GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

GIAC Enterprises Air Services Group

GIAC Practical Assignment
Version 1.0

Edward G. Miller
December 2001

© SANS Institute 2000 - 2002 Author retains full rights.

Table Of Contents

1.0 GIAC Enterprises Air Services Group…… 4
1.1 ASG Information Technologies Infrastructure…….. 4
1.1.1 Corporate Headquarters (CHQ)……4
1.1.2 Hangar Complex……5
1.2 Business Operations…….. 6
1.2.1 Administrative Support……..6
1.2.2 Marketing/Advertising……6
1.2.3 Satellite Sites/Remote Users……...6
1.2.4 AEG Corporate……... 6

2.0 ASG Security Policy……...8
2.1 Areas of Risk…….. 8
2.1.1 Routers and ASG Information System Security…….. 8
2.1.1.1 Threats/risks……8
2.1.1.2 Consequences if exploited……8
2.1.1.3 Mitigation of Threats/Risks…… 9
2.1.2 Security/Protection of Satellite Site/Mobile Users…….. 9
2.1.2.1 Threats/Risks……10
2.1.2.2 Consequences if exploited……10
2.1.2.3 Mitigation of Threats/Risks…… 10
2.1.3 Security/Protection of Publicly Accessible Web site……11
2.1.3.1 Threats/Risks……11
2.1.3.2 Consequences if exploited……11
2.1.3.3 Mitigation of Threats/Risks ……11
2.1.4 Passwords……..11
2.1.4.1 Threats/risks……12
2.1.4.2 Consequences if exploited……12
2.1.4.3 Mitigation of Threats/risks…….. 12
2.1.5 Rapid Detection of Intrusions……12
2.1.5.1 Threats/Risks……12
2.1.5.2 Consequences if exploited……13
2.1.5.3 Mitigation of Threats/Risks ……13
2.2 ASG Remote Access Policy……13
2.2.1 Security/protection of Satellite Site/Mobile Users Policy….13
2.2.1.1 Purpose……..13
2.2.1.2 Scope……...13
2.2.1.3 Policy Statement……14
2.2.1.4 Responsibility……14
2.2.1.5 Action……15
2.2.2 Password Policy……..16
2.2.2.1 Purpose……..16
2.2.2.2 Scope……..16
2.2.2.3 Policy Statement……16
2.2.2.4 Responsibility……18

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.2.2.5 Action……18
2.2.3 Router Security Policy……19
2.2.3.1 Purpose……..19
2.2.3.2 Scope……..19
2.2.3.3 Policy Statement……...19
2.2.3.4 Responsibility……20
2.2.3.5 Action……21

3.0 Password Procedures……22
3.1 Setting Passwords on Servers……22
3.1.1 Assign Boot/Power Password……22
3.1.2 Changing NT 4.0 Operating System Login Password…….22
3.2 Setting Passwords on Desktops/Mobile hosts (DT/MH):.....22
3.2.1 Assign Boot/Power-up Password.....22
3.2.2 Setting Operating System Password for Local Log-On.....23
3.3 Managing User Passwords.....23
3.3.1 Making New User Account Passwords.....23
3.3.2 Forgotten Passwords.....24
3.3.3 Changing Passwords on User Accounts.....24
3.3.4 Mitigate Password Violation (s).....24

Figure 1.....26
References.....27

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1.0 GIAC Enterprises Air Services Group

GIAC Enterprises Air Services Group (ASG) is a rotary wing services group located at the Colorado Springs International Airport (CIA), Colorado Springs, Colorado. ASG occupies a prominent regional position providing diversified rotary wing services focusing on Heavy Lift Transport (HLT), Executive Transport (ET), Emergency Medical Service (EMS), and the Recreational Transport (RT) markets. ASG operates 40 specially configured Sikorski UH60 helicopters tailored to meet unique specifications required in each market and employs corporate aviation professionals from both civilian and military marketplaces. In order to meet the diversified needs of customers ASG operates each of it's four divisions as unique entities concentrating on distinct requirements of each market place.

1.1 ASG Information Technologies Infrastructure

The ASG corporate campus is a 2 building complex; ASG Corporate Headquarters and the ASG hangar complex co-located within 500 yards of each other at CIA. Within the hangar complex each of ASG's 4 divisions (HLT, ET, EMS, RT) operate as unique autonomous entities. As needed ASG populates satellite off campus sites to support customer market needs. ASG is partnered with Aviation Enterprises Group (AEG) for maintenance and supply support for all ASG entities. AEG corporate is located in Denver, Colorado however it maintains an onsite office within the ASG hangar complex

The ASG IS infrastructure is based on Cisco's secure blueprint for enterprise networks (SAFE) design. SAFE takes a, "defense-in-depth approach to network security design" which focus on the "expected threats and their methods of mitigation."[1] "The SAFE strategy results in a layered approach to security where the failure of one system is not likely to lead to the compromise of network resources."[2] An integral charter of the SAFE strategy is the concept of modular design and ASG employs this concept throughout it's IT infrastructure.

1.1.1 Corporate Headquarters (CHQ)

CHQ is nerve center of all ASG operations. Per fig. 1, CHQ maintains primary information system resources (servers, management systems, security systems) and acts as the single point of connectivity (entry and exit) to the public sector for corporate and hangar complexes. This assures efficient, effective and secure management of all data and system resources. Further, ASG employs the module concept throughout the SAFE infrastructure (fig. 1). The advantage of this concept is that, "it allows the architecture to address the security relation between the various functional blocks of the network" and "it permits designers to evaluate and implement security on a module by module basis, instead of attempting

[1] Sean Covery and Bernie Trundel, "Cisco SAFE: A Security Blueprint for Enterprise Networks," 2000 Cisco Systems, Inc., 08 Dec 2000. http://cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm. 1.
[2] Covery/Trundel 1.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the complete architecture in a single phase."[3] Specific Modules include: Management, Server, Corporate User and Internet modules.
As noted in fig. 1 traffic entering CHQ is routed through 3 distinct traffic paths; VPN/RAS, Email, and Web into CHQ. Each path employs a unique mixture of hardware and software tailored to meet functionality and security requirements. Below is a listing of hardware and software supporting CHQ, Hangar Complex and Mobile users.

Servers/Workstations: Dell	**Operating System Software:**
PDC	MS BackOffice Suite
BDC	MS BackOffice Suite
Web	MS Internet Information Server 5.5
DNS	LYNX
Email	MS Exchange 5.5 SP4
File	NT FileShares
SSL	Netscape Iplanet
FTP	NT FTP
Access	Oracle
OTP	Oracle
Workstation/Host:	
Dell Desktops	NT 4.0
Remote Workstations:	
Dell Desktops	NT 4.0, Cisco VPN Client Software
Switches/Routers/IDS:	
Cisco L2/L3 Switches	Cisco IOS
Cisco Router	Cisco IOS
Cisco VPN router	Cisco IOS
Cisco IDS	Cisco IOS
Firewalls/Dell Servers:	
	Raptor (Web)
	Gauntlet (Email)
Dell workstation/notebook	ZoneAlarm Pro 2.0

1.1.2 Hangar Complex

The hangar complex is a single building divided into 4 distinct divisions. As identified above each division is autonomous and operates as a single entity including administrative, operational, maintenance, safety and training departments. As seen in fig. 1 each division maintains a BDC, File, and Email server and is linked to CHQ via VLANS through a Cisco Switch. Though each division has distinct mission requirements there is commonality between each and information sharing is a efficiency ASG

[3] Covery/Trundel 1.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

mandates. This information share is accomplished through employment of a corporate intranet.

1.2 Business Operations

ASG is a services based corporation centered around each of it's 4 divisions; Heavy Lift – construction, logging, salvage; Executive Transport – corporations, entertainment industry, personal charters, city and state government; EMS – local and state hospitals; Department of Interior (search and rescue at national parks); Recreational Transport – ski industry, sight seeing, fishing. Corporate functional/ informational support to these marketplaces varies and is subdivided into 4 sub-areas; Administrative Support, Marketing/Advertising, Satellite Sites/Remote Users, Partnerships. Informational Infrastructure required to support these marketplaces is as follows:

1.2.1 Administrative Support

Administrative support is performed at both the corporate and divisional level. Corporate hosts the ASG Primary Domain Controller (PDC), Backup Domain Controller (BDC), intranet site, main file servers, data base servers, email servers, management systems, web cashing services and public website. Divisional administrative support is organic providing division specific email, file, and data base services. Divisional data and files are replicated to corporate on a daily basis. Backup Domain controllers are maintained within each division for stability, security, and redundancy.

1.2.2 Marketing/Advertising

Primary marketing and advertising is performed via ASG's public accessible website. As the primary marketing tool it is essential that customers and/or prospective customers have unimpeded access on a 24/7 pull basis.

1.2.3 Satellite Sites/Remote Users

Satellite sites are employed on an as needed basis, are temporary in duration and are located at remote airport facilities where connectivity is varied (broadband, modem, and Ethernet). Satellite/Remote users require secure inbound and outbound access to solicit maintenance, operational, and administrative databases at both corporate and divisional levels and email services on a 24/7 basis. Connectivity at these sites is accomplished through use of hardware (desktops/notebooks) running VPN client software.

1.2.4 AEG Corporate

AEG Corporate is ASG's prime aviation maintenance and supply contractor and maintains a branch office within the ASG hangar complex. Like ASG satellite sites and remote users, AEG users require inbound and outbound access to select databases and email services. However unlike

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

AEG satellite/remote users the level of access to ASG resources by AEG is curtailed.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.0 ASG Security Policy

Security at ASG (physical, informational etc.) is paramount and is exercised at all levels, from corporate management to mail room employees. It is recognized that failure to employ adequate physical resources and employ a robust plan of execution could lead to, "Loss of company assets, Loss of revenue/market share, Loss of intellectual property, Loss of privacy and damage to reputation."[4] In effort to combat this ASG has identified 5 areas of concern. These include: Routers and ASG Information Security; Security and Protection of ASG's Satellite Site/Mobile Users; Security and Protection of ASG's Publicly Accessible Web Site; Passwords; Rapid Detection of Intrusions.

2.1 Areas of Risk

2.1.1 Routers and ASG Information System Security

The perimeter (outer boundary) is the first and most important line of defense from the public side in and the last line of defense for traffic leaving the network. ASG employs a "Defense In Dept"[5] view of network security and earmarks the perimeter as paramount to enterprise defense. Key elements of this outer boundary are routers, physical barriers (fences, buildings, doors, etc.) and firewalls. As per figure1, ASG takes consorted efforts to protect production systems from cyber threats. Routers are the first and last enterprise guards tasked with filtering and routing traffic destine to and from ASG. Physical barriers protect ASG assets (hardware, software etc.,). Firewalls though a primary defense asset are not discussed in this forum.

2.1.1.1 Threats/risks[6]

- Unauthorized access to the enterprise from outside by unauthorized parties (hackers, crackers, vandals etc.)
- Threats from internal users including disgruntled employees, corporate spies, visiting guests, and inadvertent bumbling of users and/or administrators whose actions perpetrate/allow unauthorized access into the enterprise.

2.1.1.2 Consequences if exploited[7]

- Loss of company assets (Damage to computers, loss data, service disruptions etc.)
- Loss of revenue/market share (Competing rotary wing service providers)
- Loss of intellectual property (Procedural doctrine etc.)
- Loss of privacy (Customer information, employee information, financial information)
- Damage to reputation. (Loss in trust)

[4] Stephen Fried, "9.1 SANS Security Leadership," Part 1. 1-18.
[5] Fried 1-25.
[6] Covery/Trundel 36.
[7] Fried 18.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.1.1.3 Mitigation of Threats/Risks

- Access Control (Physical/Enterprise):
  - Physical security – Router security is impossible without physical security. "If your Internet Access Router is physically accessible, an attack can gain User EXEC mode access by logging on locally through the console or AUX port."[8] At ASG there are 3 layers of physical security. Layer 1 - Primary access points (lobby etc) to buildings are controlled by armed security guards on a 24/7 basis. Guards check entrant credentials, issue/recover visitor badges and monitor alarms. Emergency exits, utility exits, and windows are alarmed to alert guards of breached access points. Closed circuit cameras (CCTV) are positioned at all ingress and egress points. Layer 2 – Internal sensitive or critical areas (computer rooms, wiring closets, utility spaces, operations spaces) are protected by electronic key systems. Access into these spaces is via encoded cards capable of limiting access to specified times, has the capability to lockout specified cards and log all entrance and exits. CCTV like Layer 1 protection is utilized. Layer 3 – Least privilege is exercised throughout ASG. This principle limits damage that can result from accident, error or unauthorized access.[9]
  - Enterprise – The enterprise was designed with security at the forefront. ASG employs a Single Point of entry performing surveillance on traffic entering and exiting the enterprise. Unauthorized Access is mitigated through filtering at the ISP (prior to reaching the enterprise), at the Enterprise Outer Router and at all ASG firewalls.

2.1.2 Security/Protection of Satellite Site (SS)/Mobile Users (MU)

ASG road warriors (Satellite sites and mobile users) have the same requirements while on the road as when in the office.[10] Within the office they are protected by perimeter security defenses however while on the road the security of the enclave is void. Specifically, "The remote user is invisible. This means that any formal or informal security measures operating at the work site will not be effective."[11] Secondly, Information is transmitted over a possibly insecure line where interception of data can null and void the basic properties of information security; confidentiality, integrity, and availability.

---

[8] Richard Langley, "Securing Your Internet Access Router," 23 Jan 2001, 08 Dec 2001. http://www.sans.org/infosecFAC/firewall/router.htm. 2.

[9] S. Rao Vallabhaneni, CISSP Examination Textbooks Vol. 1: Theory (Illinois: SRV Professional Publications) 383-393.

[10] Jason Halpern, "Safe VPN IPSec Virtual Private Networks In Depth," 2001 Cisco Systems, Inc., 10 Dec 2001. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm. 13.

[11] Cimarron Boozer, "Remote Access Security," 17 Dec 2001. http://nsi.org/Library/Compusec/sec-wp.htm . 3

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.1.2.1 Threats/Risks[12]

- Access Control (Unauthorized access to the enterprise from outside by unauthorized parties (hackers, crackers, vandals etc.)
- Interception of and alteration of data to include capture of user logins and passwords.
- Malicious Logic infections

2.1.2.2 Consequences if exploited[13]

- Loss of company assets (Damage to computers, loss data, service disruptions etc.)
- Loss of revenue/market share (Competing rotary wing service providers)
- Loss of intellectual property (Procedural doctrine etc.)
- Loss of privacy (Customer information, employee information, financial information)
- Damage to reputation. (Loss in trust)

2.1.2.3 Mitigation of Threats/Risks

- Access Control User Authentication
  - Protect host (notebook/desktop) from theft. Immediately notify ASG of stolen systems in order to prevent same from being used to penetrate the enterprise
  - Password protect Netbios, and password protected screen saver utilizing dissimilar passwords. Password protecting the Netbios will prevent stolen systems from accessing the network.
  - Password protect workstations and portable systems with direct access to the network :
  - Power/Boot password (Password to access the client/host)
  - Operating system password (username/password for local client/host access to the operating system)
  - Network Operating System password (NT domain authentication with single sign for network resource access)
  - Untrusted clients accessing resources (using telnet, etc.,) within ASG
  - Utilize one-time-passwords (OTP) for logins

- Interception and alteration of data:
  - Encryption of Data (protecting communications from eavesdroppers). ASG utilizes a corporate VPN (128 bit or triple DES) for all satellite and remote user connections.

[12] Covery /Trundel 36.
[13] Fried 18.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.1.3 Security/Protection of Publicly Accessible Web site

ASG, as many successful corporations markets it's services on a publicly accessible website. Fifty-eight percent of ASG's annual revenue is realized through effective advertising on this medium. Protection of this valued marketing forum is paramount.

2.1.3.1 Threats/Risks

- Corruption and/or defacement of Web site
- Malicious Logic infections (Propagation of malicious logic to other platforms, e.g. Code Red)

2.1.3.2 Consequences if exploited[14]

- Loss of revenue/market share (Competing rotary wing service providers)
- Loss of privacy (Customer information, employee information, financial information)
- Damage to reputation. (Loss in trust)

2.1.3.3 Mitigation of Threats/Risks[15]

- Corruption and/or Defacement:
  - Utilize Encrypted Management tools (SSH, SSL, SFTP) to manage the Website.
  - Author webpages with trusted scripts and use secure protocols.
  - Malicious Logic Infections
  - Keep Service Packs, Patches and virus definitions updated
  - Utilize Full web-access logging
  - Utilize FTP drop for web update from ASG web developers (FrontPage hooks risk is high for intrusion)
  - Host all web pages on separate physical disk from operating system disk
  - Require all scripts be reviewed by ASG webmaster before posting to ensure no misbehave code is allowing access to operating system binaries
  - Require scripts directory to be properly permissioned.

2.1.4 Passwords

At ASG, "It All About The Data." Security (physical, technical, administrative etc.) is aimed at protecting corporate information systems for the sole purpose of protecting the data (programs, files, databases and other information). The integral element that brings all elements of security together is passwords. Passwords are the keys to ASG's network and can fall into the wrong hands just

[14] Fried 18.
[15] Eric Bowden, "Securing Your Website, It pays to Be Paranoid." 17 Dec 2001. http://www.bugnet.com/analysis/0108/ftwebsecure.html.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

as Physical keys can.[16]

2.1.4.1 Threats/risks[17]

- Loss of data confidentiality (disclosure to unauthorized parties or processes)
- Loss of data integrity (loss of accuracy and completeness through deliberate or accidental acts)
- Loss of data availability (loss of timely and reliable access by authorized individuals)

2.1.4.2 Consequences if exploited[18]

- Loss of revenue/market share (Competing rotary wing service providers)
- Loss of intellectual property (Procedural doctrine etc.)
- Loss of privacy (Customer information, employee information, financial information etc.)
- Damage to reputation. (Loss in trust)

2.1.4.3 Mitigation of Threats/risks:

- Loss of Data confidentiality
  - Effective selection, protection and management of passwords
  - Encrypt files/data
- Loss of Data integrity
  - Effective selection, protection and management of passwords
  - Encrypt files/data
- Loss of Data availability
  - Effective selection, protection and management of passwords
  - Ensure real time rollback logging
  - Backup archived (Incremental/differential/full) providing minimized loss of data.

2.1.5 Rapid Detection of Intrusions

The prime purpose of ASG's intrusion detection system (IDS) is to monitor traffic on both host and network components, compare anomalies against known attack signatures, and to notify key personnel of impending attacks on the information system infrastructure. Though the ASG's information system department prides themselves on efficient and thorough configuration of firewalls and routers the possibility of miss-configuration is very real. As indicated above, ASG depends on the concepts of layered defense and I DS is an integral part of this concept.

2.1.5.1 Threats/Risks

- Undetected network/host attacks
- Inadvertent access and release of proprietary ASG information

[16] Randy Smith, "Protect Your Passwords, Simple steps to restrict intruders' access to your accounts," 20 Dec 2001. http://www.win2000mag.com/Articles/Print.cfm?ArticleID=3844. 1
[17] Vallabhaneni 6.
[18] Fried 18.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Stealing of intellectual material

2.1.5.2 Consequences if exploited[19]

- Loss of revenue/market share (Competing rotary wing service providers)
- Loss of intellectual property (Procedural doctrine etc.)
- Loss of privacy (Customer information, employee information, financial information)
- Damage to reputation. (Loss in trust)

2.1.5.3 Mitigation of Threats/Risks

- Installation of Hosts IDS (HIDS) and Network IDS (IDS) throughout the ASG enterprise. When the IDS sensors detects something that it considers an attack it can take action to prevent the attack and/or notify management.[20]
- Enable automatic baseline thresholds/alerts activating ASG InfoSec personnel beepers and/or call back function for alert purposes.

2.2 ASG Remote Access Policy

2.2.1 Security/protection of Satellite Site (SS)/Mobile Users (MU) Policy

2.2.1.1 Purpose[21]

The purpose of this policy is to define standards for connecting to GIAC Enterprises Air Services Group (ASG) network from any host. These standards are designed to minimize the potential exposure to ASG from damages that may result from unauthorized use of ASG resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to public image, damage to critical ASG internal systems.

2.2.1.2 Scope[22]

This policy applies to all ASG employees, contractors, vendors and agents with an ASG owned or personally-owned computer or workstation used to connect to the ASG network. This policy applies to remote access connections used to do work on behalf of ASG, including reading or sending email and viewing Intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, VPN, SSH, SSL, cable modems, DSL modems, etc.

---

[19] Fried 18.
[20] Covery/Trundel 7
[21] "The SANS Security Policy Project: Remote Access Policy," 18 Dec 2001. http://www.sans.org/newlook/resources/policies/policies.htm
[22] "The SANS Security Policy Project: Remote Access Policy"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.2.1.3 Policy Statement[23]

- General:
  - It is the responsibility of ASG employees, contractors, vendors and agents with remote access privileges to ASG's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to ASG.
  - General access to the Internet for recreational use by immediate household members through the ASG network on personal computers is permitted for employees that have flat-rate services. The ASG employee is responsible to ensure the family member does not violate any ASG policies, does not perform illegal activities, and does not use the access for outside business interests. The ASG employee bears responsibility for the consequences should access be misused.
  - Review the Acceptable Encryption Policy, Virtual Private Network (VPN) Policy, Wireless Communication Policy, and Acceptable Use Policy for details of protecting information prior to accessing the corporate network via remote access methods, and acceptable use of ASG's network.
  - For additional information regarding ASG's remote access connection options, including how to order or disconnect services, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

2.2.1.4 Responsibility[24]

- ASG InfoSec Office:
  - Review and revision of this policy document on a continued basis
  - Configuration management of all hosts connected to ASG network.
  - Approval of all non standard host configurations on a case by case basis.
  - Risk analysis of remote system infrastructure (hardware/software).
  - Training to all remote system users on a bi-annual basis.
  - Updating, patching and installation of fixes to all remote system software (operating system, VPN host software, etc.).
  - Real time auditing/logging of all remote sessions.
  - Contingency planning to include incident response and post-incident investigations.
- ASG Employees:
  - Adhere to ASG guiding policies and user agreements.
  - Safeguard ASG assets (hardware, software, data, etc).
  - Notify ASG Information Systems office immediately of all incidents, to include theft of assets, compromise of systems, malicious logic infestations/attacks etc.

[23] "The SANS Security Policy Project: Remote Access Policy"
[24] "The SANS Security Policy Project: Remote Access Policy"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Will not circumvent or attempt to circumvent ASG security measures (software/hardware).
- Adhere to specified action items as listed below.

- Third Parties Connected to ASG's network (contractors, vendors and agents):
  - Adhere to ASG guiding policies and user agreements.
  - Safeguard ASG assets (hardware, software, data, etc).
  - Notify ASG Information Systems office immediately of all incidents, to include theft of assets, compromise of systems, malicious logic infestations/attacks etc.
  - Will not circumvent or attempt to circumvent ASG security measures (software/hardware).
  - Adhere to specified action items as listed below.
  - Will limit access to authorized ASG files and data approved by ASG management.

2.2.1.5 Action[25]

- General:
  - Secure remote access must be strictly controlled on a continuous basis. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass phrase see the Password Policy. (Always)
  - At no time should any ASG employee provide their login or email password to anyone, not even family members.
  - ASG employees and contractors with remote access privileges must ensure that their ASG owned or personal computer or workstation, that is remotely connected to ASG's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user. (Always)
  - ASG employees and contractors with remote access privileges to ASG's corporate network must never use non-ASG email accounts (i.e., Hotmail, Yahoo, AOL) or other external resources to conduct ASG business, thereby ensuring that official business in never confused with personal business. (Never)
  - Routers for dedicated ISDN lines configured for access to the ASG network must meet minimum authentication requirements of CHAP at all times. (Always)
  - Reconfiguration of a home user's equipment for the purpose of split-tunnel or dual homing is not permitted at any time. (Never)
  - Non-standard hardware configurations must be approved by the ASG information systems office and be approved security configurations to access to hardware prior to applying non-standard configurations. (Always)

[25] "The SANS Security Policy Project: Remote Access Policy"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- All hosts that are connected to ASG internal networks via remote access technologies must use the most up-to-date anti-virus software (Norton Anti-virus Professional Edition), this includes personal computers. Live Updates are required prior to connecting to the ASG network. Third party connections must comply with requirements as stated in the Third Party Agreement. (Always)
- Personal equipment that is used to connect to ASG's networks must meet the requirements of ASG owned equipment for remote access before connection to the network. (Always)
- Organizations of individuals who wish to implement non-standard Remote Access Solutions to the ASG production network must obtain prior approval from the ASG InfoSec office before implementation. (Always)

2.2.2 Password Policy

2.2.2.1 Purpose[26]

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of ASG's entire corporate network. As such, all ASG employees (including contractors and vendors) with access to ASG systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.2.2.2 Scope[27]

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ASG facility, has access to the ASG network, or stores any non-public ASG information.

2.2.2.3 Policy Statement[28]

- General:
  - All system-level passwords (e.g., root, enable, NT admin, application administration accounts etc.) must be changed on at least a quarterly basis.
  - All production system-level passwords must be part of the InfoSec administered global password management database.
  - All user-level passwords (e.g. email, web, desktop computer, etc.) must change at least quarterly.

[26] "The SANS Security Policy Project: Password Policy," 18 Dec 2001. http://www.sans.org/newlook/resources/policies/policies.htm
[27] "The SANS Security Policy Project: Password Policy"
[28] "The SANS Security Policy Project: Password Policy"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- User accounts that have system-level privileges granted through group membership or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All users-level and system-level passwords must conform to the guidelines.

- Guidelines:
  - Password Construction. Passwords are used for various purposes at ASG. Some of the more common uses include; user level accounts, web accounts, email accounts, screen saver protection, voicemail passwords, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.
  - Poor, weak passwords:
    - The password contains less than eight characters.
    - The password is a word found in a dictionary (English or foreign).
    - The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "ASG", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers
    - Word or number patterns like aaabbb, qwerty, zyxqvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
  - Strong passwords:
    - Contain both upper and lower case characters (e.g., a-z, A-Z)
    - Have digits and punctuation characters as well as letters (e.g.,0-9, !@#$%^&*()_+)= etc.)
    - Are at least eight alphanumeric characters long.
    - Are not a word in any language, slang, dialect, jargon, etc.
    - Are not based on personal information, names of family, etc.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Note: Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

2.2.2.4 Responsibility

- ASG InfoSec Office:
  - Review and revision of this policy document on a continued basis.
  - Provide Training to system users and system administrators /managers on a bi-annual basis.
  - Maintain OTP systems for remote access hosts
  - Contingency planning to include incident response and post incident investigations.

- ASG Employee/contractors/agents:
  - Adhere to password protection standards as outlined in "Action" section below.
  - Notify ASG Information Systems office immediately of lost or compromised passwords.

2.2.2.5 Action[29]

- General:
  - Change all system-level passwords e.g., root, enable, NT administration, application administration accounts etc. (Quarterly)
  - Change user-level passwords e.g. email, web, desktop computer, etc. (Quarterly)
  - Comply with Password Protection Standards: (Always)
    - Do not use the same password for ASG accounts as for other non-ASG access
    - Where possible, don't use the same password for various ASG access needs.
    - Don't share ASG passwords with anyone, including administrative assistants or secretaries.
    - Treat all passwords as sensitive, confidential ASG information.
    - Don't reveal a password over the phone to anyone.
    - Don't reveal a password in an email message.
    - Don't reveal a password to the boss.
    - Don't talk about a password in front of others.
    - Don't hint at the format of a password (e.g., "my family name").
    - Don't reveal a password on questionnaires or security forums.
    - Don't share a password with family members.
    - Don't reveal a password to co-workers while on vacation.

[29] "The SANS Security Policy Project: Password Policy"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Don't write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system (including Palm Pilots) without encryption.

- If someone demands a password, refer them to this document or have them call the InfoSec office. (As required)
- If an account or password is suspected to have been compromised, disable the account and report the incident to InfoSec. (Immediately)
- Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it. (Periodically)
- Access to the ASG network via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase. (Always)
- Accounts will systematically lock upon 3 failed password attempts. Face to face account enabling (account unlock) is mandatory except for shared-secret or pass-phrase verification. (Always)

2.2.3 Router Security Policy

2.2.3.1 Purpose[30]

The purpose of this policy is to define minimal security configuration for all router connections to a production network or used in a production capacity at or on the behalf of ASG.

2.2.3.2 Scope[31]

This policy applies not only to the ASG Enterprise Outer Router but at various levels to all routers connected to ASG production networks. Routers within internal secure (R&D, DEVELOPMENTAL, etc) labs are not addressed nor fall under the umbrella of this document.

2.2.3.3 Policy Statement

Every router must be protected by and/or meet the following configuration standards:

- General:[32]
  - All maintenance must be done while logged on locally or Telnet accessed from hosts located within the InfoSec office.
  - All maintenance services capable of being accessible/employed from outside the enterprise shall be disabled.
  - Stop RIP (Router Interface Protocol) and OSPF (Open Shortest Path First) protocol on the Internet by inbound and outbound.

---

[30] "The SANS Security Policy Project: Router Security Policy," 18 Dec 2001. http://www.sans.org/newlook/resources/policies/policies.htm

[31] "The SANS Security Policy Project: Router Security Policy"

[32] "Improving Security on Cisco Routers," Cisco Systems, Inc., 19 Dec 2001. http://www.cisco.com/warp/public/707/21.html.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Disable CDP (Cisco Discovery Protocol) on all interfaces.
- Disable inbound Telnet from the Internet.
- Disable Telnet listener completely.

- General 2:[33]
  - No Local user accounts are to be configured on routers. Routers must use TACACS+ for all user authentication.
  - The router enable password will be maintained in a secure encrypted form. Router enable password will be set to the current production router password from the router's support organization.
  - The following shall be disallowed:
    - IP direct broadcasts
    - Incoming packets at the router sourced with invalid addresses e.g., RFC 1918
    - TCP small services
    - UDP small services
    - All source routing
    - All web services running on the router
    - DNS lookups
  - Corporate standardized (non-default, ie., public) SNMP community strings are mandatory.
  - Access rules are to be added/revised/eliminated as business needs arise.
  - Router's must be included in the corporate enterprise management system with a designated point(s) of contact.
  - Each router must have the following banner posted in clear view; "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities (maintenance, programming etc.) shall be logged. Violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device.

2.2.3.4 Responsibility

- ASG InfoSec Office:
  - Review and revision of this policy document on a continued basis
  - Contingency planning, to include incident response and post incident investigations.
  - Exercise a 2 layered review (security administrator/manager of router configuration and ACL's.
  - Maintain real-time access list for authorized network administrators.
  - Chair a quarterly review board for authorized services (ports and protocols allowed by ACL). Members will include InfoSec Manager, IS Administration manager, AEC representative, divisional representatives.

[33] "The SANS Security Policy Project: Router Security Policy"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.2.3.5 Action [34]

- Password Management
  - Maintain passwords on TACACS+ or RADIUS authentication server. (Always)
  - Protect locally configured passwords for privileged access according to ASG Password Policy document. (Always)
  - Set "enable secret command." (At initial configuration)
- Controlling Interactive Access
  - Configure router to require users on local asynchronous at console terminals to log in before using the system. (At initial configuration)
  - Restrict access to define IP numbers or workstations. (Always)
- Commonly Configured Management Services
  - Maintain router configurations on FTP server that has limited access. (Always)
  - Disabled SNMP on bastion routers. Utilized on trusted side only. (Always)
- Warning Banner
  - Update banner (As Necessary)
- Logging
  - Enable AAA logging (Always)
  - Review logs (Daily)

© SANS Institute 2000 - 2002, Author retains full rights

[34] "Improving Security on Cisco Routers" 20.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.0 Password Procedures

3.1 Setting Passwords on Servers

3.1.1 Assign Boot/Power Password

- How:
  - Power up server
  - Select F2. Scroll to Pg. 2
  - Set system to "Enable". Put in password per ASG password standards. Policy is assigned per registry entry. Mandatory requirements are automated including a 9 character string with at least 3 of the following; Upper case letters, lower case letters, special characters and numbers. The system will not accept invalid passwords
  - Set Status to "Locked"
  - Exit and reboot.
- Why: Protect all Server (s) from unauthorized access.
- Who: ASG InfoSec Personnel
- When: During server setup or reload

3.1.2 Changing NT 4.0 Operating System Login Password

- How :
  - Power up server
  - Type in Boot Password
  - Type User Name, Password and Domain
  - Select User Manager
  - Select Server
  - Select Policies
  - Select Account Policy:
  - Max Password – Expires 90 days
  - Min Password – Expires 0 days
  - Minimum Password Length – 9 Characters
  - Password Uniqueness – Remember 10 Passwords
  - Account Lockout – 3 bad logon attempts
  - Reset counter after – 30 minutes
  - Lockout duration - Forever
  - Exit and reboot
- Why: Protect all Server (s) from unauthorized access and establish password account policy.
- Who: ASG InfoSec Personnel
- When: During server setup or reload

3.2 Setting Passwords on Desktops/Mobile hosts (DT/MH):

3.2.1 Assign Boot/Power-up Password

- How:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Power up DT/MH
- Select F2. Scroll to Pg. 2
- Set system to "Enable." Put in password per ASG password standards. Policy is assigned per registry entry. Mandatory requirements are automated including a 9 character string with at least 3 of the following; Upper case letters, lower case letters, special characters and numbers. The system will not accept invalid passwords
- Set Status to "Locked"
- Exit and reboot.

- Why: Protect all DT/MH (s) from unauthorized access.
- Who: ASG InfoSec Personnel
- When: During DT/MH setup or reload

3.2.2 Setting Operating System Password for Local Log-On

- How:
  - Power up DT/MH
  - Enter User Name, Password
  - Select User Manager
  - Select Server
  - Select Policies
  - Select Account Policy:
  - Max Password – Expires 90 days
  - Min Password – Expires 0 days
  - Minimum Password Length – 9 Characters
  - Password Uniqueness – Remember 10 Passwords
  - Account Lockout – 3 bad logon attempts
  - Reset counter after – 30 minutes
  - Lockout duration - Forever
  - Exit and reboot

- Why: Protect all DT/MH (s) from unauthorized access.
- Who: ASG InfoSec Personnel
- When: During DT/MH setup or reload

3.3 Managing User Passwords

3.3.1 Making New User Account Passwords

- How:
  - Authenticate Identity:
  - New user must be present with photo I.D. Must be escorted by HR representative
  - View Training Video on ASG Password Policy
  - Read and sign ASG Password Policy. New user will select a "shared secret"(e.g., mothers maiden name, best friends mothers

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

cats name) or will be assigned a pass-phrase. These will assist in authenticating the user if passwords are forgotten.
  - Assign Interim User Password (s) for network and identified host accessing the network. Interim passwords will be selected via a password generator. Department Head is responsible for identifying services/systems new employee is authorized to access under user password.
  - New user is required to change password at first login to authorized network systems.

- Why: Protect ASG by educating/training new employees as to proper password protocol when receiving new accounts.
- Who: InfoSec personnel and new user
- When: Immediately upon hiring of new personnel

3.3.2 Forgotten Passwords

- How:
  - Authenticate Identity
  - User must report in person with valid photo ID card to InfoSec office or
  - Remotely with "shared secrets." This prevents social engineering techniques commonly used by hackers
  - If properly Identified account is unlocked, new password assigned (password generator)
  - User is prompted to change password at next login using ASG password policies.
  - Repeated failed attempts to authenticate will result in lock out of user account prompting in person authentication.
- Why: Safeguard system from social engineering attempts
- Who: User
- When: Prior to accessing the enterprise

3.3.3 Changing Passwords on User Accounts

- How:
  - Force password changes from server throughout selected areas of ASG due to compromised password (s)
  - At next login user will be required to change password
- Why: Compromised passwords (shoulder surfing, inadvertent disclosure, system intrusion)
- Who: Lockout by InfoSec. Password changes throughout enterprise as per the severity of compromise/intrusion.
- When: Immediately

3.3.4 Mitigate Password Violation (s)

- How:
  - Lockout accounts of violator (s) at server console

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

    - Counsel violators.
    - View Training Video on ASG Password Policy if this is a repeat offense.
    - Reread and sign ASG Password Policy.
    - Change password at first login to authorized network systems.
- Why: Prevent compromise of ASG data, software, systems etc.
- Who: Counseled by InfoSec.
- When: Immediately

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC AIR SERVICES
Group

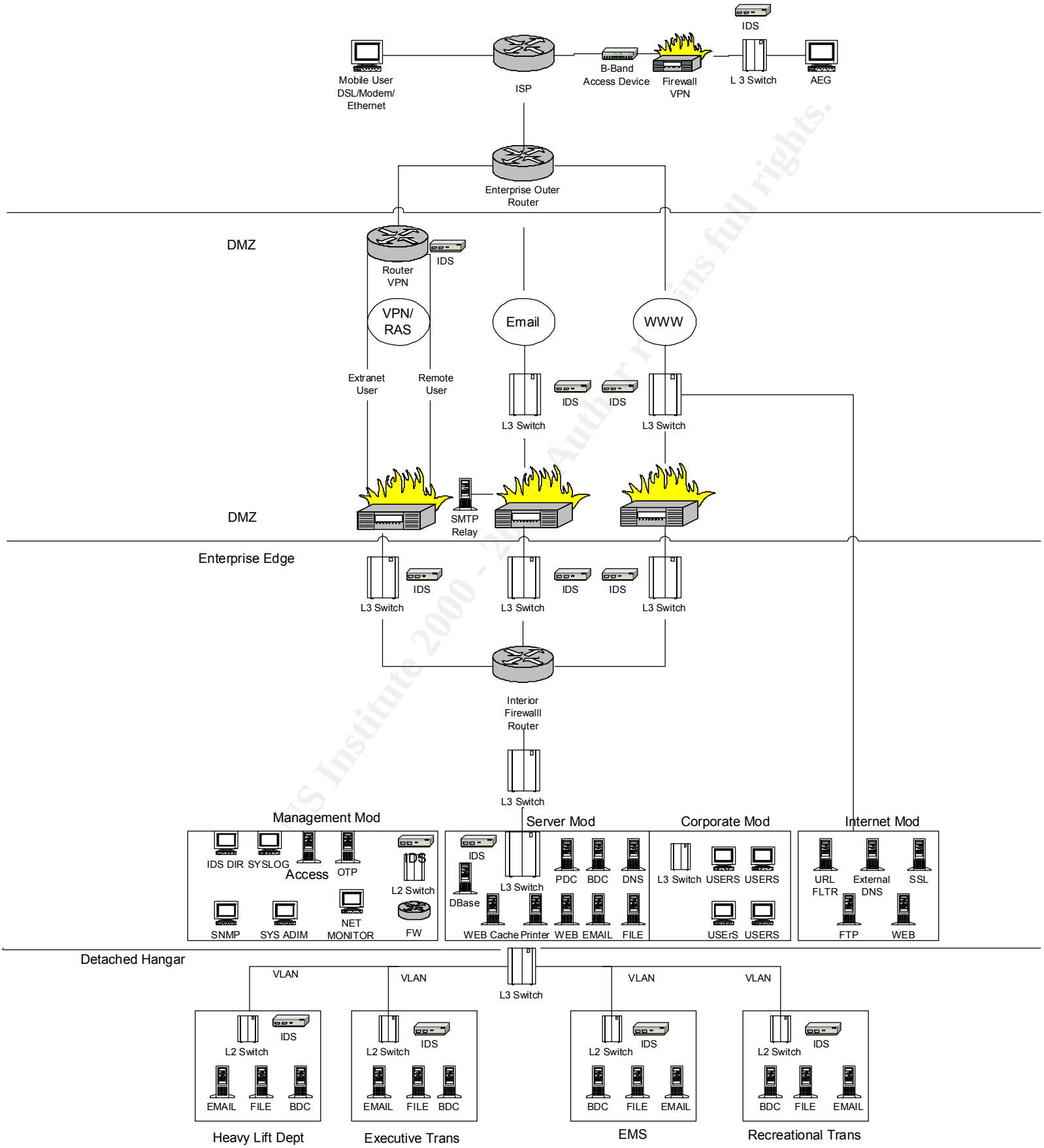

Figure 1.
As part of GIAC practical repository.

© SANS Institute 2000 - 2002
Author retains full rights.

References

1. Sean Covery and Bernie Trundel, "Cisco SAFE: A Security Blueprint for EnterpriseNetworks," 2000 Cisco Systems, Inc., 08 Dec 2000. http://cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm.

2. Stephen Fried, "9.1 SANS Security Leadership," Part 1

3. Richard Langley, "Securing Your Internet Access Router," 23 Jan 2001, 08 Dec 2001. http://www.sans.org/infosecFAC/firewall/router.htm.

4. S. Rao Vallabhaneni, CISSP Examination Textbooks Vol. 1: Theory (Illinois: SRV Professional Publications)

5. Jason Halpern, "Safe VPN IPSec Virtual Private Networks In Depth," 2001 Cisco Systems, Inc., 10 Dec 2001. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm.

6. Cimarron Boozer, "Remote Access Security," 17 Dec 2001. http://nsi.org/Library/Compusec/sec-wp.htm

7. Eric Bowden, "Securing Your Website, It pays to Be Paranoid." 17 Dec 2001. http://www.bugnet.com/analysis/0108/ftwebsecure.html

8. Randy Smith, "Protect Your Passwords, Simple steps to restrict intruders' access to your accounts," 20 Dec 2001. http://www.win2000mag.com/Articles/Print.cfm?ArticleID=3844

9. "The SANS Security Policy Project" 18 Dec 2001. http://www.sans.org/newlook/resources/policies/policies.htm

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.