

SifoWorks U Series in HiChina

Success Story



BACKGROUND

HiChina is one of the largest domain name and web-hosting service provider in China. Started in 1996, with investments from U.S.'s risk investment company IDG and Newbridge Capital, HiChina has become the flagship for China's internet service industry. HiChina has been focusing on building an e-infrastructure in China using high cost-to-performance virtual host technology to help companies set up their own website to conduct online trading with minimum capital.

Years of hard work has allowed HiChina to establish a strong network operation management system and software development capacity. HiChina has helped its clients register almost 600,000 Chinese and English domain names, and has provided fast, stable, secure web and email hosting services for over 100,000 enterprises. Its massive server farms, found in Beijing, Shanghai, Hong Kong, U.S.A., and others cities, has helped China companies to accomplish e-commerce and become the new economic engine of the world.

HiChina's headquarters is located in Beijing, with branches in major Chinese IT cities such as Shanghai and Guangzhou. Thousands of agencies from 31 cities all over China have signed up with HiChina, tapping into its vast business capabilities for a wide range of customer services.

With market demands, data transmission between each level of branches has increased significantly, and the demand for real-time data has soared. HiChina systems have relied on the Internet for inter-connectivity, but with massive data transmission demands, data security is a serious consideration, and an urgent problem to solve.

ANALYSIS

Based on the current network situation and needs, the VPN should be set up to accomplish the following goals:

- Headquarters and each branch office can access each other quickly and securely via the Internet.

Customer

HiChina

Industry

Domain Name and Web Hosting

Business Challenge

Headquarters and branch offices needed to communicate via Internet securely, quickly and easily. Ensure VPN is reliable, easy to manage and expandable.

O₂Security Solution

SifoWorks U Series

Benefits

SifoWorks U Series is: Robust, Feasible, Integrated, Affordable and Secure

- Ensure the key node in the VPN is reliable.
- The VPN is easy to manage and maintain.
- The network is expandable

To fulfill the above goals, the proposed VPN solution is based on the following design principles:

1. In accordance with the country's related law.
2. Balanced assessment of need, risk and cost: quantitative analysis on threats and possible risk, and then design the standards and measures for the system's security policies.
3. Integration: using system engineering perspectives and methods to analyze the network's security issues, and create specific policies.
4. Consistency: network security problems should exist in the whole network's operation cycle, and customized security system structure should be consistent with network security needs.
5. Ease of implementation: policies that are overly complicated and impose high demand on users decrease security.
6. Adaptability and flexibility: able to adapt to changes in the network's performance and security needs, and ability to be modified quickly.
7. Multi-layered protection: to build a multi-layered protection system, where each layer protects and complement each other. When a layer is breached, the other layers can still ensure the security of the information.
8. Redundancy: for better network expandability, the VPN's processing capability must consist of redundancy to prepare for future network device link expansion.

DEPLOYMENT

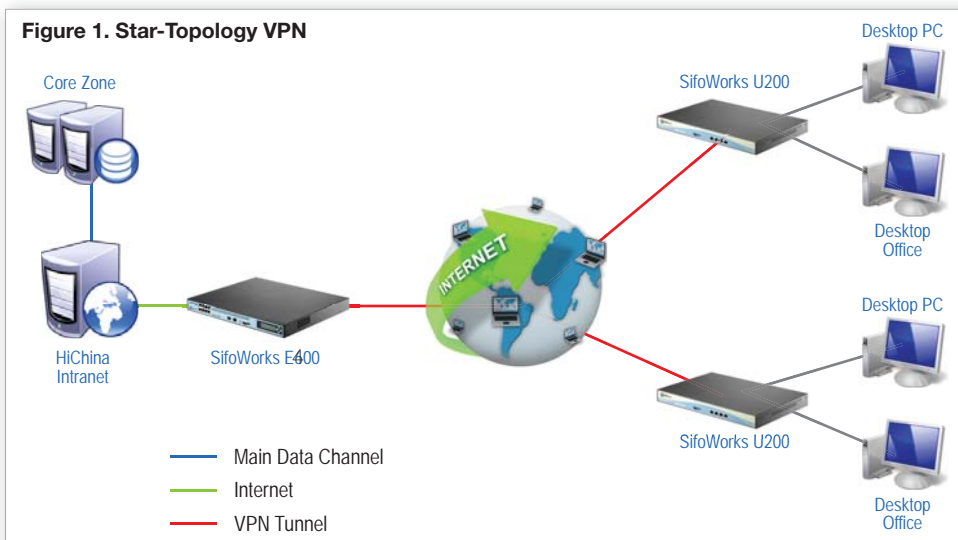


Figure 1. shows a Star-Topology VPN deployment. This deployment structure connects the branches to the headquarters via VPN.

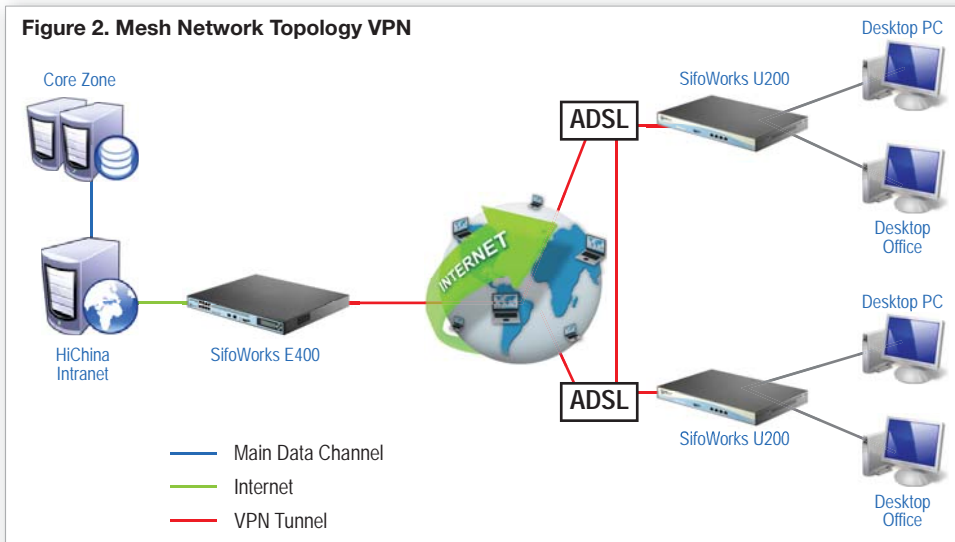


Figure 2. shows a Mesh Network Topology VPN deployment, which besides connecting each branch with headquarters, also allows branches to inter-transmit data securely via the VPN. At the same time, corresponding access rules are set up at the firewall to ensure effective control over business operation.

As shown in the diagrams, SifoWorks E400 firewall will be deployed as the VPN gateway at the headquarters' network exit. In each branch office's gateway SifoWorks U-Series is deployed as the branch's VPN gateway.

Implement corresponding security policies, such as:

- Setting up the VPN system using Wizards, following the step-by-step instructions to build the connections between headquarters and branches.
- Configure strict access control policies, for example: setting up a policy where only the necessary port is opened for access to LAN zone, and ensure that only a specific internal host address can access the WAN zone.
- Utilizing the firewall's NAT function to conceal internal IP addresses, thus preventing IP address (TCP/UDP port) scanning – a prelude to a hacker's attack.
- SifoWorks U-Series firewall is capable of performing real-time scanning on a wide range of traffic such as HTTP, FTP, POP3, SMTP, etc. This ensures that viruses, worms and malware embedded in web pages and email are stopped at the gateway.
- Using URL filtering technology, the system is shielded from most unhealthy websites, effectively blocking harmful access and reducing risk of virus infection.
- Using the firewall's powerful real-time monitoring function, specific access can be immediately disconnected in time. Also, detailed auditing can be done on firewall connections using its web auditing functions.
- For Instant Messaging and P2P downloading tools that creates security loopholes and hogging network bandwidth, SifoWorks U-Series allows the company to manage these tools with ease. HTTP and FTP uploading and downloading content can also be controlled by blocking specific attachment filenames and filtering out ActiveX, Java and Cookie information embedded in web pages.

Deployment's main features:

- **Robustness:** the VPN comes with its own internal security operating system powered by dedicated chips.
- **Adaptability:** able to adapt to structural changes of the network due to adjustment or expansion.
- **Standardization:** built in accordance to the standard IPSec protocol.
- **Feasibility:** fast deployment and maintenance with no disruption to normal business operations.
- **Integrated:** providing network security access control, encrypted transmission, node authentication, user authentication and security auditing functions.
- **Headquarters VPN gateway** supports static IP while each branch VPN gateway supports dynamic IP.
- **Low cost:** helps companies build their own private network using the Internet as backbone.
- **Secure:** using certificates for authentication and asymmetric encryption method to protect secret key exchange. Encryption algorithm is also very reliable.
- Supports network-mesh traffic.
- Seamless support for NAT traversal

ABOUT O₂SECURITY

O₂Security Limited is a subsidiary company of industry-leading analog and digital IC chip designer O₂Micro (NASDAQ: OIIM). O₂Security provides complete, comprehensive security solutions that are easy to use and maintain. Since its inception in 2003, O₂Security Ltd. has consistently developed highly-anticipated products that meet the needs of the network security industry. Nearly 70% of its research capital goes into developing new products and enhancing existing ones to meet current market trends.

O₂Security Ltd. has service offices located in many regions around the world including; the United States, Taiwan, Singapore, Malaysia, Indonesia, Philippines, Vietnam, Thailand and various locations in China. This allows us to provide localized and on-site support to our clients, gather information on security issues and emerging market trends on a global scale, continually improve and develop new products in response to market changes and meet the needs of our customers.

O₂Security

3118 Patrick Henry Drive
Santa Clara, CA 95054

Tel: 1.408.987.5920

Fax: 1.408.987.5929

www.o2security.com

Email: sales_us@o2security.com

support_us@o2security.com
