

# Korean Information Service Corporation

## Korea Telecom Subsidiary Improves Service, Reduces Costs with Secure VoIP VPN

Partnering with Fortinet, the Korean Information Service Corporation (KOIS), a unit of Korea Telecom, deployed a VoIP/data VPN using Fortinet's FortiGate Network Protection Gateways to provide comprehensive network security and to manage mission critical voice and data communication between its call center and home-based call-center agents. Estimating a rapid return on investment, KOIS plans to increase its number of home-based call agents in the VPN, further reducing operational costs.

### Situation

After regular business hours, KOIS routes directory assistance calls to home-based call agents who answer telephone requests and perform database searches from their home PCs. Using ISDN services to connect these home agents, KOIS faced high line costs and substandard performance and service levels. A rising number of customer complaints forced KOIS to search for a new solution or return its home agents to the call center, increasing overhead costs and decreasing employee morale.

KOIS chose to replace ISDN connections with high-speed, Internet-based ADSL connections and to build a VoIP/data VPN to transmit voice and data communication between the call center and telecommuters. While the solution resolves performance issues, security risks associated with Internet based connections needed to be resolved to make the VoIP VPN a viable solution.

The VoIP/data VPN needs to meet stringent requirements to successfully manage the transmission of critical and sensitive data using Internet-based connections. A new solution must:

- Improve system performance, and provide system stability and reliability, producing less than a 1% error rate every 24 hours;
- Provide voice quality that matches the service quality provided by conventional telephone lines;
- Offer fast response times, allowing home agents to receive data base search results within 2 seconds;
- Integrate seamlessly, requiring no reconfigurations of the legacy network.

Security is a primary concern due to the large volume of sensitive data transmitted between the call center and home agents. In today's environment, where Internet users face continuous and ongoing security risks, KOIS requires complete network protection that addresses all security issues including firewall and VPN security, Antivirus (AV), worm scanning and content filtering.



**Korea Telecom**

*"Our directory service is a critical offering used by millions of customers. We chose Fortinet because the company delivered a reliable, high-performance solution that met our rigorous requirements and high standards for system availability, voice quality/performance, system response time, and most important, airtight security for our crucial data resources."*

**- Mrs. Young-Hwa Lee  
Senior Systems Manager**

# Korean Information Service Corporation

## Korea Telecom Subsidiary Improves Service, Reduces Costs with Secure VoIP VPN

### Solution

Converging voice and data communication in a VoIP/data VPN provides a cost-effective solution for the KOIS call center and geographically dispersed home agents; however, Internet-based connections increase security risks that conventional VPN technologies alone cannot resolve.

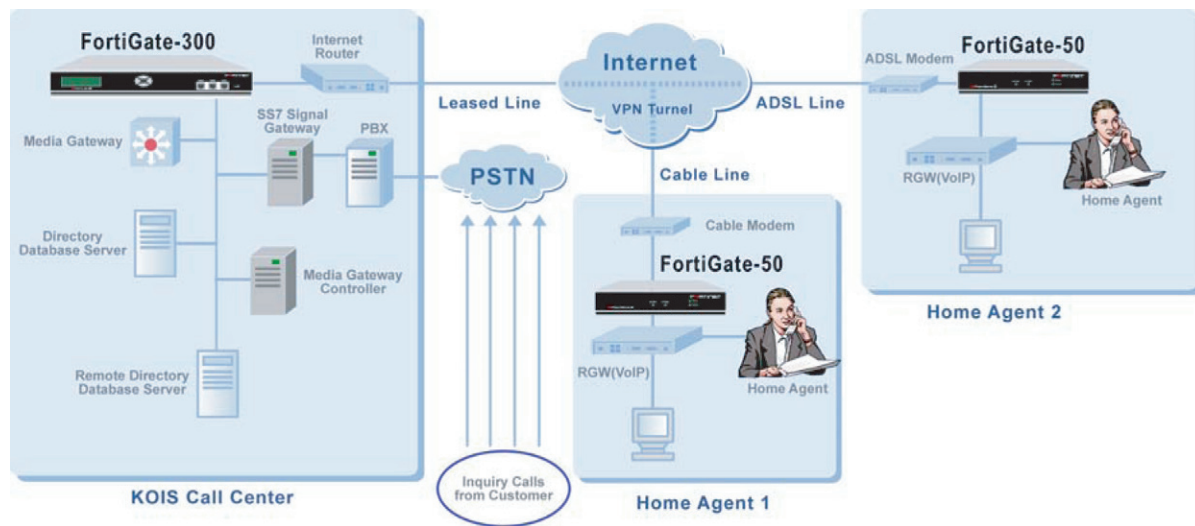
KOIS deployed FortiGate Network Protection Gateways to fully secure the VPN while maintaining required performance levels and system requirements. FortiGate-300 Network Protection Gateways were installed at the call center, and FortiGate-50 Network Protection Gateways were installed at each home agent's site.

When a customer calls KOIS, the call is routed over the PSTN to the KOIS PBX. The Media Gateway converts the voice call to IP packets, the status of home agent is then obtained from the Media Gateway Controller. The Media Gateway Controller routes the voice packets to the FortiGate-300 Network Protection Gateway where they are encrypted and transmitted over the Internet in a VPN tunnel. The home agent's FortiGate-50 decrypts the voice packets and the home agent receives them as an IP telephone call.

When a home agent requests data, the request is encrypted by the home agent's FortiGate-50 and sent over the VPN tunnel to the FortiGate-300 where it is decrypted and sent to the Remote Directory Database Server. Data is returned over the same VPN tunnel.

Voice and data communication pass through the FortiGate-300 and FortiGate-50 in both transmit and receive directions, providing security for incoming and outgoing calls and data transmission.

### KOIS VoIP VPN Deployment



# Korean Information Service Corporation

## Korea Telecom Subsidiary Improves Service, Reduces Costs with Secure VoIP VPN

### Success

Internet connections pose a constant security risk to the KOIS VPN and the KOIS call center internal network. Conventional firewalls or VPN tunnels do not stop viruses or banned content. Host-based AV software provides end-user protection only and does not provide sufficient protection to the KOIS VPN where telecommuters connect to the network from home computers. Other residents in the home may share the same computer and may unknowingly introduce a virus or worm from an email attachment or other Internet source. The FortiGate-300 protects the KOIS call center internal network from Internet threats. To protect the KOIS network from



FortiGate300

increased exposure to threats introduced by home users, each home user's FortiGate-50 provides intrusion detection and antivirus and worm protection for the home network. In addition the FortiGate-50s and the FortiGate-300 at the KOIS network edge remove viruses from all content transmitted over the VPN.

Fortinet was able to provide network security and meet the stringent system requirements KOIS needed to deploy a VoIP VPN solution:

- Voice encryption for the VPN tunnel is accelerated by FortiASIC™ Content Processors, resulting in VoIP calls that match voice quality benchmarked by calls made over telephone lines.
- High performance FortiASIC™ Content Processors provide real time antivirus and content screening as well as data encryption/decryption.
- Traffic shaping guarantees that latency-sensitive voice applications are given priority.
- FortiGate Network Protection Gateways seamlessly integrate, at the network edge, with existing network configurations.
- FortiGate Network Protection Gateways combine firewall, virus and worm scanning, intrusion detection, and content and URL filtering in a single, cost-effective platform, reducing equipment and management costs.

Fortinet and KOIS performed a three-month trial of the ADSL VoIP/data network secured by FortiGate Network Protection Gateways. No service problems were found during the trials. Call transfer costs were reduced. Service quality and productivity improved.

KOIS now plans to increase its number of home agents and decrease the number of call agents in the central site over the next two years, further reducing overhead costs by decreasing space requirements at its headquarters. Ken Xie, founder and CEO of Fortinet Inc. states: "With the Fortinet data/VoIP VPN solution in place, KOIS can continue to scale. They have the flexibility to increase the number of remote call center agents to meet rising customer demand while reducing operating costs demonstrably."

### Learn more at [Fortinet.com](http://Fortinet.com)

[Fortinet.com/contact](http://Fortinet.com/contact)

Tel: +1-408-235-7700 - Sales: +1-866-868-3678 - Tech Support: +1-866-648-4638