Avoiding IT Services Failures with Change Management Automation and Configuration Optimization

By Mariusz Stawowski – ISSA member, Poland Chapter

Join the Discussion Connect

The most common cause for losing IT services availability is human error within the process of implementing changes. Change management automation and configuration optimization can greatly reduce costs resulting from this unavailability.

Abstract

The most common cause for losing IT services availability is human error within the process of implementing changes. Changes in the configurations of network and security devices should be done in a planned and controlled way to minimize the number of errors. This is made possible by implementation of appropriate change management procedures (e.g., based on ITIL or COBIT) and the use of specialized tools to support and enforce practical implementation of these procedures. Change management automation and configuration optimization can greatly reduce costs resulting from IT services unavailability.

Human error within the process of implementing changes is the most common cause for losing IT services availability. Network and safeguard configurations are becoming more and more complicated, increasing the difficulty of properly controlling configuration changes.

The problem is known to IT staff and managers and confirmed by many reports, including Deloitte: "The 6th Annual Global Security Survey,"[1] Juniper Networks: "What's Behind Network Downtime,"[2] etc. The human factor problems stem from a variety of reasons: people may be tired, distracted, unaware, careless, ill, stressed, lazy, inexperienced, inadequately educated, or simply do not have enough time or good will. The most effective way to achieve independence from the weakness of human factor is the use of dedicated tools that perform the operations.

Nowadays the loss of IT services availability in most cases is a result of network failures. Almost all modern applications run in a networking environment. Lack of network availability immediately translates into a lack of IT services availability. Changes in the configurations of network and security devices should be done in a planned and controlled way to minimize the number of errors in the process. This is made possible by implementation of appropriate change management procedures (e.g., based on ITIL or COBIT) and the use of specialized tools to support and enforce practical implementation of these procedures.

In practice, there are many situations where human error causes the problems:

- IT staff record the changes irregularly, making proper change control impossible
- Documents where the changes are recorded become barely legible and in practice useless
- IT staff unwittingly cause loss of IT services availability by reckless change of the configuration of some network or security device
- Excessive size increase of firewall configurations (including unnecessary rules and objects in the policies), creating a "hole" in the safeguards

1 "Protecting what matters: The 6th Annual Global Security Survey," 2009 Deloitte Touche Tohmatsu. Document is available at http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_fsi_GlobalSecuritySurvey_0901.pdf.

2 "What's Behind Network Downtime? Proactive Steps to Reduce Human Error and Improve Availability of Networks," 2008 Juniper Networks. Document is available at http://netscreen.com/solutions/literature/white_papers/200249.pdf.

- IT staff do not understand oversized configurations and make wrong decisions
- IT staff do not have enough knowledge or time to maintain the configurations
- Network and security configurations are not regularly audited
- IT staff do not understand the network structure and, consequently, make wrong decisions
- Device failure occurs and IT staff do not have up-to-date configuration backup
- IT staff do not know what ports the applications are running on in the network; as a result they cannot properly configure the network safeguards
- IT staff do not know if firewall rules are still needed or the rules' business justification
- Lack of appropriate business justification, risk verification, and approval of the configurations changes

These kinds of problems can be limited by implementation of appropriate procedures and deployment of dedicated tools for optimizing the network and security configurations as well as automation of an entire change management process. In this scope the reduction of human error directly translates into lower costs resulting from the loss of IT service availability and other consequences, including the loss of the company's reputation and consumer confidence. The article describes these issues on case studies and practical usage examples of dedicated tools. Examples of developers include Tufin Software Technologies,[3] AlgoSec,[4] and FireMon.[5]

In the network a huge number of elements (i.e., network and security devices) are involved and the potential consequences of their failure can directly result in company losses, i.e., the customers cannot order products, the invoices cannot get paid, the employees cannot do their jobs, and so on. Change automation means a lower level of human involvement, which helps to reduce errors and IT staff remediation efforts (e.g., less time required to diagnose and resolve problems).

IT staff record the changes irregularly, making proper change control impossible

Change control in the scope of configuring network and security devices (among others, i.e., firewalls, routers, switches) based on traditional, manual methods such as event logs (or similar documents) requires continuous registration of all changes. The change control process demands strict discipline and time devotion on the administrator's part. In practice IT staff record the changes irregularly, which makes proper change control impossible. The problem can be solved with dedicated tools that maintain a database of all monitored devices. The tools monitor the devices in real time and automatically register the changes of the devices' configurations.

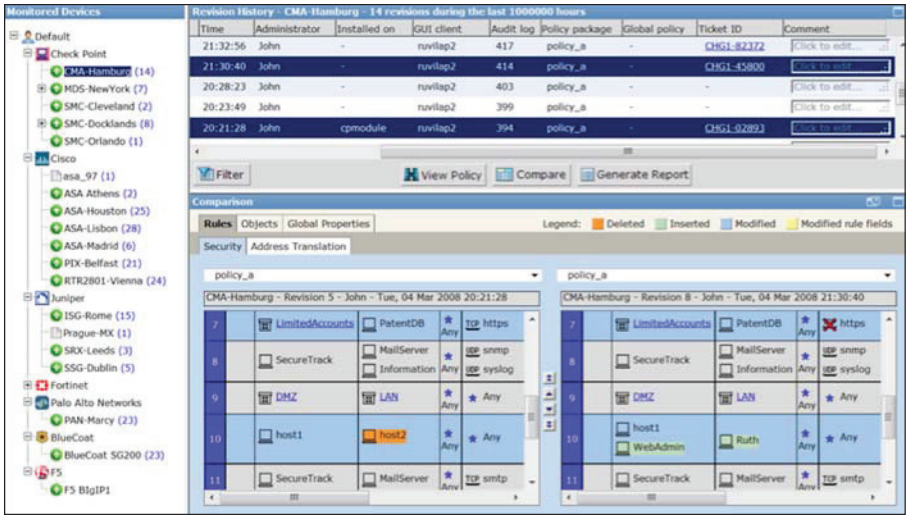

Figure 1 – Dedicated tools monitor the devices and automatically record the configuration changes as well as enable quick search and comparison of selected configurations.

Documents where the changes are recorded become barely legible and in practice useless

With traditional, manual methods the size of data stored within the change history quickly turns the search for specific pieces of data into a time-consuming process. Event logs and other documents storing historical information turn out to be of little help. Use of dedicated tools enable quick search, analysis, evaluation, and comparison of various configurations, including the historical ones. Figure 1 shows an example of a tool that automatically records a device's configuration changes and enables administrators to compare and analyze selected configurations.

IT staff unwittingly cause loss of IT services availability by reckless change of the configuration of some network or security device

Often important IT services are being disrupted as a result of a configuration change to a network device (e.g., router, switch, firewall). Finding the cause of the problem requires performing the analysis of configuration information of multiple devices – a time-consuming process. The services stay unavailable the entire time the administrators analyze the data. A solution can be provided by dedicated tools that compare in real time the implemented configuration changes to the organization's business continuity policy, i.e., IT services that network access always should be available. An alert is issued whenever a change breaches the policy, e.g., change made in firewall policy blocks an access to important IT service. The tools also allow the administrators to quickly find

3 More information about Tufin Software Technologies can be found at http://www.tufin.com.

4 More information about AlgoSec can be found at http://www.algosec.com.

5 More information about FireMon can be found at http://www.firemon.com.

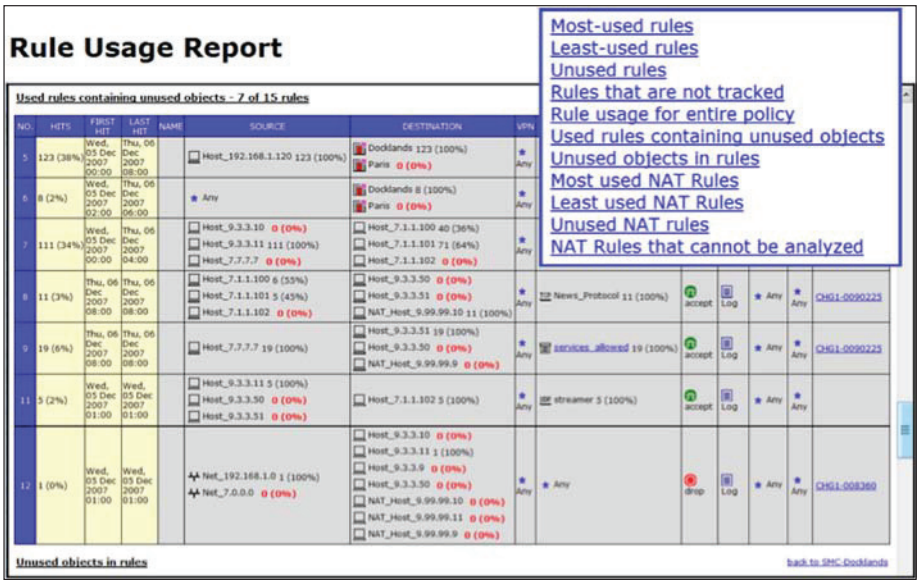

Figure 2 – Automatically generated report about the usage of firewall policy allows the administrators to optimize the configuration as well as increase the network assets safety and safeguards performance

a security device in the network that blocks or permits an access to particular IT services.

Excessive increase of firewall configuration creates a "hole" in safeguards

The configurations of security devices contain more and more needless elements, threatening IT systems safety and decreasing the safeguards' performance. Another negative effect is that the configurations of network safeguards expand and become less and less understandable to the administrators. Excessive increase in the size of the security configuration (including unnecessary rules and objects in the policies) creates a "hole" in safeguards. Dedicated tools allow efficient optimizing and maintenance of the configurations, e.g., discovering needless policy rules and objects that allow unnecessary access to IT services. Figure 2 presents an automatically generated report about the usage of firewall policy that allows the administrators to optimize the configuration (i.e., delete unused rules and objects).

IT staff do not have enough knowledge or time to properly maintain the configurations

Network and security systems are complicated. In practice extensive knowledge and experience are required on the administrators' part to maintain optimal configuration of the network and security devices. Administrators do not always have sufficient time to ensure configuration correctness. Regular auditing is required to preserve the compliance of the protections' configurations with the organization's security policy. However, in practice the network and security configurations are not regularly audited. Dedicated tools can quickly analyze the correctness of introduced configuration changes, e.g., their compliance with good practices and security requirements specific to the company. The tools can verify network firewall policies as well as configuration correctness of routers and switches.

IT staff do not know the network structure and, consequently, make wrong decisions

In many cases the network structure within a company is so complicated that administrators find it difficult to make the right decisions. It often results in configuration errors. Figure 3 presents a dedicated tool that automatically generates the picture of network topology based on the network devices' running configurations. The tool also allows the administrators to quickly find the location of network elements.

The device failure occurred and IT staff do not have up-to-date configuration backup

The company's security policy requires the IT staff be ready for device failure and always maintain an up-to-date backup of the configuration. In practice, however, it often happens that after restoring the device configuration from backup, the backup copy turns out to be out of date. It takes a lot of time to determine the missing configuration elements and during that time the IT services are unavailable. Tools that automatically register all configuration changes also enable the ad-

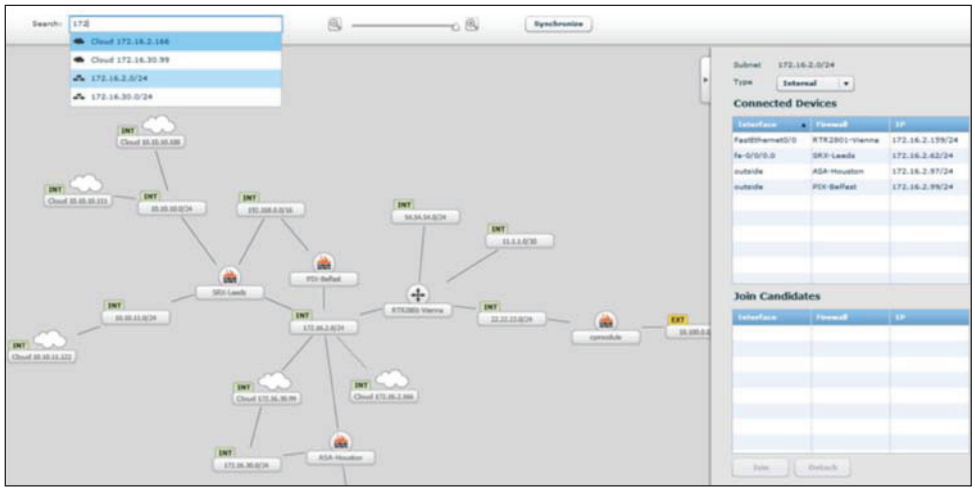

Figure 3 – Visualization of the network topology based on the network devices' running configurations aids the process of understanding and analyzing the changes.

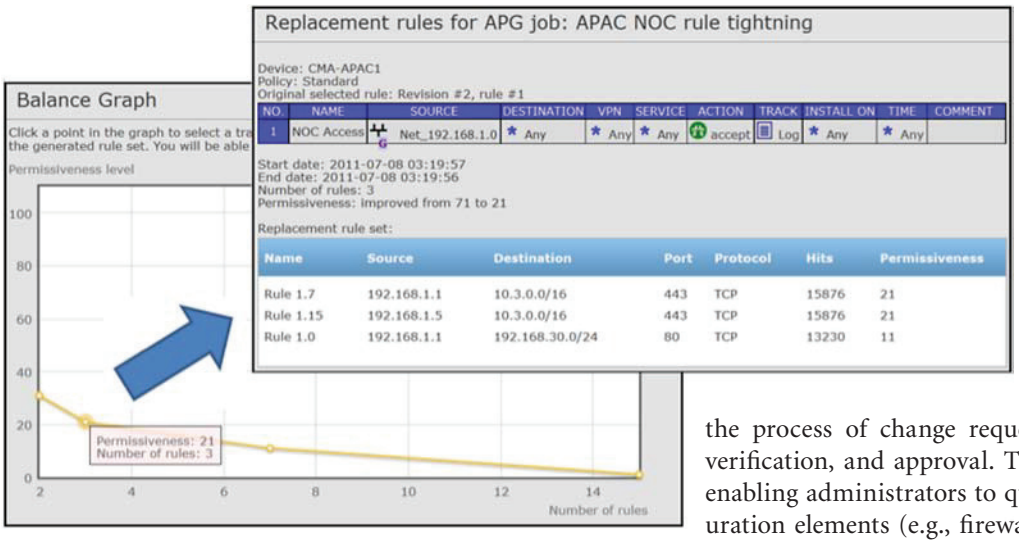

Figure 4 – The tools automatically analyze the application traffic in the network and generate recommended firewall configuration.

ministrators to quickly identify differences between specified configurations (e.g., new and legacy configurations). Administrators can copy missing configuration elements.

IT staff do not know what ports the applications are running on

Administrators do not always know which network protocols (i.e., TCP/UDP ports) should be allowed to ensure the correct functioning of a given application. As a result they open too many ports, causing "holes" in the network safeguards. Determining this information by manual analysis of the network traffic (without dedicated tools) is time-consuming and risky – too restrictive controls can disturb the applications availability for legitimate users. Also in this case dedicated tools help administrators to establish correct protection configurations based on automatic analysis of the network traffic that goes through particular devices and is permitted by particular rules. Additionally they can select appropriate permissiveness of firewall policy (using so called balance graph) – the more accurate policy, the more rules are defined. Figure 4 presents an example of automatic policy generation.

Deployment of such tools imposes a formal structure and flow on how changes are planned, approved, and implemented.

Lack of appropriate business justification, risk verification, and approval of configurations changes

Administrators receive the requests for changes from different people in many different ways (verbal, email, etc.). Configuration changes conducted in an uncontrolled way threaten the IT services availability and the company's data safety. Administrators often forget how long the implemented change should stay valid for (e.g., a firewall rule), the reason for its implementation, who the requestor was, etc. Finding this information requires contacting many people and devoting a lot of time. The solution is deployment of tools that automate the process of change request, business justification, risk verification, and approval. The tools log the entire process, enabling administrators to quickly determine which configuration elements (e.g., firewall rules) are no longer needed, and, if required, the administrators can contact responsible individuals (e.g., users requesting IT services access).

Conclusions

Human error in the process of device configuration changes (such as networking and security devices) is the most common cause of loss of IT services availability as well as security incidents (e.g., loss of confidential data, malware infection, etc.). Dedicated tools for change management automation and configuration optimization can help companies conduct changes in planned and controlled ways, and reduce the costs of IT services unavailability. Additionally the deployment of such tools in the company imposes a formal structure and flow on how changes are planned, approved, and implemented. Automating this process not only increases IT services availability but also saves IT staff time and allows them to concentrate on higher-value tasks (e.g., new projects, IT service improvements). Less IT staff time and effort is required to manually conduct the changes. Less IT staff time and effort is required to detect, diagnose, and repair faults resulting from errors introduced during manual changes. Furthermore, the network is more reliable and predictable – employees can be more productive; customers obtain better service, etc.; and it can help the company achieve and maintain legal and regulatory compliance.

About the Author

Mariusz Stawowski, Ph.D., is Director of Professional Services of CLICO, a security technologies distributor and service provider located in Poland. For more than 12 years he has been responsible for management of security projects. He holds CISSP and PRINCE2 Practitioner certificates. His doctoral dissertation was elaborated at the Military University of Technology in the special field of IT systems security auditing and network protections designing. Mariusz can be contacted at mariusz.stawowski@clico.pl.