Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Centralized Tracking and Risk Analysis of 3rd Party Firewall Connections

Firewall rules are a reflection of a company's security policies, business goals, and organizational changes. Enterprises must perform frequent audits to confirm that firewall rules align with strategic or operating changes. Managing the technical risks of a firewall must also be coordinated with an effort to effectively present these risks to management. In GIAC Enterprises, security leaders and auditors prioritized the need for individual business units to validate their existing external firewall connections. The go...

Copyright SANS Institute
Author Retains Full Rights

AD

# Centralized Tracking and Risk Analysis of 3rd Party Firewall Connections

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2 – Case Study in Information Security

Submitted By: Neeta Maniar
Submitted On: March 11, 2005

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

## TABLE OF CONTENTS


**Abstract** ..... **3**
**Executive Summary** ..... **3**
**Background** ..... **3**
Company Description ..... 3
Overview of Firewalls and Firewall Policy ..... 4
Defense in Depth at GIAC Enterprises ..... 4
**Before Snapshot** ..... **5**
**Approach** ..... Error! Bookmark not defined.
Solution Alternatives ..... 6
Solution Components ..... 7
3rd Party Firewall Dashboard Design ..... 8
Risk Analysis ..... 9
**Impact** ..... Error! Bookmark not defined.
Use Cases ..... 10
**Future Enhancements** ..... **10**
**Conclusion** ..... **11**
**References** ..... **11**
**Contributions** ..... **12**
**Appendix A: Process Map** ..... **13**
**Appendix B: Risk Analysis Matrix** ..... **14**
**Appendix C: 3rd Party Connections Dashboard View** ..... **15**
**Appendix D: Solution Alternatives Analysis** ..... **16**
**End Notes** ..... **17**


© SANS Institute 2005 Author retains full rights.

## Abstract

Firewall rules are a reflection of a company's security policies, business goals, and organizational changes. Enterprises must perform frequent audits to confirm that firewall rules align with strategic or operating changes. Managing the technical risks of a firewall must also be coordinated with an effort to effectively present these risks to management.

In GIAC Enterprises, security leaders and auditors prioritized the need for individual business units to validate their existing external firewall connections. The goal of this case study was to simplify the firewall ruleset validation process by creating a central database of rulesets that enables reporting on existing vendor connections. The overall impact included compliance with auditing requirements, a more robust risk assessment of firewall rulesets, and centralized visibility bringing about management response.

## Executive Summary

According to the 2004 Ernst & Young Global Information Security survey, only 20% of organizations view information security as a CEO level of priority[1]. As this survey reflects, the urgency in mitigating security risks is difficult to convey to upper management. Security teams must be diligent in not only identifying the technical risks, but in effectively presenting these risks to management. The more visibility and evidence that is provided to management, the greater chance they will prioritize security projects that will minimize risk. "As organizations move toward increasingly decentralized business models through outsourcing and other external partnerships, it becomes ever more difficult for them to retain control over the security of their information and for senior management to comprehend the level of risk to which they are exposed."[2]

GIAC Enterprises has a very decentralized structure. There are over ten business units, each of which has its divisions. Maintaining control of who has access to our internal network and critical assets becomes a daunting task. In GIAC Enterprises, security leaders and auditors have prioritized the need for individual business units to validate their existing external firewall connections. This paper provides the approach taken in GIAC Enterprises to 1) centralize all reporting of 3rd party vendor connections, and 2) provide a comprehensive risk analysis based on both technical and business risks.

## Background

<u>Company Description</u>

GIAC Enterprises is a global enterprise comprised of several business units, each of which interacts with many external vendors who require access to the

© SANS Institute 2005 Author retains full rights.

internal network. Each business unit has its own security leader, each of whom is informally responsible for reporting to the Global Security Leader in the Corporate division. In this decentralized environment where thousands of devices must be tightly secured, standardization of security policies and consistent tracking for compliance requirements is high priority among security leaders, upper management, and external auditors. It is a company-wide objective to centralize all the business unit firewall connections in a way that allows ease of reporting, especially to management.

Overview of Firewalls and Firewall Policy

In GIAC Enterprises, firewalls are a first layer of defense from perimeter attacks. In most implementations, firewalls filter packets and control flow of traffic in and out of the network. This paper focuses on inbound requests from external vendors to the GIAC Enterprises internal network. Firewall rulesets are configured to block most inbound requests with the exception of connections to external vendors initiated internally. These rules specify source IP, destination IP, port, action (accept/deny), and protocol for each connection. Not only do rulesets define the connection, they also reflect a company's security policies, business goals, and organizational changes. The National Institute of Standards and Technology (NIST) highly recommends that at the minimum, enterprises perform audits on a quarterly basis to confirm that their firewall rules align with strategic or operating changes[3]. The next section explains how auditing is a crucial part of GIAC Enterprise's Defense in Depth solution.

Defense in Depth at GIAC Enterprises

The principle of Defense in Depth states that multiple layers of protection should be used to protect critical devices on the network[4]. The GIAC Enterprises defense in depth begins with:

- Perimeter routers to filter out unwanted network traffic from the internet,
- Internet facing firewalls to control flow of traffic to DMZ and LAN,
- Firewalls in front of the GIAC Enterprises LAN to further filter traffic to the private network, and
- 3rd party Cisco PIX firewalls configured with inbound firewall rules from external vendors.

Intrusion prevention systems are also used to track and block malicious packets in transmission to our network. Additionally, company policy requires antivirus, host-based intrusion detection systems, and desktop firewall protection for those attacks that make it through the initial outer layers. Given that a security device is only as strong as its configuration, we can establish yet another layer of defense, which is the frequent auditing of critical devices that our defense in depth technologies are configured to protect.

© SANS Institute 2005 Author retains full rights.

In GIAC Enterprises, auditing requirements are carried out in accordance with the Sarbanes-Oxley Section 404 (SOX 404) government regulation, which requires companies to include in their annual reports a report of management on the company's internal control over financial reporting[5]. SOX 404 also requires an audit of these internal controls by an external auditor. Within GIAC Enterprises, SOX "Level 1" rating represents the most critical rating. It indicates that devices or systems interact with financial or strategic data. Since SOX Level Ratings take into account the value of an asset to the business, they are an essential component of the risk analysis carried out in this case study.

**Before**

A 2003 year-end audit indicated that GIAC Enterprises did not have a process to perform periodic reviews of its existing 3rd party firewall connections. It specified that a periodic review was required to verify that configurations and rule sets are conforming to the standards and to the original request approved by the business units.

Since this review, GIAC Enterprises has taken measures to begin tracking 3rd party firewall connections. The GIAC Enterprises global infrastructure team generated a monthly report per GIAC Enterprise business unit that included a technical risk analysis based on port for each 3rd party rule created. For the business units, these text-based, lengthy reports were difficult to manage and understand at a glance. Each business unit had to develop its own approach to translate raw firewall ruleset data into vendor-specific information that was more useful for internal reporting and business risk assessment. The original ruleset data provided to each business unit listed protocol type, source IP, destination IP, business, ports, and risk. This type of output brought with it several deficiencies and risks.

From a process perspective, each business unit had to either create a script or manually try to resolve each IP address to host names and vendor names. An additional effort was needed to add in business-specific descriptions and filtering capability that made the reports useful to management. This was a duplication of efforts to translate the initial output, which caused a loss in productivity across the company.

In terms of data requirements, the report did not include functional sponsor of each connection or the vendor name for the source. Expiration dates and mitigations for high-risk connections also were not being tracked. Additionally, there was not an easy way for businesses to tie each rule to business unit level projects or applications related to the connection.

From an auditing point of view, the original report contained a risk rating that did not factor in a weight for the SOX level, a key indicator used in the company to designate device/system criticality. Each business unit had to devise its own

© SANS Institute 2005 Author retains full rights.

process to integrate device risk with the associated firewall connection risk. Also, because the source vendor names were not being tracked, there was not an easy way to identify connections for unknown sources, which is a key auditing requirement.

The vulnerabilities that this case study addressed include expired open connections and untracked connections from unknown sources, both of which leave unnecessary exposure into our internal network. The threat we wanted to prevent was the compromise of critical data through these open connections. If an attacker were to exploit any of the high-risk open connections, the impact could be as damaging as the compromise of our most critical strategic or financial data. In this way, mitigating these risks through improved visibility to security teams was another step towards protecting the confidentiality, integrity, and availability of our assets[6].

**During**

Solution Alternatives

My goal for this project was to design an approach to simplify the 3rd party firewall ruleset validation process and to create a more robust risk assessment of these rules. See *Appendix D* for an analysis of the alternatives considered. In evaluating solutions, several factors were considered:

- If possible, the solution must leverage existing resources in the company to minimize costs and development work required
- The solution must significantly reduce the amount of manual work a business must do to interpret the ruleset reports for auditing requirements.
- Solution must provide flexible reporting both at a business level and company-wide.
- The vendors related to open connections must be tracked centrally.
- The solution must track business-specific parameters for auditing requirements.

One option was to modify initial firewall configuration report to include the additional required fields, such as vendor name, connection sponsor, and expiration date. The infrastructure team would store the resulting reports in a central doc management system accessible to each of the businesses. Each business would input their data into spreadsheet report for further filtering. As the firewall configurations are already highly unorganized, adding extra fields would increase the complexity. Business units would not have capability to directly manage changes to these fields when needed. Even though the reports would be in a central location, there would be limitations on reporting, and the business units would have to create their own method to filter and analyze thousands of rules in many cases.

© SANS Institute 2005 Author retains full rights.

Another option was to purchase a vendor solution. Research showed that there are some commercial solutions for enterprise reporting and managing of firewall rules. The interface used for advanced dashboard solutions such as Checkpoint's SmartCenter[7] can be used as benchmarks for our internal customization efforts towards business security dashboard reporting. For example, the SmartCenter solution provides hierarchical policy management, so reports on firewall rules can be viewed at the Corporate level or per business unit. Solsoft Security Reporter[8] is another dashboard that can map business processes to firewall configurations for compliance reporting. Solutions such as these require significant level of customization in our firewall environment, as well as a larger budget than was available.

The optimal solution was to feed reports from our risk analysis tool into a dashboard. Additional scripting in the dashboard would identify which vendor each connection was related to. Each business would then log in to view their vendor connections and add in business risk ratings. They would also retrieve reports by vendor, by IP address, by risk, and so forth. This is a much more flexible reporting solution requiring minimal effort from the business units. Despite the higher development costs, the benefits of improved reporting and reduction of duplicate tracking processes exceeds the cost. For this reason, a centralized dashboard design was the most acceptable solution meeting the requirements of the company security leaders and infrastructure team.

Solution Components

The solution is composed of a dashboard-like interface which presents the information in a central database, and a risk analysis calculation based on National Institute of Standards and Technology (NIST) guidelines. The resources and tools used included:

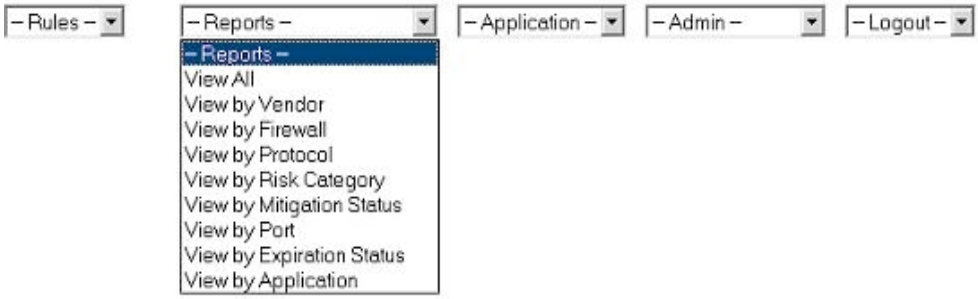
- Firewall Risk Analysis Tool[9]: The GIAC Enterprises infrastructure team developed a tool that assigns a technical risk rating for the firewall rulesets of each business. The risk tool identifies severity levels by checking for high-risk ports. *Appendix B* shows a risk analysis matrix used to define criteria for these ratings. The risk rating from this tool is factored into the overall risk rating discussed in the Risk Analysis section of this paper.
- 3rd Party Connections Dashboard[10]: The backend for the dashboard is a database storing the 3rd party rulesets for all the business units. Through the front-end web application, business users can view reports of their specific connections.
- ARIN/DNS script[10]: This script will map source IPs to vendor using the American Registry for Internet Numbers (ARIN)[11], which is an Internet registry that enables IP address queries. The DNS script will map destination IPs to host names. This will make it easier to quickly discern the server/targets for these rules.

© SANS Institute 2005 Author retains full rights.

To view how all of these components work together, see *Appendix A*. The output from the Firewall Risk Analysis tool is parsed by the ARIN/DNS lookup script, and then feeds into the dashboard database. All the rulesets are separated by business, so that each user logging in can view only the rulesets for his business. At the Corporate level, the reports can be rolled up for a company-wide view of all the 3rd party connections.

**3rd Party Firewall Dashboard Design**

The dashboard application provides the interface to the central database. The database contains the 3rd party ruleset configuration data for all the businesses, and the associated vendors and applications. Upon logging in, a user is authenticated and authorized to view only the data specific to his or her business. At the Corporate level, an admin user can view connection data for the whole company. The dashboard application is designed with the following menu options:




Through the dashboard, a business user can perform the following functions:

<u>View Reports</u>

View reports by any category and drill down to see specific rule configuration detail. For example, users can view a list of unique vendors and number of connections per vendor. From there, they can drill down from vendor name to see all associated rulesets with that vendor. See *Appendix C* for the lowest level detail report.

<u>Update/Add New Application Data</u>

Enter in the names of any applications and related Sarbanes-Oxley levels, which can later be tied into the 3rd party connections. The GIAC Enterprise business units assign various SOX Levels to applications, and these applications may be mapped to projects. It's essential that these firewall rules can be associated with applications so that they can later be factored into business level risk analyses.

© SANS Institute 2005 Author retains full rights.

Update Rules

Filter the rules according to any field, and apply updates to a connection or group of connections. At the lowest level report, a user can specify mitigation actions, connection sponsors, expiration dates, descriptions of which projects the rulesets are associated with, and Sarbanes-Oxley (SOX) Levels for the connections. If a user enters in a SOX Level, this is calculated into the total risk level, which is discussed in the Risk Analysis section of this paper.

**Risk Analysis**

The risk analysis for this case study merges both business-defined risk ratings and the technical risks assigned by infrastructure teams. According to NIST, "…the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization."[12]

The NIST components for carrying out a Risk Analysis are[13]:

1) Threat : The potential for a threat source to exploit a vulnerability. The threats that untracked, unnecessary open connections may cause include potential DOS attacks on exposed critical systems, potential unauthorized control of critical system, and potential compromise of sensitive GIAC Enterprises data.
2) Vulnerability : Flaw or weakness in system security. The vulnerability in this study includes open third party connections that are expired, have high exposure levels, and have no mitigation.
3) Likelihood: Capability level of the threat source and the controls in place to prevent compromise. We measure likelihood by exposure level and mitigation. High exposure level and no mitigation results in a high threat likelihood.
4) Impact: Damage a compromise of information assets would cause, based on criticality of those assets. The impact as defined by the business units includes device SOX Level ratings. A SOX Level 1 would be assigned a high impact rating.
5) *Risk:* Function of likelihood of a given threat exploiting vulnerability, and the resulting impact of the exploit on the organization.

Given a formula[14] where Risk = Threat Likelihood x Impact, the calculated risk assessment for GIAC Enterprises 3rd party firewall connections is:

Risk = (Exposure Level x Mitigation Rating) x SOX Level

- Exposure Level: High = 5, Medium=3, and Low=1.
- Mitigation: Unmitigated=5, Mitigated=0, and In Progress=3
- SOX Level: Level 1= 5, Level 2=3, Level 3= 1

© SANS Institute 2005 Author retains full rights.

If a connection has an exposure level of 5 (high risk port), a mitigation rating of 5 (no mitigation associated with the ruleset), and a SOX Level rating of 5 (Level 1 device criticality), the resulting risk value would be 125, which indicates the most high risk connection given all the factors.

**After**

Use Cases

There are several cases where a business unit leader requires these dashboard reports to make a decision. For example, in many cases, rulesets cannot be mapped to a known source, or vendor. In one scenario, a business indicated that they wanted to filter all the rulesets by the ones that are unknown, and specify that all of these are from a particular vendor. Another security leader needed the dashboard to apply specific mitigation actions to a ruleset that has been expired, was mitigated, or has a high-risk port open. Once a user has noticed that a ruleset has expired, the decision would be to either submit a request to terminate the connection, or enter in a new expiration date. Also, if a new vulnerability is identified that affects a specific port, a security leader can quickly check if that port has an open external connection and take the necessary precautions. A business can associate various rules to related projects, and then do a quick search to retrieve all the rules applying to a given project.

Another use case relates to SOX 404 compliance. Two key metrics for the company's Sarbanes Oxley IT 404 requirements are 1) the total number of 3rd party connections, and 2) the total number of connections that are not audited or resolved to a vendor. By referring to the dashboard, a business can view how many total existing 3rd party connections it has, as well as how many rulesets there are with unknown connections. In this way, this solution helps to meet the internal auditing requirements as well.

Overall, this solution impacts several areas of the organization. It ensures compliance with SOX requirements to measure and track 3rd party firewall connections. It centralizes visibility into 3rd party connections enabling management to form solid decisions based on known facts. It integrates the SOX Level device ratings with the more technical exposure levels based on port analysis. At a high level, this solution improves management of firewall rulesets across the company, which will in turn lowers the risk to our most critical assets.

**Future Enhancements**

This dashboard was one effort to centralize reports across the company, but there are several other places in our Defense in Depth strategy where there is an opportunity to further integrate reporting and alerting. In later phases of this solution, the goal will be to correlate high risk 3rd party connections with other

© SANS Institute 2005 Author retains full rights.

systems, such as the intrusion prevention systems and firewall alerts. To make the process more efficient, we can add an alerting mechanism to notify business units when their high-risk connections have expired. Another area of improvement may also be the risk analysis. I would like to further define the list of ports and risk levels based on services used by those ports. Finally, an improvement area that would help to simplify security metrics reporting is to integrate the company's existing security metrics dashboard with the dashboard created for this case study.

**Conclusion**

In summary, GIAC Enterprises had a need for a more measurable, centralized solution for managing 3rd party firewall rulesets. Building upon existing company toolsets and applying industry standards such as NIST, this case study resulted in a dashboard reporting 3rd party connections from a centralized storage base. Not only did this solution improve visibility to upper management and external auditors, it simplified the process of tracking rulesets for each business unit. With this better visibility, the security teams across the company can track their open 3rd party connections and take the appropriate actions, thus reducing the risk to our most critical assets. Future generations of this solution will focus on integrating these reports with other security systems in GIAC Enterprises, and further improving the risk analysis.

**References**

Check Point Software Technologies Ltd. SmartCenter/SmartCenter Pro. 2004. <http://www.checkpoint.com/products/downloads/smartcenter_datasheet.pdf>

Erst & Young. Global Information Security Survey 2004. <http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf>.

Ernst & Young. "CEOs Aware, but Not Acting on Threats to Information Security." September 23, 2004. <http://www.ey.com/GLOBAL/content.nsf/International/Press_Release_-_2004_Global_Information_Security_Survey>.

SANS Institute. Track 1- SANS Security Essentials Defense-in-Depth. Volume 1.2. SANS Press, Sept 2004.

SANS Institute. Track 1- SANS Security Essentials Networking Concepts. Volume 1.1. SANS Press, Sept 2004.

Solsoft Inc. Security Intelligence for Complex Networks. 1997-2005. <http://www.solsoft.com/pages/formulaire/formulaire.php?id=1394>

© SANS Institute 2005 Author retains full rights.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. January 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

United States. Securities and Exchange Commission. "SEC Implements Internal Control Provisions of Sarbanes-Oxley Act; Adopts Investment Company R&D Safe Harbor." 2003-66. Washington D.C. May 27, 2003. <http://www.sec.gov/news/press/2003-66.htm>.

Wack, John, Ken Cutler, Jamie Pole. Guidelines on Firewalls and Firewall Policy. January 2002. <http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>

American Registry for Internet Numbers. WHOIS Help. <http://www.arin.net/tools/whois_help.html>

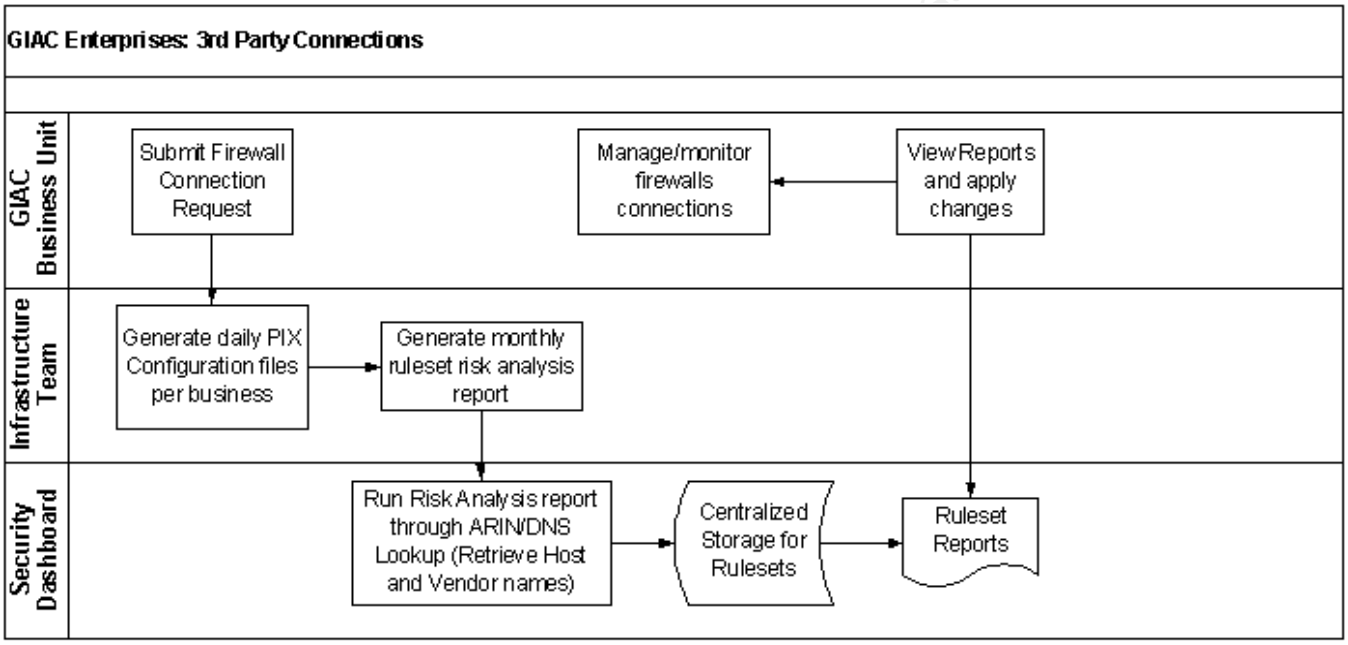
**Contributions**

My individual contributions to this project included the requirements gathering, research, analysis, design, overall risk assessment, and project management for the development. A member of the GIAC Enterprises Infrastructure team had coded the risk analysis tool that was leveraged for the final risk analysis for this case study. A member of the GIAC Enterprises security development team provided technical assistance and scripting required for the security dashboard application.

© SANS Institute 2005, Author retains full rights.

## Appendix A: Process Map

This diagram represents the new process of storing the rulesets centrally in the security dashboard for viewability to each business unit. The original process sent a report directly from the infrastructure team to the business units.




© SANS Institute 2005 Author retains full rights.

## Appendix B: Risk Analysis Matrix

The GIAC Enterprises infrastructure team developed a tool that outputs a risk rating for the firewall rulesets of each business. This port risk analysis is included in the final risk assessment output of this project. The risk matrix used identifies a risk level of High, Medium, or Low based on port protocol, and service type. This was a subjective assessment based on the infrastructure team's standards. See a sample of the risk matrix used below:

| Risk Matrix | | | |
|---|---|---|---|
| Name | Protocol | Description | 3rd->LAN |
| | 0/tcp | Reserved | Explain |
| | 0/udp | Reserved | Explain |
| tcpmux | 1/tcp | TCP Port Service Multiplexer | Explain |
| tcpmux | 1/udp | TCP Port Service Multiplexer | Explain |
| compressnet | 2/tcp | Management Utility | Explain |
| compressnet | 2/udp | Management Utility | Explain |
| compressnet | 3/tcp | Compression Process | Explain |
| compressnet | 3/udp | Compression Process | Explain |
| rje | 5/tcp | Remote Job Entry | Explain |
| rje | 5/udp | Remote Job Entry | Explain |
| echo | 7/tcp | Echo | Explain |
| echo | 7/udp | Echo | Explain |
| discard | 9/tcp | Discard | Explain |
| discard | 9/udp | Discard | Explain |
| systat | 11/tcp | Active Users | Explain |
| systat | 11/udp | Active Users | Explain |
| daytime | 13/tcp | Daytime (RFC 867) | Explain |
| daytime | 13/udp | Daytime (RFC 867) | Explain |
| qotd | 17/tcp | Quote of the Day | Explain |
| qotd | 17/udp | Quote of the Day | Explain |
| msp | 18/tcp | Message Send Protocol | Explain |
| msp | 18/udp | Message Send Protocol | Explain |
| chargen | 19/tcp | Character Generator | Explain |
| chargen | 19/udp | Character Generator | Explain |
| ftp-data | 20/tcp | File Transfer [Default Data] | Medium |
| ftp-data ftp | 20/tcp | File Transfer [Default Data] | Medium |
| ftp-data | 20/udp | File Transfer [Default Data] | High |
| ftp | 21/tcp | File Transfer [Control] | Medium |
| ftp | 21/udp | File Transfer [Control] | High |
| ssh | 22/tcp | SSH Remote Login Protocol | Medium |
| ssh | 22/udp | SSH Remote Login Protocol | High |
| scp | 22/tcp | SSH/SCP Secure Copy | Medium |
| telnet | 23/tcp | Telnet | Medium |
| telnet | 23/udp | Telnet | High |
| | 24/tcp | any private mail system | Explain |
| | 24/udp | any private mail system | Explain |
| smtp | 25/tcp | Simple Mail Transfer (Sendmail) | Extreme |
| smtp | 25/udp | Simple Mail Transfer | Explain |
| nsw-fe | 27/tcp | NSW User System FE | Explain |
| nsw-fe | 27/udp | NSW User System FE | Explain |
| msg-icp | 29/tcp | MSG ICP | Explain |

© SANS Institute 2005 Author retains full rights.

## Appendix C: 3rd Party Connections Dashboard View

User can filter rulesets by any field. Also sort by clicking on category name.

User can click on app name to see details (SOX Level, description, sponsor, exp date).

3rd Party Connections: GIAC Enterprises Business Unit A

| | Firewall | Description | Source IP | Vendor | Dest IP | DNS Name | Port | Protocol | Exposure Level | Application | Expiration | Status | Mitigation Details | Overall Risk |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Search | firewall1 | | 4.5.6.0/24 | * | * | * | * | * | High ^ | * | * | Unmitigated^ | * | High ^ |
| | firewall1 | Sub-business | 4.5.6.0 | Vendor A | 1.2.3.4 | test.com | 80 | tcp/ip | High | TestApp | 2/16/2005 | Mitigated | Removed Connection | Medium |
| | firewall1 | Sub-business | 4.5.6.1 | Vendor A | | | | | High | TestApp | 2/16/2005 | Unmitigated | | High |
| | firewall1 | Sub-business | 4.5.6.2 | Vendor A | | | | | High | TestApp | 2/16/2005 | Unmitigated | | High |
| | firewall1 | Sub-business | 4.5.6.3 | Vendor A | | | | | High | TestApp | 2/16/2005 | Unmitigated | | High |
| | firewall1 | Sub-business | 4.5.6.4 | Vendor A | | | | | High | TestApp | 2/16/2005 | Unmitigated | | High |
| | firewall1 | Sub-business | 4.5.6.5 | Vendor A | | | | | High | TestApp | 2/16/2005 | Unmitigated | | High |
| | firewall1 | Sub-business | 4.5.6.6 | Vendor A | | | | | High | TestApp | 2/16/2005 | Unmitigated | | High |
| | firewall1 | Sub-business | 4.5.6.7 | Vendor A | | | | | High | TestApp | 2/16/2005 | Unmitigated | | High |
| | | | | | | | | | | | | | | High |
| | | Sub-business | | Vendor A | | | | | | TestApp | 2/16/2005 | Unmitigated | | |
| | | Insert Description | | Select Vendor | | | | | | Select App | Insert Expiration Date | Select Status | Insert Mitigation Details | |
| | | Set | | Set | | | | | | Set | Set | Set | Set | |

Submit Changes  Cancel

User can set a selected group of rules to be updated with vendor, application, expiration, mitigation status, or mitigation details.

© SANS Institute 2005 Author retains full rights.

## Appendix D: Solution Alternatives Analysis

| | | Solution Alternatives<br>5=Meets requirement, 3=Partially meets requirement, 1=Does not meet requirement | | |
|---|---|---|---|---|
| **Requirement** | **Description** | Modify Firewall Config Business Report to include required fields.Store Report in central doc management sytem. | Build New Dashboard Application (Leverage Existing Security Dashboard Backend) | Commercial Dashboard Solution |
| Centralized tracking/management of vendor connections | Centralized storage of 3rd party vendors and related rulesets. | 3 | 5 | 5 |
| Provide ease of Implementation | Development work should not take more than a few months. If possible, levereage existing resources. | 3 | 3 | 1 |
| Provide flexible reporting, at both a business unit level and company-wide level | Filter by various fields in the configurations, for example see all rulesets by vendor or by risk. | 3 | 5 | 5 |
| Cost-effective | Leverage existing resources to reduce cost. Outsource for any coding, or use internal dev resources. | 5 | 3 | 1 |
| Track business-specific parameters for auditing | SOX Level, expiration date, connection sponsor, mitigation actions, project description | 3 | 5 | 3 |
| | | 17 | 21 | 15 |

For the second option, though it may cost extra with development, the benefits of improved reporting and reduction of duplicate tracking processes exceeds the cost.

© SANS Institute 2005 Author retains full rights.

**End Notes**

[1] Ernst & Young. Global Information Security Survey 2004. Pg 3

[2] Ernst & Young. "CEOs Aware, but Not Acting on Threats to Information Security."

[3] Wack, John, Ken Cutler, Jamie Pole. Guidelines on Firewalls and Firewall Policy. Pg 37.

[4] SANS Institute. Track 1- SANS Security Essentials Defense-in-Depth. Pg 12.

[5] United States. Securities and Exchange Commission. "SEC Implements Internal Control Provisions of Sarbanes-Oxley Act; Adopts Investment Company R&D Safe Harbor."

[6] SANS Institute. Track 1- SANS Security Essentials Defense-in-Depth. Pg 14-15.

[7] Check Point Software Technologies Ltd. SmartCenter/SmartCenter Pro.

[8] Solsoft Inc. Security Intelligence for Complex Networks.

[9] The Firewall Risk Analysis Tool was created by a member of the GIAC Enterprises infrastructure team.

[10] The ARIN/DNS Script and dashboard application was coded by a member of the GIAC Enterprises security team.

[11] American Registry for Internet Numbers. WHOIS Help.

[12] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Pg 7.

[13] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Pg 12-15.

[14] Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Pg 24.

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Last Updated: May 24th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Malaysia @ MCMC 2013 | Cyberjaya, MY | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| SANS Pen Test Berlin 2013 | Berlin, DE | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| Industial Control Systems Security Training - Houston | Houston, TXUS | Jun 10, 2013 - Jun 15, 2013 | Live Event |
| Security Impact of IPv6 Summit 2013 | Washington, DCUS | Jun 14, 2013 - Jun 16, 2013 | Live Event |
| SANSFIRE 2013 | Washington, DCUS | Jun 14, 2013 - Jun 22, 2013 | Live Event |
| SANS Canberra 2013 | Canberra, AU | Jul 01, 2013 - Jul 13, 2013 | Live Event |
| Digital Forensics & Incident Response Summit 2013 | Austin, TXUS | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS London Summer 2013 | London, GB | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS Rocky Mountain 2013 | Denver, COUS | Jul 14, 2013 - Jul 20, 2013 | Live Event |
| SANS Mumbai 2013 | Mumbai, IN | Jul 22, 2013 - Jul 27, 2013 | Live Event |
| SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification | Washington, DCUS | Jul 22, 2013 - Jul 26, 2013 | Live Event |
| SANS San Francisco 2013 | San Francisco, CAUS | Jul 29, 2013 - Aug 03, 2013 | Live Event |
| SANS SEC 560: Network Penetration Testing @ Bangalore 2013 | Bangalore, IN | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| SANS Boston 2013 | Boston, MAUS | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| Critical Security Controls Summit | Washington, DCUS | Aug 12, 2013 - Aug 18, 2013 | Live Event |
| Industrial Control Systems Security Training - DC | Washington, DCUS | Aug 12, 2013 - Aug 16, 2013 | Live Event |
| SANS Thailand 2013 | Bangkok, TH | Aug 19, 2013 - Aug 31, 2013 | Live Event |
| SANS Virginia Beach 2013 | Virginia Beach, VAUS | Aug 19, 2013 - Aug 30, 2013 | Live Event |
| Mobile Device Security Summit 2013 | OnlineCAUS | May 30, 2013 - Jun 06, 2013 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |