

Juniper Networks Secure Access SSL VPN – Performance and Scalability with Juniper Networks DX

Enable Employees, Partners, and Consultants to Stay Connected Anywhere and at Anytime

SSL virtual private network (VPN) technology is quickly becoming the industry standard for providing remote access to employees as well as extranet access for partners, consultants, and customers. Today, most enterprises have replaced or plan to replace their current IPSec VPN solutions for remote access with SSL VPN. Why? It provides the lower cost, ease of maintenance, granular control, and anytime anywhere access that IT leaders demand for both normal business usage as well as emergency scenarios.

The Challenge

However, as the remote access community continues to expand, many businesses are struggling with a unique set of challenges. These challenges are becoming more prevalent as distances between end points and actual resources and applications grow longer and networks get more congested. This can result in Web application performance degradation and loss of revenue and productivity. What's more, the vast majority of enterprise applications today have been Web-enabled, using the HTTP protocol. HTTP has built-in inefficiencies and suffers from various performance problems over the WAN. What's needed is an effective way to optimize SSL VPN to meet today's ever-increasing scalability and performance demands.

The Juniper Networks Solution for Managing Growth and Scalability for Remote Access

Juniper Networks Secure Access SSL VPN enables remote users to stay connected from anywhere and at anytime. The Juniper Networks DX product line provides the scalability and performance required to maximize SSL VPN investments and ensure productivity is never compromised. Why is this now so important? The enterprise network perimeter continues to dissolve as companies increase their efforts to remain competitive and improve productivity by maximizing resources and shortening cycle times. With the Juniper Networks Secure Access SSL VPN, there is no trade-off between increasing competitiveness and improving productivity.

Load Balancing to Increase Scalability

Many enterprises today employ load balancers to distribute and scale Web server deployments. The same approach can be taken with SSL VPN solutions. By deploying a load balancer, like the Juniper Networks DX appliance, in front of multiple Juniper Networks Secure Access appliances, enterprises and service providers can distribute the load of SSL VPN traffic across the available Secure Access nodes. This increases scalability by supporting more concurrent users. The Juniper Networks DX appliance also ensures that backend nodes, for example, are online and working. It accomplishes this by performing a comprehensive health check first before actually sending any traffic through.

One of the requirements of a good load balancer is to provide a persistent or "sticky" way to ensure a user's connections remain bundled together for better efficiency. Various methods offer a variety of ways to ensure session stickiness. However, the best practice is to utilize Source IP persistence like the Juniper Networks DX appliances offer.

Global SSL VPN Load Balancing for Business Continuity and Disaster Recovery

With the criticality of online communication today, organizations must employ robust solutions. This does not just mean high-availability, it means exercising due care and implementing a business continuity plan to keep the company running in the event of a disaster. Global Server Load Balancing (GSLB) is one important component of this. GSLB enables an organization to roll-out multiple backend (data center-based) solutions with a unified (virtualized) entry point. Based on Domain Name System (DNS), the GSLB function of the DX monitors all nodes in the solution and ensures users will not be geographically distributed to alternate locations. Additionally, the DX initiates a ping test from nodes in order to identify the shortest hop between the end-user and the deployed nodes. This not only provides disaster recovery support, it also increases productivity by ensuring the fastest link is used for the SSL VPN session.

Beyond Load Balancing: Application Optimization

Load balancing provides many benefits to improve the scalability of the Secure Access SSL VPN devices. By front-ending the Secure Access devices, Juniper's DX solution provides real and tangible benefits at Layer 7 by accelerating Web applications and overcoming limitations posed by them across the WAN. For remote access portal users accessing the Secure Access devices over the WAN, this translates into better application performance and faster downloads. The DX provides these benefits by inspecting and optimizing the HTTP protocol at Layer 7. Using features such as caching, compression, and protocol optimization, the DX can significantly reduce the overhead associated with common protocols such as TCP and HTTP.

The Juniper Networks DX appliances deliver much more than just load balancing. The appliances are designed for application acceleration and protocol optimization. The appliances can:

- Rewrite HTTP requests and responses with AppRules
- Filter URLs for which users should not be allowed to access
- Redirect users to different sites or locations on-the-fly
- Provide DoS protection for backend servers
- Ensure HTTP protocols are formatted properly and utilize appropriate syntax

Using sophisticated Layer 7 features, the DX provides clean HTTP transactions to the SSL VPN traffic, enabling the Juniper Networks Secure Access appliance to work more efficiently. It filters and sanitizes all HTTP traffic. Features such as URL filtering on the DX remove unwanted traffic before it reaches the Secure Access appliance. HTTP protocols incorrectly formatted or using erroneous syntax are bounced back before getting to the Secure Access appliance for processing. The Secure Access SSL VPN appliance receives only requests that are correct and inspected. This results in the Secure Access appliance spending less time in processing erroneous requests and more time processing real user requests. The processing by the DX considerably reduces overhead and processing for the SSL VPN solution, providing more headroom and resources for real remote user requests. This translates into more users being able to access applications remotely without any degradation in performance—and no loss of productivity.

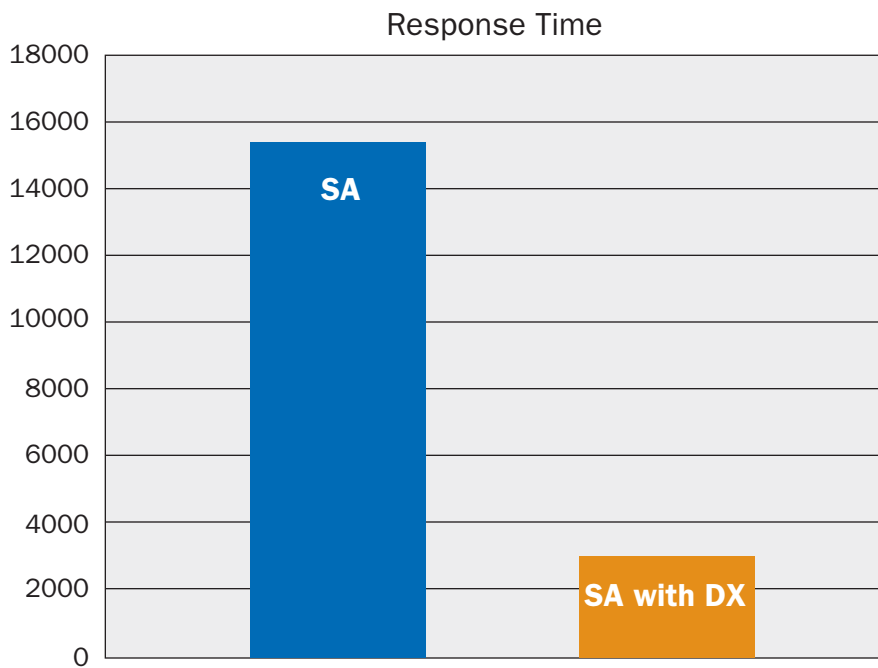
Solution Components

Validation – Performance Test Results

Juniper Networks conducted a series of tests using the Juniper Networks DX appliance to front-end multiple Secure Access SSL VPN appliances. The benefits outlined below validate how Juniper Networks DX appliances can provide a considerable boost in both performance and scalability for a Secure Access SSL VPN deployment. This boost provides performance gains in excess of 30 percent. Furthermore, it enables a Secure Access deployment to scale more linearly than previously possible.

WAN test results below consisted of the following configuration:

- Spirent Web Avalanche and Reflector simulating 1,000 SSL VPN users
 - WAN simulation was enabled (768Kbps limited)
 - Packet loss of 5 percent and 100ms latency was induced as outlined below
- Outlook Web Access (HTTP) transaction profile
 - Users access their inbox, calendar, and contact list several times
 - They then log out and log back in, and then repeat the process
 - Authentication was Active Directory
 - Several Web ACLs were configured on the Secure Access
 - The DX was configured in Layer 7 (HTTP Cluster) mode
 - Compression was enabled on the DX
 - OWA Mode was enabled on the DX



The above results clearly demonstrate that, in a WAN environment, the Juniper Networks DX appliances can provide a considerable boost in end-user performance (and by extension, productivity) by reducing overall end-user response time in a real life scenario.

Scalability with DX

Scalability benefits also are considerable. Typically, with a 4-unit Secure Access cluster, one can expect 2,500 users per box, with the OWA test used above. But in a WAN environment, the overhead of latency, packet loss, and re-transmissions can force a Secure Access deployment to be scaled back in order to maintain acceptable user response times. The DX, however, increases this user capacity, while maintaining the same acceptable user response times.

**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, 25/F
ICBC Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

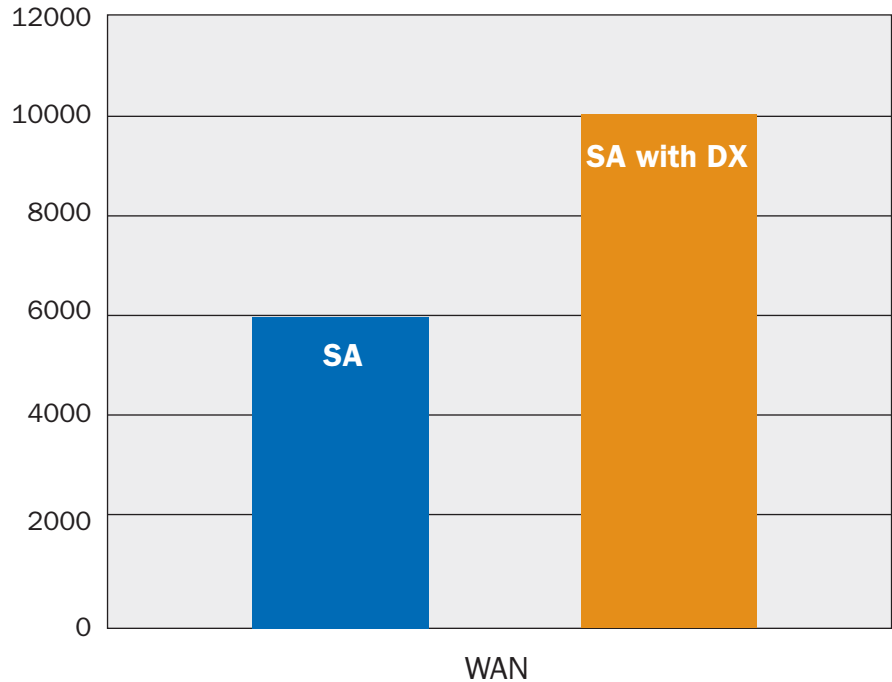
**EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS**

Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44-(0)-1372-385500
Fax: 44-(0)-1372-385501

Copyright © 2007, 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.



Concurrent Users



NOTE: WSAM, JSAM, and Network Connect, which utilize NCP (Juniper's Proprietary HTTPS-based Network Communications Protocol), do not benefit as greatly as with Core access. This is because the NCP protocol does not contain compressible data, so the benefits are limited to the TCP optimization functions of the DX.

Juniper Networks Integrated Solutions for Maximizing Productivity

Today, the SSL VPN is the defacto standard for remote access. Enterprises are challenged with a consistent and continuing explosive growth in their remote access user community as the enterprise perimeter continues to dissolve. This, combined with the performance challenges posed by Web applications over the WAN, can lead to loss of revenue and productivity as remote access users experience sluggish applications. Juniper Networks market leading Secure Access SSL VPN appliances, combined with Juniper Networks DX appliances, provide enterprises with a best-in-class solution for optimizing remote access needs and preventing productivity loss.

Offloading some of the SSL VPN traffic to Juniper Networks DX appliances allows Secure Access appliances to accomplish more important tasks and to scale to support more users per node without degrading performance. Users can experience application performance and response time improvements of up to 30 percent by adding a Juniper Networks DX to the remote access equation. This enables enterprises to maximize remote access investments, improve productivity, and increase revenue.

Next Steps

Contact your Juniper Networks partner or sales representative for more information.

About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.