

U.S. Department of Labor The Mine Safety and Health Administration scales secure remote access quickly and cost-effectively with Juniper Networks SSL VPN

Organization:

Department of Labor, Mine Safety and Health Administration

Industry:

Federal Government

Challenge:

Improve productivity by extending highly secure remote access to MSHA remote workers that is easy to deploy and manage, cost effective, and easy to use.

Solution:

Juniper Networks NetScreen Secure Access SSL VPN

The Benefits:

- High levels of security at the end-points and for applications/files being accessed
- Ease of deployment and management for IT Staff
- Ease of use for employees
- Improved efficiency for all

Background

Founded in 1913, the U.S. Department of Labor was established to foster and promote the welfare of the job seekers, wage earners, and retirees of the United States. The Department is focused on improving working conditions, advancing opportunities for profitable employment, protecting retirement and health care benefits, helping employers find workers, strengthening free collective bargaining, and tracking changes in employment, prices, and other national economic measurements.

An agency within the Department of Labor, the Mine Safety and Health Administration (MSHA), is responsible for promoting the health and safety of all those employed in mines, both metal and non-metal. MSHA helps to reduce deaths, injuries, and illnesses in the nation's mines with a variety of activities and programs. The agency develops and enforces safety and health rules applying to all U.S. mines, helps mine operators who have special compliance problems, and makes available technical, educational and other types of assistance. MSHA works cooperatively with industry, labor, and other Federal and state agencies toward improving safety and health conditions for all miners. Committed to providing its customers as well as its employees with clear and easy-to-access information, MSHA embraces information technologies and solutions that improve network performance without sacrificing security.

Challenge

In early 2003, the option to work from a remote location on a high-speed network connection was unavailable to most MSHA employees. Employees who traveled or who wished to work from home only had access to the MSHA network through dial-up connections with servers located in Arlington, VA and Denver, CO. Many of these employees utilized faster and easier to use Internet connections at home and were discontented with the dial-up networking arrangement.

On a case by case basis, the agency began to approve the use of Internet Protocol secure (IPSec) virtual private networks (VPN) to allow employees to work from their own connections. This capability was used primarily by network administrators and managers with home computers and high speed Internet connections – fewer than 20 employees were approved to connect remotely using this solution.

MSHA quickly learned that the IPSec VPN capability drained network management resources and caused problems that impacted both system performance and

“The Juniper Networks solution provided us with a way to provide users with broadband remote access to our network at any time from anywhere, without allowing viruses or worms to penetrate our network.”

Syed Hafeez
Information Security Officer
Department of Labor, the Mine Safety and
Health Administration

support. Computer support technicians often needed to travel to individual connection points to configure the computers of individuals using the IPsec VPN solution. Once configured, the trouble was not over. Consistent faults in the network system and firewalls caused a help desk nightmare – with a disproportionate amount of network support required to service the needs of a relatively small number of remote employees. As an additional difficulty, the IPsec VPN client software sometimes interfered with employees’ personal use of their home computers, particularly instant messaging and Web-based e-mail.

Solution

In the spring of 2003, the MSHA embraced an Enterprise Architecture (EA) governance process to ensure that information technology initiatives were closely aligned with and supported the business needs of the agency. Under this process, an EA Steering Committee comprised of MSHA program executives collaboratively identified and established priorities for all information technology initiatives. The steering committee quickly identified improved remote access as the number one priority for fiscal year 2004, and MSHA allocated funding.

With funding in place, MSHA conducted an analysis to identify the best solution to its remote access and networking problems. Considering the importance of implementing a remote access technology that offered secure and assured networking without increasing network management time, MSHA decided upon a secure sockets layer virtual private network (SSL VPN) solution. MSHA’s analysis revealed that SSL VPN eliminated the need for client-software deployment, changes to internal servers, and costly ongoing maintenance and support. Further, SSL VPN secure-access appliances allowed MSHA to benefit from a lower total cost of ownership over traditional IPsec client solutions, while improving end-to-end security features. The SSL VPN allowed the agency to place a device behind the corporate firewall to enable employees to establish a connection from any browser.

Syed Hafeez, Information Security Officer, MSHA, explained the attraction of the SSL VPN solution. “We were concerned about the potential danger involved in giving broadband remote access to our users from any unmanaged system that they requested,” Hafeez said. “The costs involved in a network compromise under these circumstances caused us major anxiety.”

Additionally, MSHA sought to implement an SSL VPN security solution that was FIPS Level 2 compliant. Having identified the appropriate technology for remote access, the agency reviewed a number of solutions that could provide this technology. Through this competitive review, MSHA identified the Juniper Networks Secure Access 3000 as the top SSL VPN for consideration. The Secure Access 3000 provided MSHA with a secure remote access solution that was FIPS compliant and could be easily managed.

Implementation

With testing complete, MSHA received the SSL VPN hardware in November 2004. Juniper Networks’ employees provided on-site training to the technical administrators to demonstrate exactly how to set up the network in the most secure manner – empowering MSHA technicians with complete knowledge of how the Juniper Networks SSL VPN worked and the benefits it provides.

MSHA began piloting the Secure Access 3000 in February 2005. In just a few short months, word spread like wildfire throughout the agency that a superior option for remote workers was available. Employees began volunteering to participate in the testing procedures in order to improve their remote access to the MSHA network. The test group quickly grew to more than 200 users. One senior manager even volunteered to try out the Secure Access 3000 while on travel, connecting to the network from an Internet kiosk to conduct his daily business activities.

During the final stages of the Secure Access 3000 implementation in April and May 2005, MSHA implemented the remote access capability for all eligible employees – a total of 2,200 users. The agency noted the immediate flexibility and ease-of-use that the SSL VPN solution offers to employees – the technology allows network managers to significantly scale back the amount of time spent managing configuration and security issues associated with remote access. Remote users have gained so much confidence in the solution that they no longer assume troubles connecting to the MSHA network are due to the remote security solution.

An incident during the early stages of implementation demonstrated the ease-of-use of the SSL VPN. Remote users were required to download a patch to enable their machines to connect to the MSHA network. Before the SSL VPN solution, this type of glitch would have taken days to fix and required many help-desk hours. With the Juniper Networks Secure Access 3000 in place, every remote user was able to install the patch without the use of the help desk.

“An unexpected benefit of the Secure Access 3000 implementation is the ability to conduct secure, Web-based meetings across the enterprise,” said George Fesak, Director of Program Evaluation and Information Resource, MSHA. “MSHA’s software development group has already used the appliance to demonstrate a new application to 32 agency users and managers located across the nation.”

With Juniper Networks SSL VPN in place, everyone benefits. MSHA employees gain the privilege of a secure and assured remote network. Agency network administrators gain easier installation and maintenance of the network. The MSHA help-desk support team gains the ability to focus on agency-wide, rather than remote-only, problems. Most importantly, the secure and assured access that MSHA now enjoys will enable employees to work more efficiently to serve the American workforce.



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