

# Blood Systems Relies on Juniper Networks Integrated Security, Access and Data Center Acceleration Solutions to Give Life to Its WAN



**Industry:** Healthcare

**Company:**

Blood Systems

**Challenges:**

- Upgrade nationwide frame relay WAN to a fully meshed MPLS network and deploy new routers with enhanced capabilities at 84 locations
- Support immediate expansion of remote access connectivity to all employees in the event of a pandemic
- Protect key medical equipment that's unable to run antivirus from inbound and outbound threats
- Maximize WAN investment with application acceleration

**Network Solution:**

- Juniper Networks J-series Services Routers J6300 and J2300
- Juniper Networks Secure Services Gateway 550 (SSG 550) Firewall/IPSec VPN
- Juniper Networks Secure Access 4000 (SA 4000) SSL VPN Appliance
- Juniper Networks WXC and WX application acceleration platform

**Selection Criteria:**

Conducted competitive evaluation of three leading router vendors and chose Juniper Networks routers for their high performance and strong value. Deployed additional Juniper integrated security, remote access and application acceleration solutions based on the initial experience.

**Results:**

- Optimized network value and improved operational efficiency with a Juniper integrated security and application acceleration solution
- Centrally staged router deployment for MPLS network with 84 sites so that non-technical medical staff could plug in the routers—with 100% success
- Met business continuity goals by enabling employees to work from home in the event of an emergency
- Protected key medical equipment that cannot run antivirus software against inbound and outbound threats
- Enabled the deployment of storage-area network synchronization and disaster recovery between primary data center and disaster recovery site

*"Juniper Networks routers are so much simpler than our previous routers. Juniper put a lot of thought into the management of the J-series routers and its JUNOS software. We've saved huge amounts of time in configuration and deployment."*

**Jeff Stephens,**  
Network Engineering Manager,  
Blood Systems

For more than 60 years, Blood Systems, one of the country's oldest and largest blood service providers, has been offering its life-giving services throughout the Western U.S. Through its non-profit community blood centers—United Blood Services and Blood Centers of the Pacific—the company provides blood, blood components and special services to patients in more than 500 hospitals in 18 states ranging from California to the Gulf Coast and from Texas up to the Canadian border. The organization is second only to the American Red Cross in blood collection.

With such critical care services at the heart of its business, Blood Systems relies heavily on keeping employees across 84 locations in close touch with one another. To do this, they must also provide employees with access to the applications they need, whether they're working under ordinary circumstances or in extraordinary situations like a natural disaster or pandemic.

### Challenges

Blood Systems relied on a frame relay network to connect each of the company's sites to a data center that ran email, blood banking applications and other general office applications.

"The contract with our carrier was up, so we wanted to upgrade the bandwidth and the technology we were using," says Jeff Stephens, network engineering manager at Blood Systems. "We decided to switch to an MPLS network, so we put out a competitive bid." The existing edge routers were old, and Blood Systems decided to upgrade its routers in conjunction with the WAN upgrade.

### Selection Criteria

After issuing an RFP, Stephens performed a thorough evaluation of the three leading router providers. He put routers from the three vendors through their paces, and selected Juniper Networks J-series Services Routers for their ease of deployment.

"Juniper Networks routers are so much simpler than our previous routers. Juniper put a lot of thought into the management of the J-series routers and its JUNOS™ software. We've saved huge amounts of time in configuration and deployment," Stephens says.

This was Blood Systems' first foray into Juniper Networks gear, but with the company's solid reputation in the carrier space, Stephens knew it would translate well to his enterprise. That initial decision led to an integrated solution with Juniper routing, security and application acceleration.

### Solution

Blood Systems wanted to optimize its network for business value, migrating to the latest WAN services to increase flexibility and to support business continuity requirements so that the nation's blood supply wouldn't be interrupted in the face of a natural disaster or pandemic.

The new Blood Systems network is anchored by Juniper Networks J-series Services Routers. Blood Systems uses the J6300 router at its primary data center in Scottsdale, AZ and at a disaster recovery site located in nearby Tempe, AZ. Designed for branch and regional offices, the J6300 delivers unmatched router performance with firewall, Network Address Translation (NAT), IPSec and other services enabled. It supports a rich set of MPLS, IPv6, quality of service and multicast features. Major locations are connected via DS-3 lines to the

MPLS WAN, which is supplied by Qwest. Smaller locations, which have T-1 connections or higher, use J2300 routers to connect to the MPLS WAN. The routers support the use of OSPF on the Blood Systems' internal network, as well as BGP routing on Qwest's MPLS network.

Internet traffic is backhauled over the MPLS network to the primary data center. From there, Blood Systems uses the Juniper Networks Secure Services Gateway 500 Series Firewall/IPSec VPN platform to provide Internet access to most locations. The SSG 500 delivers an ideal mix of performance, security and LAN/WAN connectivity for regional and branch office deployments. Traffic flowing in and out of the branch office is protected from worms, spyware, trojans and malware by a complete set of Unified Threat Management (UTM) security features, including stateful firewall, IPSec VPN, Intrusion Prevention System (IPS), antivirus (includes anti-spyware, anti-adware, anti-phishing), anti-spam, and Web filtering.

For Blood Systems, supporting access to critical business applications from anywhere is far more challenging than providing remote access to a handful of employees who travel or work from home. As a vital link in the blood supply chain, Blood Systems must be prepared to fully function even during a major disaster or widespread disease outbreak. To sustain the organization's workflow through any kind of disaster, Blood Systems turned to Juniper Networks Secure Access 4000 (SA 4000) SSL VPN Appliance.

"We need to make sure there's an adequate blood supply in the event of a bird flu pandemic," says Stephens. "To do that, we must provide the capacity to allow employees to work from home if they are not able to travel or if we don't want them to travel."

Employees had SSL VPN access to the company's resources, but the existing VPN wouldn't scale to support an immediate and total expansion of remote access connectivity in the event of a disaster. With the SA 4000 and the ICE (In Case of Emergency) license option, Blood Systems can be confident that it can provide remote access capabilities at peak demand from a large number of users.

Designed for mid- to large-sized organizations, the SA 4000 appliance provides cost-effective remote access from standard Web browsers. It has rich access-privilege management functionality that makes it easy to provide remote access to employees and

others without making any changes to the infrastructure or clients. Different employee and visitor populations can use exactly the resources they need, while adhering to enterprise-security policies.

IT particularly appreciates the Secure Meeting option, which is a cost-effective, easy-to-use Web conferencing tool. Like the SSL VPN, no software needs to be deployed and it allows people to share applications in real time. "Secure Meeting is especially useful for providing IT support to telecommuters and traveling users," Stephens says. "We use it for support now, and longer term our training department can use it for Web conferencing."

Blood Systems also relies on Juniper Networks WXC application acceleration platform to meet its business continuity and disaster recovery requirements. The WXC platform optimizes existing bandwidth and accelerates application performance over the WAN, delivering faster application response times while reducing bandwidth consumption and prioritizing mission-critical traffic.

"The WXC allows us to do storage-area network synchronization and maximize the DS-3 connections traffic between our primary data center and our disaster recovery site," says Stephens. "The Juniper Networks WXC allows the existing link to support more traffic, so we can maximize our WAN investments."

Molecular Sequence Reduction™ (MSR™) is the flagship compression algorithm used by the WX platform. The MSR compression technology recognizes repeated data patterns and replaces them with labels, dramatically reducing WAN volumes. The labels are replaced by the missing data at the far end of the WAN link, so no information is lost during transmission. Network Sequence Caching is similar to the MSR technology in that it also reduces WAN transmissions by replacing redundant data patterns with a small label before sending across wide area links. However, while the MSR technology operates entirely in memory, Sequence Caching utilizes onboard hard drives installed on WXC platforms to record and store larger data patterns for a longer period of time, enabling the detection of redundant traffic last seen days or even weeks earlier.

### Results

Most of the benefits from the Juniper Networks router deployment can be accounted for in operational efficiencies. Blood Systems has a small IT staff who must provide IT services to offices located across half the United States. That calls for high-performance, cost-effective and easy-to-manage solutions.

The ease of deploying Juniper routers greatly facilitated the MPLS rollout. Stephens and his IT team centrally configured the routers for 84 locations, and then shipped the routers to the sites, which non-technical medical staffers plugged in. The routers powered up, and everything worked flawlessly in all locations.

Stephens notes that network visibility has improved. He uses the J-Flow feature on the J-series routers for traffic engineering and capacity planning. "I need visibility into the traffic that flows through the full-mesh MPLS network but that doesn't flow through our data center. We looked at putting probes at the remote sites, but that would have been too expensive," he says. IP traffic flow statistics are summarized into J-Flow records, and then Blood Systems uses these summaries for service assurance and troubleshooting as well as traffic analysis to assist with traffic engineering and capacity planning. IT also uses the WX Central Management System (CMS) to monitor applications and gain enterprise wide visibility to gauge application performance, site metrics and traffic patterns for long-term planning as well as troubleshooting and analysis.

The UTM protection provided by the SSG platforms has been particularly useful in the non-profit's national donor testing laboratories in Tempe, AZ and Bedford, TX, which have medical equipment that can't run antivirus software. "We can't install antivirus software on certain medical and test equipment at these locations because it invalidates configurations that are approved by the Food and Drug Administration. We've implemented high availability pairs of SSGs to isolate the medical device PCs from the rest of the network," Stephens says. "The SSGs provide deep inspection and antivirus to provide protection against inbound and outbound threats. The SSGs have solved a real issue for us."

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

### Next Steps and Lessons Learned

Stephens plans to continue the rollout of the Juniper Networks SSL VPN, replacing the pockets of IPSec VPNs still in use. "There are issues with IPSec VPNs, such as the overhead of installing client software and problems with NAT when people are trying to work from a hotel," he says.

Stephens is investigating Juniper Networks unified access control (UAC) solutions to provide another layer of protection. "We have medical device networks that we have to keep isolated," he explains. "We sometimes call on non-IT staff to help deploy new equipment in remote facilities. We need to make sure that they're plugging devices into the right place. We're looking at network access control to boost our security in this area."

Next up is compliance with the Health Insurance Portability and Accounting Act (HIPAA) regulations, as the non-profit is rolling out new applications that require HIPAA compliance. This will make the UTM protection on the SSGs even more valuable, and reinforce the need for Juniper Networks UAC. "We're very excited about the prospect of integrating a NAC solution with our SSG security solution," he says. "We think it will integrate very well."

### For More Information

To find out more about Juniper Networks products and solutions, visit <http://www.juniper.net>.

### About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

