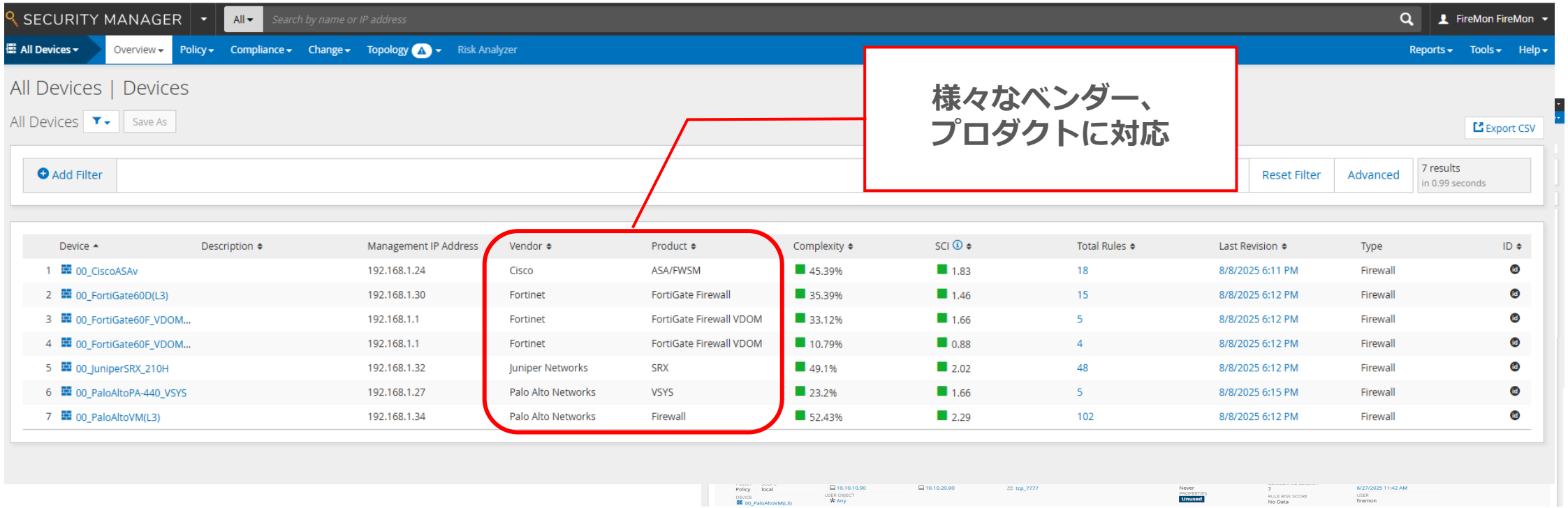
統合管理機能

統合管理機能（マルチベンダー）

SecurityManager

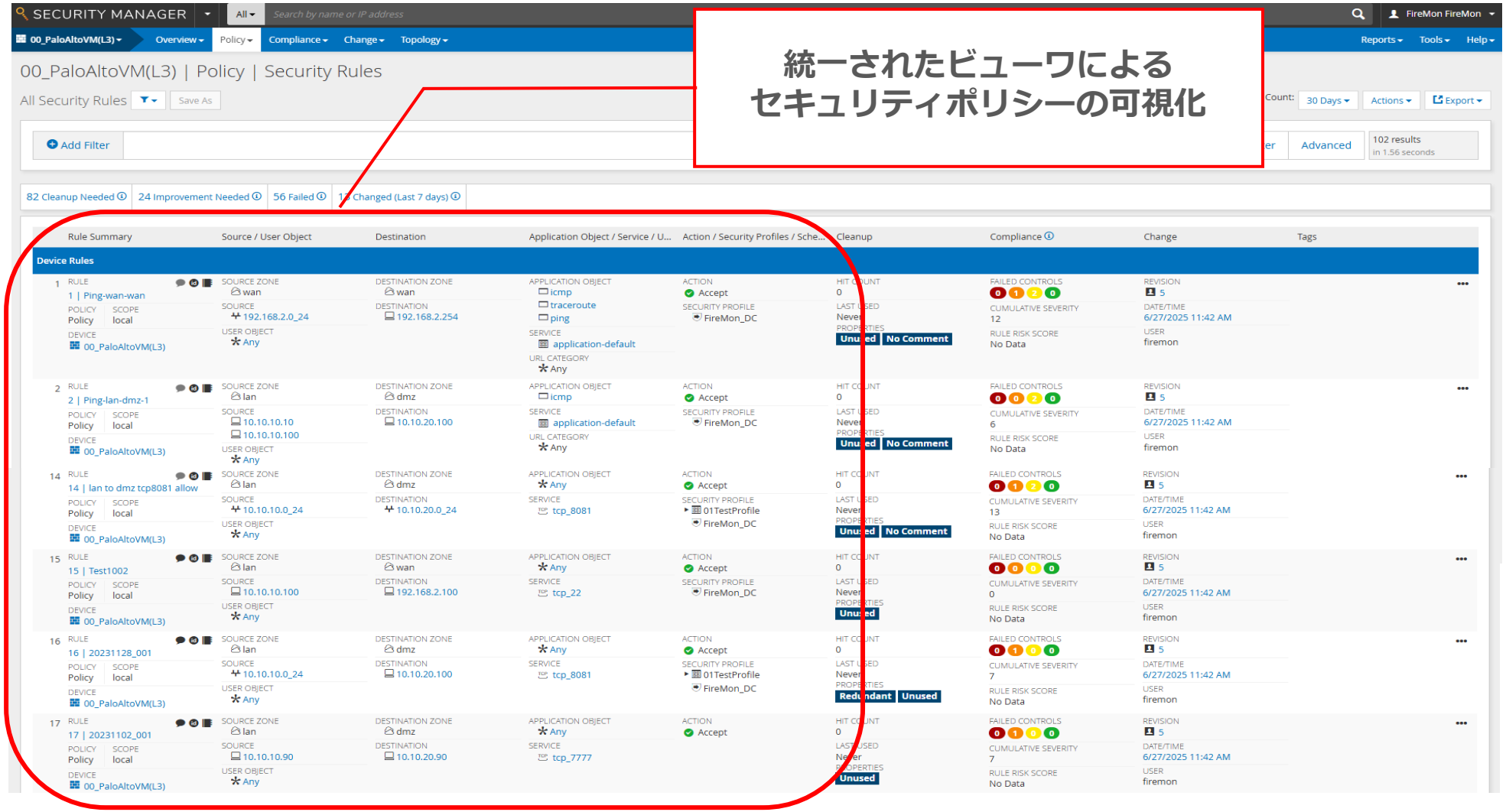
・FireMon SecurityMangerにより、マルチベンダーのファイアウォール、ルータなどを統合管理し、ネットワークトポロジマップによるネットワーク構成を簡単に把握することが可能です。

社内、クラウドなどのあらゆる環境に配置されたデバイスを１つの統一されたビューワーで管理することができ、セキュリティポリシー設定状況や変更履歴などの情報を一元的に可視化することが出来ます。



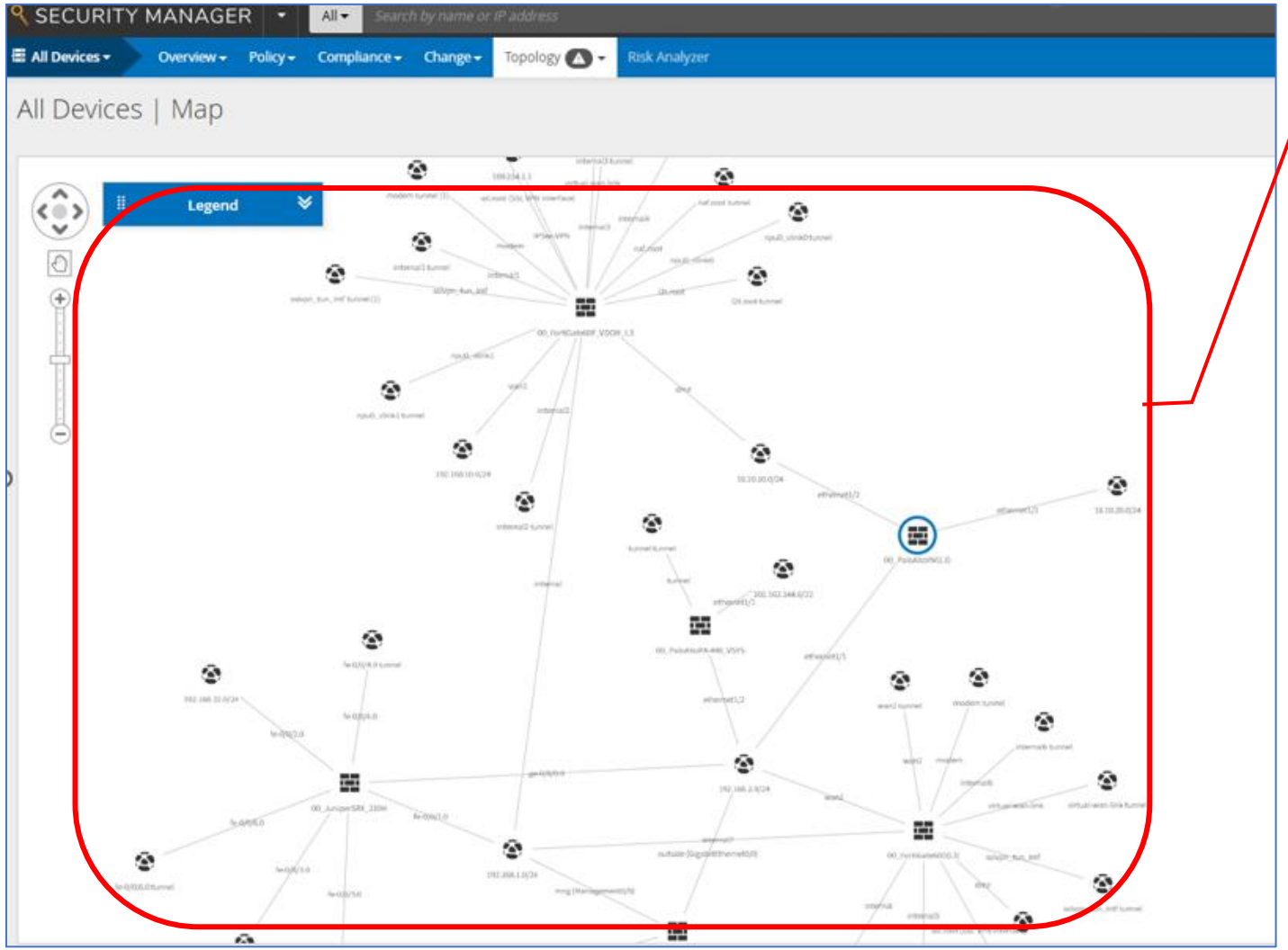
統合管理機能（可視化_セキュリティポリシー）

SecurityManager



統合管理機能（可視化_トポロジマップ）

SecurityManager



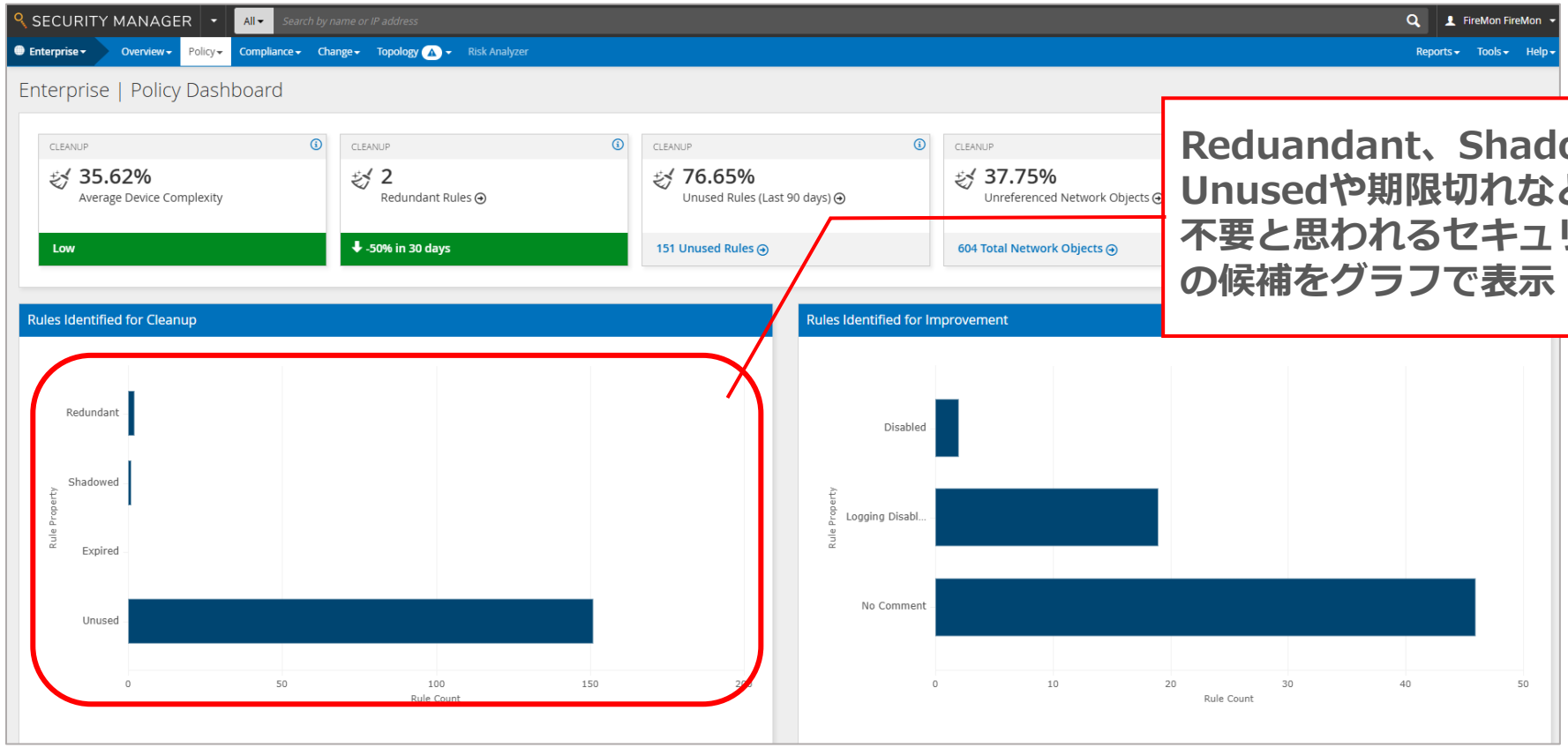
自動収集した結果からトポロジマップを生成

自動生成されたマップを手動で修正することも可能

統合管理機能（ルール分析）

SecurityManager

・ルール分析
取り込んだファイアウォールのルールを分析し、Redundant、Shadowed、Unusedなどの、
不要なセキュリティポリシーを検出
日々の運用で肥大化するルールの棚卸、クリーンアップをすることが可能

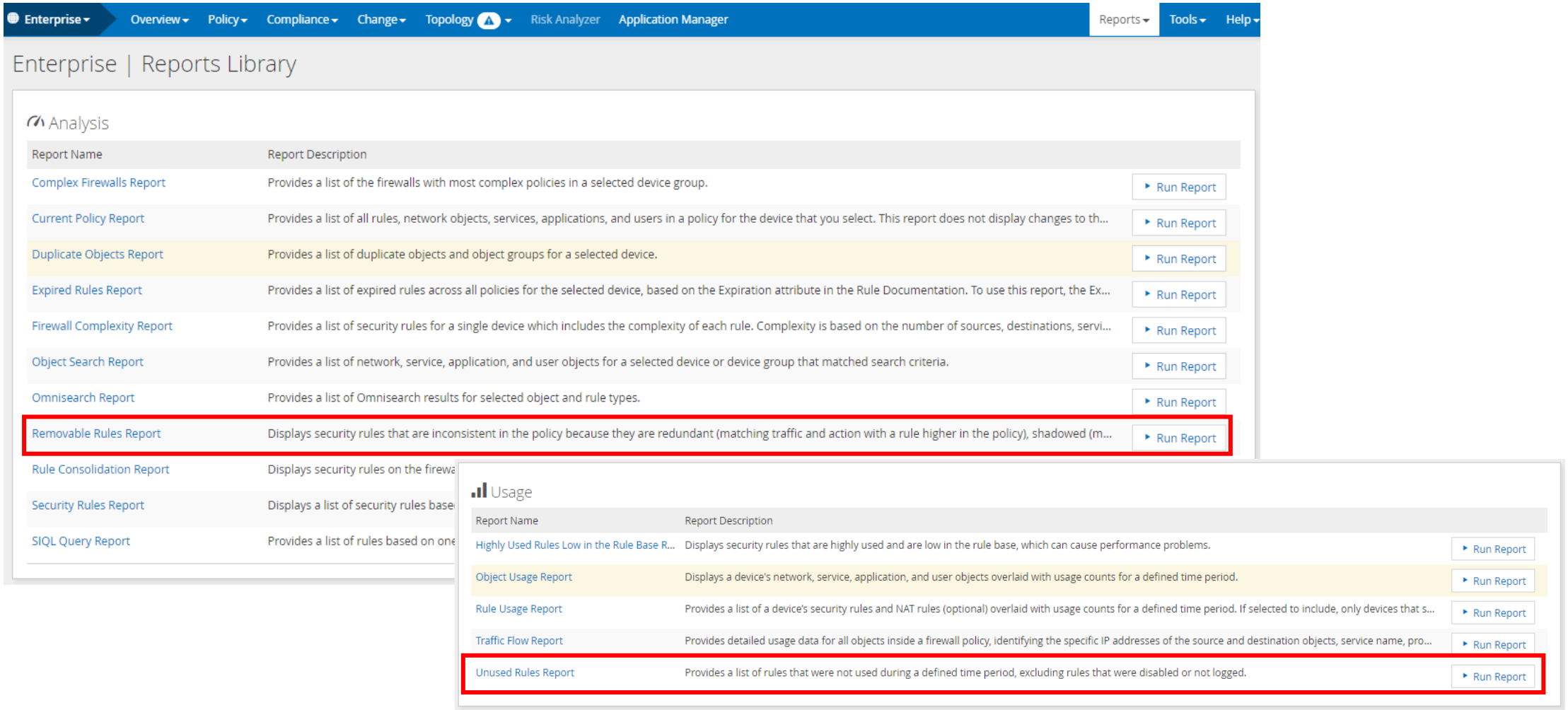


Reduandant、Shadowed、Unusedや期限切れなど、不要と思われるセキュリティポリシーの候補をグラフで表示

統合管理機能（レポート機能 その１）

SecurityManager

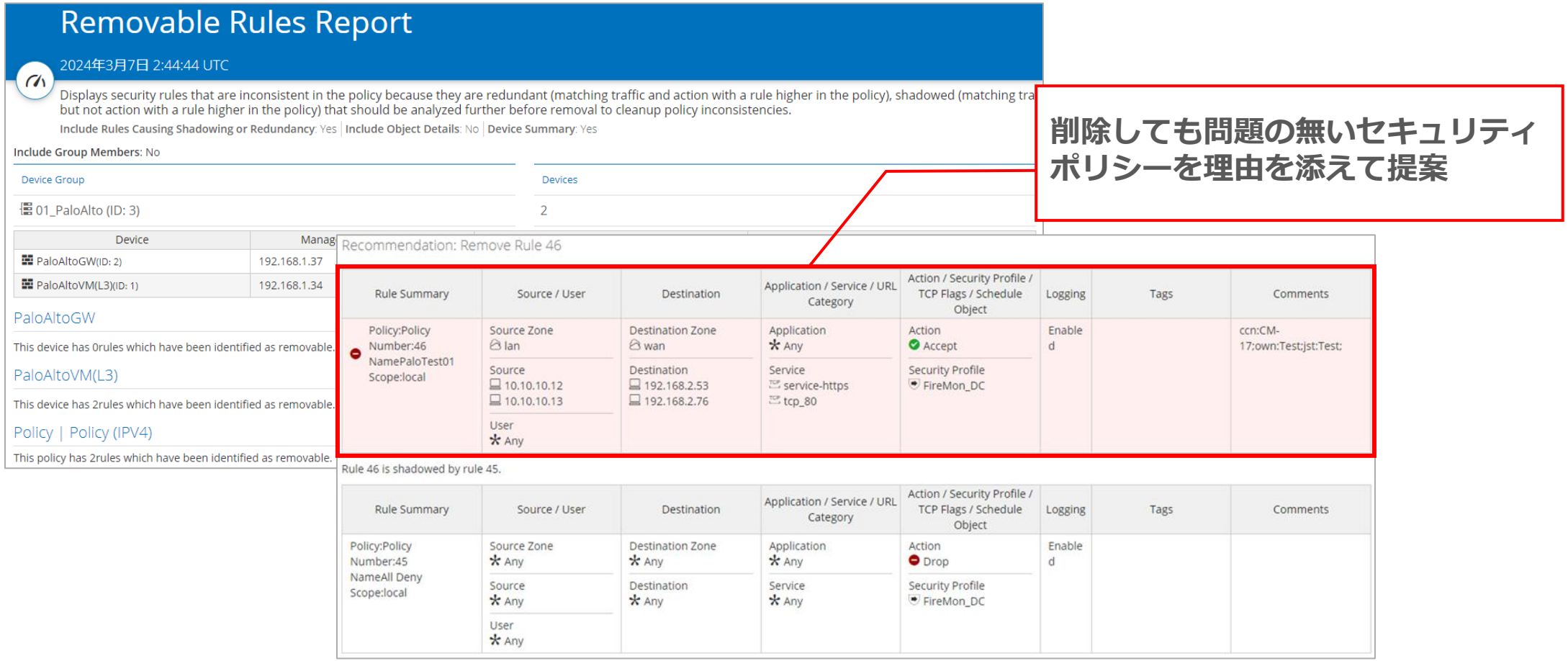
・レポート機能
様々なレポート出力に対応、分析したルールの詳細をレポートとしても出力可能



統合管理機能（レポート機能 その2）

SecurityManager

・Removable Rules Report
　削除可能なセキュリティポリシーの提案レポート



Removable Rules Report

2024年3月7日 2:44:44 UTC

Displays security rules that are inconsistent in the policy because they are redundant (matching traffic and action with a rule higher in the policy), shadowed (matching tra
but not action with a rule higher in the policy) that should be analyzed further before removal to cleanup policy inconsistencies.

Include Rules Causing Shadowing or Redundancy: Yes | **Include Object Details**: No | **Device Summary**: Yes

Include Group Members: No

Device Group	Devices
01_PaloAlto (ID: 3)	2

Device	Manag
PaloAltoGW(ID: 2)	192.168.1.37
PaloAltoVM(L3)(ID: 1)	192.168.1.34

PaloAltoGW

This device has 0rules which have been identified as removable.

PaloAltoVM(L3)

This device has 2rules which have been identified as removable.

Policy | Policy (IPV4)

This policy has 2rules which have been identified as removable.

削除しても問題の無いセキュリティポリシーを理由を添えて提案

Recommendation: Remove Rule 46

Rule Summary	Source / User	Destination	Application / Service / URL Category	Action / Security Profile / TCP Flags / Schedule Object	Logging	Tags	Comments
Policy:Policy Number:46 NamePaloTest01 Scope:local	Source Zone lan Source 10.10.10.12 10.10.10.13 User Any	Destination Zone wan Destination 192.168.2.53 192.168.2.76	Application Any Service service-https tcp_80	Action Accept Security Profile FireMon_DC	Enable d		ccn:CM-17:own:Test;jst:Test;

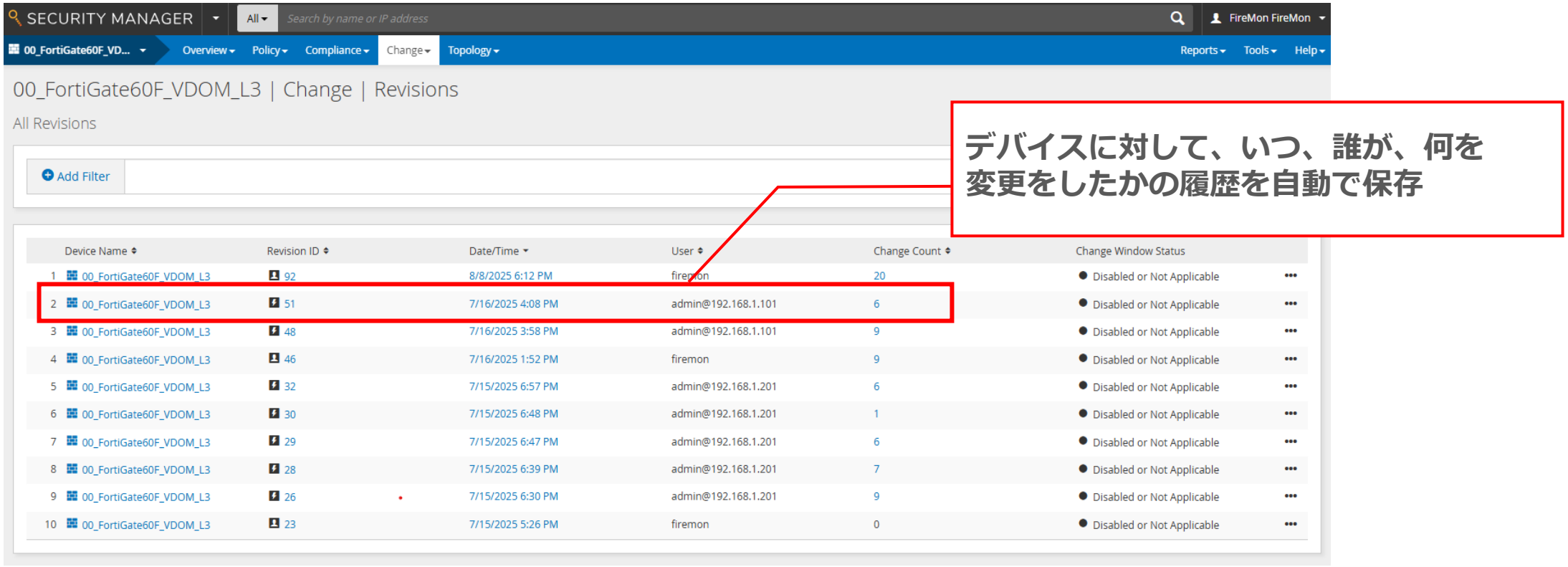
Rule 46 is shadowed by rule 45.

Rule Summary	Source / User	Destination	Application / Service / URL Category	Action / Security Profile / TCP Flags / Schedule Object	Logging	Tags	Comments
Policy:Policy Number:45 NameAll Deny Scope:local	Source Zone Any Source Any User Any	Destination Zone Any Destination Any	Application Any Service Any	Action Drop Security Profile FireMon_DC	Enable d		

統合管理機能（変更管理 その１）

SecurityManager

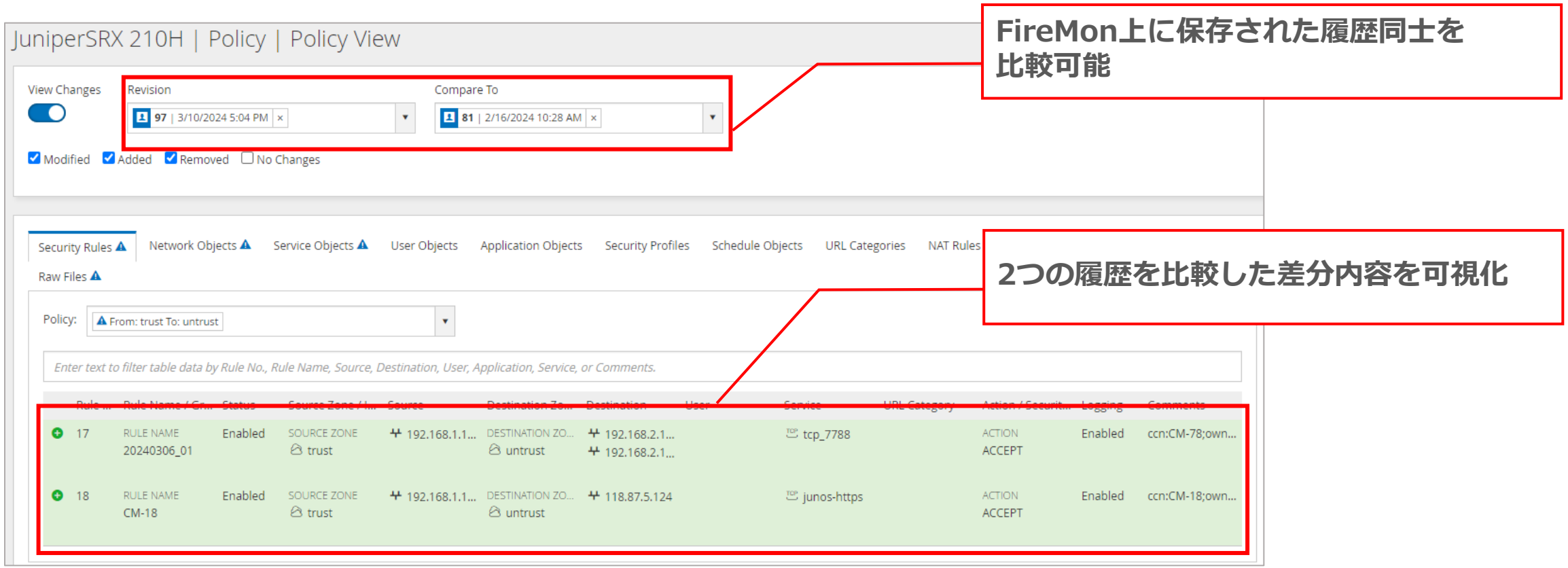
・変更管理
　管理しているデバイスで変更が行われた場合、FireMonがデバイスから最新の設定を収集、保存して変更内容の履歴を残します。
　セキュリティポリシーの履歴保存だけでなく、過去のセキュリティポリシーの比較も簡単に可能



統合管理機能（変更管理 その２）

SecurityManager

・変更管理（履歴の比較）



FireMon上に保存された履歴同士を比較可能

2つの履歴を比較した差分内容を可視化

統合管理機能（アクセスパス解析）

SecurityManager

・アクセスパス解析（Access Path Analysis）
　可視化したトポロジーマップを利用して、指定した通信要件が管理しているネットワークをどのように通過するか、セキュリティポリシーが許可されているか、などを解析可能