


JUNIPER NETWORKS WALKS A MILE IN CUSTOMERS' SHOES AT INTEROPNET 2007



Industry: Events and Tradeshows

Challenges: Interop organizers were challenged with setting up an event network, InteropNet, which would be used by event attendees, exhibitors and the press for a variety of activities. The network needed to run reliably in full public view for the duration of the event.

Solution: Interop organizers turned to Juniper Networks products and solutions to rapidly build and operate a secure, high-performance, open network for the event. Juniper Networks engineers donated their time on a volunteer basis to create the network.

Results: InteropNet operated flawlessly and securely in full public view during the course of the Las Vegas and New York Interop events. Attendees, exhibitors and members of the press were able to use the network throughout the shows.

Interop is a leading technology event that brings IT and business leaders together to see the latest technologies in action. For over 20 years, Interop has fueled the revolution and evolution in IP networking. And where does Interop turn for reliable, high-speed networking services for exhibitors, conference rooms and attendees? [The InteropNet!](#)

The InteropNet is built in collaboration with hand-selected, innovative vendors and volunteers who come together to take on the ultimate networking challenge—creating a network that provides reliable, high-speed networking services to all Interop exhibitors, conferences and meeting rooms—the most high-profile assignment in the business. Building the massive InteropNet is the ultimate networking challenge. This dream network addresses the complete networking needs of any organization and sets the bar for innovation and expertise. Throughout the InteropNet's 20-year history, it has owed many thanks to its ever-growing, dynamic and resourceful community

Open Network Requirements Prove Challenging

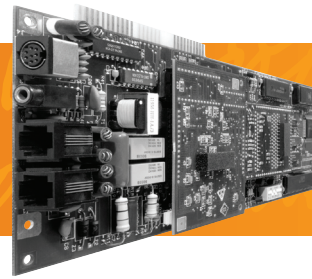
As the official security provider for Interop Las Vegas and New York 2007, Juniper engineers were tasked with setting up and managing the Interop event network. The network had to be constructed rapidly—within just a few days—and provide reliable, secure, continuous access to exhibitors, attendees and the press for a variety of activities, including product demonstrations, research, email and Web access.

Requirements for the InteropNet network included a high degree of security to protect against unwanted traffic or malicious activity such as IP theft, denial of service (DoS) attacks, worms and viruses, as well as performance issues and downtime. At the same time, the network had to support multi-vendor technologies to allow ubiquitous access to all parties.

Key objectives for the project included:

- Design, stage, set up and operate the InteropNet
- Rapidly build and operate, in full public view, a model open, multi-vendor network
- Provide exhibitors, attendees and press ubiquitous network access
- Protect the network against unwanted traffic, including denial of service floods and worms
- Protect the network infrastructure, management systems and users

Critical to the project's success was flawless operation, as well as the ability to run advanced technologies being showcased at the event. InteropNet is heavily used by thousands of unknown users; anyone can walk up and log on. Users need access to the Internet and other appropriate resources, but the show network must be protected against misuse, DoS floods and deliberate attacks. Tried-and-true closed security



policies are impractical in open or community-based networks such as those used in research, education, or in this case, on the trade show floor. As such, an open security policy was necessary. Juniper Networks engineers pulled out all the stops in terms of employing best practices for security and performance, and in the process, learned a lot about network operations in highly complex, open networks.

Open and Accessible, Yet Secure Infrastructure Allows Constant Access

The InteropNet solution included the following components from Juniper Networks product families:

- Juniper Networks M7i Multiservice Edge Routers
- Juniper Networks J6350 Services Routers
- Juniper Networks ISG2000 Integrated Security Gateway with integrated Intrusion Detection Prevention (IDP)
- Juniper Networks Steel-Belted Radius Server
- Juniper Networks IC6000 Unified Access Control Appliance
- Juniper Networks Network and Security Manager

To protect against misuse and unwanted traffic, Juniper Networks designed the InteropNet infrastructure to support IPv4, SSL and IPsec encrypted transport, multicast, J-flow record feed and port mirror feeds. In the network operations center (NOC), a Trusted Network Connect (TNC) policy distribution point and node validation for network access control (NAC) enforcement were employed, along with RADIUS/AAA for authentication. The NOC also ran security element management, attack updates, policy editor and log analysis. Security enforcement included DoS flood mitigation, firewall access control and intrusion prevention.

Juniper Networks J6350 Services Routers were deployed at the exhibition hall to protect the network perimeter. The J Series performed policing and push filters upstream using the BGP flow specification. From there, the J Series routers connected to M Series Multiservice Edge Routers, which were co-located at a Qwest data center. The routers provided a load-balanced path to the Internet, while protecting InteropNet against DoS floods and other attacks coming in from the Internet.

Juniper Networks ISG2000 with integrated intrusion detection and prevention (IDP) protected the Internet connection and the NOC. The routers provided DDoS protection, access control using stateful inspection firewalls, and deep packet inspection with multi-gigabit performance.

First-hand Experience at Interop Provides Insight

“Participating in InteropNet allowed us to walk a mile in our customers’ shoes,” says Mike Swarm, a security solutions engineer and the lead InteropNet engineer from Juniper Networks. “Designing and building the InteropNet Event Network gives us first-hand insight into the real-life challenges of network operations. It also provides us with an extremely taxing and hostile operating environment in which we can prove and hone our networking and security best practices. Those best practices make their way back to our systems engineers, who assist our customers with their network designs.”

InteropNet provided closed access to the NOC, for users or systems. Network access control (NAC) was enforced to give engineers in the NOC access to InteropNet using Juniper Networks Unified Access Control (UAC), which tied user identity, device integrity and location information with session-specific policy that was enforced by Juniper devices throughout the network. UAC provided enforcement using 802.1X-enabled infrastructure, media access control (MAC)-based authentication or existing Juniper firewalls. Users who connected via 802.1X were authenticated via a Juniper Networks Steel-Belted RADIUS/AAA server to ensure users accessing the network over remote/VPN connections or 802.1X had complied with all security policies. Juniper Networks VPN Gateways enabled engineers to access InteropNet remotely from any Web browser.

The InteropNet security engineering team leveraged a new capability in the ISG2000 to create “smart attack” filters. Swarm likens the “smart attack” filters to an MP3 player’s smart play list, which automatically builds a play list based on the categories a person selects. “We built a smart list of vulnerabilities, which includes highly unwanted attacks, medium severity attacks, worms and trojans, or whatever else the security team puts in there,” says Swarm. “The smart filter automatically adds the appropriate signatures to the list.” This capability makes it easier to select the appropriate signatures for protecting the network against attacks.

The ISG2000 firewall and Intrusion Prevention System (IPS) with smart attack signatures also protected shared network services, including Domain Name System (DNS), authentication, authorization and accounting (AAA), Network Time Protocol (NTP), Element Management system, Trivial File Transfer Protocol (TFTP)/Simple File Transfer Protocol (SFTP) and SNMP. InteropNet leveraged closed policies to protect those assets, since there were only a limited number of known users and systems that had access.

Flood protection was enforced at both Layer 3 and Layer 4 in the routers. Juniper Networks firewalls and IDP performed correlation by inspecting flows at the higher layers of the OSI model and alerting routers of any suspicious traffic.

Juniper Networks Applies Lessons Learned in the Field

Given the complexity and highly secure nature of InteropNet, the project was a tremendous learning experience for Juniper Networks engineers. "As engineers at Juniper Networks, we learn a lot about using our own products at InteropNet," said Swarm. "We find out whether we can run a network of this size and complexity with only two engineers – as many of our customers do every day. Then we turn this learning into best practice App Notes for our field engineers and our customers."

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.

Corporate And Sales Headquarters

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

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. "Engineered for the network ahead" and JUNOSE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered marks, 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.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

