



Incumbent Local Exchange Carrier Automates Network Security

Executive Summary

Customer: Farmers Telecommunications Cooperative

- Telecommunications
- Alabama, USA
- 18,000 customers

Business Challenge

- Accommodate more broadband subscribers
- Respond to security threats before performance is affected
- Facilitate complex troubleshooting

Network Solution

- One-chassis solution: router with integrated modules for security and network analysis
- Security software for monitoring network health
- Network telemetry data for service analysis

Business Result

- Enabled a proactive rather than reactive response to network issues, including security
- Eliminated time-consuming, manual troubleshooting steps
- Acquired capabilities needed for future voice, video, and managed security service offerings

Farmers Telecommunications Cooperative simplified troubleshooting using Cisco® Router with Cisco monitoring and management tools.

Business Challenge

Farmers Telecommunications Cooperative (FTC) is the incumbent local exchange carrier (ILEC) serving the northeast region of Alabama, founded by citizens in 1952 to provide reliable telephone service in their area. Today FTC serves 18,000 telephone customers and 7000 Internet customers on DSL and dialup. FTC also provides wireless data service for customers beyond the reach of DSL.

In 2004, FTC began promoting a bundle for long-distance telephone and ADSL service, and the number of DSL subscribers more than tripled in the first year. Rapid growth created urgent new network requirements. The obvious need was for additional DSL termination capacity. But other needs emerged as well. “The larger the network, the more important it is to have automated network management capabilities, especially with a small IT staff,” says Jerry Smith, Internet operations manager for FTC. “Growth also makes network security even more crucial because you become more visible to hackers.”

Indeed, soon after introducing the new service, FTC experienced its first denial-of-service (DoS) attack, launched from within the network by hackers who had compromised customers’ computers. “When the attack occurred I was able to use a network analyzer to identify the nature of the attack and stop it before it did major harm,” says Smith. “But the incident convinced us we needed a way to protect ourselves that did not depend on me or another IT staff member being present in our offices. We needed visibility into all traffic flowing across our networks, and continuous monitoring for anomalous network behavior.”

FTC approached vendors of broadband router access servers (BRAS) and network security solutions and conducted field trials. Smith began with two requirements: the ability to detect security threats and automated response. After the first trials he added another requirement: “I wanted to know what the solutions did today – not what the vendor expected them to do in six months.”

Network Solution

FTC selected a BRAS and network security solution from Cisco Systems® provided by Information Engineering of Huntsville, Alabama, a Cisco Premier Certified Partner. Paul Coggin, manager of network technologies for Information Engineering, met with FTC many times to understand its needs. He says, “Although FTC’s immediate need was for DSL termination, further discussions revealed a need for a more automated and adaptive approach to network security, as well as the network management capabilities required for future voice and video service offerings.”

Information Engineering deployed a single-chassis solution consisting of the Cisco 7613 Router with slots populated by a Cisco Firewall Services Module (FWSM), Cisco Intrusion Prevention System (IPS) module, and Cisco Network Analysis Module (NAM). Six multiprocessors on a Cisco Multiprocessor WAN Application Module (MWAM) replaced standalone routers that FTC used to connect to its original DSL network, its new ADSL network, and its wireless cellular subsidiary. “A single redundant chassis with multiple service modules provides exceptional ease of management, which is especially appealing for ILECs and other service providers with limited IT staff,” says Coggin.

Cisco NAM facilitates troubleshooting by collecting real-time statistics on all network traffic flows. Built-in Cisco NetFlow technology collects telemetry data from the routers themselves. Smith and his team analyze the NetFlow data using open-source network analysis software to understand trends and plan capacity for various traffic types including voice, peer-to-peer, and Web.

Because Cisco NAM is deployed on the core switch fabric, it can collect data from all of FTC’s networks: DSL, cellular, and corporate. “Cisco NAM helps us quickly identify the source of a range of problems, from slow performance to a customer’s inability to authenticate to quality-of-service [QoS] issues,” says Smith. “It has already paid for itself a few times over by detecting multiple small problems that don’t necessarily bring down the network but nevertheless affect performance.” In the past, when Smith spotted problems he first had to locate the correct subnet, which could take hours, and then connect a network analyzer. “With Cisco NAM, I can simply say, ‘Monitor these subnets, collect the data, and I’ll look at it later,’” he says. “I save hours for each incident.”

Cisco Security Monitoring, Analysis, and Response System (MARS) software complements Cisco NAM by providing a snapshot of the networks, including all routers and switches. It continuously aggregates and correlates alerts and logs from the router’s service modules, spotting anomalies much faster than a human could. Cisco Security MARS superimposes relevant information on a network map so IT staff can instantly see the location of security issues. “Cisco routers and switches produce a tremendous amount of information, and the answer to network problems is generally buried within all that information,” says Smith. “But when network performance is compromised, we don’t have the days or weeks it would take to sort through it all. Cisco Security MARS does it much more quickly, identifying for us the precise area of the network where the problem resides. It reduces network ‘noise’ and just shows me what’s important.”

“The Cisco NAM and Cisco Security MARS give us the automated capabilities to ensure consistent network performance. I would not have attempted to offer IP/TV prior to deploying the Cisco solution because we simply did not have the required security, QoS, monitoring, management, and reporting capabilities.”

– Jerry Smith, Internet Operations Manager, FTC

Business Results

The integrated solution from Cisco meets FTC's current needs for DSL termination, security, and management, and it equips the network to provide future voice and video services.

Network security posture has improved. "Security must be the primary concern in any service provider network, no matter the size," says Smith. The first time Smith used Cisco Security MARS, the network map showed numerous current attacks. When he looked at the map in January 2006 there were no attacks, an improvement he attributes to the effectiveness of the Cisco FWSM and Cisco IPS modules in enforcing policy, as well as a security assessment that Information Engineering provided.

Moreover, Cisco NAM and Cisco Security MARS enable a proactive rather than reactive response. Cisco NAM provides visibility into every network, subnet, and VLAN. It gives the IT group a visual representation of virus and worm traffic and other issues in real time, before they become a problem, so that IT no longer finds out about problems from customer phone calls or upstream service providers. "ILECs often don't know they have a network problem until it's widespread and causing outages," says Coggin. "With Cisco Security MARS, FTC finds out about problems as they occur – when there is time to take action before the problem becomes noticeable." For example, if someone in IT logs into the supervisor engine and inadvertently changes configuration settings, Smith receives automatic notification.

Troubleshooting takes far less time. "Before we had the single-chassis solution, if I wanted to collect data from other network routers, I had to grab my network analyzer, locate the VLAN with the problem, and mirror the port," says Smith. "By that time, half the day was gone. Now that all traffic flows through a single router, I no longer need to spend time looking for the correct VLAN and port. The Cisco network monitoring and management tools free me from constantly monitoring for problems, and instantly alert me to important issues."

Secure instrumentation and visualization, as well as QoS, have prepared FTC to introduce voice and video service offerings. Voice and video traffic is less forgiving of network issues than data traffic because infections that might merely slow Internet traffic can bring real-time voice and video service to a halt, according to Smith. "If an infected network carries Internet traffic only, you might simply notice that the network is a bit slow," Smith says. "But if the network also carries real-time voice and video traffic, service can slow to a crawl or stop entirely. The Cisco NAM and Cisco Security MARS give us the automated capabilities to ensure consistent network performance. I would not have attempted to offer IP/TV prior to deploying the Cisco solution because we simply did not have the required security, QoS, monitoring, management, and reporting capabilities. Now we do."

Next Steps

FTC plans to introduce voice and video services in 2006. It also plans to take advantage of the traffic shaping capabilities of the Cisco 7613 Router to offer tiered pricing based on bandwidth usage. FTC will use the Cisco NAM to determine which applications use the most bandwidth and help formulate policy. Future plans might include managed security services for business customers, such as managed firewall or managed intrusion prevention. Integrated network management and security capabilities give FTC the confidence to expand its service offerings to fulfill its mission to remain the area's premier provider.

Product List

Routers and Routing Systems

- Cisco 7613 Router

Interfaces and Modules

- Cisco Multiprocessor WAN Module (MWAM)

Network Management

- Cisco Network Analysis Module (NAM)
- Cisco Security Monitoring, Analysis and Response System

Security and VPN

- Cisco Firewall Services Module (FWSM)
- Cisco Intrusion Prevention System (IPS) Module



For More Information

For more information about Cisco network management solutions, visit:

http://www.cisco.com/en/US/products/hw/modules/ps2706/prod_module_series_home.html

For more information about Cisco Security Monitoring, Analysis and Response System, visit: www.cisco.com/go/mars

For more information about Cisco Network Analysis Module, visit: www.cisco.com/go/nam

For more information about Cisco 7600 Series Routers, visit: www.cisco.com/go/7600

For more information about Cisco NetFlow technology, visit: www.cisco.com/go/netflow

For more information about managed services for businesses, visit: www.cisco.com/go/managementservices

This customer story is based on information provided by Farmers Telecommunications Cooperative and describes how that particular organization benefits from the deployment of Cisco products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)