nAppliance NETWORKS

Net-Gateway nUAG Remote Access Series

Unified Access Gateway Appliance

Next-generation, highly-scalable, Microsoft Forefront powered unified remote access appliances with comprehensive application filtering, SSL VPN and DirectAccess capabilities for browser-based remote access, Identity based web portals, corporate-wide endpoint health compliance enforcement, granular policy control, single-sign-on and robust application publishing optimization

Comprehensive, secure access to corporate resources

Access anywhere

Empowers users to be productive from virtually any device or location

Forefront UAG acts as a consolidated gateway from a diverse range of endpoints and locations, providing access through a single portal. Remote users, including employees, partners, and customers, can access Web and non- Web applications and gain full VPN access to corporate networks including internal file shares and client server applications.

Simplifies secure remote access

Forefront UAG supports publishing a wide range of Microsoft applications, including Microsoft SharePoint®, Microsoft Exchange Server, Remote Desktop Services, and Microsoft Dynamics® CRM through predefined optimizer modules. These modules include optimum settings and rules for securing specific applications and are based on deep research into application behavior, browser–server interactions, and endpoint requirements. UAG also supports third-party applications such as CRM, ERP, and HR.

Administrators can publish the following types of applications using Forefront UAG:

- Web applications and Web farms via reverse proxy.
- RemoteApps through a Forefront UAG portal by using Remote Desktop Services (Terminal Services) with an integrated Remote Desktop Services Gateway.
- Non-Web applications over a secure connection using socket or port forwarding as well as VPN connections.

Extends Windows DirectAccess

Forefront UAG delivers DirectAccess to legacy applications and resources running on existing infrastructure and supports down-level and non-Windows clients through integrated SSL VPN capabilities and other connectivity options.

Integrated security

Enhances security and increases corporate compliance

- Limits exposure through a combination of granular access policies, deep endpoint health inspection, and user authorization information.
- Enables administrators to set up policies that specify prerequisites that endpoints must meet for each transaction. They can implement these using built-in Forefront UAG or Network Access Protection (NAP) policies downloaded from a Network Policy Server (NPS).

Enables a variety of strong authentication methods

- Integrates with Active Directory® and easily overlays a wide variety of third-party authentication solutions and repositories, allowing for strong authentication and enforcement through granular policies. This helps ensure that only authorized users or groups can access particular applications or execute transactions.
- Leverages credentials provided during a session to enable single sign-on to internal applications.

Simplified management

Reduces total cost of ownership by consolidating infrastructure

- Delivers remote access connectivity through a combination of VPN, SSL VPN, Web publishing, and DirectAccess. This enables organizations to standardize and consolidate a disparate infrastructure onto one cost-effective platform.

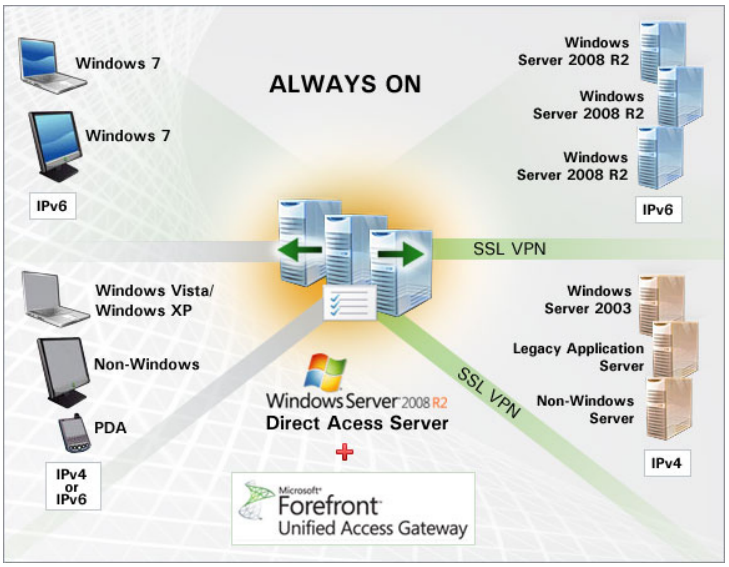
Simplifies deployment and ongoing management

- Facilitates the grouping of multiple Forefront UAG servers into an array. All array members share the same configuration and can be managed as a single entity.
- Uses wizards to simplify initial deployment and key ongoing tasks.
- Easily integrates Forefront UAG logging through Microsoft SQL Server® and management through System Center Operations Manager.

Product Highlights:

- Anywhere, secure remote access to corporate resources for employees, partners, and customers from both managed and unmanaged PCs and mobile devices
- Easy access to messaging, collaboration, and other resources, increasing productivity while maintaining compliance with policy
- A single, centralized and easy solution for administrators to deliver access and implement granular policies based on the user's identity and the health of the device increases internet access protection with resiliency
- Unlimited system scalability and high availability support thru built-in NLB clustering options
- Choice of Five purpose-built "Turn-Key" appliance platforms, component-level redundancy, scalable architecture built using multi-core 64-bit architect, LOM – remote out-of-band system management, crypto accelerators for application peak performance at full load and high port density for non-stop network performance, throughput and redundancy
- Easy field maintenance, embedded PiT online image recovery, restore and factory reset
- Powered by Microsoft Forefront Unified Access Gateway (UAG) 2010 on Hardened Windows Server 2008 R2 offers seamless IT-Infrastructure integration
- Worldwide appliance maintenance and support services

UAG and DirectAccess Technology Benefits:

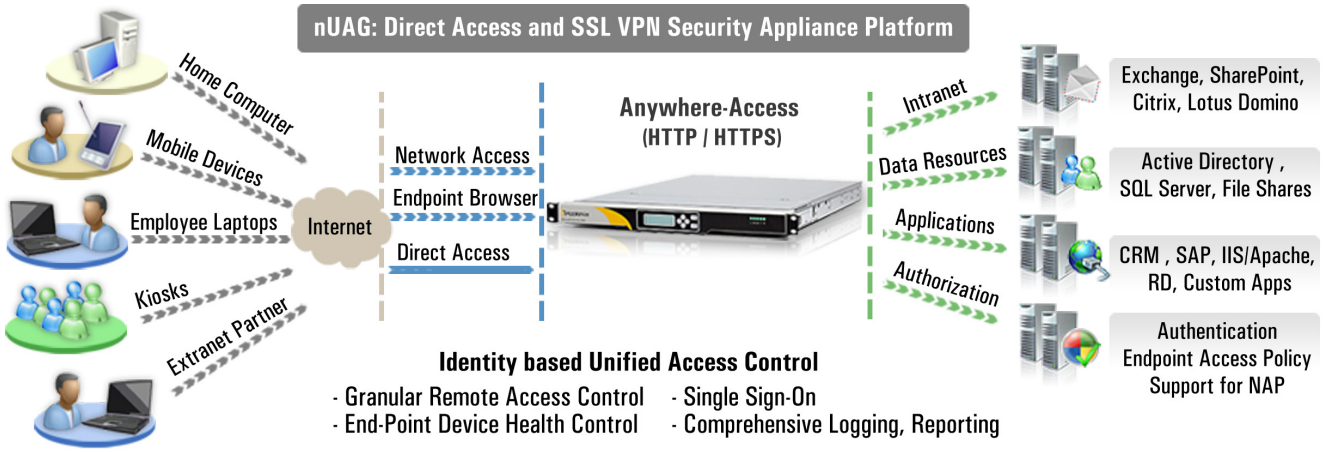


UAG takes DirectAccess deployments to a new level

DirectAccess technology enables mobile workers connect seamlessly and more securely to their corporate network file share, intranet web sites, and line-of-business application thru an internet connection –without the need to VPN. It helps:

- Extend access to line of business servers with IPv4 support such as Windows 2003 and non-Windows servers.
- Provide SSL VPN access for down level (Vista/XP) and non-Windows clients as well as PDAs.
- Enhance scale and management through array management capabilities and integrated load balancing.
- Simplify deployment and adinistration using wizards and automated tools.
- Deliver a hardened, edge-ready, solution that can swiftly be deployed.

nUAG Deployment: Unified Remote Security Delivery Infrastructure



Net-Gateway nUAG Remote Access Appliance Features

High Availability, Scalability and Array Management	
High Scalability and Reliability	Scales linearly using Microsoft built-in NLB array technology for high-availability and failover
Network Access Manageability	
Configuration Flexibility	Standard configurations for widely-deployed enterprise applications, and extensive customization capabilities.
Comprehensive Policy	Framework Standard application access settings and endpoint policy configurations ensure minimal integration overhead and low ongoing management costs.
Logging and Reporting	Supports monitoring, logging, reporting for management and accounting.
Network End-Point Access Controls	
Endpoint Compliance Checks	Endpoint policy allows administrators to define compliance checks according to standard variables including presence of security software and UAG-specific components such as Attachment Wiper.
End-User Experience	Delivers a standard SSL VPN portal and log in pages for easy set up, customization and low administrative overhead.
Certificate Management	Built-in certificate authority enables administrators to grant a user a trusted endpoint certificate for a specific machine on request.
Endpoint access policies	Provides endpoint policies using built-in Forefront UAG polices, or with Network Access Protection (NAP) policies downloaded from a Network Policy Server (NPS)
Remote Connectivity Options	
Extensive Remote Connectivity Options	•DirectAccess: Extend the benefits of DirectAccess across the infrastructure, enhances scalability, and simplified deployment and ongoing management •Client/Server Connector provides out-of-the-box secure access to client/server applications including Microsoft Exchange, Lotus Notes native client, Citrix, Microsoft Terminal Services, FTP and Telnet •Multiple tunneling modes including Port and Forwarding •Network Connector allows administrators to install, run and manage remote connections that give users full network-layer connectivity over a security-enabled transparent connection. Extends remote users the same functionality, if they were connected to the corporate network.

Features and Benefits

- All-in-One Unified Remote Access Gateway Appliance. A single device which provides remote anywhere access to corporate resources, integrated security with granular access control and centralized management for business and enterprises of all sizes.
- Application Optimizers. Multiple Intelligent Application Optimizers for secure publishing, integrated software modules with pre-configured settings designed for secure remote access to widely used Microsoft and non-Microsoft line of business applications such as:
- Exchange Outlook Web Access, Shared Point Portal, Microsoft Dynamics CRM, RD Terminal Services
- Lotus Domino Web Access, IBM Web Sphere, SAP Portals
- Endpoint, NAC Security Management. Endpoint security management and verification ensures endpoint health, compliance, session control, single-sign-on. Helps meet corporate information usage guidelines through client-side cleanup
- Centralized Policy Based Access Control. Centralizes policy management, controlling access by protocol or application type and by user, group, roles, schedules, content type tied to Active Directory
- Easy Windows MMC based Manageability. Offers industry most advance feature and familiar windows interface
- Future-Proof, Lowest Total Cost of Ownership. Exceptional ease of implementation enables IT leaders to be confident that their network, users, client devices, and application are protected with the leading Microsoft Forefront security appliance family celebrated for assured performance and lowest TCO
- Centralized Appliance Management through ONEface™. nAppliance Intuitive system management tools provide local and remote appliance configuration, upgrades, health monitoring, event logging, reporting and call home functionality
- Embedded Appliance Field Recovery. nAppliance embedded ARRMS™ recovery system combined with advanced LCD functionality offers easy network setup and configuration, appliance image recovery/backup/restore, and advance remote lights-out-management (LOM) based Out-of-Band appliance manageability
- Superior Forefront Product Technology, Value and Support. Enjoy state of the art system and application integration, best price-to-performance-ratios in the industry, deployment assistance for Microsoft TMG and UAG technologies, global technical support, efficient appliance life cycle management and upgrades, and above all future proofing with Microsoft Forefront Security Architecture.

nAppliance NETWORKS

Microsoft Forefront Unified Access Gateway

RSA The Security Division of EMC

nAppliance Networks, Inc.
540 Dado Street, San Jose, CA 95131, USA
Phone: 1-408-895-5000 (Local) 1-877-895-nAPP (6277) (US-Toll Free) 011-408-895-5000 (International)
Fax: 1-408-943-8222/8101 Email: info@nappliance.com Website: http//www.nappliance.com

nAppliance NETWORKS

nAppliance Forefront Appliance Platform
Featuring Microsoft Forefront Edge Security

Forefront Appliance Platform

nAppliance appliance platforms are purpose-built, high performance hardware devices and a set of custom-nAppliance designed system management tools which form the foundation of our Microsoft powered "Turn-Key" Forefront edge security system solutions.

Comprehensive, secure remote access to corporate resources

Microsoft Forefront Security Hardened Appliances Platforms built for Network Edge Security Services

Our appliance platforms are designed for organizations that want an integrated leading edge hardware security software service offering from Microsoft on an optimized hardware platform. It offers best-of-breed Microsoft Forefront Edge security service software packaged with nAppliances pre-configured, security hardened and support solution with virtually no maintenance.

nAppliance power of it system and hardware management software provides a complete plug and play solution for Microsoft Forefront Threat Management Gateway (TMG) and Universal Access Gateway (UAG) edge security software suites. Our standard business edition appliances are deployed as a standalone device and enterprise edition appliances can be deployed as a standalone device or high-availability (HA) with network load balancing (NLB) for optimal service resiliency.

Purpose-Built: Scalable family of Network Security Appliance Platforms for business of all sizes

nAppliance offers a wide range of hardware configurations, each of the models are pre-configured with most optimized hardware components and system management tools to meet our customers unique business requirements. Configures are fine tuned to deliver various levels of system performance, capacity, scalability and availability required to meet the requirements of small to large size business, small to large size enterprise and branch offices.

nAppliance running Microsoft Forefront Edge Security systems provide the security and management benefits of special purpose hardware products, and provide the familiar management interfaces of other Microsoft technologies. Security appliances often have special purpose hardware specific to network security. Appliance products running Microsoft Embedded Edge Security technologies have the following unique advantages:

Appliance Advantage: Security Hardened Configuration for "Out-Of-the-Box" Experience

Each security appliance has various software and hardware components installed and integrated. This configuration is then carefully tuned and hardened to maximize the security posture of each system. This hardening is exhaustive, costly and difficult to provide in general IT hardware and only software implementations, but imperative on edge security devices.

nAppliance has the lowest total cost of ownership as compared to traditional software alternatives. The nAppliance appliance-based architecture eliminates many of the costs of traditional systems management including software and hardware procurement, installation, off-site training, and the resources required for ongoing upgrades, system maintenance and technical support. Our appliance advantage offer security hardened configuration for "Out-Of-the-Box" experience.

Product Highlights:

Hardware Platform Advantage: Advance Appliance System Configuration for Maximum Performance

- **Multi-Core 64-bit architecture for high-performance network security:** nAppliance appliance design includes multi-core x86 architecture, high-speed processor cache, larger memory and multi lane PCIe bandwidth, designs for maximized performance, scalability and reduced power consumption. It provides accelerated deep packet inspection and content protection against ever evolving complex attack in real time from both inside and outside the network perimeter.
- **Enterprise grade high availability:** nAppliance appliances take system fault tolerance and failover to new level for core network security service appliances. Our appliances offer:
  - Hardware availability thru components level redundancy of disks, power supply and fans.
  - Windows operating system availability through system image redundancy and online PiT snapshot recovery system.
  - Network level system availability thru network load balancing and fail-over systems.
- **High Copper and Fiber network port density:** The high port-density Gigabit Ethernet interfaces provide the performance and operational flexibility and redundancy required to secure a high-availability network infrastructure, along with economies of scale needed by large, enterprise, data centers, and service providers.
- **Embedded high performance SSL acceleration hardware for 100% TCP/IP Offload:** High performance hardware SSL acceleration co-processor from Cavium helps reduce CPU workload and provides following benefits:
  - Shorter response time delay: The reduction in CPU load results in reduced delay for each of the individual clients.
  - Increased burst rate thru faster SSL handshake: It can support 100's of new concurrent logins per second. It provides significant burst rate performance gain and system stability over software-only solutions.
  - Increased Peak Time Performance: Reduced CPU workload helps increases the number of transaction each of the appliance system can process.
  - Increased Security: Server private keys are stored in write-only flash devices embedded into the Cavium processors as oppose to storing it on hard disk drives, making unauthorized access more difficult.
- **HSM certificate management:** HSM hardware provides a certificate repository and generation facility. Certificates can be compromised if a system is compromised, unless the certificates are generated and stored in these special hardware components.
- **Integrated security audits:** nAppliance appliance systems are built, packaged and receives a complete security audit on completed system by our security system experts. Various software add-ons, hardware components and system configurations will change a system profile; each of configuration is tested and audited for security and reliability on ongoing basis.

nAppliance Forefront Powered Appliance Platform Advantage

Microsoft Forefront Edge Security Software Optimized Platforms

Oneface Windows System Manager
- Centralized management system.
- Backup Manager, Update Manager, HW Fail-Over Manager, Configuration and Alert Manager
- SNMP based real-time system enviornment and health monitoring

Packaged Microsoft Forefront Edge Security Suite
- Platform Optimization: Pre-installed, pre-tested and certified.
- Security Audit: Pre-hardened security policies
- Microsoft Embedded Windows Server 2008 R2 and Forefront Gateway Security Optimized

Reliable, Non-Stop System Availability
- Enterprise Grade, higher MTBF Parts
- Redundant Disks, Fans and PS
- Redundant OS Image on Disk
- Remote Lights-Out (LOM) based Out-of-Band management
- Flash based Embedded ARRMS technology for bare-metal recovery
- Standalone or HA/NLB configurations

Oneface Embedded Recovery Manager
- nAppliance designed Appliance Recovery and Remote Managment System (ARRMS) technology
- Failure-proof in-field hardware image maintenance services for easy appliance PiT Online Recovery, Backup, Restore and Factory Reset

Scalable, High Performance Hardware
- Multi-Core 64-bit architecture
- Large LAN port density, higher throughput and redundancy
- SSL HW Accelerator, 100% CPU Offload
- HSM Certified HW and Management
- High capacity, Enterprise performance, Redundant SATA and SAS disks

Oneface Embedded LOM Manager
Remote Appliance HW Management
- Lights-Out iKVM (IPMI) support for BIOS level access using standard web browser over internet

Appliance Support, Services and Accountability
- Help Desk Options include Silver, Gold and Platinum 24x7 Support Plans
- Forefront certified expert support via web, email and phone
- Advance Hardware Replacement
- Microsoft Forefront OEM Partnership
- Support service centers in USA, Europe & Asia

Custom-Tailored , Multiple Configurations
- Entery Level: Model -500 provides low cost small business solution
- Business Class: Model-1500 and 2500 provide entry level SMB or small enterprise or branch office solutions
- Enterprise: Model-3500 and 5500 are best suited for large enterprise and branch offices

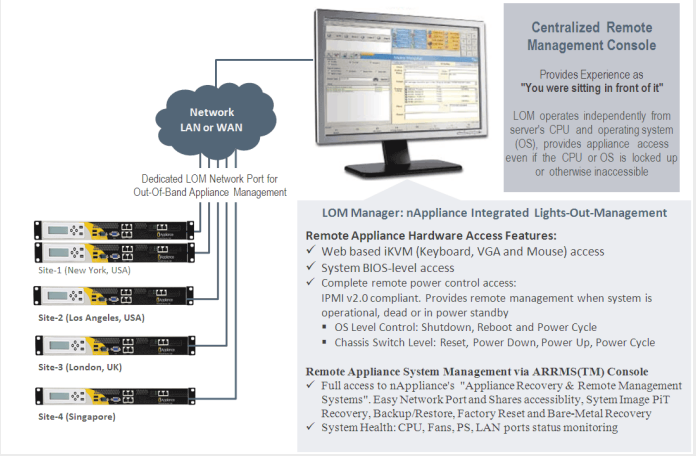
Oneface Embedded LCD Manager
- Graphical LCD for easy headless deploymnet and field-maintenance

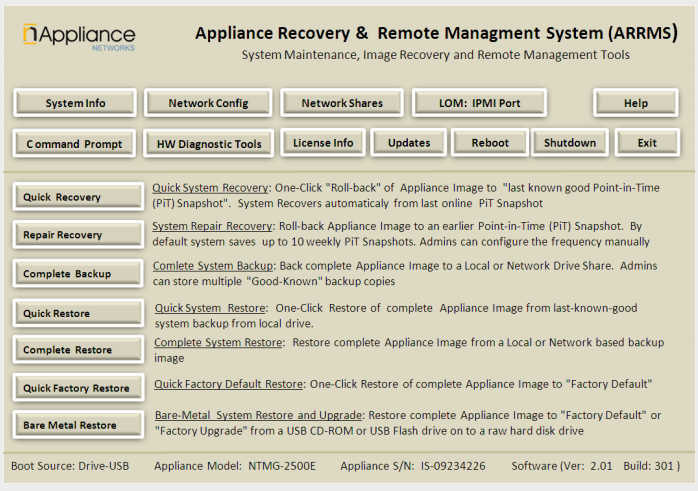
Oneface System Managment Tools

Net-Gateway - Purpose Built Appliance Hardware Platforms

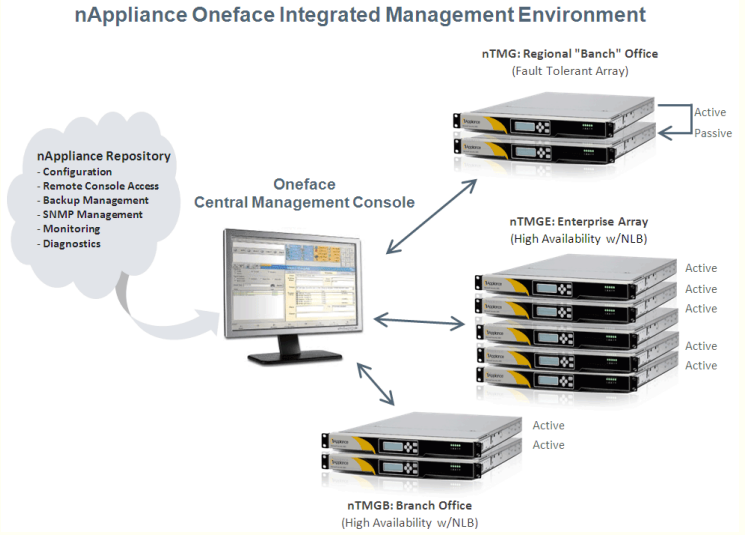
Worldwide Support Coverage - Forefront TMG and UAG Sales, Help Desk and Warranty Services

LOM Manager: Embedded Lights-Out-Management System





Features and Benefits



Oneface Appliance System Manager

Data The nAppliance nUAG 3500U is an enterprise grade, comprehensive, secure remote access management gateway appliance based on embedded version of Microsoft Forefront Unified Access Gateway 2010 Data The nAppliance nUAG 3500U is an enterprise grade, comprehensive, secure remote access management gateway appliance based on embedded version of Microsoft Forefront Unified Access Gateway 2010
Data The nAppliance nUAG 3500U is an enterprise grade, comprehensive, secure remote access management gateway appliance based on embedded version of Microsoft Forefront Unified Access Gateway 2010

Data The nAppliance nUAG 3500U is an enterprise grade, comprehensive, secure remote access management gateway appliance based on embedded version of Microsoft Forefront Unified Access Gateway 2010

nAppliance Networks, Inc.
540 Dado Street, San Jose, CA 95131, USA
Phone: 1-408-895-5000 (Local) 1-877-895-nAPP (6277) (US-Toll Free) 011-408-895-5000 (International)
Fax: 1-408-943-8222/8101 **Email:** *info@nappliance.com* **Website:** *http//www.nappliance.com*

nAppliance
application protection & acceleration

Net-Gateway nUAG: Remote Access SSL VPN Series
Microsoft Forefront Powered Universal Access Gateway Appliances

Compare Product Specifications




Models: nUAG (Product Specifications)	1500U	2500U	3500U	5500U
Deployment Type (Business / Enterprise)*	Small, Medium	Medium	Large	Very Large
Recommended Named Users for Appliance (1:2)*	1,000	2,000	10,000	15,000
System Performance				
Concurrent Users (Low Activity Usage, < 5 Apps)	600	1,200	5,000	7,500
Concurrent Users (Medium Activity Usage, 5-10 Apps)	400	800	3,000	5,000
Concurrent Users (High Activity Usage, 11-20 Apps)	150	300	1,200	2,000
Concurrent Users (Power Usage, 20+ Apps)	100	150	700	1,000
Burst Mode: Concurrent New User Login / Minute	90	100	200	350
Burst Mode: Concurrent New User Login < 3 minutes	250	250	500	1,000
High Availability & Scalability				
Internal: HA via Microsoft Windows NLB	Yes	Yes	Yes	Yes
External: HA via 3rd Party Load Balancer (High Scalability)	Yes	Yes	Yes	Yes
Hardware Specifications				
Network Ports: LAN PCIe (RJ45)	(7) 6 - GbE (Rear) LAN + 1 - iKVM	(9) 8 - GbE (Rear) LAN + 1 - iKVM	(9) 8 - GbE (Rear) LAN + 1 - iKVM	(9) 8 - GbE (Rear) LAN + 1 - iKVM
Lights Out Remote Management (iLOM)	Yes (KVM over IP & KVM over Web)	Yes (KVM over IP & KVM over Web)	Yes (KVM over IP & KVM over Web)	Yes (KVM over IP & KVM over Web)
Hardware Crypto Accelerator CPU-Off-Load (Cavium)	No	Yes, 64-bit PCIe	Yes, 64-bit PCIe	Yes, 64-bit PCIe
TPS Throughput: SSL	Software Only	17,000	17,000	17,000
CPU-Qty / Core Type	(1) Intel Core-i3	(1) Intel Xeon X3430	(1) Intel Xeon E5520	(2) Intel Xeon E5520
CPU Cores / Cache	2 / 4MB	4 / 8MB	4 / 8MB	4 / 8MB
Memory-RAM	4 GB DDR3 ECC	8 GB DDR3 ECC	12 GB DDR3 ECC	16 GB DDR3 ECC
Hard Disk: System OS	(2) 3.5" Internal	(2) 3.5" Internal	(2) 2.5" Hotswap, Front	(3) 2.5" Hotswap, Front
Disk- Qty / Type	500 GB, SATA2 Enterprise	500 GB, SATA2 Enterprise	300 GB, SATA2 Enterprise	300 GB, SAS Enterprise
Disk-Mirror Hardware RAID	Yes, SATA2 RAID-1	Yes, SATA2 RAID-1	Yes, SATA2 RAID-1	Yes, SAS RAID-1 (512MB Cache + Battery Backup)
Disk: Spares	No	No	Yes, Optional	Yes, Included
Flash Disk: Appliance Recovery OS				
ARM / FFRS**: Flash based Field Recovery System	Yes	Yes	Yes	Yes
LCD Interface w/6-Keypad	No	Yes, Graphical	Yes, Graphical	Yes, Graphical
Power Supply Module	Single	Single	Dual, Hotswap	Dual, Hotswap
Power: Univeral 110-120V	260 Watts	260 Watts	2 x 650 Watts	2 x 650 Watts
Ports (USB / RS232 / VGA)	2 / 1 / 1	2 / 1 / 1	2 / 1 / 1	2 / 1 / 1
Form-Factor	1U 2-Post	1U 2-Post	1U Rackmount 4-Post	1U Rackmount 4-Post
Dimensions (H x W x D)-inch	1.75 x 17 x 14 (Short Depth)	1.75 x 17 x 14 (Short Depth)	1.75 x 17 x 27	1.75 x 17 x 27
Appliance Management: Value Add Features by nAppliance				
LCD Console Manager				
Headless Appliance Configuration and Maintenance	Yes	Yes	Yes	Yes
ONEface: Appliance System Manager				
Web-Based Appliance Setup and Management	Yes	Yes	Yes	Yes
Automatic Software Updates (from nAppliance)	Yes	Yes	Yes	Yes
ARRMS: Embedded Recovery Manager**				
Quick Recovery - One Click PiT Online/Offline Image Roll-Back	Yes	Yes	Yes	Yes
Complete Backup / Recovery from Local and Network Drives	Yes	Yes	Yes	Yes
Restore Image to any Last Good Known State	Yes	Yes	Yes	Yes
Quick Factory Retore to Factory Default Image	Yes	Yes	Yes	Yes
Baremetal System Retore and Upgrade	Yes	Yes	Yes	Yes
LOM (Lights Out) Appliance Manger				
IPMI based, BIOS Level Out of Band Management	Yes	Yes	Yes	Yes
Lights-Out-Manager: Client-Based, CLI	Yes	Yes	Yes	Yes
Lights-Out-Manager: iKVM over https (Web Based)	Yes	Yes	Yes	Yes
Centralized Multi-Appliance Management Option	Yes	Yes	Yes	Yes
ONEface based Health Monitoring, SNMP Traps	Yes	Yes	Yes	Yes
Forefront Management: Microsoft Built-In Support				
Microsoft UAG System Manager				
UAG System Manager	Yes	Yes	Yes	Yes
Operational Management				
Automatic Software Updates (from Microsoft)	Yes	Yes	Yes	Yes
SCOM: Microsoft System Center Operation Manager	Yes	Yes	Yes	Yes
Microsoft Licensing Provision & Coverage				
Appliance System Software				
Appliance Windows System Software, Included				
Hardened Microsoft Embedded Operating System	Windows Server 2008 R2, 64 bit	Windows Server 2008 R2, 64 bit	Windows Server 2008 R2, 64 bit	Windows Server 2008 R2, 64 bit
Microsoft Forefront Edge Security Suite, Included				
Forefront UAG 2010 Edition	Yes, Single Processor License	Yes, Single Processor License	Yes, Single Processor License	Yes, Two Processor License
Microsoft License: User / CAL Required	Yes, 10 CALs bundeled	Yes, 10 CALs bundeled	Yes, 10 CALs bundeled	Yes, 10 CALs bundeled
nAppliance Warranty: Standard Service and Support				
Standard: Express Replacement, 30 Days	Yes	Yes	Yes	Yes
Standard: Help Desk Support, 30 Days	Yes	Yes	Yes	Yes
Standard: Hardware Depot Repair - 1 Year	Yes	Yes	Yes	Yes
Upgrade: Hardware Express Replacement - Multi-Year	Optional	Optional	Optional	Optional
Upgrade: Help Desk Support - Multi-Year	Optional	Optional	Optional	Optional
Pricing (MSRP) - USA				
nUAG: Price w / 10 CAL Users Bundeled				

Ver 1.0

** Performance Guidelines Only, Actual performance may vary depending upon networkking and application environment.*

nAppliance Networks, Inc. 540 Dado Street, San Jose, CA 95131, USA
Phone: 1-408-895-5000 (Local) 1-877-895-nAPP (6277) (US-Toll Free) 001-408-895-5000 (International)
Fax: 1-408-943-8222/8101 Email: info@nappliance.com Website: http//www.nappliance.com