



IP Telephony

Contact Centers

Mobility

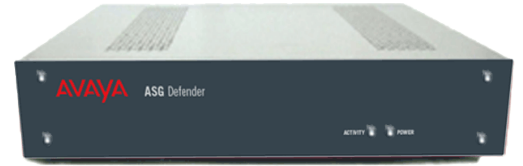
Services

**FACT
SHEET**

ASG Defender

The Environment

Providing remote administrative access to devices on the voice and data network is critical to ensuring business continuity. Unfortunately, providing such access often conflicts with corporate security standards, and those set forth by regulations such as HIPAA and Sarbanes-Oxley. The ASG Defender allows organizations to manage remote administrative access by internal technicians and outside vendors alike. Those technicians and vendors who are permitted to manage devices can easily connect to them, while unauthorized parties are completely locked out. Best of all, Defender makes it easy to prove to auditors that there have been no breaches.



Securing Administrative Access

- Authentication
Secure network access requires unique credentials for all authorized users that can not be lost, stolen, or otherwise compromised. Unfortunately, due to the limitations of most devices, it is not possible to provide each authorized administrator with his/her own credentials, and the inherent weakness of password protection makes it impossible to guarantee that credentials are used only by the appropriate person

The ASG Defender eliminates risks due to insufficient administrative logins and the weaknesses of password authentication. The ASG Defender supports hundreds of unique users, and enables each user to have their own unique username that is consistent for all systems. ASG Defender supports a wide range of strong authentication methods, eliminating the risk of unauthorized access

- Encryption
Encrypting sensitive information while in transit across the corporate network is not only prudent, but specifically required in certain legislation. Unfortunately, not all network equipment supports administration over encrypted channels, and those that do frequently rely on outdated algorithms.

The Defender helps bridge the gap between secure clients and legacy devices by translating between clear-text protocols such as telnet and serial and secure protocols for transmission over the network. For newer devices, the ASG Defender provides passthru support for end-to-end encryption with session capture and recording. This provides confidence to auditors and management that sensitive data cannot be accessed through eavesdropping on authorized sessions.

Monitoring and Alarming

While preventing unauthorized access to network equipment is essential, it alone is not sufficient to ensure that a network runs smoothly. Reliable operation requires constant awareness of administrative activity by internal and external parties, of alarms raised by network devices, and of a device's physical environment.

The ASG Defender provides advanced monitoring and alarming features to provide awareness to both Avaya Services and customer Operations Centers. Defender can recognize and process alarms from Avaya and non-Avaya products and simultaneously deliver those alarms to multiple destinations via SNMP, e-mail, dial-out and pager. The Defender also provides alarming on authentication and other internal events, providing proactive notification when equipment is being accessed. Finally, environmental monitoring provides notification of power failure, high and low temperature, water, humidity, smoke, and physical access or cable removal before damage occurs.

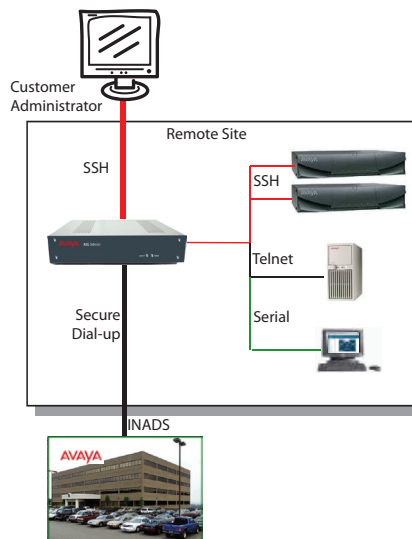
Audit and Compliance

Due to increasingly stringent standards pertaining to controls of IT systems, simply having a secure network is no longer sufficient. It is now critical to be able to certify network security to internal and external auditors as well as senior management. Unfortunately, network diversity makes it nearly impossible to create and enforce consistent security policies for remote administration. For this reason, it is necessary to implement a system to secure, control, monitor, and record all administrative access.

The ASG Defender's comprehensive set of features allow IT organizations to meet the demands of the

most stringent regulations and audits. Defender maintains logs of all events including successful and failed authentication, alarms, access to attached devices, errors and more. These logs can be automatically transferred to other systems such as ASG Guardian for storage and analysis. For more detailed activity monitoring, the Defender can be configured to record entire sessions for all character-based administration. Like the logs, session recordings can be automatically sent to a central server for long-term archival.

Typical Defender Implementation



Defender Specifications:

OS: Linux 2.6.11
 Modem: 1 v.90/56Kflex, RJ11 (Internal)
 Serial ports: 2 or 4 (RJ45)
 IP Ports: 30 (Logical)
 Ethernet: 100BaseT x 2 (RJ45)
 Console port: DB9 (300bps-115.2Kbps)
 USB Ports: 4 (For Future Use Only)

Real-World Interface (4-port only):
 3 Temperature Sensors
 5 Contact Closure Inputs
 Storage: 94Mb Internal Buffer
 Dimensions: 12"W x 1.75"H x 11"D - 6lbs
 Power: 100-240VAC 50/60Hz
 Operating Temp: 32°F - 113°F (-4°C - 45°C)

Storage Temp: -4°F - 140°F (-20°C - 60°C)
 Humidity: 10% - 90% non-condensing
 Approvals:
 FCC Part 15, Class A, EN55022, Class A
 EN50024
 Wall or Shelf Mountable

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.

AVAYA

COMMUNICATIONS
 AT THE HEART OF BUSINESS

avaya.com

Key Defender Features

- Connectivity Support
 - Inbound: Dial-up, IP, Console
 - Outbound: Dial-up, IP, Serial Port
- Two Factor Authentication
 - 3DES Challenge/Response
 - ASG Key
 - RADIUS
 - Callback
- Encryption Support
 - AES, 3DES, DES
 - SSH, SFTP, IPsec, SCP
- Alarm Handling
 - Receipt: SNMP, Serial, Contact Closure
 - Delivery: SNMP, Dial-out, Pager, SMTP
- User Management
 - Separate Avaya and Customer User Tables
 - Restrict access by device, time, login count
 - 200+ Unique user ids
- Certified Avaya Platforms
 - Communication Manager
 - Modular Messaging
 - Definity
 - Intuity Audix
 - Intuity LX
 - Avaya IR
 - Avaya Predictive Dialer
 - Avaya CMS

© 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 • 12345

