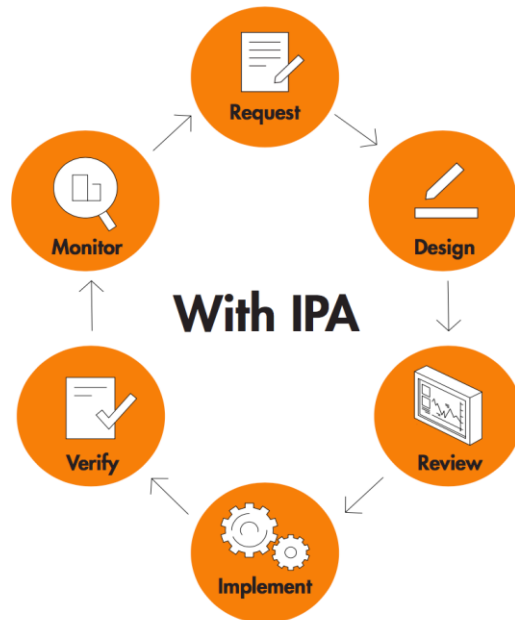


自動化（PolicyAutomation）

FireMon PolicyPlannerによって提供されるワークフローを使用することにより、管理しているデバイスに対して、セキュリティポリシーの新規作成/変更/削除などを実施することが出来ます。ワークフローで承認された設定は、FireMonによって自動で設定されます。

この機能により以下のメリットが考えられます。

- ・ 人の作業による、設定ミスの撲滅
- ・ マルチベンダー対応により、運用スタッフの平準化
- ・ ワークフローによる管理負荷の軽減



Step 1: リクエスト : チケットの作成及び設定要件の入力

Step 2: デザイン : 設定ポリシーの導入先や登録ルールなどを決定
レコメンド機能の利用

Step 3: レビュー : 自動設定する内容の承認
Compliansチェックの利用

Step 4: 実装 : 設定する内容を自動で当該Firewallに設定要求

Step 5: 検証 : 自動設定したものが間違いなく設定されているかを検証する

Step 6: 監視 : 設定したルールについて
可視化対象としてモニタリング実施
(Security Manager)

- ・ルールレコメンデーション機能（推奨設定の提示）
要求された動作を実現するために、現在の動作を分析し、変更が必要なデバイスに対するセキュリティポリシーをデザインして提案を実施します。
ルールの挿入位置を最適に判断して提示されるため、設計作業の効率が劇的にアップします。
※手動による設計も可能

通信要件に対する提案

Enterprise | AccessRequest_11_11_0 | CM-18 | Rule Recommendations

1 Create Change Plan 2 Review & Choose Objects

Requirement Details View Details

Source	User	Destination	Applications	Service	Action
192.168.1.111	(empty)	118.87.5.124	(empty)	https	Accept

Device Group: All Devices x Requirement Scope to Consider: ☒ Partial address space ☐ Complete address space Run

Devices with Changes (3) Error (0)

Select the recommended changes to apply.

Policy	Scope	Description	Details
FortiGate60D(L3)	(none)	Recommend creating a rule above the referenced rule because it completely matches the requested access but with a different action	Explain
JuniperSRX 210H	(none)	Recommend creating a rule above the referenced rule because it completely matches the requested access but with a different action	Explain
PaloAltoGW	local	Recommend creating a rule above the referenced rule because it completely matches the requested access but with a different action	Explain

Next Cancel

詳細なデザイン

Policy	Scope	Description
JuniperSRX 210H	(none)	Access Path Analysis
(none)	(none)	Add new host object: 118.87.5.124
From: trust To: untrust	(none)	Recommend creating a rule above the referenced rule because it completely matches the requested access but with a different action

Create this rule above the reference rule:

An orange token indicates a change input that cannot be resolved (matched) to an existing or newly created object. Please click on the orange tokens to search for existing objects. You can also create new objects, if necessary.

Rule Number: (empty)

Source Zone: trust x Destination Zone: untrust x

Source: 192.168.1.111 x Destination: 118.87.5.124 x Service: junos-https x

Rule Name: CM-18 Action: Accept Log: Enabled Comments:

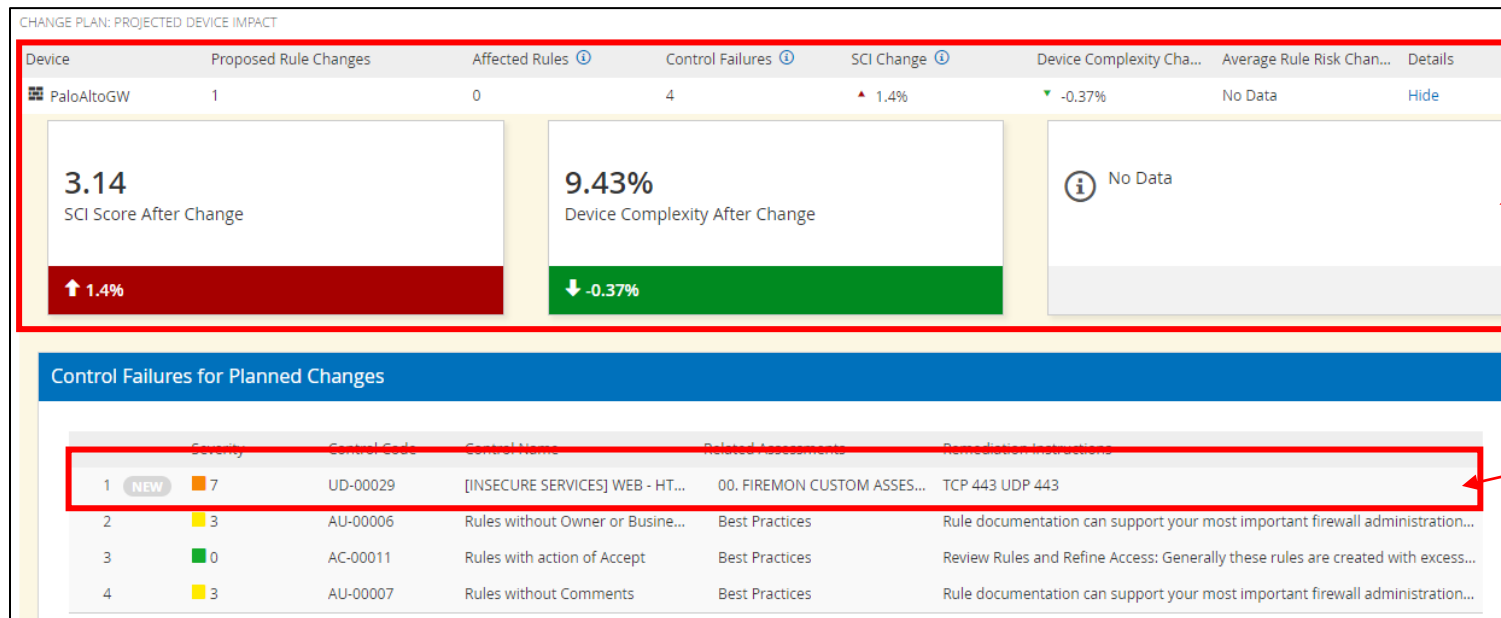
Hide Reference Rule

Rule Number	Source Zone	Destination Zone	Source	Destination	Service
17	trust	untrust	Any	Any	Any

Rule Name	Action	Log	Comments
trust-to-untrust	Drop	Disabled	(empty)

- ・コンプライアンスチェック機能

設計された“セキュリティポリシー”に対するコンプライアンスチェックを行うことで、実際に“セキュリティポリシー”が設定された時、ネットワークセキュリティにどのような影響があるかを“設定前”に確認することが可能です。



設定を反映した場合の
数値化したリスクの増減提示

コンプライアンス違反の
詳細を提示

FireWallの管理画面に全くアクセスすることなく、FireMon上から対象のFirewallに対してセキュリティポリシーの投入が可能です。

設計内容のImplement

Automation Assistance Run Selected Refresh Statuses 0 | 5 | 0 | 0 | 0 | 0

	Task							Implementation	
	Device	Connecting via	Policy	Scope	Change IDs	Dependencies	Description	Status	Comment
☒	JuniperSRX 2...			(none)	OBJ-24	(none)	Create network host object: 118.87.5.124	Pending	
☒	JuniperSRX 2...		From: trust T...	(none)	RUL-23	OBJ-24	Recommend creating a rule above the referenced rul...	Pending	
☒	PaloAltoGW			local	OBJ-22	(none)	Create network host object: 192.168.1.111	Pending	
☒	PaloAltoGW			local	OBJ-23	(none)	Create network host object: 118.87.5.124	Pending	
☒	PaloAltoGW		Policy	local	RUL-22	OBJ-22, OBJ-23	Recommend creating a rule above the referenced rul...	Pending	

Statusが"Pending"から
"Completed"になると設定が完了

Automation Assistance Run Selected Refresh Statuses 0 | 0 | 0 | 0 | 5 | 0

	Task							Implementation	
	Device	Connecting via	Policy	Scope	Change IDs	Dependencies	Description	Status	Comment
	JuniperSRX 2...			(none)	OBJ-24	(none)	Create network host object: 118.87.5.124	Completed	
	JuniperSRX 2...		From: trust T...	(none)	RUL-23	OBJ-24	Recommend creating a rule above the referenced rul...	Completed	
	PaloAltoGW			local	OBJ-22	(none)	Create network host object: 192.168.1.111	Completed	
	PaloAltoGW			local	OBJ-23	(none)	Create network host object: 118.87.5.124	Completed	
	PaloAltoGW		Policy	local	RUL-22	OBJ-22, OBJ-23	Recommend creating a rule above the referenced rul...	Completed	

• Verify機能

FireMonが実施したImplementの内容と、対象Firewallの最新の設定内容を読み込んで検証を行い、Implementした内容が投入されていることを確認します。

Verification

Change Plan

Comments

Attachments

Task History

Ticket History

Hide All Requirements

Requirement REQ-19

Add Connectivity

Describe the (new) access desired

Source	Destination	Service	Action	Expiration Date
192.168.1.111	118.87.5.124	https	Accept	(empty)
User	URL Categories	Application	Security Profile	Review Date
(empty)	(empty)	(empty)	(empty)	(empty)
Device Group				
All Devices				

CHANGE PLAN

☒ System Notes

Changes				Verification		
Change ID	Policy	Scope	Description	Details	Status	Comment
JuniperSRX 210H						
OBJ-24	(none)	(none)	Create network host object: 118.87.5.124	Show	Pending	System note: Did not meet all autoverification requirements
RUL-23	From: trust To: untrust	(none)	Recommend creating a rule above the referenced rule because it completely matches the requested access but with a different action	Show	Pending	System note: Did not meet all autoverification requirements
PaloAltoGW						
OBJ-22	(none)	local	Create network host object: 192.168.1.111	Show	Pending	System note: Did not meet all autoverification requirements
OBJ-23	(none)	local	Create network host object: 118.87.5.124	Show	Pending	System note: Did not meet all autoverification requirements
RUL-22	Policy	local	Recommend creating a rule above the referenced rule because it completely matches the requested access but with a different action	Show	Pending	System note: Did not meet all autoverification requirements