CHECK POINT™

Mastering Compliance

Unveiling the power of Compliance Blade

Roberto Quinones-Cruz

4-17-2024

YOU DESERVE THE BEST SECURITY

Agenda

- Introduction to the Compliance Blade
- Key features
- Technical Dive and How-To
- Demo
- Roadmap
- Conclusion and Q&A

Compliance Blade – Introduction

Compliance Blade lives in Security Management

Check Point Quantum

Helps you get the most security from your Check Point Platform

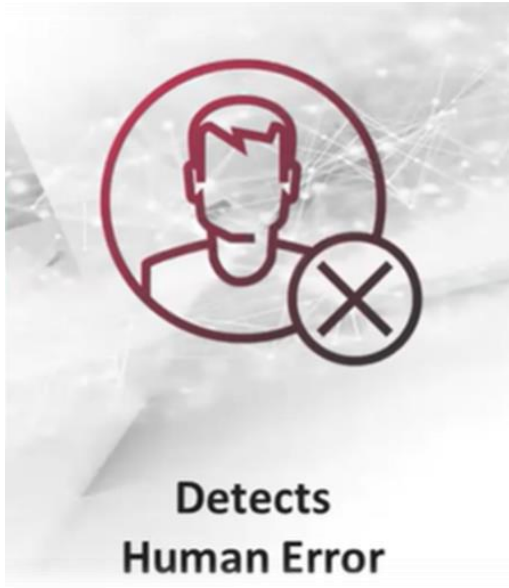
Configuration Management

- Eliminating Poor Configurations
  - Rules using any, any, accept
  - Anti-spoofing is disabled
  - Expired or unused rules
  - Uncommented or undocumented rules

- 300+ Predefined Check Point Security Best Practices
- Customizable best practices to match your environment
- Monitoring changes in real-time

Detect Changes

- Misconfiguration of Gaia OS parameters
- Building non-compliant firewall rules
- Adhering to company configuration standards
- Auditable changes

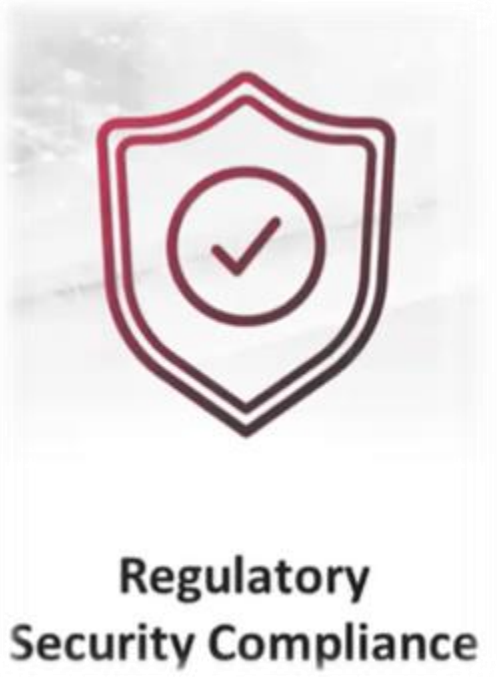


Mistakes happen, but mistakes can be detrimental to your security posture!

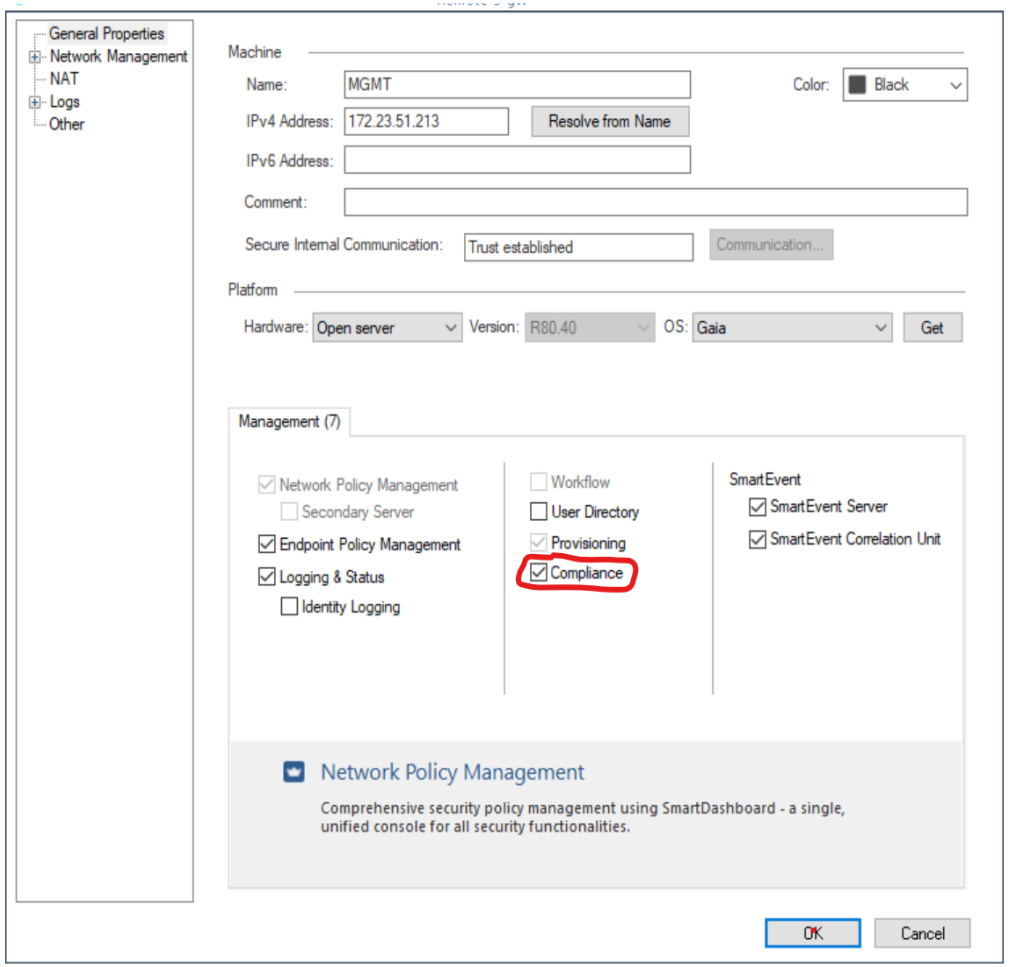
Regulatory Compliance

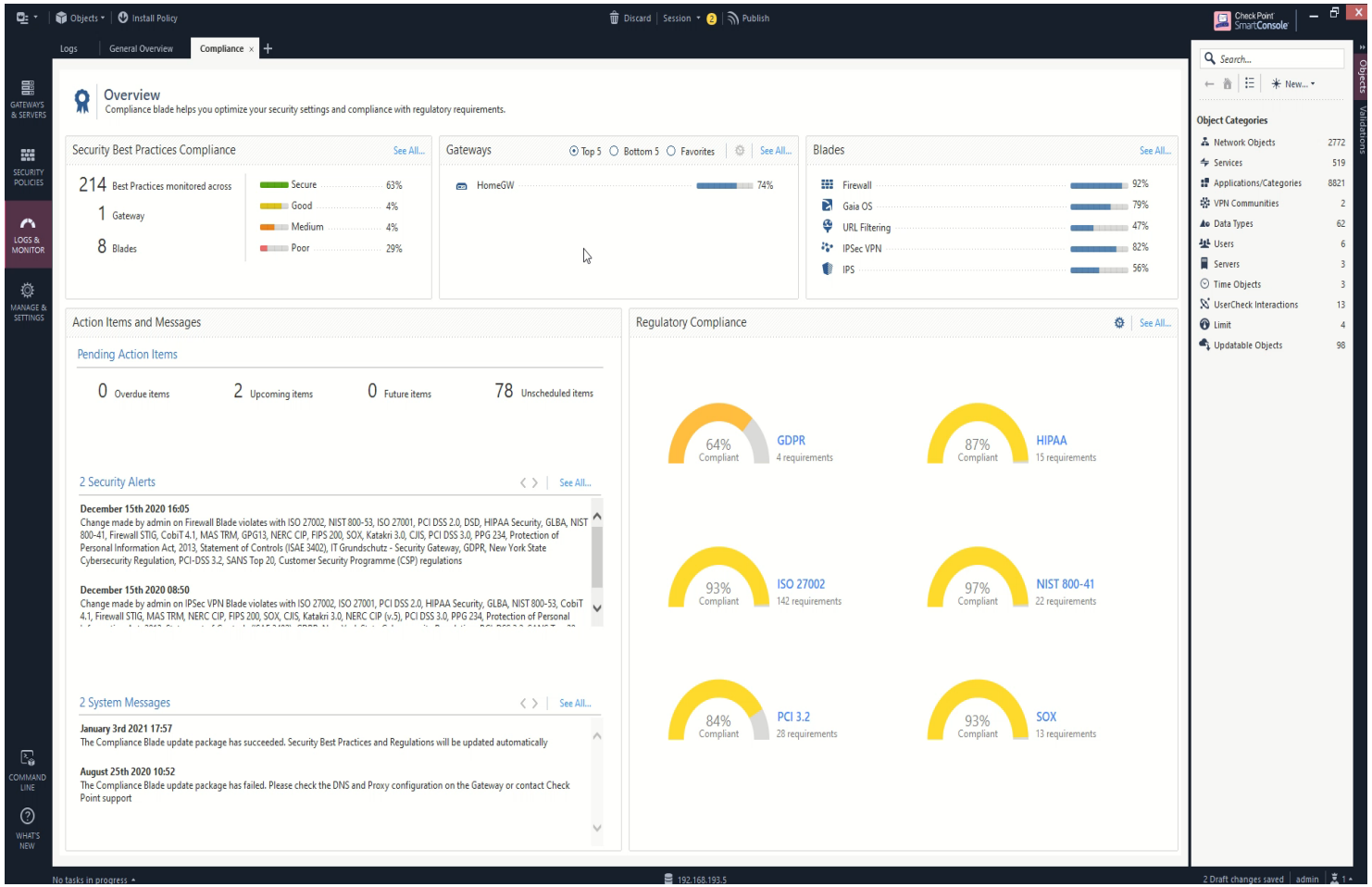
- Translates thousands of complex regulatory requirement into actionable Security Best Practices
- Built In Check Point Regulations
- Build custom compliance regulations

  for your Business Requirements



Compliance Blade View – Technical Dive





Policy Best Practice

Security Best Practices

Blade:Firewa

Active	Blade	ID	Name	Status
☑	Firewall	FW102	Check that Anti-Spoofing has been activated on each Gateway	Poor
☑	Firewall	FW103	Check that Anti-Spoofing is set to Prevent on each Gateway	Poor
☑	Firewall	FW107	Check that there is an additional log server defined for each Gateway for the storage of Firewall logs	Poor
☑	Firewall	FW150	Check the Expiration settings for User Accounts	Poor
☑	Firewall	FW153	Check that each rule has a Comment defined	Poor
☑	Firewall	FW156	Check the Expiration settings for Administrator Accounts	Poor
☑	Firewall	FW108	Check that Firewall runs a script before deleting old log files	Medium
☑	Firewall	FW116	Check that NAT/PAT is enabled in the Gateway Properties	Medium
☑	Firewall	FW130	Check that 'Stealth Rule' is Defined in Access Policy	Medium
☑	Firewall	FW143	Check the Hit Count data configuration	Medium

Relevant Objects: 1 out of 2 items are secure

Active	Rulebase	Rule Index
☑	Corporate_Policy/Network	
☑	Branch_Office_Policy/Branch_Office_Policy Netwo	3

Security Alert Details

Change Details

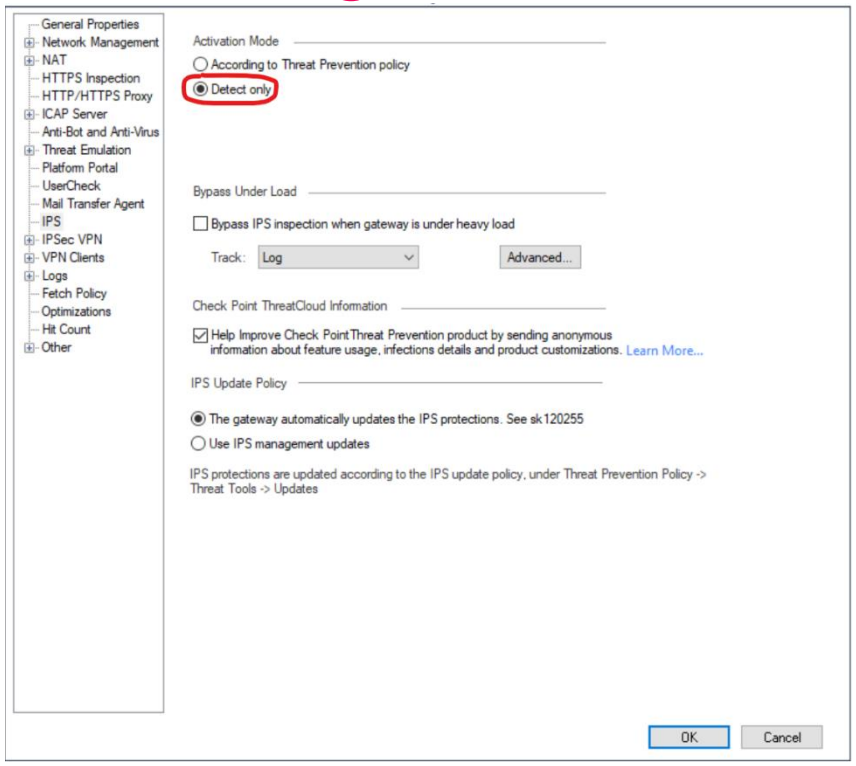
Date: 13/3/2024 18:36
Host: 172.23.51.1
User: admin

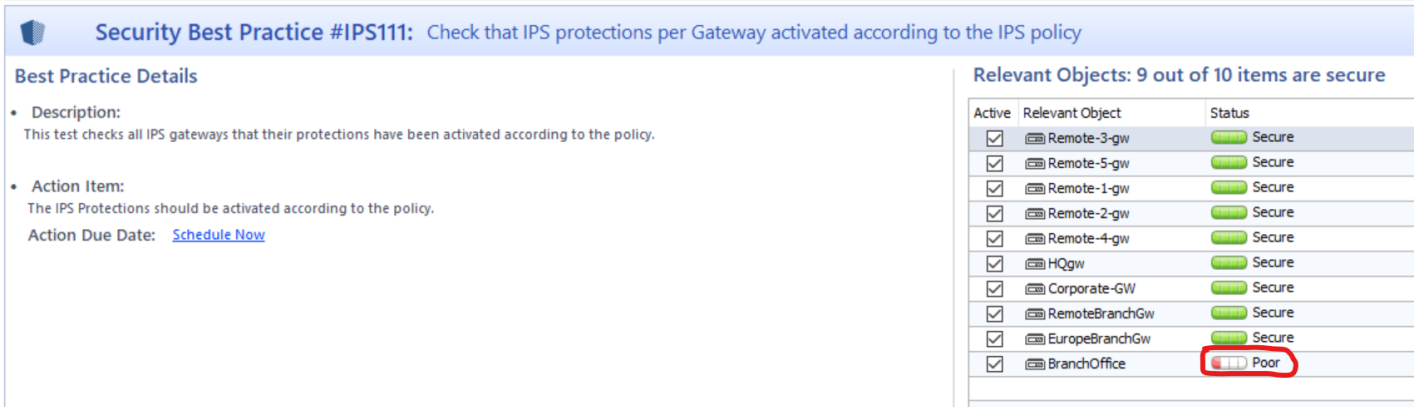
Security Best Practice Details

ID: FW130
Title: Check that 'Stealth Rule' is Defined in Access Policy
Previous status: Secure
New status: Poor
Action Item: The 'Stealth Rule' in the Access Policy needs to be defined as follows: Source= Any; Destination= Security Gateway ; Service= Any; Action= Drop; Track= Not None ; Install on= Policy Target ; Time= Any. Note that the Stealth rule should be set in the top part of the policy. The Compliance Blade scans the top 30% of each Access Policy when searching for the Stealth rule.

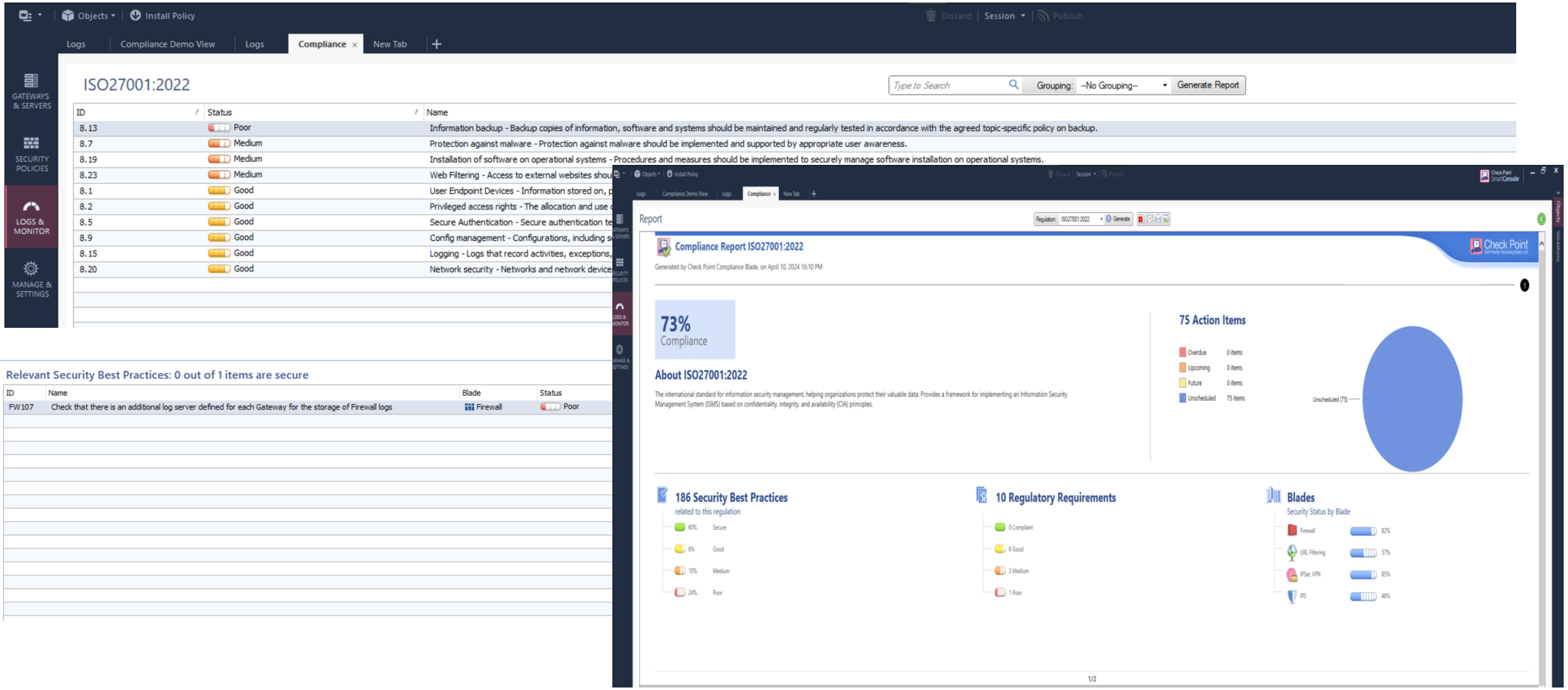
No.	Name	Source	Destination	VPN	Servi				
Security Gateways Access (1-2)									
1	Administrator Access to Gateways	Admins	Corporate-GW	Any					
2	Stealth Rule	Any	Corporate-GW	Any	Any	Any	Accept	Log	Policy Targets

Configuration Best Practice





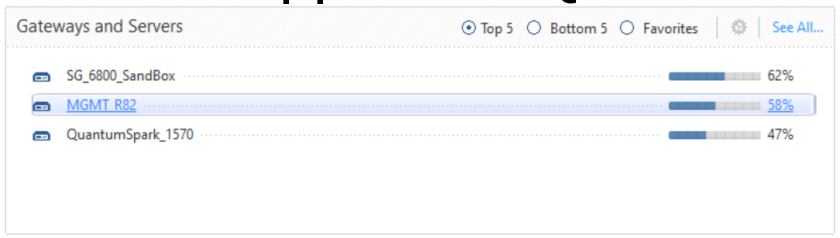
Regulatory and Frameworks

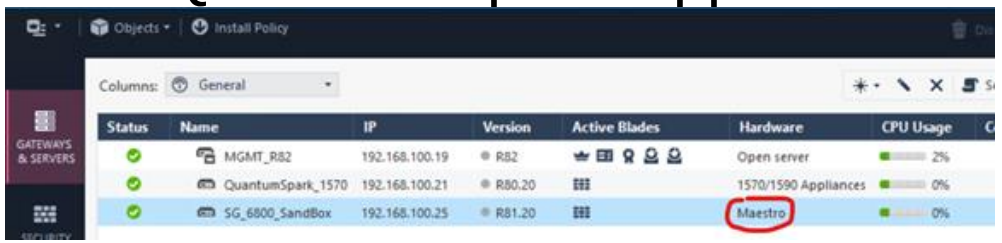


Demo

Roadmap Compliance Blade R82 Management

Added support for Quantum Maestro and Quantum Spark Appliances:





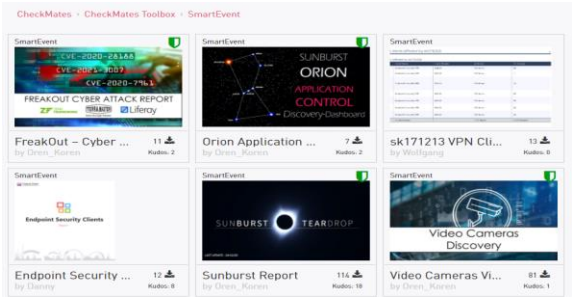
- Gaia OS Best Practice support for Maestro Security Groups by checking each Security Group Member individually and presenting a consolidated Best Practices status.
- Applying relevant Gaia OS Best Practices on Quantum Spark Appliances.
- Added Gaia OS Best Practice support for Log Servers.

Additional Resources

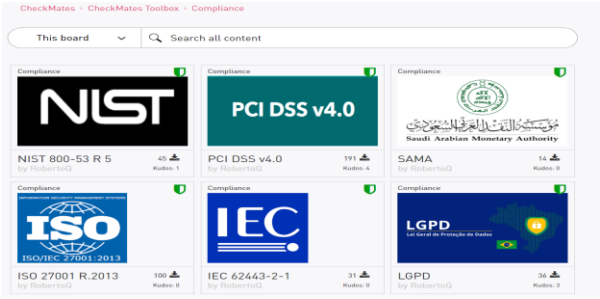
Check Point CHECKMATES

CHECKMATES TOOLBOX

SmartEvent



Compliance Blade



Summary

Q&A

- Compliance Blade is EASY to use and customizable
- Can help detect and fix misconfigurations
- Generate Compliance reports (ISO, GDPR, SOX, PCI DSS and more)

CHECK POINT™

Thank You!

YOU DESERVE THE BEST SECURITY