

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.

IDS Load Balancer Security Audit: An Administrator's Perspective

SANS GIAC Systems and Network Auditor
Version 2.1, Option 1

Michael Hotaling
December 27, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Executive Summary....4
Part I: Preparing for the Audit....5
Background....5
Objective....6
Scope....6
Role....6
Risk Evaluation....9
Assets....9
Threats....9
Impacts....9
Risk Calculation....10
State of Practice....13
Part II: Develop the Audit....16
Information Gathering....16
The Audit Checklist....17
A. Preventing Unauthorized Access....18
A1 Segregate Management Traffic From Corporate Network....18
A2 Review Log Server Security....20
A3 Do Not Specify a Default Route....23
A4 Encrypt Management Sessions....23
A5 Require Authentication for Access....25
A6 Change Default Passwords....26
A7 Restrict sources of administrative sessions....27
A8 Idle sessions should time out within five minutes....28
A9 Enforce Minimum Password Length....29
A10 Verify that commands cannot be received on Listen / Monitor ports....30
A11 Ensure there are no unneeded listening ports....31
B. Preventing Unauthorized or Unintentional Changes....32
B1 Use accounts with minimal privilege for the task at hand....32
B2 Restrict simultaneous administrative sessions....33
B3 Each Balancer manager must use unique credentials....36
B4 Successful and failed login attempts should be logged....37
B5 Failed logins should not reveal information about valid accounts....38
B6 A warning banner should be displayed prior to any type of CLI access…38
B7 Log system and security events to a separate log server....39
B8 Synchronize time to reference clock....40
B9 Keep Time in UTC....42
C. Policy, Procedure, and Other Issues....42
C1 Implement a change control procedure....42
C2 Review backup, restore, and continuity plans....43
C3 Logs should be reviewed in a reasonable time....43

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C4 Ensure documentation is complete, current, and correct.....44
C5 Ensure system is current on patches and updates.....44
C6 Install and verify the operation of a redundant power supply.....45
C7 Review Environmental Conditions.....46
C8 Review Physical Security.....47
Part III: Conduct the Audit.....49
Residual Risk.....64
Auditability.....65
Part IV: Report Findings.....66

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Executive Summary

The following report details the security assessment of a load balancer to be used in a Network Intrusion Detection deployment for GIAC Enterprises. It includes analysis of risks to the system, followed by development of an audit checklist derived from company IT policies and industry best practices. The audit was performed and the results were used to draw conclusions about the security and residual risk to the system, which is presented in the final section.

The audit was conducted on a preproduction system by GIAC technical staff.

Please note that GIAC Enterprises is a fictitious company. Identifying information used in this report has been changed.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Part I: Preparing for the Audit

Background

GIAC Enterprises is a large North American transportation and logistics company specializing in just-in-time delivery of critical freight. The Internet is central to company operations, with a significant customer reliance on Web-based applications for, among other things, scheduling pickup and delivery, tracking shipment status, and account management. With this significant role of Internet services, information security is a primary concern. Multiple layers of network defenses have been installed to protect company assets, including firewalls, intrusion detection systems (IDS), virtual private networks (VPN), and antivirus software.

IDS works by analyzing system or network activity for indications of suspicious or hostile activity. Host IDS (HIDS) may review system logs, intercept operating system calls, and verify the integrity of files to protect an individual computer. Network IDS (NIDS) monitors traffic on a network, using some criteria to determine what is suspicious. Some use signatures of known attacks to generate alerts. Others monitor for anomalies, deviations from standards or a baseline for a particular network. Still others use statistical or flow models to identify events of interest. Each type of system has strengths and weaknesses.

In an effort to provide improved NIDS capabilities, GIAC is implementing a load balancing switch tailored for network monitoring installations. The product selected is a Top Layer[1] IDS Balancer 3510. It provides functionality similar to other "Layer 7" or application load balancers, with additional features specific to IDS implementations. The GIAC IDS team has tested the Balancer for functionality and performance, and management has requested a security review before it is put into production use.

Manufacturer	Top Layer
Model	IDS Balancer AS3510
Type	Network device
Software version	V2.20.007
Boot ROM version	V3.01
Options	Redundant AC power supply

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Objective

The purpose of this assessment is to validate the secure configuration of the Balancer and that its addition will not significantly increase risk to the monitoring infrastructure. The existing IDS components have all undergone extensive security reviews, both prior to installation and periodically during their operation.

Scope

The audit included only the security of the Balancer itself. It did not include IDS sensors, management and reporting systems, or the infrastructure required to support the deployment including Shomiti Ethernet taps, a Cisco Catalyst 3524 switch, and a Sun Solaris log server. Secure configuration and auditing have been extensively covered for both Solaris and Cisco IOS, including CIS benchmarks[2] and SANS Step-by-Step[3] and Gold Standard[4] documents. It did not cover the performance, usability, or other aspects of the IDS Balancer as those were evaluated separately by the IDS team.

The assessment was conducted by a network engineer (from outside the IDS team) and a security engineer from the IDS team. Three days were set aside for the planning and execution, which took place during normal working hours in a lab environment.

The depth of the assessment was restricted and did not cover, for example, application level security of the Web / Java administration interface or cryptanalysis of the implementation of SSL and SSH for encryption.

Role

The role of IDS in GIAC's network is to reduce risk by providing flexible, accurate, and timely detection and alerting of hostile activity. As a passive system (rather than an active defense such as a firewall), IDS is able to identify suspect traffic without disrupting legitimate communications. It may be able to detect reconnaissance and other precursors to an attack, shifting the balance of time based security in favor of a defender rather than the attacker[5]. If the first GIAC learns about a server compromise is Tripwire alerts (the bad guy is already changing files on the system), we have missed much of the opportunity to defend that system. IDS also provides detailed log trails of activity on networked systems, which could yield forensic evidence in the event of a compromise.

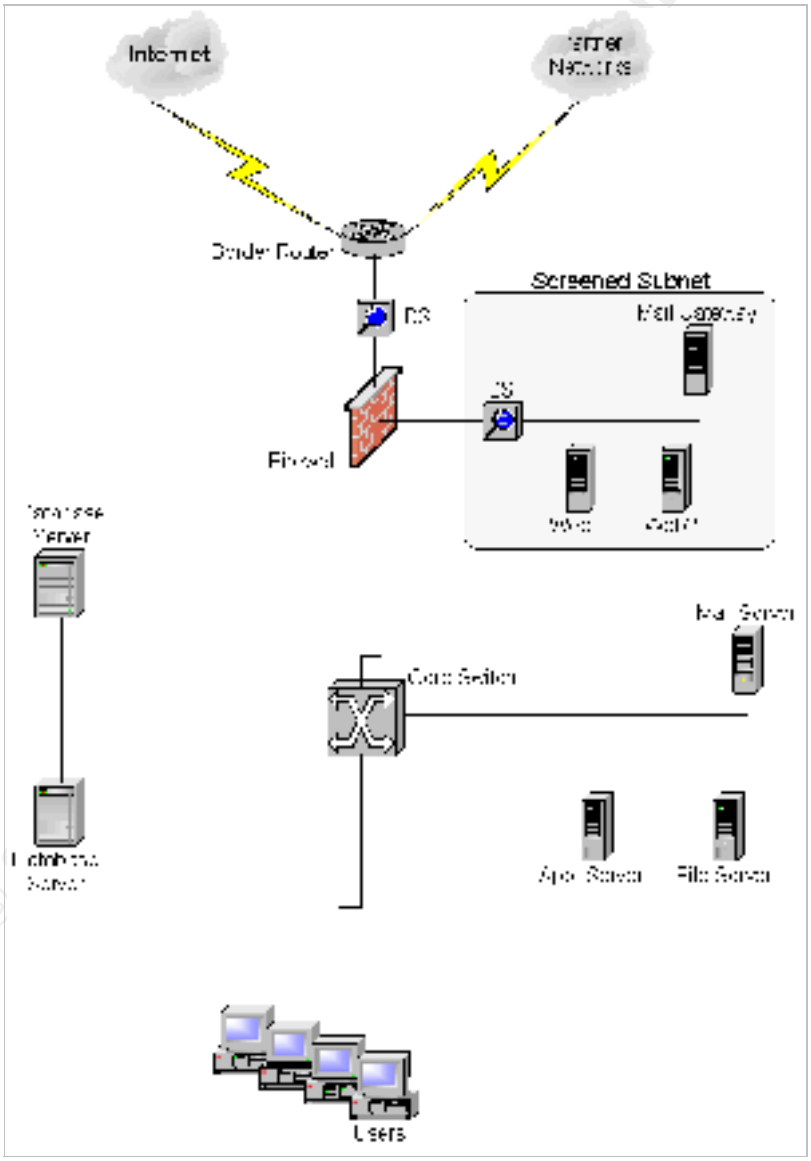
To put this in audit terms, the IDS systems help GIAC achieve goals defined by

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

COBIT such as:

- DS5.7 Security Surveillance: IDS is one form of surveillance
- DS5.10 Violation and Security Activity Reports: IDS logs provide data necessary for various security reports
- DS5.11 Incident Handling: IDS logs may also play a central role in incident handling; the data they contain may be much more trusted than anything recovered from a compromised system, where an attacker has been able to manipulate logs at will

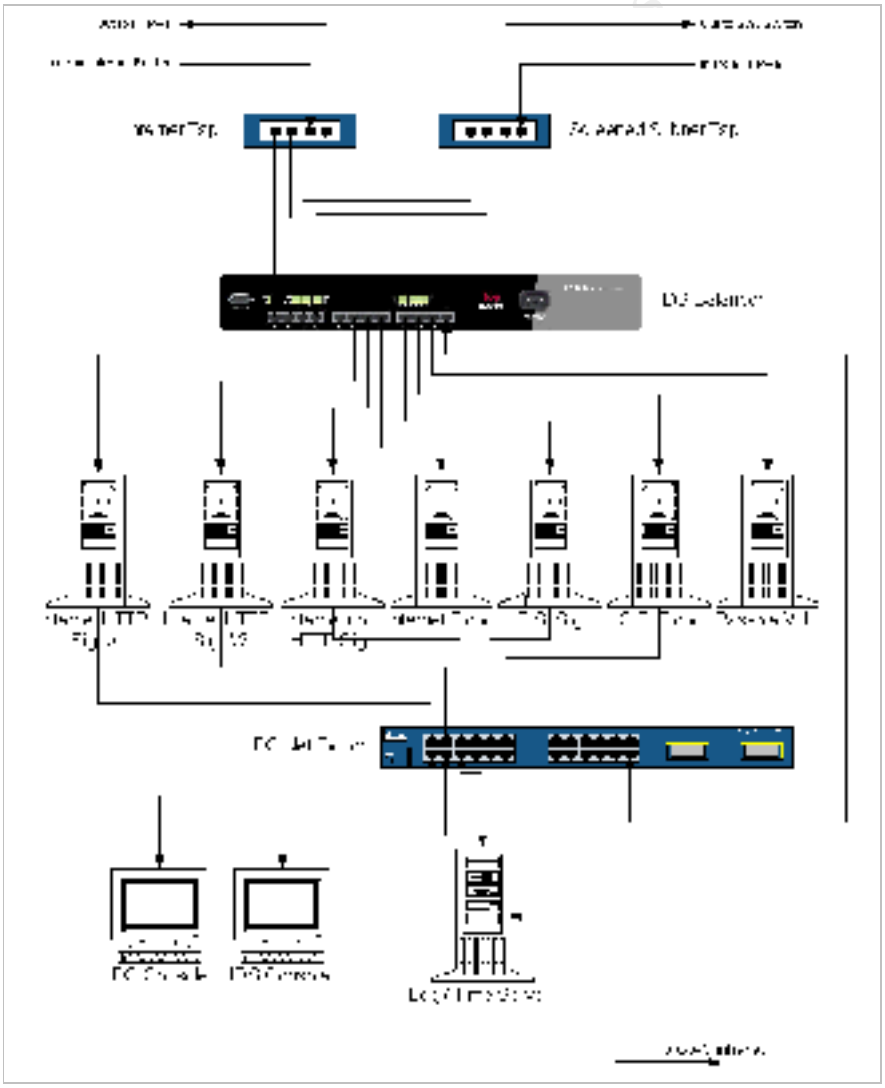
The following diagram is a high-level representation of the GIAC network.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The role of the Balancer in the IDS system is to aggregate traffic from Ethernet taps into “flows” (also called “sessions” or “streams”), and distribute them to appropriate IDS sensors. The Balancer provides unique abilities to separate traffic into different types, load balance across multiple sensors, and send duplicate traffic to multiple sensors for different types of processing. This is a key requirement for GIAC because while the existing deployment uses a combination of signature and anomaly based analysis, the next step for the IDS team will be to implement a passive vulnerability analysis system such as SourceFire's RNA[6] or Tenable's NeVO[7]. As a central component of the security deployment the IDS Balancer will be treated with the same attention and care as other security components such as firewall, antivirus, and authentication systems.

The following diagram shows the IDS network setup:



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk Evaluation

In order to evaluate the risk to the system, a number of parameters had to be identified: what is at risk (the assets), what are the threats, and what are the possible consequences for the business. From these, a prioritized list of controls to address the risks was developed. The assessment measured compliance with those controls.

Based on a risk evaluation form[8], a number of risk categories were considered. These were identified as being applicable to the Balancer deployment:

- access risk
- business disruption risk
- data integrity risk

Assets

The primary asset, in this case, is the service provided by the Balancer: the timely, complete, accurate transfer of network data from the taps to the appropriate sensors. The Balancer itself also has a value and must be considered.

Threats

The threats to the assets are:

- external attacker: someone outside the organization intending to do harm to GIAC
- internal attacker: someone with inside access, intending to do harm
- accident, misconfiguration, and similar: this results from the actions of someone with access, but no intent to do harm
- failure: including hardware, software, and environmental problems; examples include a hardware component within the Balancer failing or a natural disaster

Impacts

The most significant impacts identified were unauthorized access that could lead to undetected configuration changes or exposure of sensitive data. It is possible that the Balancer could be reconfigured to ignore certain traffic, effectively blinding the IDS sensors to some attacks. Another possibility is that traffic could be monitored via the Balancer. This is significant because of the sensitivity of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

some of the traffic processed by the Balancer. In both of these cases the impact is more subtle, less likely to be noticed, and therefore could be a long-term concern. The impact to GIAC could be not only reduced network security, but also disclosure of sensitive information.

The other impacts identified generally involved Balancer downtime which would interrupt all IDS functions. This would cost GIAC staff time to respond to the problem and the additional risk of running without IDS coverage. This is considered a somewhat lower concern because an outage of the Balancer would be quickly noticed by IDS analysts when their consoles got very quiet. Additional focus was placed on controls to ensure an efficient response in order to minimize the duration of any disruption.

Risk Calculation

All security components of GIAC's network are considered sensitive and receive a high level of attention and scrutiny, due to the greater potential impact of a failure compared to some other network components. When calculating risk, then, staff are more conservative in their evaluations. Risk is calculated from these components:

- vulnerabilities (what can go wrong)
- exposure (the likelihood of that going wrong)
- impact (how bad it would be if it went wrong)

The three factors are combined in some way to determine risk. For this situation, a value between one and three (low, medium, and high) were assigned to "exposure" and "impact". The values were added to determine overall risk, where a low risk is two, a medium risk is three or four, and high risk is five or six.

Different methods can be used to calculate risk. For example, some assign a value to the vulnerability in addition to the exposure and impact. Some multiply the values instead of adding them. In the case of systems where GIAC has low risk tolerance, the formula used here provides consistency and proper valuation.

In the table below, the "exposure" column factors in existing controls to address the risk, and "impact" considers the worst case outcome for the company. For example, consider the vulnerability of someone gaining unauthorized access by taking advantage of a weak password: the exposure is rated low while the impact is rated high. These combine to give a medium risk. In the "impact" column, any potential impact beyond disruption of IDS services is noted.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Outcome	*Vulnerability*	*Exposure*	*Impact*	*Risk*
Unauthorized Access	Inadequate network segregation (management interface accessible outside IDS network, including modems, VPNs, etc.)	2	3 Balancer integrity	High
	Compromised credentials (sniffed, guessed)	1	3 Balancer integrity	Medium
	Weak password (including default, blank)	1	3 Balancer integrity	Medium
	Exploit sent in input traffic	3	3 Balancer integrity	High
	Exploit sent over management network	1	3 Balancer integrity	Medium
	An attacker gains physical access to the Balancer	1	3 Balancer integrity	Medium

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Outcome	***Vulnerability***	***Exposure***	***Impact***	***Risk***
Denial of Service	Exploit sent in monitored traffic	3	3	High
	Exploit sent in management traffic	1	2	Medium
	An attacker gains physical access to the Balancer	1	3 Physical loss	Medium
Misconfiguration	Multiple simultaneous administrative sessions	1	1	Low
	Inadequate change control	2	2	Medium
	Inadequate separation of duties	2	3	High
Service Interruption	Hardware failure	1	3	Medium
	Software failure	1	3	Medium
	Environmental failure	1	2	Medium

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Outcome	*Vulnerability*	*Exposure*	*Impact*	*Risk*
	Interruption prolonged due to inadequate controls, documentation, procedures, etc.	2	2	Medium

State of Practice

Researching a secure configuration for the Balancer began with the GIAC IT security policy, which establishes guidelines for all systems involved in GIAC's operations. This also provides the background necessary to make implementation decisions, including system classification, risk tolerance, and frame of reference.

The next step was to review documentation provided by Top Layer for the product. The IDS Balancer Configuration and Management manual[9] (hereafter "manual") provides the most complete reference on configuring the Balancer, and contains a chapter devoted to security issues (chapter seven, Performing IDS Balancer Security and Access Tasks, pages 162-182). The release notes[10] provided more up-to-date information about additional features and fixes incorporated into the Balancer since the publication of the manual. It was important to review the vendor's documentation because it provided information about what types of control processes could be implemented. The Balancer, like many other appliance-type devices, has a simplified configuration that does not contain a full range of options that would be available on a general purpose operating system.

Top Layer has published a number of white papers, case studies, and other documents. These were reviewed but they tended to focus on the features of their products and related marketing aims, and did not provide significant value regarding secure configuration of their products[11].

Top Layer's support resources, available to customers with a support agreement, includes frequently asked questions, a knowledge base, and other useful information setting up and managing their products. Some, though limited, information useful for securing the Balancer was discovered.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The next step was to search online resources that have been useful to GIAC staff for security information in the past. These included the SANS reading room[12] and GIAC certification papers[13]. For example, each posted GSNA certification practical was downloaded and a few data points about each were entered into a spreadsheet, including the audited entity (for example, an Apache Web server on Red Hat Linux), the perspective of the audit (either independent auditor or administrator), and a locally assigned category (network device, operating system, application).

Similar research was done in the Reading Room, with particular attention paid to sections on Auditing and Assessment, Best Practices, Intrusion Detection, Network Devices, and Threats / Vulnerabilities. While no previous reports specifically addressed the IDS Balancer, a good deal of related work was identified.

Some of the papers that were useful are:

- Don Weber (GSNA #92): Sourcefire Intrusion Detection System Deployment: An Auditor's Perspective
- Leigh Haig (GSNA #85): Auditing a CacheFlow Proxy Solution: An Auditors Perspective
- Darren Wassom (GSNA #47): Auditing a Distributed Intrusion Detection System: An Auditors Perspective
- Azim Ferchichi (GSNA #35): Audit of Solaris 8 platform
- Travis Hildebrand (GCUX #212): Step-by-Step Configuration of a Solaris 9 syslog server

A resource that has been very helpful for securing other systems have been the CIS[14] benchmarks and tools. These are assessment programs for commonly used systems such as Solaris, Linux, Windows, and Cisco routers running IOS. These projects are the result of collaborative effort of many experts throughout the industry. The result is a document that can be used by technical (but non-security) staff to significantly improve the security of a system, and a tool to measure compliance with their standards. So while these resources do not directly cover the IDS Balancer, the concepts involved were very applicable to this situation.

MITRE maintains the Common Vulnerabilities and Exposures (CVE) listing, which provides “standardized names for vulnerabilities and other information about security exposures”[15]. Similarly, SecurityFocus maintains an extensive

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

vulnerability database which “provides security professionals with the most up-to-date information on vulnerabilities for all platforms and services”[16]. Both of these were searched for information relating to the Balancer, using terms “toplayer”, “top layer”, “ids balancer”, “load balancer”, “ids”, and “balancer”. For CVE, both candidates and full entries were searched. Both listed only one interesting reference, an announcement from 2000 regarding a different product (AppSwitch) crashing when it received malformed traffic[17]. This did not help develop the checklist, but it did validate the threat of denial of service to the Balancer.

Although in the technology field their contents are sometimes out of date before they are published, books are a very valuable resource to security professionals. This was especially true in the case of this assessment, where best practices and principles used in other systems were applied to the configuration of the Balancer. Some of the books that were applicable for this audit were:

- *Network Intrusion Detection*, Second Edition, Northcutt and Novak; 2001, New Riders, Indianapolis, Indiana
- *Inside Network Perimeter Security*, Northcutt, Zeltser, et. al.; 2003, New Riders, Boston
- *Practical UNIX Security*, Garfinkel and Spafford; 1991, O'Reilly and Associates, California
- *Security in Computing*, Second Edition, Pfleeger, Charles; 1997, Prentice Hall, New Jersey

Email lists provide forums for discussing a variety of topics, and searchable archives are a key for finding useful information. An advantage to mailing lists is that they often have the latest information on a given topic. They also provide a discussion format, where the details of a topic are hashed out from multiple perspectives. On the other hand, like anything on the Internet, lists need to be viewed with a skeptical eye. Lists are often open for posts from anyone, with no requirements for knowledge, experience, or rational thought. Subscribing to a list for a short while will often reveal which posters are worth reading and which are not. When searching archives, it is advisable to read a few posts and responses from an individual before accepting what they write at face value.

A Web site, MARC[18], maintains a searchable archive of around 1,500 mailing lists. Lists that are useful for researching vulnerabilities in products include bugtraq and full-disclosure. The focus-ids list, hosted by Securityfocus, has high quality content covering a wide range of issues related to intrusion detection.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Snort website contains IDS documentation and papers from independent authors as well as various vendors: http://www.snort.org/docs/

A general search of the Web, using Google[19], was conducted but did not reveal much information beyond what was available from the above resources. The searches started narrowly looking for relevant information with keywords “top layer”, “ids balancer”, “secure configuration”, “audit”, etc. (for example, “'top layer' secure configuration”). The search was then broadened by searching more generically for “load balancer audit” and similar. Finally, searches were conducted for security of other load balancers and similar devices (F5 BigIP, Nortel Alteon, Cisco CSS, etc.).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Part II: Develop the Audit

Staff identified three ways to audit the Balancer: using the command line interface (CLI), using the Web interface (also called TopViewSecure), or by copying the configuration file to a separate system and analyzing it there. Each has advantages and disadvantages.

The primary benefit of analyzing a copy of the configuration file is that the auditor is not working on the Balancer itself, minimizing the risk of inadvertently making a change. This method also affords the best opportunity to script the tests, ensuring repeatability. On the other hand, that is the least common way for staff to manage the device – they normally use either the CLI or the Web interface – and the syntax of the configuration file is not always consistent with the other interfaces.

TopViewSecure provides a "point and click" interface that may appeal to many people. That is not a significant consideration for GIAC staff, whose normal environments are Unix and IOS, which are largely managed from a CLI.

One advantage to using the CLI is the ease with which a complete session can be recorded – the entire test session can be copied from the terminal window into a text file. It is also more efficient to display a few lines copied from a terminal window than multiple screen shots for a single test. Finally, there is some detail that is available in the CLI that is not in the Web interface. After weighing all of these considerations, the auditors decided to use the CLI to conduct the assessment.

Information Gathering

Before conducting the audit, the following information had to be gathered about the environment. Some tests in the checklist will reference these items:

IP address of the Balancer	192.168.200.13
IDS management network	192.168.200.0/24
IP addresses of authorized management stations	192.168.200.40 – 192.168.200.49
IP addresses of other systems on the IDS network	192.168.200.10 – 192.168.200.13 192.168.200.50 – 192.168.200.56
Management protocols	SSH, HTTPS, syslog, FTP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

IP address of the Balancer	192.168.200.13
Names of administrators	Mike Hotaling, Steve Smith, Lisa Adams, Joe Hogan, Barry Edwards

The Audit Checklist

As a result of the risk analysis and research done in section one, the following checklist was developed to ensure the secure configuration of the IDS Balancer. Wherever possible, tests are included to both verify the configuration and the operation of a particular control process – that the Balancer is performing as it is configured.

Each checklist item is presented in a table, as shown below:

#.# Title			
Objective	This field briefly states the control process being used to meet a security objective.		
Description	This is a more detailed description of the process being tested.		
Risk	High, Medium, or Low, as determined in the Risk Assessment portion of section one.		
Test	The steps involved in testing for for compliance.		
Control Type	Preventative, Detective, or Corrective	**Test Type**	Subjective or Objective
Compliance	The specific result that indicates compliance with the test, including screen output when appropriate. Additional descriptive information is included as necessary.		
Reference	Where to get more information.		

Many of the tests listed below involve logging in to the IDS Balancer to view configuration or log files. Other tests must be run from a separate system (such as a port scan using nmap). The following conventions are used:

- All `fixed width font` is text copied directly from a terminal window
- `MON>` at the beginning of a line indicates a session logged in to the Balancer with Monitor (read only) access
- `SEC>` at the beginning of a line indicates a session logged in to the Balancer with Administrator (read and write) access

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- `$` is the prompt of an unprivileged user on a Unix system
- `#` is the prompt of the root (superuser) account on a Unix system

A. Preventing Unauthorized Access

A1 Segregate Management Traffic From Corporate Network	
Objective	Limit unauthorized access to the Balancer by separating administrative network from other networks.
Description	The Balancer uses one Ethernet interface (#12) for management. This should be connected to a network reserved for IDS management functions. Only authorized staff should have access to this network. Controls should be in place to prevent any outside access, including VPN or modem access.
Risk	High
Test	1. Examine network diagram. Ensure that it shows proper segregation. 2. Review cabling and other infrastructure to ensure it matches diagram. 3. Scrutinize any areas where outside access is possible. In this case, the only points at which one device has connections to both the IDS management network and another network are: • The Balancer, with inputs via taps from monitored networks. Taps provide a unidirectional flow of information, which has been verified by the IDS team. • The server that provides logging, time synchronization, and alerting, a Solaris system. Review the security of this system, as covered in item A2 below.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A1 Segregate Management Traffic From Corporate Network			

Test (continued)	4. Based on information included in the Information Gathering section above, use a packet capture tool to identify unauthorized systems on the IDS network. Any device found in that capture is invalid and should be investigated.
	• Use TCPDump with the following options to capture all network traffic from any host **not** in the list above (note that this requires root access):
	`# cd /usr/local/sbin`
	`# ./tcpdump -n -v -e -s 1514 -F /tmp/local_host -w /tmp/invalidhost.cap`
	The options used above are:
	-n: do not resolve DNS names
	-v: provide verbose output
	-e: provide layer two information
	-s: set the capture length to 1514 bytes to ensure complete capture
	-F: use the file specified as the filter expression
	-w: write output to the specified file
	The first five lines of the file /tmp/local_host are:
	`# head -5 /tmp/local_host`
	`not host 192.168.200.10`
	`and not host 192.168.200.11`
	`and not host 192.168.200.12`
	`and not host 192.168.200.13`
	`and not host 192.168.200.40`
	• Let the capture run for one hour, then stop it by pressing Control-C.
	• Review the above file with the following command:
	`# ./tcpdump -n -v -X -r /tmp/invalidhost.cap`		

Control Type	Preventative	**Test Type**	Subjective

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A1 Segregate Management Traffic From Corporate Network	
Compliance	1. The network documentation shows proper separation 2. The operational cabling matches the documentation (note that this cannot be fully tested until the Balancer is put into production) 3. The log server is secure. See A2 below. 4. The capture file is empty.
Reference	• Information on the operation of Ethernet taps: http://www.finisar.com/media/product_document_detail/site2_2072393414_site2_1684740469_ProsandConsofTappingandMirroring.pdf • TCPDump manual page: http://www.tcpdump.org/tcpdump_man.html • IDS Security and using a separate management network: *Inside Network Perimeter Security*, Northcutt, Zeltzer, et. al.; 2003, New Riders Publishing, Boston; pages 177-178;

A2 Review Log Server Security	
Objective	Prevent unauthorized access to the IDS management network by securing the log server, which has access to both that network and the corporate LAN.
Description	The log server provides a logging and alerting facility, as well as time synchronization for the IDS network. However, its connectivity between the two networks does add an exposure in that if the log server is compromised, the attacker will have network access to the IDS hosts.
Risk	High

© SANS Institute 2004, All rights retained.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A2 Review Log Server Security			

Test	Log in to the log server
	
	1. Check the versions of SSH and SSL running
	`$ /usr/local/bin/ssh -V`
	
	2. Verify that Tripwire agent is running
	`$ ps -eaf |grep twagent`
	
	(The remaining tests require root access)
	3. Verify that routing is disabled
	`# ndd -get /dev/ip ip_forwarding`
	
	4. Run the CIS benchmark and check for negative results
	`# /opt/CIS/cis-scan`
	`# grep Negative /opt/CIS/cis-most-recent-log`
	
	(Perform this test from another host on the corporate network)
	5. Use nmap to verify the listening ports on the corporate interface
	`# cd /usr/local/bin`
	`# ./nmap -n -v -p 1-65535 192.168.175.35`
	`# ./nmap -n -v -sU -p 1-65535 192.168.175.35`
	
	The options used above are:
	-n: do not perform DNS resolution
	-v: provide verbose output
	-p: scan the port range listed
	-sU: perform a UDP scan
	192.168.175.35 is the target address		

Control Type	Preventative	**Test Type**	Subjective

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A2 Review Log Server Security	

Compliance	1. SSH is at version 3.7.1p2; SSL is either 0.9.6l or 0.9.7c
	`OpenSSH_3.7.1p2, SSH protocols 1.5/2.0, OpenSSL 0.9.7c 30 Sep 2003`
	
	2. Tripwire agent is running
	`root 534 1 0 Nov 20 ? 52:13 /usr/local/tripwire/tfs/bin/twagent --start`
	
	3. IP routing is disabled
	`0`
	
	4. Any “Negative” results should be examined and either corrected or justification provided.
	
	5. TCP: only port 22 for SSH and 1169 for Tripwire agent
	`Interesting ports on 192.168.175.35:`
	`(The 65533 ports scanned but not shown below are in state: closed)`
	`PORT STATE SERVICE`
	`22/tcp open ssh`
	`1169/tcp open unknown`
	
	UDP: only ports 123 for NTP and 514 for syslog:
	`Interesting ports on 192.168.175.35:`
	`(The 65533 ports scanned but not shown below are in state: closed)`
	`PORT STATE SERVICE`
	`123/udp open ntp`
	`514/udp open syslog`

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A2 Review Log Server Security	
Reference	• The current version of OpenSSL is available at the project's homepage: http://www.openssl.org/ • The current version of OpenSSH is available at the project's homepage: http://www.openssh.com • CIS Solaris benchmark: http://www.cisecurity.org/bench_solaris.html • The nmap manual page is available at: http://www.insecure.org/nmap/data/nmap_manpage.html

A3 Do Not Specify A Default Route	
Objective	Reduce the risk of a Balancer compromise by not specifying a default route, which would be required for any communication back to an outside network.
Description	Many network communications (including attacks) require bi-directional communication between the two hosts. For example, TCP connections, which are used for many common protocols such as SSH, HTTP, and FTP, cannot be established without completing a three-way handshake between the two endpoints. Using taps on the input interfaces of the Balancer prevents any outbound communications that way, but it is possible that return traffic could be sent out the management interface. The risk of exposure from this asymmetric routing can be reduced by not configuring a default route for the management interface. All of the systems the Balancer needs to communicate with, including the time / log server, and management workstations are located on the management network. There is no reason to specify a default route.
Risk	Low

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A3 Do Not Specify A Default Route				

Test	This parameter is listed in the “subsystem” configuration:
	`MON> show subsystem`
	
	Note: The Balancer has limited capability to verify this configuration. The traceroute utility, available on many other platforms, would be an ideal way to do this. The only diagnostic utility on the Balancer is ping, which is only available to users with administrative access:
	
	`SEC> ping 10.1.1.1`			

Control Type	Corrective	**Test Type**	Objective	
Compliance	`Default Router : 0.0.0.0`			
Reference	Auditors' experience.			

A4 Encrypt Management Sessions	
Objective	Use encryption to provide confidentiality for administrative and monitoring sessions on the network.
Description	Administrative and monitoring sessions contain sensitive data including authentication credentials and configuration information. Encrypting this traffic prevents an adversary from learning about the device or gaining unauthorized access. Unencrypted protocols are also more susceptible to session hijacking attacks, where an attacker could take over an active session with the rights of the hijacked user. The protocols used for administration and monitoring are: • SSH • TopViewSecure (HTTPS) • Syslog • FTP (used occasionally for uploading / downloading software images) Staff recognizes that syslog and FTP are not encrypted protocols, so the tests listed below are to confirm that the protocols are configured as securely as possible. Details regarding the risks involved in this and research into alternatives is provided in the Audit Results section below.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

<table>
<tr><th colspan="4">A4 Encrypt Management Sessions</th></tr>
<tr><td>Risk</td><td colspan="3">Medium</td></tr>
<tr><td>Test</td><td colspan="3">1. Ensure unencrypted administrative protocols are disabled.
<code>MON> show management-access</code>

2. Capture a management session:
• Log in to a management workstation and start a packet capture:
<code># /usr/local/sbin/tcpdump -n -s 1500 -w /tmp/crypto.cap host 192.168.200.13</code>

• In another terminal window, open an SSH session to the Balancer
<code>$ ssh -l monitor 192.168.200.13</code>

• Log in to the Balancer

• Generate some traffic in the SSH session
<code>MON> show log event</code>

• Log off of the Balancer</td></tr>
<tr><td>Test (continued)</td><td colspan="3">Stop the TCPDump capture by pressing Control-C

• Review the capture file. Examine the packet payloads for signs of unencrypted data.
<code># /usr/local/sbin/tcpdump -nXr crypto.cap |more</code></td></tr>
<tr><td>Control Type</td><td>Preventative</td><td>Test Type</td><td>Objective</td></tr>
<tr><td>Compliance</td><td colspan="3">1. Acceptable methods of remote access are TopViewSecure (HTTPS) and OpenSSH. Telnet, TopView, and TopFlow should be disabled.
<pre>Service   Access   Allowed IP Range
+----------------+---------+---------------
TopView   deny
Telnet   deny
SNMP   deny
TopFlow   deny</pre>
2. After session establishment, no packet payloads are readable.</td></tr>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A4 Encrypt Management Sessions	
Reference	• The vulnerability, risks, and remediation for this attack are covered in the 2003 SANS Top 20 Internet Security Vulnerabilities list as item U5, “Clear Text Services”. This is available on the Web at: http://www.sans.org/top20/#u5 • Page 174 of the manual recommends disabling any service not actively in use.

A5 Require Authentication For Access			
Objective	Restrict access to the Balancer to authorized administrators by requiring authentication prior to access.		
Description	Authentication using a username and password combination is one of the most common methods of restricting access to a system. Any system that permits access without proper credentials is susceptible to modification by unknown parties.		
Risk	Medium		

Test	Attempt to gain access via SSH without legitimate credentials. This includes using an invalid username and password, and a valid username with a blank password, and a valid username with the wrong password.
	
	(note the password fields in blue are hidden from view)
	
	1. SSH to the Balancer with an invalid username:
	`$ ssh -l nobody 192.168.200.13`
	`nobody@192.168.200.13's password: asdf1234`
	
	2. attempt to use a valid username with a blank password to login
	`$ ssh -l monitor 192.168.200.13`
	`monitor@192.168.200.13's password: [blank]`
	
	3. attempt to use a valid username with a bad password to login
	`$ ssh -l monitor 192.168.200.13`
	`monitor@192.168.200.13's password: asdf1234`		

Control Type	Preventative	**Test Type**	Objective
Compliance	All access requires authentication. Attempting to gain access with invalid credentials fails. The following message is displayed: `Permission denied, please try again.`		

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A5 Require Authentication For Access	
Reference	Auditors' experience.

A6 Change Default Passwords			
Objective	Prevent unauthorized access to the system via well known credentials by changing default passwords.		
Description	Systems are often shipped from the factory with default username and password combinations that are publicly available in published documentation. If left unchanged an unauthorized person could use those credentials to gain access to the system. The auditor can verify that these have been changed by attempting to log in to the Balancer using the factory credentials. The accounts from the factory are “siteadmin” and “monitor”, with “toplayer” as the password for both.		
Risk	Medium		

Test	SSH to the Balancer and attempt to log in using credentials above:
	
	`$ ssh -l monitor 192.168.200.13`
	`monitor@192.168.200.13's password: toplayer`
	
	`$ ssh -l siteadmin 192.168.200.13`
	`siteadmin@192.168.200.13's password: toplayer`		

Control Type	Preventative	**Test Type**	Objective
Compliance	Permission should be denied when using default accounts and passwords. `Permission denied, please try again.`		
Reference	• Page 162 of the manual lists the default accounts as “siteadmin” and “monitor”, and the default password for both as “toplayer”. Page 165 of the same document recommends users change the password for the siteadmin account. • The SANS Top 20 document, item U4, describes “widely known” passwords as a vulnerabilities: http://www.sans.org/top20/#u4 • Page 242 of *Inside Network Perimeter Security* describes the importance of changing default passwords on network devices.		

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A7 Restrict Sources Of Administrative Sessions			
Objective	Prevent unauthorized access to the Balancer by restricting the source addresses of administrative sessions.		
Description	In order to reduce the risk of unauthorized access, the IDS Balancer should not accept access from addresses outside the administration group. Acceptable addresses are listed in the Information Gathering section above.		
Risk	Medium		

Test	1. Access restrictions are configured in “management-access”:
	`MON> show management-access`
	
	2. Use a test system with an address outside the acceptable range.
	
	3. Attempt to SSH to the IDS Balancer:
	`$ ssh -l monitor 192.168.200.13`		

Control Type	Preventative	**Test Type**	Objective

Compliance	1. Restrictions are in place for SSH and TopViewSecure:
	`TopViewSecure restrict 192.168.200.40->192.168.200.49`
	`OpenSSH restrict 192.168.200.40->192.168.200.49`
	
	2. The local system's address is not in that range:
	`$ /sbin/ifconfig -a`
	`dmfe0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2 inet 192.168.200.54 netmask ffffff00 broadcast 192.168.200.255`
	
	3. Attempt to SSH fails:
	`ssh: connect to host 192.168.200.13 port 22: Connection timed out`		

Reference	Page 174 of the manual recommends restricting the IP addresses that can access the Balancer.		

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A8 Idle Sessions Should Time Out Within Five Minutes			
Objective	Reduce risk of unauthorized access by expiring idle administrative sessions in five minutes.		
Description	Inactive administration sessions should timeout, requiring the user to re-authenticate. This reduces the risk of someone abusing a session that a valid administrator opened and walked away from. It also lessens the likelihood that multiple people will be in contention for read-write access.		
Risk	Medium		

Test	1. Session timeouts are managed in the security configuration:
	`MON> show security`
	
	2. SSH to the Balancer:
	`$ ssh -l monitor 192.168.200.13`
	
	3. Let the session sit idle for five minutes.
	
	4. Verify that the session times out.		

Control Type	Preventative	**Test Type**	Objective

Compliance	1. Timeouts are configured for five minutes (300 seconds):
	`console-cli-timeout : 300`
	`telnet-cli-timeout : 300`
	`ssh-cli-timeout : 300`
	
	2. The session is disconnected:
	`MON> Received disconnect from 192.168.200.13`
	`$`		

Reference	Auditors' experience.		

A9 Enforce Minimum Password Length	
Objective	Prevent unauthorized access via a weak password.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A9 Enforce Minimum Password Length			
Description	Using passwords as an authentication mechanism is useful as long as the password is difficult to discover. The "strength" of passwords can be described as a function of how long it would take an attacker to recover a password. Factors that make passwords stronger are their randomness, their length, and how often they change. A completely random one character password could be cracked in seconds. At the same time, a twelve letter word found in a dictionary would not last much longer. The only mechanism available for ensuring the strength of passwords on the Balancer is minimum length.		
Risk	Medium		

Test	1. Verify that the Balancer is configured with a minimum password length of eight characters:
	`MON> show security`
	
	2. Attempt to create a user with a short password.
	`SEC> set user test1 access monitor`
	`Enter new password`
	`=> abc123`		

Control Type	Preventative	**Test Type**	Objective

Compliance	1. The Balancer is configured for a minimum password length of 8 characters:
	`minimum-password-length : 8`
	
	2. The Balancer does not accept a short password:
	`Error: Passwords must be 8 - 255 characters in length.`
	`Invalid or malformed parameter values`		

Reference	Page 164 of the IDS Balancer Configuration and Management guide discusses configuring minimum password length. *Network Security*, Kaufman, Perlman, Speciner; 1995, Prentice Hall, New Jersey; Chapter 8, pages 205 – 222 provides extensive information on authentication, strength of passwords, and related issues.		

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A10 Verify That Commands Cannot Be Received On Listen / Monitor Ports			
Objective	Prevent unauthorized access to the Balancer by ensuring that it does not respond to administrative access on Listen or Monitor ports.		
Description	The possibility exists to inject administrative commands in the most exposed point of the Balancer – the network streams on Input and Monitor ports. This constitutes the most exposed facet of the Balancer since it processes ALL traffic on the tapped (and often least trusted) networks. This type of vulnerability has been demonstrated in both TCPDump and Snort, applications that passively capture and process network traffic off of the wire. The Balancer's risk is somewhat lower because its traffic processing is restricted to header information from packets. Further, because of the way the Balancer is deployed, it would be very difficult to attack since there is no direct way for the Balancer to establish a session back to outside networks.		
Risk	High		

Test	1. Connect a test system to a Listen port.
	
	2. Start a packet capture:
	`# tcpdump -n -v -e -s 1514 -w /tmp/listen.cap`
	
	3. Allow the capture to run for 30 minutes. Verify that there is no traffic coming from the Balancer.
	
	4. Attempt to SSH to the Balancer's IP address.
	`$ ssh -l monitor 192.168.200.13`
	
	5. Connect a test system to a Monitor port.
	
	6. Attempt to connect using SSH.
	`$ ssh -l monitor 192.168.200.13`		

Control Type	Preventative	**Test Type**	Objective

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A10 Verify That Commands Cannot Be Received On Listen / Monitor Ports	
Compliance	3. There are no packets in the capture file. 4. There is no response from the Balancer. `ssh: connect to host 192.168.200.13 port 22: Connection timed out` 6. There is no response from the Balancer. `ssh: connect to host 192.168.200.13 port 22: Connection timed out`
Reference	Auditors' experience.

A11 Ensure There Are No Unneeded Listening Ports			
Objective	Reduce the risk of unauthorized access to the system by disabling unnecessary listening ports.		
Description	Permitted forms of remote administration are TopViewSecure (HTTPS), using port 443/tcp and SSH, which uses 22/tcp. Any other listening ports should be scrutinized because they represent services available for network communications, and could provide unauthorized access.		
Risk	Medium		

Test	1. Perform a TCP scan of all possible ports:
	`# /usr/local/bin/nmap -n -v -sS -p 1-65535 192.168.200.13`
	2. Perform a UDP scan of all possible ports:
	`# /usr/local/bin/nmap -n -v -sU -p 1-65535 192.168.200.13`		

Control Type	Preventative	**Test Type**	Objective

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A11 Ensure There Are No Unneeded Listening Ports	

Compliance	1. A TCP scan should find ports 22 and 443 open, and all others either closed or filtered:
	
	`PORT STATE SERVICE`
	`22/tcp open ssh`
	`443/tcp open https`
	
	2. A UDP scan should indicate that no ports are open. Depending on whether or not the IP stack of the target system returns ICMP unreachable messages, nmap will either indicate the ports are filtered or closed:
	
	`(no udp responses received -- assuming all ports filtered)`
	`All 65535 scanned ports on 192.168.200.13 are: filtered`
	
	OR
	
	`All 65535 scanned ports on 192.168.200.13 are: closed`

Reference	Auditors' experience.

B. Preventing Unauthorized or Unintentional Changes

B1 Use Accounts With Minimal Privilege For The Task At Hand	
Objective	Reduce the risk of misconfiguration by only using read-write access when necessary.
Description	Access to systems often does not involve making changes. Logging in with read-only access for sessions that do not involve modifications significantly reduces the risk of inadvertent changes to the Balancer.
Risk	High
Test	Review procedure to ensure that people use a monitor account for read-only activities. Review logs for indications that read-write is used unnecessarily. This test will be more effective in subsequent audits when the Balancer is in production use.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B1 Use Accounts With Minimal Privilege For The Task At Hand			
Control Type	Preventative	**Test Type**	Subjective
Compliance	Users only use accounts with administrative access when they intend to make changes to the configuration.		
Reference	Jeff Langford published a paper titled Implementing *Least Privilege at your Enterprise* that is available at: http://www.sans.org/rr/papers/index.php?id=1188		

B2 Restrict Simultaneous Administrative Sessions	
Objective	Prevent contention and misconfiguration that could result from multiple simultaneous administrative sessions by only permitting one at any given time.
Description	Having multiple concurrent administrative sessions to a device can lead to misconfiguration.
Risk	Medium

Test	1. This restriction is configured in the security group:
	`MON> show security`
	
	2. SSH to the Balancer with Administrative access and note the permissions granted:
	`SEC> show session`
	
	3. Open another terminal window and start a second SSH session to the balancer, also with administrative access, and review session status:
	`SEC> show session`
	
	4. Open a Web browser and connect to the Balancer using an account with administrative access. Note the permissions
	`SEC> show session`
	
	5. Close the Web browser from step #4 and SSH session opened in #3 above. Connect to the Balancer's console port and log in as an administrator. Note the access granted:
	`SEC> show session`

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

<table>
<tr><th colspan="4">B2 Restrict Simultaneous Administrative Sessions</th></tr>
<tr><td>Control Type</td><td>Preventative</td><td>Test Type</td><td>Objective</td></tr>
<tr><td>Compliance</td><td colspan="3">1. The balancer is configured for exclusive read-write access:

exclusive-rw-login : True

2. When there is only one SSH session, the access granted is the same as the access requested:

User Name Access Level
Method IP Address

(actual) (requested)

+---------------+---------------+---------------+----------+------------

*"mikeh" security-admin security-admin ssh
0.0.0.0</td></tr>
<tr><td>Compliance (continued)</td><td colspan="3">3. A second SSH session is only granted monitor access:

User Name Access Level
Method IP Address

(actual) (requested)

+---------------+---------------+---------------+----------+------------

*"mikeh" security-admin security-admin ssh
0.0.0.0

"siteadmin" monitor security-admin ssh
0.0.0.0

4. Only the first admin session, the top SSH session, has read-write access:

User Name Access Level
Method IP Address

(actual) (requested)

+---------------+---------------+---------------+----------+------------

*"mikeh" security-admin security-admin ssh
0.0.0.0

"siteadmin" monitor security-admin ssh
0.0.0.0

"mikeh" monitor security-admin web
192.168.200.47</td></tr>
</table>

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B2 Restrict Simultaneous Administrative Sessions	

Compliance (continued)	5. Note that it is possible to have an administrative session from the console and the a network based session at the same time. This is a safeguard in the system for remote deployments and cannot be changed. See page 170 of the manual:
	`User Name Access Level Method IP Address`
	`(actual) (requested)`
	`+--------------+--------------+--------------+---------+-----------`
	`*"mikeh" security-admin security-admin ssh 0.0.0.0`
	`"siteadmin" security-admin security-admin console 0.0.0.0`
	
	NOTE: any account that has read-write permissions may "preempt" any other read-write session, if necessary, in order to gain access. See page 170 of the manual. This should not be a significant issue for GIAC since sessions timeout in five minutes.

Reference	Page 164 of the IDS Balancer Configuration and Management guide discusses configuring exclusive administrative access.

B3 Each Balancer Manager Must Use Unique Credentials	
Objective	Enforce the use of individual username and password combinations by managers to provide granular account management and meaningful audit trails.
Description	Each individual with access to the IDS Balancer should use a unique username and password. People should not use shared accounts. This ensures that event logs contain meaningful information regarding who made changes or logged in to the system at a particular time. This also simplifies managing accounts when people separate from GIAC by not requiring changes to shared accounts.
Risk	Medium

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B3 Each Balancer Manager Must Use Unique Credentials			
Test	Verify that procedures require that each team member use individual credentials. Review logs for signs that the procedure is not being followed. This would include successful logins from many computers, perhaps simultaneously, all using the same account. See step B4 for details on reviewing logs for successful logins.		
Control Type	Corrective	**Test Type**	Subjective
Compliance	All users use individual credentials to log in to the IDS Balancer.		
Reference	See GIAC IT security policy.		

B4 Successful And Failed Login Attempts Should Be Logged	
Objective	Maintain a meaningful audit trail of system events including information about successful and failed login attempts.
Description	Information regarding both successful and failed login attempts should be logged. This information should include the method of access, source address, the date and time, and the account that was accessed. Repetitive failed login attempts could indicate an unauthorized person trying to gain access to the system. Successful logins provide a variety of useful information, including who accesses the system, how often, and from where.
Risk	Medium

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B4 Successful And Failed Login Attempts Should Be Logged				

Test	The default configuration is to log these events and this parameter cannot be modified.
	
	1. Verify logins are being properly logged:
	• Connect to the IDS Balancer using SSH with valid credentials:
	`$ ssh -l monitor 192.168.200.13`
	• Connect to the IDS Balancer using SSH with invalid credentials:
	`$ ssh -l mark 192.168.200.13`
	
	2. Repeat above steps using the Web interface.
	
	3. Log in to the IDS Balancer and review the event log for information about the above connections:
	`MON> show log event`			

Control Type	Detective	**Test Type**	Objective	
Compliance	All login attempts should create entries in the event log. The logs should include source address, date and time, and the account that was used.			
Reference	*Inside Network Perimeter Security*, pages 238 – 241;			

B5 Failed Logins Should Not Reveal Information About Valid Accounts	
Objective	Make it more difficult for attackers to enumerate account information by sending the same response to all failed login attempts.
Description	Some systems send different “access denied” messages depending on whether the failure was due to a bad username or bad password. This enables an attacker to identify valid usernames, reducing the work they have to do to gain access. Systems should respond consistently to failed login attempts.
Risk	Low

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B5 Failed Logins Should Not Reveal Information About Valid Accounts			

Test	1. SSH to the Balancer with a valid account but a bad password. Note the response.
	`$ ssh -l monitor 192.168.200.13`
	`monitor@192.168.200.13's password: asdf123`
	
	2. SSH to the Balancer with an invalid username and password. Note the response.
	`$ ssh -l mark 192.168.200.13`
	`mark@192.168.200.13's password: asdf123`		

Control Type	Corrective	**Test Type**	Objective
Compliance	Response to failed login attempts should be consistent: `Permission denied, please try again.`		
Reference	SANS Courseware 2003, Track 7 (Auditing Networks, Perimeters, and Systems) Day 3 (Auditing Web-Based Applications), pages 179 – 181;		

B6 A Warning Banner Should Be Displayed Prior To Any Type Of CLI Access	
Objective	Inform anyone who connects to the Balancer that it is a private system and that activity is monitored.
Description	It is considered a best practice to provide a warning banner on protocols that support it, including serial, telnet, SSH, and FTP access. The warning banner should indicate that a system is private and intended only for permitted uses. It should also indicate that access may be monitored to avoid potential legal issues with recording activity. The details of this are often determined by legal departments and formalized in corporate policy.
Risk	Low

Test	1. Verify the configuration:
	`MON> show security`
	
	2. SSH to the IDS Balancer and note whether or not banners are displayed.
	`$ ssh -l monitor 192.168.200.13`
	`monitor@192.168.200.13's password:`

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B6 A Warning Banner Should Be Displayed Prior To Any Type Of CLI Access			
Control Type	Corrective	**Test Type**	Objective

Compliance	1. The custom warning banner should be configured:
	`cli-login-banner : custom`
	`custom-cli-banner :`
	`"Authorized use only. All activity may be monitored and reported."`
	
	2. Warning banners should be displayed upon any access that supports their display.
	`Authorized use only. All activity may be monitored and reported.`		

Reference	See GIAC IT security policy.		

B7 Log System And Security Events To A Separate Log Server	
Objective	Maintain integrity and availability of Balancer logs by sending them to a separate log server.
Description	Where security is a concern it is often advisable to set up a dedicated log server to collect logs from other systems. In most systems it is advisable because one of the first things attackers often do when compromising a system is to erase traces of their activity from log files. If those logs are on a separate server it is more likely that they will survive. This also offloads the overhead of processing the logs to the log server, which can improve performance. Also, the IDS Balancer, as with many devices, does not contain a hard disk or other mass storage device to record any significant amount of logs. Sending logs to a different server is required in order to maintain log archives.
Risk	Medium

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B7 Log System And Security Events To A Separate Log Server			

Test	1. This is configured in syslog-host:
	`MON> show syslog-host`
	
	2. Review local logs on the Balancer:
	`MON> show log event`
	
	3. Ensure the logs on the syslog server match:
	• Log in to syslog server
	`$ ssh 192.168.200.51`
	• review the file containing Balancer logs:
	`$ tail /var/adm/messages`		

Control Type	Corrective	**Test Type**	Objective

Compliance	1. The Balancer is configured to send logs to a syslog server:
	`Host IP Port Admin Facility`
	`+----------+----------+---------+-------`
	`192.168.200.51 514 enabled local-0`
	
	2. Logs on the syslog server match local logs on the Balancer.		

Reference	See SANS Courseware, 2003 Track 2 (Firewalls and Perimeter Protection) Day 4 (Defense In-Depth) pages 150 – 155; Brenton, Baccam, and Northcutt;		

B8 Synchronize Time To Reference Clock	
Objective	Ensure accurate time in log files.
Description	The clock on many systems, including the IDS Balancer, can be synchronized to a reference clock. This ensures highly accurate time for all properly configured systems, and aids correlating events in log files. It should also use an optimal time synchronization interval.
Risk	Low

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B8 Synchronize Time To Reference Clock			

Test	1. Verify the NTP servers and synchronization interval are properly configured:
	`MON> show ntp`
	
	2. Verify the implementation:
	Unlike some NTP clients, the Balancer does not provide a way to verify the NTP status. In lieu of a proper way to query the status, the following tests were conducted:
	• First, verify that the clock is approximately right:
	`MON> show clock`
	
	• Start a sniffer on the alert server. The configuration indicates an interval of 17 minutes (1020 seconds), so let the sniffer run for at least that long. Observe any synchronization attempts.
	`# ./tcpdump -n -X host 192.168.200.13 and port 123`
	
	Monitor the log for any entries generated by the above tests.
	
	Another alternative that was considered was to set the time to a wrong value and verify that the time was corrected. The problem with that approach is that NTP does not necessarily synchronize immediately – it takes a while for a client to be "comfortable" with a server. Also, if the time difference is too large NTP will not correct it.		

Control Type	Corrective	**Test Type**	Objective

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B8 Synchronize Time To Reference Clock	

Compliance	1. NTP server should be configured as 192.168.200.40, 192.168.200.45
	`NTP servers :`
	`...`
	`IP Address`
	`+--------------`
	`192.168.200.45`
	`192.168.200.40`
	`...2 servers found.`
	
	Synchronization interval should be 17 minutes
	`query-interval : 1020`
	
	2. The packet capture should show the Balancer make a request and the server respond within the 17 minute window.

Reference	Good information on all aspects of NTP is available on the Web at: http://www.ntp.org A note on optimal polling intervals is mentioned here: http://www.ntp.org/ntpfaq/NTP-s-algo.htm#Q-ALGO-POLL-BEST

B9 Keep Time In UTC			
Objective	Ensure consistent timestamps on logs from security systems.		
Description	Correlation of logs from systems located in different timezones is simplified if all logs are recorded using the same timezone. GIAC has standardized on the UTC format.		
Risk	Low		
Test	Execute the following command from CLI: `MON> show clock`		
Control Type	Corrective	**Test Type**	Objective
Compliance	`Local Time Zone : UTC`		
Reference	Inside Network Perimeter Security, Northcutt, Zeltser, et. al.; 2003 New Riders Publishing, Boston. Page 506.		

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C. Policy, Procedure, and Other Issues

C1 Implement A Change Control Procedure			
Objective	Ensure a consistent, controlled system environment by carefully managing how changes are made to the system.		
Description	A change control procedure involves everything from explaining why a change is necessary to what steps will be taken if changes have to be backed out. The plan should involve enough people to maximize the chances of catching bad changes before they are applied.		
Risk	High		
Test	Review the change control procedure for the Balancer. Check for inclusion of documentation, approval, review, and other key elements.		
Control Type	Preventative	**Test Type**	Subjective
Compliance	The change control procedure is documented, understood, and followed by administrators of the system.		
Reference	Auditors' experience.		

C2 Review Backup, Restore, And Continuity Plans	
Objective	Ensure system availability by implementing appropriate measures for backing up and recovering from failures or disasters.
Description	A prolonged system interruption can be avoided by ensuring effective backups are available when necessary. Backups should include everything necessary to restore a system, including original media, local configuration files, documentation, and so on. Backups should be made frequently enough to minimize the risk of loss. Complete backups should routinely be rotated off-site in case, for example, a fire destroys the data center. Restoration plans include, for example, complete instructions on how to perform all necessary steps to get systems back in working order.
Risk	High

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C2 Review Backup, Restore, And Continuity Plans			
Test	Review backup documentation and schedule. Verify that the schedule is followed. Verify that backup media is stored in a locked enclosure. Ensure that backup media is being rotated off site. Ensure that old backup media is destroyed prior to being discarded.		
Control Type	Corrective	**Test Type**	Subjective
Compliance	Backups are current, consistent, and available. Staff are aware of procedures and follow them.		
Reference	*Computer Security Basics*, pages 93 – 98;		

C3 Logs Should Be Reviewed In A Reasonable Time			
Objective	Avoid missing indications of important events by monitoring system log files.		
Description	Logs are often generated for events that could impact the security or availability of a system, but they are not useful unless someone reads them. Fortunately much of the IDS team's work revolves around analyzing log files so it should not be too difficult to manage the logs from the Balancer.		
Risk	Medium		
Test	Ensure that the analysts review Balancer logs and that they know how to respond to events. This will be more significant when the system is in production.		
Control Type	Detective	**Test Type**	Subjective
Compliance	Logs are reviewed. Significant events receive an appropriate and timely response.		
Reference	*Inside Network Perimeter Security*, pages 501 – 506;		

C4 Ensure Documentation Is Complete, Current, And Correct	
Objective	Avoid misconfiguration and reduce downtime by maintaining appropriate documentation.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C4 Ensure Documentation Is Complete, Current, And Correct			
Description	System documentation should clearly communicate the current state of a system as well as information that might be necessary to troubleshoot a problem. Mistakes can be reduced by describing not only how a device is configured, but why. The documentation should be available to all staff members who might need access.		
Risk	Low		
Test	Review Balancer documentation. Ensure the following is provided: • System manuals • Network diagram • Product model, serial number, all relevant hardware, firmware, and software versions • Product support information (including contract info) • Configuration information • Backup, restore, recovery procedures • Support contact information (including phone number, email address(es), Web site password) • Administration team contact information		
Control Type	Preventative	**Test Type**	Subjective
Compliance	All of the above should be present and represent the current configuration of the system.		
Reference	Auditors' experience.		

C5 Ensure System Is Current On Patches And Updates	
Objective	Reduce risk of Balancer compromise, downtime, or other interruption by staying current on all product patches and updates.
Description	Software vendors release product updates over time to address security, performance, and availability issues, as well as adding features. Systems are often compromised using publicized flaws for which fixes exist. This can be avoided by installing updates as they become available.
Risk	Medium

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C5 Ensure System Is Current On Patches And Updates			
Test	1. Obtain a list of current patches, version numbers, and updates from TopLayer support. 2. Check the versions in use on the Balancer. `MON> show version` 3. Compare the list against the software that is running on the Balancer. Note any differences in the list.		
Control Type	Preventative	**Test Type**	Subjective
Compliance	The running versions should be current when compared to the list provided by TopLayer support. Exceptions may be made in the event of known bugs, incompatibilities, etc.		
Reference	*Inside Network Perimeter Security*, page 249 – 250;		

C6 Install And Verify The Operation Of A Redundant Power Supply	
Objective	Increase Balancer availability by utilizing redundant hardware components as available or appropriate.
Description	Although hardware failures are not very common, they can cause system downtime. That disruption can be avoided in many cases by using redundancy. One of the most common hardware failures, in GIAC's experience, is power supplies. A redundant power supply is one of the few options available for the Balancer.
Risk	Medium

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C6 Install And Verify The Operation Of A Redundant Power Supply			
Test	1. The status of the power supplies can be verified at the CLI: `MON> show environment` Note: LEDs on the front panel of the Balancer also indicate the operation of both power supplies. This cannot be verified via TopViewSecure. 2. Although it is beyond the scope of this assessment to simulate a hardware failure, system stability can be checked when only one power supply is functioning by disconnecting each, one at a time, from the power source. 3. Review logs to see if they indicate changes in power supply status.		
Control Type	Preventative	**Test Type**	Objective

Compliance	1. The status indicates that both power supplies are working properly.
	`Power Supply 1 status: Working`
	`Power Supply 2 status: Working`
	
	2. The Balancer runs, without interruption, when only one power supply is available.
	
	3. Logs should indicate any change in status of either power supply.		

Reference	Auditors' experience		

C7 Review Environmental Conditions	
Objective	Ensure Balancer availability by providing appropriate environmental conditions.
Description	The Balancer has specific environmental operating conditions relating to temperature and humidity. Operating the device outside of those specifications could result in stability problems or damage to the device.
Risk	Low

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C7 Review Environmental Conditions				
Test	1. The Balancer has a temperature monitor that can be checked with the following command: `MON> show environment` 2. The data center air handler unit control panels display the humidity of the air.			
Control Type	Preventative		**Test Type**	Objective
Compliance	1. The temperature must be in the 0° – 40° Celsius range `Temperature : 27 degrees C` 2. The humidity must be in the range 5 – 95%: The air handler reported 49% humidity, with a target of 50%.			
Reference	IDS Balancer Data Sheet, page 4: http://www.toplayer.com/pdf/TLN_IDS_Balancer.pdf			

C8 Review Physical Security			
Objective	Prevent interruption of service or loss of the Balancer by ensuring appropriate physical security measures are in place.		
Description	A popular saying among information security pros is that if a bad guy has physical access to a target the game is over.		
Risk	Medium		
Test	Building: GIAC headquarters is located in Miami, Florida and is the location of the corporate data center, which houses the Balancer. GIAC owns the property and building, but it is not considered a secure / restricted facility. During business hours visitors are common and policies regarding escort, sign-in / sign-out, visitor badges, etc. are not strictly enforced. Room: The data center facility itself is much more secure. It is located on the second floor of the building. There are two entrances / exits, each requiring an access card. Operations staff is present all of the time. Rack: The IDS systems are located in a single rack enclosure, with no other systems sharing that space.		
Control Type	Preventative	**Test Type**	Subjective

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

C8 Review Physical Security	
Compliance	Unauthorized people are not able to access the Balancer.
Reference	*Computer Security Basics,* pages 237 - 243, Russel, Deborah and Gangemi, G.T.; O'Reilly & Associates, Sebastopol, CA, 1991;

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Part III: Conduct the Audit

The following shows the results of selected tests from the assessment. These tests were chosen for one of the following reasons:

- they check for compliance in an area that was identified as high risk
- they demonstrate a thorough test, often by checking a configuration and then using a tool to verify its implementation
- they contain information specifically referenced in the conclusions

As mentioned in section two, all output lines that begin "MON>" were conducted after logging into the Balancer with Monitor privileges, as follows:

```
$ ssh -l monitor 192.168.200.13
monitor@192.168.200.13's password:

Authorized use only.  All activity may be monitored and
reported.

MON>
```

A2 Review log server security - PASS

```
mikeh@workstation$ ssh 192.168.175.35
mikeh@192.168.175.35's password:
Last login: Mon Nov 24 16:48:51 2003 from workstation1


Authorized use only.  Activity may be logged and reported.


$ /usr/local/bin/ssh -V
OpenSSH_3.7.1p2, SSH protocols 1.5/2.0, OpenSSL 0.9.7c 30 Sep
2003
$ ps -eaf |grep twagent
root   534     1  0   Nov 20 ?       52:13
/usr/local/tripwire/tfs/bin/twagent --start
$ su -
Password:
Sun Microsystems Inc.   SunOS 5.8       Generic February 2000
Authorized use only.  Activity may be logged and reported.


# ndd -get /dev/ip ip_forwarding
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
0
# /opt/CIS/cis-scan
# grep Negative /opt/CIS/cis-most-recent-log
Negative: 3.13 Serial login prompt not disabled.
Negative: 6.1 /usr is not mounted read-only.
Negative: 7.8 EEPROM isn't password-protected.
Negative: 8.10 Default umask may not block world-writable.
Check /etc/.login.
Negative: 8.10 Default umask may not block group-writable.
Check /etc/.login.
Negative: 6.6 Non-standard SUID program /usr/local/libexec/ssh-
keysign
Negative: 6.6 Non-standard SGID program /usr/local/bin/lsof
# exit
$ exit
mikeh@workstation$ su -
Password:
root@workstation# cd /usr/local/bin
root@workstation# ./nmap -n -v -p 1-65535 192.168.175.35

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-
25 13:15 EST
Host 192.168.175.35 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.175.35 at 13:15
Adding open port 22/tcp
Adding open port 1169/tcp
The SYN Stealth Scan took 13 seconds to scan 65535 ports.
Interesting ports on 192.168.175.35:
(The 65533 ports scanned but not shown below are in state:
closed)
PORT   STATE SERVICE
22/tcp open  ssh
1169/tcp open  unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 14.127
seconds

root@workstation# ./nmap -n -v -sU -p 1-65535 192.168.175.35
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-
25 13:48 EST
Host 192.168.175.35 appears to be up ... good.
Initiating UDP Scan against 192.168.175.35 at 13:48
Too many drops ... increasing senddelay to 50000
The UDP Scan took 10708 seconds to scan 65535 ports.
Adding open port 514/udp
Adding open port 123/udp
Interesting ports on 192.168.175.35:
(The 65533 ports scanned but not shown below are in state:
closed)
PORT    STATE SERVICE
123/udp open  ntp
514/udp open  syslog

Nmap run completed -- 1 IP address (1 host up) scanned in
10708.082 seconds
```

The first test above verifies that the versions of SSH and SSL in use are the most current. The second ensures that the Tripwire agent is running, which reports violations back to a central server. The third test shows that routing is disabled for this system. The fourth test examines the results of a CIS benchmark run for any negative findings. Finally, nmap is run to ensure that the only ports listening on the corporate intranet are the ones that are needed.

It is beyond the scope of this report to document all of the steps involved in using the CIS benchmark. It is worth noting, however, that it provides a fairly thorough assessment of the security of a system. The additional tests run here were intended to supplement the CIS tool in a way that is tailored to this system. The negative findings for this system were examined with respect to the function of this system and were deemed acceptable.

The results of the CIS test were in line with expectations for this system. For example, enabled serial logins and the lack of EEPROM passwords are acceptable because this machine runs headless (there is no local console) and adequate physical controls are in place. The umask is set properly in /etc/default/login, as specified by documentation. The SUID / SGID programs are necessary for the operation of the system. The remaining risk that can be addressed is to mount /usr read only, which would prevent modification of system binaries. This will require a reboot of the system and will need to be scheduled. Frequent Tripwire scans are a compensating control in the interim, and they will continue in the future.

One of the most significant remaining risks to this system is a compromise that takes advantage of a bug in OpenSSH or OpenSSL. Mitigating factors against those risks are a strict patching and updating schedule, kernel hardening as

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

covered in the CIS tool, and extensive logging and alerting of local system activity such as that provided by Tripwire.

A3 Do not specify a default router - PASS

```
MON> show subsystem

 System Settings:
  ...

   Device:
   -------
    Name                        : "Device A"
    IP Address                  : 192.168.200.13/24
    Default Router              : 0.0.0.0

    MAC Address                 : 00-10-D1-03-82-70
    SW Version                  : "V2.20.007"
    HW Type                     : "AS3510"
    Serial number               : 400111206170114
    Configuration Seq. Number : 16


   SNMP:
   ----
    SysName     : ""
    SysContact  : ""
    SysLocation : ""
    SysUpTime   : 2676783


   Notepad:
   +------
   ""
   ------+


MON> ping 10.1.1.1
Sending Ping #1 to 10.1.1.1 ........ Timed Out
Sending Ping #2 to 10.1.1.1 ........ Timed Out
Sending Ping #3 to 10.1.1.1 ........ Timed Out
Sending Ping #4 to 10.1.1.1 ........ Timed Out
```

The tests above show that the device has not been configured with a default route, which would be required to send traffic outside of the IDS management network. The simple test – admittedly less than ideal – run to verify the configuration was to send a ping to an address outside the local network. The pings timed out, but a preferable test would have been to run a traceroute, which is not available on the Balancer.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This control is one of many that are intended to isolate the IDS management functions from outside network.

A4 Encrypt administrative sessions - FAIL

These tests were in place to verify that encryption is used to protect the integrity and confidentiality of administrative sessions.

```
MON> show management-access
  Management Access Settings:
   ...
   Service            Access    Allowed IP Range
   +------------------+---------+---------------
   TopView            deny
   Telnet             deny
   SNMP               deny
   TopFlow            deny
   TopViewSecure      restrict  192.168.200.40->192.168.200.49
   OpenSSH            restrict  192.168.200.40->192.168.200.49
```

This test shows that unencrypted access to the Balancer has been disabled.

The use of encryption was verified by capturing an administrative session over SSH:

```
# /usr/local/sbin/tcpdump -n -s 1514 -X -r /tmp/crypto.cap |more
14:39:59.523229 arp who-has 192.168.200.13 (ff:ff:ff:ff:ff:ff) tell
192.168.200.45
0x0000   0001 0800 0604 0001 0003 ba08 2cc1 c0a8        ............,...
0x0010   c82d ffff ffff ffff c0a8 c80d                  .-..........
14:39:59.523899 arp reply 192.168.200.13 is-at 0:10:d1:3:82:70
0x0000   0001 0800 0604 0002 0010 d103 8270 c0a8        .............p..
0x0010   c80d 0003 ba08 2cc1 c0a8 c82d 0000 0000        ......,....-....
0x0020   0000 0000 0000 0000 0000 0000 0000             ..............
14:39:59.524075 192.168.200.45.54389 > 192.168.200.13.22: S
585120678:585120678(0) win 24820 <nop,nop,sackOK,mss 1460> (DF)
0x0000   4500 0030 a0cb 4000 4006 8870 c0a8 c82d        E..0..@.@..p...-
0x0010   c0a8 c80d d475 0016 22e0 3ba6 0000 0000        .....u..".;.....
0x0020   7002 60f4 11af 0000 0101 0402 0204 05b4        p.`.............
14:39:59.525491 192.168.200.13.22 > 192.168.200.45.54389: S
2980724626:2980724626(0) ack 585120679 win 8192 <mss 1460>
0x0000   4500 002c 435b 0000 4006 25e5 c0a8 c80d        E..,C[..@.%.....
0x0010   c0a8 c82d 0016 d475 b1aa 3f92 22e0 3ba7        ...-...u..?.".;.
0x0020   6012 2000 423a 0000 0204 05b4 0000             `...B:........
14:39:59.525539 192.168.200.45.54389 > 192.168.200.13.22: . ack 1 win 24820
(DF)
0x0000   4500 0028 a0cc 4000 4006 8877 c0a8 c82d        E..(..@.@..w...-
0x0010   c0a8 c80d d475 0016 22e0 3ba7 b1aa 3f93        .....u..".;...?.
0x0020   5010 60f4 11a7 0000                            P.`.....
14:39:59.537759 192.168.200.13.22 > 192.168.200.45.54389: P 1:23(22) ack 1 win
8192
0x0000   4500 003e 435c 0000 4006 25d2 c0a8 c80d        E..>C\..@.%.....
0x0010   c0a8 c82d 0016 d475 b1aa 3f93 22e0 3ba7        ...-...u..?.".;.
0x0020   5018 2000 6dc3 0000 5353 482d 322e 302d        P...m...SSH-2.0-
0x0030   4f70 656e 5353 485f 322e 3970 320a             OpenSSH_2.9p2.
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
14:39:59.537819 192.168.200.45.54389 > 192.168.200.13.22: . ack 23 win 24820
(DF)
0x0000   4500 0028 a0cd 4000 4006 8876 c0a8 c82d        E..(..@.@..v...-
0x0010   c0a8 c80d d475 0016 22e0 3ba7 b1aa 3fa9        .....u..".;...?.
0x0020   5010 60f4 11a7 0000                            P.`.....
14:39:59.538421 192.168.200.45.54389 > 192.168.200.13.22: P 1:23(22) ack 23
win 24820 (DF)
0x0000   4500 003e a0ce 4000 4006 885f c0a8 c82d        E..>..@.@.._...-
0x0010   c0a8 c80d d475 0016 22e0 3ba7 b1aa 3fa9        .....u..".;...?.
0x0020   5018 60f4 11bd 0000 5353 482d 322e 302d        P.`.....SSH-2.0-
0x0030   4f70 656e 5353 485f 332e 3170 310a             OpenSSH_3.7.1p2.
14:39:59.538968 192.168.200.13.22 > 192.168.200.45.54389: . ack 23 win 8170
0x0000   4500 0028 435d 0000 4006 25e7 c0a8 c80d        E..(C]..@.%.....
0x0010   c0a8 c82d 0016 d475 b1aa 3fa9 22e0 3bbd        ...-...u..?.".;.
0x0020   5010 1fea 59e1 0000 0000 0000 0000             P...Y.........
14:39:59.539745 192.168.200.45.54389 > 192.168.200.13.22: P 23:503(480) ack 23
win 24820 (DF)
0x0000   4500 0208 a0cf 4000 4006 8694 c0a8 c82d        E.....@.@......-
0x0010   c0a8 c80d d475 0016 22e0 3bbd b1aa 3fa9        .....u..".;...?.
0x0020   5018 60f4 1387 0000 0000 01dc 0b14 1c4a        P.`............J
0x0030   ce58 543c 2cac ab84 c8d7 24e1 6209 0000        .XT<,.....$.b...
0x0040   003d 6469 6666 6965 2d68 656c 6c6d 616e        .=diffie-hellman
0x0050   2d67 726f 7570 2d65 7863 6861 6e67 652d        -group-exchange-
0x0060   7368 6131 2c64 6966 6669 652d 6865 6c6c        sha1,diffie-hell
0x0070   6d61 6e2d 6772 6f75 7031 2d73 6861 3100        man-group1-sha1.
0x0080   0000 0f73 7368 2d72 7361 2c73 7368 2d64        ...ssh-rsa,ssh-d
0x0090   7373 0000 004a 6165 7331 3238 2d63 6263        ss...Jaes128-cbc
0x00a0   2c33 6465 732d 6362 632c 626c 6f77 6669        ,3des-cbc,blowfi
0x00b0   7368 2d63 6263 2c63 6173 7431 3238 2d63        sh-cbc,cast128-c
0x00c0   6263 2c61 7263 666f 7572 2c61 6573 3139        bc,arcfour,aes19
0x00d0   322d 6362 632c 6165 7332 3536 2d63 6263        2-cbc,aes256-cbc
0x00e0   0000 004a 6165 7331 3238 2d63 6263 2c33        ...Jaes128-cbc,3
0x00f0   6465 732d 6362 632c 626c 6f77 6669 7368        des-cbc,blowfish
0x0100   2d63 6263 2c63 6173 7431 3238 2d63 6263        -cbc,cast128-cbc
0x0110   2c61 7263 666f 7572 2c61 6573 3139 322d        ,arcfour,aes192-
0x0120   6362 632c 6165 7332 3536 2d63 6263 0000        cbc,aes256-cbc..
0x0130   0055 686d 6163 2d6d 6435 2c68 6d61 632d        .Uhmac-md5,hmac-
0x0140   7368 6131 2c68 6d61 632d 7269 7065 6d64        sha1,hmac-ripemd
0x0150   3136 302c 686d 6163 2d72 6970 656d 6431        160,hmac-ripemd1
0x0160   3630 406f 7065 6e73 7368 2e63 6f6d 2c68        60@openssh.com,h
0x0170   6d61 632d 7368 6131 2d39 362c 686d 6163        mac-sha1-96,hmac
0x0180   2d6d 6435 2d39 3600 0000 5568 6d61 632d        -md5-96...Uhmac-
0x0190   6d64 352c 686d 6163 2d73 6861 312c 686d        md5,hmac-sha1,hm
0x01a0   6163 2d72 6970 656d 6431 3630 2c68 6d61        ac-ripemd160,hma
0x01b0   632d 7269 7065 6d64 3136 3040 6f70 656e        c-ripemd160@open
0x01c0   7373 682e 636f 6d2c 686d 6163 2d73 6861        ssh.com,hmac-sha
0x01d0   312d 3936 2c68 6d61 632d 6d64 352d 3936        1-96,hmac-md5-96
0x01e0   0000 0004 6e6f 6e65 0000 0004 6e6f 6e65        ....none....none
0x01f0   0000 0000 0000 0000 0000 0000 0000             ..............
0x0200   0000 0000 0000 0000                            ........

...

14:40:05.591297 192.168.200.13.22 > 192.168.200.45.54389: P 1359:1407(48) ack
1127 win 8192
0x0000   4500 0058 4373 0000 4006 25a1 c0a8 c80d        E..XCs..@.%.....
0x0010   c0a8 c82d 0016 d475 b1aa 44e1 22e0 400d        ...-...u..D.".@.
0x0020   5018 2000 6d4f 0000 4ff8 eab2 890a c732        P...mO..O......2
0x0030   dee2 6b83 75a1 c6c6 a1c2 3812 2b6b fc13        ..k.u.....8.+k..
0x0040   288f d674 3b9a 620d 67ea a5e1 4662 f2f2        (..t;.b.g...Fb..
0x0050   65e9 efc6 cf1e c714                            e.......
14:40:05.592524 192.168.200.45.54389 > 192.168.200.13.22: P 1127:1511(384) ack
1407 win 24820 (DF) [tos 0x10]
0x0000   4510 01a8 a0da 4000 4006 86d9 c0a8 c82d        E.....@.@......-
0x0010   c0a8 c80d d475 0016 22e0 400d b1aa 4511        .....u..".@...E.
0x0020   5018 60f4 1327 0000 a97b 0ad7 60f4 87ef        P.`..'...{..`...
0x0030   3ff6 3b93 ebe8 832f 9be8 58af 8824 56f5        ?.;..../..X..$V.
0x0040   c76f 2907 41c8 d4f9 6c0b 45e7 72a8 cc1d        .o).A...l.E.r...
0x0050   c2c0 25dd 4c49 c548 3c8e edab 063c dcc7        ..%.LI.H<....<..
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
0x0060   9234 2067 f7a0 7874 1f10 f694 4456 ef9a        .4.g..xt....DV..
0x0070   7379 3982 1fa9 30fc 43ef 263c a98b fded        sy9...0.C.&<....
0x0080   3c1b ed32 2140 3f4b 6e5c 1183 2c0c 6665        <..2!@?Kn\..,.fe
0x0090   544e 9f17 5281 43c4 6641 73c4 c94d 4b1e        TN..R.C.fAs..MK.
0x00a0   55c0 06a3 7f24 4202 b20e f061 ba9e cccc        U....$B....a....
0x00b0   0e16 8433 eed1 dbab e10b ef74 4da5 ce89        ...3.......tM...
0x00c0   2f28 36ad 0ef6 3cea b34a 23ef 95ee d474        /(6...<..J#....t
0x00d0   99eb 7203 6027 d58b 6a9b 97aa 667c 1e69        ..r.`'..j...f|.i
0x00e0   d5dd e619 6cde 920c 3d46 6252 7246 abeb        ....l...=FbRrF..
0x00f0   f711 b462 e656 5ea3 0d06 b4ab 8720 3e86        ...b.V^.......>.
0x0100   df2b ab21 9854 83ac 3de5 7945 559e e939        .+.!.T..=.yEU..9
```

The above trace is an SSH session established from a management workstation to the Balancer. The first few packets show normal negotiation of supported encryption and key management algorithms. This is followed by packets of encrypted traffic which is incomprehensible.

However, communications initiated from the Balancer cannot be protected with encryption. Two cases where this is implemented on the GIAC network are sending logs to a syslog server and using FTP to upload or download configuration files and software images.

The FTP transfers should be an occasional event. Nonetheless, a common option for protecting file transfer is to use SFTP, which is implemented as part of SSH. The software and configuration for the Balancer is stored on flash memory on a PC-Card storage device. Another option for managing the software would be to manage Balancer software on multiple flash cards rather than using FTP to transfer.

Syslog alternatives exist which provide authentication and encryption, but they are not as standardized and are often unavailable for appliances. An alternative method of protecting syslog traffic is to encapsulate it in IPSec. This is an option on some devices which can provide encryption services, such as Cisco routers[20].

Although there is some risk in using unencrypted management protocols, in this case the risk is less than the cost of alternatives. Since SFTP and IPSec are not available to protect these communications, the options are:

- manually move flash cards around which is very cumbersome
- do not back up or install new software or configurations, which violates other objectives and controls
- accept the risk of using FTP

- do not use syslog, so there would be no log archives
- accept the use of syslog

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The most acceptable alternatives at this point are to use FTP and syslog to perform functions necessary to the operation of the Balancer. The risk of using these is reduced because there is careful control over which staff have access to the IDS management network which is isolated from other corporate functions. Future software releases should be monitored because it is likely that they will address either or both of these issues.

A11 Ensure there are no unneeded listening ports - FAIL

```
# nmap -sS -n -v -p 1-65535 192.168.200.13

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-
25 10:24 EST
Host 192.168.200.13 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.200.13 at 10:24
Adding open port 22/tcp
Adding open port 443/tcp
Adding open port 7/tcp

The SYN Stealth Scan took 20945 seconds to scan 65535 ports.
Interesting ports on 192.168.200.13:
(The 65532 ports scanned but not shown below are in state:
filtered)
PORT    STATE SERVICE
7/tcp   open  echo
22/tcp  open  ssh
443/tcp open  https
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Randomized

Nmap run completed -- 1 IP address (1 host up) scanned in
20945.334 seconds
```

The output above was from a full TCP SYN scan. The test failed because nmap found a port open that was not supposed to be: port 7 which is normally associated with the echo service. Echo is service used to diagnose problems and research did not identify any security risk associated with having this listening port. Future tests will accept this port being open. Also note that the Balancer does not respond with to scans to closed ports with “Reset” packets, which significantly slows scanning down. Future tests should take advantage of the timing options in nmap to improve performance.

```
# ./nmap -sU -n -v -p 1-65535 192.168.200.13
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-
26 10:36 EST
Host 192.168.200.13 appears to be up ... good.
Initiating UDP Scan against 192.168.200.13 at 10:36
The UDP Scan took 4735 seconds to scan 65535 ports.
(no udp responses received -- assuming all ports filtered)

All 65535 scanned ports on 192.168.200.13 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in
4735.099 seconds
```

This output shows the results of a UDP scan from nmap. No ports were open in this case, which was the expected result.

B2 Restrict simultaneous administrative sessions - PASS

```
MON> show security
  Security settings:
  ...
  console-cli-timeout      : 300
  telnet-cli-timeout       : 300
  ssh-cli-timeout          : 300
  minimum-password-length  : 8
  exclusive-rw-login       : True
  cli-login-banner         : custom
  custom-cli-banner        :

"Authorized use only.  All activity may be monitored and
reported."
```

The output above shows the Balancer configured to only permit one administration session at a time.

```
SEC> sh session

 Current Management Sessions:
  ...
  User Name       Access Level                    Method     IP
Address
                   (actual)        (requested)
  +---------------+---------------+---------------+----------+--------
----
 *"mikeh"         security-admin  security-admin  ssh        0.0.0.0
  "siteadmin"     monitor         security-admin  ssh        0.0.0.0

  ...2 sessions found.


SEC> sh session

 Current Management Sessions:
  ...
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  User Name       Access Level                    Method     IP
Address
                   (actual)        (requested)
  +---------------+---------------+---------------+----------+--------
----
 *"mikeh"         security-admin  security-admin  ssh        0.0.0.0
  "siteadmin"     monitor         security-admin  ssh        0.0.0.0
  "mikeh"         monitor         security-admin  web
192.168.200.47

  ...3 sessions found.


SEC> sh session

 Current Management Sessions:
  ...
  User Name       Access Level                    Method     IP
Address
                   (actual)        (requested)
  +---------------+---------------+---------------+----------+--------
----
 *"mikeh"         security-admin  security-admin  ssh        0.0.0.0
  "siteadmin"     security-admin  security-admin  console    0.0.0.0

  ...2 sessions found.
```

The output above shows the three different scenarios tested to verify the restrictions: at the top, a second SSH session that requested read-write access was only granted read permissions because another session was running. The middle test shows the same with the addition of a Web session. The last test shows the only case where concurrent read-write sessions are acceptable, and that is if the second is initiated at the console.

B4 Log all login attempts – FAIL

```
MON> show log event
2003-11-24 11:18:43  INFO <auth> Management Session 2 Started:
2003-11-24 11:18:43  INFO <auth>     User              : monitor
2003-11-24 11:18:43  INFO <auth>     Method            : SSH
2003-11-24 11:18:43  INFO <auth>     From IP Address   : 0.0.0.0
2003-11-24 11:18:43  INFO <auth>     Access Requested  : Monitor
2003-11-24 11:18:43  INFO <auth>     Access Granted    : Monitor
```

Above shows a successful SSH login

```
2003-11-24 12:10:24  WARN <auth> Local authorization rejected
for name: "monitor" from IP 0.0.0.0
```

While this is a failed SSH (bad password). This can be deduced because we know “monitor” is a valid account.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
2003-11-24 12:10:45  WARN <auth> Local authorization rejected
for name: "mark" from IP 0.0.0.0
```

This is a failed SSH (bad username). We know this because “mark” is not a valid username.

```
2003-11-24 10:16:24  INFO <auth> Management Session 1 Started:
2003-11-24 10:16:24  INFO <auth>     User              : monitor
2003-11-24 10:16:24  INFO <auth>     Method            : Web
2003-11-24 10:16:24  INFO <auth>     From IP Address   :
192.168.200.46
2003-11-24 10:16:24  INFO <auth>     Access Requested : Monitor
2003-11-24 10:16:24  INFO <auth>     Access Granted   : Monitor
```

Above is a successful TopViewSecure authentication

```
2003-11-24 10:10:21  WARN <auth> Local authorization rejected
for name: "monitor" from IP 192.168.200.46
```

Failed TopViewSecure (password)

```
2003-11-24 10:10:34  WARN <auth> Local authorization rejected
for name: "mark" from IP 192.168.200.46
```

Failed TopViewSecure (username)

```
2003-11-26 10:18:59  INFO <auth> Session 1 closed
2003-11-26 10:13:47  INFO <auth> Session 1 closed
```

Logout events, whether because the user quit the session (above) or the session timed out (below) were indistinguishable in the logs.

The test fails because the source IP address is not logged for SSH sessions. In addition to local logs, syslog logs and session information (available via “show session”) were checked to see if they reported properly. All produce the same result, a recorded IP address of 0.0.0.0. A support call was placed staff learned that this is a known issue that should be addressed in a future software release.

```
MON> show session

 Current Management Sessions:
  ...
  User Name       Access Level                    Method     IP
Address
                  (actual)        (requested)
  +--------------+---------------+---------------+----------+--------
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
----
 *"mikeh"         security-admin  security-admin  ssh        0.0.0.0
  "mikeh"         monitor         security-admin  web
192.168.200.46

  ...2 sessions found.
```

This shows the output of the session table.

B7 Send logs to a separate log server - PASS

```
MON> show syslog-host

  Host IP           Port       Admin     Facility
  +-----------------+----------+---------+-------

  192.168.200.51    514        enabled  local-0

MON> show log event
...
2003-11-24 14:14:44  INFO <auth> Management Session 1 Started:
2003-11-24 14:14:44  INFO <auth>     User             : monitor
2003-11-24 14:14:44  INFO <auth>     Method           : SSH
2003-11-24 14:14:44  INFO <auth>     From IP Address  : 0.0.0.0
2003-11-24 14:14:44  INFO <auth>     Access Requested : Monitor
2003-11-24 14:14:44  INFO <auth>     Access Granted   : Monitor
```

The section above shows local logs (on the Balancer) of a successful SSH login.

```
$ tail /var/adm/messages
...
Nov 24 14:14:45 [192.168.200.13.129.27] Management Session 1 Started:
Nov 24 14:14:45 [192.168.200.13.129.28]     User             : monitor
Nov 24 14:14:45 [192.168.200.13.129.29]     Method           : SSH
Nov 24 14:14:45 [192.168.200.13.129.30]     From IP Address  : 0.0.0.0
Nov 24 14:14:45 [192.168.200.13.129.31]     Access Requested : Monitor
Nov 24 14:14:45 [192.168.200.13.129.32]     Access Granted   : Monitor
Nov 24 14:14:45 [192.168.200.13.129.33] Security Alarm, User [monitor]
login successfully
```

This shows the logs on the syslog server of the same event.

This test shows the logs being successfully sent to the log server.

B8 Synchronize time to a reference clock - PASS

```
MON> show ntp

 NTP Settings:
  ...
  NTP Client :
   ...
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
   broadcast-delay     : 0
   query-interval      : 1020
   act-as-server       : Off
   query               : On
   receive-broadcasts  : Off
   send-broadcasts     : Off

  NTP servers :
   ...
   IP Address
   +--------------
   192.168.200.45
   192.168.200.40

  ...2 servers found.
```

This test shows the NTP configuration for the Balancer. Two time servers are specified and the synchronization interval is 17 minutes (1020 seconds).

Many NTP clients provide the ability to verify their operation. In Cisco IOS, for example, this can be accomplished this way:

```
SWITCH1#show ntp status
Clock is synchronized, stratum 3, reference is 192.168.200.45
nominal freq is 381.4697 Hz, actual freq is 381.4697 Hz, precision is
2**17
reference time is C312E1E1.4FCED152 (16:08:01.311 UTC Tue Nov 18 2003)
clock offset is 5.1680 msec, root delay is 12.57 msec
root dispersion is 30.53 msec, peer dispersion is 3.30 msec
SWITCH1#show ntp associations

      address         ref clock     st  when  poll reach  delay
offset    disp
*~192.168.200.45   10.10.10.100     2    22    64  377     1.6    5.17
3.3
 * master (synced), # master (unsynced), + selected, - candidate, ~
configured
```

In Solaris, it is possible this way:

```
$ /usr/sbin/ntpq
ntpq> peers
     remote           refid      st t when poll reach   delay   offset
disp
==============================================================================
========
*192.168.175.30      .GPS.       1 u  976 1024  377    10.99    0.523

ntpq> associations
ind assID status  conf reach auth condition  last_event cnt
===========================================================
  1 53076  f644   yes   yes   ok   sys.peer   reachable  4
```

Without the ability to run a similar test from the Balancer, the test selected was to run a sniffer on the NTP server and monitor for queries and responses. The

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

capture follows:

```
# ./tcpdump -n -X host 192.168.200.13 and port 123
tcpdump: listening on eri0


17:17:35.457778 192.168.200.13.8888 > 192.168.200.45.123:  v3 client
strat 0 poll 4 prec -6
0x0000   4500 004c 1346 0000 4011 55cf c0a8 c80d        E..L.F..@.U.....
0x0010   c0a8 c82d 22b8 007b 0038 188d db00 04fa        ...-"..{.8......
0x0020   0001 0000 0001 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000                                 ......
17:17:35.459091 192.168.200.45.123 > 192.168.200.13.8888:  v3 server
strat 2 poll 4 prec -15 (DF)
0x0000   4500 004c 96f9 4000 ff11 d31a c0a8 c82d        E..L..@........-
0x0010   c0a8 c80d 007b 22b8 0038 3035 1c02 04f1        .....{"..805....
0x0020   0000 0358 0000 05d9 bf09 c8fa c36f a395        ...X.........o..
0x0030   13bc 8000 3fc5                                 ....?.
17:34:33.760982 192.168.200.13.8888 > 192.168.200.45.123:  v3 client
strat 0 poll 4 prec -6
0x0000   4500 004c 1348 0000 4011 55cd c0a8 c80d        E..L.H..@.U.....
0x0010   c0a8 c82d 22b8 007b 0038 3545 db00 04fa        ...-"..{.85E....
0x0020   0001 0000 0001 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000                                 ......
17:34:33.762340 192.168.200.45.123 > 192.168.200.13.8888:  v3 server
strat 2 poll 4 prec -15 (DF)
0x0000   4500 004c 20ab 4000 ff11 4969 c0a8 c82d        E..L..@...Ii...-
0x0010   c0a8 c80d 007b 22b8 0038 8387 1c02 04f1        .....{"..8......
0x0020   0000 036f 0000 057d bf09 c8fa c36f a795        ...o...}.....o..
0x0030   1632 7000 3fc5                                 .2p.?.
17:51:31.874720 192.168.200.13.8888 > 192.168.200.45.123:  v3 client
strat 0 poll 4 prec -6
0x0000   4500 004c 134a 0000 4011 55cb c0a8 c80d        E..L.J..@.U.....
0x0010   c0a8 c82d 22b8 007b 0038 3aeb db00 04fa        ...-"..{.8:.....
0x0020   0001 0000 0001 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000                                 ......
17:51:31.876065 192.168.200.45.123 > 192.168.200.13.8888:  v3 server
strat 2 poll 4 prec -15 (DF)
0x0000   4500 004c a99f 4000 ff11 c074 c0a8 c82d        E..L..@....t...-
0x0010   c0a8 c80d 007b 22b8 0038 f000 1c02 04f1        .....{"..8......
0x0020   0000 02f7 0000 05c1 bf09 c8fa c36f ab95        ............o...
0x0030   0963 d000 3fc5                                 .c..?.
```

This packet capture shows the polling from the Balancer to the NTP server, and the responses. This, together with the observation that the clock appears to be accurate seems to verify that the clock is synchronizing properly.

C5 Ensure system is up-to-date on patches and updates - PASS

```
MON> show version

Top Layer Networks, Inc. IDS Balancer AS3510-TB
Build: Thu Jun  5 17:11:27 2003
Kernel Version: V2.20.007  Release State: PROD
Boot Rom Version: V3.01
```

The information above shows the running versions of all software on the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Balancer. After logging in to Top Layer's support Web site, the following information was retrieved from the section for downloading current software:

SOFTWARE RELEASE CODE/UPGRADE INSTRUCTIONS
Product: IDS Balancer **Software:** V2.20.007 **Date:** 6/10/03

The Balancer is running the current version of software.

C6 Install and verify the operation of a redundant power supply - PASS

```
MON> show environment
IDS Balancer Environmental Info:
Temperature : 27 degrees C
Fan 1 status : Running
Fan 2 status : Running
Power Supply 1 status: Working
Power Supply 2 status: Working


Dec 19 16:12:42 [192.168.200.13.128.254] Redundant Power
Failure, Power Supply 1
```

The test above shows the normal state of operation with both power supplies working properly. System stability was observed when either power supply was disconnected, and it continued operating properly. The last line above shows the log entry generated when the internal power supply (#1) fails. No logs are generated when the second power supply is disconnected.

Additional findings: port scan logging

A test that was not conducted but that should have been included based on an observation made during the audit was to check for log entries indicating attempted access using a denied method:

```
2003-11-24 10:49:48  WARN <Security>   HTTP management
connection from 192.168.200.76 blocked
2003-11-24 10:51:22  WARN <Security>    Previous message
repeated 1 times
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
2003-11-24 10:51:22  WARN <Security>   Telnet management
connection from 192.168.200.76 blocked
2003-11-24 10:53:28  WARN <Security>    Previous message
repeated 1 times
2003-11-24 10:55:03  WARN <Security>    Previous message
repeated 1 times
2003-11-24 10:55:03  WARN <Security>   HTTP management
connection from 192.168.200.76 blocked
2003-11-24 10:58:46  WARN <Security>    Previous message
repeated 1 times
2003-11-24 10:58:46  WARN <Security>   Telnet management
connection from 192.168.200.76 blocked
2003-11-24 11:01:53  WARN <Security>    Previous message
repeated 1 times
2003-11-24 11:01:53  WARN <Security>   HTTP management
connection from 192.168.200.76 blocked
2003-11-24 11:05:07  WARN <Security>    Previous message
repeated 3 times
2003-11-24 11:05:07  WARN <Security>   Telnet management
connection from 192.168.200.76 blocked
2003-11-24 11:09:05  WARN <Security>    Previous message
repeated 1 times
2003-11-24 11:09:05  WARN <Security>   SNMP management access
from 192.168.200.76 blocked
2003-11-24 11:18:43  INFO <Security>    Previous message
repeated 1 times
```

Additional findings: Old OpenSSH version

In test A4 above, a packet capture was presented showed the negotiation of encryption protocols between the Balancer and the management station. During the audit staff noticed that the Balancer is running a very old version of OpenSSH (version 2.9p2, which is highlighted in the listing above). A number of security problems have been discovered in OpenSSH since that version, as well as the supporting OpenSSL libraries of similar vintage.

This was initially both surprising and disconcerting, because it could add an unforseen risk to the system. Research in the TopLayer support pages and knowledge base revealed that this concern has been addressed in KB959, which states:

> "Top Layer products are not susceptible to the recently announce OpenSSH vulnerability (versions prior to 3.7.1) which appear to occur as a result of buffer management errors. Specifically, this is an issue with freeing the appropriate memory size on the heap, where in certain cases, the memory cleared is too large and might cause heap corruption."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This only addresses to the most recently discovered bugs, and references are made to the CERT and OpenSSH advisories. There is still some concern because other security flaws have been found since the version of OpenSSH running and they were not addressed.

Residual Risk

After conducting the audit staff has a much better understanding of the risks to the system as it will be deployed. An aspect of risk that remains unclear is the Balancer's susceptibility to attacks in the monitored traffic. The remaining vulnerabilities would generally require inside access to exploit. Each area of concern has had at least one corrective or compensating control applied, and future audits will ensure that system security is maintained at a high level.

The configuration of the Balancer, considering the architecture of GIAC's IDS deployment, addresses the identified risks as well as possible. The primary areas of residual risk are a potential exploit in the monitored traffic, an improper change to the cabling that exposes the IDS management network, exploit via the log server, or a hostile insider.

Concerns remain about the older versions of OpenSSH and OpenSSL that are running on the system, though these should be inaccessible to anyone except authorized administrators.

Some traffic remains unencrypted, though there is no alternative. The traffic is limited to the segregated IDS management network, and is key to the operation of the system.

Some logs lack detail about the source address of connections. Staff expects this to be remedied in a future release, and until then the type of access is tightly controlled.

Finally, there is no logging if the secondary power supply fails. Some potential solutions have been identified that would help automate detection of a failure and these will be investigated.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditability

The IDS Balancer is certainly auditable. A number of possible methods of performing the audit were identified. Although its configuration is different than other systems in use at GIAC, it took very little time to become familiar with it. This was aided by the fact that the configuration is simplified, with limited options.

It was nice that no performance validation test showed the system behaving differently than it was configured. The exceptions discovered are areas where the system cannot perform as desired, or the configuration is a compromise between different conflicting alternatives.

The cost of conducting the audit was minimal, and sufficient documentation has been developed to reduce future costs for maintaining the system.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Part IV: Report of Findings

Summary

The goal of this assessment was to determine whether or not the IDS Balancer was configured securely before adding it to GIAC's intrusion detection deployment. After identifying risks to the system, the configuration was checked against internal policy, published documentation, and industry best practices. The findings of the audit are that, while the system is not without risk, significant effort has been made to minimize the risk to the system and to GIAC Enterprises.

Report

IDS is deployed in GIAC's network as a component in the overall information security architecture. It reduces risk to corporate assets by providing a passive detection capability that alerts the security team when problems arise. It also adds significant logging capability (detail) that may significantly improve the response to any security incident by potentially reducing impact of an incident (help identify the scope of the intrusion which leads to an appropriate response – cleanup or bare metal wipe, which reduces downtime which saves money). It also provides sufficient evidence in case a legal action is taken against an attacker.

The Balancer contributes to a more effective IDS deployment by allowing more fidelity in logging and enabling application of multiple analysis methods to the same traffic. This will be crucial during the next phase of IDS, passive vulnerability analysis.

For all of this, GIAC is not in the business of providing IDS products or services. A disruption to this capability will not directly affect the company's ability to do business. It is not likely to interrupt operations or lose us customers. The cost involved is an indirect one that involves either additional staff time for response to an incident to the extreme case where an attacker disables the IDS function as a part of a larger attack. If that's the case, there likely is a direct cost to the company (lost revenue, compromised data, etc.), though it is not tied directly to the IDS.

The audit identified 28 individual controls to be put in place to either reduce or compensate for some risk to the system. The majority of the steps required to secure the Balancer were performed by the IDS team prior to the assessment, as

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

evidenced by 25 controls passing their tests.

Exceptions

A4: Encrypt Administrative Sessions
While normal administrative access to the Balancer is protected by encryption, two maintenance functions are not. One is used to for backups and upgrades, while the other is used to constantly send logs to a server.

Unencrypted protocols expose the system to risk because, if they are captured, an attacker may use the data they contain to gain access to or learn about the system. Although neither of these protocols are used to send passwords to the Balancer in the clear, they do contain configuration, status, and other sensitive information.

While there is currently no way to correct this weakness, access to the network where the Balancer is managed is tightly controlled and closely monitored. Staff will monitor future software releases for updates that would correct this. Other controls that help to reduce the risk posed by this exception are:

- A1: Segregate Management Traffic from the Corporate Network
- A2: Secure the Log Server (which is the gateway between the two networks)

A11: Ensure There are no Unneeded Listening Ports
Listening ports are a concern for security-sensitive systems because each one represents a service running on the system that could have vulnerabilities that an attacker could exploit. One unneeded listening port, echo, which is used for diagnosing network problems, was discovered. Unlike the administrative protocols (SSH, HTTPS, SNMP), this service cannot be disabled.

Research did not discover security problems in the echo service. Running this service does not represent a significant exposure and future tests will be modified to allow for this.

Other controls that help reduce the risk:

- A1: Segregate Management Traffic from the Corporate Network: even if a vulnerability were found in the echo service, the network segregation would make it difficult to exploit from outside GIAC's network.
- A2: Secure the Log Server

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

B4: Log All Login Attempts
The risk identified is that, if these events are not logged, someone may try endlessly to gain access to a system with no fear of being discovered. The only way to ensure that this does not happen is to log all significant events and ensure the logs are reviewed.

The Balancer does maintain logs for all successful and failed login attempts, but logs for certain kinds of connections do not contain some critical information – the source address of the connection. Staff contacted the vendor, they are aware of the issue, and they expect to address it in a future software update. That update will not cost GIAC as we have a maintenance agreement on the Balancer.

One possible workaround to this problem would be to disable the service that does not get logged properly. Unfortunately, that is the primary method staff intends to use to manage the Balancer, so the preference is to accept the risk. Some mitigating factors for this are:

- A1: Segregate Management Traffic from the Corporate Network
- A4: Encrypt Management Sessions
- A7: Restrict Sources of Administrative Sessions

As with the other exceptions, the inaccessibility of the management interface on the Balancer from other networks is a significant factor. The other considerations are that most management traffic, including all that contains authentication credentials, are encrypted. Further, the Balancer will only accept connections from a very narrow range of source addresses.

Additional Concerns

Some areas do not qualify as exceptions to the audit but are areas where some risk exists.

The following item is uncorrectable because it is unsupported in the current architecture:

Use strong authentication: the preferred control process for protecting

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

authentication in GIAC is to use ACE/Server, which is a token-based authentication scheme. The Balancer could likely make use of the ACE/Server, however that is not supported by the architecture of the network – the ACE/Server must be on the corporate intranet to use with other infrastructure and critical systems, while separating management functions of the IDS network is a high priority. In the end, it was considered preferable to keep the IDS management traffic segregated and accept weaker password protection than to make the systems more accessible with the benefits that would bring.

The following items are uncorrectable because they are unsupported in the product:

Enforce strong password protection (such as aging, complexity, and history): the preferred method of protecting authentication of critical systems is to use dual-factor authentication, as described above; when that is not possible for whatever reason, we fall back to normal "good password" practices such as minimum length, minimum and maximum aging, complexity, history, dictionary checks, etc. Of these, the Balancer only supports minimum length, which is not really sufficient (for example, with other controls in place, many people accept a minimum password length of eight characters; "password", one of the worst passwords to use (common use, dictionary word, etc.) passes the minimum length requirement.

Verify operation of redundant power supplies: although testing indicated that the unit functioned properly with only one (either) power supply functioning, log entries were only created when the primary power supply failed. The front panel of the unit does indicate the status of both power supplies, as does a "show environment". For now, this will be done procedurally. Staff is investigating the possibility of having the log server use SSH, with keys for authentication, log in and verify the operation on a cron job.

Authenticate time synchronization: messages between a time client and time server can be authenticated in order to ensure they are legitimate; although the risk of not using authenticated time synchronization is low, the cost of implementing it is sufficiently low that GIAC technical staff use it wherever possible. In this case, the Balancer does not support the feature, so we are willing to accept the risk.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1 http://www.toplayer.com
2 http://www.cisecurity.org/
3 https://store.sans.org/store_item.php?item=70
4 https://store.sans.org/store_item.php?item=93
5 Auditing Principles and Concepts, course material for day one of SANS' audit track; Hoelzer, David; pp. 1-20 – 1.21; 2003
6 http://www.sourcefire.com/products/rna.html
7 http://www.tenablesecurity.com/nevo.html
8 Miller, Jim; http://www.auditnet.org/docs/planning/riskevaluationform.pdf
9 *IDS Balancer Configuration and Management*, Top Layer Networks; May 2003, software version 2.2; part number 990-0072-03;
10 IDS Balancer Release Notes, Top Layer Networks; June 2003, software version 2.2; part number 990-0171-01
11 (Please note that access to some resources requires free registration) http://www.toplayer.com/content/resource/index.jsp
12 http://www.sans.org/rr/
13 http://www.giac.org/cert.php
14 http://www.cisecurity.org/
15 http://www.cve.mitre.org/about/
16 http://www.securityfocus.com/corporate/company/index.shtml
17http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0619
http://www.securityfocus.com/bid/1258
18 http://marc.theaimsgroup.com/
19 http://www.google.com/
20 SANS Institute Courseware 2003, Track 2 (Firewalls and Perimeter Protection) day 5 (VPNs), pages 173-180; written by Brenton, Elfering, Baccam, and Northcutt;
See also: *Inside Network Perimeter Security*, pages 210 – 216;

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.