SOLARWINDS TECH TIPS

Reduce Network Risks with Secure Configuration Management

Learn about the security aspect of configuration management for network devices

Share:

solarwinds
Unexpected Simplicity™

All network devices require scripts or configurations that determine how they should work in a network. These configurations are manually written and differ from vendor to vendor. Furthermore, device configurations change frequently due to application or technology deployments, network expansions, organizational changes and device failures or end-of-life replacements. Deploying and managing device configurations in large networks with hundreds of devices makes it a time consuming, extensive process that is very error-prone.

BT/Gartner[1] has estimated that 65% of cyber-attacks exploit systems with vulnerabilities introduced by configuration errors. This is one of the major reasons why configuration and change management has been gaining significance in the security aspect of the network. Misconfigurations known as vulnerabilities create huge security risks. Some examples include:

- A misconfigured HSRP (Hot Standby Router Protocol) can be responsible for the backup link not working
- Unidentified security holes or unintended backdoor in the firewall
- Intended VPN tunnel not used due to IPSec (Internet Protocol Security) configuration error
- Inconsistent QoS (Quality of Service) configurations impacting VoIP (Voice over IP) performance

Most organizations implement internal and external regulatory standards for device configuration and management. However, they may not necessarily follow them. This may be due to the difficulty of enforcing the process or lack of control or negligence. Whatever may be the reason, the price to pay is big. Companies incur huge costs due to these network incidents and suffer even more damage to reputation and brand value.

Internal staff also plays a major role in the occurrence of these incidents. 36% of the worst security breaches in 2013 where caused by inadvertent human error[2]. Therefore, major causes of serious network breaches are not only failure in technology and processes, but also people.

It’s a fact that we cannot completely eliminate security risks, but it is possible to implement methods to eliminate bad configurations and introduce stronger change control. Reducing IT risks calls for serious consideration and is a grave matter of concern. In this document, we peruse through secure configuration management, the challenges, and some tips for solutions.

What is Secure Configuration Management?

Fundamentally, secure configuration management refers to the set of security policies and procedures applied on systems, applications, and network devices.

Based on industry type, operations and even budgets, every organization formalizes its own set of regulatory measures and standards that it intends to accomplish both for quality and security. Once these guidelines are determined and established, steps must be taken to introduce a set of controls that help monitor and ensure that they are followed. In simple terms, explained below are some relevant procedures associated with secure configuration management.

- **Configuration Management (CM)** is defined as a set of activities focused on establishing and maintaining reliability of the devices in the network. This can be accomplished through monitoring and control of specific processes that deal with configuration and change management of those devices.
- A **Configuration Item (CI)** is an identifiable part of a system, namely hardware, software, firmware, documentation, or a combination thereof that is impacted by a configuration control like a configuration change, backup, compliance, etc.
- A **Baseline Configuration** is a set of specifications for a device, or CI within a device, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
- A **Configuration Management Plan (CM Plan)** is a detailed design of the various roles, responsibilities, policies, and procedures that must be applied when managing configuration of network devices. The basic parts of a CM plan include:
    - Configuration Control Board (CCB) – Also known as Change Control Board, this is a group of qualified people who are responsible for the process of approving and controlling device changes.
    - Configuration Item Identification – The method used to select the configuration items that need to be placed under configuration management (CM).

- Configuration Change Control – The process for managing updates to the baseline configurations and any other change associated with device configuration.
- Configuration Monitoring – The process for assessing compliance with established baseline configuration and policies along with reporting mechanisms that point out non-conformances.
- Configuration Remediation – After configuration assessments are performed, the policy violations need to be rectified to meet compliance specifications. Remediation can be issued and applied after change approvals from the designated groups.

Challenges in Secure Configuration Management

Increases in network and device complexity directly impacts efforts that go into device manageability and enforcement of security policies. The biggest challenge is the lack of visibility across the entire network. Administrative activities that support configuration and change control comprise of device inventory, creation and approval of baseline configurations, establishing change approval processes, creating compliance policies and reports, and remediation of violations. Let's take a look at the challenges faced in each of these categories with respect to secure configuration management.

- **Managing network devices and infrastructure:** Determining or taking an inventory of the devices in the network, especially those that fall within the monitoring and management control of security policies, can be challenging. **Different devices and vendors in an ever changing network pose a big challenge to maintain accurate and updated records of device details.** It's important that you know what devices are running in the network and which of them are in use. Unused devices lying around in the network can be a medium for unauthorized access.
- **Creating and maintaining baselines for device configurations:** Network devices like routers, firewalls and switches all have specific controls or configurations that determine segmentation, inspection, permission and encryption of traffic. It's mandatory to **maintain an up to date repository of baseline configurations** that can be used to compare a change and ensure that the configuration is stable and within the framework of internal policies and

regulatory mandates. ‘Last known good configuration’ is a life saver in cases of bad changes leading to disruption of the network.

- **Enforcing security and compliance policies:** The major difficulty here lies in holistically following compliance polices and documentation processes. **Unmonitored policy violations lead to failed audits and expose your network to risks.** Again, a great deal of time and effort goes into preparation of reports required to prove compliance for audit requirements. By enforcing compliance you are being proactive and not reactive.
- **Diagnosis of configuration errors:** Monitoring software helps detect the existence of a network problem but they offer little detail to **correlate and deduce that the problem was caused due to a configuration error**. Hence, administrators need to be able to take immediate remediation actions to fix issues caused due to erroneous device configurations.
- **Manually intensive process and dynamic environments:** Manual processes result in errors. Common device configuration tasks that **consume a great deal of time and effort** are: Analyzing changes before they are applied, checking configurations against corporate policies and standards, extensive use of complex and error-prone Command Line Interface (CLI), applying the same configuration change to multiple devices, documenting changes for approvals and audit trails, and so on.
- **Change detection and control:** Most times there is no knowledge of who made what change and when. Discrepancies are detected only when there is an issue or when the network goes down. Misconfigurations mostly go unnoticed or are overlooked as a cause of network downtime. Not having a change control process in place results in bad changes that can lead to connectivity issues, reduced performance, and security vulnerabilities.

Tips to Ensure Secure Configuration Management

It’s high time that organizations consider configuration management and change control as a part of security controls and processes that are essential to implement rather than nice to have. Here are a few tips that help gain control and bridge security vulnerabilities caused due to device configuration changes and inefficient management of device configurations.

1. Avoid configuration errors by analyzing configuration changes before they are applied.
2. Check configurations against corporate polices and external standards like PCI, HIPAA, and ITIL.
3. Reduce room for manual errors by standardizing and consolidating management of multi-vendor devices. This helps simplify deployment of standard configurations on multiple devices.
4. Follow a change approval process and implement user roles to restrict access to making configuration changes.
5. Establish and maintain baselines for devices in the network—critical devices most importantly.
6. Know what devices are running in your network and remove unused devices.

It's important to automate tasks and eliminate risks associated with human errors. Enforce compliance and regulatory measures to ensure that standards are met and there are no missed vulnerabilities in configurations. SolarWinds® Network Configuration Manager (NCM) is one such tool that can help you stay in control and effectively manage you Network Configuration and Change Management (NCCM). In short, secure configuration management is a combination of steps taken to satisfy a set of regulatory policies that help reduce the risk of security vulnerabilities due to misconfigurations.

Key Benefits of SolarWinds Network Configuration Manager

- **Automatically discover and import devices** into the NCM database regardless of vendor. No manual effort in individually adding devices to be managed.
- **Quickly fix a bad configuration change** by replacing a known good configuration from a backup. You can easily schedule automatic backup jobs as required and maintain an archival history of baselines and stable configurations.
- **Monitor unauthorized and erroneous changes to quickly fix network issues** and reduce downtime. Be notified every time a configuration change is made.
- **Easily prepare reports for capital budget forecasts and device replacement plans**. Maintain device inventory details and record end-of-sale and end-of-life dates for your Cisco® and Juniper® devices.
- **Save time and reduce errors** by automating and execute bulk configuration changes in real time or as scheduled tasks.
- **Effectively implement security, risk, and regulatory controls.** Create policies and be alerted on policy violations.

LEARN MORE »   DOWNLOAD FREE TRIAL

References

1 Gartner RAS Core Research Note, Ronni J. Colville, George Spafford:
http://img2.insight.com/graphics/no/info2/insight_art6.pdf

2 Security breaches in 2013: http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack®, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.