信安世纪 infosec

NetOpti Series Application Delivery Controllers

DATASHEET

信安世纪 infosec

NetOpti Series next-gen ADCs optimize the availability, performance and security of cloud services and enterprise applications while reducing cost and complexity in the data center.

NetOpti Series next-generation application delivery controllers (ADCs) cost-effectively drive industry-leading performance across a robust set of availability, acceleration and security features to deliver unmatched overall value. Available as high-performance appliances that feature the latest in hardware acceleration and energy-efficient components or as agile virtual appliances that enable flexible pay-as-you-go business models, NetOpti Series ADCs are engineered to boost application performance in modern data center, cloud and virtual environments and speed ROI for service provider, enterprise and public sector organizations.

Highlights And Benefits

- Dedicated appliances from 10 Gbpsto 200 Gbps and virtual appliances with support for one to eight vCPUs to scale- up and scale-out as needed; also available on popular public cloud marketplaces such asAWS and Azure
- Integrated Layer-4 to Layer-7 server load balancing, link load balancing, global server load balancing, connection multiplexing, caching, compression, traffic shaping, DDoS protection, IPv6 and web application security
- High-performance, kernel-level Layer-7 policy engine to enable customizable application traffic management without impacting performance orscalability
- Multi-layered security, first line of defense includes hardened OS, kernel-level web firewall, forward- or reverse-proxy, DDoS protection for guarding applications without compromising performance
- Secure Application Access to authenticate and authorize user access to diverse web and other non web applications via flexible integration with local Auth, SAML, LDAP, RADIUS or OAuth for Single Sign-On
- Built-in SSL/TLS accelerator to offload SSL/TLS encryption/decryption from web and application servers for increased efficiency, capacity and return on investment (ROI)
- SSL intercept (SSLi) decrypts/encrypts SSL traffic to enable observability and enforcement for Infosec and 3rd-party security services
- Industry-leading SSL/TLS throughput and TPS (ECC/RSA) with unmatched price-performance and rich certificate management features
- Intelligent ISP link load balancing improves availability and performance, and enables cost-effective link utilization
- Enables 5-nines application availability and accelerates application performance by up to 5x
- Application-specific certifications, guides and policies for rapid deployment and accelerated delivery of business-critical enterprise applications
- ePolicy™ L7 application scripting and eRoute™ L4 routing for custom control of application traffic
- IPv6 gold certification for IPv4 preservation, IPv4/6 translation and IPv6 migration
- InfoseceCloud™ RESTful API and XML-RPC for seamless interaction with cloud management systems and 3rd-party monitoring solutions
- Integration with VMware Aria Suite Orchestrator and Microsoft System Center, as well as OpenStack for load balancing-as-a-service (LBaaS)
- Space-efficient, redundant-power hardware appliances that consume 10-35% less power versus alternative solutions
- Familiar CLI, intuitive cloud-friendly WebUI and centralized management for ease of use and configuration

Features

Server Load Balancing

NetOpti Series application delivery controllers ensure 99.999% availability for cloud services and enterprise applications. Leveraging robust distribution algorithms, health check mechanisms, clustering and failover capabilities, NetOpti Series appliances maintain connections, ensure persistence, direct traffic away from failed servers and intelligently distribute application services across multiple servers for optimized performance and availability. NetOpti Series can load balance traffic for a wide variety of protocols at Layers 2, 3, 4 and 7, including WebSocket and WebSocket Secure.

Layer-7 Policy Engine

Customized traffic management is often a trade-off between performance, control and ease-of-use. Unlike ADCs that rely on complex, compute-intensive scripting to enable custom Layer-7 policies, Infosec supports a vast library of policies that are hard-coded atthe kernel level, are configurable with point-and-click simplicity via the WebUI or CLI, and can be combined and nested to create advanced customized application traffic management. With Infosec's unique approach to Layer-7 traffic management, customers get the best of all worlds: ease of use, granular control and superior performance and scalability.

SSL/TLS Acceleration & Offloading

The majority of internet traffic is now protected by SSL/TLS encryption, which ensures data privacy and integrity; however, SSL/TLS comes with a cost in terms of processing compute-intensive 2048-bit encryption. Infosec SSL offloading reduces the number of servers required for secure applications, improves server efficiency and dramatically improves application performance. The NetOpti Series also simplifies SSL certificate/key management to enable intelligent content management and routing.

In addition, the NetOpti Series provides SSL acceleration to offload compute-intensive key exchange and bulk encryption, and delivers industry-leading client-certificate performance. SSL acceleration is ideal for scaling secure SaaS offerings, e-commerce environments, and business-critical applications that require high-volume secure connectivity.

TheNetOpti Series' SSL/TLS engine includes advanced security to minimize the possibility of attacks, thus further enhancing the security of applications and servers. For example, if an SSL renegotiation attack is detected, the NetOpti Series can disable SSL renegotiation or enable rate limiting. Secure SSL renegotiation is also supported. In addition, some applications may support only SSL 3.0 or TLS 1.x, which have proven to be vulnerable to attacks. The NetOpti Series can bridge from current SSL/TLS versions to provide improved client-side security without requiring changes to the server or application.

NetOpti Series SSL/TLS processing is performed in hardware to provide high performance and capacity, as well as industry-leading TCO.

SSL Intercept

SSL-encrypted data traffic is increasing rapidly, which can place data centers and enterprises at risk – in many cases, encrypted traffic cannot be inspected by security appliances such as firewalls, IDS/IPS, data loss prevention and deep packet inspection, thus bypassing these important security measures.

Infosec's SSL Intercept capability decrypts SSL traffic, allowing 3rd-party appliances to inspect them fully, then re-encrypts before forwarding the traffic to its destination. Flexible deployment options include L2 or L3 mode, integrated or distributed mode, forward or reverse proxy, and load balancing across multiple 3rd-party security appliances. In addition, anNetOpti Series ADC can operate as a Webagent service to implement explicit forward proxy mode for additional security.

As an option, the Webroot BrightCloud Threat Intelligence Service is available for the NetOpti Series. BrightCloud includes reputation services that protect users from malicious sites, as well as a web classification service to allow blacklisting of inappropriate sites and/or whitelisting of sites for which traffic must flow without inspection due to regulatory and other requirements – such as financial or healthcare sites that contain confidential personal information.

WebWall Web Application Firewall and DDoS Protection

With WebWall®, Infosec's suite of web application security capabilities, NetOpti Series application delivery controllers can protect against distributed denial of service (DoS/DDoS) and malformed URL attacks and allow a wide range of Layer 2 through Layer 7 protective policies to be stacked atop one another for increased security.

NetOpti appliances are security-hardened to protect applications and servers from L4 and L7 DDoS attacks at the application, session and network layers, and support content filtering to guard against protocol and application DDoS attacks as well as Syn-flood, tear drop, ping-of-death, Nimda, Smurf and other malicious attacks. In addition, Infosec's DDoS protection features machine learning for anomaly detection and automatic configuration of threshold values. NetOpti appliances also feature extensive access control lists, network address translation and stateful packet flow inspection – all executed atthe kernel level – to guard against attacks and unauthorized access without impacting performance or scalability.

In addition, integrated web application firewall capabilities provide deep application data inspection – beyond IP and TCP headers – to deal with attacks such as SQL injection and cross-site scripting. Deployable in front of multiple web or application servers, Infosec's web application firewall detects and responds to signatures for known application vulnerabilities and is programmable to deal with future threats.

Secure Application Access

Web-based and other applications typically require secure authentication in order to grant access to users; however, when users require access to multiple applications, or applications include subsystems that also require authentication, the process of logging in can become cumbersome and difficult. TheNetOpti Series supports Secure Application Access and multiple AAA methods including Security Assertion Markup Language (SAML), LDAP, RADIUS and OAuth to allow users to Single Sign-On (SSO) just once, and gain access to all applications for which they are authorized; Single Log-Out closes all active logins at session's end. Serving as a SAML SP, theNetOpti Series interacts with a SAML IdP (such as Infosec's AG Series SSL VPN) to securely authenticate the user, thus simplifying and streamlining access.

Link Load Balancing & GSLB

Link load balancing (LLB) and global server load balancing (GSLB) ensure 99.999% availability for wide area network (WAN) connections and geographically dispersed sites and hybrid cloud environments. Link load balancing with end-to-end health monitoring and dynamic routing detects outages and monitors performance in realtime to distribute traffic across multiple WAN connections for a premium, always-on end-user experience. Ideal for geographically distributed applications, multi-site architectures and hybrid cloud applications, global server load balancing directs traffic away from failed data centers or cloud services and intelligently distributes services between sites based on proximity, language, capacity, load and response times for maximum performance and availability. In addition, Infosec's GSLB supports mixed health check relationships across SDNS service pools, as well as EDNS-client-subnet to provide improved resolution services and thus improve the user experience.

Application Acceleration

NetOpti Series appliances leverage multiple acceleration technologies and optimizations to deliver a premium end-user experience for a wide range of applications and data services. In-memory caching increases server efficiency and improves seek and response times by over 500%, hardware or software compression can reduce bandwidth utilization and end-user response times by more than half and TCP connection multiplexing aggregates millions of short-lived client connections into persistent fast lanes that increase server efficiency by up to 70% while improving application performance.

ePolicy L7 Application Scripting

Where Infosec's Layer-7 policy engine cannot meet application traffic management requirements, ePolic scripting allows transactions and content to be manipulated to achieve traffic distribution that improves data center efficiency and mitigatesthe effect of delivering applications over the internet.

eRoute L4 Routing

Using eRoute, inbound and outbound WANtraffic may be load balanced across multiple ISP links based on preset and user-defined algorithms and directed across routes optimized for maximum stability and performance. Additional L4 traffic management features include VLANs, port forwarding, port and link redundancy and the ability to bundle multiple low-cost links to improve bandwidth utilization and reduce cost.

Application-Specific Certifications

In conjunction with ISVs and application developer partners, Infosec NetOpti Series appliances have been certified to provide load balancing, acceleration and security for enterprise applications such as Microsoft, Oracle, Epic, eClinicalWorks and others. Leveraging deployment guides, businesses can take the guesswork out of application delivery. Following simple step-by-step instructions, IT can rapidly and confidently configure NetOpti appliances for optimized delivery of business critical applications.

Traffic Shaping & QoS

Traffic shaping optimizes application traffic on WAN links to improve bandwidth utilization and end-user response times. Supporting user-defined policies, NetOpti Series appliances prevent bandwidth-intensive applications from over-utilizing WAN links and ensure essential applications are prioritized to meet service level agreements. Used in conjunction with link load balancing, global server load balancing and QoS features such as filters and class-based queuing, traffic shaping can dramatically improve application performance.

IPv6 Support

For organizations needing an IPv6 web presence, server load balancing protocol translation (SLB-PT) transforms existing IPv4 web sites into IPv6 compatible sites and greatly reduces the need for duplicate equipment, content and management. Where there is a need to make the most of depleted IPv4 resources, NAT and dual NAT (dual-stack IPv6) allow multiple clients to utilize a single IPv4 address. In migration environments, Infosec IPv6 solutions support both NAT64 and DNS64 to enable IPv6 clients to connect with IPv4 servers and content. To ensure a consistent application experience across IPv4 and IPv6 clients and networks – and to enable fully-capable, next-generation solutions – IPv6 feature parity is supported for allInfosecNetOpti Series application delivery controllers.

Management & Integration

NetOpti Series application delivery controllers are simple to install and offer intuitive configuration and management via a cloud-friendly, intuitive WebUI and a familiar command line interface. Using the administration tool kit, network managers can view the status for a wide range of system parameters, enable services on the fly and automate configuration using XML-RPC or RESTful API. Leveraging extensible APIs, application and network intelligence can be integrated with third-party and cloud monitoring and management or exported for optimizing complementary data center systems. In addition, the NetOpti Series supports VMware Aria Suite, Microsoft System Center, Ansible, Terraform and other automation tools for intelligent management of application infrastructure.

eCloud API & Open Stack Integration

To meet the deployment and management requirements of load balancing and application delivery in the cloud, Infosec's eCloud API provides a script-level interface for cloud management systems to manage and monitor Infosec devices and assist in interactions between cloud operating systems and virtual machines running Infosec load balancing. For cloud providers and enterprises leveraging the OpenStack architecture for cloud management and automation, Infosec's integration with OpenStack load balancing-as-a-service (LBaaS) creates a standardized means to rapidly integrate with and control Infosec technology.

Product Editions

NetOpti Series hardware appliances support two product editions. AppVelocity supports a rich server load balancing and application acceleration feature set optimized for local traffic management. The AppVelocity-E edition is purpose-built to provide industry-leading throughput and transactions per second for elliptic curve cryptography (ECC) traffic. ECC is increasingly used as an alternative to RSA encryption. AppVelocity-E models deliver enhanced security for HTTPStraffic and superior ECC performance, along with the same robust feature set included in AppVelocity-S.

All AppVelocity product editions include link load balancing and support global server load balancing as an option. vNetOpti virtual appliances include all features and software modules found on Infosec's NetOpti Series application delivery controller dedicated appliances.

Physical & Virtual Appliances

Dedicated NetOpti Series appliances leverage a multi-core architecture, SSDs, software or hardware SSL and compression, energy-efficient components and 10 GigE or 40 GigE to create solutions purpose-built for scalable traffic management. Whether running on Infosec'sAVX Series Network Functions Platform, on common hypervisors or on many popular public cloud marketplaces, vNetOpti virtual appliances are ideal for organizations seeking to benefit from the flexibility of virtual environments, offer infrastructure services and new elastic business models or evaluate Infosec application delivery with minimal risk and up-front cost.

NetOpti Series Specifications

Availability

Layer 2-7 Policy & Group Management	Multi-level virtual service policy routing – Static, default and backup policies and groups – Layer 2-7 application routing policies – Layer 2-7 server persistence – Application load balancing based on round robin, weighted round robin, least connections, RTSP, shortest response, minimum misses, SNMP, Server Application State Protocol (SASP), QoS DNSdomain and DNS security extensions
Layer 2-3 Load Balancing	IP/MAC based load balancing for any IP protocol – Round robin, persistent IP and return to sender – Firewall, IPS/IDS, anti-spam, anti-virus and composite applications – L2 bridging support
Layer 4 Load Balancing	TCP, TCPS and UDP protocols – Round robin, weighted round robin, least connections and shortest response – Persistent IP, hash IP, consistent hash IP, persistent IP + port and port range – All single port TCP applications, NNTP, RADIUS, SMTP, IMAP and POP3, DNS server support – Composite IP application support
Layer 7 Load Balancing	HTTP 0.9/1.0/1.1/2/3, HTTPS, QUIC, SSH, DNS, FTP, TFTP, RDP, RTSP, SIP-TCP, SIP-UDP, RTSP, ASP, IOT, Radauth, Radacct, Diameter, and WebSocket – L7 content switching (QoS network and client port - SSL and SIP session ID - HTTP URL, host name, cookie and any header - hash header, cookie and query) – URL redirect and HTTP request/response rewrite – HTTP request filter – DDoS protection
Server Persistence	Source + destination IP, Client IP, SSLID, HTTP header, URL, cookie, application – Individual session control
Content Routing & Switching	One arm, configurable reverse or transparent proxy mode per VIP – Configurable reverse or transparent proxy mode, triangle mode , ICAP – Nested L7 and L4 policies – Combine L7 and L4 policies
Global Server Load Balancing	Application availability from multiple locations worldwide – DNS DoS protection – DNSSEC man-in-the-middle protection – DNS over TLS (DOT) and HTTPS (DOH) - Global site/ service selection – Proximity and IP persistence – Load balancing between multi-site SSL VPN deployments – SNMP pool – Mixed health check instance relationships – EDNS-client-subnet support -full DNS – A, MX, AAAA, CNAME, PTR, SOA, etc.

ePolicy L7 Application Scripting	Customize SLB policies and combine with SLB methods to enable load balancing among real services – Analyze packet contents of HTTP, simple object access protocol (SOAP), extensible markup language (XML) and diameter protocols – Receive, send, analyze, and discard generic TCP and TCPS packets – Perform pattern matching for text data – Control TCP connections – Monitor and capture traffic statistics
eRoute L4 Routing	Policy-based routing based on port, source/destination IP, UDP protocols, TCP – RIPv1, RIPv2 and BGP, OSPF support – Return to sender (RTS)/IP flow persistence – Port forwarding, link aggregation and port redundancy – Transparent to VPN remote access
Application, Server & Link Health Checks	ARP, ICMP, TCP, HTTP/HTTPS, DNS, Radius, MySQL, MsSQL, RTSP, SIP single port/protocol health checks – Multi-port health checks – Health checks by protocol and content verification – Link health checks based on physical port, ICMP and user-defined L4 – Next gateway health checks, destination path health checks – Ensure availability and performance of applications over WAN links from a single point of management – Scriptable customer-defined composite health checks
Clustering / High Availability	Up to 32 nodes – Active/active, active/standby – Standard VRRP - Configuration synchronization – Application-specific VIP health checks – Stateful session failover (TCP, SSL, persistency) – Automatic ISP failover - RFC 2338, Floating IP , MAC support - failover decision/health check conditions including, Gateway, CPU overheated, system memory, process, unit failover, group failover - multiple communication links
Single System Image	Create a single VIP (single ADC instance) out of any number of dedicated, virtualized or virtual NetOpti appliances – Enable ultimate flexibility in scaling out
IPv6	Full IPv6 support – DNS64 & NAT64 – Dual Stack Lite – IPv6 to IPv4 and IPv4 to IPv6 NAT and full IPv6 addressing – IPv6-ready gold certified
Networking	Link aggregation, VLAN/MNET, NTP – Static and port-based NAT, advanced NAT for transparent use of multiple WAN links, Jumbo frame
Link Load Balancing	Outbound: round robin, weighted round robin, shortest response time, target proximity/dynamic detection – Inbound: round robin, weighted round robin, target proximity/dynamic detection – Integrated DNS – Outbound DNS proxy

Acceleration

Application Performance	Dynamic detect – Client connection persistence – Connection multiplexing – TCP buffering – Tune TCP (Idle, Wait, Close, Alive, Window Scale, Sack , MSS, Time Stamp) - IEEE 802.3ad link aggregation

SSL Acceleration (2048 & 4096- bit)	Hardware SSL processing – SSLv3 and TLSv1 .0/1 . 1/1 .2/1 .3 – 4096-bit maximum cipher key size (RSA or ECC) – End-to-end security (server-side SSL communication) – SSL session reuse and timeout control – Cipher strength reduction – Customizable cipher suite order – Customizable SSL error pages – Sharableto multiple SLB services – SSL selfcheck – Server name indication (SNI)
Compression	Hardware or software accelerated – Virtualized compression – Inline HTTP processing – Compresses HTML, XML, Javascripts and CSS – Compresses Microsoft file formats (DOC, XLS, PPT) and PDF
Caching	Virtualized, memory-based caching – HTTP 1.1 compliant, policy-based caching
Traffic Shaping	Guarantees application performance – Rate shaping for setting user-defined rate limits (bps, Kbps, Mbps, Gbps and pps, Kpps, Mpps, Gpps) on critical applications – QoS for traffic prioritization – Supports CBQs and borrow and unborrow bandwidth from queues – Advanced ACL (SLB QoS) – Supports QoS filters based on ports and protocols including TCP, UDP and ICMP

Security

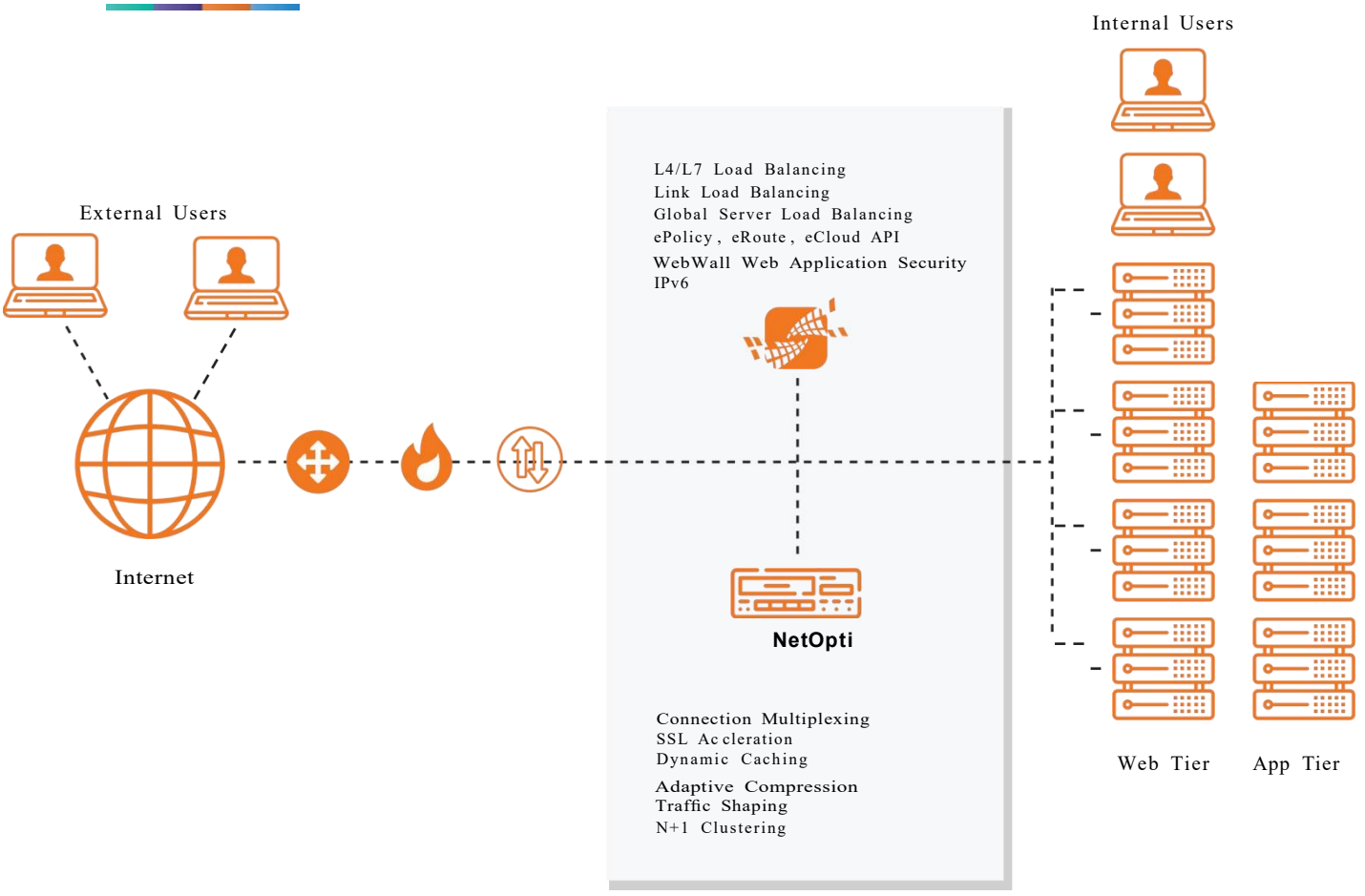
WebWall Web Application Security	Hardened OS – Secure access only, access control based on client certificate information and access method – Customer configurable SSL/TLS version, cipher suite and minimum cipher strength – Tamper-proof key and certificate protection – WebWall stateful packet-inspection firewall – Over 1000 ACL rules without performance degradation – Proxy-based firewall – TCP syn-flood protection – Flash and surge event protection – DoS protection – HTTP access method control –URLfiltering – HTTP/DNS cache for mitigating DDoS – Web Application Firewall – Deep application data inspection for dealing with attacks such as SQL injection and cross-site scripting – Detects and responds to known application vulnerabilities – Programmable to deal with future threats
DDoS Protection (SLB)	Protocol Attacks: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapsar (CC), Hashdos, DNS poisoning, DNS NXDomain flood, Tunneling attack – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option –HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ACK flood, FIN/RST flood, Connection flood, TCP Flood , UDP flood –Machine leaning oftraffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic and exploits.
SSL Intercept	L2 or L3 mode, integrated or distributed mode, forward or reverse proxy mode – Webagent service

Client-Server Certificate Management	CSR and private key generation – Self-signed certificate support – Import certificate and private key – Import certificate format – Extensive certificate support – Certificate backup and restore – Wildcard certificate support – Server Name Indication (SNI)
Client Certificate Authentication & Authorization	Turbo client certificate verification – Root and intermediate CA import – Basic client certificate verification – Certificate chain support – Certificate revocation list (HTTP, FTP, LDAP) – Online certificate status protocol (OCSP, HTTP/HTTPS) – Certificate-based access control – Inside SSL server, two-way certificates
Client Certificate Application Integration	Parse client certificate field information with different language/encoding – Pass individual field/ group and field/customer format to back-end applications – HTTP header, URL and cookie – Integrated with proxy rewrite – Detailed SSL statistics
Secure Application Access	AAA support for Security Assertion Markup Language (SAML), LDAP, RADIUS and Open Authorization (OAuth) protocols – Supports definition of multiple AAA methods for multifactor authentication – Supports web single sign-on (SSO) and web single logoff (SLO) – Serves as a SAML SP (service provider) – Supports restriction on number of sessions, session timeout and session reuse

Management

System	Centralized cluster management – Secure CLI, WebUI and SSH remote management – XML-RPC for integration with 3rd - party management and monitoring – SNMP V2/V3 and private MIBs – Syslog (UDP orTCP) – Administrator and operator account management – Email, paging and alerting capability – Multiple c onfiguration files and unit configuration s ynchronization – Online troubleshooting – Real-time monitoring – Auto clean up of idle resources in high utilization condition - Role-based administration control – HTTP/2 support – Top-10 statistics for users of IP, TCP, UDP a nd ICMPtraffic – multiple configuration files with 2 bootable partitions
eCloud API	Interface for cloud management systems to control and monitor hardware and virtual NetOpti appliances– Assists interaction between components such as virtual machines in CloudOS environments –Remote management of NetOpti appliances – Notification of events on NetOpti appliances – eCloud demo integrated onNetOpti appliance – Supports integration with OpenStack Load Balancing-as-a-Service (LBaaS), VMware Edge Cloud Orchestrator and Microsoft System Center standards

Infosec Application Delivery Architecture



Product Specifications

• Standard o Optional	NetOpti1800	NetOpti2800	NetOpti5800	NetOpti6850	NetOpti7850	NetOpti12800
CPU	Intel	Intel	Intel	Intel	Intel	Intel
Max. L4 Throughput	10Gbps	20Gbps	40Gbps	80Gbps	120Gbps	200Gbps
Max. SSL Throughput	5Gbps	15Gbps	20Gbps	45Gbps	45Gbps	90Gbps
Max. SSL TPS (RSA 2K)	20K	40K	40K	80K	80K	150K
Max. ECC TPS (ECDSA P256)	10K	20K	20K	40K	40K	75K
1 GbE Copper	●	●	●	●	●	●
1 GbE Fiber	○	○	○	○	○	○
10 GbE Fiber	●	●	●	●	●	○
40 GbE Fiber				○	○	○
100 GbE Fiber						●
Power Supply (Hot Swappable)	NetOpti1800, 2800			Dual Power: AC(100V-240V、6.5A Max), DC(240V、4.5A Max)		
	NetOpti5800			Dual Power: AC(100V-240V、6.5A Max), DC(240V、4.5A Max)		
	NetOpti6850,7850 , 12800			Dual Power:AC(100V-240V、10A Max), DC(240V、5A Max)		
Maximum Power Supply Output（W)	450W			800W		
Dimensions(W × D × H)	547mm*435mm*44.5mm			549.9mm*435mm*88mm		
Environmental	Operating Temperature: 0° to 45° C, Humidity: 0% to 95%, Non condensing					
Regulatory Compliance	GB 42250,ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A					
Safety	CSA, C/US, CE, IEC 60950-1, CSA 60950-1, EN 60950-1					
Support	Gold, Silver and Bronze Level Support Plan					
Warranty	1 Year Hardware, 90 Days Software					