



## Simplified HIPAA compliance using the 3Com Embedded Firewall

December 2001

### Disclaimer:

*This white paper contains Secure Computing Corporation product performance information that is meant as a guide to customers. Performance is greatly influenced by traffic profiles and how the hardware and software are set up and configured. Therefore, the performance data within implies no guarantee by Secure Computing that the customer will realize the same performance levels.*

**SECURE**  
COMPUTING

#### Secure Computing Corporation

##### Corporate Headquarters

4810 Harwood Road  
San Jose, CA 95124

**tel** +1.800.379.4944

**tel** +1.408.979.6100

**fax** +1.408.979.6501

#### International Headquarters

**tel** +44.1753.410900

**fax** +44.1753.410901

[www.securecomputing.com](http://www.securecomputing.com)

# T A B L E O F C O N T E N T S

## Simplified HIPAA compliance using the 3Com Embedded Firewall

Abstract . . . . .	.3
Introduction . . . . .	.3
About HIPAA . . . . .	.4
The challenge . . . . .	.5
The Embedded Firewall concept . . . . .	.6
Introducing the EFW . . . . .	.6
Benefits of the EFW . . . . .	.7
Implementing HIPAA roles and categories with the EFW . . . . .	.7
EFW benefits for HIPAA compliance . . . . .	.9
Endnotes . . . . .	.10

## Abstract

The 3Com Embedded Firewall (EFW), developed in conjunction with Secure Computing Corporation, provides an easy-to-deploy mechanism to enforce privacy rules recently established under the Health Insurance Portability and Accountability Act (HIPAA). The new privacy rules are intended to reduce the risk of an individual's private health information being used in an inappropriate manner or without the individual's permission. In particular, the rules require health care organizations to restrict access to personal health information in accordance with staff or employees' roles and duties within the organization. The EFW helps enforce such restrictions by controlling how desktop computers share data and which servers they can interact with. These centralized restrictions can be tailored to the individual organization's situation, and they can also evolve to respond to changes in privacy regulations and in the organization's operating environment.

## Introduction

Electronic health records play an essential role today in reducing costs and increasing the effectiveness of health care. However, the ease with which organizations can share electronic health care data has raised significant public concerns about personal privacy. Most people want to keep the details of their health affairs private; in a number of cases, people have suffered tangible losses when sensitive health information was released. While most health care professionals strive to protect patients' privacy, the sheer size and complexity of the health care industry makes it impossible to ensure privacy simply by relying on individuals' ethical behavior.

In response, Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which, among other things, provides electronic health care records with a measure of legislative oversight. As part of the Act, Congress has directed the Department of Health and Human Services to establish rules to protect the privacy of patient's health care information when stored in computer files. These rules will have a significant impact on how computing systems handle personal health care information.

A particularly significant HIPAA requirement is that health care organizations restrict access to sensitive personal health care information according to the duties of their employees. For example, a billing clerk needs access to information about patient visits and associated diagnostic codes, but does not need access to the patient's detailed treatment records. A nurse may need access to patients' treatment records, but not to billing records. An appointments clerk needs to produce records describing upcoming patient visits, but doesn't need access to the resulting treatment or billing records. Under the HIPAA privacy rules, each organization must identify the roles it recognizes (nurses, clerks, etc.) and the categories of information it handles (appointments, treatment, billing) and identify which roles need to use which categories.

While many organizations already implement access restrictions along these lines, modern networking technologies tend to weaken those restrictions. Even if a site provides separate servers for different categories of information and separate workstations for people working in different roles, it is very difficult to prevent unintentional data sharing even though such sharing may violate HIPAA rules. In general, organizations can't afford to implement physically separate networks for billing and patient treatment even if they can afford to implement physically separate servers. So there is a very real risk of violating HIPAA rules, and worse, suffering a significant privacy breach, unless additional protection is provided.

The 3Com Embedded Firewall (EFW), developed in conjunction with Secure Computing Corporation, helps address HIPAA privacy compliance in today's unsettled environment. The EFW resides on one of 3Com's low-cost network interface cards (NICs), which may be installed in each computer on the network. The EFW ensures that the computer only communicates with other computers appropriate to its owner's role and the categories of information it normally handles. A site administrator can centrally establish and maintain the user roles and information categories for the site's computers to reflect their assigned operations. Each EFW enforces its access rules regardless of what happens to its host computer: neither a strong virus infesting the host's operating system, nor even a wayward administrator on an individual computer, can interfere with EFW's access restrictions. Moreover, the EFW system maintains logs of which computers access one another, in support of HIPAA audit requirements. The overall EFW system provides clear and tangible evidence that the organization is complying with the letter of the HIPAA privacy rules.

It is important to recognize that no system can unconditionally guarantee the privacy of patient data as it is used in today's health care organizations. The HIPAA rules do not strive for such a goal; instead, they encourage organizations to restrict access to people who must use the information for their professional duties as much as is practical. Conventional operating systems, like Microsoft Windows and variants of Unix, provide access control mechanisms that can enforce privacy protections. Unfortunately, these mechanisms have the disadvantage of being difficult to maintain and, when used at all, it is difficult to determine if the restrictions have been set up correctly. The EFW provides simple, scalable, and easy to verify protections that clearly demonstrate that the organization enforcing HIPAA-mandated privacy restrictions. Moreover, the EFW's protections can be tailored as the organization's systems evolve to provide either tighter network-level controls or to loosen the network-level controls as other easy-to-verify mechanisms are put in place.

The rest of this paper examines the EFW's role in implementing HIPAA privacy rules in greater detail. First, we will look at the HIPAA privacy rules. Next we will look at the challenges these rules pose to typical health care organizations. Then we will look at the technical features of the EFW that help a health care organization comply with HIPAA privacy rules. Finally we will look at a specific example of how EFW would benefit a medical clinic with several physicians and the corresponding support staff.

## About HIPAA

HIPAA was passed by Congress to improve the efficiency and effectiveness of the health care system, as well as reduce the incidence of fraud. These efficiency improvements will require increasing automation of patient records and electronic health care information transfers. The push for standardization of diagnostic codes and the increasing computerization of patient information, combined with increasing transfers of that information between the relevant parties, poses many new security and privacy risks that never existed before. In recognition of this increased risk, the drafters of this legislation included provisions for information privacy and the regulation of information systems security. There are several procedural and technical solutions explicitly stated in the rules that work towards those goals.

As part of its Administrative Simplification section, HIPAA included many requirements for establishing rules for managing and protecting "individually identifiable health information." Such information refers to any electronic health information (including demographic, provisional, financial, or conditional) that can reasonably identify—or be identified with—a specific individual (as defined in section 1171(6) of the Social Security Act).

With the issuance of final HIPAA rules by HCFA (Health Care Financing Administration), maintaining privacy of medical records is a legal requirement—all large health care organizations that maintain or transmit electronic

health information must comply by April 2003 (small organizations have an additional year). However, ensuring that patient information is kept private and secure presents a technological challenge for most organizations. Key privacy requirements include:

- Identify different categories of medical information (e.g., distinguish between billing records and treatment records)
- Establish access restrictions that restrict staff members of health care organizations to the categories of information that are appropriate to their professional role and associated duties (i.e. billing clerk, nurse, appointments clerk, laboratory technician, physician, etc.)
- Keep records of who tries to access what categories of information

Note that the roles and categories identified above are purely examples, and don't reflect explicit requirements. Rather, the rules require each health care organization to establish individual policies to identify its own roles and categories, to define the corresponding access restrictions, and to outline how the restrictions will be enforced.

Many organizations already implement access restrictions along these lines. Billing systems are often relatively mature computing systems that are rarely used by treatment professionals. Treatment-oriented data systems, like the emerging systems for electronic patient records, are usually implemented on different computers than the billing systems, providing a *de facto* separation. Fundamentally, the HIPAA rules encourage organizations to preserve and extend such restrictions.

## The challenge

However, the HIPAA privacy rules pose a challenge to some organizations already, and will pose challenges to others as their computing systems evolve. As new systems replace old ones, there may be financial and efficiency incentives to weaken existing separation between billing and treatment systems. In fact, some organizations have already crossed the line in which all such data is centralized on a single mainframe or set of shared servers.

Of course, it is possible to enforce separate categories on a shared server, particularly if such restrictions are built into a custom medical records management application. Such restrictions can be very difficult to implement and maintain, however, if the categories and roles must be implemented in terms of Windows or Unix access control rules. It is very easy for such rules to go stale as employees change jobs, increasing the risk of a privacy breach subject to HIPAA sanctions. Moreover, many people already use spreadsheets and word processors to work out special problems, do research, or correspond with patients. This gives individual desktop computers the potential to violate HIPAA privacy rules if some people can access computers containing information in inappropriate categories.

Most members of the health care community strive to protect patient privacy, regardless of whether records are kept on paper or in computers. While on paper, the privacy of patients' records is relatively easy to monitor, simply because a snooper usually needs to be in physical possession of the paper record. Snooping is far easier to do and harder to monitor in electronic patient records. Moreover, it is very difficult to assess whether privacy controls have been set up correctly on commercial systems when using their built-in access control mechanisms. Even though the site's administrators may have set up and maintained the controls properly, it's extremely difficult to verify their correctness. Sites need a mechanism that provides higher confidence that fundamental restrictions are in place.

## The Embedded Firewall concept

Many Internet sites have installed one or more firewall systems to filter traffic between the site and its Internet service provider. These firewalls usually examine the network-oriented properties of this traffic, like host addresses, protocol identifiers, and the port numbers that often indicate which higher-level application protocols are being used. Sites typically configure the firewalls to detect and block unexpected traffic or attempts to use undesirable protocols. Some sites also use such mechanisms to filter out traffic from specific, predefined Internet host addresses. A strong inducement for using firewalls is to block protocols whose server software isn't entirely reliable and may provide unintended back doors into the host computer. By installing the firewall at the perimeter, the site blocks attempts by outsiders to attack weak network software that might reside on the site's computers.

A well-known shortcoming of perimeter firewalls is that they only protect the site from external attack. Attacks that are blocked when originated from the outside may succeed if launched from inside the site's security perimeter. The problem of insider attacks on computing resources is attracting more concern, as such attacks have become more visible in recent years.<sup>1</sup> Subverted software, like viruses and worms, can also cause damage from the inside once they manage to get past the perimeter firewall defenses. Software-based "distributed" and "personal" firewalls can address these problems by placing the firewall filtering on the individual hosts. The host-based filtering will block attacks regardless of whether they originate inside or outside of the site. Unlike personal firewalls, a distributed firewall system provides a mechanism to coordinate the hosts' filtering policies, usually to comply with security concerns of the site's proprietor.<sup>2</sup>

The work with host-based firewalls noted above focused on solutions that were installed into the host's operating system. This has the shortcoming that an attacker can disable the firewall if an attack on the host succeeds; this very problem has already affected host-based personal firewalls.<sup>3</sup> Even if the firewall uses the operating system's access restrictions to protect itself from a subverted user, there is still a risk that the subverted user will be able to acquire enough operating system privileges to overcome those access restrictions.

## Introducing the EFW

DARPA-sponsored research has yielded an alternative approach that incorporates the firewall function into a "policy-enforcing NIC" producing today's EFW.<sup>4,5</sup> This approach enforces the firewall filtering policy even if the entire host operating system is subverted, since the NIC software can protect itself from host-based attacks on its behavior. A central host serves as a "policy server" for a particular set of NICs; the policy server is responsible for establishing the firewall filtering rules used by the NICs under its control.

The EFW is a premium feature of the 3Com 3CR990 "Intelligent NIC." The 3CR990 contains a special chip set and associated firmware to provide cryptographic acceleration for data links using the IP Security Protocol (IPSEC). In particular, the board contains specialized integrated circuits to provide Triple DES encryption and SHA-1 hashing. The NIC hardware costs less than US\$100 each and is compatible with standard Microsoft personal computer software and with Linux.

## Benefits of the EFW

The EFW provides several benefits that can't be gained through perimeter firewall mechanisms, conventional host-based access control mechanisms, or host-based software firewalls:

- Network access control is applied at the host computer itself and can't be bypassed even if an insider launches an attack from within the site's local network.
- The EFW's enforcement mechanism is fully self-contained. The host containing the EFW cannot modify or disable the network access rules being enforced.
- Unlike personal firewalls, or built-in filtering by Microsoft Windows, viruses can't disable the EFW's defenses.
- The management of EFWs is centralized, which provides a simple way of establishing and enforcing a site-wide access control policy. A site may have one or more policy servers if needed to handle subsets of the site's EFW-protected computers.
- EFWs can protect both the site's servers and individual desktop computers. The central policy server coordinates access control rules of the computers.
- Because the EFW is an independent mechanism, it is relatively simple to verify that it is enforcing the rules and separations it claims to enforce. The EFW provides much better assurance of secure operation than is available from Unix- or Microsoft Windows-based access control rules.
- The EFW automatically maintains a centralized log of successful and unsuccessful access attempts involving EFW-protected computers.

## Implementing HIPAA roles and categories with the EFW

The EFW allows a health care organization to keep computers separate according to the roles of their users and the categories of information they contain. The EFW implements the type of privacy protection required by HIPAA and provides a way of demonstrating that the organization is in fact implementing HIPAA's safeguards.

The first step is to install 3Com's EFW-capable NICs in the site's servers and desktop computers. This involves retrofitting existing computers, but new computers can be ordered from major manufacturers with the appropriate NIC already installed. In either case, this is a more practical solution than trying to physically rewire the organization's networks in order to enforce the necessary separation.

While the NICs are being installed, the site's administrator should define "groups" of NICs on the EFW policy server to correspond to the roles and categories being enforced. There should be a separate group for each role or set of roles that may be assigned to a single individual. If some individuals share a desktop computer, then there must be a group defined that encompasses all of the roles of all individuals who may legitimately share that computer. There should also be a separate group defined that encompasses every set of information categories handled by individual server computers. To see what this means for a real health care organization, consider the following example, based on implementing HIPAA protections in a group practice clinic.

A typical clinic belonging to a group practice will have a number of physicians, nurses, clerks, and other administrative personnel. The clinic may also have a lab and an x-ray facility. There will probably be desktop computers or computer terminals in every physician's office, at nurses' desks, and for clerks and other administrative personnel. The clinic naturally handles a variety of health-related and non health-related information. Health related information includes treatment records (including physicians' and nurses' notes on patient visits, lab

results, x-rays, etc.), billing records, appointment records, and related data. Non health-related information includes those items appearing in a typical business, including supply management, payroll, building management, and similar records.

For the EFW to enforce roles and categories based on these distinctions, the site must establish separate groups to reflect those distinctions. Here is an example of how to define those groups:

**Appointments Group:** this includes computers used by clerks to enter and update the clinic's appointments calendar, and receptionists who check in patients arriving for appointments. The clerks have full access to the calendar and handle patients' requests to schedule visits for various purposes. This group does not have access to information about the results of those visits, nor to billing information related to those visits. The receptionists may have access to health insurance information in order to ensure that up-to-date insurance information is collected and that copayments are made as necessary.

**Treatment Group:** this includes computers used by nurses to manage the inflow of patients for appointments and, if electronic patient records are implemented, to capture clinical data collected about the patient (weight, height, temperature, basic symptoms, etc.). The medical records, clinical lab, and x-ray facility are also in this group, as are desktop computers used by physicians. Personnel responsible for diagnosing and treating patients will generate diagnostic codes within this group, and those codes are provided to the billing group. Otherwise, people within the treatment group share little information with the billing group, and can not otherwise access patients' billing information.

**Billing Group:** this includes computers that generate billing information related to patient visits and interact with health insurance providers to collect payments. This group also generates bills to send to patients for costs that are not covered by insurance and to process the associated accounts receivable. Some organizations may include non-medical receivables and payables in this group as well.

**Administrative Group:** this includes computers that are used for non-medical administrative activities. This separate group would probably only exist in larger clinics that have one or more separate departments dedicated to such activities.

Once these groups are defined within the policy server, the administrator will identify which servers and workstations belong to which group. The assignment depends on who uses the workstation in question and what categories of information reside on the server in question. The workstations used by nurses and physicians, as well as servers containing treatment records, are all assigned to the Treatment Group. Desktop computers used by appointments clerks and receptionists belong to the Appointments Group. Equipment and workstations used to handle insurance and billing belong to the Billing Group. Certain servers are shared among groups: the nurses can examine the appointment calendars on the Appointments Group's server, and members of the Treatment Group are given access permission to provide the diagnostic codes associated with a patient's visit to the Billing Group's server.

As the EFW NICs are installed into computers and brought on-line, the policy server installs the appropriate access control rules in each NIC. From then on, the EFW enforces access restrictions on that computer.

Clearly, no clinic will be able to implement a perfect separation between the different roles and categories, that is, one that perfectly minimizes privacy risks. However, it is essential that the clinic provide a best effort to do so, and provide a migration path that allows it to improve its protections over time. The EFW provides such a facility. Even if every group in the clinic shares a single server today, the EFW can still enforce appropriate restrictions on desktop computers. As the clinic's computing environment evolves, the EFW provides the necessary mechanism to further tighten the access restrictions to better enforce HIPAA's intended restrictions.

## EFW benefits for HIPAA compliance

Here is a summary of the four major benefits the EFW brings to the problem of complying with HIPAA privacy rules.

### 1. Tangible evidence of compliance

The EFW provides explicit, demonstrable mechanisms that enforce HIPAA-mandated privacy restrictions, and it provides a complete, centralized logging process to track associated network accesses. Third party auditors can verify that the site is enforcing HIPAA rules by examining the access control rules enforced by the EFW's policy server.

### 2. Explicit separation of roles and categories

The EFW explicitly enforces separation between computers on the network that serve different roles and/or handle different categories of sensitive health care information. The EFW deployment provides clear evidence that the health care organization is enforcing separation according to user roles and information categories in accordance with HIPAA rules.

### 3. Centralized logging of network accesses

Each EFW generates reports on its network traffic, and those reports are regularly transmitted to the central policy server. This provides a record of the types of network accesses that occur on the site's network. This type of logging satisfies important requirements established in the HIPAA rules for privacy record keeping.

### 4. Adaptable to evolving requirements

Many observers believe that HIPAA signals the beginning of a long-term change in how the health care industry handles confidential patient data. It's too soon to tell just how much protection will be legally required this year or in the future. Recently, courts have started holding organizations accountable for meeting basic standards of due care in regards to information security. Courts widely recognize the notion to a "right of privacy," and it is hard to predict the level of expectation the legal community finally settles on with respect to appropriate privacy measures.

The EFW helps organizations address this uncertainty by allowing them to adapt to changing requirements. Computers are most efficient when they share information with little or no control, but such sharing clearly contradicts the notion of privacy protection and intent of HIPAA. Nonetheless, practical operations today will undoubtedly promote increased data sharing. EFW lets each site tailor its information security and privacy protection measures implement as much sharing as is practical, and it also provides clear evidence that the site preventing unnecessary information sharing. Since the EFW is centrally managed, it is easy to fine-tune its access rules in response to future changes in legal requirements and community expectations.

## Endnotes

- <sup>1</sup> Computer Security Institute and Federal Bureau of Investigation, “Computer Crime and Security Survey,” Computer Security Institute, 2001.
- <sup>2</sup> Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith, “Implementing a Distributed Firewall,” *7th ACM Conference on Computer and Communications Security*, Athens, Greece, November 2000.
- <sup>3</sup> Aoife White, “New Trojan Disables Firewall Defenses,” *Network News*, May 2001.
- <sup>4</sup> Tom Markham and Charles Payne, “Security at the Network Edge: A Distributed Firewall Architecture,” *DARPA Information Survivability Conference and Exposition II*, Anaheim, CA, June 2001.
- <sup>5</sup> Charles Payne and Richard Smith, “The Releasable Data Products Framework,” *DARPA Information Survivability Conference and Exposition II*, Anaheim, CA, June 2001.