



Firewall Summary

Completed on Thu Jul 15 11:28:13 CDT 2010

This report provides a summary of the rule cleanup and security audit analyses performed by the batch summary edition of Athena FirePAC.

The rule cleanup analysis identifies opportunities for simplifying the firewall configuration by removing unnecessary rules, and unused network and service objects. The security audit analysis evaluates security checks based on best practice recommendations for firewall policies drawn from industry sources such as NIST, NSA, SANS Institute, and CIS (refer to the standard checks listed in the appendix).

Rule Analysis

The removable rules identified by Athena have no role to play in controlling traffic flow through the network and simply bloat your rulebases. The effect of bloating is not only increased exposure to attacks, but it also creates a stranglehold on the change process, adding significant time and expense to firewall management activities and compliance reviews. These rulebases also have an adverse impact on network performance, service delivery and the ability to execute major infrastructure projects such as upgrading security devices or adding networks.

Risk Summary


Evaluating the security profile of firewall devices requires complex algorithms that evaluate actual rules for dangerous services allowed to destination hosts. Using an offline model of the device based on the interfaces, objects, access lists, address translations, VPNs, routing rules, access-group statements and other constructs that control how the IP traffic flows through the firewall, Athena performs the most consistent and thorough security analytic function possible.

Athena recommends that immediate attention is given to the high severity issues discovered during this assessment and that an action plan is generated to remediate failed checks.

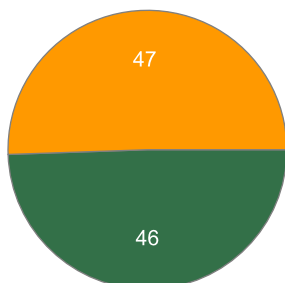
Firewalls Analyzed

No.	Name	Model	IP	Profile	Complexity
1	acmecorp-pix	CiscoPIX	62.59.14.189	Standard	MEDIUM ⓘ
2					
3					
4					
5					

Firewall Summary Report - acmecorp-pix

No.	Name	Model	IP	Profile	Complexity
1	acmecorp-pix	CiscoPIX	62.59.14.189	Standard	MEDIUM 

Rule Summary



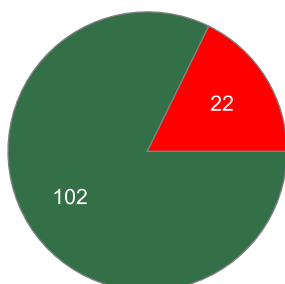
● Valid Rules ● Removable Rules

Total Rules :	114
ACL Rules :	93
Redundant and Shadowed Rules :	19
Unused Rules :	28
Disabled Rules :	0
Time Inactive Rules :	0
Unreferenced Network Objects :	1
Unreferenced Service Objects :	1
Rules with Unused Objects :	0
Rules with Logging Enabled :	85
Unused Network Objects :	0
Network Objects with Unused Members :	0
Unused Service Objects :	0
Service Objects with Unused Members :	1

30.7% of access control rules can potentially be removed from the rule base.

100% of the rules were analyzed for usage.

Security Audit



● Passed Checks ● Failed Checks

Total Checks :	124
Passed Checks :	102
Failed Checks :	22
High Risk :	6
Medium Risk :	5
Low Risk :	11

17.74% of 124 security checks failed.

Reports Generated

Report Name	Description
Cleanup and Optimization	Analyzes the rule structure and usage data to find redundant and unused rules
Security Audit	Identifies security risks in the firewall policies
VPN Audit	Identifies all IPSEC point-to-point VPN's in firewall
Services Summary	Identifies sources and destinations for all services allowed by the firewall policy
PCI DSS Compliance	Assess firewall compliance with PCI DSS v1.2 requirements

Report Name	Description
PCI Zone Dangerous Rules Analysis	Identify rules occurring most frequently in failed PCI security checks
PCI Zone Detailed Policy Findings	Identify services allowed to or from PCI zone
PCI Zone Failed Policy Checks Detail	Details of failed PCI policy checks
Configuration	Presents the firewall configuration in a readable format