Security In The Internet Economy

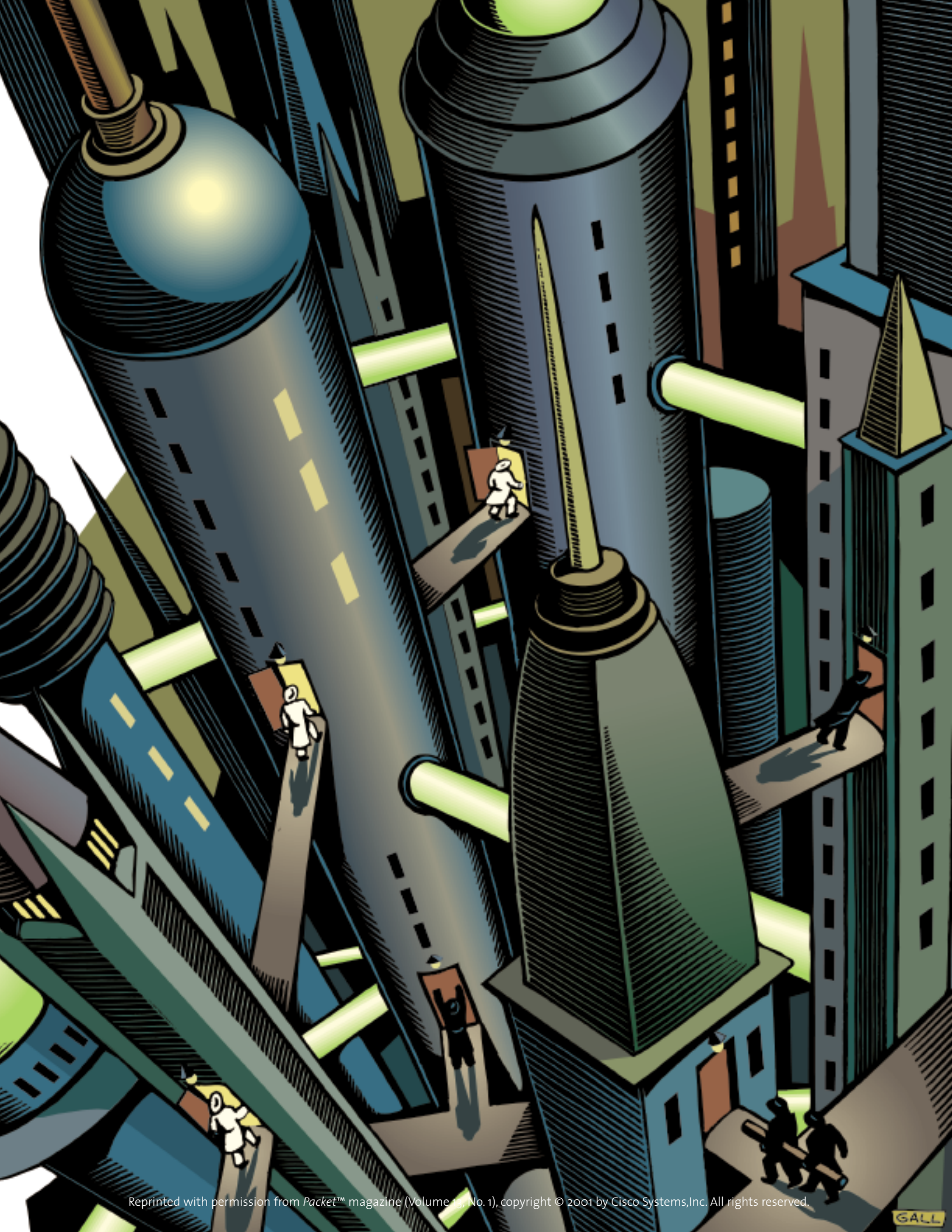
Security and Openness. The Success of your business may hang in the balance.

"Advocacy and belief go hand in hand. For there can be no true freedom of mind if thoughts are secure only when they are pent up." —US Justice William O. Douglas

Since the dawn of civilization, security had a singular purpose: keep the bad guys out. For most of history, that meant building strong walls to stop the bad guys, with small, well-guarded doors to provide secure access for the good guys. This strategy worked well for the fortress-like world of mainframe computers, but with the advent of personal computers, LANs and the wide-open world of the Internet, more and larger entrances were required.

By **JOHN PESCATORE**

ILLUSTRATIONS BY CHRIS GALL



SECURITY TRENDS LONG TERM

Security in 2000	Security by 2010
Lumpy	Distributed
Visible and intrusive	Transparent and enabling
In the factory	In the product
An overhead cost	A cost of sales
Product oriented	Service oriented

EVOLUTION OF SECURITY: Over the next ten years, security will become less "lumpy," moving from discrete elements to being distributed and transparent throughout the network. Over time, the systems used in the factory to protect our products will be embedded in the very products shipped to customers. Security will become more of a feature and less of a cost.

The firewall became the electronic analogy of the moat and drawbridge, striking a balance between open access and increased security. As e-business continues to grow, finding this balance will be critical as it becomes harder and harder to tell the good guys from the bad guys. The rise of mobile commerce and wireless networks will be like the cannon to castle walls, exploding the old model, demanding that security solutions be seamlessly integrated, more transparent, and more flexible.

In the first wave of computer use, mainframes were kept in well-secured computer rooms and users could connect only via dumb terminals from approved locations over static, point-to-point connections. From a security perspective, life was good. If the rise of LANs and the personal computer rocked the security boat, the Internet threatened to sink it completely. The introduction of the firewall in 1995 allowed successful businesses to balance security with simple outbound access to the Internet (mostly for e-mail and Web surfing) for positive impact to the business bottom line.

This balance was short lived, as the use of extranets—defined by Gartner as the use of Internet technologies to connect internal business processes to external parties—began to grow. Businesses were soon realizing tremendous cost savings by connecting supply chain management and enterprise resource planning systems to business partners, sales-force automation systems to mobile employees, and by providing electronic commerce connections to business customers and consumers. The firewall began to be augmented by intrusion detection, authentication, authorization, and vulnerability assessment systems. Today, successful companies have once again struck a balance by keeping the bad guys out with increasingly complex ways of letting the good guys in.

History Repeats Itself

As in any fast-growing, vibrant industry, static equilibrium is a rare commodity in the Internet economy. A number of trends threaten to rock the balance between security and open access yet again:

- **Privacy concerns.** In 1998, the European Union passed comprehensive Data Privacy Directives that provide consumers with strong control over their personal data. Many countries outside of the US have adopted the equivalents of these privacy principles. In the US, over 1000 privacy-related bills were introduced in state legislatures in 1999 and 2000, and numerous federal-level bills are currently floating around in Congress and the Senate. A privacy backlash is clearly underway.

JOHN PESCATORE

- **Wireless access.** Increasing use of wireless LAN connections and the rapid rise of Internet access from cell phones in Europe and Asia are requiring whole new approaches to security. RF connections don't respect firewalls the way wired connections do—a wall just isn't much defense against an air attack. Moreover, the slow processors, small screens, and non-existent keyboards on cell phones and personal digital assistants (PDAs) break many of the standard approaches to access, authentication, and authorization.
- **The need for speed.** Broadband connections to the Internet from homes are exceeding projections. Many businesses are finding that multiple T1 or E1 connections to the Internet are no longer sufficient. Today's software-based security approaches have problems scaling to OC-1 and higher rates.
- **People shortages.** The IT staffing shortage has hit the security field especially hard. To solve this problem, many enterprises are moving increasingly to outsource day-to-day security management tasks. The application service provider (ASP) business model will become increasingly common in the security world. Therefore, security solutions will need to be more manageable in this outsourced model.

Prepare for Impact

While these trends will clearly alter the way we look at and design security in our networks in the long term, their short-term impact will be felt over the next two to four years as security technologies, products and services evolve to strike a balance once again.

JOHN PESCATORE is Vice President and Research Director of Network Security for Gartner. Prior to joining Gartner, Pescatore was senior consultant for Entrust Technologies and Trusted Information Systems where he founded and managed security consulting groups focusing on firewalls, network security, encryption and public key infrastructures. His 22 years experience in computer, network, and information security includes a stint with the US National Security Agency and the US Secret Service, where he developed secure communications and surveillance systems. He can be reached at john.pescatore@gartner.com.

Firewalls will take on specific roles. Network-focused firewalls operating at high speeds will be designed solely for blocking intrusion attempts. They will be hardware based, embedded in routers, appliances, network interface cards (NICs) and integrated circuits. Application-focused firewalls, on the other hand, will be deployed to process and filter a single protocol or a limited set of protocols. These protocol lookouts will be implemented first as software that runs on general-purpose servers, but eventually will be embedded in server appliances and NICs. Network-focused firewalls will be increasingly managed by outsourced services, and hosting companies will offer virtual firewalls (firewall in the cloud solutions) that provide secured bandwidth without requiring management of individual firewall devices. Application-level firewalling will be primarily adopted and managed by high-end, security-conscious enterprises such as financial institutions, government agencies and other regulated or heavily legislated industries such as healthcare.

Intrusion detection systems (IDSs) will have a similar split personality. Network-based intrusion detection will remain primarily signature based, while the need for speed will drive IDS sensors to be embedded in high-speed appliances and network routing and switching devices. Host-based intrusion detection will need to focus more on detecting transaction-level incidents, leaving low-level attacks for detection by network-based intrusion detection. Network-based IDS will follow the firewall trend towards outsourcing, while host-based IDS monitoring will remain self managed. Organizations such as banking, insurance, telecommunications, and governments will create transaction-level incident signatures for use with host-based transaction incident management across marketplaces and trading exchanges.

Vulnerability assessment tools will be used primarily by consulting and system integration firms, while most enterprises will use self-service, Web-based vulnerability scans to indicate a vulnerability that requires investigation by an expert. The price of such scans will drop to levels where daily tests will be used to assure that vulnerabilities are rapidly found and rectified. This will provide the logical equivalent of the "check engine" light on the corporate security dashboard.

"As e-business continues to grow, finding this balance will be critical as it becomes harder and harder to tell the good guys from the bad guys."

Encryption will become increasingly commonplace at both the network and application layers. As Windows 2000 with IPsec support (and future releases with IPv6 stacks) become more widespread, the use of smart NICs and VPN-enabled routers will decrease the cost and complexity of continuous network encryption. The use of Secure Sockets Layer (SSL) to secure application-to-application communications tunneled over HTTP using protocols such as the Simple Object Access Protocol (SOAP) will increase rapidly. Crypto acceleration in NIC cards and in load balancing and caching appliances will become the rule.

Security management solutions will need to evolve from device, data and packet monitoring to transaction-level management. Security policy will need to integrate business conditions and priorities with security inputs to define dynamic alert and alarm levels rather than the static levels driven by low-level inputs we have today. Security standards based on Extensible Markup Language (XML) definitions will be used to support the management of multivendor environments and enable the integration of network- and application-level inputs.

Authorization and privilege management systems will become the focus point for integration of network-level "keep the bad guys out" controls and application-level "let the good guys in" controls. By managing Lightweight Directory Access Protocol (LDAP)-based directories that contain user, process, and object security attributes, authorization systems will have architectural mech-

Continued on page 59

Security, Continued from page 57

anisms for implementing security policy driven by business rules across e-business networks and systems. Various methods of authentication, from username/password pairs to digital certificates to biometrics will be used simultaneously, and authorizations will use level-of-authentication attributes as another means to determine access rights. XML-based interfaces will play a major role, providing the lingua franca for security solutions to integrate and interoperate with business platforms and rules.

The Future Is Wide Open

Over the next two to four years, best-of-breed multivendor solutions will dominate in large enterprises, while single-vendor security suites primarily will be deployed in small and mid-sized businesses or those enterprises that buy into large-scale network management frameworks. Vendors who provide architectural solutions and open interfaces, adhere to industry standards, and aggressively partner with third-party security solution providers will obtain leadership positions in the increasingly crowded security industry.

While we can project a logical path for security technologies and products to become more comprehensive and more effective, the most critical element of network security will always be process and people. Business directives and security policies must be integrated right from the start. Security shouldn't be an afterthought once the business plan and network are complete.

Businesses who successfully lead in the information age will be those that efficiently find the balance between protecting corporate and customer information, and making sure good ideas and creativity are not "pent up" and made ineffective. Security managers and administrators must continually refresh their skills to keep ahead of the bad guys without getting in the way of the good guys. Change is constant. Security achieved by fighting change is false security, equivalent to building more walls as the cannons start firing. ▲▲

FURTHER READING

For more information, visit the following URLs:

- **Gartner Group: www.gartner.com**
- **Computer Security Resource Center of the National Institute of Standards and Technology: csrc.nist.gov/**
- **International Computer Security Association's certified product list: www.icsa.net/html/labs**
- **List of up-to-date vulnerabilities and fixes: securityfocus.com**
- **Computer Security Institute: gocsi.com**
- **The System Administration, Networking and Security Institute: sans.org**