



Security Policy Analysis For AcmeCorp

Completed on Thu Jul 24 18:29:07 CDT 2008

This report contains an assessment of network security risk factors for AcmeCorp using AthenaVerify, a product offering an innovative and proactive approach to security policy compliance and network risk assessment.

Executive Summary

Best Practices Analysis

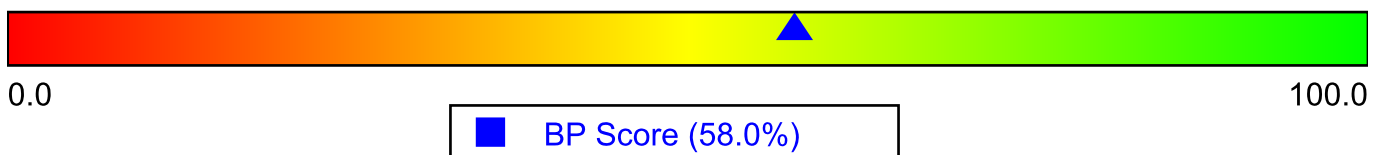
We have compiled a list of standard guidelines that represent best practices for configuring network security policies. These are based on recommendations provided by the National Security Agency (NSA), SANS Institute, Neohapsis, and other experts in the field. They are applicable to the AcmeCorp topology.

We have used AthenaVerify Best Practices Engine to check whether or not these guidelines have been implemented in the AcmeCorp topology for each applicable topology element and then arrived at pass/fail determination for each topology element applicable to a best practice and then the best practice as a whole. We summarized the BestPractices Analysis with BP Summary Score: 58%, which is computed in percentage terms by looking at how many topology elements passed for each best practice. On the whole, 2 out of 24 best practices completely complied in our analysis.

Based on the property of best practices, we have classified best practices into following categories: Access Policy, Device Configuration, and Network Architecture. For each category, we calculate category summary score as a percentage score, i.e. the pass percentage of the topology elements that have been analyzed for each best practice belonging to the category. Category BP scores are shown in the Category Scores section. Out of 24 best practices, we consider 11 best practices to be critical. Among those critical best practices, we observed 10 failed in our check.

A description of each individual best practice and our detailed findings are presented in a subsequent section. Each practice may be applied at different levels in the network, i.e. individual network device or a group/type of networks.

BP Score



BP Score By Category

BP Category Scores

The Best Practice Score table below is organized by each best practice category and shows the score for each Best Practice category. The BP Pass/Total indicates how many best practices complied out of the total number of best practices within the category. This gives you an idea of how many best practices are completely compliant with in the network topology. A best practice is determined to have Passed only if all the network elements that have been evaluated for the best practice have passed. The Category Score however does take into consideration how many network elements that have been evaluated are compliant instead of a straight none or all score (i.e score of 1 for a bp if all network elements evaluated for that bp comply, 0 otherwise) for each bp.

