

Enterasys Secure Networks™ for VoIP

Enabling and Securing Voice over IP in *Any* Network

Overview

Security is among the top concerns of enterprises deploying voice over IP systems today. Enterprises need to detect unauthorized use of VoIP systems, prevent service disruptions and eavesdropping, and monitor for new threats against the voice infrastructure – all while ensuring reliability and quality of service. Rather than approaching VoIP security in a haphazard fashion, Enterasys recommends an intelligent, automated and integrated approach to enable and secure wired and wireless VoIP communications.

Enterasys enables and secures IP Telephony solutions from 3Com, Alcatel, Asterisk, Avaya, Cisco, Mitel, NEC (Sphere), Nortel, Panasonic, Polycom, ShoreTel, Siemens and others. Enterprises worldwide want to ensure the same reliability, quality, manageability, mobility and security of the traditional PBX with new voice-over-IP (VoIP) and unified communications solutions. The Enterasys Secure Networks for VoIP solution delivers a way to sense and automatically respond to security threats against the IP telephony infrastructure; enforce network access control policies; and comply with regulations for monitoring and safety. You can learn more about our open-architecture, standards-based approach to supporting any convergence application from any vendor by reading our [whitepaper](#).

The Enterasys Solution

The Enterasys Secure Networks™ architecture is a unique approach to networking and security that integrates intelligent switching, routing and wireless products, (The Security-Enabled Infrastructure); Network configuration and management software applications, (The Visibility and Control); Intrusion prevention and Network Access Control, (The Advanced Security Applications).

With these three fully integrated components, Enterasys Secure Networks™ delivers important capabilities required to enable and secure a VoIP solution.

Choice

Enterasys maintains a long-standing commitment to standards-based technologies and open-architected systems. Leveraging this commitment, Enterasys offers a solution that will support any VoIP application from any vendor. An Enterasys solution can identify and control any voice application running on the network and ensure it is secured and prioritized based on the business requirements. The open architecture approach gives organizations the choice necessary to deploy the right business application at the right time, for the right reasons. There is no dependency in the network architecture restricting the converged applications that can be deployed.

Reliability

An Enterasys solution assures customers of the ability to meet capacity and Power over Ethernet (PoE) requirements to support IP phones connecting to the converged network. A single Matrix® N-Series switch can accommodate over 500 PoE ports with fault-tolerant power management to keep voice services working to every connected endpoint. Enterasys products support all of the standard technologies necessary to ensure full redundancy and communications resiliency (technologies such as 802.1w, 802.1s, 802.3ad, OSPF, VRRP). Beyond the standard technology features, Enterasys embeds innovative broadcast flooding protection and communication flow overrun protection in switches to ensure that dangerous network traffic patterns do not result in communication failures for critical voice services.

Benefits

Choice

- Open-architecture, standards-based interoperability with VoIP products from multiple vendors – voice is just another application enabled by Enterasys Secure Networks™ without locking you into something proprietary.

Reliability

- Device and network high-availability ensures the continuity of voice services.

Quality

- Discover, classify and prioritize voice communications to ensure service-level demands.

Manageability

- Central visibility and control over VoIP communication and security policies.

Mobility

- Voice over wireless without delay or compromise.

Security

- Prevent and automatically respond to security threats against the VoIP service.

**There is nothing more important
than our customers.**

Quality

An Enterasys solution can discover and classify an IP phone the moment it connects to the network. Once the IP phone is detected, the Enterasys solution can enforce appropriate security and communication policies in the network to ensure the quality of the voice service. Convergence End Point (CEP) detection methods include LLDP-MED, destination IP address and Layer 4 Port, SIP, H.323, H.245, Cisco Discovery Protocol, and Siemens CoreNet. Enterasys switches also support multi-user, multi-method authentication to identify and classified more than one device on a single Ethernet connection. Once an IP phone is detected, Enterasys switches will automatically enforce VoIP communication policy rules for prioritization, rate shaping and security of voice traffic.

Manageability

An Enterasys solution provides centralized visibility and control of specific network features important to voice communications in a converged network environment. IP phones can be quickly and easily located, voice communication policy rules are centrally established and globally distributed, and responsive action to security threats is automated. Management software provides IT administrators with a single central location for establishing communication and security policy rules for voice services, and an easy distribution method for getting the policy rules out to the entire network infrastructure.

Mobility

An Enterasys solution can provide wireless communications with performance levels sufficient to accommodate the low-latency requirements of VoIP. Enterasys Wireless Controllers and Access Points support innovative Direct Path Forwarding which allows forwarding of traffic to occur at the AP and not through the controller. This is an important capability for VoIP because the WLAN controller can introduce latency into the communication path.

Security

An Enterasys solution includes the ability to centrally manage a set of communication policy rules which can restrict the type and amount of network traffic directed at specific voice related servers. Also, policy rules can be enforced to ensure that critical services are not “spoofed” causing disruption or theft of critical communications. In addition to proactive security of VoIP resources, events occurring on the network that can compromise the voice service can be detected, and ultimately mitigated in order to preserve the voice system continuity. Security appliances have the ability to detect specific threats against voice communications by using a strong set of VoIP attack signatures – including decoders for H.323, H.245, SIP and MGCP. Once threats against voice services are detected, automated services can be used to locate the exact source of the threat and take appropriate action eliminating the threat.

Solution Capability	Enterasys Products
Choice	<ul style="list-style-type: none">• VoIP products from 3Com, Alcatel, Asterisk, Avaya, Cisco, Mitel, NEC (Sphere), Nortel, Panasonic, Polycom, ShoreTel, Siemens and others• Matrix® and SecureStack® switches with high capacity, standards-based PoE capacity
Reliability	<ul style="list-style-type: none">• Matrix®, SecureStack® and RoamAbout® switches, routers and wireless with device and device-to-device redundancy and resiliency features
Quality	<ul style="list-style-type: none">• Matrix®, SecureStack® switches with policy enforcement for voice service-level requirements
Manageability	<ul style="list-style-type: none">• NetSight® software with centralized visibility and control of voice communication policies, security and endpoint location<ul style="list-style-type: none">– Console: Device and network resiliency configuration– Policy Manager: Establish VoIP service-level and security policies– NAC Manager: Endpoint location and compliance reporting– Automated Security Manager: Automation for threat mitigation– Inventory Manager: Capacity planning for CEP deployment
Mobility	<ul style="list-style-type: none">• RoamAbout® WLAN Controllers and Access Points with Direct Path Forwarding
Security	<ul style="list-style-type: none">• Matrix® and SecureStack® switches with policy enforcement for VoIP security• Dragon® Intrusion Detection and Prevention with specific VoIP threat signatures

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

