Type of Microsoft Forefront TMG Editions	Standard	Enterprise (Datacenter)	Branch Office
Scale Up: Processor Support	Up to 4 CPU's	Unlimited	Up to 4 CPU's

* Requires at least one Enterprise Edition nTMGE appliance license, EMS: Enterprise Management Server

** Requires subscription;

*** Requires Exchange License

معرفی مدل nGSA (Gemalto Strong Two-Factor Authentication)

http://www.ironnetworks.com/products/NetGateway-nGSA

استفاده از دو فاکتور احراز هویت، می تواند یک لایه امنیتی قویتر اضافی را با استفاده از دو متد مختلف احراز هویت کاربران، برروی شبکه فراهم سازد، که این عبارتند از: استفاده از Username و Password و روشهایی مانند token، Software Application یا passcode. **nAppliance Gemalto Strong Authentication Server (nGSA)**، یک سرور یکپارچه سازی شده واحد است که از مجموعه گسترده ای از device های مورد استفاده توسط کاربران، و شیوه های احراز هویت مناسب برروی دسترسی های کاربران موبایل به منابع سازمانی پشتیبانی می کند این Option ها، شامل تکنولوژی

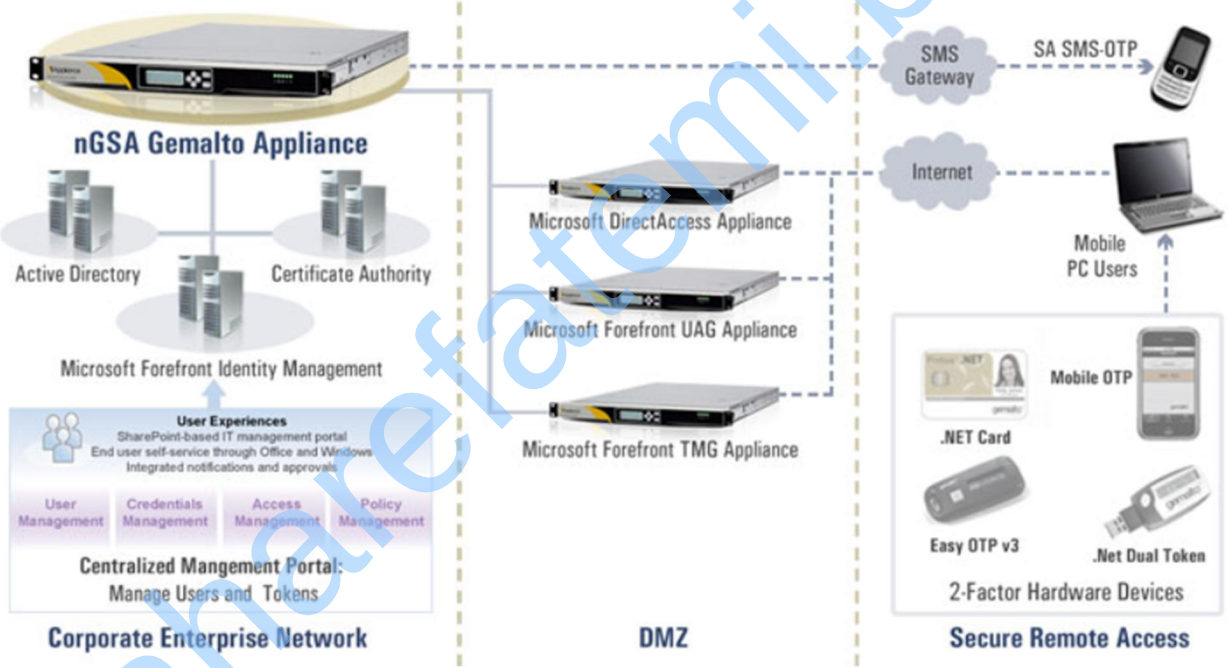
one-time password (OTP)، جهت پشتیبانی کامل از public key infrastructure (PKI) مبتنی بر smart card و نیز توسعه bio-metric می باشد.

Component های نرم افزاری nGSA Appliance

راهکار nGSA nAppliance، با تکنولوژیهای مختلف مایکروسافت و3rd party SSL VPN ، messaging، reporting و invoicing یکپارچه شده است

- **Microsoft Forefront Identity Manager Appliance (mFIM)**
- **Microsoft DirectAccess Networking Appliance (mDA)**
- **Microsoft Forefront UAG Security Appliances (mUAG)**
- **Microsoft Forefront TMG Security Appliances (mTMG)**

معماری توسعه nGSA, Microsoft DirectAccess & FIM Appliance



تمامی ویژگیهای nAppliance ها در یک نگاه