

# FIREMON



## Improve Security **Operations** Improve Security **Outcomes**

Automation at play: How automation elevates your network security posture  
Dawid Kowalski– Sr Technical Director EMEA

Improve Security **Operations**. Improve Security **Outcomes**.

# Would you agree?

You've spent a lot of money on....



# Consequences of Ignoring Security Policies

*Through 2023, “99% of firewall breaches will be caused by misconfigurations, not firewalls.”*

**Gartner®**



**Exposed breach avenues and vulnerabilities** from policy misconfigurations



**Run the risk of unplanned outages** due to configuration errors in firewall policies



**Increased staffing costs** to keep up with manual change processes and compliance reporting



**Incur fines and risk lawsuits from compliance violations** caused by firewall changes

**Assigner:** Fortinet

**Published:** 2022-10-18 **Updated:** 2022-10-19

An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

## Product Status

Vendor & Product	Affected
Fortinet	FortiOS 7.2.1, 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0; FortiProxy 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0; FortiSwitchManager 7.2.0, 7.0.0
Fortinet FortiOS, FortiProxy, FortiSwitchManager	

## References

- <https://fortiguard.com/psirt/FG-IR-22-377>
- <http://packetstormsecurity.com/files/169431/Fortinet-FortiOS-FortiProxy-FortiSwitchManager-Authentication-Bypass.html>

View additional information about [CVE-2022-40684](#) on NVD.

(Note: The NVD is not operated by the CVE Program)

<https://www.cve.org/CVERecord?id=CVE-2022-40684>

<https://www.fortinet.com/blog/psirt-blogs/update-regarding-cve-2022-40684>

```
# show user local
edit "fortigate-tech-support"
    set accprofile "super_admin"set vdom "root"
    set password ENC [...]
next
```

Fortinet recommends that customers validate their configuration to ensure that no unauthorized changes have been implemented by a malicious third party, regardless of whether they have upgraded.



# Three steps to improve Network Security Posture Management

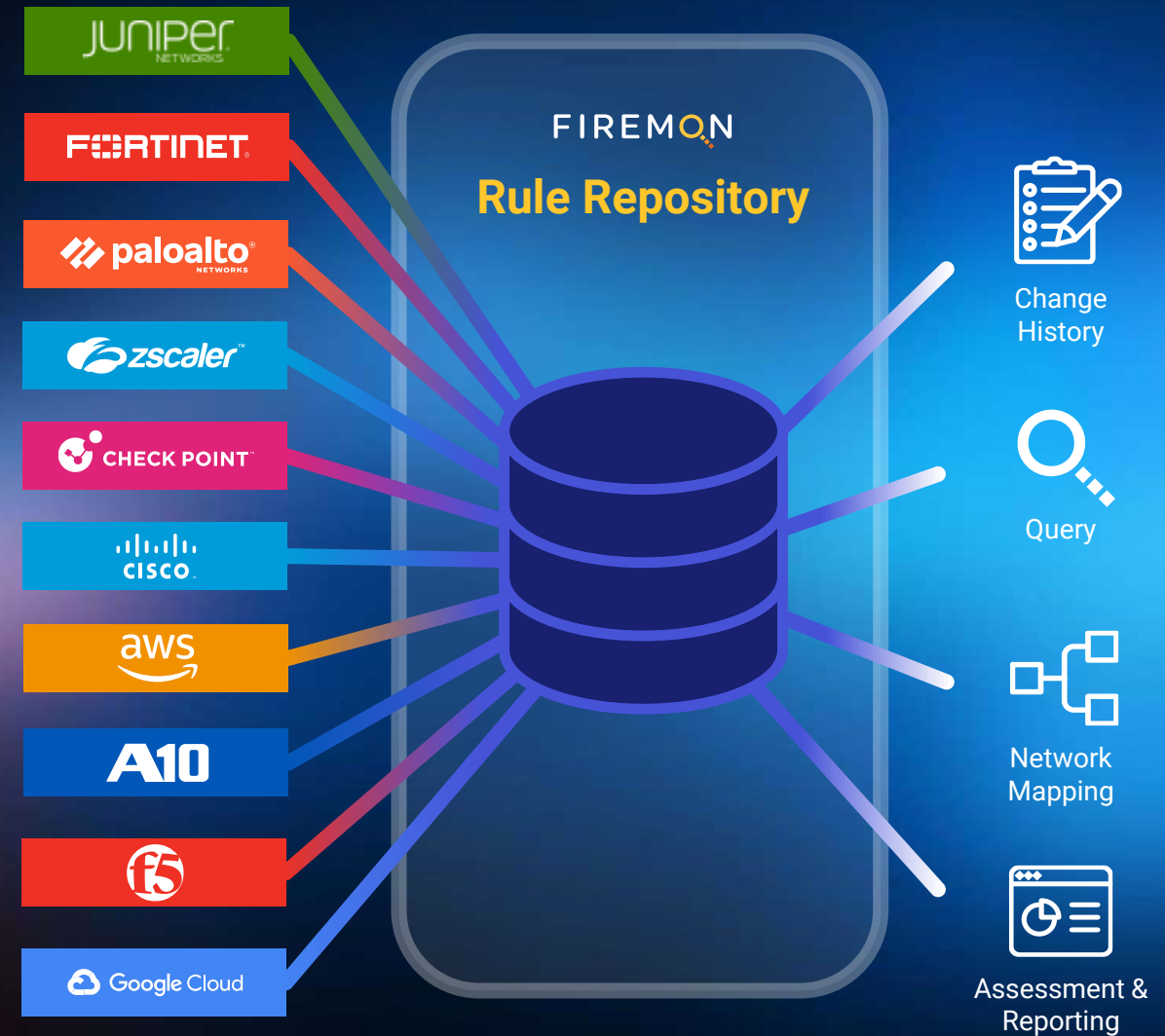




# A Real-Time **Inventory** of Devices and Rules

- Gathers devices and policies across the entire environment
- Translates multi-vendor policies into a consistent, centralized rule database
- Full visibility and control for reporting, audit tracking, and policy management
- Realtime change detection and analysis

**Out-of-the-box support for 80+ vendors and versions**





SECURITY MANAGER

All

Search by name or IP address

Search

dawid.kowalski@firemon.com

Enterprise

Overview

Policy

Compliance

Change

Topology

Risk Analyzer

Reports

Tools

Help

Enterprise | Overview Dashboard

GENERAL

15

Device Inventory

CHANGE

0%

Devices Revised (Last 7 days)

0 Devices Revised

CLEANUP

22.28%

Unused Rules (Last 90 days)

178 Unused Rules

COMPLIANCE

1.85

Average Security Concern Index

No change in 90 days

Devices Recently Revised (Last 10)

View All

Device Name	Last Revision	SCI	% Change (Trend)
Palo Alto-01-6	9/1/2022 6:43 PM	0.69	No change in 90 ...
Fortigate	7/21/2022 10:27 PM	2.41	No change in 90 ...
Cisco-ASA-00-07	6/1/2022 3:41 PM	2.43	No change in 90 ...
Juniper-SRX_20...	5/31/2022 5:09 PM	2.25	No change in 90 ...
cisco ASA 01-42	5/20/2022 10:17 PM	2.57	No change in 90 ...
Cisco-ASA-01-41	5/20/2022 10:17 PM	2.63	No change in 90 ...
demo-chkpt-R80...	5/13/2022 8:47 PM	0	Not enough hist...
demo-chkpt-gw	5/13/2022 8:45 PM	1.49	No change in 90 ...

Rule Search

SOURCE

Search for IPv4/IPv6 address or network/netmask

Include: \*Any

DESTINATION

Search for IPv4/IPv6 address or network/netmask

Include: \*Any

SERVICE

Search for protocol/port

Include: \*Any

APPLICATION

Search for application name (exact match)

Include: \*Any

USER

Search for user name (exact match)

Include: \*Any

Search



## All Devices | Policy | Security Rules

Access - allow public IP to private IP on more then three services



Save



Hit Count:

30 Days

Actions

devicegroup { id = 1 } AND rule { (((disabled = false and source is disjoint from ('10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16')) and destination intersects ('10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16')) and service.portcount > 3) }

Run

Reset Filter

Basic

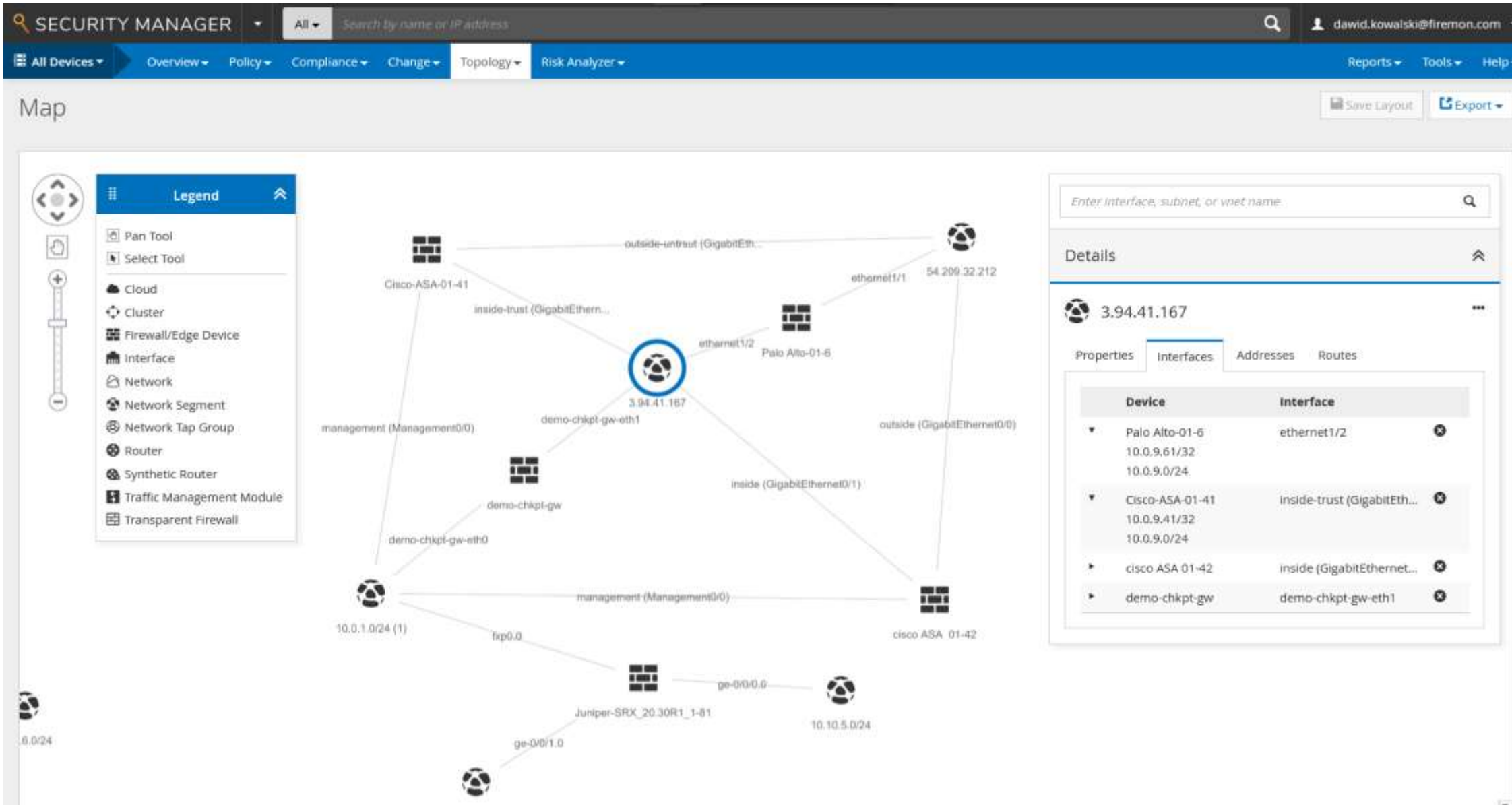
63 results

In 0.30 s

21 Cleanup Needed ? 51 Improvement Needed ? 61 Failed ? 0 Changed (Last 7 days) ?

Rule Summary	Source / User Object	Destination	Application Object / Service	Action / Security Profiles / ...	Cleanup	Compliance <span>?</span>	Change	Tags
1 RULE 25   ac1-21fb4a44/inbound/2 POLICY acl-21fb4a44/inbound DEVICE AWS Account (Keith)	SOURCE 66.17.5.141/32	DESTINATION * Any	SERVICE TCP/8000-8050	ACTION Accept	HIT COUNT 0 LAST USED Never PROPERTIES Logging Disabled No Comment	FAILED CONTROLS 2 3 5 0 CUMULATIVE SEVERITY 54 RULE RISK SCORE No Data	REVISION 56496 DATE/TIME 4/20/2021 4:46 PM USER firemon	
2 RULE 950   ac1-0493a4ec1408957e POLICY FMDEMO-MGMT/inbound DEVICE AWS Account Lab	SOURCE 4.4.4.4/32	DESTINATION * Any	SERVICE UDP/666-999	ACTION Accept	HIT COUNT 0 LAST USED Never PROPERTIES Logging Disabled No Comment	FAILED CONTROLS 2 2 5 0 CUMULATIVE SEVERITY 47 RULE RISK SCORE No Data	REVISION 62671 DATE/TIME 6/23/2022 2:28 PM USER DC_automated	
3 RULE 200   ac1-0f957b44bba9c6ba POLICY qa.dev1.spk1.mgmt-sn-acl/in	SOURCE 30.30.30.100/32	DESTINATION * Any	SERVICE TCP/30-35	ACTION Accept	HIT COUNT 0 LAST USED Never	FAILED CONTROLS 2 2 5 0 CUMULATIVE SEVERITY 47	REVISION 45640 DATE/TIME 11/22/2020 1:12 AM	





# Consolidated Compliance and Risk Assessments

- Over 20 preconfigured reports
- Customizable reporting and alerts using over 500 included controls
- Add custom controls with SiQL search
- Unified dashboard with real-time Security Concern Index (SCI)
- Access path analysis and “what if” attack assessments
- Qualys, Rapid7, and Tenable integrations enrich rules with vulnerability data

## COMPLIANCE



# 4.55

Average Security Concern Index

Increase of 5.08% in 70 days



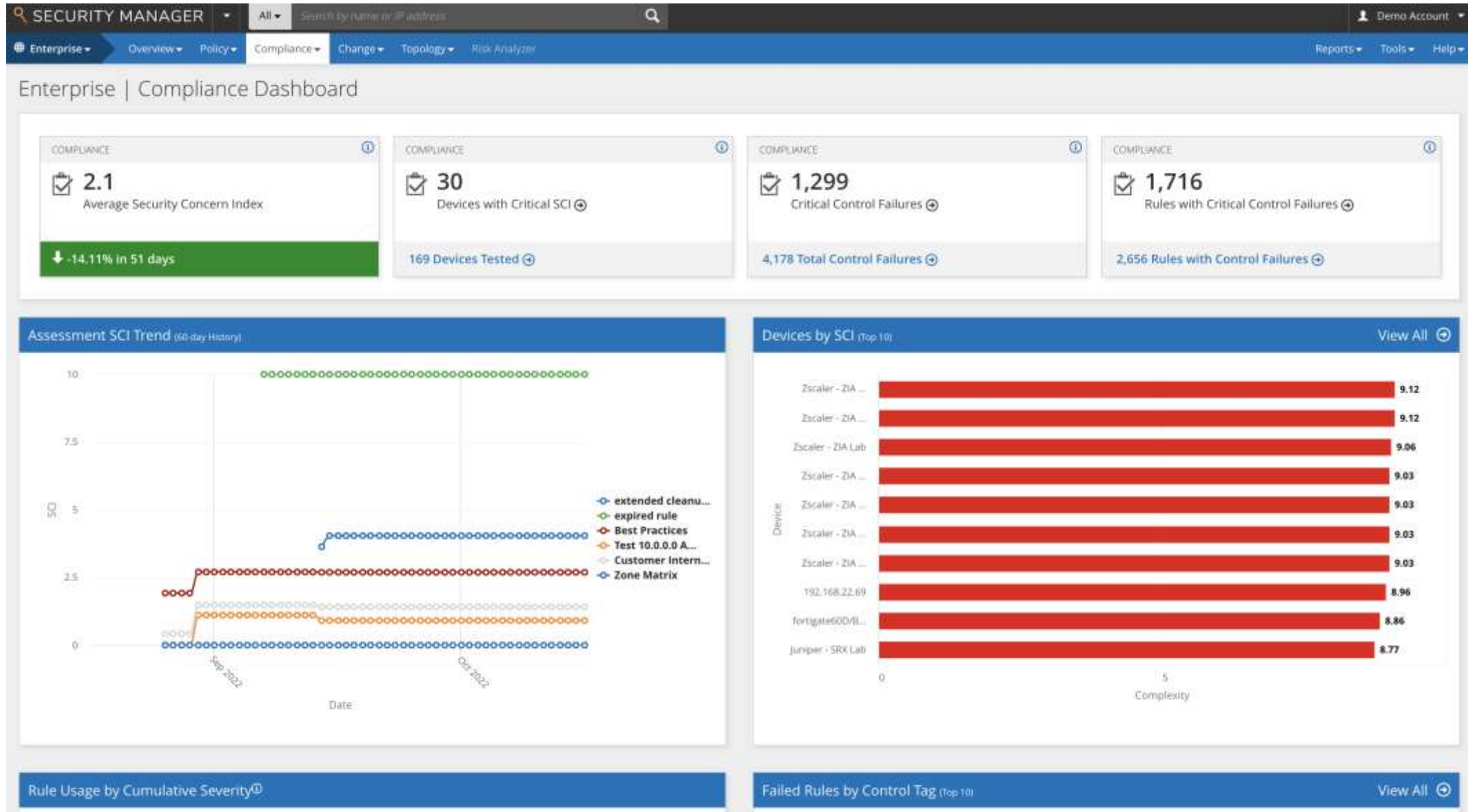
## Out-of-the-Box Reports Include:

### Compliance

- PCI-DSS
- NERC-CIP
- NIST
- HIPAA
- GDPR
- ISO/IEC 27001
- Sarbanes-Oxley

### Assessments

- Asset exposure analysis
- Insecure services
- App outage protection
- Rules allowing bad actors
- Overly Permissive access





SECURITY MANAGER

All

Search by name or IP address

All Devices

Overview

Policy

Compliance

Change

Topology

Risk Analyzer

Reports

Tools

Help

All Devices | Compliance | Assessment Results

All Assessment Results

			Control Failures ①				Other Control Results ①						
Assessment Name	Tested Devices	Controls in Asses...	Critical	High	Medium	Low	Info	Pass	Skip	Error	Average SCI Score	SCI Trend	
1 extended cleanup	153	11	43	100	343	0	0	712	296	2	4.04	▲ 3.93 %	Run Report
2 Z - Policy Optimiz...	2	5	0	2	1	1	2	4	0	0	0	0 %	Run Report
3 NIST (SP) 800-41	3	23	0	2	15	2	18	32	0	0	0	0 %	Run Report
4 My new best prac...	14	100	152	114	129	27	112	591	275	0	0	0 %	Run Report
5 expired rule	153	1	0	0	0	153	0	0	0	0	10	0 %	Run Report
6 Best Practices	153	97	1079	1019	838	29	1184	6605	4065	2	2.93	▼ 0.45 %	Run Report
7 08 - NERC CIP vs ...	1	10	1	0	1	0	0	6	0	2	0	0 %	Run Report
8 Z - Insecure High ...	2	4	1	0	0	0	0	7	0	0	0	0 %	Run Report
9 08 - CIS Cisco Fir...	1	66	62	0	0	0	0	4	0	0	0	0 %	Run Report
10 Base Security Ass...	1	30	6	2	7	3	4	8	0	0	0	0 %	Run Report
11 Palo Alto Firewall ...	3	73	6	26	152	5	6	24	0	0	0	0 %	Run Report
12 11 - RICOHSA Sec...	1	2	0	0	1	0	0	1	0	0	0	0 %	Run Report
13 01 - Best Practices	17	100	246	201	198	27	119	525	367	0	0	0 %	Run Report
14 Z - IT Security FW ...	3	11	15	0	0	0	3	15	0	0	0	0 %	Run Report
15 Test 10.0.0.0 Asse...	153	1	0	0	0	2	0	151	0	0	0.13	0 %	Run Report
16 PCI-DSS v3.2.1	11	49	18	0	115	21	149	68	168	0	0	0 %	Run Report
17 Customer Interne...	153	2	37	0	0	39	0	230	0	0	2.43	▼ 0.54 %	Run Report
18 Zone Matrix	153	3	0	0	0	0	0	459	0	0	0	0 %	Run Report
19 08 - CIS Palo Alto	1	72	6	26	153	5	6	24	0	0	0	0 %	Run Report



## POLICY OPTIMIZER

Rule Review

Reviews

Review ID: PO-663

Rule: 2 | Policy: Inside\_access\_out | Device: Cisco - RSA-CiscoASA

Stage

Review

Created

9/6/20

Assignee

Demo Account

Updated

9/8/20

Assign

Unassign

Complete

Cancel

Save

## Rule Summary

RULE  
2 | line 4POLICY  
Inside\_access\_outDEVICE  
Cisco - RSA-CiscoASA

## Source / User Object

SOURCE ZONE  
InsideSOURCE  
Inside-NET

## Destination

DESTINATION ZONE  
AnyDESTINATION  
Any

## Application Object / Service

SERVICE  
DM\_INLINE\_TCP\_1

## Action / Security Profiles / Sc...

ACTION  
Accept

## Cleanup

HIT COUNT (LAST 30 DAYS)  
0LAST USED  
2/8/2018 11:16 PM

## PROPERTIES

Unused

## Compliance

FAILED CONTROLS  
1 2 7 0CUMULATIVE SEVERITY  
51

## RULE RISK SCORE

No Data

## Change

REVISION  
45426DATE/TIME  
11/20/2020 4:56 AM

## USER

firemon

## Tags

## Rule Decision

## Rule Decision \*

Decertify

## Rule Actions \*

- ☐ Remove Rule
- ☐ Modify Rule
- ☐ Disable Rule

## Remarks \*

## Control Failures (Top 20)

Severity	Code	Control Name	Assessment
8	AC-00024	ANY in Destination with Action of Accept	Best Practices
7	UD-00286	Missing Change Control Number	extended cleanup
6	AC-00009	Bi-directional rules (partial match)	Best Practices
5	SC-00066	Allowed Access to Private Internet Source Address	NIST (SP) 800-41
5	RA-00063	Created & Unused Rules - 60 Days	extended cleanup
5	RA-00064	Created & Unused Rules - 90 Days	extended cleanup
4	RA-00065	Created & Unused Rules - 180 Days	extended cleanup



# Easily **Create and Update** Policies

- Rule creation and change workflows
- Intelligent rule design recommendations
- Audit history captured automatically
- Option to automatically deploy changes

## ITSM Integrations

servicenow

◆ Jira Software

➤ bmc



## Recommended Changes

1. Create new rule
2. Source: Any
3. User: Remote
4. Destination: internal web 1.1.1.2
5. Service: HTTP
6. ...

Deploy





**POLICY PLANNER** | Demo Account

Access Request | Dashboard | Tickets | Create Ticket | Tools | Help

### Enterprise | Access Request | CM-632

Summary: New app access

Stage: Design | Created: 6/29/2021 10:47 PM | Updated: 10/16/2022 8:44 PM | Due Date: 7/3/2021

Assign | Unassign | Cancel Ticket | Auto Design | Need More Info | Complete | Save | Download PDF

**Requirement REQ-600** APPROVED Edit

Add Connectivity | Describe the desired access

Source	Destination	Service	Action	Expiration Date
10.0.8.32	192.168.23.13	tcp/23236	Accept	(empty)

User	Application	Review Date
(empty)	(empty)	(empty)

CHANGE PLAN | ☒ System Notes | Recommendations | Add Change

Change ID	Policy	Description	Details
<b>PA-VM</b>			
Obj-1358	(none)	+ Create network host object: 10.0.8.32	Show ...
Obj-1360	(none)	+ Create network host object: 192.168.23.13	Show ...
Obj-1357	(none)	+ Create service object: tcp_23236	Show ...
RUL-1213	Policy	+ Recommend creating a new rule at the bottom of the policy. No other rules interfered with the requested access	Show ...
<b>PA-VM-PC-TEST</b>			
Obj-1355	(none)	+ Create network host object: 10.0.8.32	Show ...
Obj-1359	(none)	+ Create network host object: 192.168.23.13	Show ...
Obj-1356	(none)	+ Create service object: TCP-23236	Show ...
RUL-1214	Policy	+ Recommend creating a new rule at the bottom of the policy. No other rules interfered with the requested access	Show ...
<b>Palo Alto - PCI</b>			
RUL-1212	Policy	No action needed, referenced rule matches some or all of the access requested	Show ...



**POLICY PLANNER** | Demo Account

Access Request | Dashboard | Tickets | Create Ticket | Tools | Help

### Enterprise | Access Request | CM-632

Summary: New app access

Stage: **Review** | Assigned: Unassigned | Priority: High | Created: 6/29/2021 10:47 PM | Updated: 10/16/2022 8:51 PM | Due Date: 7/3/2021

Buttons: Assign | Unassign | Cancel Ticket | Reject | Approve | Save | Download PDF

CHANGE PLAN: PROJECTED DEVICE IMPACT

Device	Proposed Rule Changes	Affected Rules	Control Failures	SCI Change	Device Complexity Change	Average Rule Risk Change	Details
Palo Alto - PCI	0	0	0	▲ 5.26%	■ No Change	■ No Change	Show
PA-VM	1	0	6	▼ -0.36%	▼ -0.05%	■ No Change	Show
PA-VM-PC-TEST	1	0	6	▲ 0.98%	▼ -0.68%	■ No Change	Hide

**3.7**  
 SCI Score After Change  
 ↑ 0.98%

**25.05%**  
 Device Complexity After Change  
 ↓ -0.68%

**0**  
 Average Rule Risk Score After Change  
 0%

**Control Failures for Planned Changes**

	Severity	Control Code	Control Name	Related Assessments	Remediation Instructions
1	4	UD-00283	Rules Without Owner or Business Justification	extended cleanup	Rule documentation can support your most important firewall administration tasks. For example, rule...
2	7	SC-00031	TCP High Ports with Action of Accept	extended cleanup Best Practices	Review Rules and Refine Access: Generally these rules are created with excessive access due to poorly...
3	3	AU-00006	Rules without Owner or Business Justification	Best Practices	Rule documentation can support your most important firewall administration tasks. For example, rule...
4	7	UD-00286	Missing Change Control Number	extended cleanup	Verify all rules have a Change Control number.
5	0	AC-00011	Rules with action of Accept	Best Practices	Review Rules and Refine Access: Generally these rules are created with excessive access due to poorly...
6	3	AU-00007	Rules without Comments	Best Practices	Rule documentation can support your most important firewall administration tasks. For example, rule...





POLICY PLANNER

Demo Account

Access Request

Dashboard

Tickets

Create Ticket

Tools

Help

Enterprise | Access Request | CM-616

Summary: Demo Ticket 2 - FirePower

Download PDF

Stage: Completed

Assignee: Unassigned

Priority: Medium

Created: 6/7/2021 8:48 PM

Updated: 6/7/2021 9:38 PM

Due Date: 6/17/2021

Analysis

Verification

Change Plan

Comments

Attachments

Task History

Ticket History

Requirement REQ-582

Add Connectivity

Describe the [new] access desired

Source: 192.168.102.37

Destination: 192.168.100.37

Service: tcp/55555

Action: Accept

Expiration Date: (empty)

User: (empty)

Application: (empty)

Review Date: (empty)

CHANGE PLAN

☒ System Notes



Thank you!

**FIREMON**

Improve Security **Operations**. Improve Security **Outcomes**.

[firemon.com](https://firemon.com)

Learn more;  
Come see us at

**Hall 7,  
Booth  
7-401**