Paul Maschak
June 22, 2003
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4B - Option 1

Title: Change Control Process for Firewalls

Abstract

Change is one of the inevitable facts of life we must deal with. Firewall objects and rulesets are constantly evolving in response to new threats, vulnerabilities and services. In order to provide defined Service Level Agreements to our Information Technology customers we are required to maximize availability while maintaining confidentiality and integrity of corporate data assets. As we adapt new enabling technologies for our customers' growing business requirements a high level of internal security must be maintained.

absolutely security minded administrator) to hundreds of rules with thousands of objects for a diverse organization. CC practices become essential in environments where firewall rules and objects grow beyond a simple few. From my experience caution is warranted in that the predictability of results from a change decreases rapidly as the number of rules and objects increase in complexity. A FW change may create effects which are difficult to predict given limited time constraints and resources necessary for implementation to satisfy a customer's requirements.

Working for an international corporation operating 24/7 with follow-the-sun firewall support teams necessitates solid communication with strict adherence to the control of any implemented changes. Solid methods for information transfer of change details must be available between Security Administrators (SA's) as it may not be possible to make direct contact with customers reporting a problem or even other SA's involved in a change. Failure to work within the boundaries of the CCP can have terrible consequences for not only the SA but IT customers as well.

Our multiple firewalls over time have developed into complex rulesets (over 350 rules) and thousands of objects. Some readers may even comment this is far too large to manage and a rule reduction using CC methods is called for. "The more rules you have, the more likely you or someone else will make a mistake". [3] I will personally attest to having made mistakes so that "someone else" just might be me. Even a simple typographical error can have dramatic effects such as disabling an unwanted IP address range.

FW changes may extend over multiple SA shifts and be completed by another SA team. In an effort to minimize interruptions of active services FW changes tend to be pushed during quiet hours or scheduled maintenance windows. Frequently the impacts of a change made by one SA are observed in logs or called into the Help Desk by affected customers well after the initiating SA has left for home. Inspection of FW logs alone may be insufficient in determining incident cause and resolution thus maintaining solid change documentation for review will assist in timely solutions.

Maintaining firm cost control has become very prevalent for businesses especially now during this economic downturn. Every attempt to judiciously allocate resources helps the bottom line. During the initial stages of CC process a change request is assessed with respect to risks, impact, costs, business case and priority so that a management decision whether to proceed or not can be made before committing valuable resources. [4] Without having controls in place it is easy to waste valuable finite resources.

Service Level Agreements (SLA's) define the IT services and under which conditions they are provided to customers. A Service Catalogue is the repository for all SLA's. Having a clear definition of what IT is providing to the customer through an SLA reduces the possibility of confusion and mistaken expectations while maintaining fairness for all parties. "The SLA defines the roles of both the client and the provider. As a result, the client understands exactly what they are expected to do and what the provider is agreeing to do on the client's behalf. The SLA should be as precise as possible." [5]

Furthermore, I have found that a written end-user oriented IT reference guide translating specific details and reasonable expectations of SLA's to be invaluable during the change procedure should a user's request be denied. Since the customer always has the right to appeal a denied request, management endorsed SLA's may prove to be very valuable in pre-empting unwanted confrontations. The onus of creating a justified business case will then lie squarely with the customer.

If services are created, modified or removed by implementing a change then the SLA must be amended. This is one of the final steps of CC. Please ensure documentation including SLA's, reference guides, etc. are always up to date!

Requirements of Change Control

I have separated CC requirements into 4 categories: Organization, Trouble Ticket system, Firewall and Document Revision Control System (RCS). This list is by no means an exhaustive one but rather a guideline for individuals to decide what level is appropriate in their implementation of a CC environment.

RCS practices have long been associated with software development and most UNIX installations are delivered with either RCS or Source Code Control System (SCCS) [6]. User comfort level will dictate which version control systems are used as they are equally adequate in tracking changes. I highly recommend further research on the Internet to gain knowledge on how to use RCS/SCCS or alternatively read the first 4 chapters of "Applying RCS and SCCS" by Don Bolinger & Tan Bronson. Even though the book was written in 1995 the principles of version control have remained stable.

- Organizational Requirements:
  - management buy-in and support of CCP and security practices
  - adherence by SA's to work in accordance with CCP
  - SLA to be published and maintained
  - published end-user guide explaining the SLA
  - If ISO 9000-3 is a corporate requirement then change management procedures must be complied with (seek assistance from you Quality Assurance personnel)
  - Clearly define responsibilities and authorities for all persons involved in the change process
- Trouble Ticket (TT) system:
  - system to track changes, incidents and request for services (RFS) – this may range from a full enterprise level helpdesk system to a simple data base
  - maintain a history of implemented changes in the TT
  - relate changes to specific person or in the case of a service the affected Service Owner

tie in of the TT system to a Configuration Management Database -CMDB to provide additional configuration details specific to the end user (i.e. hardware assets, operating system, user location…)
allow for multi-user update and retrieval of information

- Firewall
  restrict modification to rules, objects and services to one SA at a time
  strict adherence to procedure will prevent multiple simultaneous modifications to a Firewall rule base if not available as part of the FW software
  archiving of previous rule sets
  list the changes made with each revision
  store multiple versions of Firewall configuration data
  browser enabled rulesets, objects and services
  report revision history
  roll back changes to a prior state
  enable multi-site support
- Document RCS - “Thi

- following CMP helps to guarantee integrity of information
- maintain availability of resources for needed by customers for business operations
- implement Security “best practices”
- CC practices assist with compliance of ISO 9000-3 part 6.1.3.2
- maintain SLA levels for the customer
- satisfy and service customer business needs in a timely manner
- eliminate changes that do not meet written Security Policy guidelines
- minimize the risks of altered, stolen, inaccurate, destroyed data. Set baseline rules and standards to optimize confidentiality and integrity of the company
- it is not realistic for any SA to be able to remember all changes made to a firewall rule set
- audit changes made with the ability to review historical changes.
- following CC management procedures help maintain network security with the integrity of information
- partners requesting connectivity frequently request proof of SP and CCP before allowing network connectivity
- a centralized repository for documentation of changes
- ability to continue change process over multiple SA’s
- backup of previous rule sets
- protect intellectual property
- “Tying in an approval Process to the change tracking process ensures that changes receive authorization before they are put into production, thereby enabling users to improve the quality of their delivered product” [7]

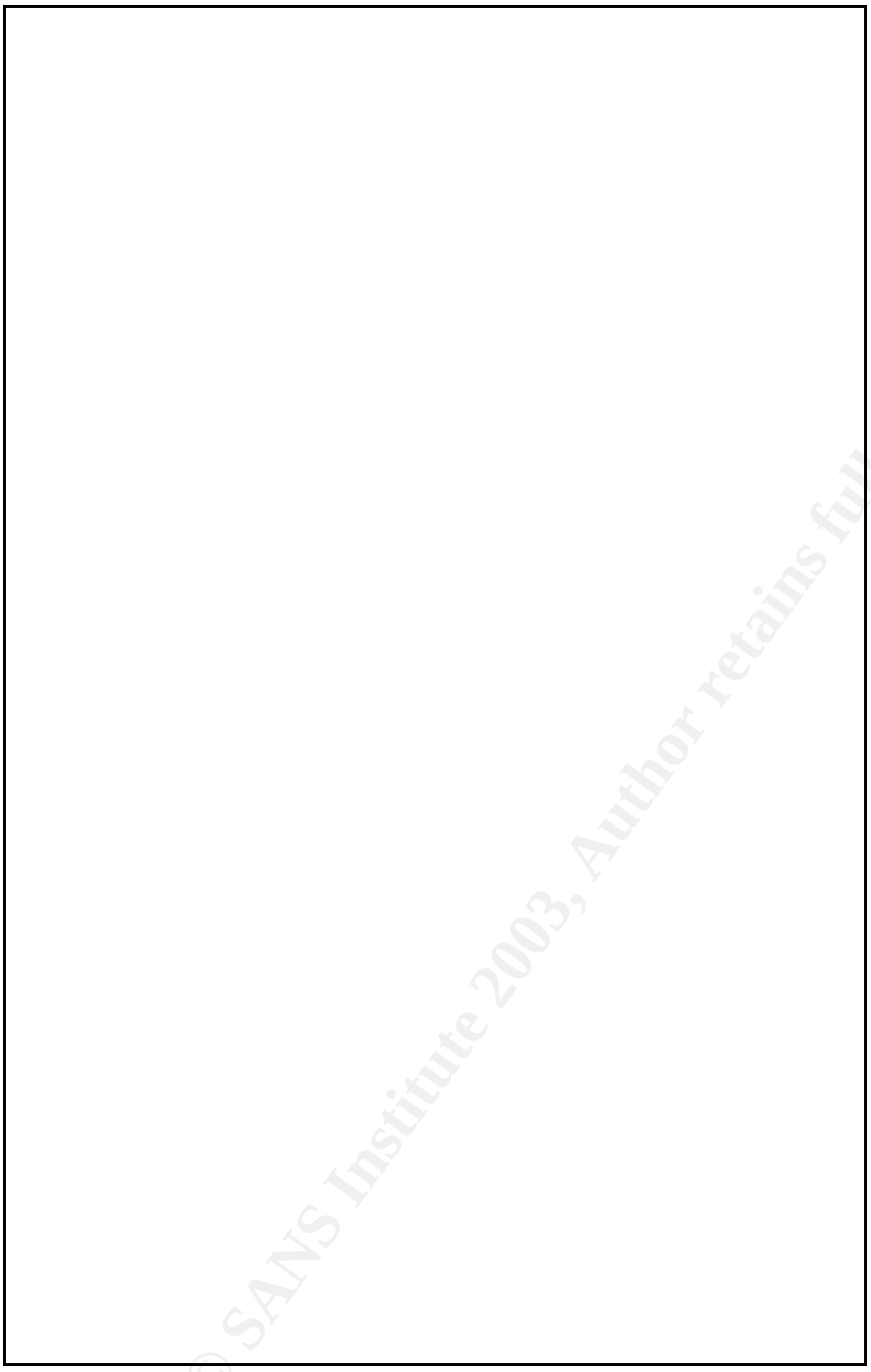
Overview of Change Process

The change process may be divided into 2 categories: General and Crisis/Emergencies. General Changes, if warranted, may require an additional stage of creating a Change Plan (see Appendix A) and a formal approval process through a Change Control Board.

General Change Process:
Step

a member of the firewall support team for the Integrity of the change with regards to:

a. Is there a justified business case exists to support the change. If necessary they will consult management or information owner for approval
b. Risk assessment impact to both existing risks and new risks that would be created by the change. Quantify the risk into High/Medium/Low. “Assign all potential changes a risk prior to scheduling the change… Identify risk levels for software and hardware upgrades, topology changes, routing changes, configuration changes …Assign higher risk levels to non-standard add, move, or change types of activity.” [8]
c. Time and cost analysis – are there sufficient funds and



Flow Diagram – General Change Process

Overview of Change Process – Emergency/Crisis Change:

A crisis occurs when SLA's can not be maintained within the time limits as agreed upon in the document. The Crisis Manager (CM) is appointed and placed in charge of resolving the situation. CM is given the responsibility and granted resources necessary to resolve the issues during the emergency. It is important to note that all activities are required to be logged throughout the duration of the crisis.

Step	Activity
1.	Help desk or Information owner submits a critical incident. (An information owner is defined as the person responsible for an application)
2.	To track the request the Help desk creates a Trouble Ticket (TT), notifies FW duty person and Crisis Manager. The Crisis Manager retains control of the TT through to resolution of the incident and is responsible for organizing all forces necessary to solve the crisis.
3.	FW team with assistance of the Crisis Manager perform a. a limited risk assessment and a priority level (1.Calamity, 2.Urgent, 3.High, 4.Medium, 5.Low) which is based on: I. urgency – the number of affected users II. severity – importance of a service for business processes b. Inventory – register all facts and activities that have led up to the crisis c. list all potential causes that could have created the crisis
4.	Crisis Manager initiates communication with appropriate affected managers.
5.	FW team tests, evaluates and documents the required change
6.	FW team implements change and pushes out new FW rulebase
7.	FW team reviews and monitors the

Flow Diagram – Emergency/Crisis Change Process

Conclusion

The extent that you incorporate Change Control largely depends upon your needs. For some there will be no choice as those decisions have been made prior to your start of employment. Others will be able to pick and choose what and how to implement. The benefits of change practices must be carefully weighed against the costs of implementation with the risks of partial solutions. It is essential that there is complete buy-in from all levels of management otherwise you may be easily stopped or thwarted.

Change control is itself subject to change and review. When you audit for security also ensure that the change processes and procedures are reviewed. The most important issue of all is solid documentation. This will enable all security administrators to identify problems and analyze the operation of the firewall now and in the future. The concept of job security through obscurity really is not applicable when it comes to firewalls. By increasing your efficiency you will have time to address more important and hopefully interesting issues rather than have to figure out entire functional operations time and time again.

Change Control practices enable you to peel back layers of change much like an onion and throw out the bad layers. Hopefully during this process you won't shed too many tears. Now is an excellent time to begin putting together Change Control Process to protect the availability, confidentiality and integrity of your infrastructure.

o happen

ges

hat the

ny expected

Remarks
DONE

9.61 119.04 219.36 Tm 0 Tc 0 Tw (

Technical steps implementation

Date & Time	Action	Action by

People:
Requestor: *Name of person(s) that requesting the Change*
Change builder: *Names of all persons implementing the change*
Future users: *Name who will use the change*

Communication:

Preparation: e.g. informing the support departments, future users

Date & Time	Action	Action by	Remarks Future users:

Appendix B - Abbreviations used in this paper

CC	change control
CCP	change control policy
CM	crisis manager
CMDB	configuration management database
CRB	change review board
FW	firewall
ISO	International Standards Organization
IT	information technology
RCS	revision control system
RFS	request for services
SA	security administrator
SCCS	source code control system
SLA	service level agreement
SP	security policy
TT	trouble ticket
VPN	virtual private network
XML	extensible markup language

References

[1] “Cisco- Network Security Policy: Best Practices White Paper”. 12 Jan 2001. URL: http://www.cisco.com/warp/public/126/secpol.html (17 May 2003)

[2] Information Technology Services, College of the Holy Cross, “Change Control Policy and Procedures, Excerpted from the Holy Cross IT Security Handbook”. 22 Feb. 2000. URL: http://www.holycross.edu/departments/its/network/change_control.pdf (17 May 2003)

[3] Lance Spitzner, “Building Your Firewall Rulebase”, October 16,2002, URL: http://www.secinf.net/firewalls_and_VPN/Building_Your_Firewall_Rulebase_.html (17 May 2003)

[4] Central Computing and Telecommunications Agency (CCTA). “Managing Successful Projects with PRINCE2.” The Stationary Office for CCTA, 2000. 81-83