働き方改革待ったなし！
残業せずにファイアウォールのポリシー管理をする方法とは？

2019年11月7日
SB C&S株式会社
ICT事業本部 販売推進本部 ネットワーク＆セキュリティ統括部
ネットワーク＆セキュリティMD1部 セキュリティプロダクト推進課
北畠 裕史

本日のアジェンダ

1. セキュリティ管理者が抱える課題
2. FireWallの統合管理ソリューションのご紹介
3. 工数削減効果

セキュリティ管理者が抱える課題

複雑化

- ✓ アプリ/サービス増加に伴うポリシー数の増加
- ✓ マイクロセグメンテーションによる台数増加
- ✓ UTMマルチベンダー管理の必要性

設定ミスのリスク

- ✓ 設定ミスによる情報漏えいリスク
- ✓ 無駄なルールによるパフォーマンス低下
- ✓ 企業コンプライアンスへの準拠

スピードアップ

- ✓ DevOpsによるアプリ開発サイクルのスピードアップ
- ✓ 脆弱性発生による、緊急ルール変更の増加
- ✓ 承認プロセスの欠落


働き方改革
生産性UP
performance

課題山積・・・

FireMonで
FireWallの統合管理と自動化を実現

課題山積・・・

FIREMON

FireMonとは

FireMon社について

- 2001年設立（「NSPM」カテゴリにおいてシェア**No.1**）
  2018年に日本への展開開始
- 実績 WWで1,500社（53か国）以上の導入実績
  過去5年間の年平均成長率：約45%成長
- Fortune500へ100社以上の導入

FIREMON

FireMon本社
Overland Park,
Kansas, USA

国内ご支援体制

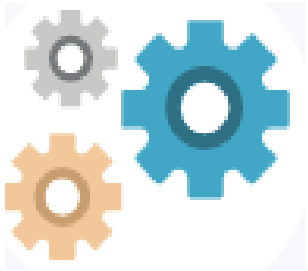
SB C&S
パートナー支援・ディストリビューター

JSECURITY
日本語による保守・テクニカルサポート

FireMonで出来る事

統合管理

コンプラ対策



自動化

FireMonで出来る事

統合管理

- ✓ マルチベンダー間のFireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の比較分析・レポート

コンプラ対策

- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック

自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

FireMonで出来る事

統合管理

- ✓ マルチベンダー間のFireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の比較分析・レポート

コンプラ対策

- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック

自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

マルチベンダー環境

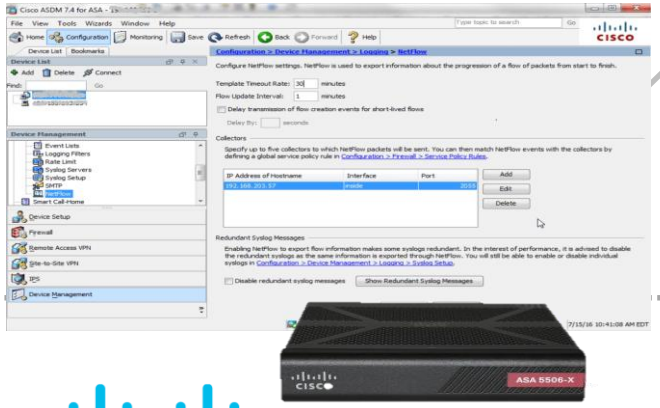
Internet

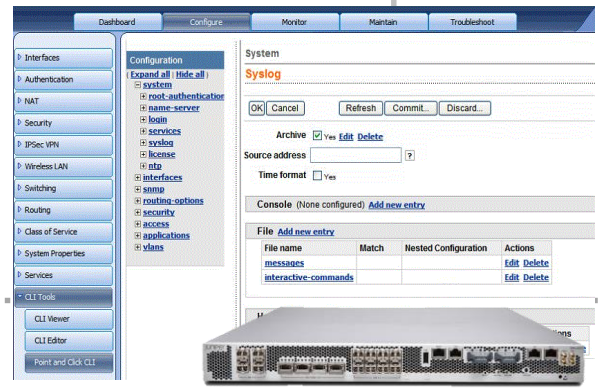
セキュリティ管理者

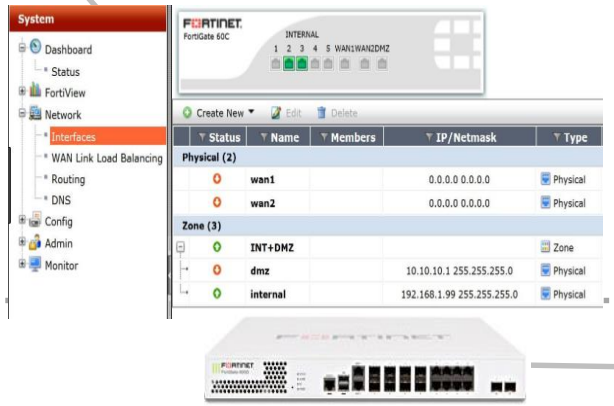
Cisco技術者

Juniper技術者

Fortinet技術者





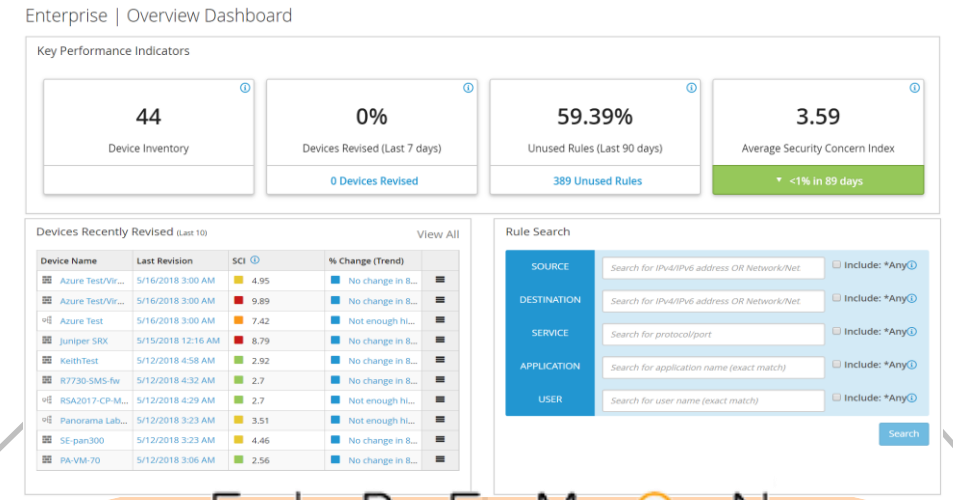


拠点A

拠点B

拠点C

一元管理



統合管理

セキュリティ管理者

FIREMON

cisco Partner
Distribution Partner

JUNIPER NETWORKS

FORTINET

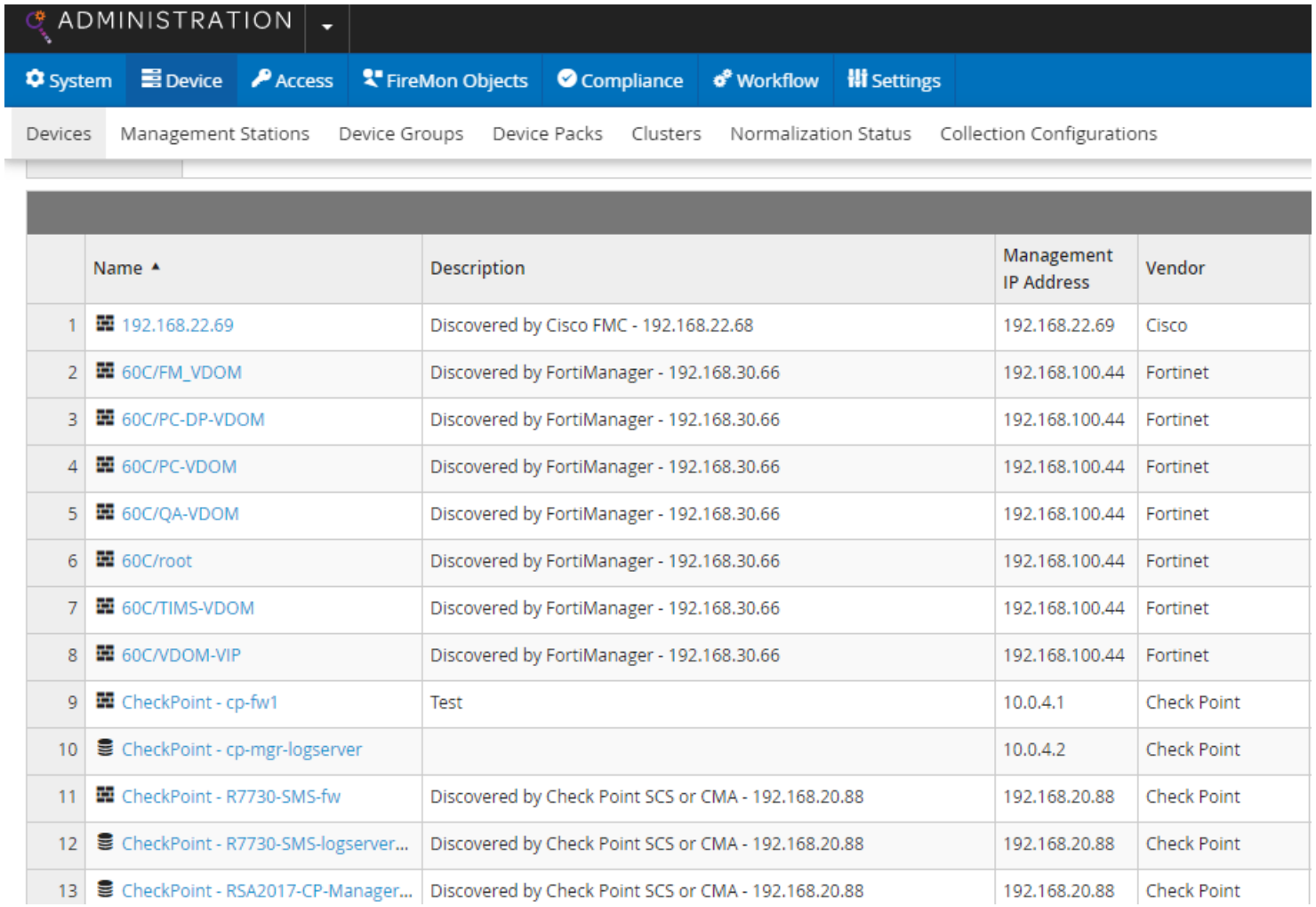
拠点A

拠点B

拠点C

マルチベンダーFWを一元管理

統合管理



	Name	Description	Management IP Address	Vendor
1	192.168.22.69	Discovered by Cisco FMC - 192.168.22.68	192.168.22.69	Cisco
2	60C/FM_VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
3	60C/PC-DP-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
4	60C/PC-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
5	60C/QA-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
6	60C/root	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
7	60C/TIMS-VDOM	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
8	60C/VDOM-VIP	Discovered by FortiManager - 192.168.30.66	192.168.100.44	Fortinet
9	CheckPoint - cp-fw1	Test	10.0.4.1	Check Point
10	CheckPoint - cp-mgr-logserver		10.0.4.2	Check Point
11	CheckPoint - R7730-SMS-fw	Discovered by Check Point SCS or CMA - 192.168.20.88	192.168.20.88	Check Point
12	CheckPoint - R7730-SMS-logserver...	Discovered by Check Point SCS or CMA - 192.168.20.88	192.168.20.88	Check Point
13	CheckPoint - RSA2017-CP-Manager...	Discovered by Check Point SCS or CMA - 192.168.20.88	192.168.20.88	Check Point

Cisco Partner
Distribution Partner

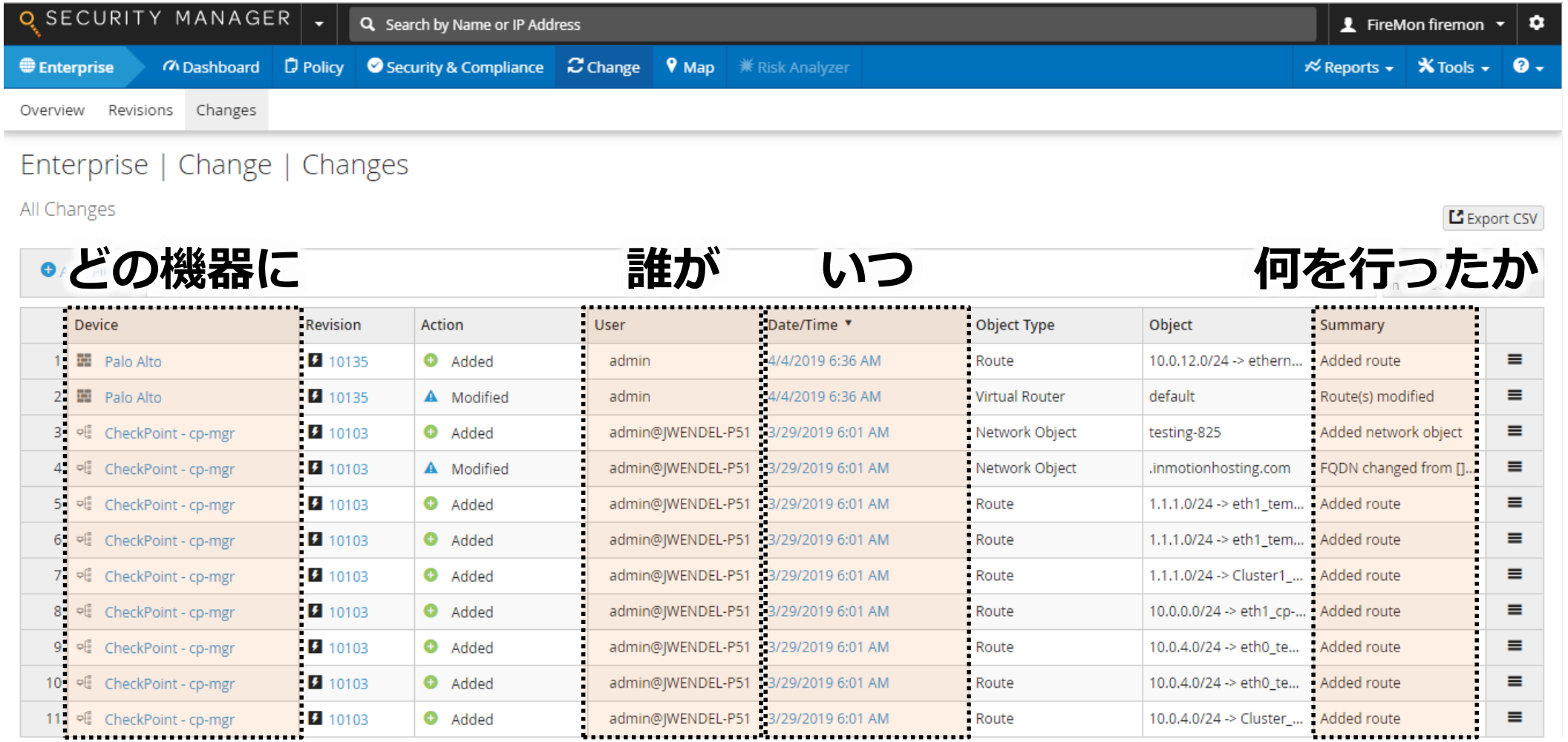
FORTINET

Check Point
SOFTWARE TECHNOLOGIES LTD.

異なるベンダーのFWの設定内容を自動で反映・一元的に可視化

リアルタイム変更履歴の管理

統合管理

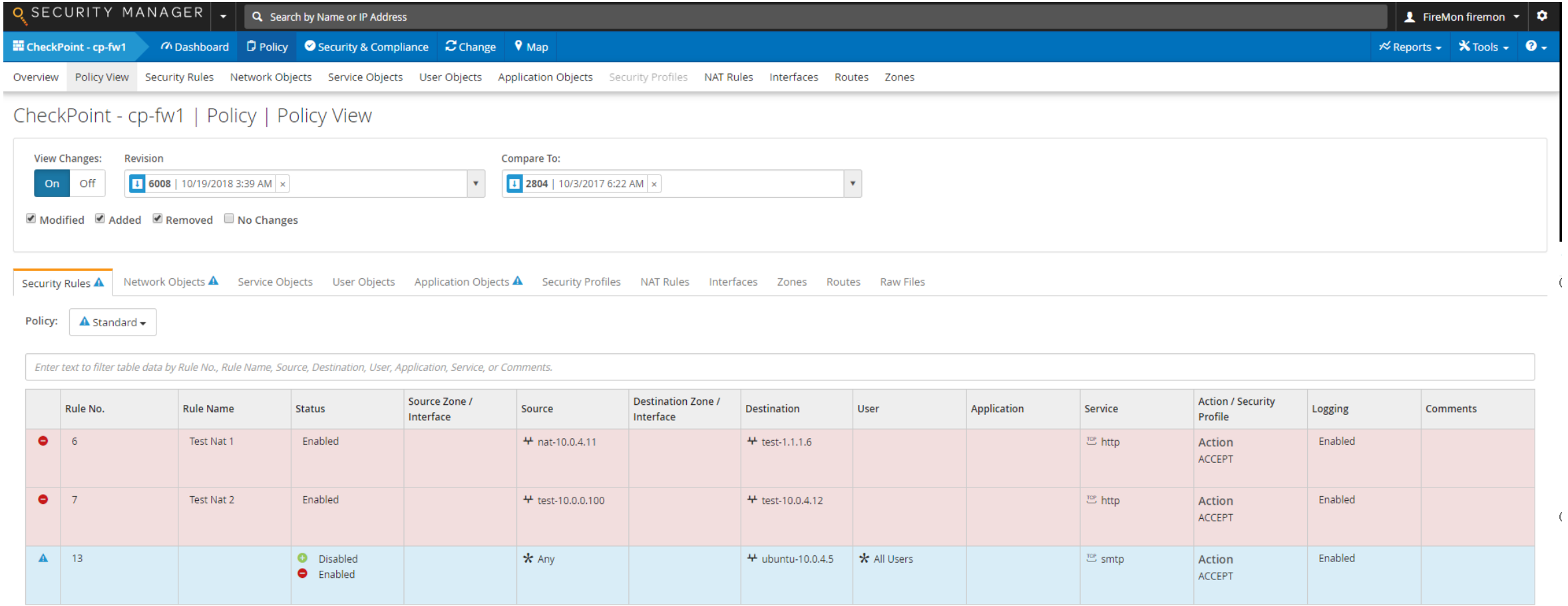


	Device	Revision	Action	User	Date/Time	Object Type	Object	Summary
1	Palo Alto	10135	Added	admin	4/4/2019 6:36 AM	Route	10.0.12.0/24 -> ethern...	Added route
2	Palo Alto	10135	Modified	admin	4/4/2019 6:36 AM	Virtual Router	default	Route(s) modified
3	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Network Object	testing-825	Added network object
4	CheckPoint - cp-mgr	10103	Modified	admin@JWENDEL-P51	3/29/2019 6:01 AM	Network Object	.inmotionhosting.com	FQDN changed from []...
5	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Route	1.1.1.0/24 -> eth1_tem...	Added route
6	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Route	1.1.1.0/24 -> eth1_tem...	Added route
7	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Route	1.1.1.0/24 -> Cluster1_...	Added route
8	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Route	10.0.0.0/24 -> eth1_cp-...	Added route
9	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Route	10.0.4.0/24 -> eth0_te...	Added route
10	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Route	10.0.4.0/24 -> eth0_te...	Added route
11	CheckPoint - cp-mgr	10103	Added	admin@JWENDEL-P51	3/29/2019 6:01 AM	Route	10.0.4.0/24 -> Cluster_...	Added route

誰が・いつ・どの機器に・何を行ったか、履歴を管理

リアルタイム変更履歴の比較

統合管理



設定変更の前と後の内容を、並べて比較確認

FireMonで出来る事

統合管理

- ✓ マルチベンダー間のFireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の比較分析・レポート

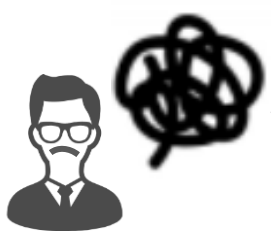
コンプラ対策

- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック

自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

重複ルール

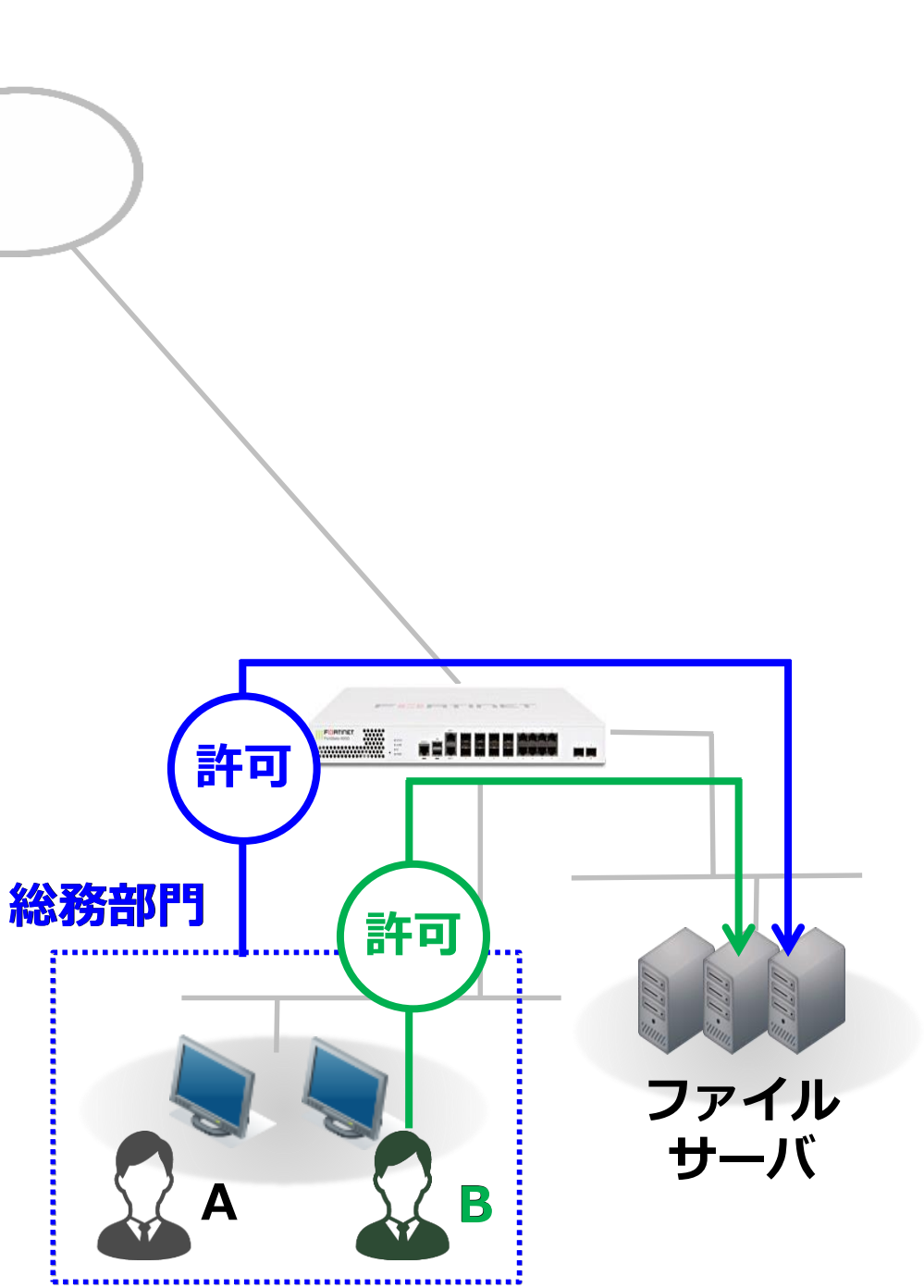


セキュリティ管理者

①総務部門からのアクセスを許可

②総務部門の担当Bからのアクセスを許可

無駄な重複ルール

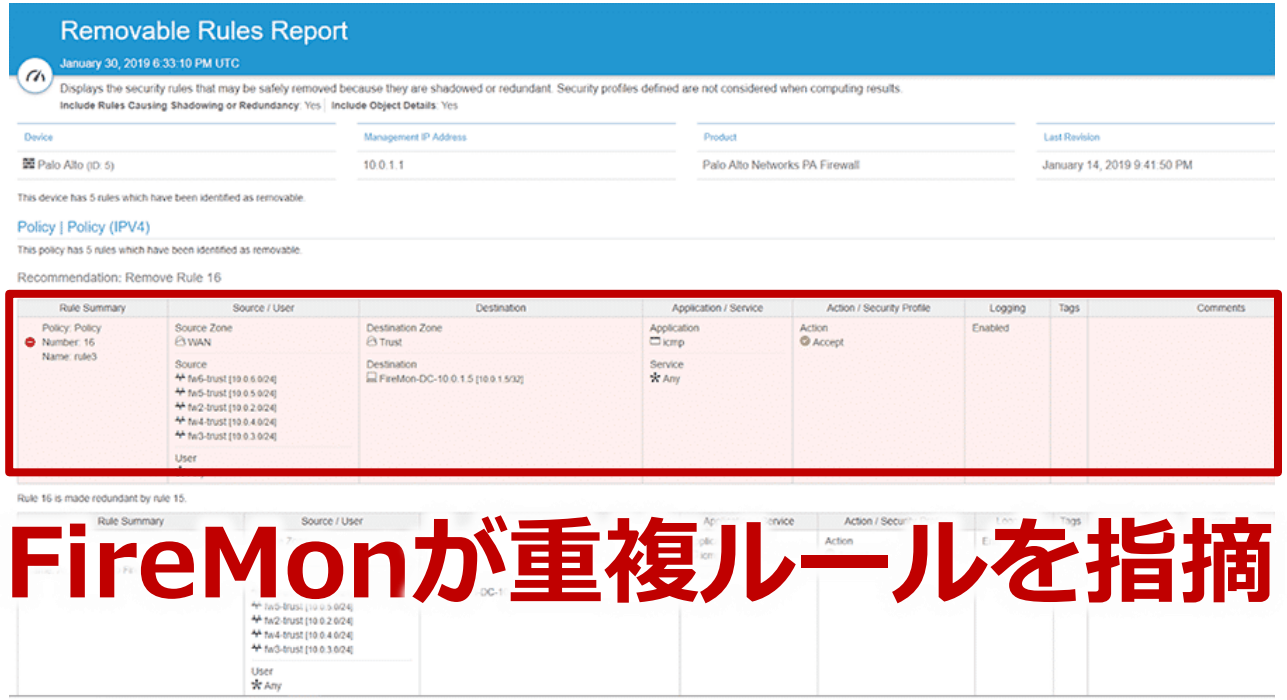


重複ルールのチェック

コンプラ対策

セキュリティ管理者

FIREMON



Removable Rules Report

January 30, 2019 6:33:10 PM UTC

Displays the security rules that may be safely removed because they are shadowed or redundant. Security profiles defined are not considered when computing results.

Include Rules Causing Shadowing or Redundancy: Yes | Include Object Details: Yes

Device	Management IP Address	Product	Last Revision
Palo Alto (ID: 5)	10.0.1.1	Palo Alto Networks PA Firewall	January 14, 2019 9:41:50 PM

This device has 5 rules which have been identified as removable.

Policy | Policy (IPV4)

This policy has 5 rules which have been identified as removable.

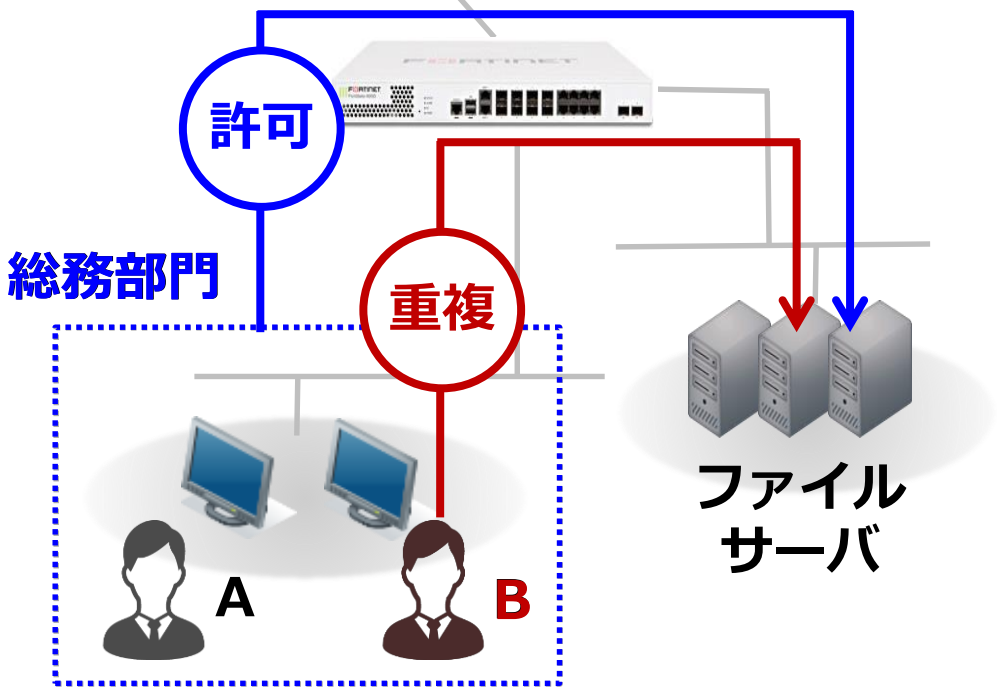
Recommendation: Remove Rule 16

Rule Summary	Source / User	Destination	Application / Service	Action / Security Profile	Logging	Tags	Comments
Policy: Policy Number: 16 Name: rule3	Source Zone: WAN Source: fw6-trust [10.0.6.0/24], fw5-trust [10.0.5.0/24], fw2-trust [10.0.2.0/24], fw4-trust [10.0.4.0/24], fw3-trust [10.0.3.0/24] User	Destination Zone: Trust Destination: FireMon-DC-10.0.1.5 [10.0.1.5/32]	Application: icmp Service: Any	Action: Accept	Enabled		

Rule 16 is made redundant by rule 15.

Rule Summary	Source / User	Action / Secur
	fw3-trust [10.0.3.0/24], fw2-trust [10.0.2.0/24], fw4-trust [10.0.4.0/24], fw3-trust [10.0.3.0/24] User: Any	Action

FireMonが重複ルールを指摘



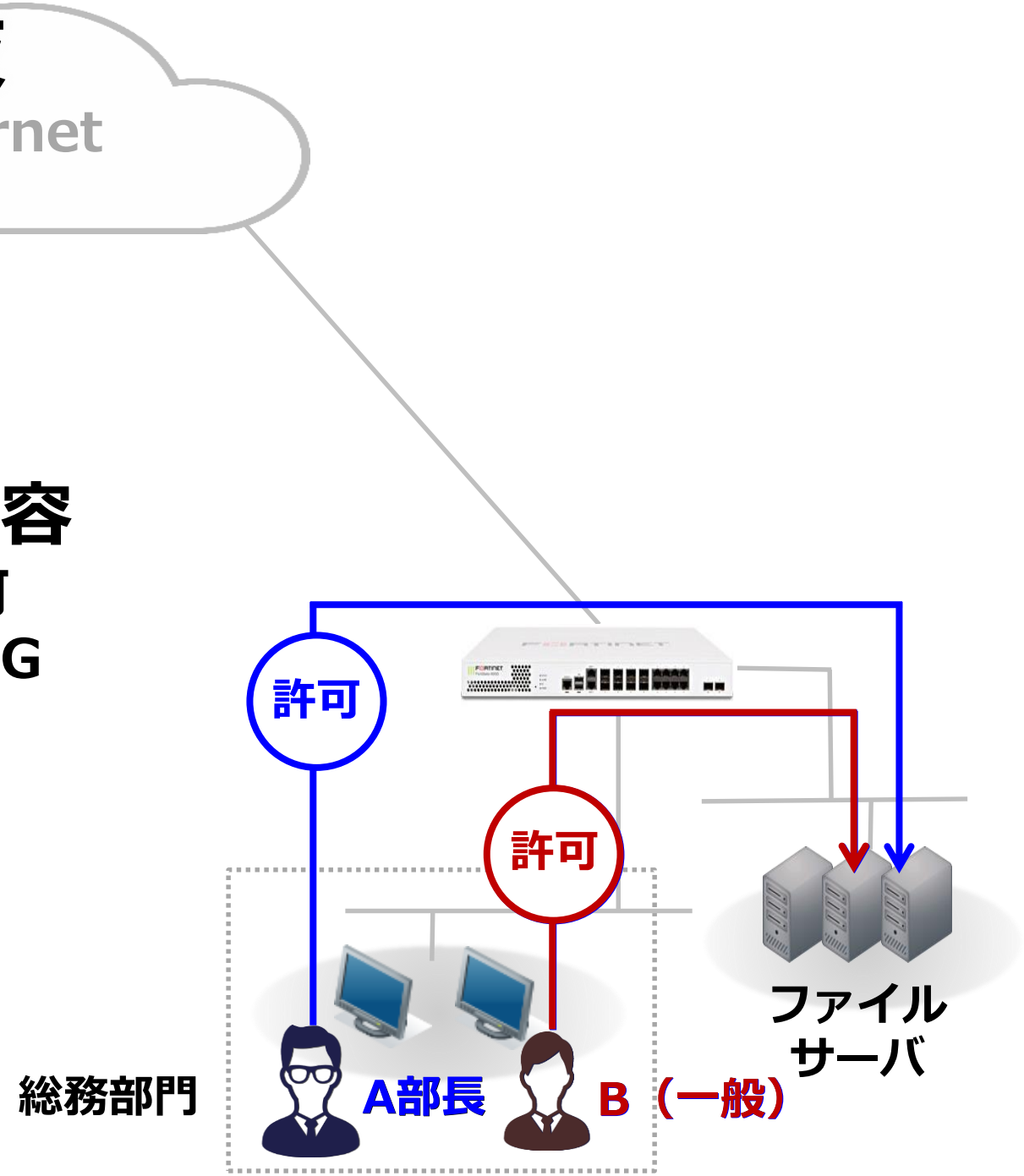
設定ミスによる内部規定違反

セキュリティ管理者

内部規定にそった正しい設定内容

- 総務部門のA部長からのアクセスを許可
- 総務部門のB（一般社員）はアクセスNG

設定ミスにより
Bからのアクセス許可

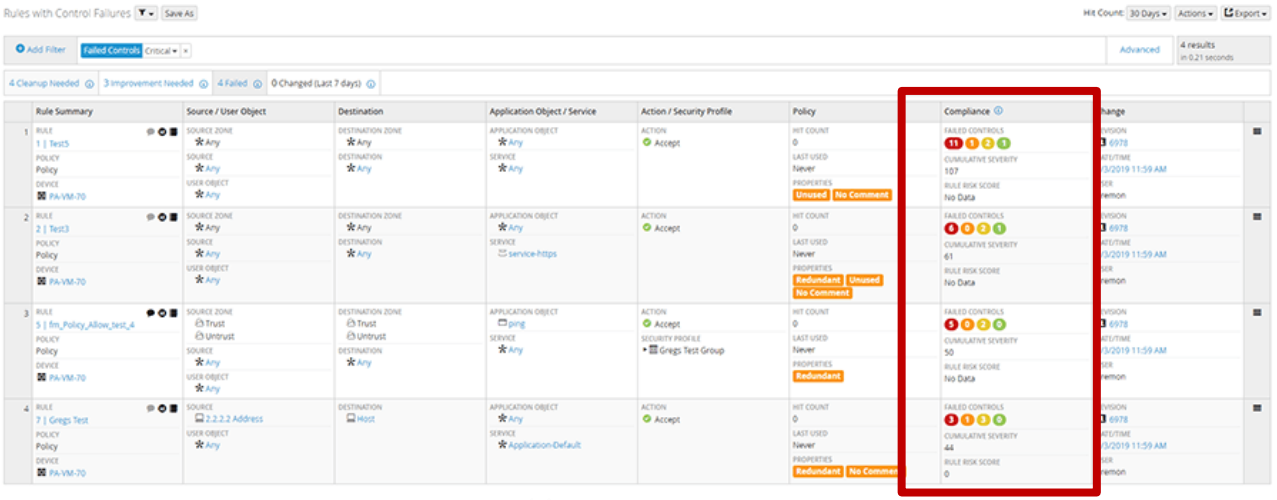


内部規定への遵守状況をチェック

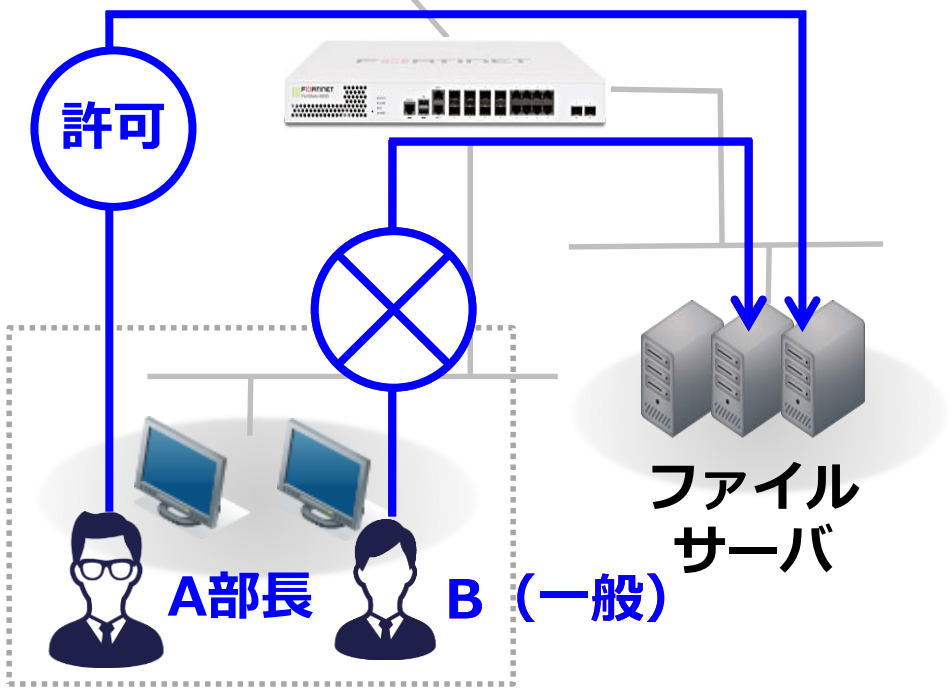
コンプラ対策

セキュリティ管理者

FIREMON



FireMonが規定違反を指摘



FireMonで出来る事

統合管理

- ✓ マルチベンダー間のFireWallを一元管理
- ✓ リアルタイム変更履歴管理
- ✓ 変更されたリビジョン毎の比較分析・レポート

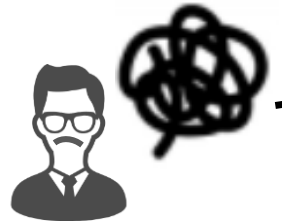
コンプラ対策

- ✓ 重複ルールのチェックやポリシー毎の使用率分析によるセキュリティ強化
- ✓ 会社内部のセキュリティ基準への遵守状況チェック

自動化

- ✓ ワークフローによる承認プロセス
- ✓ レコメンデーション機能
- ✓ ポリシーの自動プッシュ

頻発するポリシー変更依頼



セキュリティ管理者

Internet

このポート
空けて！

至急
対応依頼

ここのポート
閉じて下さい

緊急アラート
発生

新作アプリの
検証間環境を

CISCO
Partner
Distribution Partner

!!

拠点A

JUNIPER
NETWORKS

!!

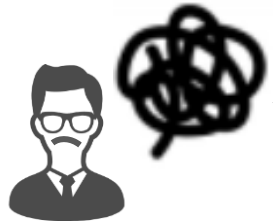
拠点B

FORTINET

!!!!

拠点C

頻発するポリシー変更依頼



セキュリティ管理者

- 毎日何件ものポリシー変更依頼が・・
- 設定ミスがないよう、細かく内容をチェック
- FW機器ごとにポリシーの設定変更を実施

ワークフロー/レコメンド機能

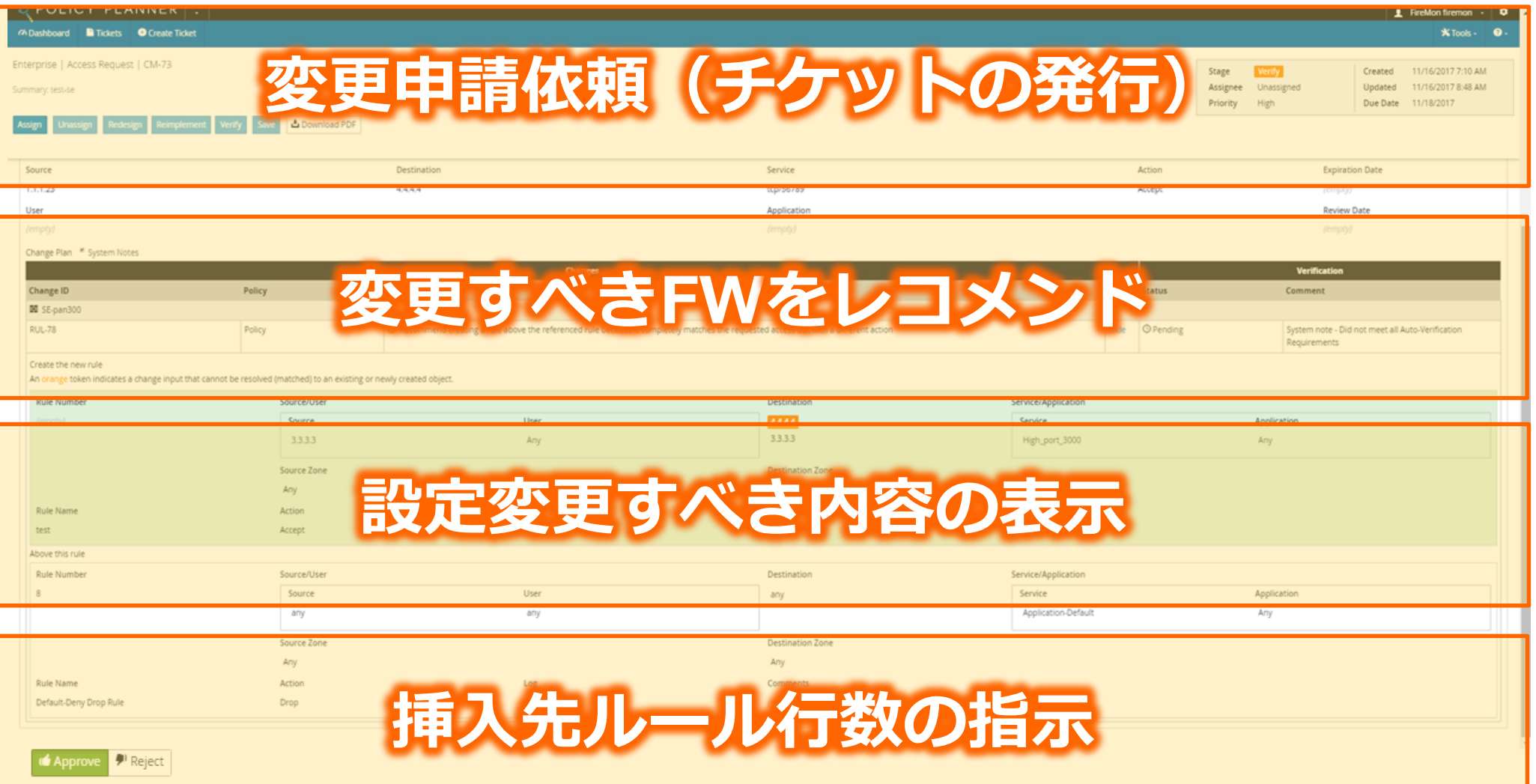
自動化

1 変更申請依頼（チケットの発行）

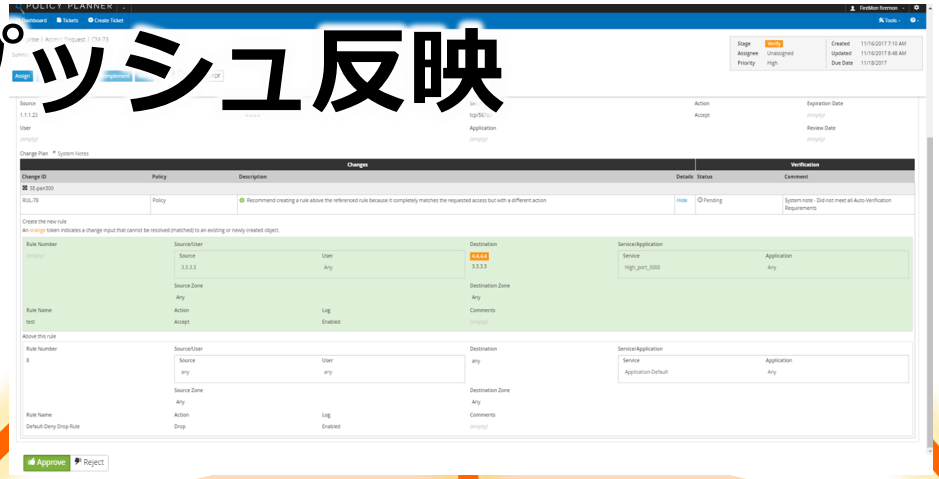
2 変更すべきFWをレコメンド

3 設定変更すべき内容の表示

4 挿入先ルール行数の指示



ポリシーを自動プッシュ反映



自動化

セキュリティ管理者

FIREMON

CISCO Partner
Distribution Partner

拠点A

JUNIPER NETWORKS

拠点B

FORTINET

拠点C

導入例から見る
費用・工数削減効果

導入想定

SB C&S

FireWall導入環境

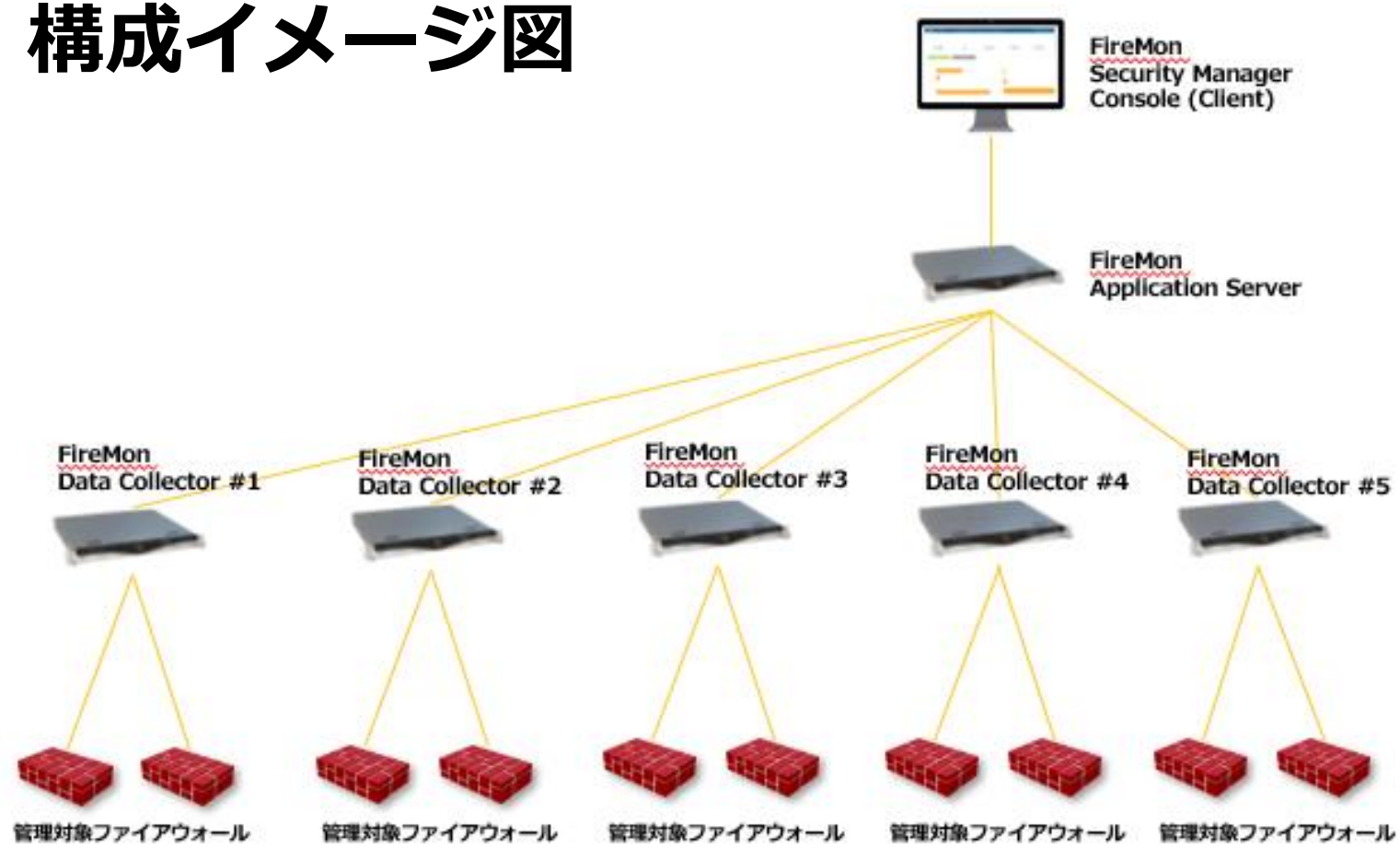
管理対象FW数：**100台**

総FWルール数：**5,000行**

FWの変更申請数：**50件**/週

FWポリシー棚卸：**1回**/四半期

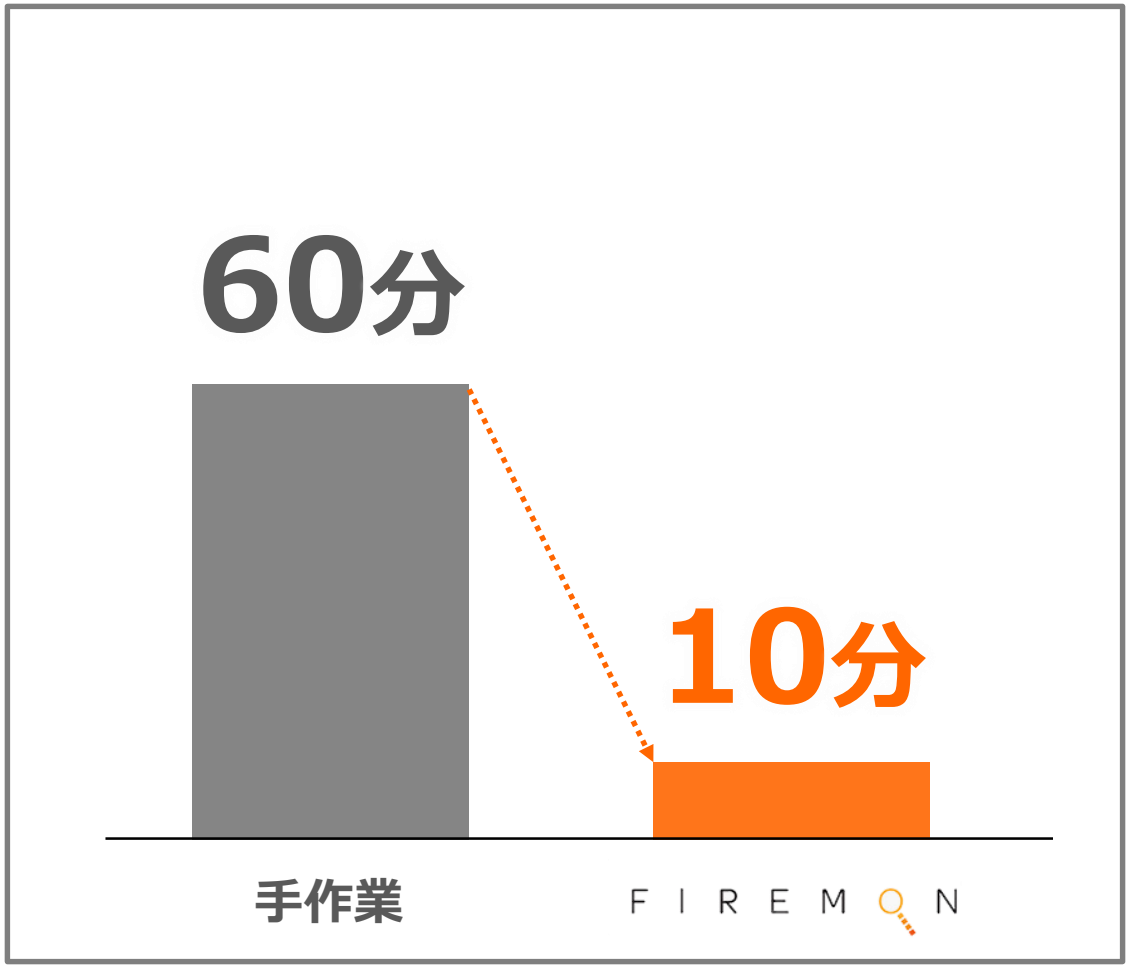
構成イメージ図



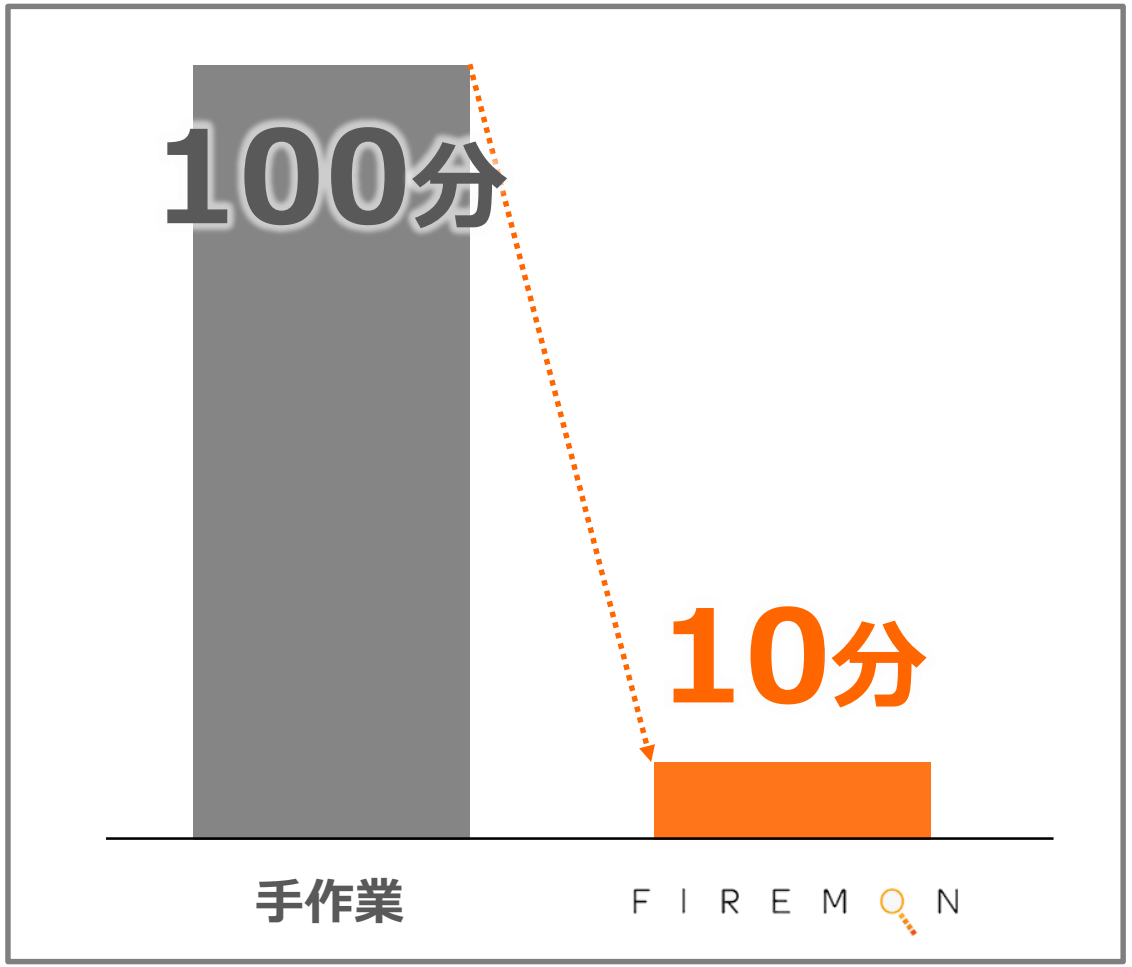
導入効果（FW1台あたり）

SB C&S

ポリシー設定変更作業



ポリシー棚卸作業



導入効果

SB C&S

ポリシー設定変更作業

約12.5人月

約2,000万円

削減

FireWall導入環境

管理対象FW数：**100台**

総FWルール数：**5,000行**

FWの変更申請数：**50件**/週

FWポリシー棚卸：**1回**/四半期

導入効果

SB C&S

FireWall導入環境

管理対象FW数：**100台**

総FWルール数：**5,000行**

FWの変更申請数：**50件**/週

FWポリシー棚卸：**1回**/四半期

ポリシー棚卸作業

約3.8人月

約600万円

削減

導入効果

設定ミスによる
重大な情報漏洩事故へのリスク

FireMonの導入効果まとめ

統合管理

コンプラ対策

自動化

「人」への負担を大幅軽減し、
「自動化」により運用のスピードアップと
設定ミス防止を同時に実現！

SB C&S

製品に関するお問い合わせ
無償検証(PoC)のご依頼お待ちしております

※お問い合わせはこちら

↓


SB C&S