

Personalized Security Services

Bringing Personalized, Self-Service Features to Subscribers

Today, service providers must offer effective protection against growing security threats to broadband networks. Subscribers want to be alerted to intrusion attempts and to stop both intentional and unintentional spread of worms by unsecured PCs. They also want to prevent botnet attacks from seizing PCs, generating spam, and launching distributed-denial-of-service (DDoS) attacks. Network-based protection from Cisco® goes beyond PC software and protects all converged services, including data, voice, video, and mobility-enabled applications. Self-service features are possible with the Service Exchange Framework and Cisco service control solutions that work together to alert subscribers to malware and then let them disinfect their computers. These features and many others are part of Cisco Personalized Security Services. These services empower users to protect their own data, home and family networks, and entire broadband communities. Service providers can deploy Personalized Security Services as new sources of revenue. Giving the subscriber these new security tools can also reduce call center workloads and costs by making it easier for subscribers to resolve threats and self-configure security settings.

Network-Based Security Technologies

Personalized Security Services are possible with the Cisco Secure Broadband Solution. Based on the Cisco IP Next-Generation Network (IP NGN) and Cisco IP NGN Carrier Ethernet network design, the solution leverages technologies deployed within the Service Exchange Framework, the service creation and management layer of the Cisco IP NGN. The Cisco Service Exchange Framework's unique ability to inspect and control per-subscriber application characteristics provides extended inspection and per-service application control. These capabilities further protect broadband community assets against DDoS attacks, viruses, botnet propagation and more, while also giving service providers the option to offer reliable network-based personalized security services.

Intelligent Cisco security products and self-defending network features maximize security without requiring additional customer premises equipment. Among the products that enable secure broadband solutions, including Personalized Security Services, are intelligent access routers and switches, network and aggregation-layer routers, broadband remote access servers, Multiprotocol Label Switching (MPLS) switches, core switches for converged IP networks, security features such as firewall feature sets, and policy control devices.

Two Cisco products provide new and unique levels of awareness and protection for Personalized Security Services:

- **Cisco Service Control Engine (SCE)** detects and controls specific real-time application content per subscriber. Its ability to classify application content and behavior and extend the security analysis by directing traffic to value-added services (VAS) server systems for detailed virus identification greatly enhances the security offered to each individual subscriber.

- Cisco Intelligent Services Gateway (ISG)**, available in intelligent edge routers, automatically detects when users are accessing the network and determines both the type of service each user wishes to access and the type of device that is being used. The Cisco ISG has the intelligence to manage access to various types of services – both IP Multimedia Subsystem (IMS) and other non-Session Initiation Protocol (SIP)-based services – by many different types of devices.

Service providers can use these products as part of the Cisco Secure Broadband Solution to offer lucrative Personalized Security Services for individual subscribers or for an entire broadband community, as described in Table 1.

Table 1. Cisco Personalized Security Services

Personalized Security Service	How it Works
Security Self-Service Station: If a computer appears to be infected with malware that is being pushed out into the broadband community, the offending outbound traffic is redirected to a self-service station to prevent the malware from spreading. At the self-service site the subscriber is guided through potential remedies. This service applies to all subscribers to protect the broadband community.	A Cisco SCE located close to the subscriber can analyze all user traffic using heuristic and behavioral analysis to recognize security threats. The Cisco SCE processes traffic directly and, if needed, uses additional screening supplied by VAS systems. After identifying an infected user device, the Cisco SCE can also block suspect traffic or notify the end user by redirecting HTTP traffic to the Self-Service Web Portal site. Once remediation has been completed, the subscriber's original subscription package is restored. Two methods enforce remediation: "Safe Harbor" directs the user to a self-service station at sign-on to scan for required preconditions (for example, supported equipment, operating system, configuration) to remediate any issues before network session begins; "Quarantine" responds to violations during an active session and dynamically restricts offending use until a remedy is selected from the self-service station.
Content Classification and Access Restriction: Adults can classify and customize restrictions to Internet content and impose time limits to protect children from what they consider offensive content. Governments or social networks can protect members from content sources deemed harmful. Providers can offer individual subscription to this service for an additional fee.	The Cisco SCE intercepts the packets coming from a home computer that has subscribed to content classification services. The Cisco SCE implements native URL access control using an internal URL cache updated from public URL repositories to comply with local filtering regulation or to promote social responsibility. The Cisco SCE can also integrate with third-party parental control systems by querying the classification of URLs and applying the appropriate per-subscriber policy.
SPAM Reduction: Cisco network intelligence can detect and block SPAM destined to an individual. Providers can offer individual subscription to this service for an additional fee.	This network-based solution uses the Cisco SCE to forward Simple Mail Transfer Protocol (SMTP) mail traffic for inspection by a VAS server.
SPAM Source Control: Cisco network intelligence can detect and redirect unregistered sources of SPAM. Providers can enforce SPAM site registration to simplify opt-in or opt-out service contracts.	This network-based solution uses the Cisco SCE to recognize end users infected by a SPAM zombie and unknowingly being used to issue SPAM messages. The Cisco SCE counts outbound, off-net, SMTP sessions against a threshold and can alert the service provider to block the suspect traffic or notify the end user once a violation is detected.
Personal Network Protection: Network intelligence can detect and block known malware and prevent privacy probing, or worm attacks to the home device. Providers can offer an individual subscription to this service for an additional fee or make the offer to an entire community.	This is a network-based solution that uses the Cisco SCE in conjunction with other specialized elements to perform heuristic and behavioral analysis to recognize denial-of-service (DoS) attacks, worms, scan/sweep attacks, and more. The Cisco SCE can log alerts for the subscriber and the provider's operational support system (OSS). Then the Cisco SCE can drop malicious traffic before it reaches subscriber assets.
Virus Propagation Protection: Network intelligence can detect and block known malware and prevent virus or worm propagation through the network. Protection can be enabled for all subscribers.	This network-based solution uses the Cisco SCE to perform heuristic and behavioral analysis to recognize distributed DoS attacks, worms, viruses, scan/sweep attacks, and more. The Cisco SCE can correlate information from multiple endpoints for effective detection. It can then send alerts to block malicious traffic or redirect the user to a Webpage that notifies them of the problem and proposes actions. The Cisco SCE can also be used in a similar way to provide parental controls for minors.

Summary

Service providers can reduce call center overhead, generate new revenue, and provide enhanced security to broadband networks with Personalized Security Services from Cisco. An array of self-service and centralized security features put access to content and the ability to configure security into the hands of individual subscribers. These security services can be used to protect individual users, families, and entire broadband communities. Utilizing the embedded security intelligence at all layers of the Cisco IP NGN and tools such as the Cisco SCE and Cisco ISG, Personalized Security Services are a compelling extension of the Cisco Secure Broadband Solution.

Contact Cisco Today to Learn More

To learn more about Cisco Personalized Security Services, please contact your Cisco account manager or visit

http://www.cisco.com/en/US/netsol/ns734/networking_solutions_sub_solution.html.



Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc. Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc., and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuickStudy, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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. (0701R)