



IP Telephony

Contact Centers

Mobility

Services

## SOLUTION BRIEF

# ASG Solution Brief



## Administrative Security Environment

Because of the prevalence and increased sophistication of attack tools, broadening diversity of vendor solutions, and the heightened sensitivity of the regulatory and legislative environments, the only way to meet evolving security standards is through a standalone security solution. The Access Security Gateway suite from Avaya can help meet the rigorous security requirements of today's enterprises.

With business trends such as outsourcing, mergers and acquisitions and high employee turnover rates, it is no longer adequate to protect information only from external threats. It is vital to track, monitor, and record the activities of legitimate users to a system, paying particular attention to administrative activities. Administrative interfaces often provide the means to adjust, disable, or otherwise tamper with the overall configuration of a system, including those features that secure the system from outside attack. It is not only malicious users that may make such changes – often, security holes are created by valid users accidentally or for 'ease-of-use' and go undetected until they are eventually exploited.

Avaya understands that implementing a secure network - whether voice, data, or converged – requires more than providing strong authentication for user logins for individual devices. While strong authentication is important, as evidenced by the widespread adoption of the ASG software option in Avaya products, the complete ASG Solution satisfies the needs of today's most security-conscious enterprises.

In response to the need for greater security, control, and accountability for converged networks, the ASG suite provides a comprehensive solution that enables enterprises to meet ever-increasing security, audit and networking requirements. The ASG Suite was developed and continues to be enhanced by an Avaya OEM partner whose sole focus is providing advanced security solutions to the world's largest enterprises.

## Secure Access Management

As organizations attempt to consolidate and centralize administrative functions, it becomes a daunting task to properly manage user access privileges for individual devices. As the number of devices and managed endpoints grows, the overhead of managing access rights grows as well. As a result, companies abandon or neglect established policies for password and user management, often resorting to shared user logins and stale, static passwords. This environment makes it far too easy for disgruntled workers, terminated former employees, and other 'trusted' third parties to access unauthorized equipment.

## Two-factor Authentication / One-time Passwords

The ASG product suite leverages two-factor, challenge/response authentication for all users, eliminating the security risks of static passwords. Because of the need to remember hundreds, or thousands of username/password combinations, system administrators frequently write passwords down in a notebook or spreadsheet, an obvious security risk. Less obvious, however are social techniques for stealing passwords such as social engineering or phishing.

ASG authentication eliminates the risk of password insecurity by providing a single set of login credentials and using a dynamic password that cannot be stolen and reused. The ASG suite provides secure authentication for nearly any device or interface regardless of age, vendor,

- The ASG suite protects both Avaya and Non-Avaya products.
- The ASG suite can secure character, web, Remote Desktop, and other hard-to-secure interfaces.
- ASG solves multiple security audit issues in a single, easy to implement solution.
- Many of the world's largest financial institutions, and government agencies, use ASG to secure administrative access to Avaya and non-Avaya devices.

or protocol, ensuring security across even very diverse networks.

### Unique User Logins

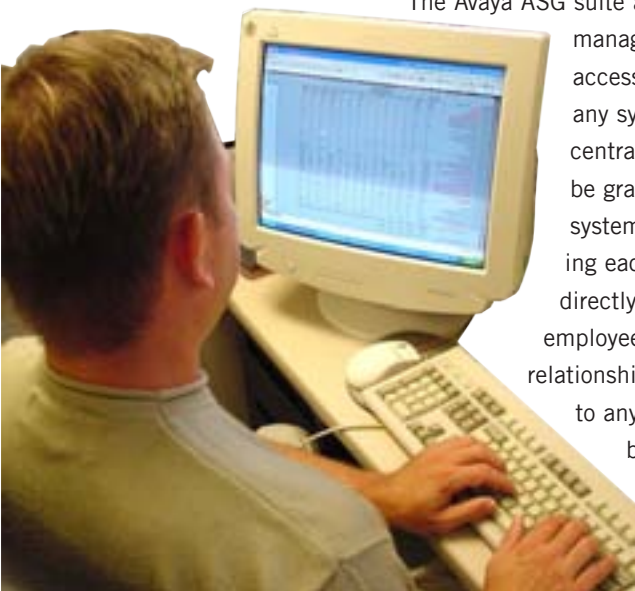
Most electronic equipment is not designed to support a complex environment with a large number of potential administrators. Equipment does not support a sufficient number of usernames to provide separate credentials for each administrator, requiring sharing of login information. This is not acceptable for audit purposes.

Avaya ASG products allow the assignment of unique authentication credentials to each administrator, regardless of the capabilities of the devices they manage. As a result, it is now possible to tightly control administrator access to devices and to specifically identify which administrator accessed a particular piece of equipment.

### Centralized Access Provision

Managing the access rights for a large, complex administrative network borders on the impossible. It is essential to tightly control access for local and remote administrators, service providers, consultants and vendors to thousands of devices across the network. Attempting to manage access to all devices locally is prohibitively time-consuming, expensive and complicated.

The Avaya ASG suite allows enterprises to manage internal and external access by any technician to any system from a single, central location. Access can be granted, limited or revoked system-wide without accessing each piece of equipment directly. In the event that an employee or business partner relationship is terminated, access to any and all systems can be instantly revoked.



## Comprehensive Logging

Retaining detailed records of who accessed and made changes to network systems is critical for audit, training, and forensic purposes. Unfortunately, capabilities of network equipment vary greatly when it comes to recording such information. The ASG suite provides advanced logging and forensic capabilities that can be used to record all administrative activity across the network.

### Logging of all session types

With the proliferation of new ways to access and administer equipment has come new challenges for maintaining access history. Web-based, PCAnywhere/Remote Desktop, and encrypted administration present challenges to maintaining comprehensive access history logs. The ASG suite enables organizations to generate and store complete access history for all devices across the network regardless of the connection method used to perform the administration. By requiring authentication prior to allowing access to administrative interfaces of any type, ASG retains a comprehensive log of all administrative activity. When combined with ASG's unique username capability, it is simple to associate a particular session with a particular user for audit, forensic or legal purposes.

### Session Recording

Frequently, audit requirements dictate a greater level of logging than simple access history. For this reason, ASG provides the capability for record entire sessions on all text-based administrative interfaces. This includes sessions through graphical front-ends such as Avaya Site Administrator. Instead of a simple keystroke logger, ASG records both input data (including non-printing characters) and the data that the system returns to the user. This enables complete session playback for future reference. All recorded sessions are centrally stored in ASG Guardian and are hyperlinked to the Access History logs.

## Out-of-Band Security

The ability of systems to access traditional dial-up connections remains important to the continued operation of both voice and data networks. Whether as a general poli-

cy, or in cases of emergency, use of the PSTN for alarming and remote access to system hardware is critical.

### Security

The ASG Guard II security appliance ensures the security of out-of-band connections, and protects them with the same strong authentication, logging, and monitoring features as in-band connections. The ASG solution eliminates the need to use ad-hoc security measures such as physically unplugging modems, which are frequently ignored and create security issues. The ASG Guard II provides the following security features for out-of-band connections

- Challenge-Response Authentication
- Call-back Authentication
- Session Logging and Recording
- User and Modem Disable Thresholds
- Encryption over Dial-up (SSH, IPsec)
- Connection Alarming (success or fail)

### Flexibility

As an organization migrates from out-of-band alarming and maintenance to in-band solutions, the ASG Guard II enables a smooth transition without impacting process and with no lapses in security. Customers may even choose to have certain devices maintained via IP and others maintained via PSTN to accommodate a mixed environment with multiple service providers / vendors and multiple access mechanisms.

### Adaptability

No two organizations are exactly alike, and individual companies' security requirements and policies vary greatly. While the ASG product suite is designed to be ready to provide secure administrative access out-of-the-box, the platform is highly configurable and can be tailored to meet the individual requirements of any enterprise. Whether the need is for integration with central Network Management Systems, delivering alarms to multiple recipients, automating complex tasks such as regularly scheduled password changes, or other customer-specific requirements, the ASG Solution can be quickly adapted to meet your needs.

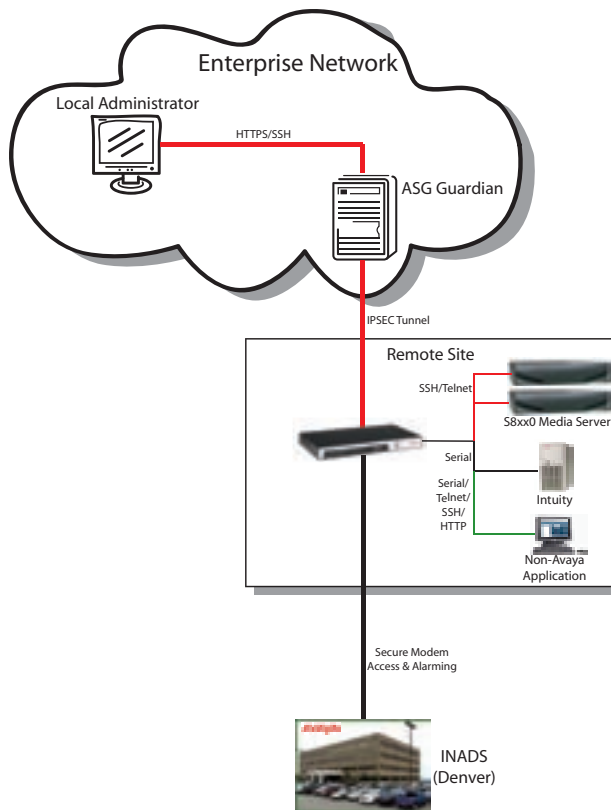


Fig. 3.1 Typical ASG Implementation

### ASG Solution Highlights

- Centralized access management for administrative users
- Multi-factor authentication for all administrative sessions
- Unique logins for all administrative users
- Access logging for all types of connections (text, web, remote desktop)
- Session recording for all character sessions
- Single, consolidated log of all administrative actions
- Secure out-of-band connectivity
- Environmental monitoring (temperature, water, humidity, power)
- Solutions to Audit Problems

**ASG Guardian**

ASG Guardian is a server-based application that provides centralized access and administration for large distributed device networks. The ASG Guardian manages login credentials for endpoint devices, eliminating the distribution of phone numbers, IP Addresses, usernames and passwords to network devices to administrative users.

ASG Guardian serves as a collection platform for alarms, logs, session histories, and other information from ASG Guard II devices in the field. Managers can set global access rights within the ASG Guardian's administrative interface, and can instantly permit or revoke access to devices across the network.

**ASG Guard II**

The ASG Guard II is a security appliance that provides local connection, security, and monitoring for endpoint devices. Featuring 4, 16, or 28 serial ports, 2 Ethernet interfaces, and two modems, the ASG Guard II provides secure remote access to any device over any protocol. The ASG Guard II supports IPSec and SSH sessions for encryption of sensitive information across the LAN, WAN, or PSTN. The ASG Guard II's internal firewall permits access only to authorized devices on the customer network, making it the ideal for securing converged environments.

**ASG SoftKey**

The ASG SoftKey is a software application that provides two-factor authentication services for access to ASG devices. The PIN-activated SoftKey calculates one-time passwords for administrative sessions based on a shared secret key in the token and the ASG system. The ASG SoftKey is compatible with Windows and Palm operating systems.

**ASG Software**

ASG Software is a system that is embedded in many Avaya products to provide two-factor authentication for remote administration. Rather than using a static username and password, the ASG Software provides dynamic, one-time passwords for administrative access.

**Learn More**

To Learn More about Avaya Access Security Gateway products, contact your Avaya Client Executive, or Authorized BusinessPartner, or visit [Avaya.com](http://Avaya.com)

**About Avaya**

Avaya enables businesses to achieve superior results by designing, building and managing their communications infrastructure and solutions. For over one million businesses worldwide, including more than 90 percent of the FORTUNE 500®, Avaya's embedded solutions help businesses enhance value, improve productivity and create competitive advantage by allowing people to be more productive and create more intelligent processes that satisfy customers.

For businesses large and small, Avaya is a world leader in secure, reliable IP telephony systems, communications applications and full life-cycle services. Driving the convergence of embedded voice and data communications with business applications, Avaya is distinguished by its combination of comprehensive, world-class products and services. Avaya helps customers across the globe leverage existing and new networks to achieve superior business results.



**COMMUNICATIONS  
AT THE HEART OF BUSINESS**

[avaya.com](http://avaya.com)

© 2005 Avaya Inc.

All Rights Reserved. Avaya and the Avaya Logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by the ®, SM or TM are registered trademarks, service marks or trademarks, respectively, of Avaya Inc., with the exception of FORTUNE 500 which is a registered trademark of Time Inc. All other trademarks are the property of their respective owners.

Printed in the U.S.A.

02/05 • MIS2744

