INNER MONGOLIA ELECTRIC POWER CORPORATION SECURES WAN WITH THE ISG SERIES

Summary

Industry: Public Utility

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 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 ISG1000 and ISG2000 Integrated Security Gateways.

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

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.

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® ISG1000 and ISG2000 Integrated Security Gateways were chosen as part of the Corporation's upgraded security framework. The ISG Series is a fully integrated firewall/ VPN/ IDP system and provides gigabit or multi-gigabit performance, a modular architecture and rich virtualization capabilities.

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 Series 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 Series.

"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

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 the ISG Series 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.

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.

3520234-002-EN April 2010

Printed on recycled paper