

Protecting From Within

*A Look at Intranet Security Policy
and Management*



Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
1 (800) 786.7638
+1.512.434.1511

Copyright 1999 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303 -1100 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, ONC+, Solaris, Trusted Solaris, SunScreen, SunScreen EFS, and Sun Security Manager are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. Information subject to change without notice.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 1999 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, ONC+, Solaris, Trusted Solaris, SunScreen, SunScreen EFS, et Sun Security Manager sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please
Recycle



Adobe PostScript

Contents

Introduction	1
The Risks — Why You Need Intranet Security	2
Technical Weaknesses	5
Human Weak Points	7
Security Policy Concepts	9
Overview	9
Steps to an Intranet Security Policy	9
Key Security Concepts	11
Securing Your Network for Business	12
Consulting	12
Software	13
Hardware	14
Training	14
Solution Providers	14
Securing Your Network For Business	14
Available Resources	15

Introduction

This document is for business executives and others who want to know more about protecting their internal networks from unauthorized use. Today, most businesses are connected to the Internet, and have taken appropriate actions to protect themselves from attack by hackers outside the network, using firewall products and technology. Yet this addresses only a portion of the vast majority of problems that affect your information technology (IT) infrastructure.

According to government and private sector sources, your IT is far more likely to be attacked or compromised by sources inside your firewall. Your internal IT can be at risk, even if you have all the right technology, if your company's security policy and procedures are poorly implemented or outdated.

This high-level overview will provide you with:

- A basic understanding of the need to protect your internal IT systems – your intranet – from unauthorized usage
- Some of the typical weaknesses in many IT systems
- Steps you can take to protect yourself
- An overview of the technologies and procedures that can be used to strengthen your intranet security

The Risks — Why You Need Intranet Security

Today, intranets are integral to more and more businesses. Economists are now hailing IT as a component in the unprecedented rise in corporate productivity. Within your own business, IT may have enabled increased productivity by enabling field employees to gain access to e-mail and other internal resources, customers to use timely pricing information, and partners to use accurate inventory and order information. Businesses are using Web technologies to increase revenues, expand market reach, and lower costs.

But these benefits can be offset by new risks. Consider the following scenarios:

- After much evaluation and careful effort, your company has selected and installed a firewall, routing all traffic to and from the Internet through this gateway. Once completed, the network administrator assigned to the project moves on to other duties, only occasionally returning to the console to modify access permissions. Management feels secure that they have protected their IT infrastructure.
- In an attempt to meet departmental goals, a product manager sets up a Web site for his or her product line. The Web server sits under a desk, and contains links to manufacturing, engineering, and sales databases. Furthermore, the product manager has installed a dial-up modem on this Web server to facilitate remote updates. MIS has no knowledge of this Web server, how it connects to the intranet, or the modem capabilities.
- In the training room, the desktops and network connect to other areas of the company. The engineering technician prefers the connection because he or she can read e-mail while installing and configuring systems, and can access patches directly from the engineering servers. The training facility is also used by student from both inside and outside the company.

Each of these scenarios presents a real ongoing risk to the hypothetical companies' IT assets and resources. In the first example, installing a strong firewall at the company Internet gateway is a good first step. But all security components, including firewalls, require constant updating and monitoring to meet new threats and track effectiveness.

The second example, while showing strong personal initiative, has opened a gaping hole in the company's network, providing relatively easy access to users both inside and outside the company to internal servers and the information stored on them.

And in the third example, while it may be much easier for the technician to have unimpeded access to company resources, the training room network provides unauthorized access to both internal and external users.

While the examples are all hypothetical, how real is the threat they pose to your business's IT? Very real. According to the Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) report *Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey*:

- 78% of the companies surveyed reported insider abuse
- 65% reported laptop theft
- 44% reported unauthorized access
- 18% reported theft of proprietary information

For those companies that could put a dollar figure on their losses, the amount totaled over \$136 million. The largest portion of this amount was losses that occurred through unauthorized access — \$50,565,000. Overall, according to the CSI/FBI report, financial losses increased 36% from the previous year, while the number of companies reporting security breaches increased to 64% of those surveyed, up from 48% the year before.

In spite of increasing crime rates for computer security, no one is suggesting that companies seal off their networks and lock up their laptops. But business organizations are wise to undertake a risk-benefit analysis, as well as create and maintain a security policy.

The first step in creating a risk-benefit analysis is appraising the value of your IT infrastructure, both in terms of real and opportunity costs.

- **Real Costs:** What is the cost of the actual hardware and software in your organization? Include the price of servers, LAN equipment, desktops, laptops, e-mail, intranet, and Web servers. Also include the value of any intellectual property contained on these servers.

- **Opportunity Costs:** The costs that would be incurred – or the revenues lost – if your employees, partners, or customers were unable to access some or all of your IT infrastructure they use on a regular basis. For example, if your employees were unable to use e-mail, or your order administration groups were unable to access inventory, accounts payable, or accounts receivable applications or data. What would be the cost if a laptop containing strategic plans was stolen? Or if a competitor was able to see and review engineering, sales, or salary plans?

After estimating the costs, determine what your company is spending to protect itself from security issues. If your company is of a reasonable size, this *should* be a simple matter of asking the staff member in charge of IT security. Unfortunately, most companies do not centralize IT security under a single department or person, so this may not be so easy. A side-effect of security management distributed throughout the company is the lack of a focused, cohesive strategy, with *ad hoc* implementation of different security technologies and procedures. In any case, estimating the amount expended by the company will in all likelihood show that a relatively small amount of resources are being used to protect significant corporate assets, and that the cost associated with being unable to use these resources and assets is even larger.

Often a derivative of this exercise is the realization that there is no plan in place for either centralized management or disaster recovery. Few businesses have thought out *in advance* what steps they will take to overcome a security breach.

A security policy is needed to address these issues. A security policy outlines the goals, strategy, and tactics that a company will take to protect its IT assets, as well as its business operations, from unauthorized use or willful attack. More information on what to consider as you develop a security policy for your company, as well what to do once it has been developed, is contained in the next section of this paper.

Technical Weaknesses

In deploying your Intranet, technology can provide many weak points. There are the somewhat obvious technology weak points, such as improperly configured firewall gateways or servers with well-known (or non-existent) root passwords. But there may be other technology-based weaknesses in your intranet as well.

- **Multiple Passwords:** As organizations deploy business-critical applications and remote access servers, and divide workgroups by LAN servers, users are expected to remember and be responsible with more and more passwords. It's not unusual for some employees to have literally dozens of passwords for access to different IT resources. The effect of too many passwords is weakened security, because users start writing them down, and because LAN administrators have administer multiple password management systems for each user.

A more secure approach is to use a single sign-on system, which provides a centralized access control list. Single sign-on systems keep a list of who is authorized to access different areas of the network, and a mechanism for providing the expected password. Users need only remember their single, unique password to sign onto the system.

Most single sign-on systems use a directory to store the names, passwords, and access controls for each user and system resource. This provides a single point of entry for administration, further tightening security.

- **Remote Access:** Perhaps the biggest single weak point in intranet security today occurs in remote access implementations – pools of dial-in modems ready to provide access to corporate network resources and information.
 - Freely available “war-dialers” – programs that will dial a programmed list of numbers and try to gain access to information – make modem pools a weak link in a security architecture. Even without correct names and passwords, many remote access servers reveal hostnames or LAN router prompts.
 - Many remote access systems transmit users names and password prompts “in the clear,” meaning that anyone listening – snooping – to the activity on a remote access port can see and record user information along with the data. Programs to do this are also freely available.
 - Many times when users are logged into the remote access system, they have access to any system resource. The danger here is that once a hacker has broken through the remote access system, they also have free access to any system resource.

There are a number of ways to secure a remote access system, including using encryption that protects traffic between user machines and remote access servers, and using enhanced password mechanisms such as token cards and RADIUS servers.

- **Viruses:** It is estimated that over 40,000 viruses exist today. Documents, not programs, typically spread viruses. Many viruses today can overwhelm e-mail servers or disk storage, while others will delete data on disk drives.

Products and technologies exist today that prevent the distribution of viruses by scanning all incoming traffic for virus signatures as well as examining stored documents.

- **Intrusion:** Certain key files should only be accessed by specific individuals. For example, password or system configuration files should only be accessed by root administrators.

Intrusion detection utilities can be installed to alert MIS managers when there are attempts to access key files, or when there are multiple failed attempts to log into any system on the network, including the remote access server.

- **Lack of Compartmentalization:** Many organizations allow access from any user to any resource on the intranet. Dividing your intranet into segments – such as human resources, engineering, manufacturing, sales, and others – protects assets and information from unauthorized users. This is readily accomplished by using firewall technology to control traffic and access between workgroups and departments.

For example, compartmentalization, which provides extra measures of security between external servers such as Web and commerce servers and the internal servers and databases, is a good idea. A secure operating environment and strict networking and access controls would be appropriate for any server that is exposed to public use and has access to internal databases.

- **Unsecured Data:** Sensitive data – including salary information, strategic plans, and intellectual property – requires extra protection. Yet on many intranets, it is accessible by anyone on the network. Advanced operating environments provide multiple levels of file protection and logging utilities to track users who access, or attempt to access, the data.

Human Weak Points

It is important not to underestimate the human factor while working to improve the security of your intranet:

- **Lack of Planning or Procedure:** In the absence of any formal policy, many departments or workgroups will implement their own security measures, or modify the intranet to address their business needs. Without a formal plan, these measures can be counterproductive, inefficient, or unknowingly create security breaches.
- **Lack of Follow-Up:** Even the best security measures require maintenance and follow up, yet often the staff members or professional services organization that installed the security technology has moved on to other tasks. New hacker tools are being created, and new “holes” are being discovered on a regular basis. Reviewing log files for possible breaches and installing patches to applications and operating environments are but two of the ongoing tasks required to maintain a secure environment.
- **Willingness to Help:** Surveys show that employees across the company, from administrative assistants to executives, will often hand out passwords to co-workers who request it, or to anyone on the telephone asking for one. Products such as token cards can prevent this, but training programs throughout the company are needed to teach and reinforce the value of good security.
- **Unwillingness to Follow Procedure:** Some users will resist following newly established procedures. Usually, they don't fully comprehend the ramifications of not following the procedures, or cite business emergencies or how inefficient the security is to their job. Training can help overcome some of these objections, and a well-designed security mechanism with the latest technologies should add little, if any, burden once fully implemented.
- **Ego:** Some employees or companies may claim they don't need assistance in creating and implementing an intranet security policy. In extremely rare exceptions, this may prove to be true. However, in practice the only people with comprehensive and current knowledge of how to protect IT systems are the people whose full-time job it is.
- **Zeal:** Some security policies and implementations create too much security, which can be expensive to install and reduce productivity. Creating burdensome security procedures may cause some users to try and subvert the established policies and procedures because they are too cumbersome.

There are many things to be considered in reviewing the IT infrastructure of a business intranet. A competent assessment is beyond the capabilities of nearly every company, and it is best to rely on the professional services of organizations that routinely provide such services.

Executive management has a strong role in corporate security: they must provide budget and ongoing support. Not only should management initiate a dedicated security team, but they should hold periodic reviews and require all employees to attend ongoing training. User roles and responsibilities should be clearly defined such that everyone understands — and supports — strong security for organizational assets.

Security Policy Concepts

Overview

Creating a comprehensive security policy for your intranet is a serious undertaking, the details of which are beyond the scope of this document. The policy for each organization will be very different from that of another organization, and the policy may outline different practices for different departments within each business. Still, there are many concepts that can be outlined that will help you in preparing and managing the task of creating a security policy.

The goal in developing a security policy is to define the organization's expectation for proper IT use, and to define procedure to prevent and respond to security incidents. An IT security policy must support and complement the overall business goals.

Steps to an Intranet Security Policy

- **Identify Assets:** Start by creating a complete list. Plan to update the lists on a regular basis.
 - **Hardware** – Desktops; laptops; PDAs; servers; network routers; remote access servers; network printers; communication lines; and other relevant devices.
 - **Software** – Business-critical applications and data; desktop applications; source code; strategic plans; customer and vendor information; operating systems; utilities, communications, and diagnostic programs; logs; archives.
 - **People** – Users; administrators; architects; security “org chart”.
 - **Documentation** – Operating manuals for hardware and software; administrative procedures.

- **Evaluate and Rank Assets:** Determine and prioritize the most critical of components, including both hardware and software.
- **Identify Risks and Vulnerabilities:** A good security policy will highlight where the organization is most vulnerable, and state the probability for each of the identified risks.
- **Defining a Policy of Acceptable Use:** Each organization embodies a different work ethic and culture. What is acceptable in one business may not be in another. For example, are certain Web sites off-limits? Can files be downloaded from the Internet? Can e-mail attachments be accepted? Is it permissible to read anyone else's e-mail? Can systems other than those owned by the company be connected to the intranet?

These are questions that each company will need to address, and to ensure compliance, communicate to everyone who works within the company.

- **Identify the Necessary Safeguards:** Apply appropriate security measures in priority order to each identified area of risk. For example, it may be recommended that servers with essential data on them be placed in locked rooms (physical security), and administrative access granted only from a console physically attached to the server. Remote users, including partners and suppliers, may need to use encryption when communicating with your company. These recommendations will vary by company and requirements.

There are two safeguards that may not be obvious, but which are very important to the overall security of a company's intranet:

- **Audit/Logging** – Alerts and alarms can help administrators keep tabs on suspicious actions around the intranet. Hackers work hard to outwit conventional security measures. Logging actions, such as remote access logins and administrative actions to key configuration files, can help identify and trace unauthorized users. Log files and reports need to be audited on a daily basis. While it's very unlikely that an administrator would catch a violator in their first act, by reviewing log files you may be able to set up procedures which identify perpetrators at a later date.
- **Incident Response** – Organizations may choose from a variety of responses upon the realization of a security violation. Planning the responses well in advance, without the pressure of an actual event, is good practice. When an incident is uncovered, there should be a clearly defined series of actions based on the violation. Roles and responsibilities should also be clearly defined.
- **Create Action Plan:** A detailed plan for a rational, phased approach to implementing the security policy is key. Progress against this plan should be reviewed by executive management on periodic basis.

- **Communication of Policy to All Users:** At the foundation of any security effort are the people who will use them each and every day, including employees, partners, and suppliers. In addition, an educational campaign should be used to help users understand the policies as well as underscore the importance of security within the organization. Note that if partners are connecting into your intranet, make sure their security measures are up to your standards.

Key Security Concepts

A network security solution should focus on five primary areas and form a solid framework to implement an enterprise network security policy.

Access Control: Information is controlled and access is granted by a predetermined security policy. This policy can be as simple as a login name and password, and as comprehensive as a directory service which defines user roles and access permissions.

Privacy: Other people on the network cannot see the contents of a message being sent. Privacy is ensured through encryption. Privacy among many users and organization is enabled by a public-key infrastructure, which manages all the necessary components, including digital certificates, key management, and encryption algorithms.

Authentication/Authorization: Granting rights for users to perform actions that would otherwise be disallowed and making sure that access or communication is with the intended user. This can be as simple as an operating system name and password, or as secure as a token-card, which supplies an ever-changing password.

Integrity: The assurance that data, system, or application files have not been tampered with.

Management: Consistent framework for ongoing management of the security products and procedures.

Securing Your Network for Business

Sun™ technology innovations have been setting standards for over a decade, and network security has been among the most important areas of development. Security has been an integral part of each and every one of our software and hardware solutions from the very beginning.

With over a decade of experience in open, network computing, Sun understands that your security needs change over time, and an incomplete or outdated security solution is a risk to your business. Through proven methodologies and practical experience, together with our solutions providers, we have a comprehensive range of solutions, including hardware and software products, assessment, training, policy development, solution design, implementation and configuration, vulnerability testing, and documentation. We can deliver a complete solution or supplement your staff to deliver the missing pieces.

Consulting

Sun's consultants have the capabilities and field-proven methodologies to assess your current security environment, design an optimal architecture, and help you implement a security solution customized for your business needs. These capabilities include security management assessment, architecture, and implementation.

Sun Professional Services also offers packaged solutions for your specific security needs, such as Firewall Services and Sun Security Manager™ Quickstart Service, which provide a more standardized approach to security issues. These packages use proven methodologies and established training modules to deliver excellent results time after time.

Software

Sun develops and markets leading software security solutions for business intranets:

SunScreen™ Secure Net is a comprehensive solution that includes SunScreen EFS™ 3.0 and SunScreen™ SKIP software, and enables users to help establish a secure business network.

- *SunScreen EFS* is an award-winning, high-performance firewall gateway that integrates powerful encryption technologies to provide the most cost-effective, scalable solution for securing every node within an enterprise. It includes *SunScreen SPF-200* to deliver a premier perimeter defense solution that features a stealth architecture, network address translation (NAT) capabilities, and remote, secure management.
- *SunScreen SKIP* provides encryption and key management capabilities to the desktop and remote users, enabling secure, authenticated communications between PCs, workstations, and servers.

SunScreen Secure Net 3.0 includes Sun Screen EFS for the Solaris™ Operating Environment on SPARC™ and Intel platforms and SunScreen SKIP clients for Windows 95, Windows NT, and the Solaris Operating Environment on SPARC and Intel platforms.

The Solaris Operating Environment is an industry-leading environment with a number of built-in security features that make it a solid, scalable enterprise foundation, including SVID-compliant access control enhancement, ASET automated audit tool, ARM account protection, and ONC+™ Federated Security authentication technologies. It also incorporates the Basic Security Model (BSM), which brings Solaris software to compliance with C2-level specifications.

Trusted Solaris™ Software is the operating system of choice for high-level security requirements, providing enhanced security to meet and exceed B1-level specifications. Configurable to fit a wide variety of customer security policies, it implements strong, role-based control of both user and system administrator actions. Data and system resources are fully protected by a multilevel file system, preventing unauthorized access by either internal or external threats.

Java™ Technology provides a simplified development and deployment platform for distributed, highly flexible network computing. The Java security model is designed as a “sandbox” of cooperating systems components, from security managers that execute as part of the application to security measures designed into the Java virtual machine and the Java language itself. The sandbox ensures that an untrusted application cannot gain access to system resources.

Hardware

Netra™ products comprise an award-winning family of simple, powerful Internet servers that have security built-in, with firewall protection and dynamic packet-level filtering to protect your network, your data, and your server.

Training

Sun Educational Services provides complete training solutions to help ensure that customers have the necessary skills to implement and manage their network security strategy. Sun's education consultants can work with customers to perform a security skills assessment to identify any skill gaps within the organization.

Solution Providers

Sun has established relationships with a number of leading software providers who have built application-level security into their products that complement the infrastructure security already. These solution providers can assess your company's needs and provide customized solutions and services that are tailored to your businesses' unique requirements.

Securing Your Network For Business

Today, companies are relying on network computing to provide very real business advantages — increasing efficiencies, lowering business costs, and providing instantaneous global access.

With the continuous adoption of network computing, access to corporate data, correspondence, and other sensitive information is now live on public networks like the Internet — which means it's vulnerable to unwanted intrusions, data altering, and interception.

Securing this information is essential, but too much security can be as counterproductive as too little. And understanding your security risks and how to minimize and monitor them is as important as installing the latest technologies.

Sun's experience in network computing gives us a clear understanding of the many complex issues involved with network security. We know that there are no simple, universal solutions — every company's network security issues are unique. That's why, together with our solutions providers, we've put together a comprehensive network security solution that provides the flexibility and extensibility required to secure your network for business.

Available Resources

- Sun Microsystems: www.sun.com/security/
- Sun Professional Services: www.sun.com/service/sunps/
- The SANS Institute: www.sans.org
- Computer Security Institute: www.gocsi.com
- Computer Operations, Audit, and Security Technology (COAST):
www.cs.purdue.edu/coast/coast.html



Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303

1 (800) 786.7638
+1.512.434.1511

<http://www.sun.com/software/>