

CHINA'S MINISTRY OF RAILWAYS SECURES INFORMATION MANAGEMENT SYSTEM WITH THE ISG SERIES INTEGRATED SECURITY GATEWAYS

Summary

Industry: Transport

Challenge: To ensure effective data exchange and security for compartmentalized network segments of a government transportation entity.

Selection Criteria: Security, rich functionality, and product and service quality at the best price-to-performance ratio.

Network Solution: Juniper Networks ISG2000 Integrated Security Gateway

Results: The ISG2000 enabled the Ministry of Railways to maintain clean separation of its three network segments – the production network, the administration network and the WAN – to maximize security and robustness. The solution also facilitated the smooth delivery of services and support, contributing to sound and secure operation of the network.

China's Ministry of Railways is in charge of the national railway network, which is the main artery of the country's transport system. The railway system handles a countless number of passengers and huge volume of cargo around the country each year.

The Ministry's railway information management system is key to China's railway development. The system is deployed nationwide and captures a tremendous volume of information. Given the vital role it plays in ensuring passenger safety and national economic development, there is no margin for error. The operational and security requirements set by the Ministry were therefore very rigorous.

As part of efforts to develop secure, convenient and comfortable railway services, the Ministry embarked on its first state-level safety project—the Network Safety Project. The initiative had the objective of ensuring the safe operation and management of the national railway system and is given the highest priority by the Ministry.

A key outcome from initial assessment was the need to ensure clean separation of network segments, by function, to maximize security and stability. Thus, it was imperative the Ministry identify an optimal solution to achieve this fundamental need.

Challenges

In addition to other security requirements, a major hurdle was that the three networks of the railway information management system—the production network, administration network and WAN—had to be kept separate without compromising effective data exchange.

It would be a fine balance between the security of the system—the solution had to be able to respond effectively to a wide range of attacks—and traffic performance. A clear network framework had to be maintained to enable services and support to be delivered easily. At the same time, overheads and maintenance costs had to be kept to a minimum, in view of the dispersed geographical distribution of network nodes.

Selection Criteria

After performing due diligence in locating such a solution, the Ministry found that Juniper Networks® stood out from its competitors with Juniper's ability to provide the most professional, advanced and qualified solutions and products. The ministry chose the Juniper Networks ISG2000 Integrated Security Gateway because of the solution's advanced features and compelling price-to-performance ratio.

With its professionalism and track record in service quality, Juniper clearly emerged as the vendor of choice for the Ministry of Railways.

Solution

The ISG2000—the industry’s first integrated security gateway with multiple best-in-class network boundary safety features—was used for primary switching in the network.

The ISG2000 incorporates a fourth-generation ASIC chip, which enables effective protection against threats in both the network and application layers, and delivers outstanding performance while reducing network complexity. The ISG2000 enables over 500,000 concurrent connections and 300 Mbps network throughput, and also supports multiple networking abilities, thus addressing the scalability requirements of the state-level project.

With the ISG2000, the Ministry of Railways is also able to separate the three networks while ensuring the effective and secure exchange of data. Content can be filtered according to the source address, target address, network protocol, services, time and bandwidth to ensure stringent access control.

In addition to being the core switch and routing device for the system, the ISG2000 itself incorporates many significant security features such as an integrated firewall, VPN and full Intrusion Prevention System (IPS) capability through the optional Intrusion Detection Prevention (IDP) security modules. The IPS capability combines multiple detection methods including robust signatures and protocol decodes to proactively identify and prevent online attacks. The signatures are also customizable, providing customers with granular-level control and flexibility.

The built-in Juniper Networks ScreenOS, a real-time, security-specific operating system, is equipped with deep-layer detection firewall technology and virtualization functions, and supports various routing protocols including BGP, RIPv2 and OSPF. The solution can thus be deployed easily in heterogeneous environments, allowing complex networks to be consolidated and optimized. It also protects the Ministry’s IT investments by putting in place a solid foundation for future upgrades.

Like all members of the Juniper Networks firewall/IPSec VPN family, the outstanding line-speed processing function of the ISG2000 ensures throughputs of over 200 Mbps, even for applications with intensive system resource requirements.

Results

With the implementation of the ISG2000, the Ministry of Railways has achieved its security requirements and separated its production network, administration network and WAN. The solution also facilitates the smooth delivery of services and support, contributing to the sound operation of the network as a whole.

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
www.juniper.net

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
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

Copyright 2010 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. 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.