ManageEngine

Firewall Analyzer

Firewall Analyzer V12

Firewall policy, configuration and log analysis software.

– What is it?

Firewall Analyzer is a policy analysis, configuration monitoring and log reporting software for security administrators to track policy changes, optimize firewall performance and maintain compliance standards.

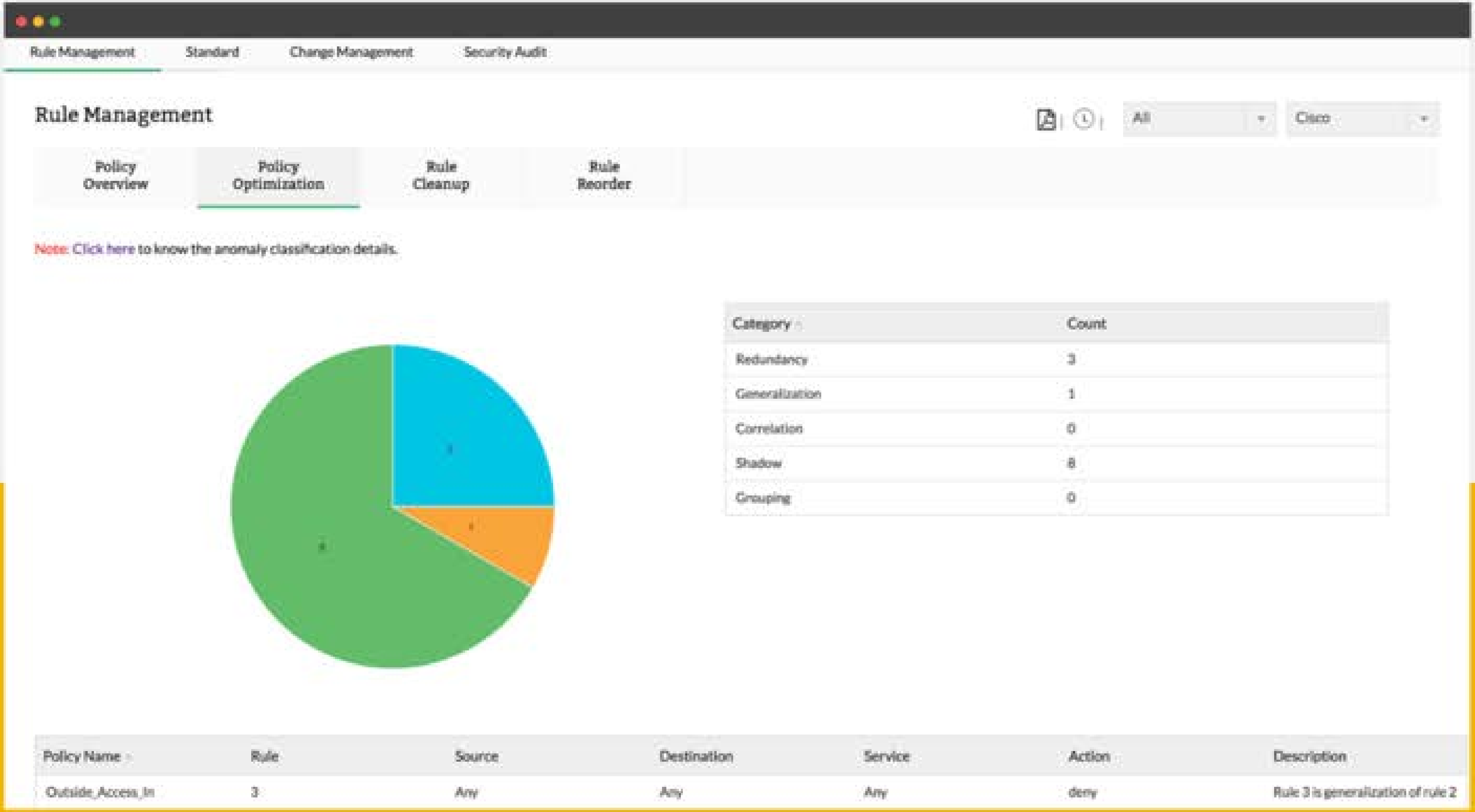
Proactively detect and prevent network security threats, make the most out of Firewall Analyzer with the following features!

- Rule management
- Compliance reports
- Log management
- Change management
- Security audit
- Alarm management

Here's why you need it!

- Streamline firewall policies, optimize rules and improve firewall performance.
- Maintain a record of all the configuration changes by automating change tracking.
- Adhere to compliance standards and identify security loopholes from out-of-the-box compliance reports
- Identify and prevent network security threats by monitoring security logs and employee internet usage.
- Effortlessly mine for security incidents from raw logs and perform forensic analysis to pinpoint threats.
- Get notified on anomalous security and bandwidth incidents directly to your mail or phone.

Rule Management



Rule Management

Note: Click here to know the anomaly classification details.

Category	Count
Redundancy	3
Generalization	1
Correlation	0
Shadow	8
Grouping	0

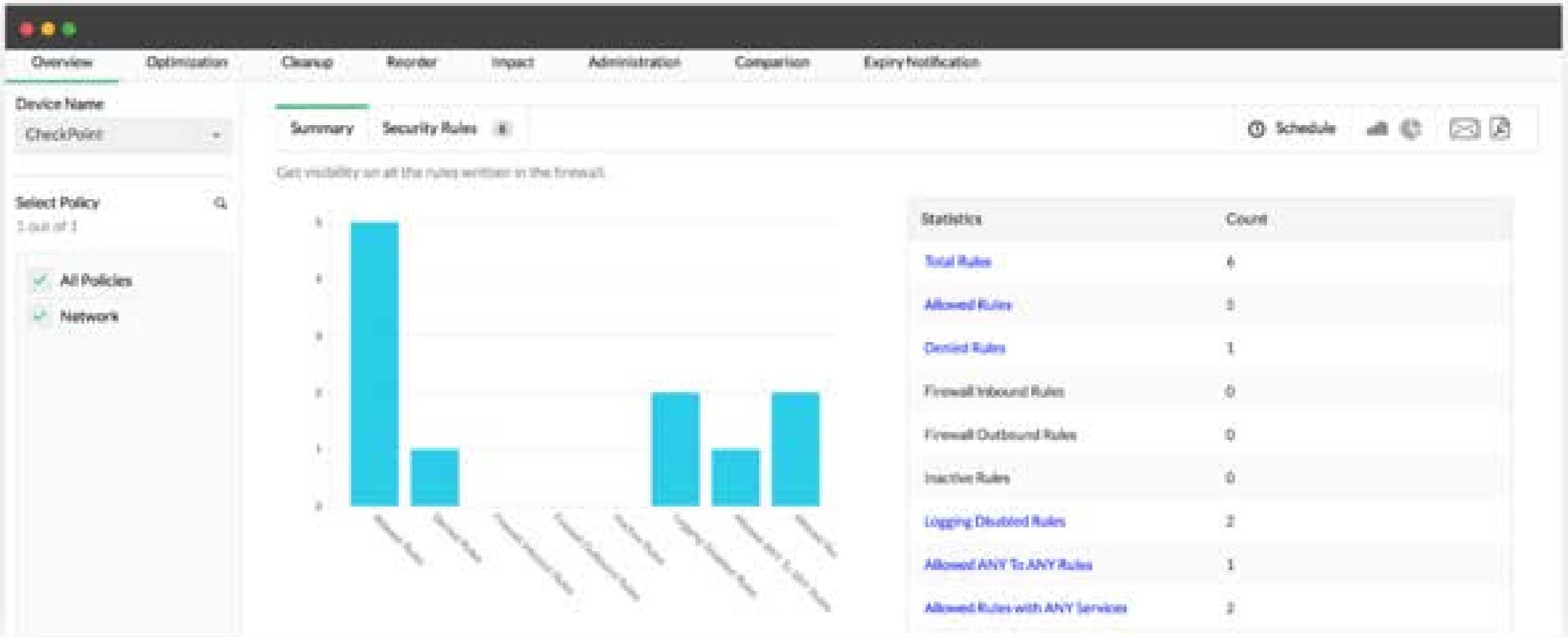
Policy Name	Rule	Source	Destination	Service	Action	Description
Outside_Access_In	3	Any	Any	Any	deny	Rule 3 is generalization of rule 2

The Importance of rule management

The heart of any firewall's performance is its rules and policies. If rules are not managed properly, it can leave your network vulnerable to attacks.

- Gain complete visibility to all the rules written in your firewall.
- Improve firewall performance by identifying and removing rule anomalies.
- Optimize rule performance by placing the rules in the correct order.
- Determine if aproposed new rule is going to impact the existing rule set negatively.
- Identify unused rules and clear them on a regular basis.

Policy Overview



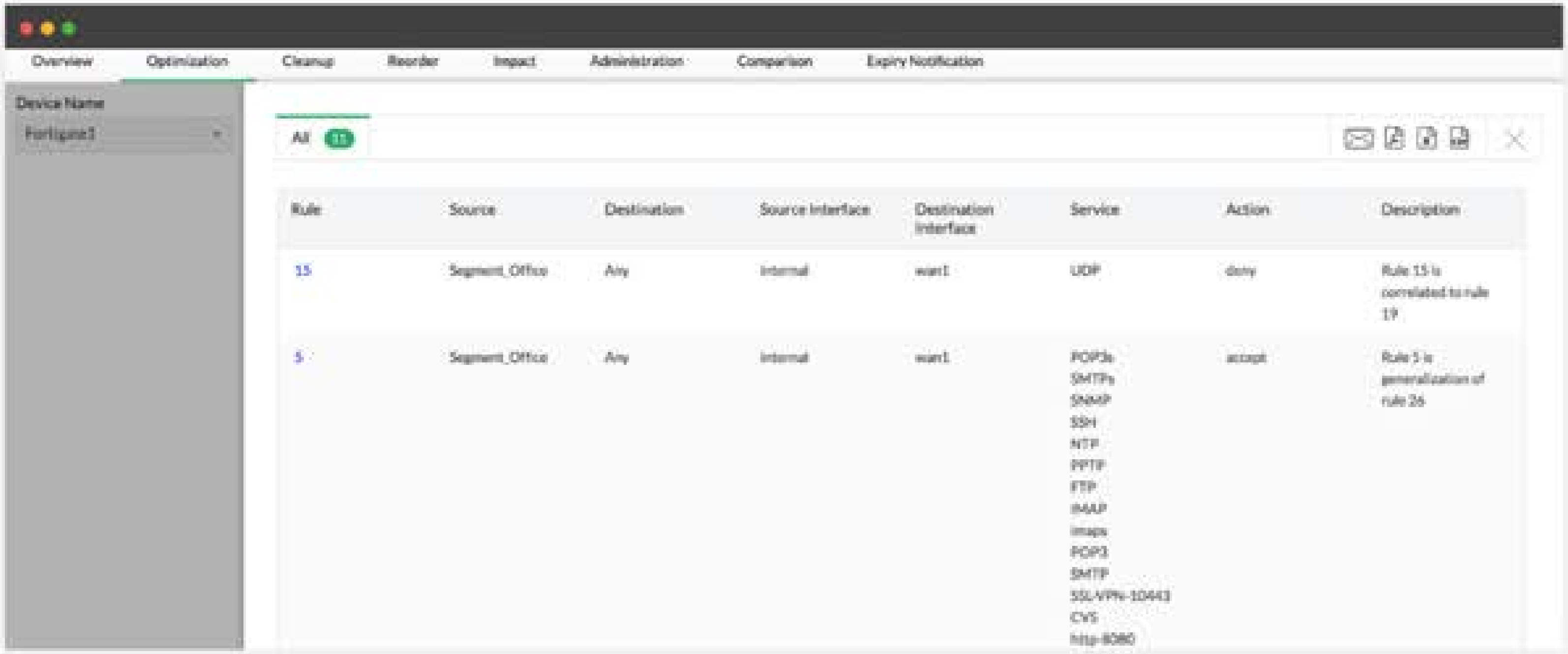
Device Name: CheckPoint

Select Policy
1 out of 1

✓ All Policies
✓ Network

Get visibility on all the rules written in the firewall.

Statistics	Count
Total Rules	6
Allowed Rules	5
Denied Rules	1
Firewall Inbound Rules	0
Firewall Outbound Rules	0
Inactive Rules	0
Logging Disabled Rules	2
Allowed ANY To ANY Rules	1
Allowed Rules with ANY Services	2

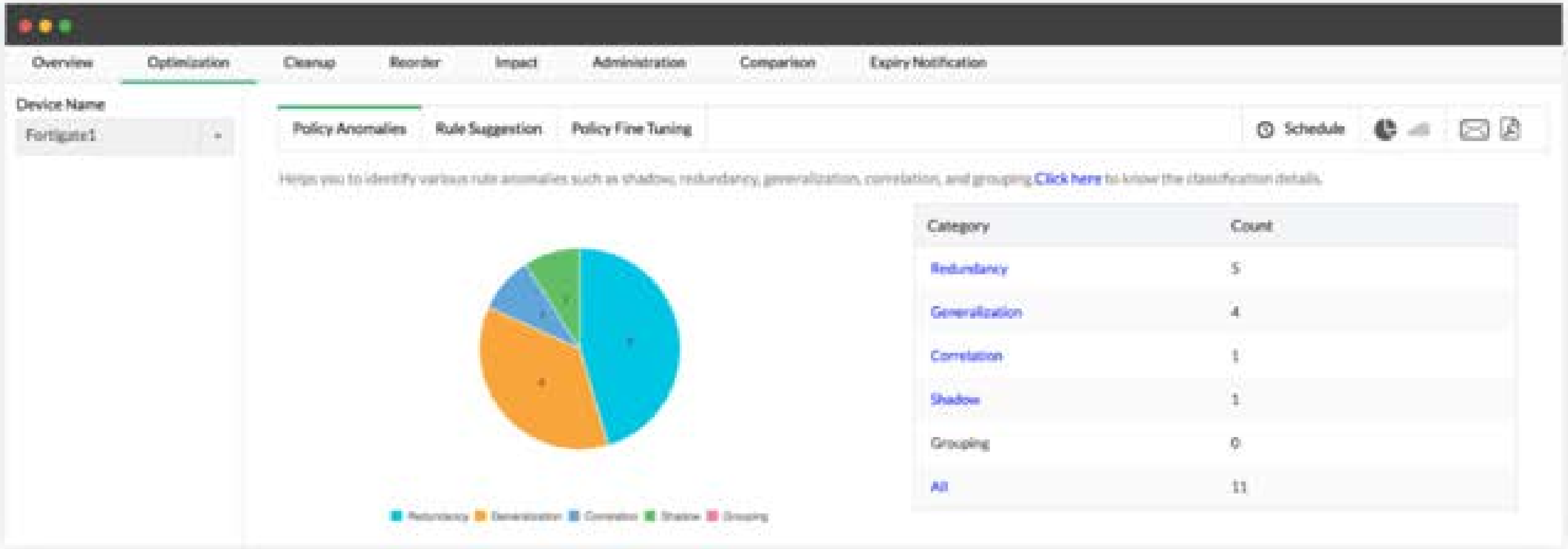


Device Name: Fortigate1

Rule	Source	Destination	Source Interface	Destination Interface	Service	Action	Description
15	Segment_Office	Any	internal	wan1	UDP	deny	Rule 15 is correlated to rule 19
5	Segment_Office	Any	internal	wan1	POP3s SMTPs SNMP SSH NTP PPTP FTP IMAP imaps POP3 SMTP SSL-VPN-10443 CVS http-8080	accept	Rule 5 is generalization of rule 26

- Gain visibility to all the rules written in a specific firewall.
- Get complete details of the listed rules, including rule number, source, destination, interface and service type.
- Easily filter rules according to multiple filter criteria.

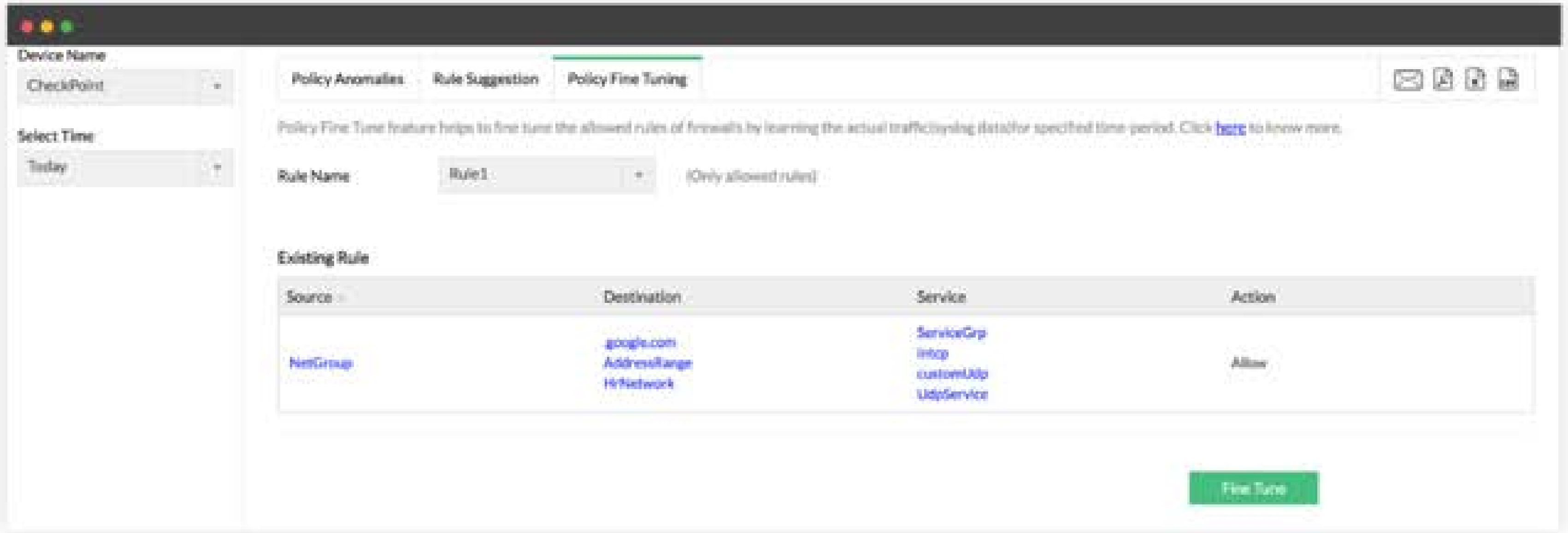
Policy Optimization



Device Name: Fortigate1

Helps you to identify various rule anomalies such as shadow, redundancy, generalization, correlation, and grouping Click here to know the classification details.

Category	Count
Redundancy	5
Generalization	4
Correlation	1
Shadow	1
Grouping	0
All	11



Device Name: CheckPoint

Select Time: Today

Policy Fine Tune feature helps to fine tune the allowed rules of firewalls by learning the actual traffic/syslog data for specified time period. Click here to know more.

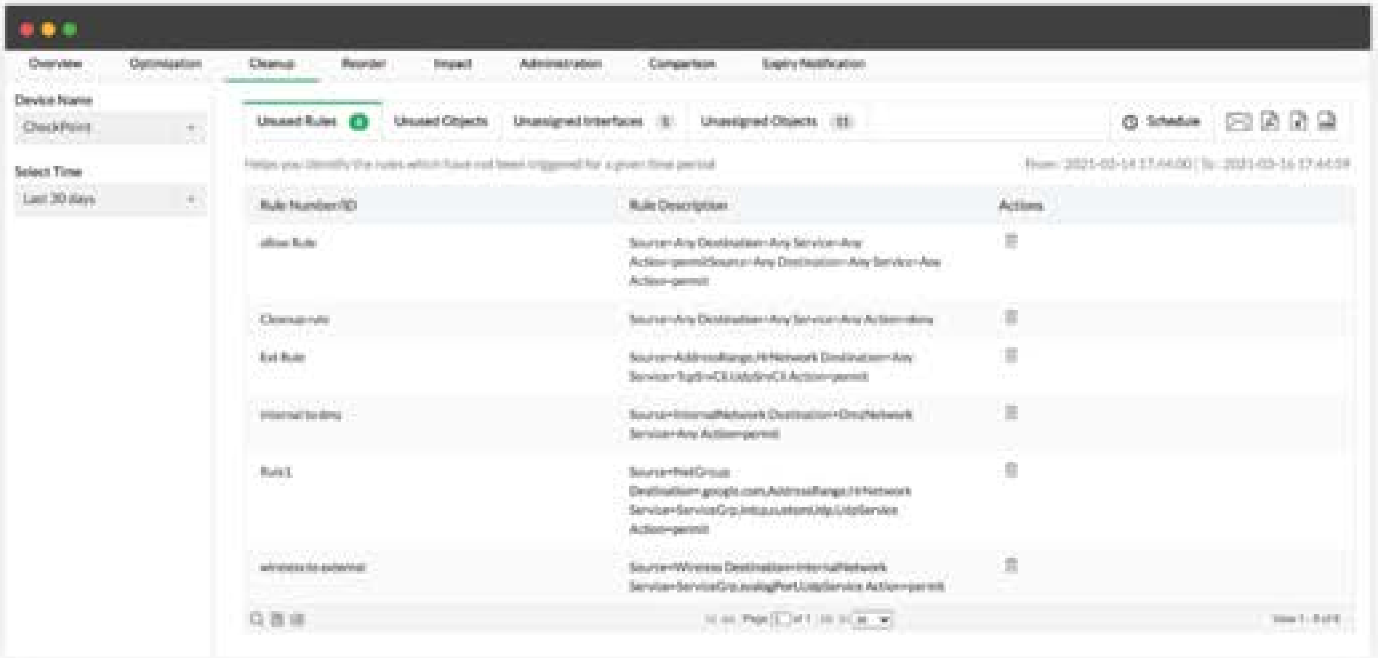
Rule Name: Rule1 (Only allowed rules)

Existing Rule

Source	Destination	Service	Action
NetGroup	.google.com AddressRange HrNetwork	ServiceGrp intcp customUdp UdpService	Allow

- Identify anomalies which negatively impact firewall performance.
- Get complete details of the different types of anomalies. Determine rules which have shadow, redundancy, generalization, correlation, and grouping anomalies.
- Easily filter anomalies according to multiple filter criteria.
- Reduce overly permissive rules by receiving rule suggestions
- Fine tune firewall rules for maximum performance

Rule Cleanup



Device Name: CheckPoint

Select Time: Last 30 days

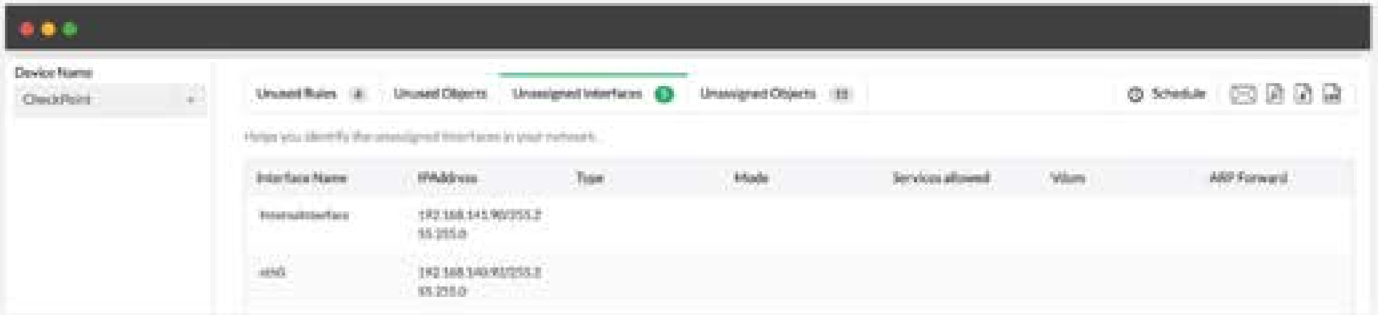
Helps you identify the rules which have not been triggered for a given time period

From : 2021-03-14 17:44:00 | To : 2021-03-16 17:44:59

Rule Number/ID	Rule Description	Actions
allow Rule	Source=Any Destination=Any Service=Any Action=permitSource=Any Destination=Any Service=Any Action=permit	🗑
Cleanup rule	Source=Any Destination=Any Service=Any Action=deny	🗑
Ext Rule	Source=AddressRange,HrNetwork Destination=Any Service=TcpSrvCll,UdpSrvCll Action=permit	🗑
internal to dmz	Source=InternalNetwork Destination=DmzNetwork Service=Any Action=permit	🗑
Rule1	Source=NetGroup Destination=google.com,AddressRange,HrNetwork Service=ServiceGrp,http,customUdp,UdpService Action=permit	🗑
wireless to external	Source=Wireless Destination=InternalNetwork Service=ServiceGrp,syslogPort,UdpService Action=permit	🗑

Page 1 of 1

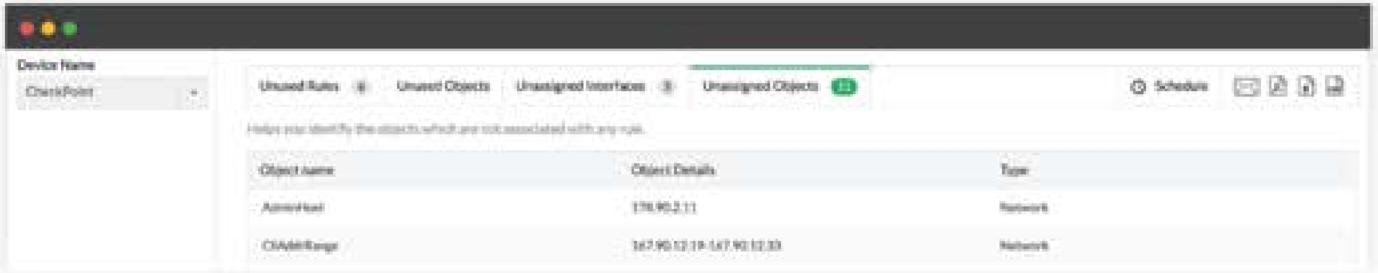
View 1 - 6 of 6



Device Name: CheckPoint

Helps you identify the unassigned interfaces in your network.

Interface Name	IPAddress	Type	Mode	Services allowed	Vlans	ARP Forward
InternalInterface	192.168.141.90/255.255.255.0					
eth0	192.168.140.92/255.255.255.0					



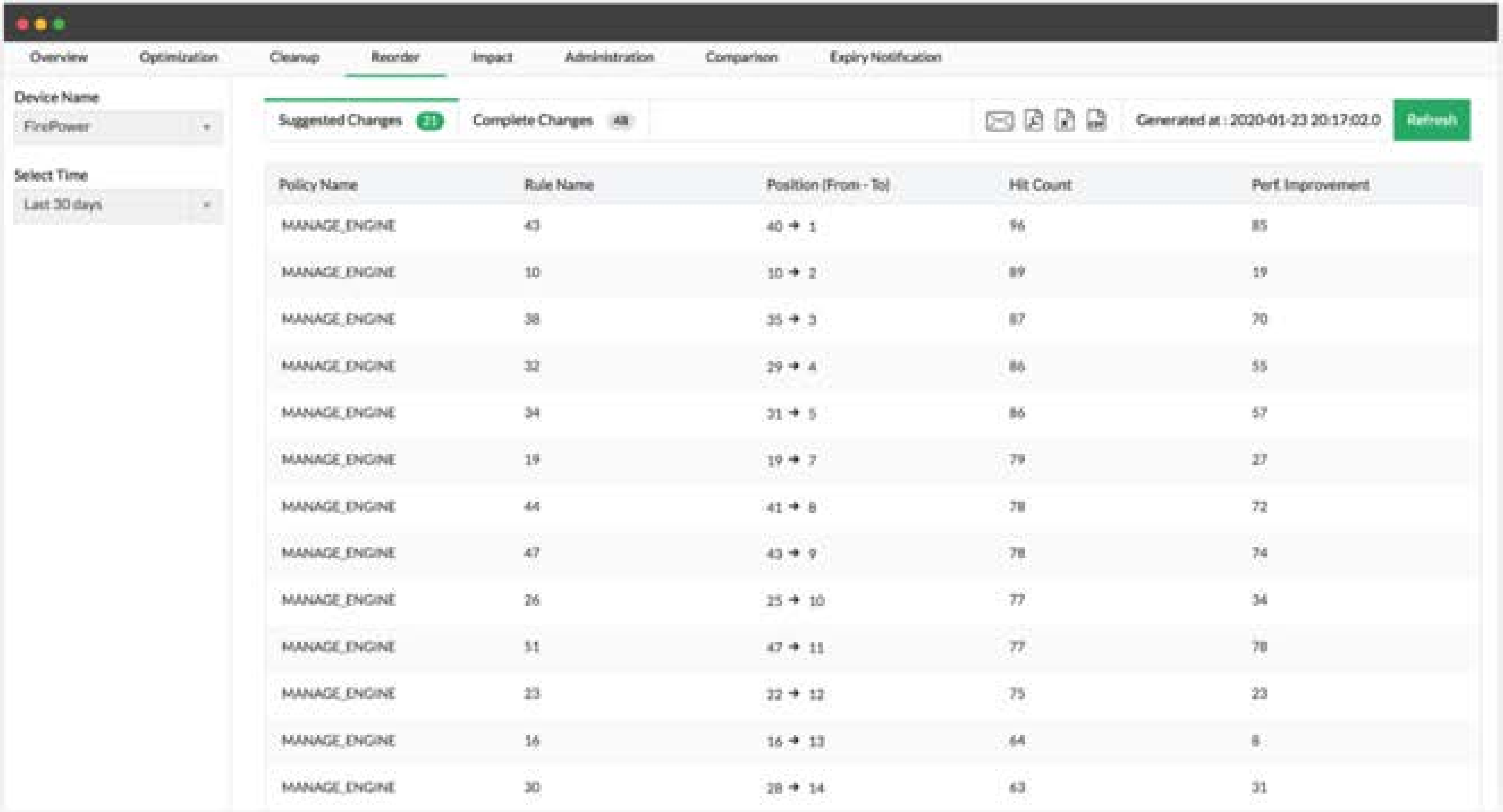
Device Name: CheckPoint

Helps you identify the objects which are not associated with any rule.

Object name	Object Details	Type
AdminHost	178.90.2.11	Network
CliAddrRange	167.90.12.19-167.90.12.33	Network

- Reduce security threats by identifying unused firewall rules, objects, and interfaces.
- Obtain a high-level overview of which rules, objects, and interfaces can be removed or deactivated.

Rule Reorder Suggestion

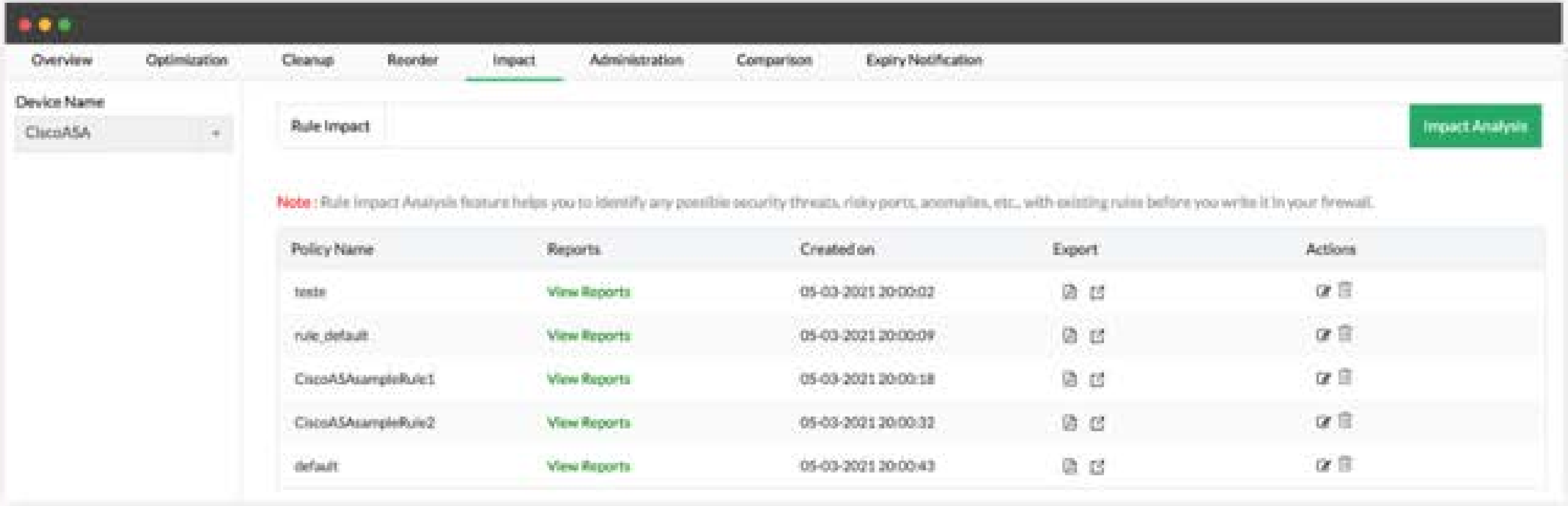


Generated at : 2020-01-23 20:17:02.0

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
MANAGE_ENGINE	43	40 → 1	96	85
MANAGE_ENGINE	10	10 → 2	89	19
MANAGE_ENGINE	38	35 → 3	87	70
MANAGE_ENGINE	32	29 → 4	86	55
MANAGE_ENGINE	34	31 → 5	86	57
MANAGE_ENGINE	19	19 → 7	79	27
MANAGE_ENGINE	44	41 → 8	78	72
MANAGE_ENGINE	47	43 → 9	78	74
MANAGE_ENGINE	26	25 → 10	77	34
MANAGE_ENGINE	51	47 → 11	77	78
MANAGE_ENGINE	23	22 → 12	75	23
MANAGE_ENGINE	16	16 → 13	64	8
MANAGE_ENGINE	30	28 → 14	63	31

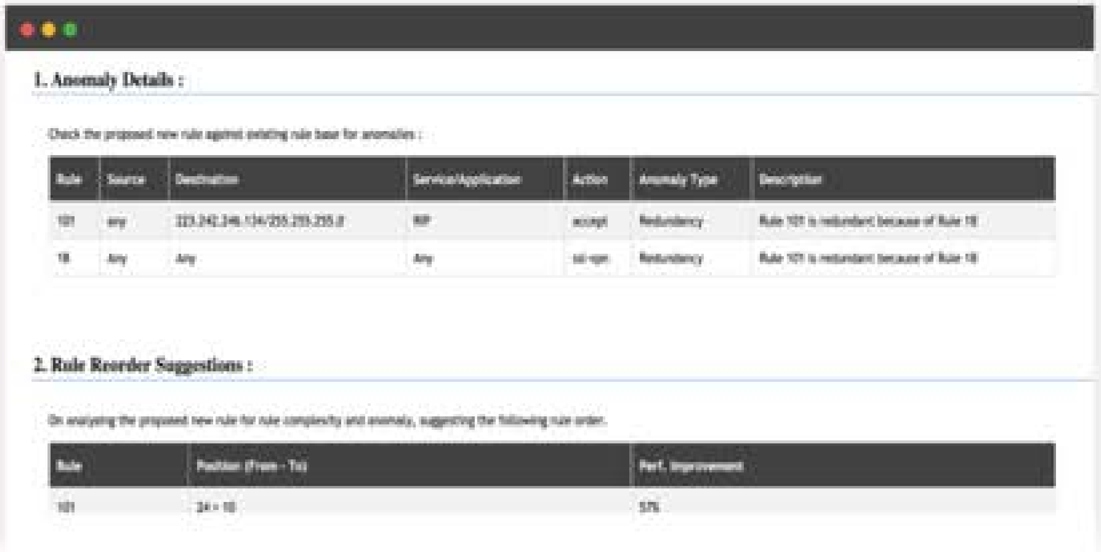
- Gain insights on how to organize firewall rules to maximize speed.
- Estimate the performance improvement for a suggested order change by correlating the number of rule hits with rule complexity and anomalies.
- Export reorder suggestions and analyze offline.

Rule Impact Analysis



Note : Rule Impact Analysis feature helps you to identify any possible security threats, risky ports, anomalies, etc., with existing rules before you write it in your firewall.

Policy Name	Reports	Created on	Export	Actions
teste	View Reports	05-03-2021 20:00:02		
rule_default	View Reports	05-03-2021 20:00:09		
CiscoASAsampleRule1	View Reports	05-03-2021 20:00:18		
CiscoASAsampleRule2	View Reports	05-03-2021 20:00:32		
default	View Reports	05-03-2021 20:00:43		



1. Anomaly Details :

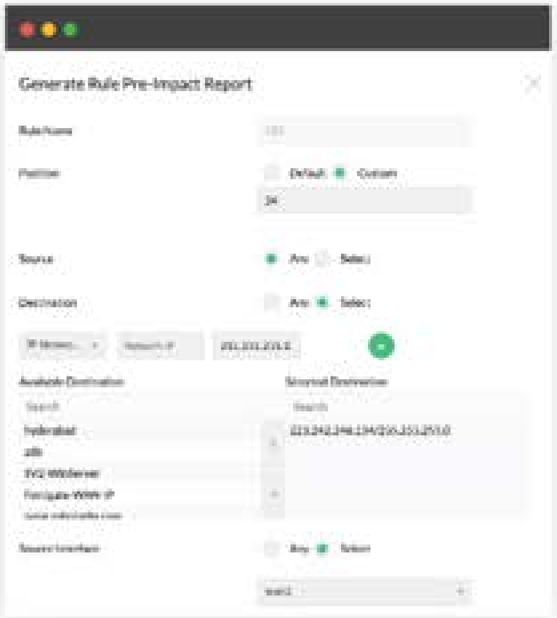
Check the proposed new rule against existing rule base for anomalies :

Rule	Source	Destination	Service/Application	Action	Anomaly Type	Description
101	any	223.242.246.134/255.255.255.0	RIP	accept	Redundancy	Rule 101 is redundant because of Rule 18
18	Any	Any	Any	ssl-vpn	Redundancy	Rule 101 is redundant because of Rule 18

2. Rule Reorder Suggestions :

On analyzing the proposed new rule for rule complexity and anomaly, suggesting the following rule order.

Rule	Position (From - To)	Perf. Improvement
101	24 → 18	57%



Generate Rule Pre-Impact Report

Rule Name: 101

Position: ○ Default ● Custom
24

Source: ● Any ○ Select

Destination: ○ Any ● Select

IP Address... Network IP 255.255.255.0

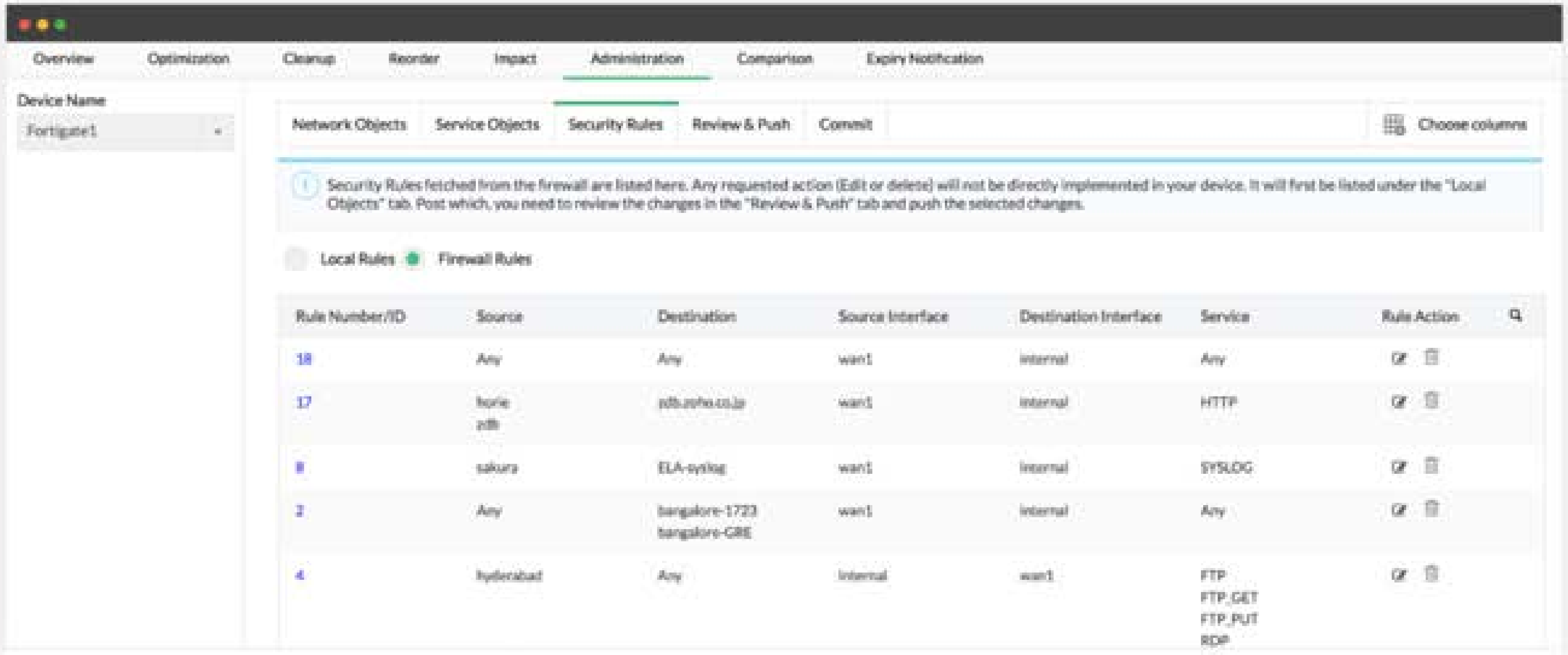
Available Destination
Search
hyderabad
zdb
SVQ WebServer
Fortigate WAN IP
[illegible]

Selected Destination
Search
223.242.246.134/255.255.255.0

Source Interface: ○ Any ● Select
wan1

- Perform in-depth impact analysis for a proposed new rule and determine if the proposed new rule will impact the existing rule set negatively.
- Use impact analysis to identify threats, understand risks, determine anomalies, and optimize the proposed new rule.

Rule Administration

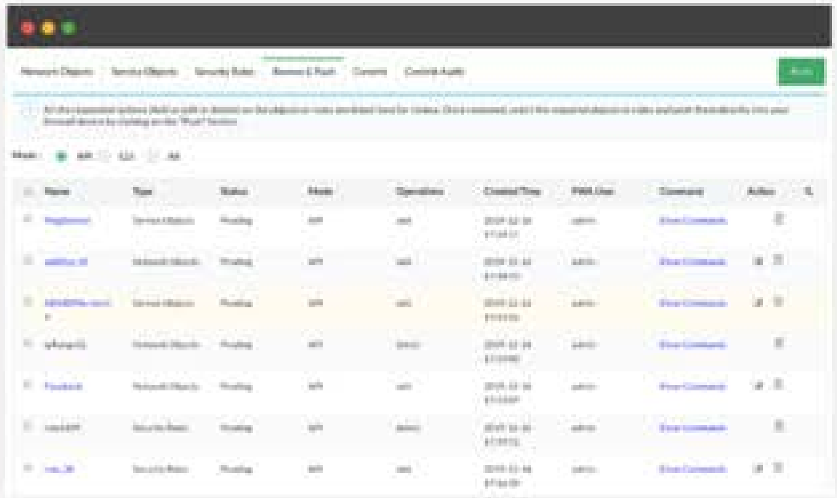


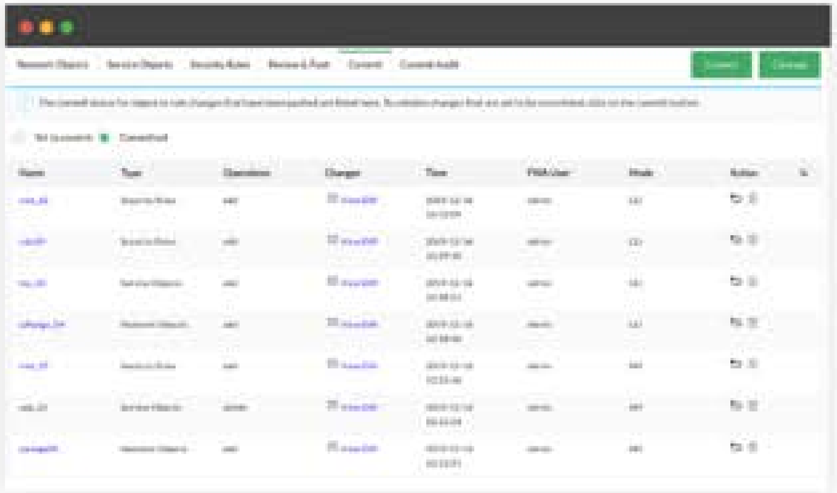
Device Name: Fortigate1

Security Rules fetched from the firewall are listed here. Any requested action (Edit or delete) will not be directly implemented in your device. It will first be listed under the "Local Objects" tab. Post which, you need to review the changes in the "Review & Push" tab and push the selected changes.

○ Local Rules ● Firewall Rules

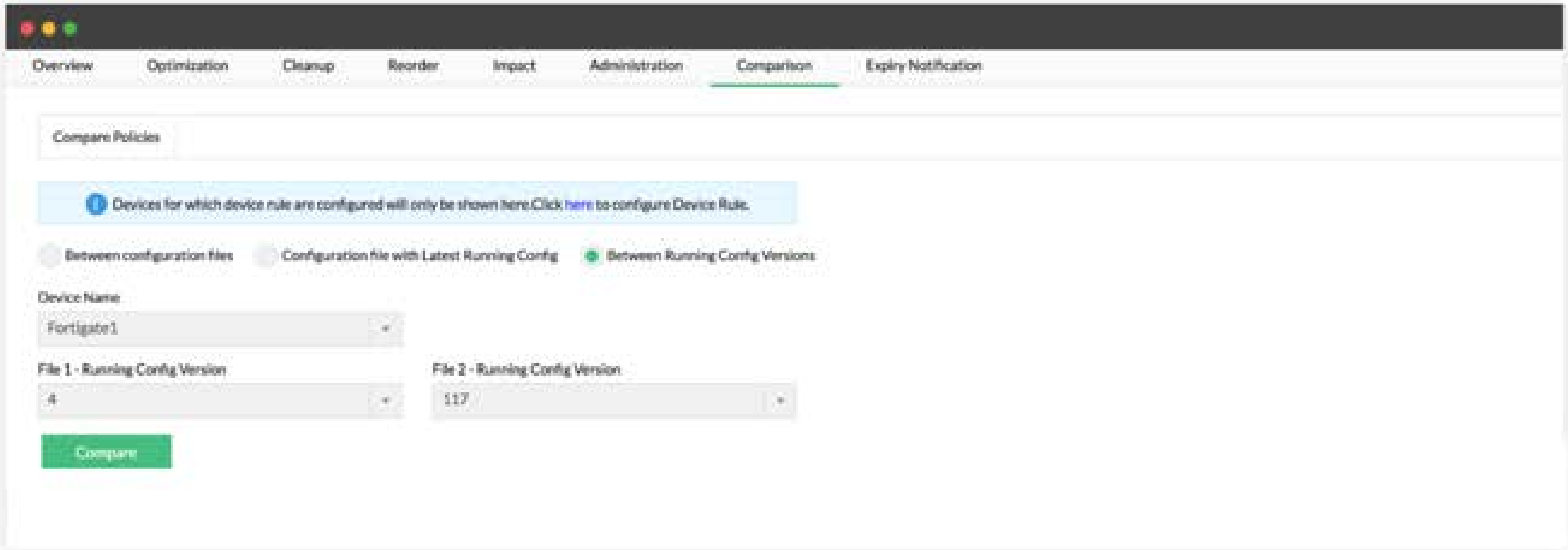
Rule Number/ID	Source	Destination	Source Interface	Destination Interface	Service	Rule Action
18	Any	Any	wan1	internal	Any	
17	horie zdb	zdb.zoho.co.jp	wan1	internal	HTTP	
8	sakura	ELA-syslog	wan1	internal	SYSLOG	
2	Any	bangalore-1723 bangalore-GRE	wan1	internal	Any	
4	hyderabad	Any	internal	wan1	FTP FTP_GET FTP_PUT RDP	





- Add, modify, and delete rules and network objects, analyze the implications of a proposed change and push changes directly to the firewall.
- Simplify firewall policy management by automating the process of firewall rule administration.

Rule Comparison



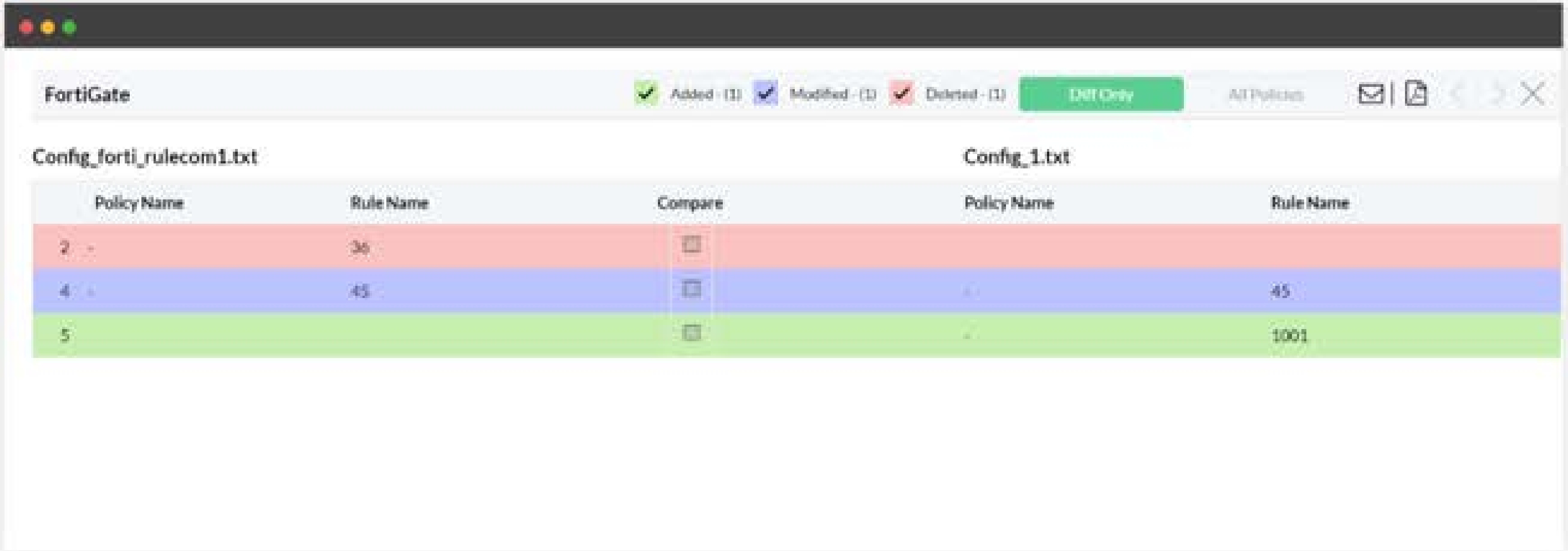
Devices for which device rule are configured will only be shown here.Click here to configure Device Rule.

○ Between configuration files ○ Configuration file with Latest Running Config ● Between Running Config Versions

Device Name: Fortigate1

File 1 - Running Config Version: 4

File 2 - Running Config Version: 117



✓ Added - (1) ✓ Modified - (1) ✓ Deleted - (1)

Config_forti_rulecom1.txt

Config_1.txt

	Policy Name	Rule Name	Compare	Policy Name	Rule Name
2	-	36	□		
4	-	45	□	-	45
5			□	-	1001

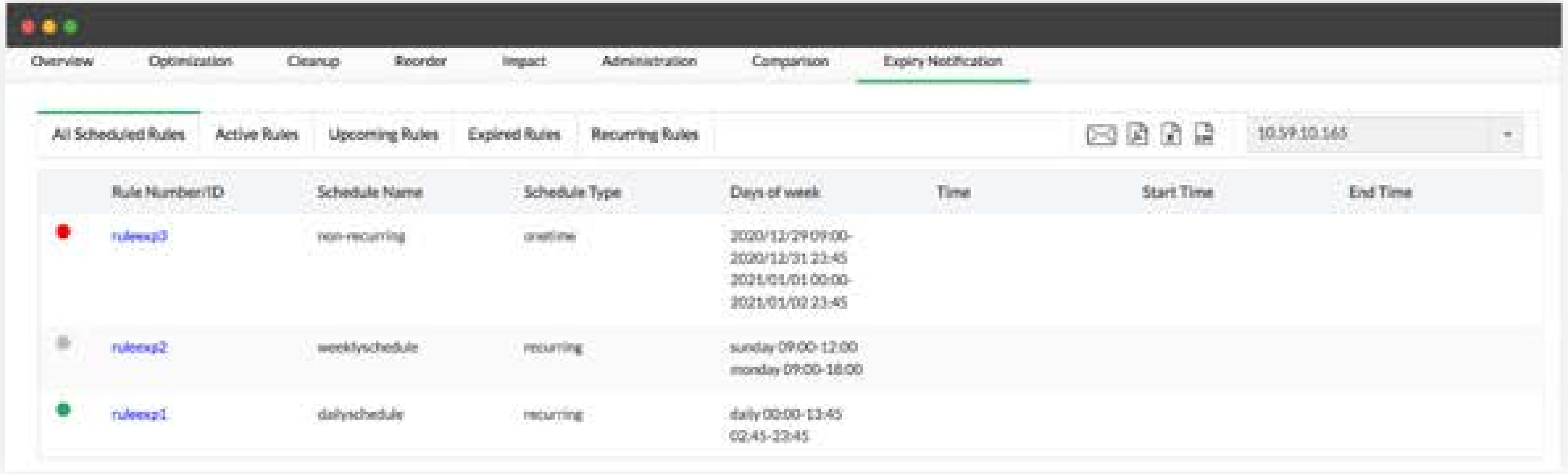
Track firewall rule changes made in the firewall

Keep a close eye on all the changes made to the firewall rule configuration

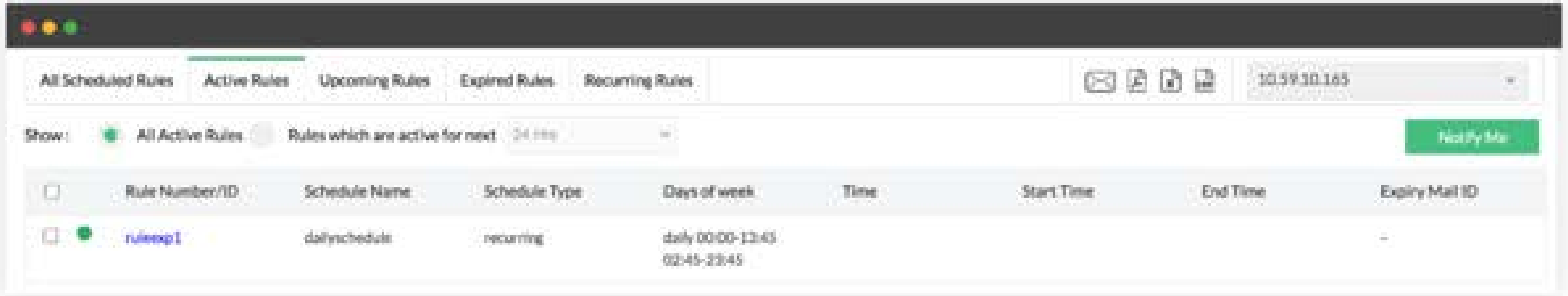
Compare configuration changes between:

- Two configuration files, which can be manually uploaded.
- A specific configuration file (taken manually) and the latest configuration
- Specific configuration versions fetched directly by Firewall Analyzer

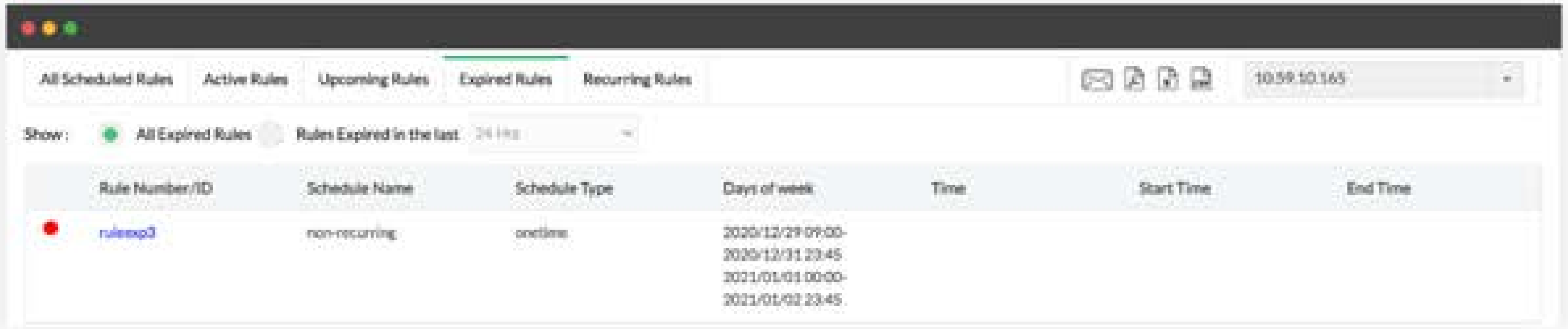
Rule Expiry Notification



	Rule Number/ID	Schedule Name	Schedule Type	Days of week	Time	Start Time	End Time
●	ruleexp3	non-recurring	onetime	2020/12/29 09:00- 2020/12/31 23:45 2021/01/01 00:00- 2021/01/02 23:45			
●	ruleexp2	weeklyschedule	recurring	sunday 09:00-12:00 monday 09:00-18:00			
●	ruleexp1	dailyschedule	recurring	daily 00:00-13:45 02:45-23:45			



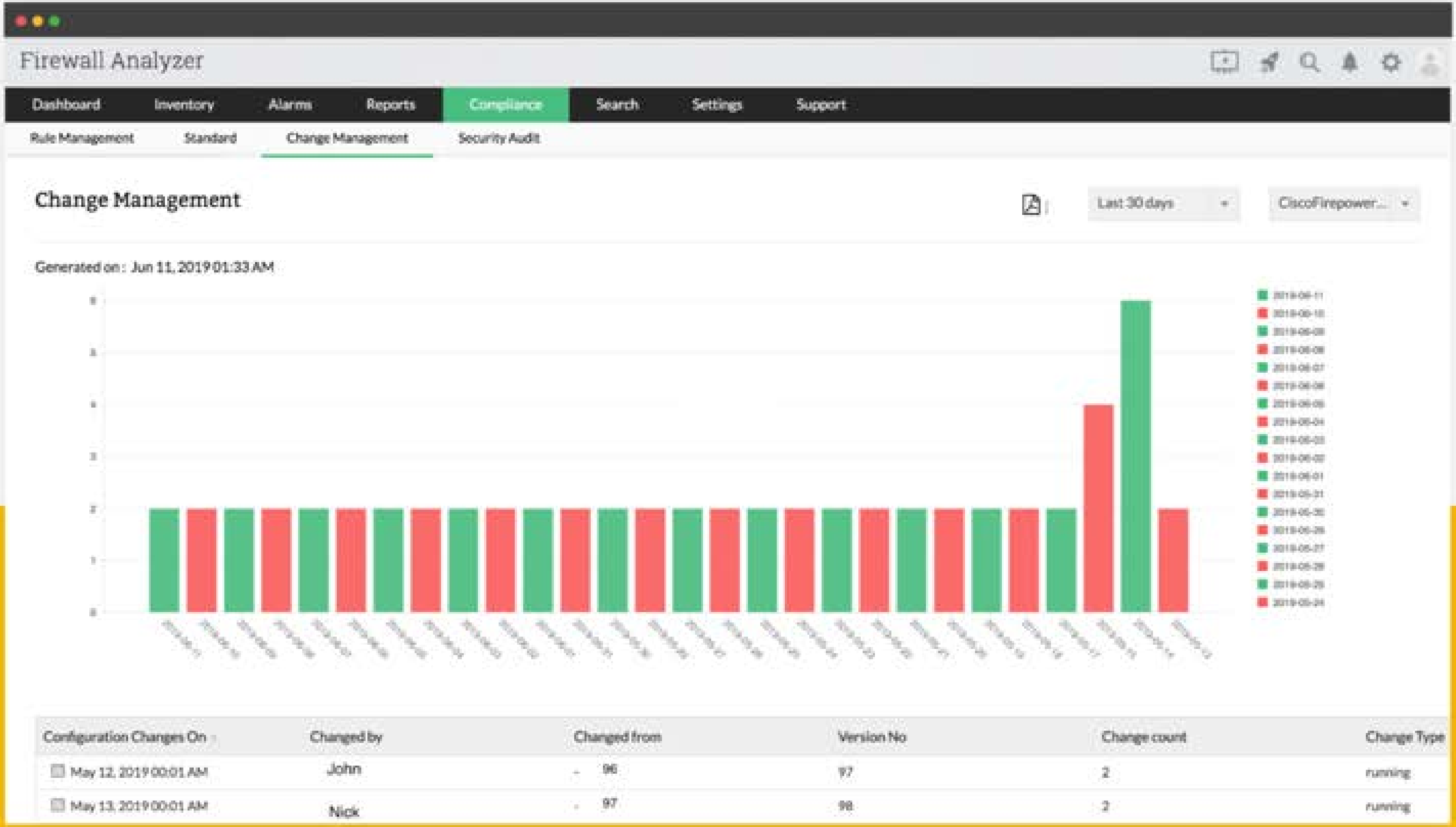
☐		Rule Number/ID	Schedule Name	Schedule Type	Days of week	Time	Start Time	End Time	Expiry Mail ID
☐	●	ruleexp1	dailyschedule	recurring	daily 00:00-13:45 02:45-23:45				-



	Rule Number/ID	Schedule Name	Schedule Type	Days of week	Time	Start Time	End Time
●	ruleexp3	non-recurring	onetime	2020/12/29 09:00- 2020/12/31 23:45 2021/01/01 00:00- 2021/01/02 23:45			

- Track the status of firewall rules and get notified on which rules have expired
- List all the firewall rules for which any kind of schedule has been set
- Enumerate all the active firewall rules for which a schedule has been set
- Catalog all the rules that are scheduled to turn active in the future
- Record all the rules that have expired
- List all the rules that are reactivated and certified on a regular basis

Configuration Change Management



Change Management

Last 30 days ▾

CiscoFirepower... ▾

Generated on : Jun 11, 2019 01:33 AM

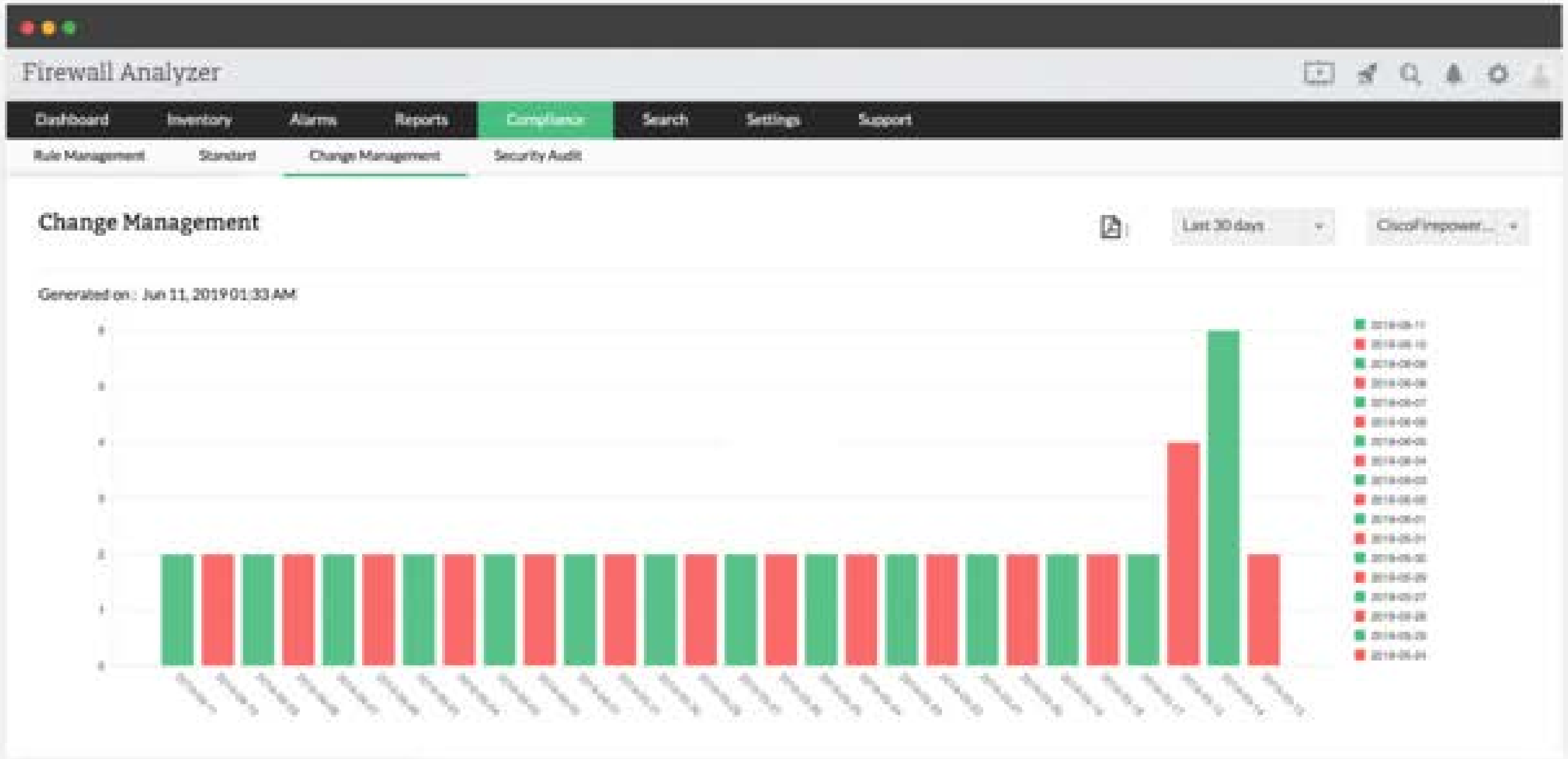
Configuration Changes On	Changed by	Changed from	Version No	Change count	Change Type
□ May 12, 2019 00:01 AM	John	- 96	97	2	running
□ May 13, 2019 00:01 AM	Nick	- 97	98	2	running

Significance of Change Management

Automated change tracking is crucial to gain better visibility into your firewall configuration and security!

- Eliminate manual change tracking.
- Secure your network by monitoring changes made to the firewall configuration.
- Change notifications helps you stay alert.

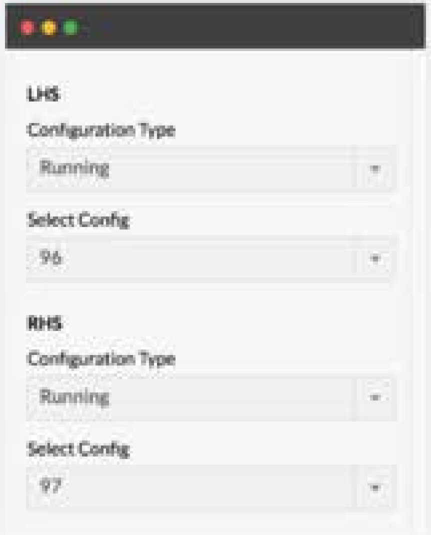
Configuration Change Tracking



Change Management

Generated on : Jun 11, 2019 01:33 AM

- Automate configuration change tracking in all your firewall devices.
- Track “what”, “who” & “when” of configuration changes.
- Receive change notifications directly to you mail.



LHS

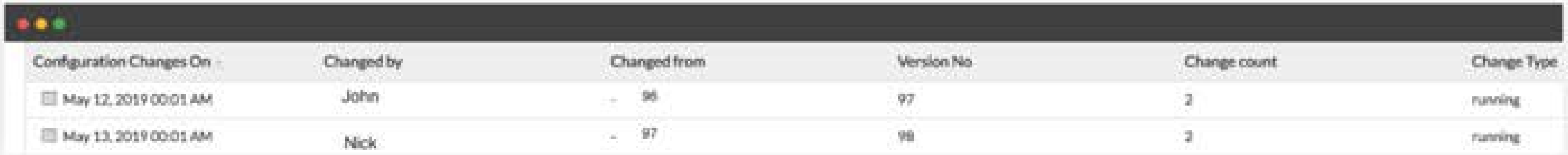
Configuration Type: Running

Select Config: 96

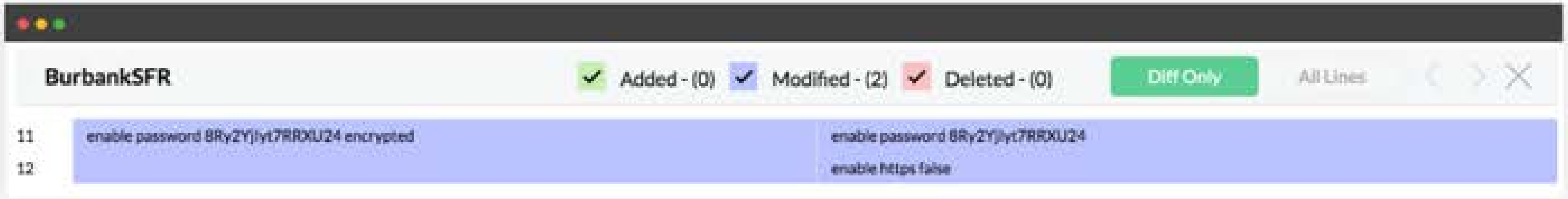
RHS

Configuration Type: Running

Select Config: 97



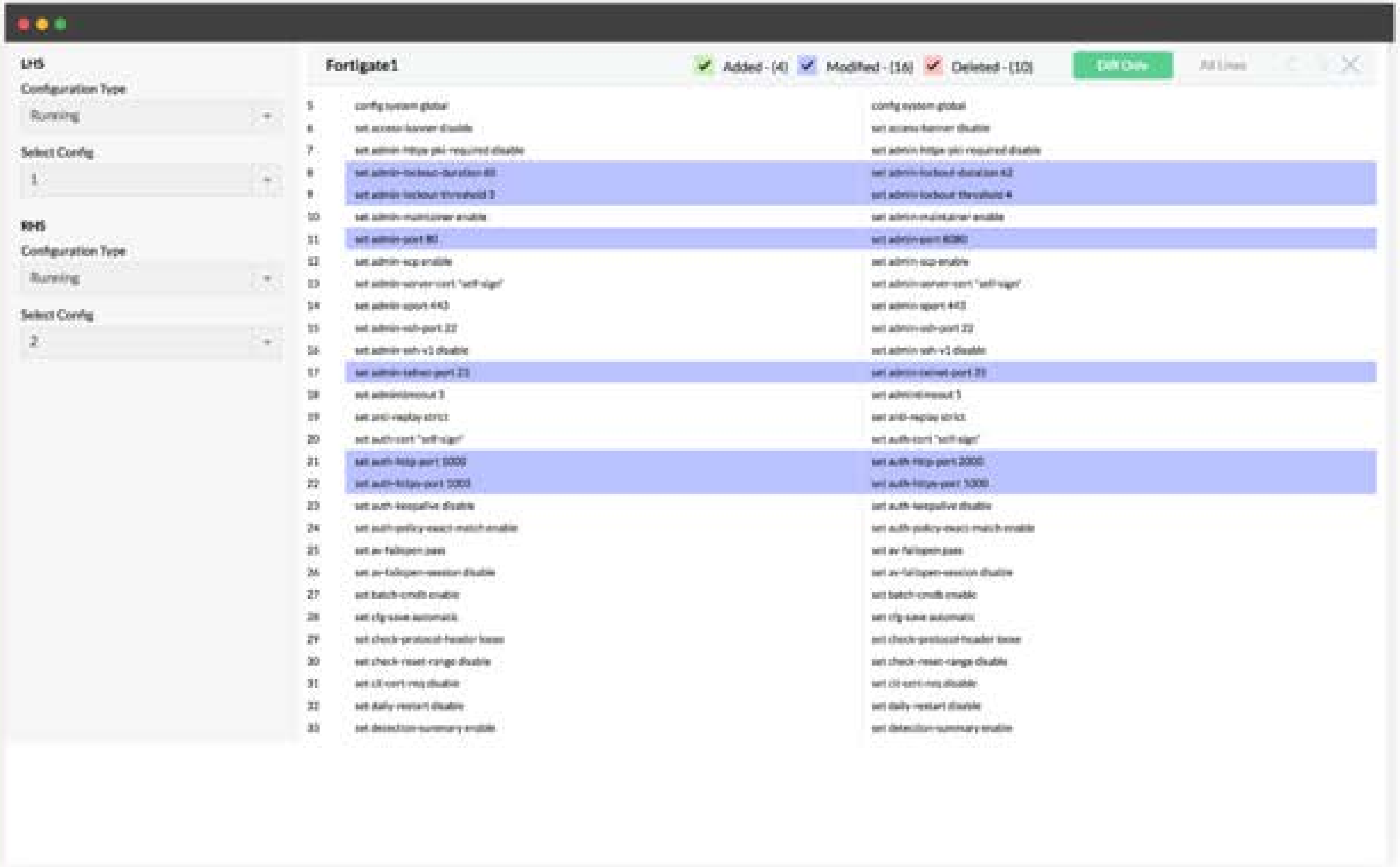
Configuration Changes On	Changed by	Changed from	Version No	Change count	Change Type
□ May 12, 2019 00:01 AM	John	- 96	97	2	running
□ May 13, 2019 00:01 AM	Nick	- 97	98	2	running



BurbankSFR

```
enable password 8Ry2YjIyt7RRXU24 encrypted      enable password 8Ry2YjIyt7RRXU24
                                                enable https false
```

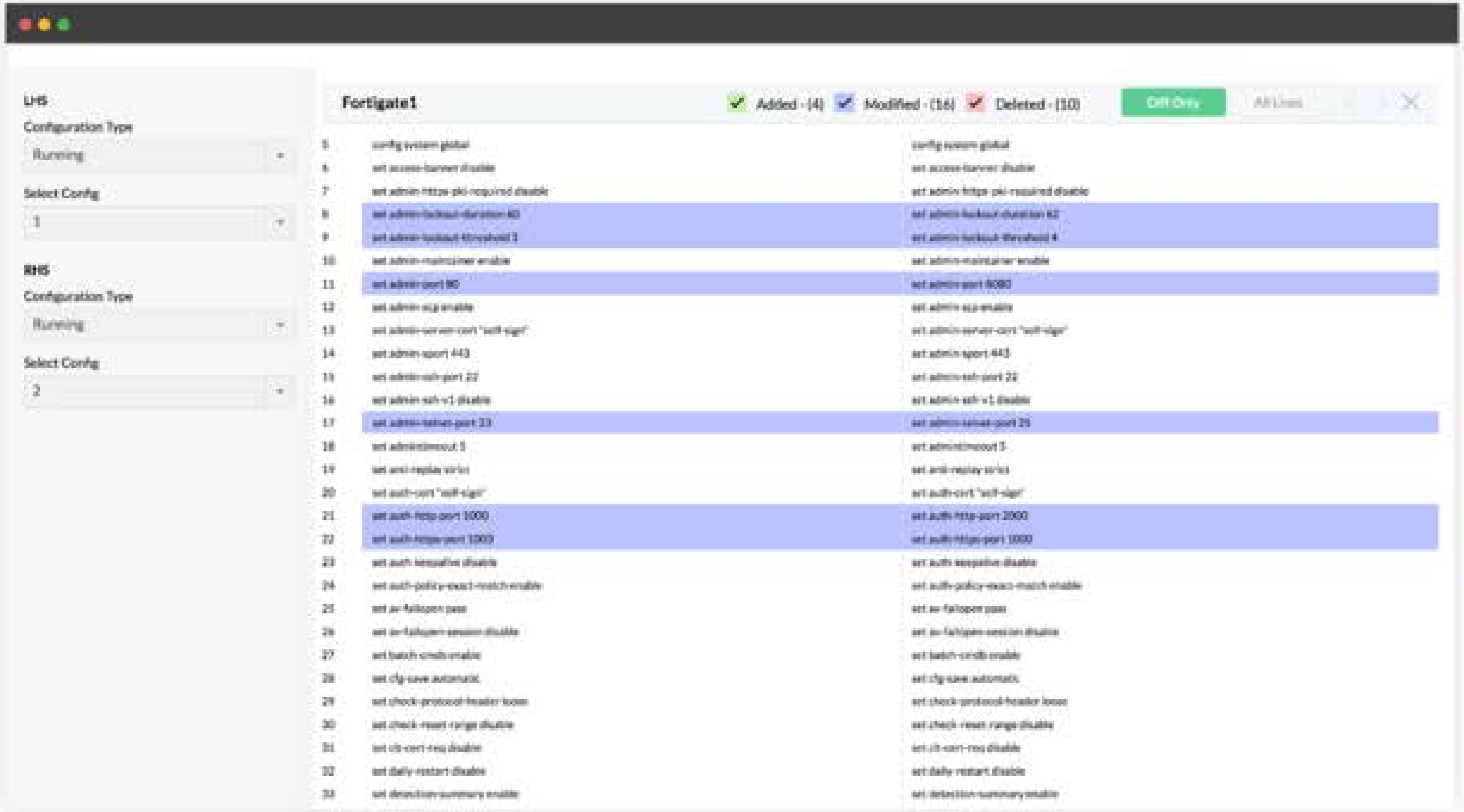
Configuration Comparison Using Diff-View



```
config system global                        config system global
set access-banner disable                   set access-banner disable
set admin-https-pki-required disable        set admin-https-pki-required disable
set admin-lockout-duration 60               set admin-lockout-duration 62
set admin-lockout-threshold 3               set admin-lockout-threshold 4
set admin-maintainer enable                 set admin-maintainer enable
set admin-port 80                           set admin-port 8080
set admin-scp enable                        set admin-scp enable
set admin-server-cert "self-sign"           set admin-server-cert "self-sign"
set admin-sport 443                         set admin-sport 443
set admin-ssh-port 22                       set admin-ssh-port 22
set admin-ssh-v1 disable                    set admin-ssh-v1 disable
set admin-telnet-port 21                    set admin-telnet-port 23
set admintimeout 3                          set admintimeout 5
set anti-replay strict                      set anti-replay strict
set auth-cert "self-sign"                   set auth-cert "self-sign"
set auth-http-port 1000                     set auth-http-port 2000
set auth-https-port 1003                    set auth-https-port 1000
set auth-keepalive disable                  set auth-keepalive disable
set auth-policy-exact-match enable          set auth-policy-exact-match enable
set av-failopen pass                        set av-failopen pass
set av-failopen-session disable             set av-failopen-session disable
set batch-cmdb enable                       set batch-cmdb enable
set cfg-save automatic                      set cfg-save automatic
set check-protocol-header loose             set check-protocol-header loose
set check-reset-range disable               set check-reset-range disable
set cli-cert-req disable                    set cli-cert-req disable
set daily-restart disable                   set daily-restart disable
set detection-summary enable                set detection-summary enable
```

- Compare configuration changes between any two configurations , side by side using Diff View.
- Easily identify changes between configuration files using color-coded change depiction.
- View added lines in green, deleted lines in red and modified lines in blue.

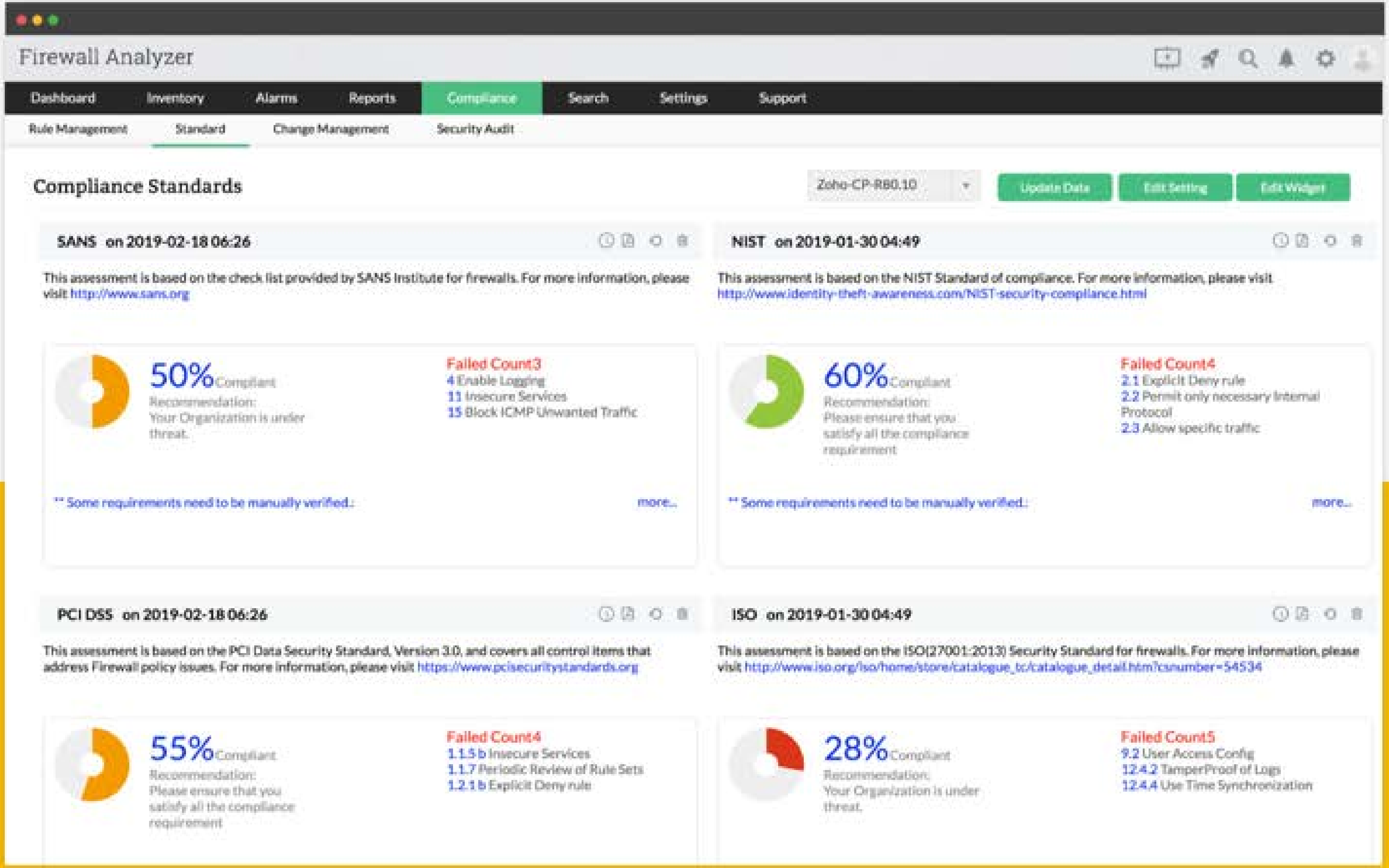
Configuration Backup



```
config system global                         config system global
set access-banner disable                    set access-banner disable
set admin-https-pki-required disable         set admin-https-pki-required disable
set admin-lockout-duration 60                set admin-lockout-duration 62
set admin-lockout-threshold 3                set admin-lockout-threshold 4
set admin-maintainer enable                  set admin-maintainer enable
set admin-port 80                            set admin-port 8080
set admin-scp enable                         set admin-scp enable
set admin-server-cert "self-sign"            set admin-server-cert "self-sign"
set admin-sport 443                          set admin-sport 443
set admin-ssh-port 22                        set admin-ssh-port 22
set admin-ssh-v1 disable                     set admin-ssh-v1 disable
set admin-telnet-port 23                     set admin-telnet-port 25
set admintimeout 5                           set admintimeout 5
set anti-replay strict                       set anti-replay strict
set auth-cert "self-sign"                    set auth-cert "self-sign"
set auth-http-port 1000                      set auth-http-port 2000
set auth-https-port 1003                     set auth-https-port 1000
set auth-keepalive disable                   set auth-keepalive disable
set auth-policy-exact-match enable           set auth-policy-exact-match enable
set av-failopen pass                         set av-failopen pass
set av-failopen-session disable              set av-failopen-session disable
set batch-cmdb enable                        set batch-cmdb enable
set cfg-save automatic                       set cfg-save automatic
set check-protocol-header loose              set check-protocol-header loose
set check-reset-range disable                set check-reset-range disable
set clt-cert-req disable                     set clt-cert-req disable
set daily-restart disable                    set daily-restart disable
set detection-summary enable                 set detection-summary enable
```

- Compare configuration changes between any two configurations , side by side using Diff View.
- Easily identify changes between configuration files using color-coded change depiction.
- View added lines in green, deleted lines in red and modified lines in blue.

Compliance and security audit



Compliance Standards

SANS on 2019-02-18 06:26

This assessment is based on the check list provided by SANS Institute for firewalls. For more information, please visit http://www.sans.org

50% Compliant

Recommendation:
Your Organization is under threat.

Failed Count3
4 Enable Logging
11 Insecure Services
15 Block ICMP Unwanted Traffic

** Some requirements need to be manually verified.: more...

NIST on 2019-01-30 04:49

This assessment is based on the NIST Standard of compliance. For more information, please visit http://www.identity-theft-awareness.com/NIST-security-compliance.html

60% Compliant

Recommendation:
Please ensure that you satisfy all the compliance requirement

Failed Count4
2.1 Explicit Deny rule
2.2 Permit only necessary Internal Protocol
2.3 Allow specific traffic

** Some requirements need to be manually verified.: more...

PCI DSS on 2019-02-18 06:26

This assessment is based on the PCI Data Security Standard, Version 3.0, and covers all control items that address Firewall policy issues. For more information, please visit https://www.pcisecuritystandards.org

55% Compliant

Recommendation:
Please ensure that you satisfy all the compliance requirement

Failed Count4
1.1.5 b Insecure Services
1.1.7 Periodic Review of Rule Sets
1.2.1 b Explicit Deny rule

ISO on 2019-01-30 04:49

This assessment is based on the ISO(27001:2013) Security Standard for firewalls. For more information, please visit http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

28% Compliant

Recommendation:
Your Organization is under threat.

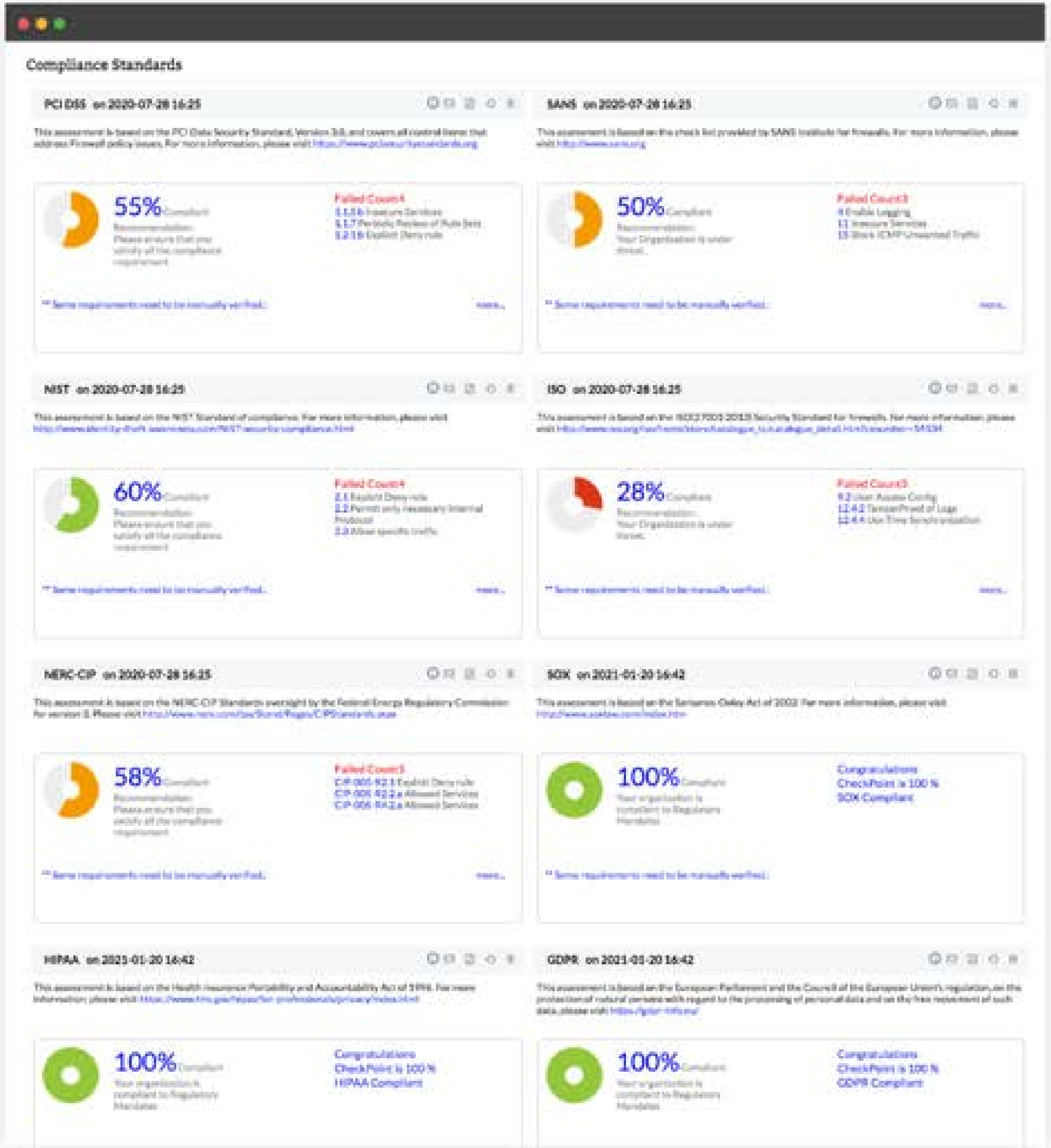
Failed Count5
9.2 User Access Config
12.4.2 TamperProof of Logs
12.4.4 Use Time Synchronization

Stay compliant with out-of-the-box compliance reports

Follow standard practices, and execute internal/external security policies to avoid legal issues with a proper compliance management!

- Stay compliant to PCI-DSS, ISO 27001, NIST, NERC-CIP, SANS, SOX, HIPAA, GDP & Basel II regulatory mandates.
- Identify configuration loop holes and stay secure.
- Generate reports on the compliance status of firewall devices.

Compliance Report



Compliance Standards

PCI DSS on 2020-07-28 16:25

This assessment is based on the PCI Data Security Standard, Version 3.0, and covers all control items that address Firewall policy issues. For more information, please visit https://www.pcisecuritystandards.org

55% Compliant

Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count:4
1.1.5.b Insecure Services
1.1.7 Periodic Review of Rule Sets
1.2.1.b Explicit Deny rule

** Some requirements need to be manually verified.

more..

SANS on 2020-07-28 16:25

This assessment is based on the check list provided by SANS Institute for firewalls. For more information, please visit http://www.sans.org

50% Compliant

Recommendation: Your Organization is under threat.

Failed Count:3
4 Enable Logging
11 Insecure Services
13 Block ICMP Unwanted Traffic

** Some requirements need to be manually verified.

more..

NIST on 2020-07-28 16:25

This assessment is based on the NIST Standard of compliance. For more information, please visit http://www.identity-theft-awareness.com/NIST-security-compliance.html

60% Compliant

Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count:4
2.1 Explicit Deny rule
2.2 Permit only necessary Internal Protocol
2.3 Allow specific traffic

** Some requirements need to be manually verified.

more..

ISO on 2020-07-28 16:25

This assessment is based on the ISO/IEC 27001:2013 Security Standard for firewalls. For more information, please visit http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

28% Compliant

Recommendation: Your Organization is under threat.

Failed Count:5
9.2 User Access Config
12.4.2 TamperProof of Logs
12.4.4 Use Time Synchronization

** Some requirements need to be manually verified.

more..

NERC-CIP on 2020-07-28 16:25

This assessment is based on the NERC-CIP Standards oversight by the Federal Energy Regulatory Commission for version 3. Please visit http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

58% Compliant

Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count:5
CIP-005-R2.1 Explicit Deny rule
CIP-005-R2.2.a Allowed Services
CIP-006-R4.2.a Allowed Services

** Some requirements need to be manually verified.

more..

SOX on 2021-01-20 16:42

This assessment is based on the Sarbanes Oxley Act of 2002. For more information, please visit http://www.soxlaw.com/index.htm

100% Compliant

Your organization is compliant to Regulatory Mandates

Congratulations
CheckPoint is 100 %
SOX Compliant

** Some requirements need to be manually verified.

HIPAA on 2021-01-20 16:42

This assessment is based on the Health Insurance Portability and Accountability Act of 1996. For more information, please visit https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

100% Compliant

Your organization is compliant to Regulatory Mandates

Congratulations
CheckPoint is 100 %
HIPAA Compliant

GDPR on 2021-01-20 16:42

This assessment is based on the European Parliament and the Council of the European Union's regulation, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, please visit https://gdpr-info.eu/

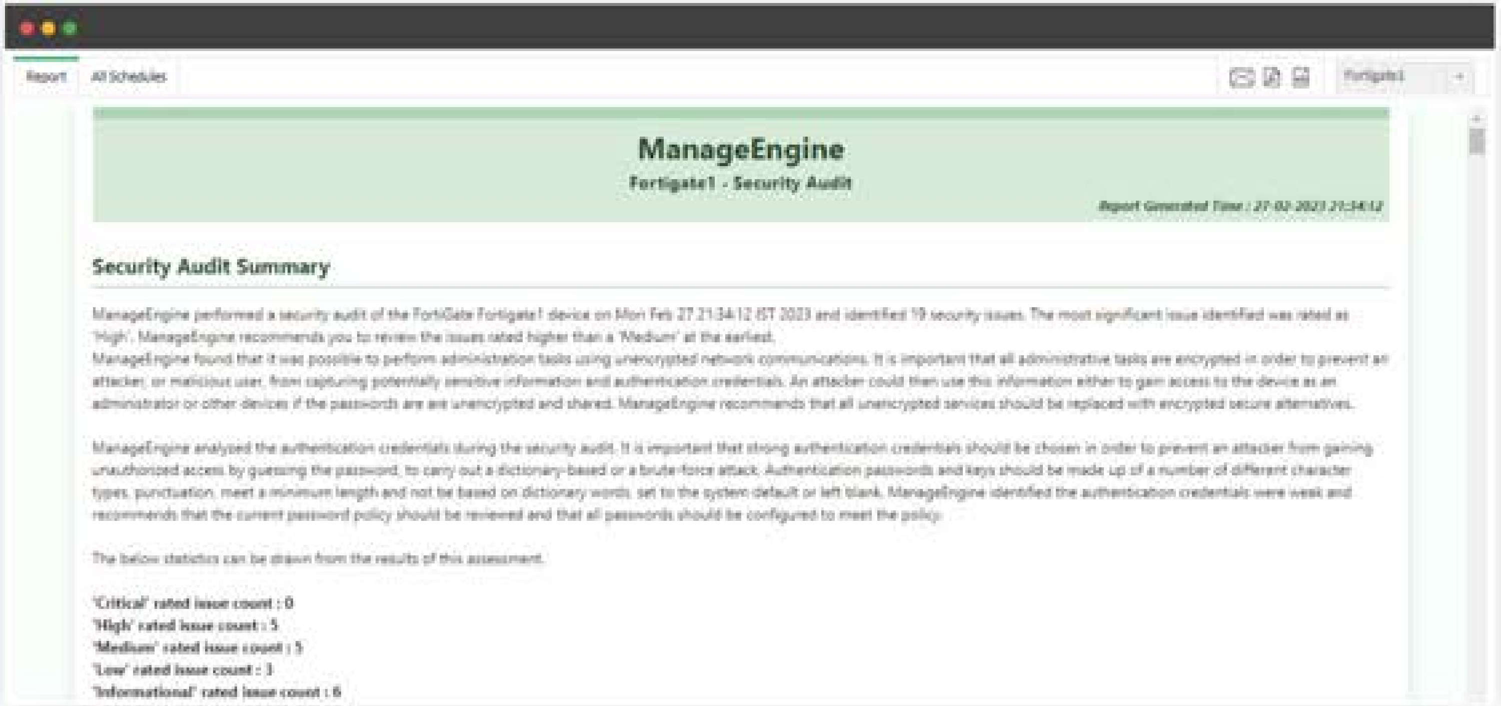
100% Compliant

Your organization is compliant to Regulatory Mandates

Congratulations
CheckPoint is 100 %
GDPR Compliant

- Secure your cardholder's data effectively by complying to PCI-DSS.
- Master information security management, by staying compliant with ISO 27001.
- Make sure your critical IT infrastructure is safe by staying compliant with NERC-CIP mandate
- Check for information security loopholes by verifying with SANS report.
- Review NIST standards with NIST compliance reports.
- Verify SOX, HIPAA, GDPR and Basel II compliance with out-of-the-box-reports

Security Audit



ManageEngine

Fortigate1 - Security Audit

Report Generated Time : 27-02-2023 21:34:12

Security Audit Summary

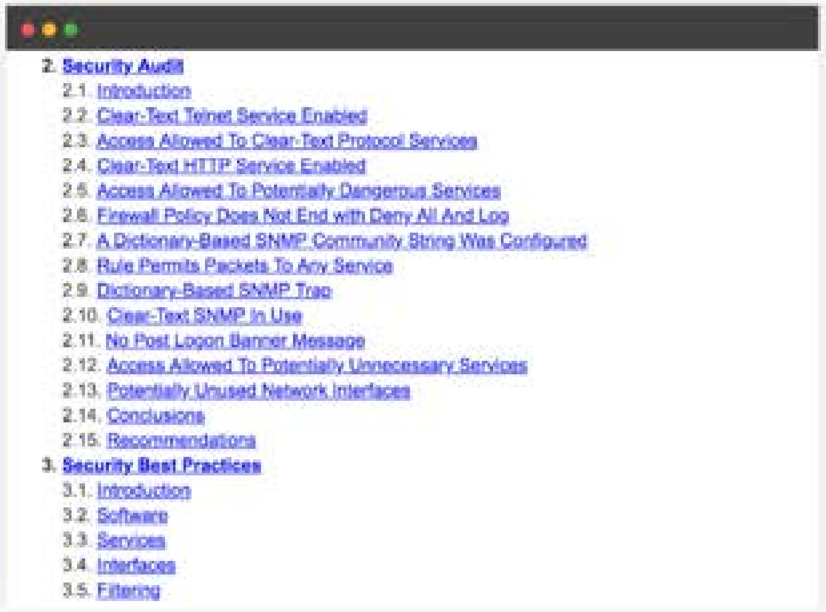
ManageEngine performed a security audit of the FortiGate Fortigate1 device on Mon Feb 27 21:34:12 IST 2023 and identified 19 security issues. The most significant issue identified was rated as 'High'. ManageEngine recommends you to review the issues rated higher than a 'Medium' at the earliest.
ManageEngine found that it was possible to perform administration tasks using unencrypted network communications. It is important that all administrative tasks are encrypted in order to prevent an attacker, or malicious user, from capturing potentially sensitive information and authentication credentials. An attacker could then use this information either to gain access to the device as an administrator or other devices if the passwords are are unencrypted and shared. ManageEngine recommends that all unencrypted services should be replaced with encrypted secure alternatives.

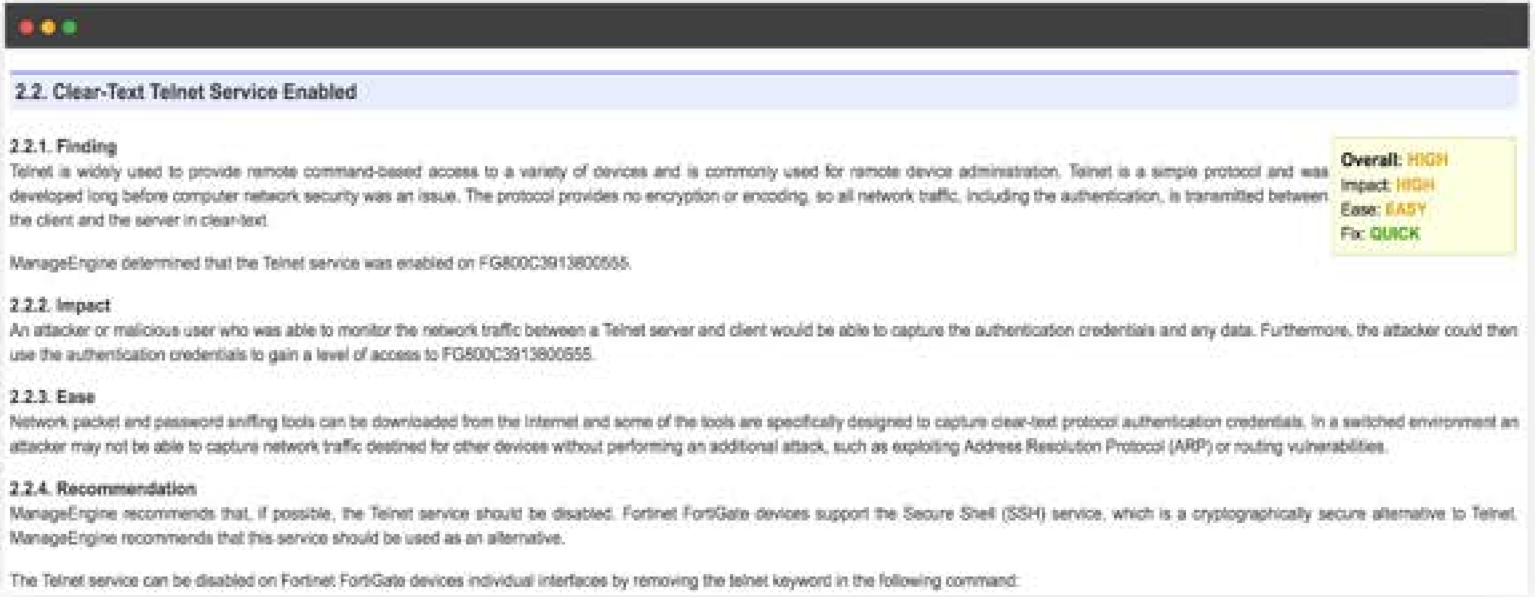
ManageEngine analysed the authentication credentials during the security audit. It is important that strong authentication credentials should be chosen in order to prevent an attacker from gaining unauthorized access by guessing the password, to carry out a dictionary-based or a brute-force attack. Authentication passwords and keys should be made up of a number of different character types, punctuation, meet a minimum length and not be based on dictionary words, set to the system default or left blank. ManageEngine identified the authentication credentials were weak and recommends that the current password policy should be reviewed and that all passwords should be configured to meet the policy.

The below statistics can be drawn from the results of this assessment.

'Critical' rated issue count : 0
'High' rated issue count : 5
'Medium' rated issue count : 5
'Low' rated issue count : 3
'Informational' rated issue count : 6

- Perform security audits on the configuration setup of your firewall and get detailed reports on any security loopholes.
- Identify the criticality of the configuration loopholes and also get the ease of attack.
- Get recommendation on industry best practices.





2.2. Clear-Text Telnet Service Enabled

Overall: HIGH
Impact: HIGH
Ease: EASY
Fix: QUICK

2.2.1. Finding
Telnet is widely used to provide remote command-based access to a variety of devices and is commonly used for remote device administration. Telnet is a simple protocol and was developed long before computer network security was an issue. The protocol provides no encryption or encoding, so all network traffic, including the authentication, is transmitted between the client and the server in clear-text.

ManageEngine determined that the Telnet service was enabled on FG800C3913800555.

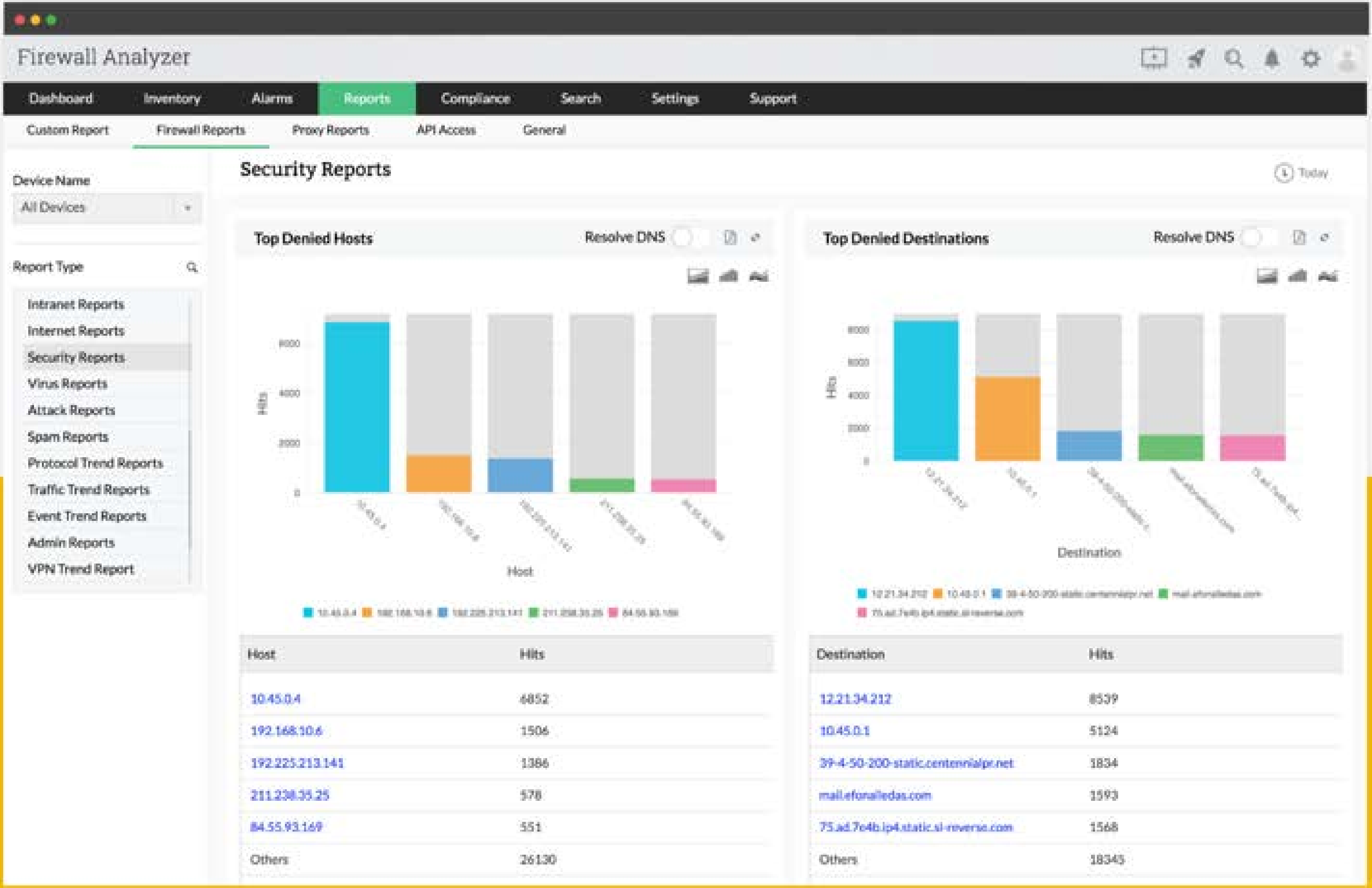
2.2.2. Impact
An attacker or malicious user who was able to monitor the network traffic between a Telnet server and client would be able to capture the authentication credentials and any data. Furthermore, the attacker could then use the authentication credentials to gain a level of access to FG800C3913800555.

2.2.3. Ease
Network packet and password sniffing tools can be downloaded from the Internet and some of the tools are specifically designed to capture clear-text protocol authentication credentials. In a switched environment an attacker may not be able to capture network traffic destined for other devices without performing an additional attack, such as exploiting Address Resolution Protocol (ARP) or routing vulnerabilities.

2.2.4. Recommendation
ManageEngine recommends that, if possible, the Telnet service should be disabled. Fortinet FortiGate devices support the Secure Shell (SSH) service, which is a cryptographically secure alternative to Telnet. ManageEngine recommends that this service should be used as an alternative.

The Telnet service can be disabled on Fortinet FortiGate devices individual interfaces by removing the telnet keyword in the following command:

Log Management



Security Reports

Top Denied Hosts

Host	Hits
10.45.0.4	6852
192.168.10.6	1506
192.225.213.141	1386
211.238.35.25	578
84.55.93.169	551
Others	26130

Top Denied Destinations

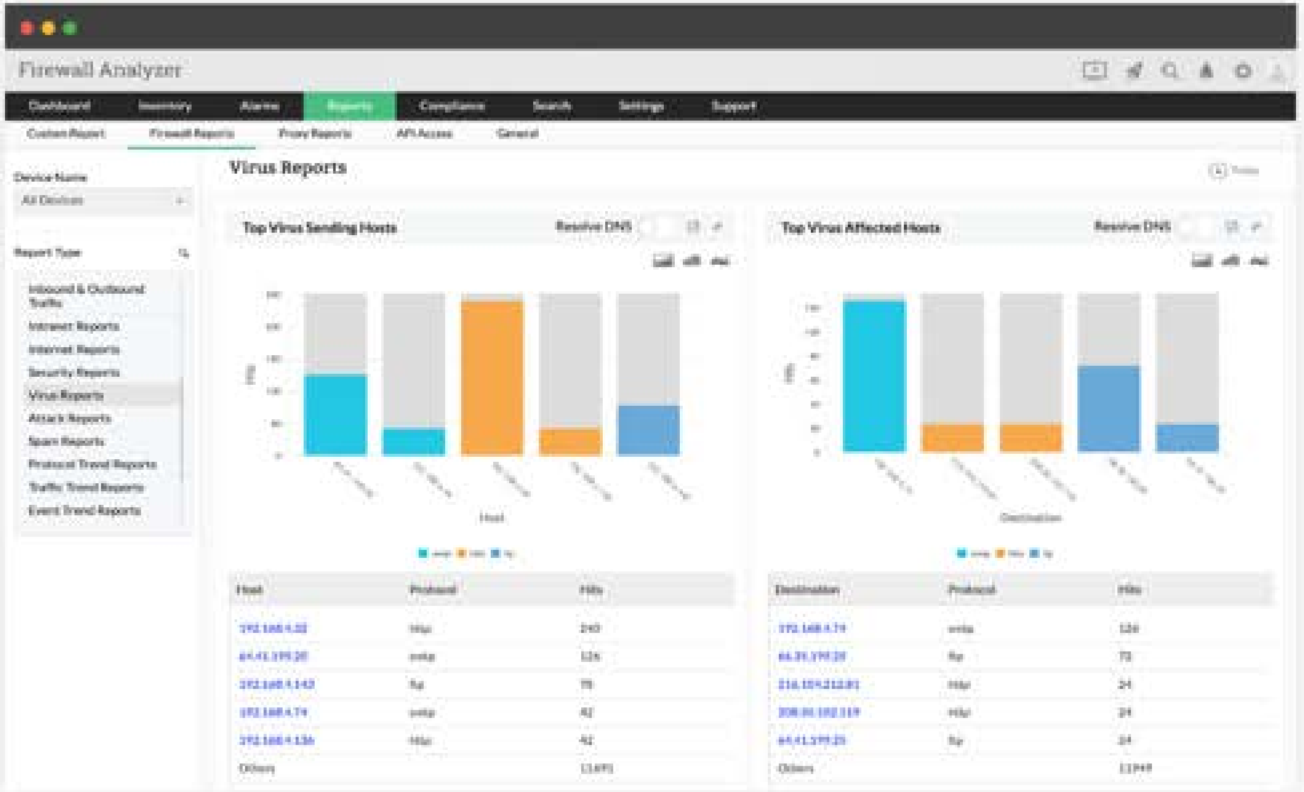
Destination	Hits
12.21.34.212	8539
10.45.0.1	5124
39-4-50-200-static.centennialpr.net	1834
mail.eforalledas.com	1593
75.ad.7e4b.ip4.static.sl-reverse.com	1568
Others	18343

Log Management is critical for network security

Analyzing syslog data will help you identify and prevent security threats in real time

- Security analysis helps in identifying internal and external threats.
- Traffic analysis helps in bandwidth management.
- Log based alerts help in instant remediation.

Security Analytics



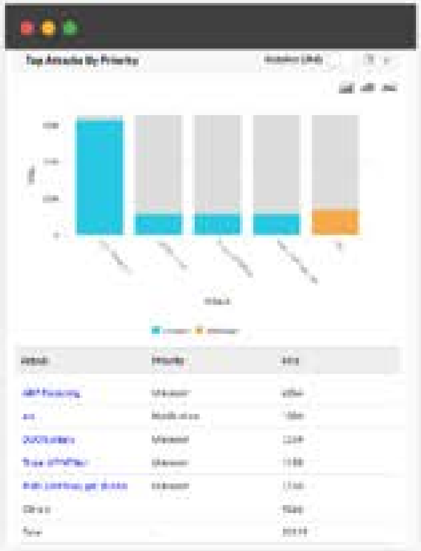
Virus Reports

Top Virus Sending Hosts

Host	Protocol	Hits
192.168.4.22	http	240
64.41.199.20	smtp	126
192.168.4.143	ftp	78
192.168.4.74	smtp	42
192.168.4.136	http	42
Others		11695

Top Virus Affected Hosts

Destination	Protocol	Hits
192.168.4.79	smtp	126
66.35.199.20	ftp	72
216.109.212.81	http	24
208.80.102.119	http	24
64.41.199.23	ftp	24
Others		11949



Top Attacks By Priority

Attack	Priority	Hits

Top Spam Receivers

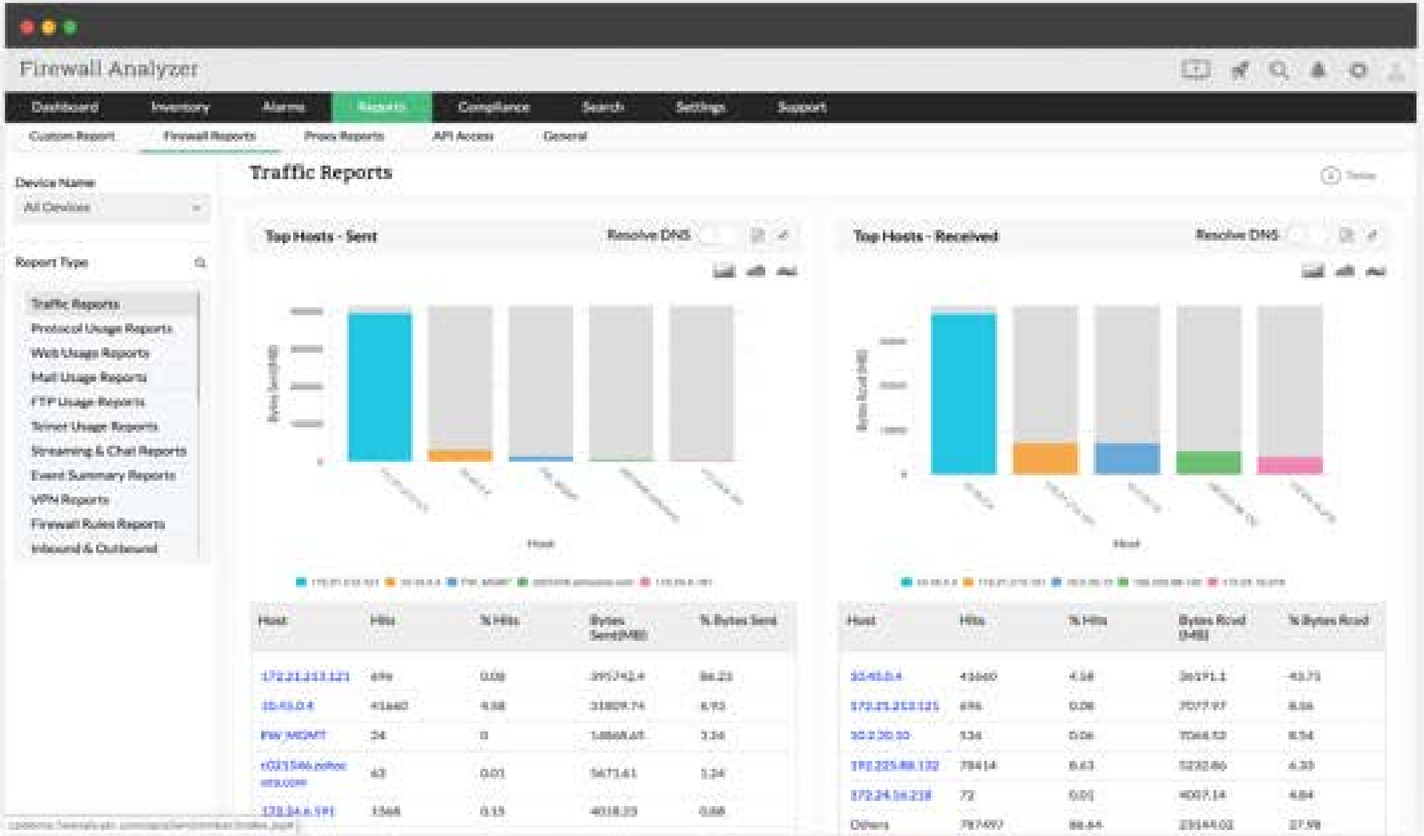
Destination	Recipient	Hits

Top Security Events

Severity	#Events	% Event Count

- Generate detailed reports on possible security threats to the network.
- Troubleshoot and resolve security issues faster by identifying and analysing virus related logs.
- Gain insights to identify and counter network attacks.
- Get detailed information on the spam activity and control spam across the network.

Traffic Analytics



Traffic Reports

Top Hosts - Sent

Host	Hits	% Hits	Bytes Sent(MB)	% Bytes Sent
172.21.213.121	696	0.08	395742.4	86.23
10.45.0.4	41660	4.58	31809.74	6.93
FW_MGMT	24	0	14868.65	3.24
c021546.zohocorp.com	63	0.01	5673.61	1.24
172.24.6.191	1568	0.15	4018.23	0.88

Top Hosts - Received

Host	Hits	% Hits	Bytes Rcvd (MB)	% Bytes Rcvd
10.45.0.4	41660	4.58	26191.1	43.73
172.21.213.121	696	0.08	7077.97	8.06
10.2.20.10	536	0.06	7066.52	8.54
192.225.88.132	78414	8.63	5232.86	6.33
172.24.16.218	72	0.01	4007.14	4.84
Others	787497	86.64	23544.02	27.98

Top Protocol Groups (Sent+Received)

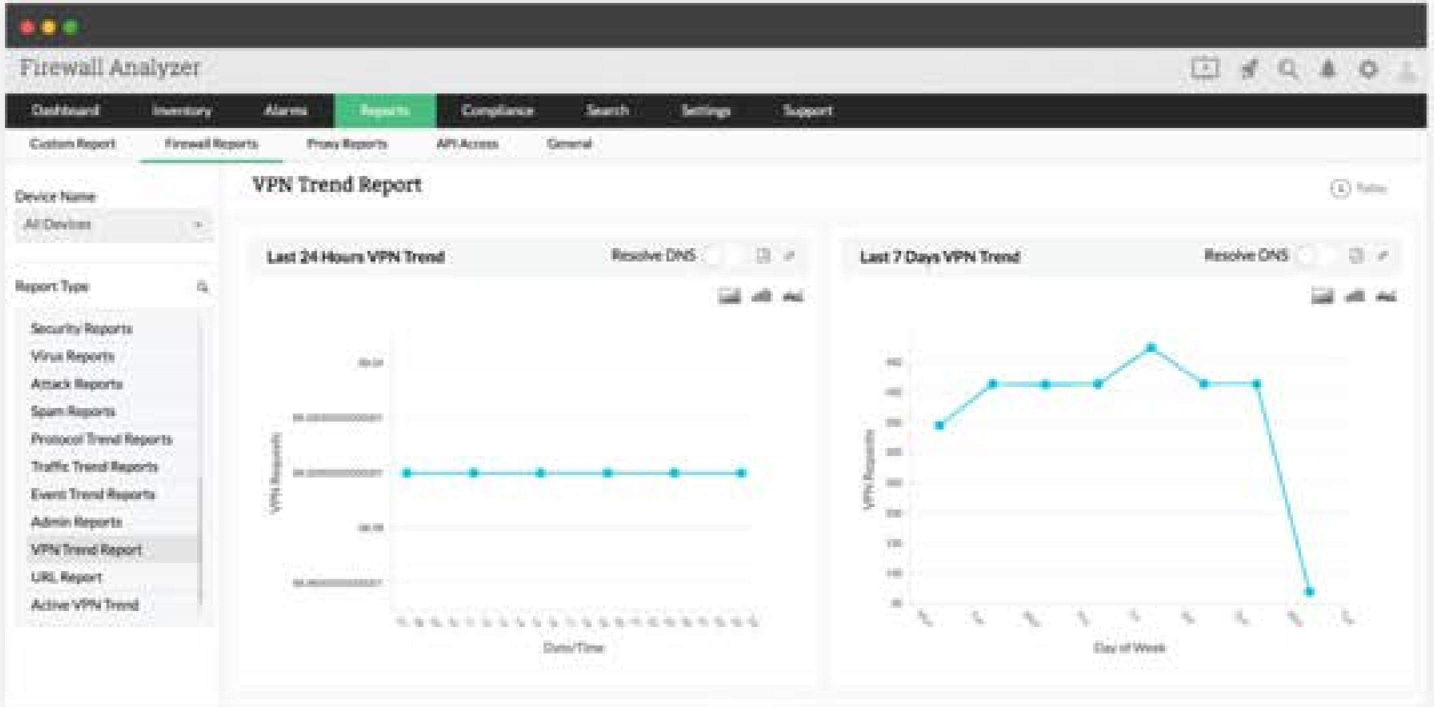
Top Users (Sent+Received)

Top Streaming and Chat Sites

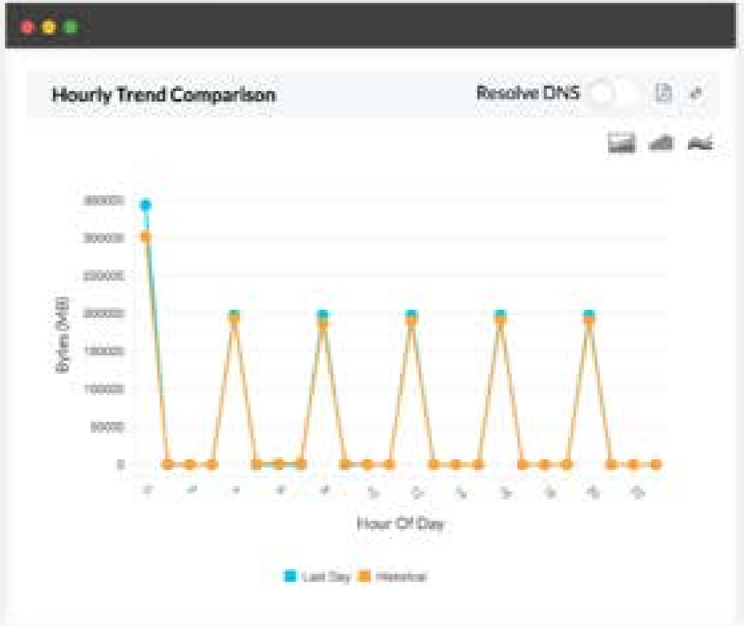
Firewall Analyzer's traffic reports help answering the following questions

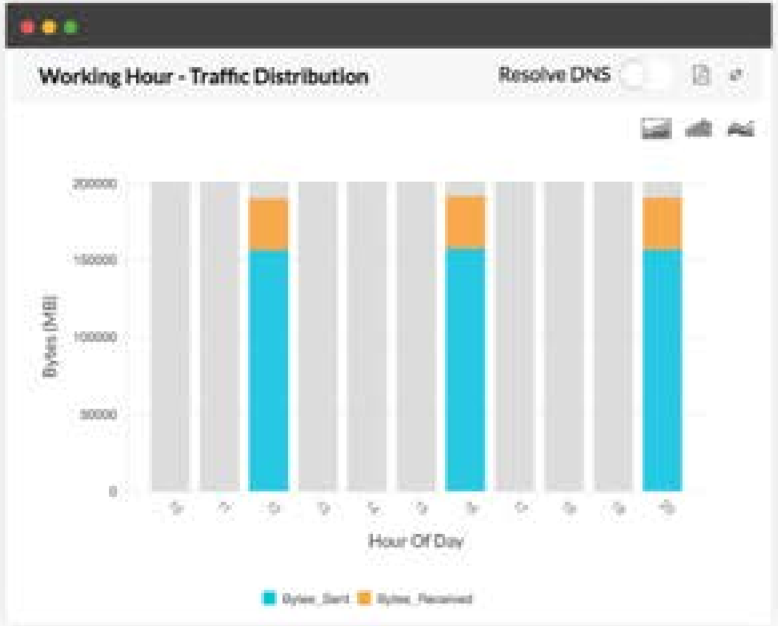
- Who is sending, receiving the traffic?
- Which host is sending, receiving the traffic?
- What is the traffic share of various protocol groups?
- What is the event severity pattern due to the traffic?

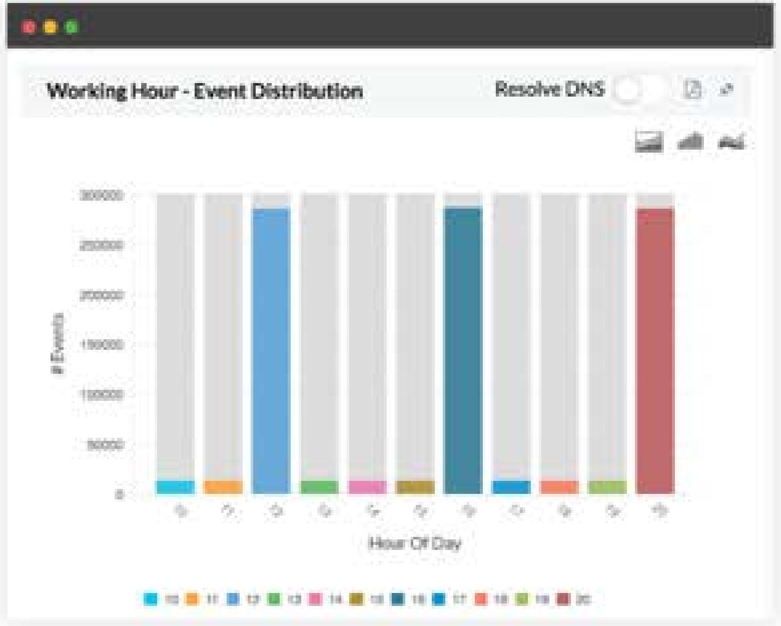
Trend Analysis



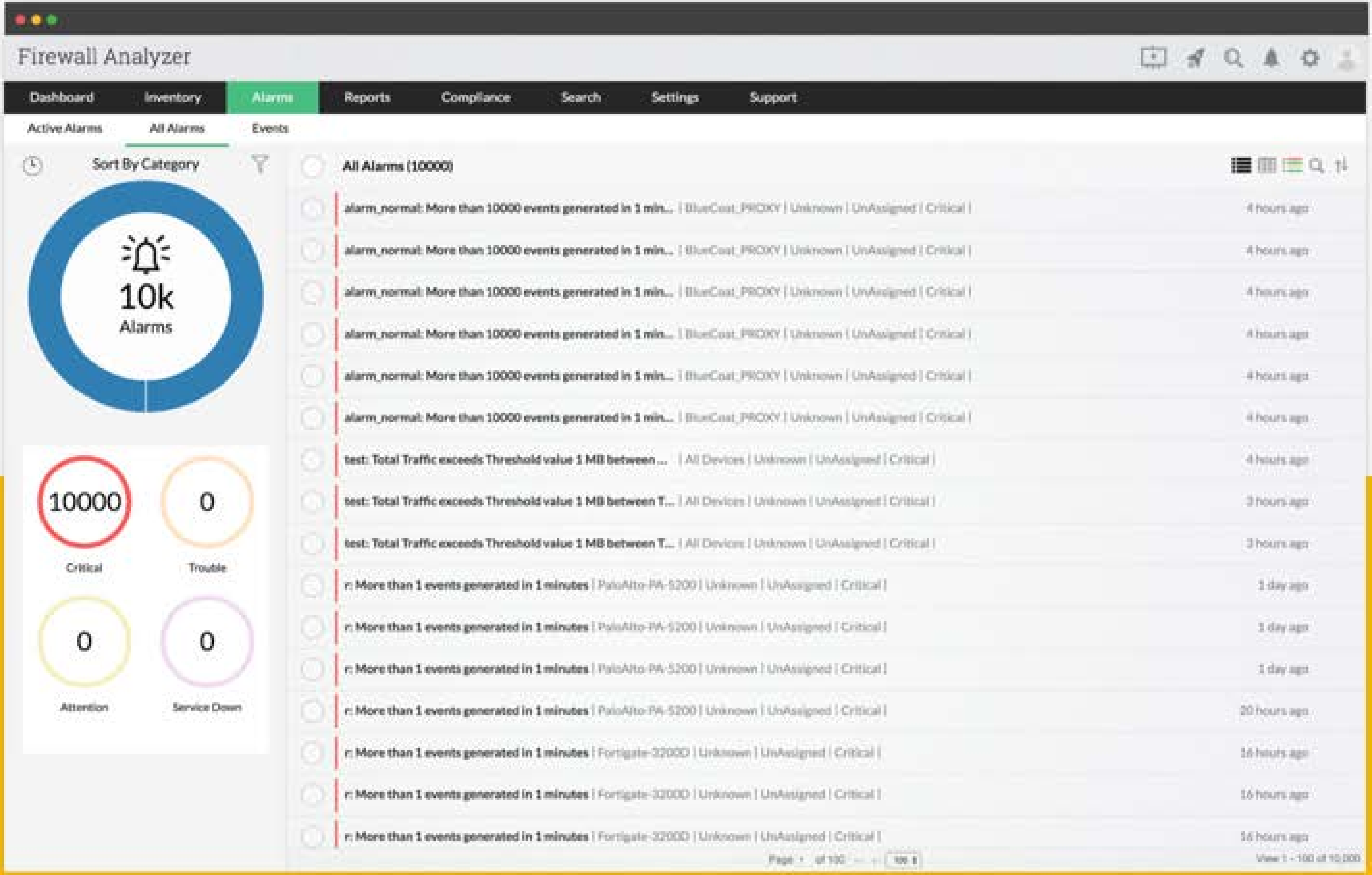
- Determine peak bandwidth usage trend across different protocols and time stamps.
- Troubleshoot links and identify security risks by analysing the event trend report.
- Identify live VPN connections and VPN related security risks using the VPN trend report.







Other significant features



All Alarms (10000)

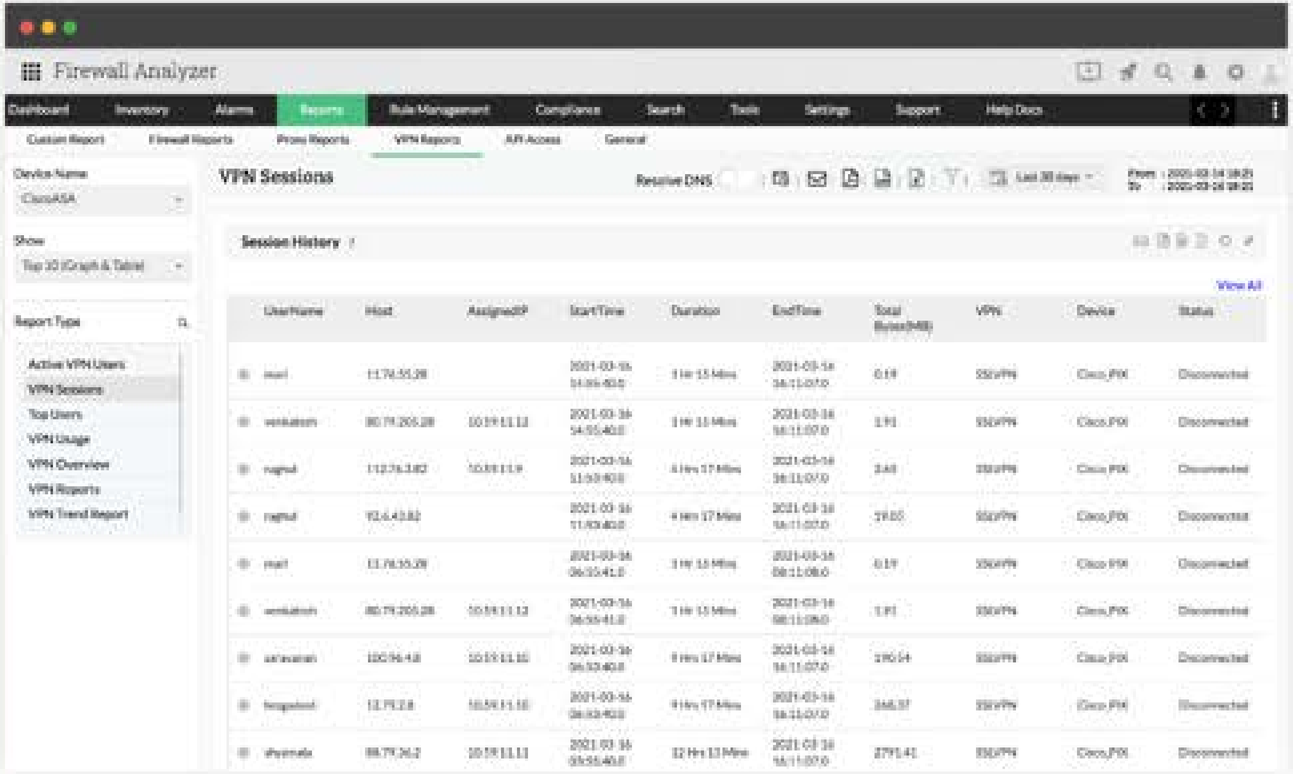
```
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical |    4 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical |    4 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical |    4 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical |    4 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical |    4 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical |    4 hours ago
test: Total Traffic exceeds Threshold value 1 MB between ... | All Devices | Unknown | UnAssigned | Critical |    4 hours ago
test: Total Traffic exceeds Threshold value 1 MB between T... | All Devices | Unknown | UnAssigned | Critical |    3 hours ago
test: Total Traffic exceeds Threshold value 1 MB between T... | All Devices | Unknown | UnAssigned | Critical |    3 hours ago
r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssigned | Critical |    1 day ago
r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssigned | Critical |    1 day ago
r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssigned | Critical |    1 day ago
r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssigned | Critical |    20 hours ago
r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigned | Critical |    16 hours ago
r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigned | Critical |    16 hours ago
r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigned | Critical |    16 hours ago
```

Page 1 of 100   100

View 1 - 100 of 10,000

VPN Reports

- Identify users connected to your VPN, the traffic consumed by them and also failed VPN logins.
- Identify IPs and their VPN bandwidth consumption. Track destinations your VPN IPs land on. Monitor active VPN sessions and identify VPN bandwidth trends



Device Name: CiscoASA

Show: Top 10 (Graph & Table)

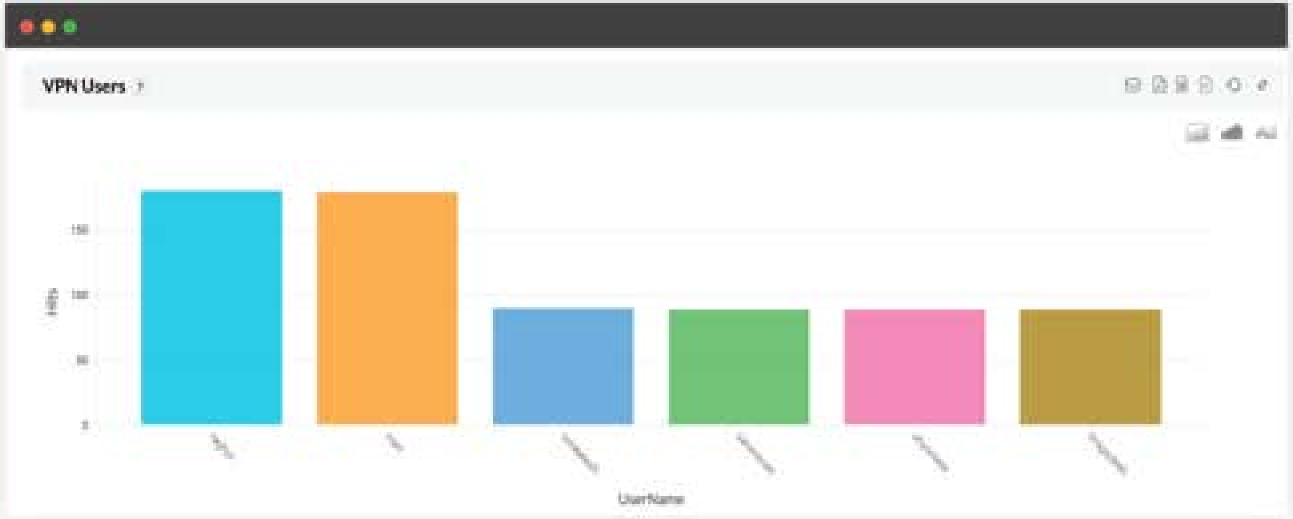
Report Type
- Active VPN Users
- VPN Sessions
- Top Users
- VPN Usage
- VPN Overview
- VPN Reports
- VPN Trend Report

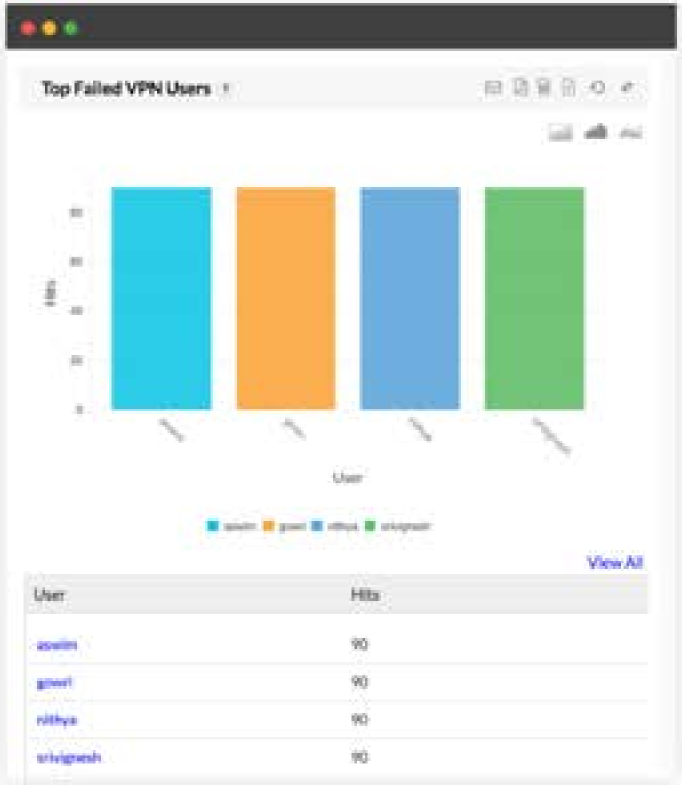
VPN Sessions

From : 2021-02-14 18:21
To : 2021-03-16 18:21

Session History

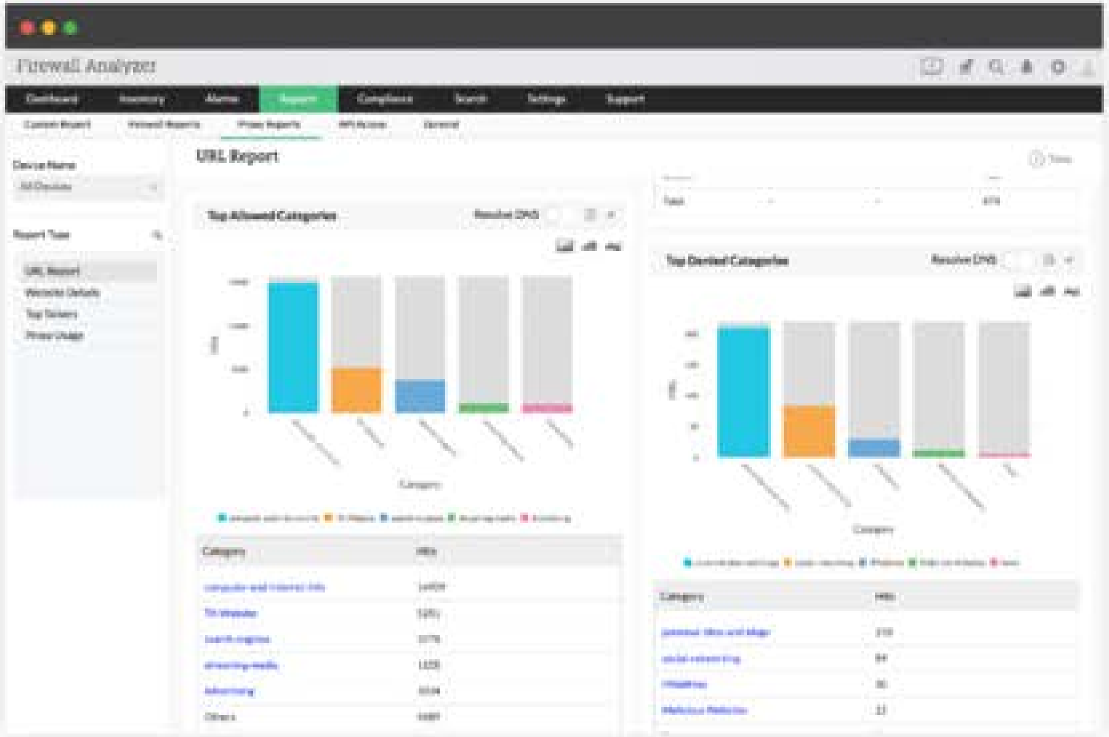
UserName	Host	AssignedIP	StartTime	Duration	EndTime	Total Bytes(MB)	VPN	Device	Status
mari	11.76.55.28		2021-03-16 14:06:40.0	1 Hr 13 Mins	2021-03-16 16:11:07.0	0.19	SSLVPN	Cisco_PIX	Disconnected
venkatesh	80.79.205.28	10.59.11.12	2021-03-16 14:55:40.0	1 Hr 13 Mins	2021-03-16 16:11:07.0	1.91	SSLVPN	Cisco_PIX	Disconnected
raghul	112.76.3.82	10.59.11.9	2021-03-16 11:53:40.0	4 Hrs 17 Mins	2021-03-16 16:11:07.0	3.43	SSLVPN	Cisco_PIX	Disconnected
raghul	92.6.43.82		2021-03-16 11:53:40.0	4 Hrs 17 Mins	2021-03-16 16:11:07.0	19.03	SSLVPN	Cisco_PIX	Disconnected
mari	11.76.55.28		2021-03-16 06:53:41.0	1 Hr 13 Mins	2021-03-16 08:11:08.0	0.19	SSLVPN	Cisco_PIX	Disconnected
venkatesh	80.79.205.28	10.59.11.12	2021-03-16 06:55:41.0	1 Hr 13 Mins	2021-03-16 08:11:08.0	1.91	SSLVPN	Cisco_PIX	Disconnected
saravanan	100.96.4.8	10.59.11.10	2021-03-16 06:53:40.0	9 Hrs 17 Mins	2021-03-16 16:11:07.0	190.14	SSLVPN	Cisco_PIX	Disconnected
hingadevi	12.79.2.8	10.59.11.10	2021-03-16 06:53:40.0	9 Hrs 17 Mins	2021-03-16 16:11:07.0	268.37	SSLVPN	Cisco_PIX	Disconnected
shyamala	88.79.26.2	10.59.11.11	2021-03-16 03:55:40.0	12 Hrs 13 Mins	2021-03-16 16:11:07.0	2791.41	SSLVPN	Cisco_PIX	Disconnected





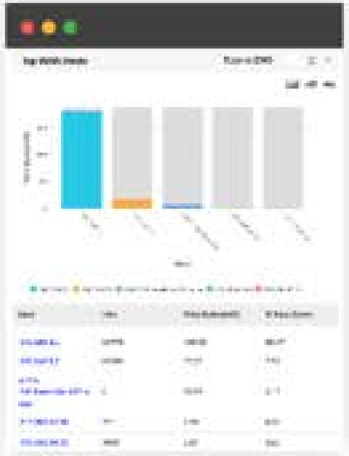
User	Hits
aswin	90
gowri	90
nithya	90
srivignesh	90

Proxy Report



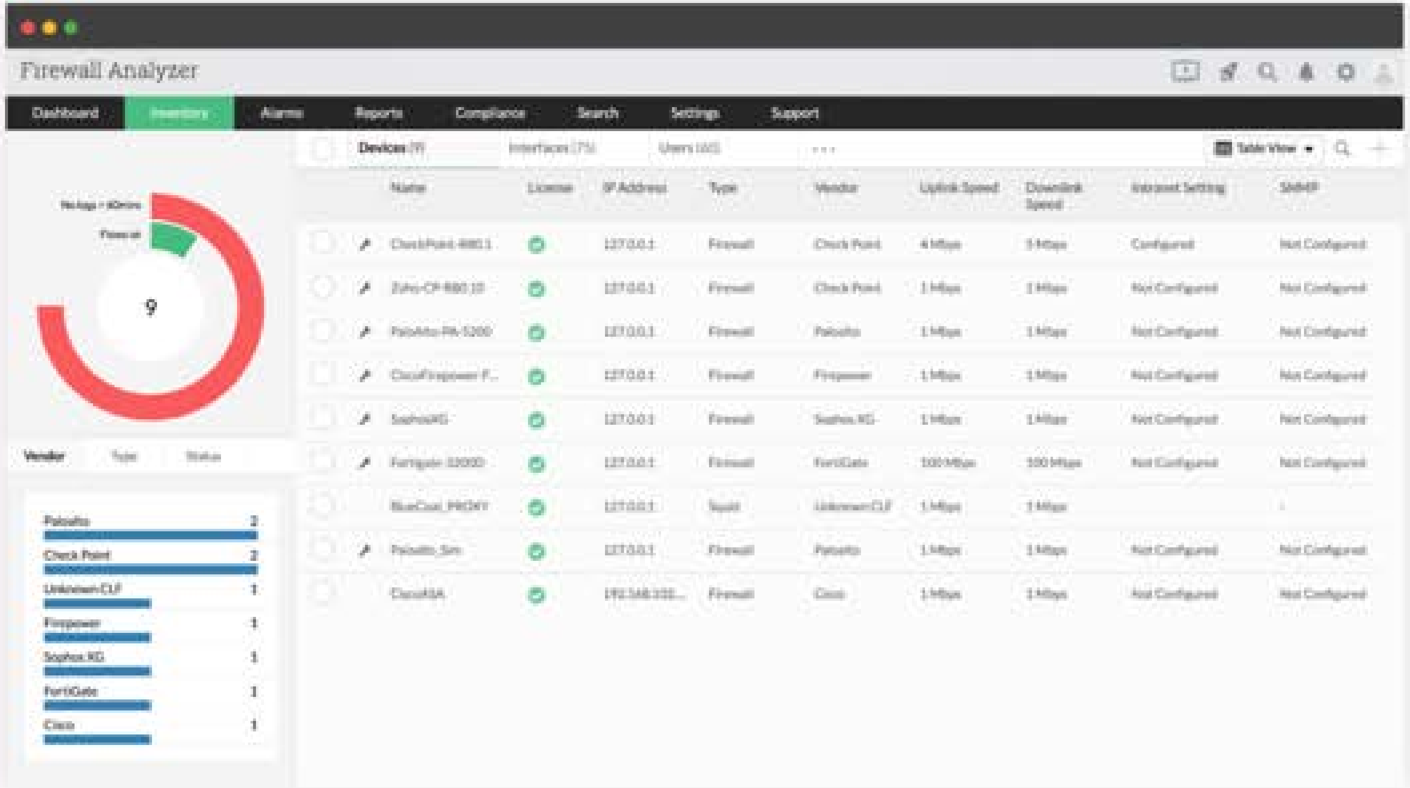
Category	Hits
computer and internet info	14929
TV Website	5251
search engines	3776
streaming media	1328
advertising	1034
Others	6687

Category	Hits
personal sites and blogs	210
social networking	84
shopping	30
Malicious Websites	13



- Collect and archive the proxy server logs, analyzes them, and generate useful corporate internet access information reports.
- Generate proxy usage and proxy virus reports
- Get the list of URLs accessed using the proxy server

Inventory report



Firewall Analyzer

Dashboard | Inventory | Alarms | Reports | Compliance | Search | Settings | Support

Devices (9) | Interfaces (75) | Users (60) | ··· | Table View

Vendor | Type | Status

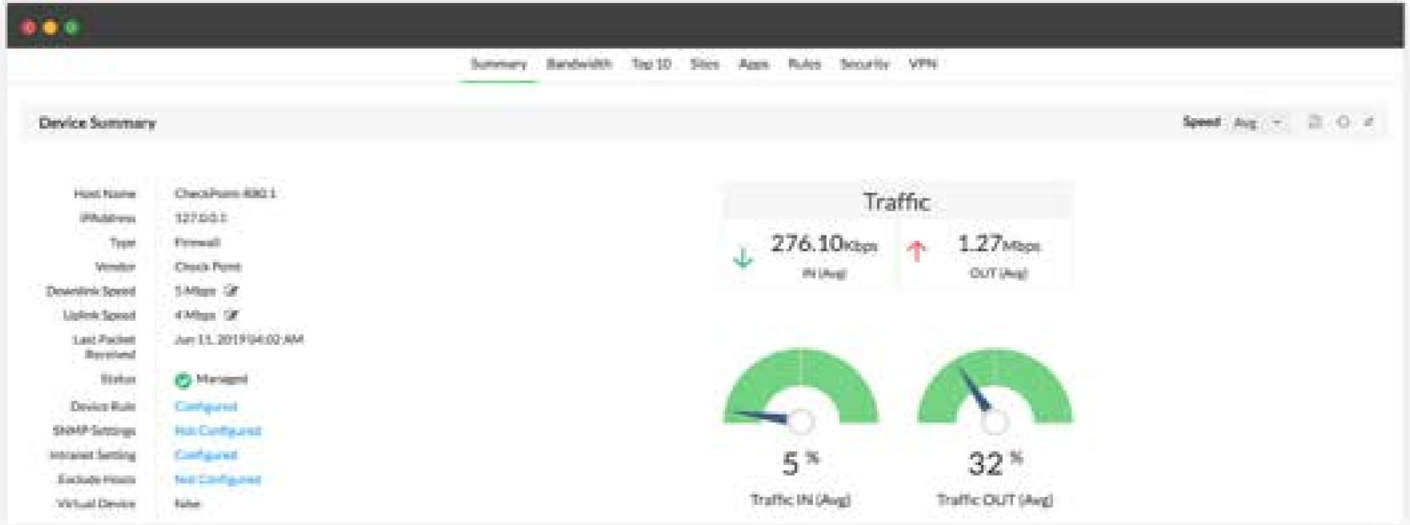
Paloalto	2
Check Point	2
Unknown CLF	1
Firepower	1
Sophos XG	1
FortiGate	1
Cisco	1

Name	License	IP Address	Type	Vendor	Uplink Speed	Downlink Speed	Intranet Setting	SNMP
CheckPoint-R80.1	✓	127.0.0.1	Firewall	Check Point	4 Mbps	5 Mbps	Configured	Not Configured
Zoho-CP-R80.10	✓	127.0.0.1	Firewall	Check Point	1 Mbps	1 Mbps	Not Configured	Not Configured
PaloAlto-PA-5200	✓	127.0.0.1	Firewall	Paloalto	1 Mbps	1 Mbps	Not Configured	Not Configured
CiscoFirepower F...	✓	127.0.0.1	Firewall	Firepower	1 Mbps	1 Mbps	Not Configured	Not Configured
SophosXG	✓	127.0.0.1	Firewall	Sophos XG	1 Mbps	1 Mbps	Not Configured	Not Configured
Fortigate-3200D	✓	127.0.0.1	Firewall	FortiGate	100 Mbps	100 Mbps	Not Configured	Not Configured
BlueCoat_PROXY	✓	127.0.0.1	Squid	Unknown CLF	1 Mbps	1 Mbps		-
Paloalto_Sim	✓	127.0.0.1	Firewall	Paloalto	1 Mbps	1 Mbps	Not Configured	Not Configured
CiscoASA	✓	192.168.100....	Firewall	Cisco	1 Mbps	1 Mbps	Not Configured	Not Configured

- Get a complete picture of everything that's happening on individual firewalls.
- Gain visibility to interfaces that are under the configured firewall devices.
- Get an overview of all the users that have accessed the internet through individual firewall devices.
- Monitor rules and cloud services accessed under a specific firewall device.

CheckPoint-R80.1

Traffic IN (Mbps)		Traffic OUT (Mbps)	
Min	Max	Min	Max
[illegible]	[illegible]	[illegible]	[illegible]



Summary | Bandwidth | Top 10 | Sites | Apps | Rules | Security | VPN

Device Summary

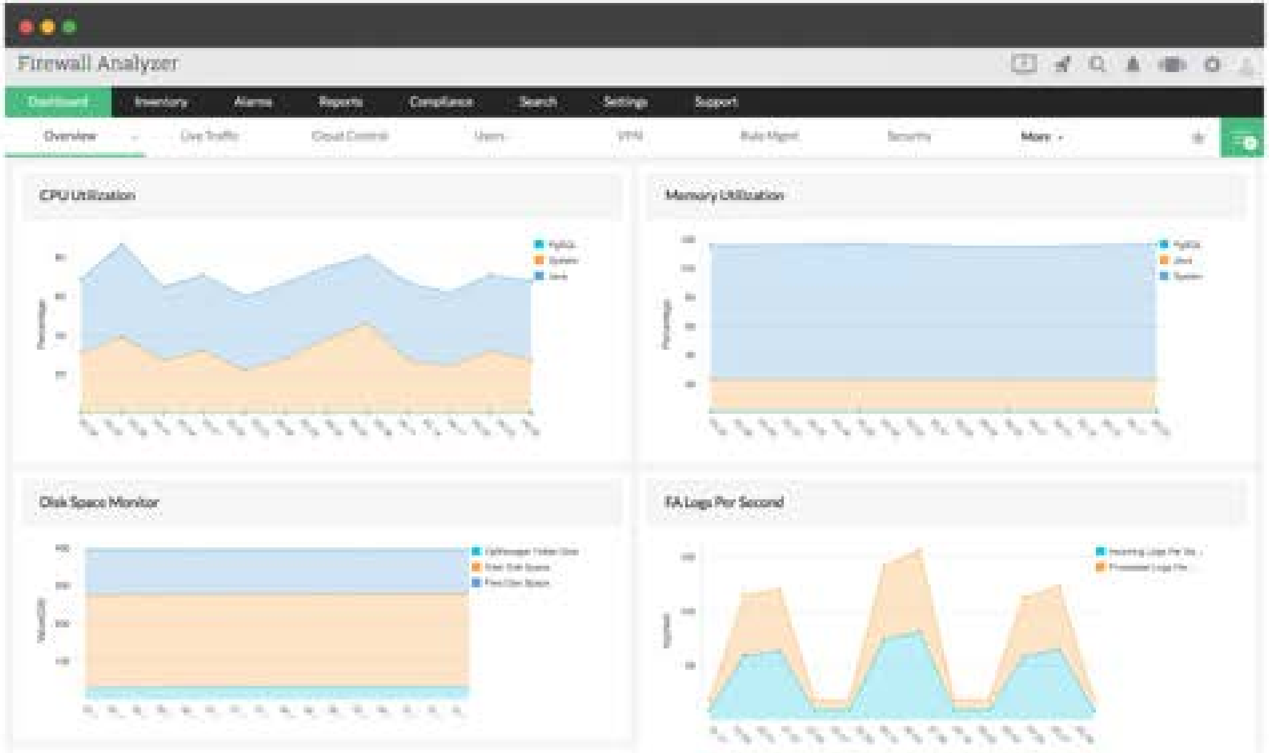
Speed Avg

Host Name	CheckPoint-R80.1
IPAddress	127.0.0.1
Type	Firewall
Vendor	Check Point
Downlink Speed	5 Mbps
Uplink Speed	4 Mbps
Last Packet Received	Jun 11, 2019 04:02 AM
Status	✓ Managed
Device Rule	Configured
SNMP Settings	Not Configured
Intranet Setting	Configured
Exclude Hosts	Not Configured
Virtual Device	false

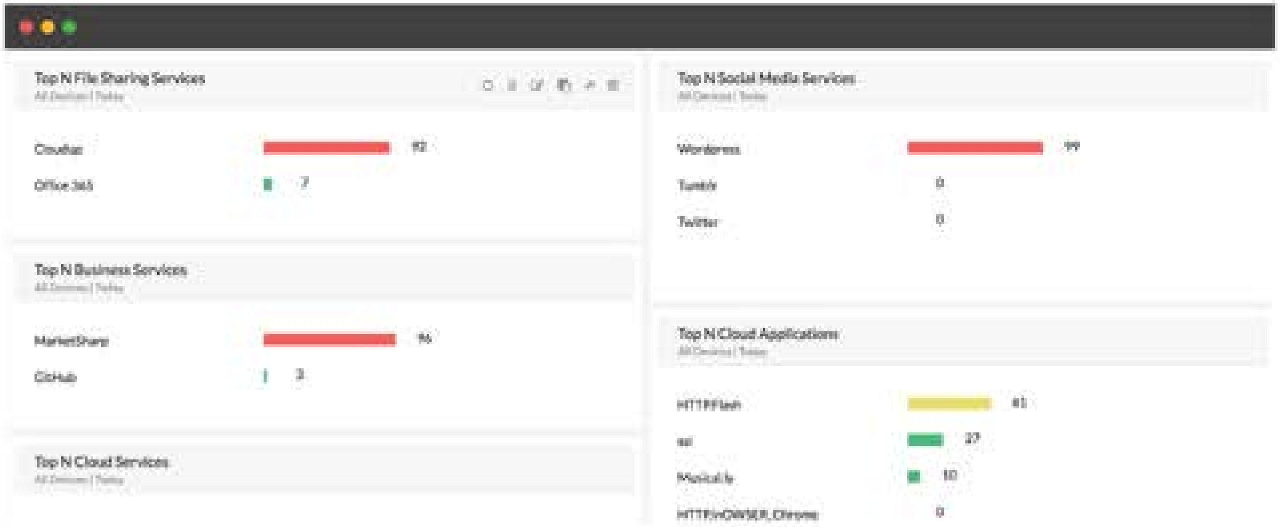
Traffic

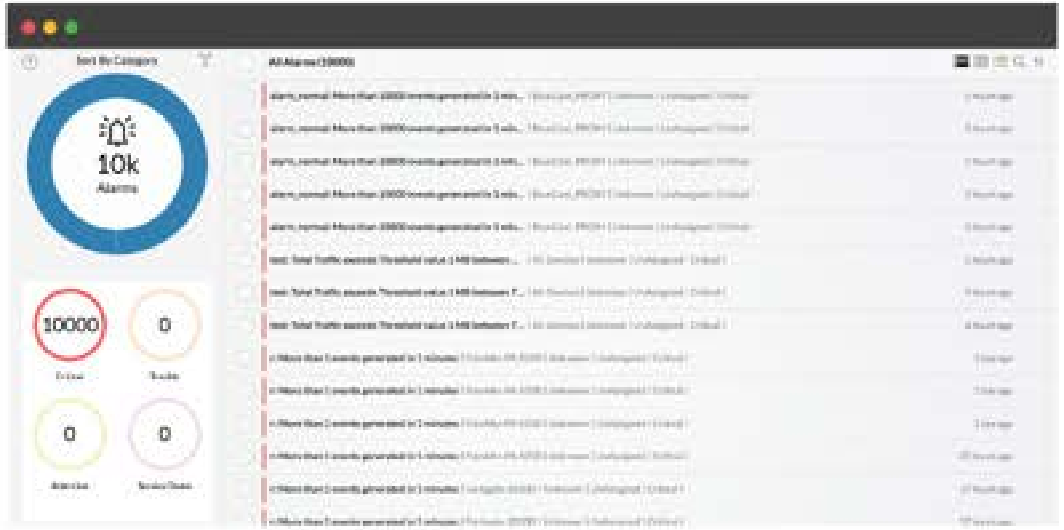
276.10 Kbps IN (Avg) | 1.27 Mbps OUT (Avg)

Dashboard, Cloud Monitoring & Alarms



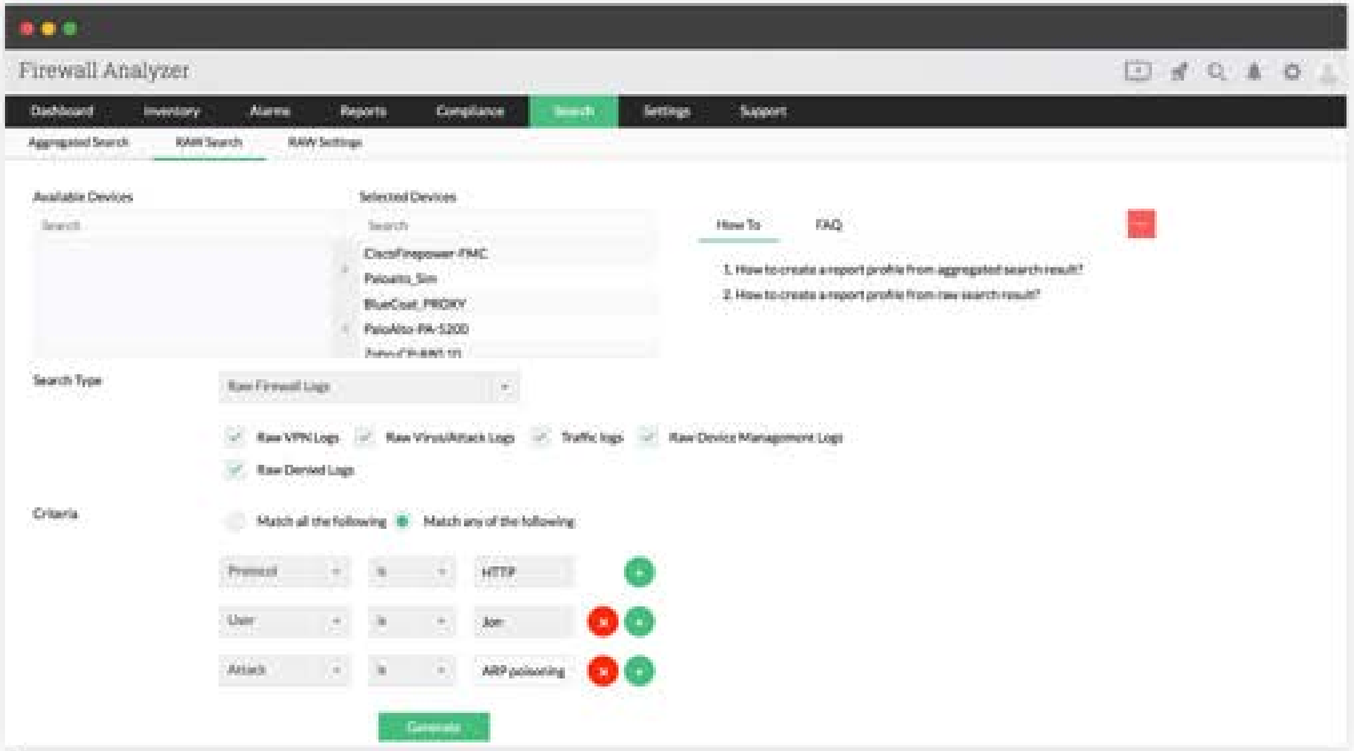
- Get a high level picture of everything that's happening on your firewall ecosystem.
- Keep a tight grip on all the cloud services running in your network.
- Trigger threshold based alerts (Both traffic and security) and get notifed directly to your mail or phone.





Forensic Log Analysis & Custom Reports

- Search the raw logs of Firewall to pinpoint the exact log entry which caused the security activity.
- Archived logs can be imported and security incident mining can be carried out by searching the raw logs.
- Generate custom reports based on specific criteria. Choose the sub-reports that you want to include in the custom report, the exact parameters to be reported on, and even the layout of the graph to be generated.



Available Devices: Search

Selected Devices: Search

CiscoFirepower-FMC
Paloalto_Sim
BlueCoat_PROXY
PaloAlto-PA-5200
ZohoCP-RM510

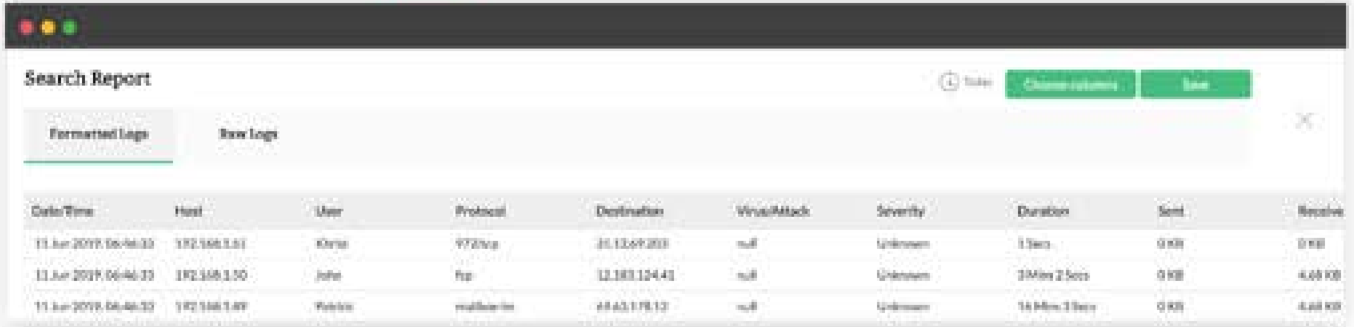
1. How to create a report profile from aggregated search result?
2. How to create a report profile from raw search result?

Search Type: Raw Firewall Logs

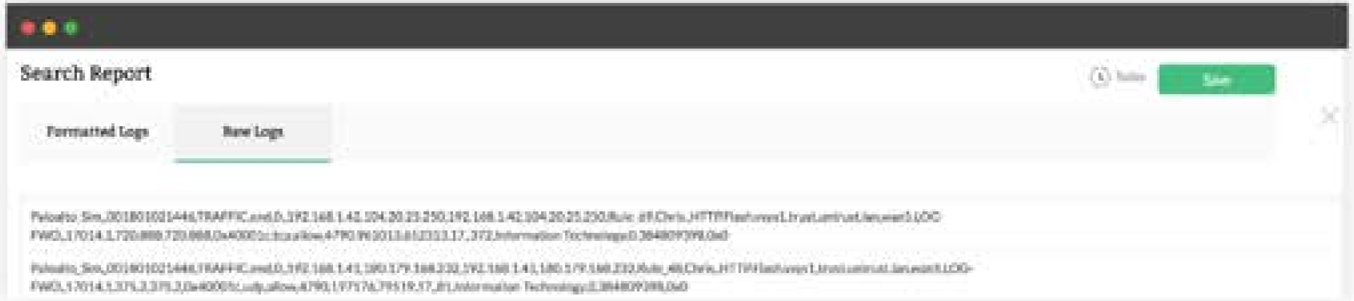
☑ Raw VPN Logs ☑ Raw Virus/Attack Logs ☑ Traffic logs ☑ Raw Device Management Logs
☑ Raw Denied Logs

Criteria: ○ Match all the following ● Match any of the following

Protocol	is	HTTP
User	is	Jon
Attack	is	ARP poisoning

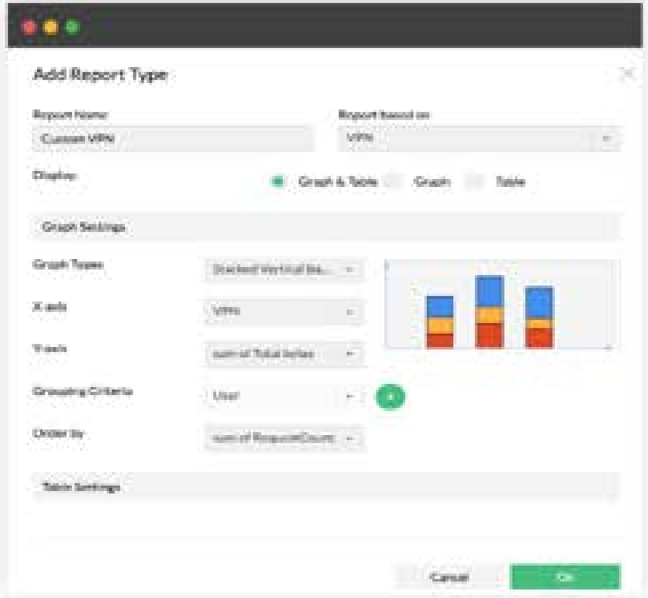


Date/Time	Host	User	Protocol	Destination	Virus/Attack	Severity	Duration	Sent	Receive
11 Jun 2019, 06:46:33	192.168.1.61	Khris	972/tcp	21.12.69.203	null	Unknown	1 Secs	0 KB	0 KB
11 Jun 2019, 06:46:33	192.168.1.50	John	ftp	12.183.124.41	null	Unknown	3 Mins 2 Secs	0 KB	4.68 KB
11 Jun 2019, 06:46:33	192.168.1.49	Patrick	mailbox-im	69.63.178.12	null	Unknown	16 Mins 3 Secs	0 KB	4.68 KB



```
Paloalto_Sim,001801021446,TRAFFIC,end,0,192.168.1.42,104.20.25.250,192.168.1.42,104.20.25.250,Rule_69,Chris,HTTPFlash,vsys1,trust,untrust,lanwan1,LOG-
FWD,17014,1,720,888,720,888,0x4000,tcp,allow,4790,9610,13,612313,17,,372,Information Technology,0,384809398,0x0

Paloalto_Sim,001801021446,TRAFFIC,end,0,192.168.1.43,180.179.168.232,192.168.1.43,180.179.168.232,Rule_48,Chris,HTTPFlash,vsys1,trust,untrust,lanwan1,LOG-
FWD,17014,1,375,2,375,2,0x4000,tcp,udp,allow,4790,1,97176,79519,17,,81,Information Technology,0,384809398,0x0
```



Report Name: Custom VPN

Report based on: VPN

Display: ● Graph & Table ○ Graph ○ Table

Graph Types: Stacked Vertical Ba...

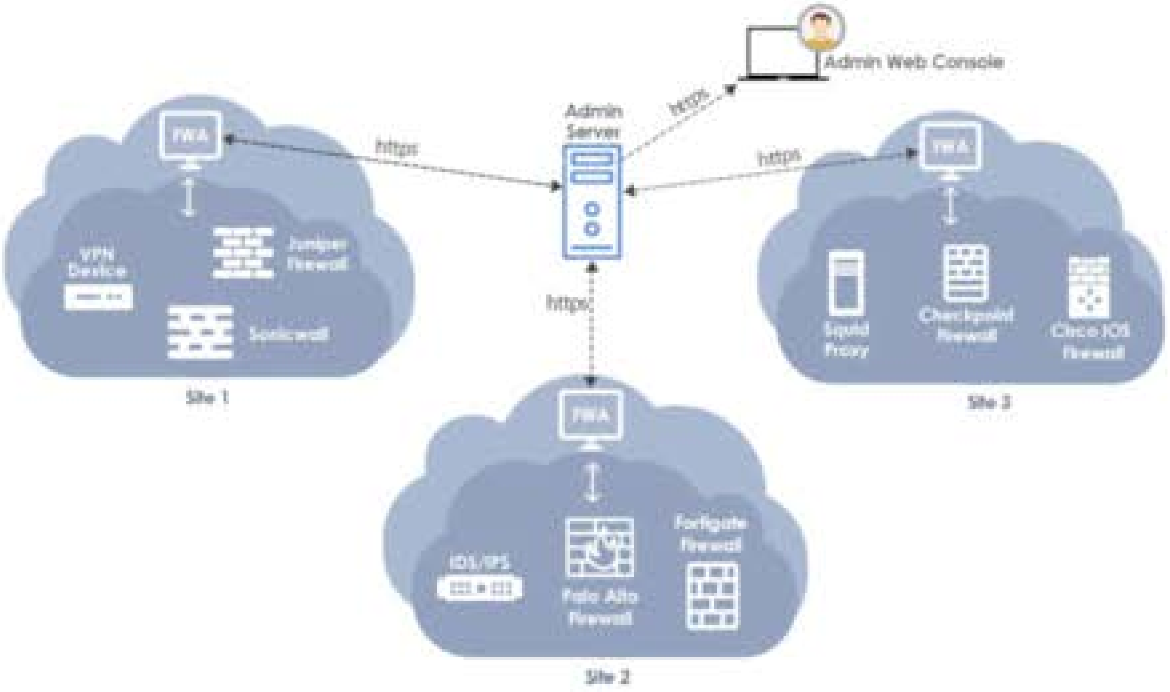
X-axis: VPN

Y-axis: sum of Total bytes

Grouping Criteria: User

Order by: sum of RequestCount

Benefits of using Firewall Analyzer



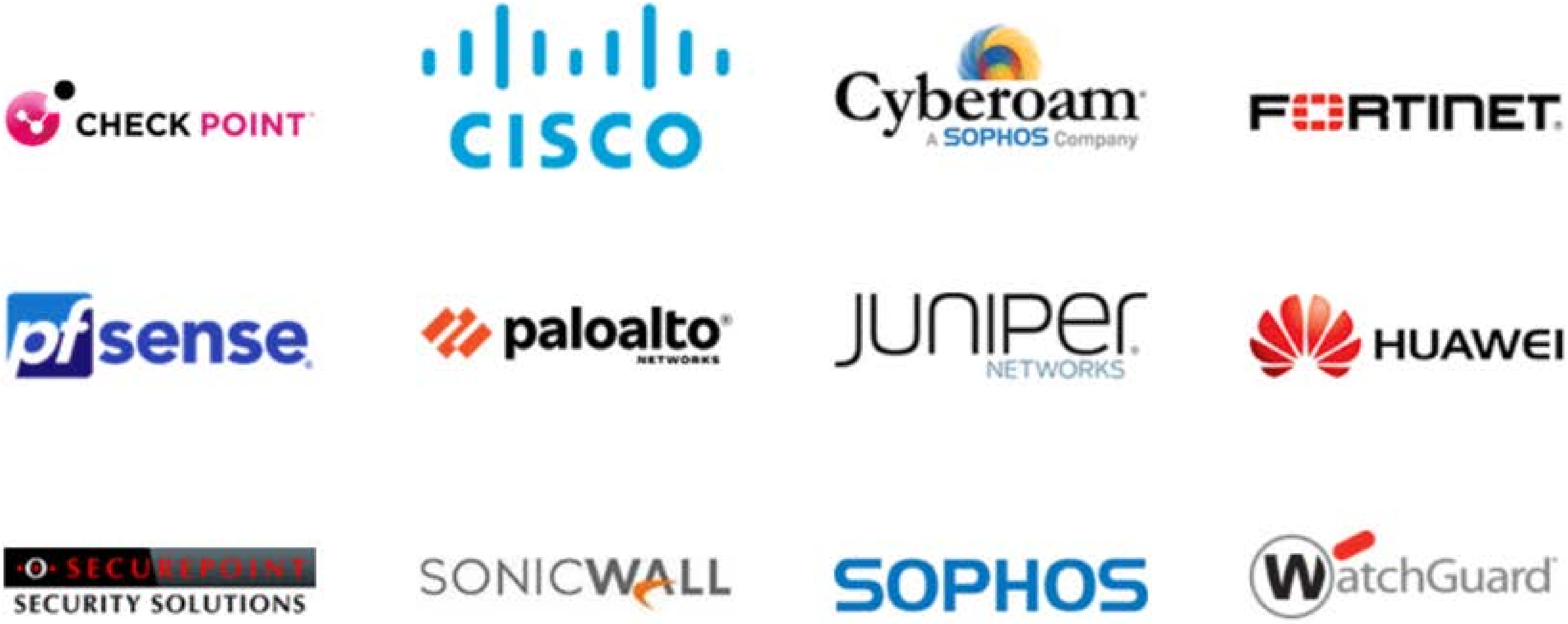
Enterprise monitoring

Monitor geographically distributed firewalls from a centralized location.

Scale smoothly upto 1200 security devices.

Multi firewall support

Supports more than 50 firewall vendors and 200 devices



Affordable Pricing

Annual subscription:

- Single firewall Monitoring starts @ $395.
- 20 device pack (Enterprise edition) starts @ $8,395.

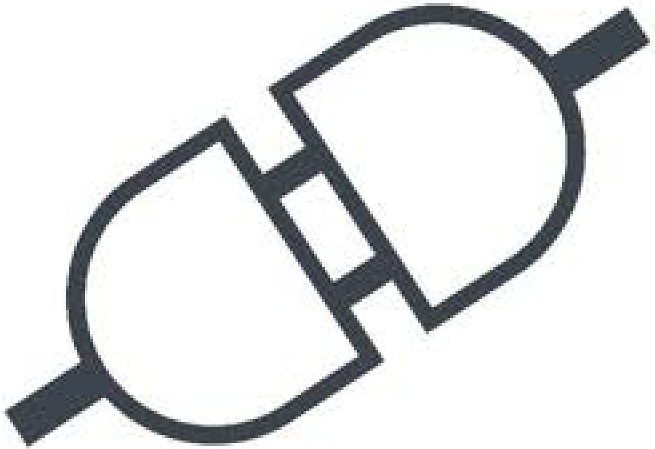
24 * 5 Technical Support

24x5 technical support for customers to gain maximum use of the product!

Integrate seamlessly with your complete network infrastructure

Tight Integration

- **OpManager:** Network and server monitoring
- **NetFlow Analyzer:**Bandwidth monitoring
- **Network Configuration Manager:** Network configuration and compliance management
- **OpUtils:** IP address and switch port management



What makes us standout?

Multi firewalls supported

Real time security alerts

Out-of-the-box reports

Highly scalable

Economical

24*5 technical support

Minimum System Requirements

Intel Xeon Quad Core 3.5 GHz

8 GB RAM

90 GB/day for 500 logs/second

PostgreSQL/MSSQL

Windows/Linux

The disk space and RAM size requirements depend on the number of devices being analyzed and the number of devices sending log information to Firewall Analyzer.

Refer: https://www.manageengine.com/products/firewall/system-requirements.html

THANK YOU

Have a better firewall management experience!

Contact:
For technical queries: fwanalyzer-support@manageengine.com
For pricing and more: sales@manageengine.com
To know more, visit www.fwanalyzer.com