

# M. D. Anderson and Cisco Systems— Fighting Cancer Across Secure Networks

## Introduction

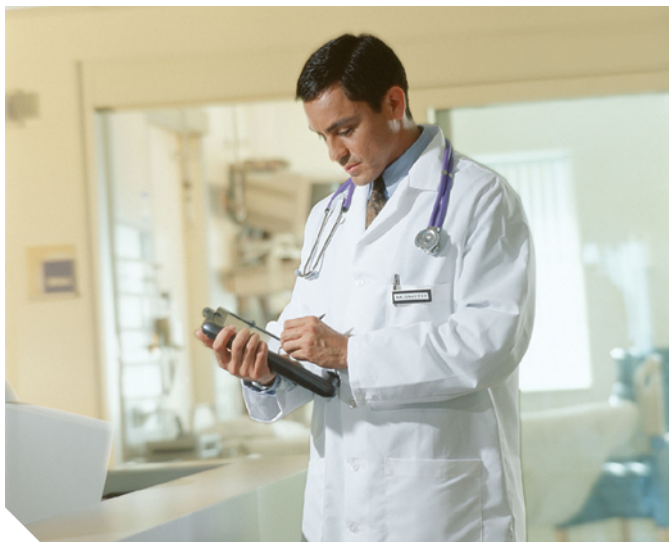
**Founded by the Texas State Legislature and the M. D. Anderson Foundation on the site of the University of Texas at Houston, the University of Texas M. D. Anderson Cancer Center is devoted to the prevention and eradication of cancer in all of its forms. Since its beginnings in 1941, more than half a million patients have come through M. D. Anderson's doors looking for answers and hope, and found both. M. D. Anderson (MDA) has trained more than 40,000 cancer professionals who work all over the world. Its researchers have paved the way for an impressive arsenal of modern cancer treatments. M. D. Anderson's mission has always remained the same: to eliminate cancer in Texas, the nation and the world.**

In the 21st century, world-class health care depends on many variables, including sufficient funding, the right people, and increasingly, robust, flexible, and secure communications infrastructures. More research and patient information traveling across intranets, extranets, and the public Internet drives the need for comprehensive security architectures. Furthermore, with the advent of the Health Insurance Portability and Accountability Act of 1996

(HIPAA), health care organizations must be prepared to comply with government regulations regarding the security and privacy of health-related data. In true MDA style, the MDA information technology (IT) organization chose to address the security challenge with the implementation of an extensive security architecture consisting of world-class solutions.

## Ensuring Privacy and Security with Cisco Solutions

MDA provides care for approximately 65,000 patients each year, and highly personal data about each patient must be securely maintained and transmitted. To provide the highest quality care, doctors often share historical and diagnostic patient records, via electronic correspondence, with a widespread team of medical professionals. In addition, doctors may need to assess critical patient data while at home or traveling. The MDA IT staff had to work diligently to effectively secure patient information, as well as personnel and financial data, that is shared among doctors and transmitted between remote locations.



Cisco Systems, Inc.

Leading the security team at MDA is Lew Wagner, Chief Information Security Officer. Mr. Wagner is responsible for protecting all electronic information as it passes in and out of MDA, and as it is processed or stored. According to Mr. Wagner, "...you have to be able to protect yourself against a broad range of attack vectors. In other words, consider that you're defending your yard from attackers. If all you had to worry about was the front yard, you could devote all your time to putting up fences in the front yard. But what if it's coming from the back yard or the side yard or from up above? What if it's coming through all of those areas at the same time? You have to be able to develop a way to watch all those sort of things." He adds, "...threats nowadays are not single vector attacks. They are multi-vector attacks that will come in across multiple phases or multiple channels."

With those considerations in mind, Mr. Wagner designed a comprehensive, layered security architecture in order to efficiently protect every area of the MDA network. The architecture was fashioned like the SAFE blueprint from Cisco—a modular approach that simplifies security design, rollout, and management as networks grow and change. A SAFE network consists of best-in-class security products and services. Working with a team of Cisco security experts, Lew Wagner and his team chose to implement a variety of Cisco-based solutions for intrusion protection, virtual private networking, firewalling, wireless access, and security management.

#### Layered Security: Intrusion Protection at M. D. Anderson

The new era of open and trusted communications brings new vulnerabilities and problems, causing health care organizations to protect their sensitive data from a wide range of network attack types. What's more, attacks are generated by not only external hackers, but also by seemingly trustworthy internal employees.

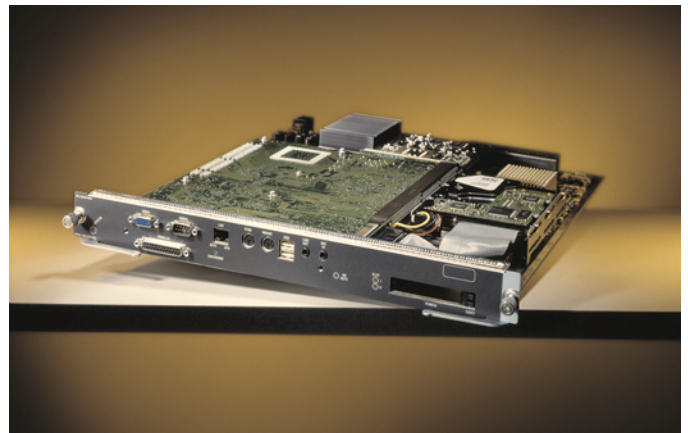
MDA deployed Cisco PIX<sup>®</sup> firewalls in its overall dynamic-defense-in-depth (D3) firewall matrix to protect critical node areas of its network. MDA chose Cisco PIX firewalls for their high fail-over and availability capabilities. However, the MDA security team knew the importance of a layered approach to security. They knew that they must implement intrusion protection technologies to counter risk and vulnerabilities that firewalls alone cannot address.

Cisco intrusion detection system (IDS) solutions deliver the complete intrusion protection necessary to safeguard organizations from costly and debilitating network attacks, such as Internet worms, denial-of-service attacks, and e-business application attacks. Incorporating the latest in attack identification techniques, Cisco award-winning IDS combats known attack types and preempts emergent attacks. Cisco IDS provides enhanced security beyond classic technologies, by addressing dynamic, changing threats and helps to increase the resiliency of e-business systems and applications.

MDA's core and divisional sites house Cisco Catalyst<sup>®</sup> 6500 Series switches that are the foundation of MDA's switched infrastructure. The Catalyst 6500 Series switches address MDA's increased requirements for gigabit scalability, high availability, and extensive services. Lew Wagner's team chose to integrate IDS functionality into their switches by implementing Cisco Catalyst 6500 IDS Services modules (Figure 1). The Cisco Catalyst 6500 IDS Services modules specifically address switched environments by incorporating IDS functionality directly into the switch back plane, enabling both switching and security functions in the same chassis. Easy to install and maintain, the Cisco Catalyst 6500 IDS Services modules do not degrade switch performance as they work around-the-clock to provide real-time protection from a wide array of attacks.

Figure 1

**Cisco Catalyst 6500 IDS Services Module**—Easy to install and maintain, the Cisco Catalyst 6500 IDS Services modules do not degrade switch performance as they work around-the-clock to provide real-time protection from a wide array of attacks.



MDA currently has eight Cisco Catalyst 6500 IDS Services modules in place. Lew Wagner talked about the Cisco IDS modules (blades) capabilities: "When we decided on the blades, we were looking for speed—we wanted something that was fast and transparent. We have had extremely good input from the IDS blades and a very close working relationship with Cisco to getting that information working for us. Now, we've got real-time intrusion detection alerts." Mr. Wagner also said about his Cisco IDS deployments, "...this has given me a view into the network flow across the institution so that I can better understand, anticipate, and proactively try to stop certain attacks that can occur either from the outside or the inside. Whereas before I had no capability to do that. This gives me, from the security perspective, ...another piece of the puzzle."

To configure and manage the Cisco Catalyst 6500 IDS Services modules, the security team chose the CiscoWorks VPN/Security Management Solution (VMS). Cisco VMS enables MDA's security administrators to monitor both normal and suspicious network

traffic, coming in and leaving the network. VMS correlates information coming from the IDS modules and enables administrators to be proactive. Cisco VMS allows MDA administrators to design, distribute, enforce, and audit network-wide security policies from a central location so they can proactively address problems.

Because of its positive experience with the Cisco Catalyst 6500 IDS Services modules, the MDA IT group decided to evaluate the Cisco host-based intrusion detection system (HIDS) solution. Cisco HIDS detects attacks occurring on the host on which it is installed. It intercepts OS and application calls, secures the OS and application configurations, validates incoming service requests, and analyzes local log files for after-the-fact suspicious activity. MDA was running a trial copy of the Cisco IDS Host Sensor when the NIMDA worm attacked many organizations throughout the world. The Cisco IDS Host Sensor was able to identify the worm and protect MDA's data infrastructure from serious damage.

#### Extending M. D. Anderson: Virtual Private Networking

With an infrastructure that's expanding, many functions at MDA are geographically dispersed. For example, the Human Resources and Facilities departments are located off site, so employee and facilities management data must be securely transmitted to and from those remote locations. Also, the off-site ambulatory treatment center houses a pharmacy and clinic to which private patient data, such as patient prescriptions, is transferred. In addition to transmitting data to remote sites, MDA communicates with other hospitals. Taking advantage of MDA's advanced capabilities, hospitals throughout the world will send patients to MDA for testing and then MDA must quickly and securely transmit the test results back to the patients' local doctors.

MDA uses Cisco VPN-enabled routers to establish secure, site-to-site VPN tunnels to its remote locations and extranet partners. MDA implemented Cisco 7200 Series VPN routers at the head-end and 7100 Series routers at the remote sites to extend its campus with IPsec-compliant, encrypted VPN tunnels. MDA also chose to use the VPN Acceleration Module for Cisco 7100 and 7200 Series routers, which provides high-performance, hardware-assisted encryption, key generation, and compression services suitable for site-to-site VPN applications.

Mr. Wagner talked about the Cisco VPN routers: "...they've been working like champs. They stay up and work all the time—if they were to go down, you would have a cessation of traffic, something we don't have time for in a life-critical environment."

Sometimes, MDA doctors aren't on site, but patients still need their expertise. MDA doctors receive calls at home for emergency evaluations and can view diagnostic images along with relevant

historical data on secure, VPN-enabled laptops or PCs. For remote access VPN connections, MDA implemented Cisco VPN 3060 concentrators (Figure 2), enabling secure connections across TCP/IP networks, including the Internet. The Cisco VPN 3060 Concentrator is a remote access VPN platform with client software that incorporates high availability, high performance, and scalability with the most advanced encryption and authentication techniques available today. MDA uses the Cisco VPN 3060 concentrators to provide doctors with remote access to patient information, as well as applications such as e-mail and meeting planning programs.

Figure 2

**Cisco VPN 3000 Series Concentrators**—Cisco VPN 3000 Series Concentrators are remote access VPN platforms with client software that incorporate high availability, high performance, and scalability with the most advanced encryption and authentication techniques available today.



#### Optimum Flexibility: Wireless Access

For the utmost efficiency and flexibility, MDA has also enabled its doctors to use free-standing or cart-based laptops in various areas of the hospital—wirelessly. Cisco wireless solutions are deployed at MDA so that doctors have the ability to review critical, real-time information while in various sections of the hospital. Cisco Aironet<sup>®</sup> access points are deployed in several areas of the facility and Cisco Aironet client adapters are installed on the laptops for the wireless clients to be authenticated and authorized.

On the network side, Cisco Secure Access Control Servers (ACSs) function as back-end databases to hold authentication information about users and user privileges. Cisco Secure ACS controls the authentication, authorization, and accounting (AAA) of users and administrators accessing the network, and thereby allows the network administrator to control who logs on to the MDA network, either through wired or wireless connections, and the privileges of each user.

Cisco wireless access allows doctors at MDA to take full advantage of their revolutionary database application, ClinicStation. Developed at MDA, the award-winning ClinicStation enables doctors and other health-care staff members to leverage several

clinical databases via a single, integrated, secure display. Every month, MDA employees perform more than 300,000 patient queries and review more than 1,000,000 clinical documents. At peak utilization, ClinicStation can handle more than 1100 simultaneous users.

One of the ways all this data, accessed wirelessly, is protected is via Lightweight Extensible Authentication Protocol (LEAP). LEAP is a Cisco proprietary 802.1X secure authentication protocol for wireless LANs that supports strong mutual authentication between clients and a RADIUS server. It provides dynamic per-user, per-session Wired Equivalent Privacy (WEP) key enhancements to mitigate a variety of network attacks.

Mr. Wagner talked about the Cisco LEAP-based approach to securing information: "With LEAP, we make the password dynamic, it changes every three minutes, so even if you do hack it, it doesn't do you any good, in three minutes it's going to change again. It's one-time password technology is basically what it is, and we are making that a standard for all of our wireless applications here."

## A Partner for Health Care Security

Cisco security technologies and products are fast, highly reliable, and protect MDA's information 24 hours a day, seven days a week. Mr. Wagner reflects, "The Cisco performance, from a bandwidth perspective, has been outstanding here." MDA's security philosophy, policy, and architecture share the spirit of the SAFE blueprint from Cisco: a modular, scalable security framework that enables the MDA Cancer Center to safely engage in e-business.

MDA has concluded that Cisco is an excellent partner for health care institutions that need to plan, implement, and deploy security throughout their extended facilities and communities. The Cisco breadth of offerings and the scalability, protection, and management they provide single out Cisco as a proven innovator and leader in the security marketplace. Cisco offers superior security experience and expertise including sales, engineering, and consulting teams of outstanding network and security experts.

For further information on Cisco integrated network security solutions, visit:

[www.cisco.com/go/security](http://www.cisco.com/go/security)



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://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](http://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](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://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 Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
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

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. . Aironet, Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, and PIX are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.  
(0301R) TS/LW4130 01/03