

統合管理機能

・ 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。

The screenshot displays the FireMon Security Manager web interface. The top navigation bar includes tabs for 'All Devices', 'Overview', 'Policy', 'Compliance', 'Change', 'Topology', and 'Risk Analyzer'. The 'All Devices' tab is active, showing a list of devices. A red box highlights the 'Vendor' and 'Product' columns, with a callout text box stating '様々なベンダー、プロダクトに対応' (Supports various vendors and products). The table lists 7 devices, including Cisco ASA/FWSM, Fortinet FortiGate Firewall, Juniper Networks SRX, and Palo Alto Networks VSYS and Firewall. The bottom status bar shows policy information and a risk score.

Device	Description	Management IP Address	Vendor	Product	Complexity	SCI	Total Rules	Last Revision	Type	ID
1	00_CiscoASAv	192.168.1.24	Cisco	ASA/FWSM	45.39%	1.83	18	8/8/2025 6:11 PM	Firewall	10
2	00_FortiGate60D(L3)	192.168.1.30	Fortinet	FortiGate Firewall	35.39%	1.46	15	8/8/2025 6:12 PM	Firewall	10
3	00_FortiGate60F_VDOM...	192.168.1.1	Fortinet	FortiGate Firewall VDOM	33.12%	1.66	5	8/8/2025 6:12 PM	Firewall	10
4	00_FortiGate60F_VDOM...	192.168.1.1	Fortinet	FortiGate Firewall VDOM	10.79%	0.88	4	8/8/2025 6:12 PM	Firewall	10
5	00_JuniperSRX_210H	192.168.1.32	Juniper Networks	SRX	49.1%	2.02	48	8/8/2025 6:12 PM	Firewall	10
6	00_PaloAltoPA-440_VSYS	192.168.1.27	Palo Alto Networks	VSYS	23.2%	1.66	5	8/8/2025 6:15 PM	Firewall	10
7	00_PaloAltoVM(L3)	192.168.1.34	Palo Alto Networks	Firewall	52.43%	2.29	102	8/8/2025 6:12 PM	Firewall	10

統一されたビューワによる
セキュリティポリシーの可視化

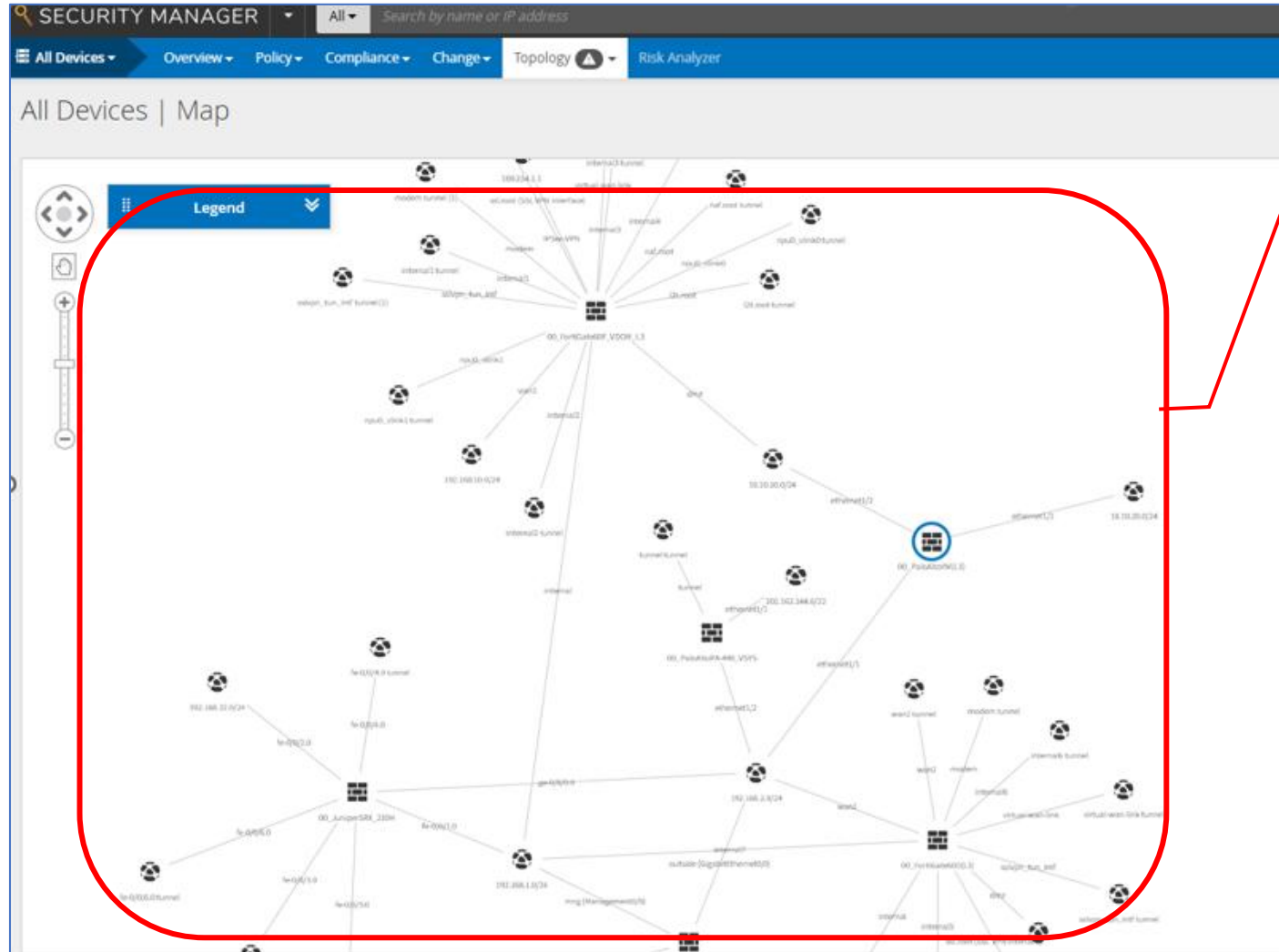
00_PaloAltoVM(L3) | Policy | Security Rules

All Security Rules [Add Filter](#) [Save As](#)

Count: 30 Days [Actions](#) [Export](#)

82 Cleanup Needed 24 Improvement Needed 56 Failed 1 Changed (Last 7 days)

Rule Summary	Source / User Object	Destination	Application Object / Service / U...	Action / Security Profiles / Sche...	Cleanup	Compliance	Change	Tags
Device Rules								
1 RULE 1 Ping-wan-wan POLICY Policy SCOPE local DEVICE 00_PaloAltoVM(L3)	SOURCE ZONE wan SOURCE 192.168.2.0_24 USER OBJECT Any	DESTINATION ZONE wan DESTINATION 192.168.2.254	APPLICATION OBJECT icmp tracert ping SERVICE application-default URL CATEGORY Any	ACTION Accept SECURITY PROFILE FireMon_DC	HIT COUNT 0 LAST USED Never PROPERTIES Unused No Comment	FAILED CONTROLS 0 1 2 0 CUMULATIVE SEVERITY 12 RULE RISK SCORE No Data	REVISION 5 DATE/TIME 6/27/2025 11:42 AM USER firemon	...
2 RULE 2 Ping-lan-dmz-1 POLICY Policy SCOPE local DEVICE 00_PaloAltoVM(L3)	SOURCE ZONE lan SOURCE 10.10.10.10 10.10.10.100 USER OBJECT Any	DESTINATION ZONE dmz DESTINATION 10.10.20.100	APPLICATION OBJECT icmp SERVICE application-default URL CATEGORY Any	ACTION Accept SECURITY PROFILE FireMon_DC	HIT COUNT 0 LAST USED Never PROPERTIES Unused No Comment	FAILED CONTROLS 0 0 2 0 CUMULATIVE SEVERITY 6 RULE RISK SCORE No Data	REVISION 5 DATE/TIME 6/27/2025 11:42 AM USER firemon	...
14 RULE 14 lan to dmz tcp8081 allow POLICY Policy SCOPE local DEVICE 00_PaloAltoVM(L3)	SOURCE ZONE lan SOURCE 10.10.10.0_24 USER OBJECT Any	DESTINATION ZONE dmz DESTINATION 10.10.20.0_24	APPLICATION OBJECT Any SERVICE tcp_8081 URL CATEGORY Any	ACTION Accept SECURITY PROFILE 01TestProfile FireMon_DC	HIT COUNT 0 LAST USED Never PROPERTIES Unused No Comment	FAILED CONTROLS 0 1 2 0 CUMULATIVE SEVERITY 13 RULE RISK SCORE No Data	REVISION 5 DATE/TIME 6/27/2025 11:42 AM USER firemon	...
15 RULE 15 Test1002 POLICY Policy SCOPE local DEVICE 00_PaloAltoVM(L3)	SOURCE ZONE lan SOURCE 10.10.10.100 USER OBJECT Any	DESTINATION ZONE wan DESTINATION 192.168.2.100	APPLICATION OBJECT Any SERVICE tcp_22 URL CATEGORY Any	ACTION Accept SECURITY PROFILE FireMon_DC	HIT COUNT 0 LAST USED Never PROPERTIES Unused	FAILED CONTROLS 0 0 0 0 CUMULATIVE SEVERITY 0 RULE RISK SCORE No Data	REVISION 5 DATE/TIME 6/27/2025 11:42 AM USER firemon	...
16 RULE 16 20231128_001 POLICY Policy SCOPE local DEVICE 00_PaloAltoVM(L3)	SOURCE ZONE lan SOURCE 10.10.10.0_24 USER OBJECT Any	DESTINATION ZONE dmz DESTINATION 10.10.20.100	APPLICATION OBJECT Any SERVICE tcp_8081 URL CATEGORY Any	ACTION Accept SECURITY PROFILE 01TestProfile FireMon_DC	HIT COUNT 0 LAST USED Never PROPERTIES Redundant Unused	FAILED CONTROLS 0 1 0 0 CUMULATIVE SEVERITY 7 RULE RISK SCORE No Data	REVISION 5 DATE/TIME 6/27/2025 11:42 AM USER firemon	...
17 RULE 17 20231102_001 POLICY Policy SCOPE local DEVICE 00_PaloAltoVM(L3)	SOURCE ZONE lan SOURCE 10.10.10.90 USER OBJECT Any	DESTINATION ZONE dmz DESTINATION 10.10.20.90	APPLICATION OBJECT Any SERVICE tcp_7777 URL CATEGORY Any	ACTION Accept SECURITY PROFILE FireMon_DC	HIT COUNT 0 LAST USED Never PROPERTIES Unused	FAILED CONTROLS 0 1 0 0 CUMULATIVE SEVERITY 7 RULE RISK SCORE No Data	REVISION 5 DATE/TIME 6/27/2025 11:42 AM USER firemon	...



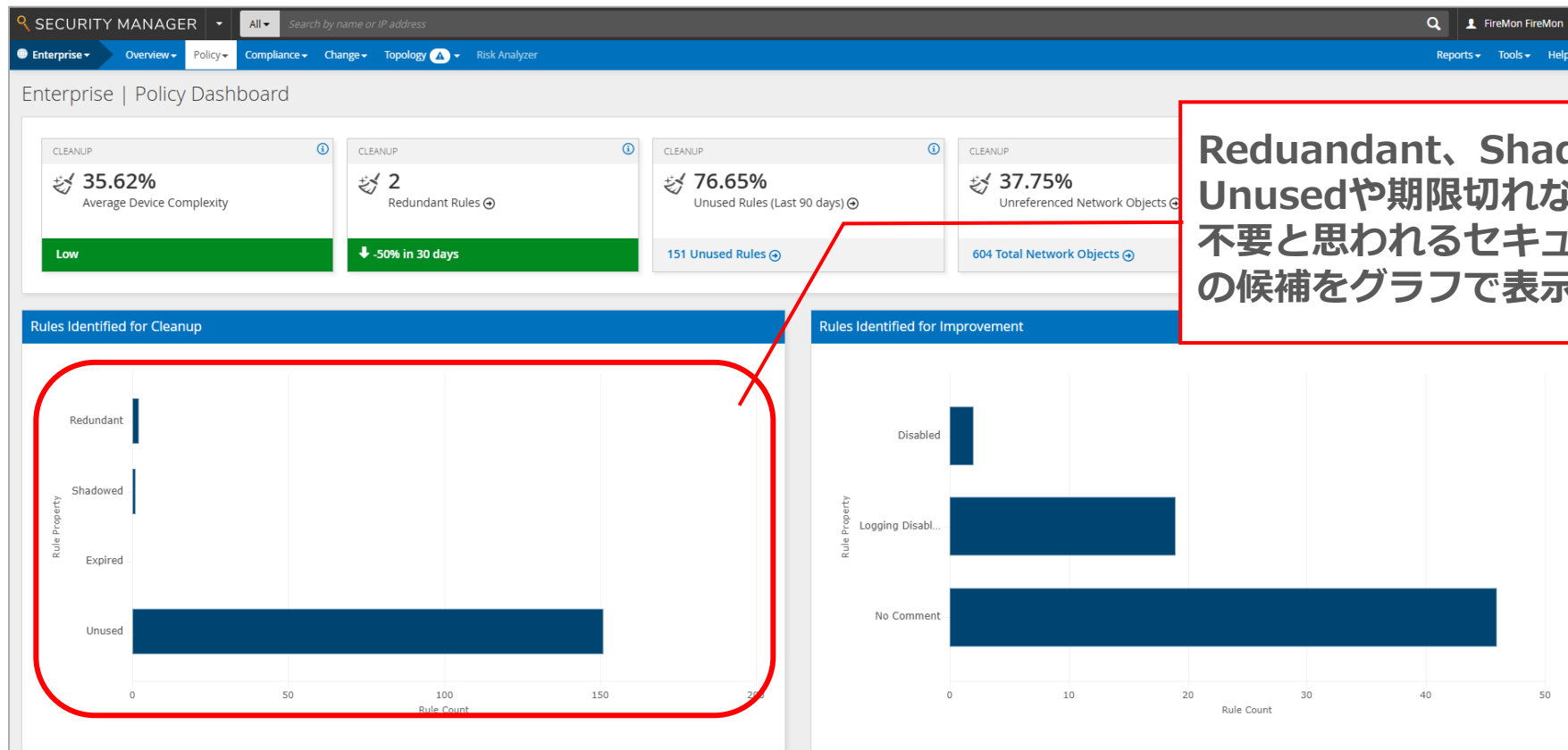
自動収集した結果からトポロジマップを生成

自動生成されたマップを手動で修正することも可能

- ・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



- ・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

The screenshot displays the 'Enterprise | Reports Library' interface. It features a navigation bar with tabs for Enterprise, Overview, Policy, Compliance, Change, Topology, Risk Analyzer, and Application Manager. The 'Reports' tab is active, showing a list of reports categorized under 'Analysis' and 'Usage'.

Analysis Category:

Report Name	Report Description	Action
Complex Firewalls Report	Provides a list of the firewalls with most complex policies in a selected device group.	Run Report
Current Policy Report	Provides a list of all rules, network objects, services, applications, and users in a policy for the device that you select. This report does not display changes to th...	Run Report
Duplicate Objects Report	Provides a list of duplicate objects and object groups for a selected device.	Run Report
Expired Rules Report	Provides a list of expired rules across all policies for the selected device, based on the Expiration attribute in the Rule Documentation. To use this report, the Ex...	Run Report
Firewall Complexity Report	Provides a list of security rules for a single device which includes the complexity of each rule. Complexity is based on the number of sources, destinations, servi...	Run Report
Object Search Report	Provides a list of network, service, application, and user objects for a selected device or device group that matched search criteria.	Run Report
Omnisearch Report	Provides a list of Omnisearch results for selected object and rule types.	Run Report
Removable Rules Report	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 (m...	Run Report
Rule Consolidation Report	Displays security rules on the firewa...	
Security Rules Report	Displays a list of security rules base...	
SIQL Query Report	Provides a list of rules based on one...	

Usage Category:

Report Name	Report Description	Action
Highly Used Rules Low in the Rule Base R...	Displays security rules that are highly used and are low in the rule base, which can cause performance problems.	Run Report
Object Usage Report	Displays a device's network, service, application, and user objects overlaid with usage counts for a defined time period.	Run Report
Rule Usage Report	Provides a list of a device's security rules and NAT rules (optional) overlaid with usage counts for a defined time period. If selected to include, only devices that s...	Run Report
Traffic Flow Report	Provides detailed usage data for all objects inside a firewall policy, identifying the specific IP addresses of the source and destination objects, service name, pro...	Run Report
Unused Rules Report	Provides a list of rules that were not used during a defined time period, excluding rules that were disabled or not logged.	Run Report

統合管理機能（レポート機能 その2）

- 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

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 traffic 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

Managed

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

PaloAltoGW

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

PaloAltoVM(L3)

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

Policy | Policy (IPv4)

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

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 Name:PaloTest01 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	Enabled		ccn:CM-17;own:Test;jst:Test

Rule 46 is shadowed by rule 45.

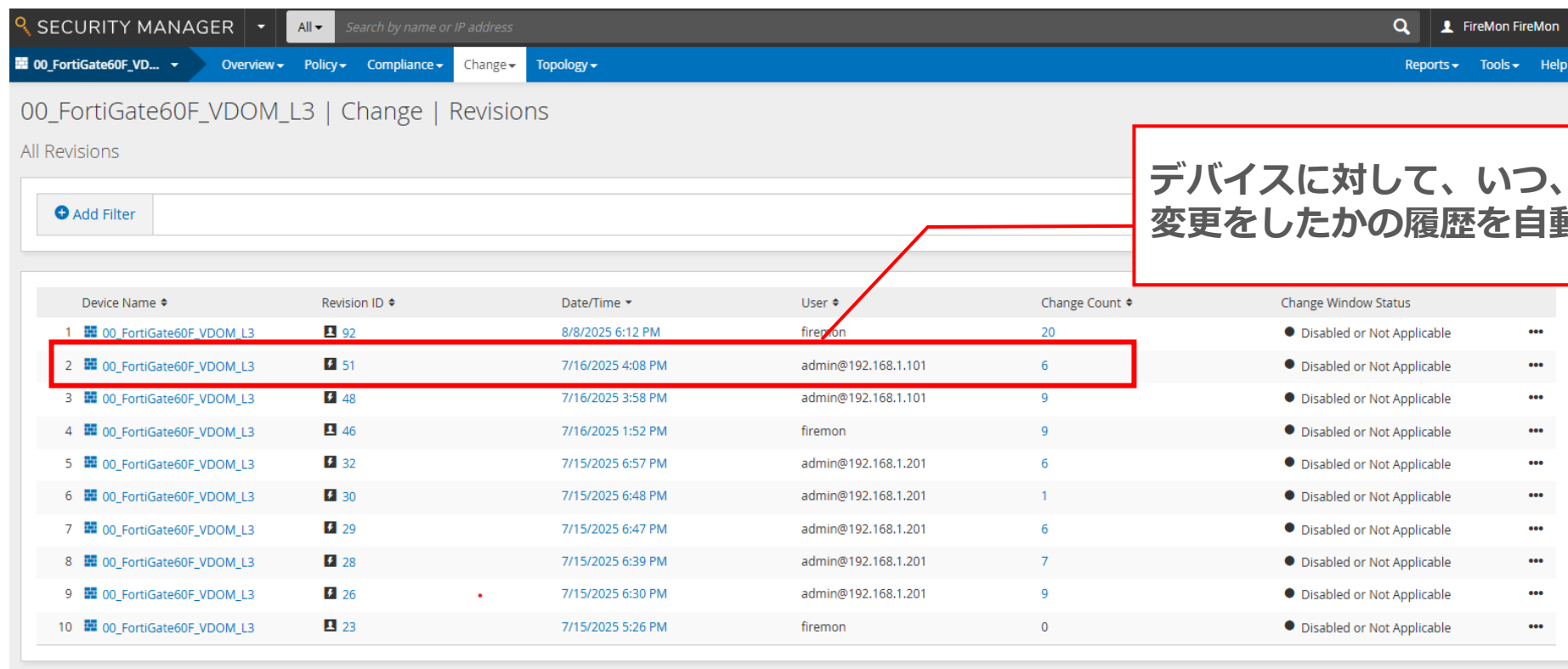
Rule Summary	Source / User	Destination	Application / Service / URL Category	Action / Security Profile / TCP Flags / Schedule Object	Logging	Tags	Comments
Policy:Policy Number:45 Name:All Deny Scope:local	Source Zone Any Source Any User Any	Destination Zone Any Destination Any	Application Any Service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

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

- 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



Device Name	Revision ID	Date/Time	User	Change Count	Change Window Status
00_FortiGate60F_VDOM_L3	92	8/8/2025 6:12 PM	firemon	20	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	51	7/16/2025 4:08 PM	admin@192.168.1.101	6	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	48	7/16/2025 3:58 PM	admin@192.168.1.101	9	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	46	7/16/2025 1:52 PM	firemon	9	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	32	7/15/2025 6:57 PM	admin@192.168.1.201	6	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	30	7/15/2025 6:48 PM	admin@192.168.1.201	1	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	29	7/15/2025 6:47 PM	admin@192.168.1.201	6	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	28	7/15/2025 6:39 PM	admin@192.168.1.201	7	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	26	7/15/2025 6:30 PM	admin@192.168.1.201	9	Disabled or Not Applicable
00_FortiGate60F_VDOM_L3	23	7/15/2025 5:26 PM	firemon	0	Disabled or Not Applicable

デバイスに対して、いつ、誰が、何を
変更をしたかの履歴を自動で保存

- 変更管理（履歴の比較）

JuniperSRX 210H | Policy | Policy View

View Changes ☒ Revision Compare To

☒ Modified ☒ Added ☒ Removed ☐ No Changes

Security Rules ▲ Network Objects ▲ Service Objects ▲ User Objects Application Objects Security Profiles Schedule Objects URL Categories NAT Rules

Raw Files ▲

Policy: ▲ From: trust To: untrust ▼

Enter text to filter table data by Rule No., Rule Name, Source, Destination, User, Application, Service, or Comments.

Rule No.	Rule Name / Comments	Status	Source Zone / Name	Source	Destination Zone / Name	Destination	User	Service	URL Category	Action / Security	Logging	Comments
17	RULE NAME 20240306_01	Enabled	SOURCE ZONE trust	192.168.1.1...	DESTINATION ZONE untrust	192.168.2.1... 192.168.2.1...		tcp_7788		ACTION ACCEPT	Enabled	ccn:CM-78;own...
18	RULE NAME CM-18	Enabled	SOURCE ZONE trust	192.168.1.1...	DESTINATION ZONE untrust	118.87.5.124		junos-https		ACTION ACCEPT	Enabled	ccn:CM-18;own...

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

- 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

The screenshot shows the 'Access Path Analysis' section of the SecurityManager interface. It includes a search bar at the top, a navigation menu, and a main area with a search form, a topology map, and a detailed path analysis results panel. Red boxes and arrows highlight specific features: the search form, the topology map, the path analysis results, and the policy status indicators.

通信要件を入力してチェックを実施

経由するデバイス、ネットワークをグラフィカルに表示

ルーティング、ポリシーの両面での通信可否の結果を表示

Access Path Analysis

Path 1

Enter network segment '192.168.1.0/24' (18)

Enter device '00_JuniperSRX_210H' (4)

Enter network segment '192.168.2.0/24' (11)

Enter device '00_PaloAlto' (3)

Enter network segment '10.10.20.0/24' (12)

Reached destination network, '10.10.20.0/24'

Packet Details

Sources	Destinations
192.168.2.32	10.10.20.100