

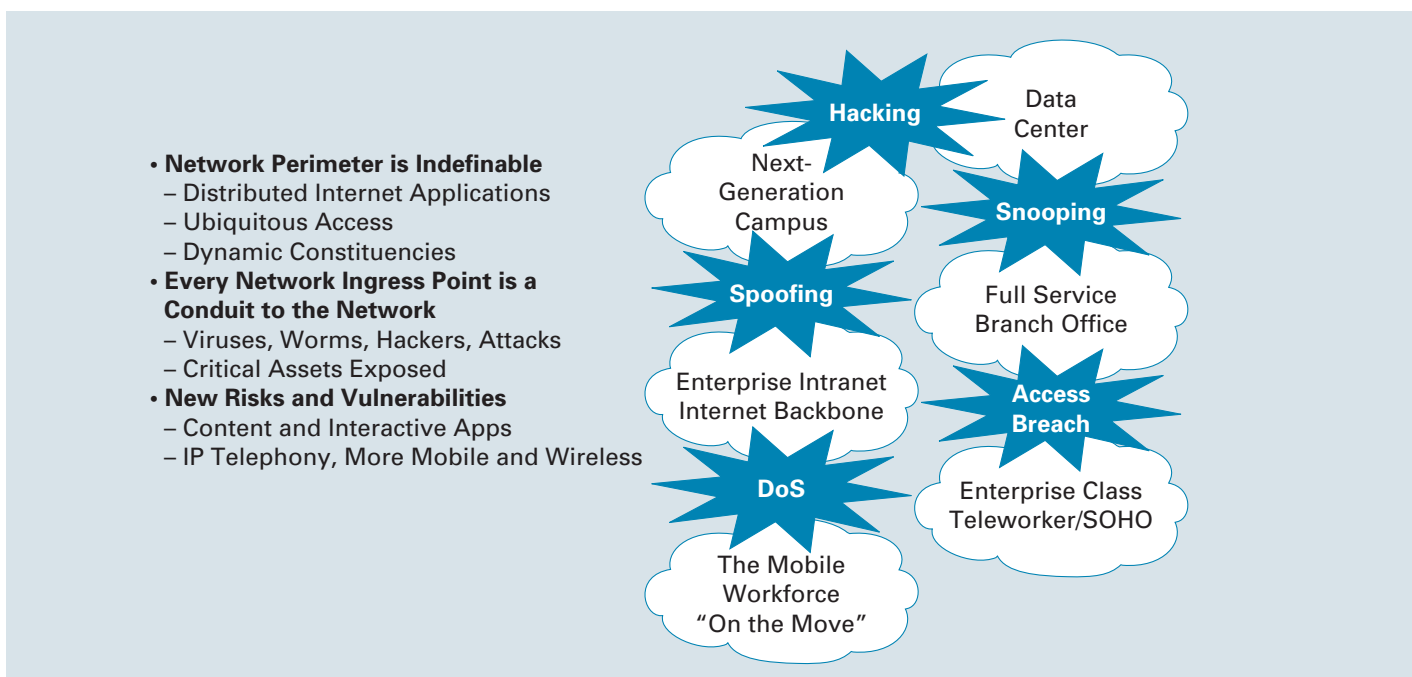
SECURING THE INTELLIGENT INFORMATION NETWORK

— By Jayshree Ullal,
Senior Vice President/General Manager, Security Technology Group

The future of networking is at a critical juncture. The industry can continue building specialized individual products or it can create unified networking systems that enable organizations to increase productivity, reduce costs, and gain competitive advantage. At Cisco Systems®, we believe the greatest benefit to our customers will come from creating holistic networks, with each element integrated and working in concert with the other parts of the communications infrastructure. Today, we are assembling the foundation for such a system, what we call the Intelligent Information Network.

No single aspect of modern networking more dramatically illustrates the need for such a systems-based approach than security. Today, there is not another network capability in more demand. As recently as two years ago, systems administrators had hours or days to respond to new network security threats. Now they only have minutes or even seconds. Unfortunately, we have all become familiar with the injection of illegal worms and viruses into the network that have spread widely and quickly around the globe. Malware like this is designed to take advantage of insecure environments, and can have nontrivial effects and significant costs. The annual cost to businesses from repairing and warding off viruses and worms is now in the billions of dollars. Until this point, network operators have had to rely on patches and point products for their security defenses, but, clearly, these options are not providing the antidote to today’s ingenious and disruptive breed of network threats.

Figure 1 The Evolved Network Security.





In response to the current needs for more robust security, Cisco is developing integrated, systemwide network defenses that enhance—both in terms of effectiveness and value—traditional point-product security offerings. The Cisco Self-Defending Network is a comprehensive approach to a secure network that is an integrated, multi-layered protection system. Cisco believes such an approach is by far the most effective way to defend networks, their applications, and their data from current and future threats. By providing networkwide system security, the Self-Defending Network helps organizations and individuals use Internet Protocol (IP)-based communications to their full potential for boosting productivity and reducing operational costs.

Undeniably, network security has become more important than ever. Converged data, voice, and video communications are now critical to businesses and individuals while the perimeter of a secure network is ill-defined. The introduction of client proliferation, mobile devices, and Voice-over-IP telephony places greater demands on the linkage between endpoint and network security. Networks contain information on practically every aspect of commerce and life, including the most sensitive data such as medical files and financial records. Such networks are no longer an ancillary operation, but rather, the means for carrying out virtually every business function including voice and video communications. Today, the network is the business and the business is the network.

Traditional Security Falls Short

Traditional information security methods—largely based on stand-alone point products, successive operating system patching, and continuous antivirus software updates—are proving insufficient to effectively address current networking security requirements. These approaches fall short because they can only protect one part of the network that is easily circumvented by new attack methods. Also, each product requires its own interface and policies, and as a result, most of these point products do not talk to one another. Finally, current network security defenses are reliant on manual control and intervention, which has proven too slow and reactive to counter the latest crop of worms and viruses.

Because of these limitations, traditional networking defenses are costing companies as much, if not more, in management overhead as from damages. Network operators are now required to add an accelerating array of antivirus software updates, operating system patches, and application fixes, often absorbing so many IT resources that crucial projects are put on hold. Routinely, companies must make unscheduled and unplanned “fire-fights” against new viruses that force IT departments into reactive and disruptive security measures.

Many historical approaches to network security have been limited by their concept of network security. Some looked to the “fortress” model, which uses firewalls and other technologies to keep everyone except authorized employees out of the network. But this approach is currently challenged by new business requirements that demand anytime, anywhere access for diverse populations—including employees, vendors, contractors, and

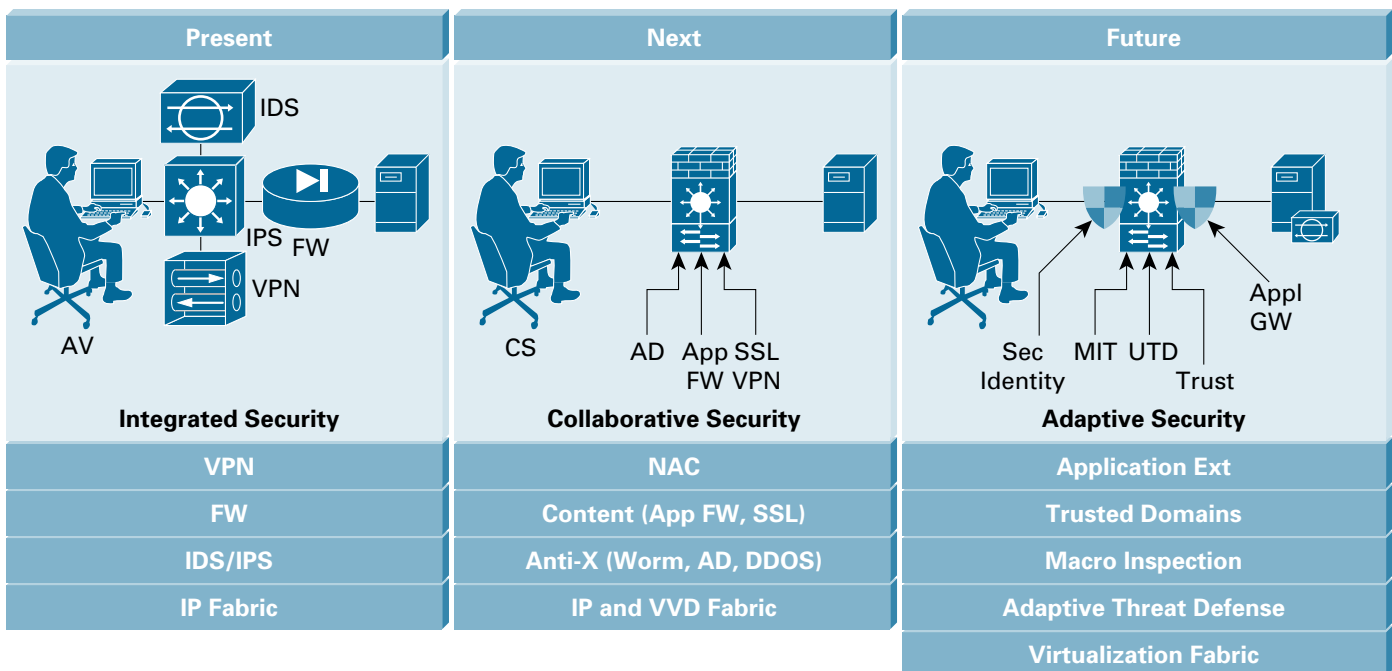
guests. In addition, internal threats continue to pose significant security dangers to organizations. Other approaches have neglected to include personal computers, servers and other “endpoints” within the structure of a network’s security, thereby ignoring key control points for stopping the growth of worms and viruses.

Adaptive Security Through Network Intelligence

Fortunately, the fundamental technology for protecting digital information and communications infrastructure from today’s security threats already exists. Network routers and switches have innate visibility into the network and its activities, as they see and control the flow of all data and IP-based communications. These core networking components, combined properly with specialized security technologies and services, such as endpoint monitoring software, will deliver unparalleled security capabilities in phases.

Cisco is now using the infrastructure of the Intelligent Information Network to form a layered and integrated lattice of protection that addresses the shortcomings of traditional security measures. Contrasting with point products, the Self-Defending Network is a *system* of defense that leverages the ubiquitous sensing and control capabilities of the network, each part communicating with the other to strengthen protection across the entire infrastructure. Such an integrated system creates a coordinated, consistent, and proactive environment to identify, mitigate, and respond to threats. The result is network security that is a unified threat baseline-capable of responding in computer-speed to security alerts, helping reduce windows of vulnerability while lowering management burdens.

Figure 2 Self-Defending Network Evolution



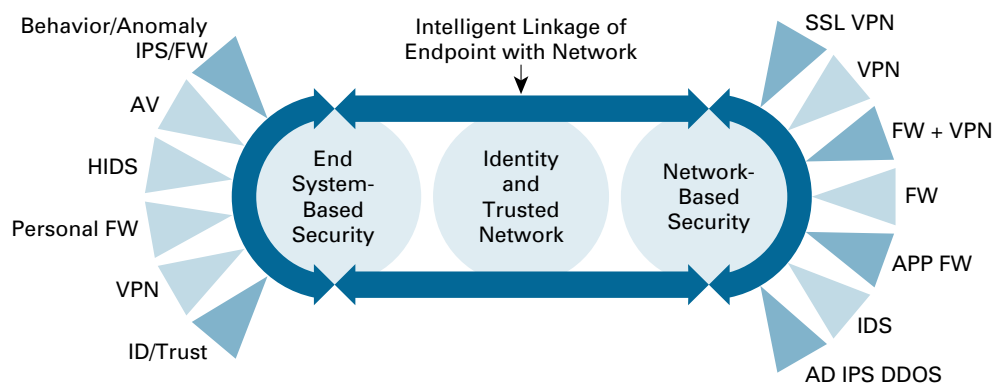


Cisco is modeling the Self-Defending Network on the way our bodies protect us and deal with infections and diseases. Like the human body's skin and membranes, the Self-Defending Network has several protective layers—VPNs, firewalls, intrusion prevention, and anomaly mitigation. When combined with advanced virtualization, deeper packet intelligence and behavioral linkages with end systems, the Self-Defending Network is able to keep out dangerous elements. But also like the human body, the network cannot completely stop all bad things from entering. People need to eat, drink, and breathe, and networks need to process and deliver information from a wide variety of external sources. With this in mind, Cisco is constructing the Self-Defending Network to work at capacity or near capacity even when invaded by detrimental entities, just as the human body can keep on functioning even when it has an infection or disease.

Endpoint Identity to Network Trust Linkages

More importantly, Cisco is designing the Self-Defending Network to evolve with the security needs of the Intelligent Information Network, as well as changes in desktop, hosts, and applications. To support the first phase of the Intelligent Information Network, the Self-Defending Network creates defense positions on the edge of the network with user and device access controls, more intelligent firewalls, intrusion prevention tools, and end-point protection with proactive, behavior-based security software, using IP as the foundational fabric. Cisco is also extending this structure of protection with advanced virtual

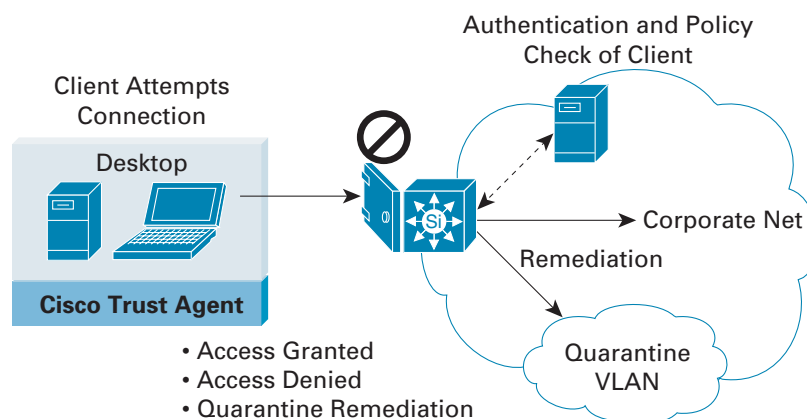
Figure 3 Collaborative Security



An Integrated System

- Endpoint Security Solutions Know Security Context and Posture
- Policy Servers Know Compliance/Access Rules
- Network Infrastructure Provides Enforcement Mechanisms

Figure 4 Cisco Network Admission Control: First Trust- and Identity-Based Security Solution



private network technologies to more effectively include remote and mobile users within the Self-Defending Network's umbrella of protection. All of these tools are bound together with centralized management for coordinated responses and synchronized policies.

Cisco's most significant security innovation for the initial development of the Self-Defending Network is the linkage between the secure IP network and the endpoints based on Network Admission Control (NAC). NAC is an industry first in bringing an important precedent for multicompany collaborations for network security. Initially, Cisco developed NAC in conjunction with leading antivirus software makers, including Network Associates, Symantec, and Trend Micro. IBM and Microsoft have since pledged support for NAC and are working in close partnership with Cisco. NAC makes it possible for networks to control access based on the security compliance of a given endpoint. NAC can assess whether a laptop, desktop, or server requesting access to the network is equipped with up-to-date antivirus software and operating system patches. NAC can also restrict access of any noncompliant devices by using Cisco routers and switches.

As the Intelligent Information Network moves into phase two over the next one to three years and begins providing more dynamic resource utilization, particularly in the data center, the evolving network security system will automatically respond to threats. Cisco will focus on speeding responses to new attacks by aggregating information from various detection technologies and tying it into dynamic policy control systems. Key to this will be the ability to identify, locate, and isolate infected systems and then coordinate the removal of harmful traffic in the network. This prevents further propagation of the virus within the rest of the environment or other linked networks.



Cisco's Self-Defending Network will work with security vendors to harness the virus and behavior detection potential of various network elements, such as e-mail servers, antivirus gateways, or even other desktops. Within the SDNI system, these devices can “tattle tale” on other network parts that are exhibiting anomalous behavior—behavior suggesting they have been coopted by a malicious program or hacker. The system of routers and switches are then used to isolate any infected devices and isolate unprotected systems while network operators are upgrading their security defenses.

The Future of Cisco Security

As we look three to five years out, network security demands will only increase as the network continues to grow in sophistication. During this third phase, the Intelligent Information Network will likely start offering virtualized applications and services, making it easier for users to access the applications and information they want, when they want, and how they want. But freely exchanging applications also opens the door to more abuses. As applications and resources traverse more frequently across multiple networks, virulent coding can also follow those paths. To protect against such attacks, the Self-Defending Network will need to conduct more detailed examination of traffic, even looking at applications or message-level information to ascertain the “intent” of the applications to more reliably and rapidly identify misuse or threats. Though technically challenging, such capabilities will provide dynamic, end-to-end application and content-level security. Along with such detailed inspections, the Self-Defending Network of the future will also require a policy-based security framework that is transparent to all applications and that can be autonomously enforced.

To facilitate these more detailed security processes, Cisco aims to “hardwire” more security functions into router and switch forwarding paths. Just as Cisco has led the industry in performance improvements for packet processing, we aim to lead the industry in high-performance security networking. The third phase of the Self-Defending Network will also require further ASIC and processor advances for performing detailed packet inspection and application-level control. Simultaneously, many of the software-based tools of today will migrate into hardware processors to become standard features, helping further reduce the impact of security functions on network performance.

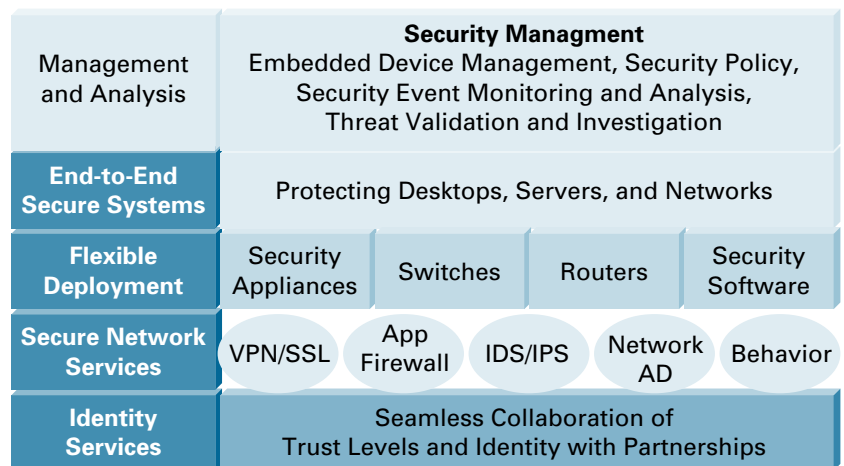
Throughout all of the phases, Cisco will form partnerships with other vendors to enrich the defense capabilities of the Self-Defending Network. The key to such a security approach is not that all parts come from one monolithic system, but, rather, that they all use industry standards to communicate efficiently and effectively with one another for a coordinated defense. Such united industry partnerships could lead to key security advances, such as universal digital identifications for applications and devices.

Clearly, corporations and network operators need an alternative to traditional point product security approaches. Cisco believes the Self-Defending Network is the answer.

Regardless of the technologies involved, the Self-Defending Network has one goal: making communications better by making networks more secure. And better communications mean better business. Significantly, the automated defense capabilities of the Cisco Self-Defending Network forms not only better security but also more cost-effective security by eliminating many of the onerous manual processes now draining IT departments.

Knowing the network is secure frees organizations and individuals to reap the many—and expanding—benefits of IP-based communications. With better security, network users can more quickly and easily gain access to applications and services. Such freedom brings productivity increases while building closer customer and partner relationships. And in the end, better security protects the most important asset of all: peace of mind.

Figure 5 Cisco Self-Defending Network Framework



CISCO SYSTEMS



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
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
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
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
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.com Website at www.cisco.com/go/offices.

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



Copyright © 2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. CableLabs, DOCSIS, and PacketCable are trademarks or registered trademarks of Cable Television Laboratories, Inc.

All other trademarks mentioned in this document or Website 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.
(0501R) De/LW7877 02/05

Printed in the USA