

Inner Mongolia Electric Power Corporation Secures WAN with Juniper Networks ISG Series



Industry: Public Utility

Company:

Inner Mongolia Electric Power Corporation

Challenges:

- Stopping worms and viruses propagating in the WAN
- Maintaining uninterruptible network uptime in keeping with the mission-critical nature of the Corporation's power generation and distribution operations
- Keeping security and network management complexities in check

Selection Criteria:

The Juniper Networks Integrated Security Gateways (ISG) Series was selected on the merits of its firewall, virtual private network

(VPN) and Intrusion detection and prevention (IDP) performance, plus overall ease-of-management and cost-effectiveness.

Network Solution:

Juniper Networks Integrated Security Gateways (ISG) 1000 and 2000

Results:

- Network threats effectively eliminated under all traffic conditions
- Application traffic protected with VPN
- Access controls to WAN tighter and more granular
- Security and network devices easier to manage

"We are very pleased with the Juniper solution which not only handles our challenge of scale, but incorporates comprehensive measures, such as IDP, allowing us to avoid the complexity of separately deploying and managing IDP devices."

Yao Qiang,
Deputy Director of Information
Communication Center,
Inner Mongolia Electric Power
Corporation

Home to 24 million people, the Inner Mongolia Autonomous Region in northern China boasts the third-largest land area among China's provinces. And undertaking the vast operation of supplying power to households and industries in the region is the state-owned Inner Mongolia Electric Power Corporation—the sole large-scale power enterprise in the province.

Employing approximately 25,000 employees and operating across various geographically dispersed subsidiaries, the Corporation also runs a vast data network. The 662 Mbps IP-based WAN connects 12 power supply enterprises and other related organizations in the province.

Challenges

With its WAN now a mainstay to the Corporation's daily operations, protecting the network from security threats has become a key business challenge. In particular, the Corporation needed to thwart worms and viruses emanating from both internal LANs and the Web.

On a broader scale, the larger challenge was to create a well-planned security infrastructure that could respond to threats via rigorous security policies and automation. The mission-critical nature of the Corporation's power generation and distribution operations, coupled with increasing reliance on the WAN as a conduit for business data exchange, meant that network downtime had to be avoided.

Selection Criteria

Last year, the Corporation embarked on an exercise to improve the security of its information network by bolstering its firewall defense capabilities. It also wanted to create a security framework that would be easy-to-manage.

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.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, 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.

From the onset, the Corporation identified three key operational goals which the chosen security solution would have to meet: a) ensure access control across all key network segments; b) protect both network (Layer 2 through 4) and application (Layer 4 through 7) traffic; and c) ensure that security and the network remain easy to manage over time.

With its WAN usage experiencing rapid growth, the last goal was a critically important one for the Corporation. "We needed a high-performance security solution that could keep pace with the network's operational levels," said Yao Qiang, deputy director of Information Communication Center, Inner Mongolia Electric Power Corporation. "Our IP-based WAN runs at 662 Mbps and we needed protection that would not slow it down," he added.

Solution

Following comprehensive technical and cost evaluation, the Juniper Networks ISG 1000 and ISG 2000 were chosen as part of the Corporation's upgraded security framework. The ISG Series is a fully integrated firewall/ VPN/ IDP system. It provides gigabit (Series 1000) or multi-gigabit (Series 2000) performance, a modular architecture and rich virtualization capabilities.

The ISG Series was successfully deployed in July 2007. As part of the deployment, the Corporation worked with Juniper Networks to redesign parts of its WAN. The exercise involved identifying different network segments based on business types and risk levels.

By the end of the exercise, the Corporation had divided its information network into a core exchange area, an Internet data center (IDC) application area, office areas, the National electric power network area, the north united electric power network area, and Internet zones.

The Corporation then proceeded to define network access paths via strict, fine-grained security policies. Firewall and access control rules were inserted between various zones to provide network and application traffic protection. To protect application traffic, the Corporation also harnessed the IDP modules on the ISG platform for key business applications, such as production and marketing applications.

A final requirement was having redundancy in its security systems. To that end, the Corporation configured the dual-machine architecture via the NetScreen Redundancy Protocol (NSRP) Full-Mesh redundancy modes in the ISG devices.

Results

Equipped with the IDP option, the ISG-series provides deep packet inspection, intelligent traffic analysis, Zero-Day protection against worms, Trojan horses, spyware, keyboard collectors and other malicious software. The presence of the ISG Series effectively stops all worms and viruses from propagating in the Corporation's WAN. It ensures that the information network and the WAN operate smoothly under all traffic conditions.

Further, with ISG's integration of firewall, VPN and IDP into a single management console, the Corporation now finds it much easier to configure, manage and administer security in its WAN.

"We are very pleased with the Juniper solution," said Yao. It not only handles our challenge of scale, but also incorporates comprehensive measures, such as IDP, allowing us to avoid the complexity of separately deploying and managing IDP devices. The clear access control policies provided through the ISG Series, coupled with clearly segmented network zones, means that information security during transmission and usage via the WAN is well safeguarded," he added.

Next Steps and Lessons Learned

Looking ahead, the Corporation plans to scale up its security coverage as WAN usage continues to increase. "Network security is an ongoing challenge that must be addressed continually," said Yao.

The Corporation also intends to work with Juniper Networks to continually identify security hotspots that might arise, and arrest problems before they infect the WAN.

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.

