

Enhanced Security for IP Communications: Integrated Network Security

IP communications technology—the convergence of data, voice, and video onto a single network—offers enterprises attractive opportunities for reducing communication costs and complexities as well as enabling progressive productivity gains. The Cisco IP Communications system delivers enterprise-class solutions for IP telephony, unified messaging, IP video and audio conferencing, IP video broadcasting, and contact centers. Enabled by Cisco AVVID (Architecture for Voice, Video and Integrated Data), Cisco IP Communications solutions dramatically improve operational efficiencies, increase an organization's productivity, enhance customer satisfaction, and enable a collaborative workforce.

The key to unlocking these tremendous gains is the confidence that comes from knowing the voice network is secure and protected from disruption. Today, Cisco Systems offers a detailed security design for Cisco IP Communications—the Cisco SAFE Blueprint for IP Telephony—which encompasses functions such as voice and data traffic segmentation, intrusion detection, voice firewalls, and security monitoring.

Integrated Network Security for IP Communications builds on the SAFE foundation to provide comprehensive system-level protection of voice assets through tight integration between IP Telephony and the IP network infrastructure. Integrated Network Security enhances voice security by extending the authentication and encryption capabilities of the data network into the voice network, thereby generating new levels of system

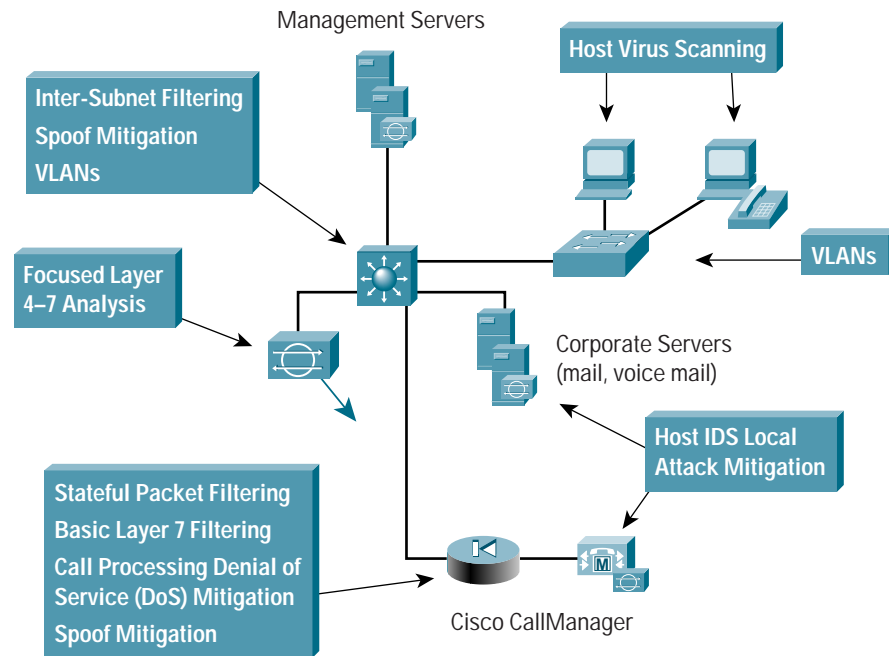
integrity, and greater protection of the system's efficiency and productivity benefits.

The SAFE Blueprint for IP Telephony from Cisco

The principal goal of the SAFE Blueprint is to provide “best practices” information for designing and implementing secure networks. The SAFE Blueprint serves as a guide to network designers when considering a network's security requirements and is based on a defense-in-depth approach to security design. This approach focuses on expected threats and methods of mitigation, rather than on simply specifying, “Put the firewall here; put the intrusion detection system there.” The SAFE Blueprint strategy results in a layered approach to security, in which the failure of one security system is not likely to lead to the compromise of network resources (Figure 1).



Figure 1
Strategy of SAFE Blueprint for IP Telephony from Cisco



The SAFE Blueprint does not offer a revolutionary way of designing networks but rather a blueprint for securing them. Through Cisco AVVID, the SAFE Blueprint emulates as closely as possible the functional requirements of enterprise networks and incorporates security elements that Cisco believes are critical to effective protection of IP communications systems. These security elements, delivered by Cisco today in a variety of forms, include the following:

- *Extended perimeter security*—This element provides the means to control access to critical IP communications applications, such as Cisco CallManager, so that only legitimate IP phones and telephony applications can access the network. Routers and switches with access control lists and stateful firewalls, as well as dedicated firewall appliances, provide the control necessary for extended perimeter security.
- *Voice privacy and secure connectivity*—To ensure communications privacy and integrity, voice media streams must be protected from eavesdropping and tampering. Data networking technologies such as Layer 2 and Layer 3 access control, stateful firewalls, and virtual LANs (VLANs) can segment voice traffic from data traffic, preventing access to the voice network (voice VLAN) from the data network (data VLAN). Stateful firewalls broker the connections between the voice and data VLANs, restricting access only to legitimate devices. VPN solutions encrypt voice traffic as it traverses the WAN.
- *Intrusion protection*—Network-based and host-based intrusion detection systems reside in the voice network to monitor and reactively respond to security events in real time. Using intrusion protection systems, network managers can obtain unprecedented visibility into the network's current data stream and security posture.
- *Security management*—As networks grow in size and complexity, so, too, does the requirement for using centralized tools to manage device, configuration, and security events. Sophisticated tools for managing security policies also enhance the usability and effectiveness of network security solutions. Policy management tools enable users to define, distribute, enforce, and audit the state of security policies through a browser interface.



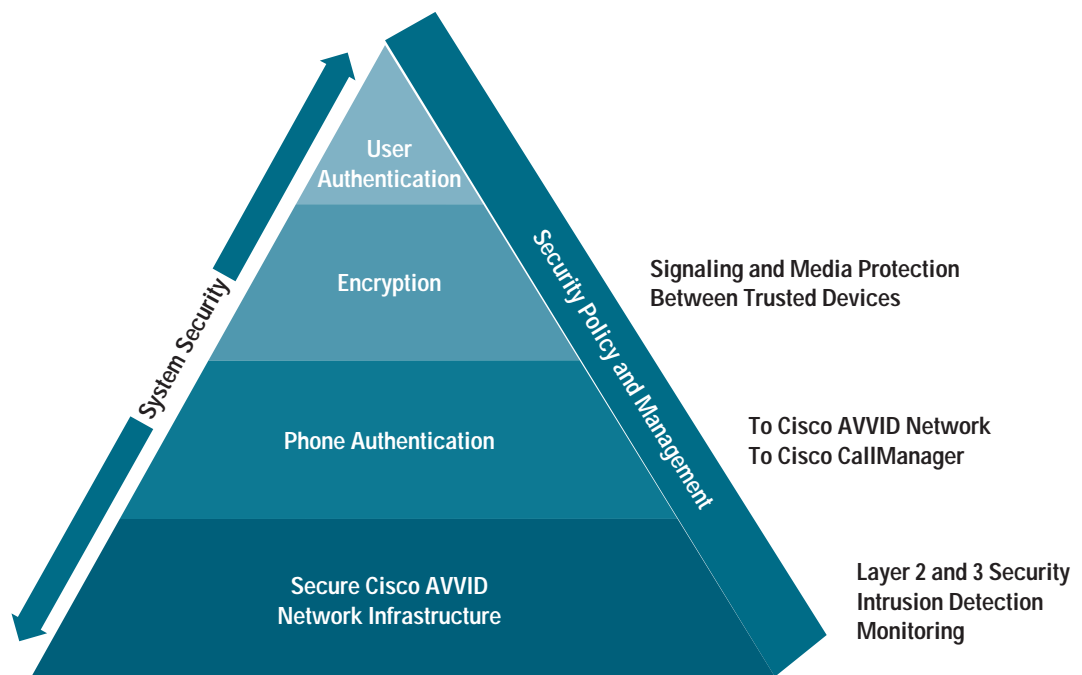
Directions for Enhanced Security in Cisco IP Communications Solutions: Integrated Network Security

Today, Cisco delivers integrated network security solutions on modular, scalable platforms that include Cisco routing and switching infrastructures as well as specialized security appliances. These solutions are complemented by Cisco offerings for security management software, consulting, and educational services.

Advanced security features, such as dynamic policy enforcement in response to attacks and misuse, provide real-time protection for enterprise networks. Embedded software solutions—plus hardware-based accelerators for firewalling, encryption, and intrusion detection—protect a Cisco network infrastructure while enabling continued high levels of performance, scalability, and reliability. By employing a policy-based management approach, Cisco also makes it easy to define, enforce, and audit security for users and devices throughout an enterprise.

A new direction, integrated network security for Cisco IP Communications, will provide comprehensive security with system-level protection, integrity, and privacy through tighter integration with the security capabilities of the data network. Integrated Network Security preserves existing investments in Cisco infrastructure, security systems and IP Communication solutions, and creates layers of security that build on each other to maximize protection of the complete communications system.

Figure 2
Layered Approach of Cisco Integrated Network Security for IP Communications



As Figure 2 illustrates, each layer of security provides specific security features and provides a solid foundation for the subsequent layers:



- *Secure AVVID network infrastructure*—Based on the SAFE Blueprint for IP Telephony, this layer provides a solid foundation with Layer 2 and Layer 3 access control, stateful firewalls, and separate VLANs for data and voice. Security appliances such as network and host intrusion detection systems and security monitoring consoles are also included in this infrastructure layer.
- *Phone authentication (phone identity)*—Ensures accurate and positive identification of IP phones and IP communications applications and devices. Standard technologies that enable identification include authentication protocols such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), Kerberos, and one-time password tools as well as new technologies such as 802.1x, digital certificates, and smartcards. Phone authentication is a two-step process. First, the phone identifies itself to the Cisco Secure AVVID network infrastructure using IEEE 802.1x to gain access to the voice VLAN. In the second step, the phone initiates mutual authentication with the Cisco CallManager.

The phone authentication layer establishes trust between devices and protects against identity theft and man-in-the-middle attacks. This level of trust is critical to the integrity of the system and the subsequent layers of encryption and user authentication.

- *Signal and voice media encryption*—When built upon a layer of authentication, encryption provides privacy between accurately identified IP phones, Cisco IP Communications applications, and network resources. Effective signal and voice media encryption requires standards-based strong cryptographic capabilities, including encryption algorithms and key management, with system-wide implementation. IP phones, conference bridges, voice gateways, and applications such as voice mail and unified messaging must all integrate into the security architecture for effective and meaningful end-to-end encryption.

Integrated network security also brings awareness of signal and voice media encryption into the network, allowing authenticated network infrastructure security services such as Network Address Translation (NAT) and stateful firewalls, to interoperate with encrypted voice. This integration maintains the topological and mobility benefits of IP telephony while enabling new levels of system security.

- *Phone user authentication (user identity)*—The final layer of security is accurate identification of the phone user. In the other layers, security is embedded within the Cisco IP Communications systems and is transparent to users. User authentication extends integrated network security out to the user for organizations that want to control network access rights based on user identification. These planned enhancements will use authentication protocols such as RADIUS and TACACS+ to expand the existing user authentication capabilities of extension mobility while integrating user security into the network infrastructure.

Integrated Network Security—Investment Protection and Comprehensive System Security

These planned integrated network security enhancements for IP Communications solutions preserve existing investments in Cisco AVVID infrastructure and IP Communications solutions, and help customers achieve levels of voice security that have not been possible in classical Time Division Multiplex (TDM) PBX systems. Integrated network security will protect Cisco IP Communications assets and transmissions while preserving operational savings and productivity gains.

For More Information

To learn more about Cisco IP Communications and Cisco voice solutions, visit <http://www.cisco.com/go/ipc>. A series of detailed white papers on the Cisco SAFE Blueprint, and about Cisco V3PN Voice and Video VPN solutions are available at: www.cisco.com/go/safe.

Cisco and selected Cisco partners also offer a full range of design, implementation, consulting, and outsourcing services to help enterprises build and operate secure IP communications systems and networks. For more information about these services, visit www.cisco.com/go/securitypartners or www.cisco.com/go/avidpartners.



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices**

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.
(0301R) SD/LW4148 02/03