

NOAA NETWORKING CASE STUDY:

**NOAA Tackles Security and Network Performance
at the Network's Edge with Juniper Router Technology**

CRA Reports

*This report was prepared by
CRA Reports, an independent
reporting agency based in
Washington, DC.*

**Copyright © 2004
All rights reserved**

NOAA Tackles Security and Network Performance at the Network's Edge with Juniper Router Technology

Executive Summary:

With the Internet now the primary channel through which NOAA gathers and shares mission critical data with its constituencies, the agency faced two major challenges:

- *Handling rapidly growing volume of traffic to and from its enterprise network; and*
- *Responding to rising malicious attempts to disrupt service or violate the integrity of its data.*

Juniper was the only vendor able to address this problem for NOAA. The company provided an edge-router technology that could tackle the traffic volume and mitigate the threats in a cost-effective manner.

Challenge:

The National Oceanic and Atmospheric Administration (NOAA) conducts research and gathers data about the global oceans, atmosphere, space, and sun. NOAA warns of dangerous weather, charts the seas and skies, guides the use and protection of ocean and coastal resources, and conducts research to better understand and manage the environment. As a result, a major part of NOAA's mission is to make a massive amount of data – such as weather maps, satellite images, and research findings – available to the research community, major sectors of industry, and the public at large.

NOAA has a large public profile because so much of what it produces for its various constituents is delivered via the Internet. The agency is also a major target of hackers, and denial of service (DOS) attacks. In the face of these threats, NOAA is tasked with keeping its data highly available.

“Our infrastructure’s ability to get that information out to stakeholders who access data over the Internet is critical. In many cases the protection of life and property is involved. We also publish or otherwise make data available on issues that are critical for many industries – such as the information that is produced and housed by the National Marine Fisheries Service. In short, there is a tremendous amount of data that must remain available, yet secure. The integrity of that data has to be assured. And even minute outages or interruptions of service are unacceptable.” – John C. Kyler, NOAA

In response to these threats, NOAA has invested heavily in a stringent layered security strategy that requires all elements of its enterprise network to contribute the agency's security posture. While NOAA has deployed state-of-the-art firewalls, intrusion detection systems and other initiatives to mitigate its exposure to attacks, there has been increased focus on having the network's edge routers – the link between the public Internet and NOAA's firewall – filter out traffic that matches the profile of known threats.

The edge-router's ability to identify and derail known malicious traffic – especially those associated with DOS attacks – before hitting the firewalls greatly enhances the efficiency of the security operation because it frees both technical and human resources to

examine, identify and remediate less obvious threats. Put another way, effective filtering at the edge-router level reduces the number of alerts that firewalls and security personnel have to address.

However, as both the nature and the number of threats grow exponentially, so have the number of filters that edge routers are required to support. This placed a burden on the existing system of edge routers that exceeded their capabilities.

“We had met the capacity limitations of the enterprise-class devices that were in place. We had reached a point where if the security group instructed us to add a filter for a known threat that was trying to do a DOS on part of our network, we were faced with making decisions about which filter we would have to take out to make room for the new filter. Moreover, the high number of filters was interfering with the performance of the network. So what we wanted was a solution that would provide us with the throughput we needed while being able to perform more filtering than we were currently doing.” – John C. Kyler, NOAA

Solution:

In early 2001, NOAA replaced the edge routers at its headquarters facility in Silver Spring, MD with the M-Series platform offered by Sunnyvale, Calif.-based Juniper Networks. The decision to install the carrier-class M-Series was made after testing revealed that the flexible and efficient design of Juniper’s Application Specific Integrated Circuit (ASIC) on the platform allowed the router to handle thousands filters without experiencing any degradation of performance on the network.

“We wanted to have the capability to support thousands of filters, since we didn’t know what the future was going to bring as far as security threats were concerned. We wanted to be able to increase our capabilities – which at the time we were running between 200 and 300 filters on one box.” – John C. Kyler, NOAA

Juniper far exceeded that requirement. Because the ASIC is designed into the heart of the M-Series router, the filtering performance required by NOAA is available on every interface. The M-Series product line supports interface speeds ranging from t-1 (1.54 Mbps) all the way up to OC48 (2.488 Gbps). The highly programmable Juniper ASICs allow NOAA to quickly enable new features as developments require – such as support for IPV6, Multicast, and virtual private networks (VPNs).

Results:

Beyond the security benefits of supporting more filters at the network’s edge, NOAA has also been able to extend the life-cycle of its hardware investment. In an era that is characterized by rapid obsolescence of technology deployments, the performance characteristics of the new Juniper routers have provided unexpected headroom in capacity. In other words, the devices’ ability to handle both increased traffic and a higher number of filters has defrayed the need to buy new technology, even as data volume and security threats rise. This has translated into significant capital investment savings. Also the port density of the M-Series routers has allowed NOAA to reduce its

ongoing operations & maintenance (O&M) costs. This is because it supports more interfaces per device than the routers that were replaced.

*“The M-20 device, for instance, has 16 available slots in which we can place the physical interface cards (PICs) that connect the router to the various modules which support different parts of our network. (In our case there are OC3 modules, Gigbit Ethernet modules, and Fast Ethernet modules, among others.) What we found was that we could buy smaller quantities of routers to establish connectivity to different facets of our network. The high density ports, which support more modules on any given router, kept the O&M costs down.” – **John C. Kyler, NOAA***

NOAA is now using the Juniper routers at its back up facilities, and is deploying the technology at other NOAA campuses around the country. By standardizing its CPE and Internet gateways on Juniper’s carrier-class technology, the agency is spending less money and getting more.