PCI Use case

Overview

In security terms, PCI compliance means that your business adheres to the PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. In operational terms, it means that you are playing your role to make sure your customers' payment card data is being kept safe throughout every transaction, and that they – and you – can have confidence that they're protected against the pain and cost of data breaches.

Current Situation with PCI Compliance without Network Automation

Without Infoblox's Network Automation:

- Device configuration standards would have to be manually documented and enforced. Configuration files would be manually backed up to a server. After the backup, you would have to run a diff program to determine if changes occurred between the current configuration backup and previous backup. If there are differences, you have to investigate and possibly fix the changes.
- You would have to log into each device to implement role-based access.
- You would have to log into each device to disable telnet, enable SSH, block HTTP access, and block FTP access.
- You would have to review each configuration file to determine if there are parameters that are out of PCI and internal compliance.
- When performing a firewall rollout, you would have to access each firewall to copy and paste the standard configuration.

All of these tasks can be automated with Network Automation.

PCI non-compliance can result in large fines as well as:

- Suspension of credit card acceptance by a merchant's credit card account provider.
- Loss of reputation with customers, suppliers, and partners.
- Possible civil litigation from breached customers.
- Loss of customer trust which affects future sales.

Network Automation with Infoblox

- Network Automation will discover all of your devices within your network. Network Automation may even find devices that were unknown to you. The discovery process is automatic and ongoing.
- Network Automation will help ensure the devices adhere to PCI DSS standards by rolling out changes to devices and continuously ensure compliance when a configuration change is detected.
- No more manual analysis of configuration files.
- Network Automation can rollout new configurations or configuration changes without constant intervention

Use Case Summaries

Network Automation can help with the following PCI requirements:

- PCI DSS Standard 1.1 – Firewall and router configuration standards. Network Automation can help in creating, backup of firewall and router configurations, and enforcing firewall and router configuration standards.
- PCI DSS Standard 1.1.4 - Description of groups, roles, and responsibilities for logical management of network components. Network Automation has role based access and can facilitate the creation of role based access to the network devices.
- PCI DSS Standard 1.1.5 - Documentation and business justification for use of all services, protocols, and ports allowed; secure and unsecure. Network Automation can help with enforcing the disabling of telnet, enabling of SSH, blocking of FTP, disabling of HTTP.

- PCI DSS Standard 1.2 - Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Network Automation can roll out configurations to firewalls and ensure that firewall configurations are consistent.
- PCI DSS Standard 1.2.1-Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. This can be done using Security Device Controller (SDC).
- PCI DSS Standard 1.2.2- Secure and synchronize router configuration files. Network Automation can do this using scripts with remediation commands.
- PCI DSS Standard 1.2.3- Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. Network Automation can do this by setting up and deploying a configuration template.
- PCI DSS Standard 1.3.1 to 1.3.5- Prohibit direct public access between the Internet and any system component in the cardholder data environment. This can be done using SDC to configure the Firewalls.
- PCI DSS Standard 2.1- Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts. Network Automation will flag this as an issue by default.
- PCI DSS Standard 2.2- Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Network Automation can help with this in developing compliance scripts.
- PCI DSS Standard 2.2.2- Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Network Automation can be used to disable unnecessary features on network devices and ensure they stay disabled.
- PCI DSS Standard 2.2.3.b - Verify that common security parameter settings are included in the system configuration standards. This can be done by viewing the configuration files that are backed up on Network Automation.
- PCI DSS Standard 2.2.3.c - For a sample of system components, verify that common security parameters are set appropriately. This can be done by viewing the configuration files that are backed up on Network Automation.
- PCI DSS Standard 2.3- Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. Network Automation can be used to enable SSH, VPN, SSL/TLS, etc. on network devices.
- PCI DSS Standard 4.1- Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. This can be done using configuration templates.
- PCI DSS Standard 7.1- Limit access to system components and cardholder data to only those individuals whose job requires such access. Network Automation has RBAC feature and can implement RBAC features onto network devices.
- PCI DSS Standard 7.2- Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to —deny all unless specifically allowed. Network Automation can be used to configure the access lists for network device access.
- PCI DSS Standard 8.1- Assign all users a unique ID before allowing them to access system components or cardholder data. Network Automation can be used to assigned usernames to network devices.
- PCI DSS Standard 8.4- Render all passwords unreadable during transmission and storage on all system components using strong cryptography. Network Automation can configure the passwords on the network devices in encrypted mode
- PCI DSS Standard 8.5.4- Immediately revoke access for any terminated users. Network automation can be used to delete usernames and passwords on network devices.
- PCI DSS Standard 8.5.15- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. Network Automation can be used to configure the network device's timeout parameter.