

COFCO GAINS MOBILITY AND SECURITY WITH JUNIPER NETWORKS



Industry: Trade, Agriculture, Energy

Challenges: Combining effective remote access with comprehensive security

Selection Criteria: Mobile office/remote access, unified management of active directory, comprehensive security, future scalability

Network Solution: Juniper Networks SA4000 SSL VPN Appliance and Juniper Networks IDP50 Intrusion Detection and Prevention Appliance

Results:

- Effective remote access to mobile offices
- Enhanced productivity
- Comprehensive security
- Compliance with corporate policies
- Operation and maintenance (O&M) cost reduction

COFCO Group Limited (COFCO) is China's leading oil and food importer and exporter, and one of its largest food manufacturers. It boasts outstanding achievements in the trade of agricultural products, biological energy development, food processing, real estate, property management, hotel operation, financial services, and other areas closely related to public life. COFCO, a large scale, industry-leading enterprise under the state owned Assets Supervision and Administration Commission, is dedicated to providing high quality products produced in harmony with nature. Oil and food imports and exports are vital lifelines of China's economy and people's livelihoods; as such, COFCO carries great responsibility for its country. Historically, COFCO has lived up to its tasks, and it has been included in Fortune magazine's list of the world's top 500 enterprises since 1994.

Challenges

COFCO's employees, both at home and on business trips, are required to access the company network at any moment to improve business efficiency, productivity, and service quality—this has become a crucial component of COFCO's infrastructure. However, COFCO's sustained, rapid development has resulted in a continuous surge in its scale and number of staff. At the same time, COFCO has increasingly modernized and enriched application needs for its office network. Hundreds of staff members telecommute, requiring a "mobile office" connected to COFCO headquarters. Furthermore, as many as 1,000 employees also need to connect to the office network by accessing the intranet via VPN while on business trips. Upgrades and further development of COFCO's mobile office capabilities were necessary in order to further sustain company and employee growth, enhance its competitiveness, and make greater contributions to the development of the national economy and people's lives.

Increasing business productivity and remote access were not COFCO's only concerns; solving the problem of the mobile office engenders severe challenges to network security. Failure to provide effective control and management of the accessed host and its members could result in a huge threat to the security of network data. Additionally, connecting endpoints can become sources of virus propagation and network attacks as well. In order to effectively improve remote access, COFCO needed a reliable solution that would enhance network security, not degrade it.



Selection Criteria

Creating an office network that combines the complexity of the mobile office with complete network security has become an insurmountable and expensive quandary for most solution suppliers. Traditional VPN access requires complex configuration and high O&M costs, and it lacks assessments of client endpoint security, making it difficult to ensure end-to-end security.

Deploying additional security products may have resolved these threats, but would have undoubtedly increased COFCO's input costs, added to the network's complexity, and resulting in a series of implementation and management difficulties.

Therefore, COFCO considered its needs for office mobility and security and placed comprehensive demands on this project. The appropriate network solution would need to:

1. Meet or exceed the demand for mobile offices and remote access through VPN
2. Achieve link data security through VPN encryption
3. Realize unified management of user accounts and administration of Active Directory (AD domain)
4. Implement certificate-based user management to ensure that only those who have received a certificate from the enterprise can gain VPN access
5. Implement effective security protection of VPN access to ensure that any worm, virus, or other threats cannot be transmitted to the intranet via the VPN
6. Simplify network management to reduce management costs
7. Provide uncomplicated, quick, and easy access for user applications

Solution

While comparing network solutions, COFCO was impressed with the simplicity, high security, and low O&M costs of Juniper Networks® products. Together, COFCO and Juniper determined that Juniper Networks SA4000 SSL VPN Appliance and Juniper Networks IDP50 Intrusion and Detection Prevention Appliance would satisfy COFCO's networking requirements, and add new value to the customer experience with a combination of mobile office, remote access, and security.

All of Juniper Networks SA Series SSL VPN Appliances use secure sockets layer (SSL) transport, the secure access protocol built into every standard Web browser. SSL sessions enable any Web-enabled device such as a corporate laptop, PDA, smartphone, or kiosk to securely access an organization's resources without the cost and complexity of installing, configuring, and maintaining any client software on user devices.

The SA Series provides security for all enterprise tasks with options for increasingly stringent levels of access control to protect the most sensitive applications and data. While almost any endpoint device is capable of accessing resources via SSL VPN, Juniper Networks SA Series SSL VPN Appliances can be set to require a number of preconditions when necessary. For example, even before a login is allowed, the appliance can be set to check the requesting device's network and device settings, including scanning for malware such as keystroke loggers, and verifying operation of endpoint security software such as antivirus applications and personal firewalls. The requestor's IP address, browser type, and digital certificates can also be examined before login is allowed, and the results can be used to grant or deny access based on corporate security policies.

The SA4000 SSL VPN Appliance uses Juniper's cutting-edge technology to enable medium-to-large sized organizations to provide cost-effective remote and extranet access from any standard Web browser. The SA4000 can provide a wealth of access privilege management capabilities, allowing users to securely access an enterprise or campus intranet without the need to change infrastructure, deploy DMZ, or install any additional software.

In order to protect COFCO's network and effectively defend against attacks from worms, trojan horses, spyware, keyloggers, and other malicious software, Juniper deployed its IDP50 Intrusion Detection and Prevention Appliance at the network edge.

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances provide comprehensive and easy-to-use inline protection to stop network and application-level attacks before they inflict any damage to the network. This minimizes the time and costs associated with maintaining a secure network. Using industry-recognized detection and prevention techniques, the IDP Series provides zero-day protection against worms, trojans, spyware, keyloggers, and other malware from penetrating the network or spreading from already infected users to others.

The IDP Series also provides information on rogue servers as well as types and versions of applications and operating systems that may have unknowingly been added to the network. Armed with this knowledge, administrators can enforce security policies and maintain compliance with corporate application usage policy. In addition, the IDP Series provides DiffServ code point (DSCP) markings to allow the upstream router to enforce bandwidth limitations on nonessential applications. Not only can administrators control the access of specific applications, they can also ensure that business-critical applications receive a predictable quality of service.

The IDP Series appliances are managed by Juniper Networks Network and Security Manager, a centralized, rule-based management solution offering granular control over system behavior, easy access to extensive logging, fully customizable reporting, and management of Juniper's firewall/VPN/IPS systems from a single user interface. With the combination of highest security coverage, granular network control and visibility, and centralized management, the IDP Series is the best solution to keep critical information assets safe.

The IDP50 Intrusion Detection and Prevention Appliance offers full intrusion prevention system (IPS) capabilities to small and mid-size businesses as well as remote offices. By offering the entire suite of IPS capabilities, businesses need not compromise on security when deploying cost-effective IPS products. The IDP50 can be deployed with third-party bypass gear to ensure continued network connectivity in case of appliance failure.

Results

During the project implementation, Juniper worked closely with its agent, Transit Beijing Guanghai Science and Technology Co., Ltd. to ensure success by providing high-quality solutions, products, and expertise. The successful deployment resulted in rich authentication capabilities and a powerful mandatory inspection mechanism for endpoint security. The new access method ensures COFCO's resource security. The network is now capable of providing different login domains for different users, realizing user-based property authorization through AD domain management, and accessing different network resources according to access permission. In addition to comprehensive network security, the new products allow COFCO to implement effective management of accessed hosts and users. Best of all, for the employees who work from a mobile office and require remote access, Juniper's SSL VPN is easy to use, can be accessed through any Web browser, and does not require any installation of a software client.

As a result, different employees of COFCO can meet their individual needs according to different authorizations, completely access necessary resources, and comply with security policies on the corporate network. COFCO and its employees have high praise for the results of the project, which has not only fulfilled their requirement for a mobile office, but also greatly improved the overall security of the network. COFCO recognized that Juniper's SSL VPN is a complete solution for its secure mobile office, not only addressing the company's demand for remote access, but fully ensuring its security.

Along with gains in network security and remote access, the Juniper installation effectively protected COFCO's prior investments, as it only required a single deployment and integrated easily with COFCO's existing network. COFCO's upgraded network exceeds its current needs, thus providing powerful scalability for future development of its network application. Most importantly, the upgrades simplify network management and maintenance, reducing O&M and management costs.

Next Steps and Lessons Learned

COFCO has taken an important step toward securing the company's future performance and competitiveness. With its new remote access capability, COFCO is in an even better position to contribute to the development of China's talent pool and economy.

COFCO's success proves the value of Juniper Networks SSL VPN as a complete mobile office solution, and reflects once again Juniper's position as an industry leader in technologies, products, and services.

For More Information

To find out more about Juniper Networks products and solutions, visit 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.

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

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
Airsides Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 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. JUNOSe is a trademark of Juniper Networks, Inc. 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.

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

