

U.S. Soccer Federation

Organization Scores Goal with Fortinet's Consolidated Network Security

Case Study

Situation

The U.S. Soccer Federation is the governing body for soccer organizations in the United States and has helped chart the course for the sport in the U.S. for more than 90 years. Since inception, the Federation's mission statement has been very simple and very clear: to make soccer, in all its forms, a preeminent sport in the United States and to continue the development of soccer at all recreational and competitive levels. Founded in 1913, U.S. Soccer is one of the world's first organizations to be affiliated with FIFA, the Federation Internationale de Football Association, soccer's worldwide governing body. U.S. Soccer has continued to grow in the 90-plus years since, and now has the largest membership among U.S. Olympic Committee national governing bodies.

The U.S. Soccer Federation has three national locations being supported by its small IT staff – the Federation's Chicago, Ill., headquarters, offices under The Home Depot Center in Carson, Calif., and the Under-17 Residency Program in Bradenton, Fla.

Having dozens of employees working from different locations, with many working over wireless networks, the Federation realized the need for perimeter security in addition to its core network security solution already deployed. The U.S. Soccer Federation started its search for a new firewall vendor that would replace the previous outdated solution and grow with the future needs of the Federation.

"When we looked for a network security vendor for our locations we were just looking for a firewall solution," said Roland Bellington, technology manager, U.S. Soccer Federation. "We quickly came to realize the power of FortiGate® multi-threat security appliance and its ability to add security functionality without having to deploy many new devices.

Solution

After looking at multiple solutions for its firewall needs, The U.S. Soccer Federation selected the Fortinet® integrated and unified threat management solution. The other vendors, Cisco and CheckPoint, had solutions that burdened the customer with a complicated licensing framework. Fortinet's unlimited user licensing model allowed for U.S. Soccer to grow without the need to monitor users and update licensing on the network security solution.

U.S. Soccer's headquarters consist of two refurbished mansions, dating to 1873 and 1886, located in Chicago's Prairie Avenue Historical District. Although located within a historic house, the network security solution is anything but archaic. Deployed in 2003, a FortiGate®-100 series appliance was used at the Chicago headquarters to provide firewall protection for the Federation's headquarters' network. As the Federation grew and the network needs expanded, the FortiGate-100 series was replaced with the enterprise level FortiGate-800 appliance. With Fortinet's unique approach to integrated and consolidated network security, the IT staff was able to easily increase the amount of network security functionalities from firewall to firewall, antivirus and anti-spam – without deploying additional devices. With content level security enabled, critical Federation information including email, employee records and accounting systems are protected from malicious attacks.

Also in 2003, U.S. Soccer opened its National Training Center at The Home Depot Center in the Los Angeles suburb of Carson. Seating 27,000 fans in its soccer stadium, The Home Depot Center offers several fields for training purposes and serves as the headquarters for the U.S. National Teams and



Deployment

FortiGate-800
FortiGate-100A
Forti-Wifi-60B

Industry

Professional Sports

"Fortinet appliances are exactly what we required and more. We started with simple goals, but have been able to easily add network security functions without additional costs and without the hassle of installing new appliances."

Roland Bellington

*Technology Manager,
U.S. Soccer Federation*

the home stadium of two teams in Major League Soccer - the Los Angeles Galaxy and Chivas USA. Located below the stadium concourse, U.S. Soccer's office must support approximately a dozen full-time staff working out of the National Training Center, as well as numerous visiting staff throughout each year; however employees initially experienced weak mobile phone coverage and poor reliability as a result of its unique environment. In order to solve this problem, a majority of the employees now use Blackberry Curves with Wifi enabled. This, however, brings up an additional security challenge for the location. If an employee is using their Blackberry to do work on the network, then the connection should be segmented and protected from other networked assets. To accomplish this goal, U.S. Soccer deployed a Fortinet FortiWifi™-60B appliance. The wifi capability of the appliance allows wireless network users to securely connect to the office network.

In addition to the FortiWifi-60B appliance deployed at the Carson location, the U.S. Soccer Federation has also deployed a FortiGate-100A appliance to provide perimeter firewall, antivirus and anti-spam protection for the wired network at the office. By protecting the network with the FortiGate-100A appliance, the IT staff is ensured that no unwanted traffic will be able to traverse the network and cause damage to the private network.

Along with the Chicago headquarters and Carson office, U.S. Soccer has a third, smaller office located in Bradenton, Florida. This location is the site of the U.S. Soccer Residency Program, where 40 players train daily, attend classes and represent the country in international competition as the U.S. Under-17 Men's National Team. In order to manage and run the program from its small office adjacent to the training fields, the staff in Bradenton relies on Fortinet's FortiWifi-60B appliance to keep them safe from network intruders including malware and other Internet-borne threats. The FortiWifi appliance in Bradenton is being used for firewall, antivirus and anti-spam protection. With very limited office space and the need for wireless access, the FortiWifi appliance was a perfect fit.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection—including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in seven programs by ICSA Labs: (Firewall, Antivirus, IPSec, SSL, Network IPS, Antispyware, and Antispam). Fortinet is privately held and based in Sunnyvale, California.

FORTINET®

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated
3 Temasek Avenue, Level 21 Centennial Tower
Singapore 039190
Tel +65.6549.7050
Fax +65.6549.7259

©2006-2008 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are trademarks or registered trademarks of the Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600. Although Fortinet has attempted to provide accurate information in these materials, Fortinet assumes no legal responsibility for the accuracy or completeness of the information. Please note that no Fortinet statements herein constitute or contain any guarantee, warranty or legally binding representation. All materials contained in this publication are subject to change without notice, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Success

Since the first FortiGate appliance installation at U.S. Soccer's headquarters, the organization has expanded its deployment of FortiGate appliances. Noted benefits include: familiarity in management due to the consistent GUI across the various models, increased security by being able to block specific, unauthorized instant messaging protocols, as well as reduced space and power requirements enabled by network security consolidation.

"Although we have a variety of Fortinet appliances deployed within the U.S. Soccer Federation network, we had absolutely no problem getting the appliances up and running and making immediate use of them," added Bellington. "The consistent GUI across the product line is great and there's something comfortable about the appliances that innately makes sense from a network manager standpoint. In the five years we have been using Fortinet, I've only had to call technical support twice."

With the increasing use of instant messaging protocols, such as AOL Instant Messenger, the importance of protecting these forms of communication becomes greater. Using Fortinet's FortiGate appliances, U.S. Soccer can block instant messaging protocols that violate acceptable use policies as well as block all instant messaging data transfers.

Fortinet's integrated and consolidated network security platform allows companies of all sizes to scale its network security solution to its current and future needs. The U.S. Soccer Federation initially needed a firewall solution, but was soon able to add antivirus and anti-spam protection as corporate needs grew. What would normally require multiple vendors and multiple appliances was done with Fortinet's unique FortiGate platform.

Bellington concluded, "The Fortinet appliances are exactly what we required and more. We started with simple goals, but have been able to easily add network security functions without additional costs and without the hassle of installing new appliances."