Juniper Networks DX Application Acceleration Platforms



Securing and Assuring Delivery of Web Applications

The growing migration toward web-enabled applications and data center simplification is driving the need for a new class of multi-function devices – application front ends (AFEs). By incorporating critical functionality to offload web server processing, accelerate web browser sessions, and secure the "web tier," the Juniper Networks DX series of application acceleration platforms deliver unprecedented application performance, security, and availability in an easy-to-manage, flexible platform.

Performance: Speed User Access, Increase Application Capacity

With the Juniper Networks DX series of application acceleration platforms, time to access business critical applications is typically cut in half – a dramatic boost in application usability and acceptance, especially for remote and branch office users. The DX platform optimizes and compresses all outgoing web data in real time with negligible latency. Content fidelity is maintained, ensuring web content is always rendered with 100 percent accuracy, bandwidth use is dramatically reduced and users experience faster page loads regardless of their location or network connection. The optional 3G Caching capability further improves user response times and offloads critical servers for improved scalability and performance.

The Juniper DX platform also increases the capacity of web and application servers by serving as a transaction broker, managing all connections and requests between servers and users. All DX platforms maximize available server and network resources, freeing web server CPUs for other tasks and yielding up to a 10x increase in web and application server capacity.

Security: Internal Firewall for the Data Center Web Tier

The "internal firewall" functionality of the DX complements existing security equipment, further protecting the "Web Tier" from potentially malicious TCP and HTTP/web-based attacks in the critical transaction zone where web-enabled applications reside. The Juniper DX platforms authenticate users and can provide per-request authorization by leveraging the existing RADIUS and LDAP infrastructure. The DX platforms also secure data and connections, protect servers from DOS and SYN flood attacks, and uniquely provide security features based on native HTTP protocol communication to enable powerful, flexible, and adaptable security capabilities.

All DX platforms support one-way or end-to-end Secure Sockets Layer (SSL), delivering secure content faster than a server can deliver clear text. The DX 3650-FIPS application acceleration platform is FIPS 140-2 Level 3 compliant, offering an even higher level of security to organizations seeking compliance with the Federal Information Processing Standard (FIPS).

Availability: Maximize With Juniper ActiveN™

The DX devices provide full layer 4-7 server load balancing functionality, supporting deployment of multiple applications and server clusters behind a single appliance. The DX platforms can also perform programmatic network, server, and application health checking through flexible scriptable health checking functionality. The DX platforms validate every web request/response by verifying the HTTP return code. Unsuccessful or anomalous requests/returns can be programmatically retried and are logged for further root-cause analysis.

Unique to the DX application acceleration platforms is the ability to deploy in an ActiveN mesh configuration, enabling up to 32 DX devices to process traffic for the same or different virtual IP addresses. With ActiveN, it is only necessary to add one box at a time to increase scalability or failover protection, as opposed to the pair of boxes and network redesign required to scale active-standby or active-active configurations.

Management: Insight Through Real-Time Information

The DX platforms shine with over 200 real-time statistics to provide extensive details on all inbound and outbound traffic. Historical data is easily time-sliced from seconds to years via online graphs, simplifying capacity planning, trending, and troubleshooting of application and network issues. By front-ending all servers, the DX devices easily enables web logging data consolidation, easing management and freeing additional server resources.

The role-based administration features of the DX platforms streamline device management, limit user authority to specific areas, and greatly increase user accountability. Complete system, administration, and audit logs provide detailed administration records.

Flexibility: OverDrive Control Environment

The Juniper DX OverDrive™ control environment is a "user API" that enables changes in application behavior without altering the application itself. The OverDrive capability can transform, update, append, prepend, or delete request or response headers or POST data, or even return content itself, whether it is HTML, JavaScript, Cascading Style Sheets, XML, or other formats.

To engage the OverDrive capability, users simply write "if-then" rules using an intuitive sentence-like control language that supports unlimited content processing actions on data streams, based on any combination of factors in both incoming user requests and outgoing server responses. For example, The OverDrive capability can be used to automatically secure application requests and responses, enabling instant security with no performance degradation and no time-consuming or costly application rewriting. The OverDrive capability can also be used to check the accuracy of every response and take configurable action to resolve failures, maximizing application availability.

	DX 3200/3250	DX 3600/3650	DX 3650-FIPS	DX 3670
Application Clusters Supported	64	128	128	128
Servers per Application Cluster	32	64	64	64
SSL Transactions per Second	3,000/5,000	5,000/9,000	5,000	18,000
NEW SSL Connections per Second	250/800	500/1,600	500*	11,000
FIPS 140-2 Level 3 Certified	No	No	Yes	No
Network Interface Options	100TX (x2)	a) Gb E-TX (x4) b) Gb E-TX (x2) and GigE Fiber (x2)	Gb E-TX (x2)	1Gb E-TX (x2)
Form Factor	1U	2U	2U	2U
Power Supply	Single	Dual redundant	Dual redundant	Dual redundant

*FIPS card specification

Features

Performance

Transaction Brokering and Connection Management

- DX multiplexing engine offloads servers – reduces server connections by a ratio of up to 1,000:1
- Terminates and persistently maintains separate internal and external TCP and HTTP/S connections (full TCP and HTTP Proxy)
- Multiplexes HTTP/S requests and supports pipelining and chunking
- Real-time HTTP 1.0 to 1.1 conversions
- Additional state-of-the-art TCP optimizations improve TCP performance, including: selective acknowledgement, slow-start with congestion avoidance, and fast retransmits

Clientless Compression

- Compresses all HTML, SHTML, DHTML, JHTML, PHTML, Javascript, J2EE, JSP, CSS stylesheets, XML, SOAP
- Internal compression policy engine includes more than 4,000 compression policies to ensure 100 percent page fidelity
- Programatically control compression of any MIME type, including doc, xls, ppt, Flash, etc., on a per-object or per-object class basis
- Web-services compression for server-to-server protocols including SOAP
- Supported by all standard browsers (IE 5.0 + , Netscape 4.0 +)

Optional 3G Caching

- Improves server performance and scalability by serving straight from internal, memory-resident cache
- Complete operational transparency to both client and server
- Reduces bandwidth usage – client-side feature programmatically enables appropriate objects to be cached client-side

LDAP and RADIUS Authentication Caching

Caches successful login attempts to reduce load on the authentication server, dramatically improving performance of authentication and authorization

Security

Network and Transport Security

- AutoSSL™ feature rewrites HTML "on the fly" to secure content without modifying the application
- End-to-end and one-way SSL with accelerated download of secure content
- Supports ARC4, RSA, DES, 3DES, AES, MD5, and SHA-1 encryption algorithms
- Defends against SYNFlood and denial of service (DoS) attacks
- Terminates and tunnels any TCP protocol over SSL for session-based, point-to-point, or client-to-gateway SSL security (including mail, Telnet, etc.)

Protocol Scrubbing (HTTP and TCP)

- Never passes packet fragments; ensures only valid, well-formed HTTP/S requests reach servers
- Delivers full function Authentication and Authorization
- Supports Client Certificate Authentication, Radius, and LDAP
- Offers full content stream inspection
- Blocks, logs, or re-writes bad URLs and malicious requests
- Provides buffer overflow inspection and protection

Native HTTP Protocol Communication

- Dynamically inspects, verifies, and re-writes client requests or server responses
- Acts on HTTP headers, POSTs, SOAP and HTML, JavaScript, etc.

Availability

Transaction Assurance

- Detects transaction errors by incorrect content within the page itself or error code
- Repairs, retries, redirects requests, shielding users from errors and increasing transaction success

SLA Monitoring and Analysis

- Tracks, monitors, and logs server response time and client download time for each HTTP/S request and response.

ActiveN High Availability

- Supports self-healing mesh of up to 64 DX Series platforms actively processing traffic to one or more VIPS with cascading failover and linear scaling
- Provides active-active or active-standby high-availability

Full L4 and L7 Server Load Balancing

- Supports full Layer 4 server load balancing of HTTP, HTTPS (SSL), FTP, and most TCP and UDP protocols
- Supports full Layer 7 load balancing based on any request method, protocol version, URL, cookie, other header, POST data, header or body content, SOAP, or XML contents
- Supports full-function, flexible, scriptable health checking, enabling programmatic verification of external devices and services
- Includes enhanced “Fewest Outstanding Requests” balancing method for HTTP/S, delivering most optimal load distribution and performance. Also supports weighted round robin, least connections, fail-over chaining, etc.
- Offers robust Layer 7 load balancing, programmatically controlled with optional OverDrive control rules

Management

Historical Statistics

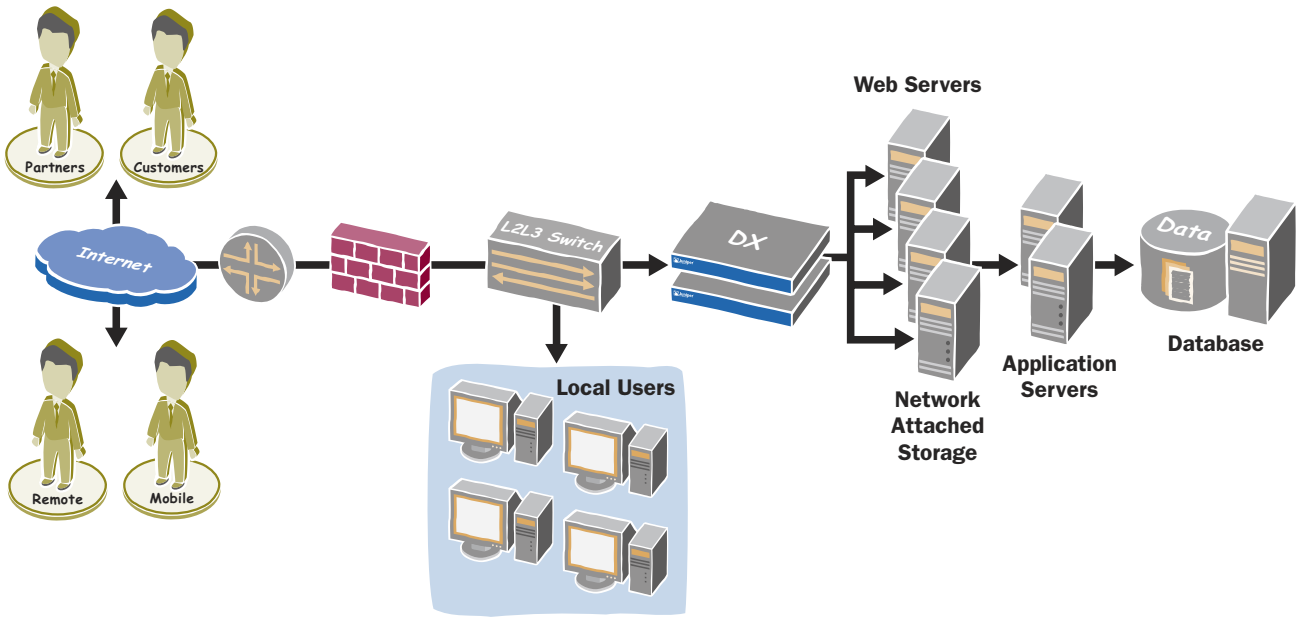
- More than 200 real-time statistics available by second, minute, hour, day, month, year

Role-based Multi-level Administrative Access

- Differentiated user access levels
- Complete system, administration, and audit logs

Administration Tools

- Web browser interface (HTTP, HTTPS) enables simplified configuration and management
- Command line interface via SSH, Telnet, SCP, or console (RS-232)
- Administration dashboard, e-mail alerts
- SNMP supported through Juniper MIB
- Configuration synchronization across multiple DX platforms, simplifing configuration and management for large scale deployments



Sample Deployment

Flexibility

- Can be configured in 1 arm or 2 arm mode
- Supports Client IP transparency – simplifies configuration and installation into an existing network
- Offers wide range of functionality – load balancing, compression, SSL, TCP offload, HTML rewrite, accounting/authentication/authorization, application firewall
- Offers performance linearity – all functions can be used simultaneously while maintaining performance linearity
- Enables drop-in replacement of existing server load balancing equipment, or can complement existing server load balancing equipment
- Supports 802.1Q VLAN Tagging – differentiates packets belonging to different VLANs in a multi-VLAN environment
- OverDrive control environment enables bi-directional modification of HTTP applications with a wide range of actions, including alert, block, groom, transform, repair, and rewrite
- Content manipulation (such as compression and 3G Caching) can be controlled with near-infinite granularity for maximum flexibility
- Available software options (all options enabled via software license – no install required)
  - DX Series OverDrive, Adaptive Content Processing environment
  - DX Series 3G Cache

Physical Specifications

Power Requirements

110 ~ 240 VAX, 50 ~ 60 Hz, auto-sensing
1U Systems: 150 Watts 2U systems: 300 Watts

Dimensions and Weight

1U Systems: 1 RU (45mm/1.8in) h x 17.1in (435 mm) w x 16.7in (425mm) d, 24 lb.

2U Systems: 2 RU (88mm/3.44in) h x 17.1in (435 mm) w x 16.7in (425mm) d, 32 lb.

Operating Environment

Temperature: 5° to 40° C
Humidity: Less than 90% humidity, non-condensing

Regulations

Emissions: FCC Class A, EN 55022 Class A, EN 61000-3-2, EN 55024 Immunity

Safety: CSA C22.2 No. 950, EN 60950

Juniper® NETWORKS

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

Copyright 2005, Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

100121-002 July 2005