

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



Change management



Compliance reports



Security audit



Log management

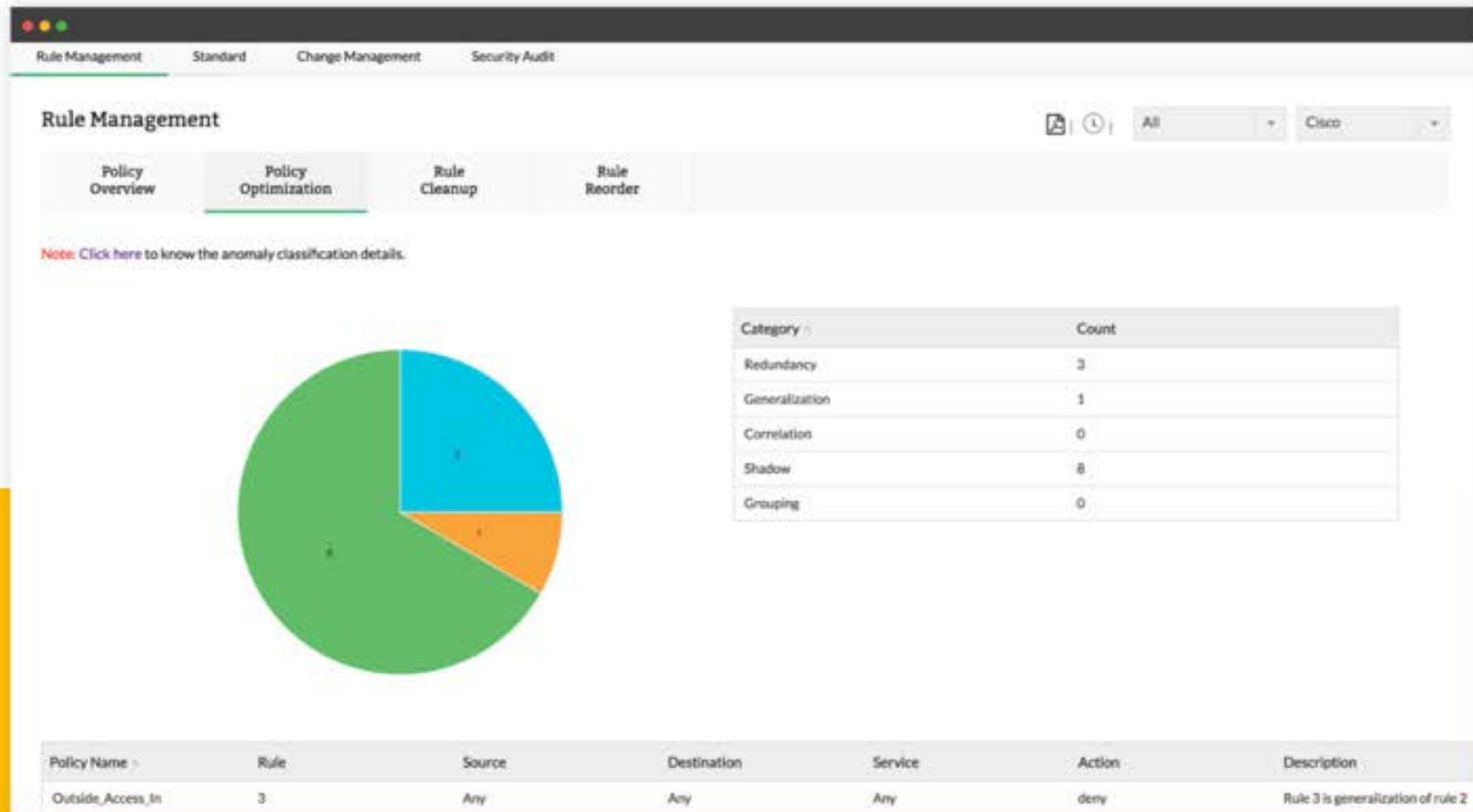


Alarm management

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



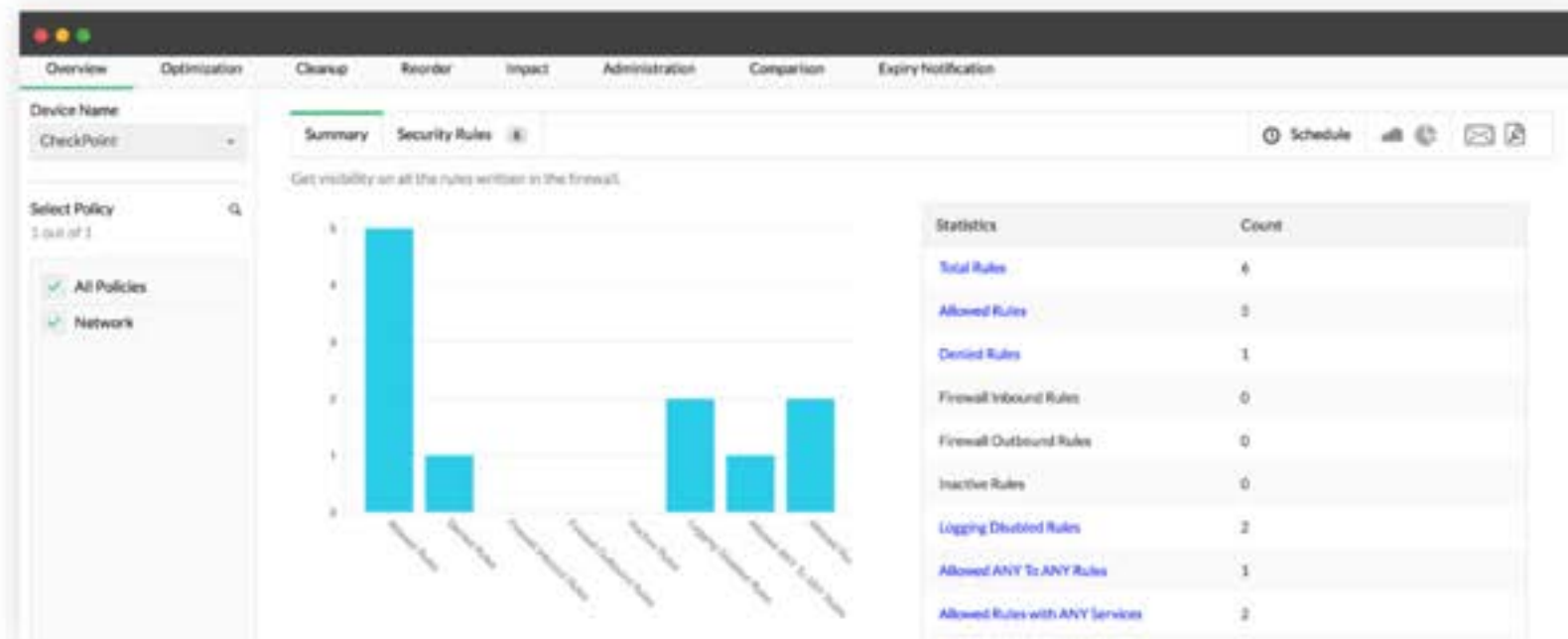
The Importance of rule management

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 a proposed new rule is going to impact the existing rule set negatively.
- Identify unused rules and clear them on a regular basis.

Policy Overview

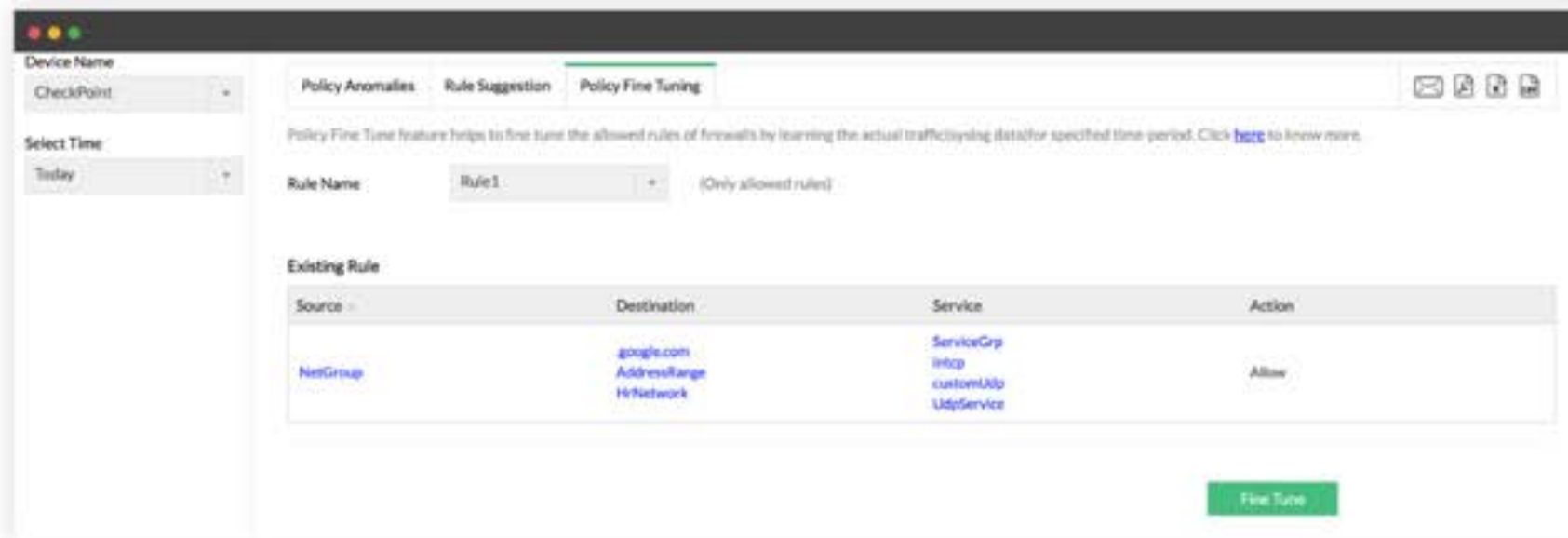


Device Name: Fortinet1

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



- 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

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 17:44:00

Rule Number/ID	Rule Description	Actions
allow Rule	Source=Any Destination=Any Service=Any Action=perm2Source=Any Destination=Any Service=Any Action=perm2	
Clear-cache	Source=Any Destination=Any Service=Any Action=clear	
Ext Rule	Source=AddressRange/1/Network Destination=Any Service=Spine/CL/Static/CI Action=perm2	
Internal to dmz	Source=InternalNetwork Destination=DmzNetwork Service=Any Action=perm2	
Rule1	Source=NetGroup Destination=groups.com/AddressRange/1/Network Service=ServiceGroup/Static/custom/https/Service Action=perm2	
wireless to external	Source=Wireless Destination=InternalNetwork Service=ServiceGroup/Static/Port/Static/Service Action=perm2	

Helps you identify the unassigned interfaces in your network.

Interface Name	IP Address	Type	Mode	Services allowed	Vlan	ADP Forward
InternalInterface	192.168.141.90/255.255.0					
eth0	192.168.140.90/255.255.0					

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

Object name	Object Details	Type
AdminNet	178.90.2.11	Network
CSAddrRange	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

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	31	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

The screenshot shows a web interface with a top navigation bar containing tabs: Overview, Optimization, Cleanup, Reorder, Impact (selected), Administration, Comparison, and Expiry Notification. On the left, a 'Device Name' dropdown is set to 'CiscoASA'. The main area is titled 'Rule Impact' and includes a green 'Impact Analysis' button. A note states: '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.' Below the note is a table listing existing rules.

Policy Name	Reports	Created on	Export	Actions
test	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		

- 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.

The screenshot shows two sections. The first is '1. Anomaly Details :', which includes a sub-section 'Check the proposed new rule against existing rule base for anomalies :'. Below this is a table with two rows of anomalies.

Rule	Source	Destination	Service/Application	Action	Anomaly Type	Description
101	any	223.242.246.134/255.255.255.0	HTTP	accept	Redundancy	Rule 101 is redundant because of Rule 18
18	Any	Any	Any	deny	Redundancy	Rule 101 is redundant because of Rule 18

The second section is '2. Rule Reorder Suggestions :', which includes a sub-section 'On analyzing the proposed new rule for rule complexity and anomaly, suggesting the following rule order.' Below this is a table with one row of suggestions.

Rule	Position (From - To)	Perf. Improvement
101	24 - 10	57%

The screenshot shows a 'Generate Rule Pre-Impact Report' dialog box. It contains several input fields and options for configuring the report generation. The 'Rule Name' field is set to '101'. The 'Position' is set to '24'. The 'Source' and 'Destination' are both set to 'Any'. The 'IP Address' field is set to '223.242.246.134'. The 'Anomaly Destination' is set to '255.255.255.0'. The 'Search' field is set to 'HTTP'. The 'Service' field is set to 'HTTP'. The 'Source Location' is set to 'Any'. The 'Search Location' is set to 'any'.

Rule Administration

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	Edit Delete
17	horie-zsh	pdbuqho.co.jp	wan1	internal	HTTP	Edit Delete
8	sakura	ELA-syslog	wan1	internal	SYSLOG	Edit Delete
2	Any	bangalore-1723 bangalore-GRE	wan1	internal	Any	Edit Delete
4	hyderabad	Any	internal	wan1	FTP_GET FTP_PUT RDP	Edit Delete

- 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.

Name	Type	Status	Mode	Operation	Created Time	FW User	Command	Action
hgggggg	Service Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit
sdhhdh-zsh	Network Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit
sdhhdh-wan1	Service Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit
sdhhdh-zsh	Network Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit
sdhhdh-zsh	Service Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit
sdhhdh-zsh	Service Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit
sdhhdh-zsh	Service Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit
sdhhdh-zsh	Service Object	Pending	add	add	2024-12-24 17:24:21	admin	View Command	Edit

Name	Type	Operation	Change	Time	FW User	Mode	Action
sdhhdh-zsh	Network Object	add	add	2024-12-24 17:24:21	admin	add	Edit
sdhhdh-zsh	Service Object	add	add	2024-12-24 17:24:21	admin	add	Edit
sdhhdh-zsh	Service Object	add	add	2024-12-24 17:24:21	admin	add	Edit
sdhhdh-zsh	Network Object	add	add	2024-12-24 17:24:21	admin	add	Edit
sdhhdh-zsh	Service Object	add	add	2024-12-24 17:24:21	admin	add	Edit
sdhhdh-zsh	Service Object	add	add	2024-12-24 17:24:21	admin	add	Edit
sdhhdh-zsh	Service Object	add	add	2024-12-24 17:24:21	admin	add	Edit
sdhhdh-zsh	Service Object	add	add	2024-12-24 17:24:21	admin	add	Edit

Rule Comparison

The screenshot shows the 'Comparison' tab in the FortiGate management interface. At the top, there are navigation tabs: Overview, Optimization, Cleanup, Reorder, Impact, Administration, Comparison (selected), and Expiry Notification. Below the tabs is a 'Compare Policies' section. A blue information box states: 'Devices for which device rule are configured will only be shown here. Click here to configure Device Rule.' There are three radio buttons for comparison criteria: 'Between configuration files', 'Configuration file with Latest Running Config', and 'Between Running Config Versions' (which is selected). A 'Device Name' dropdown menu is set to 'Fortigate1'. Below that, there are two dropdown menus for 'File 1 - Running Config Version' (set to '4') and 'File 2 - Running Config Version' (set to '117'). A green 'Compare' button is located at the bottom left of the form.

The screenshot shows the results of the rule comparison for 'FortiGate'. The interface includes a header with status indicators: 'Added - (1)', 'Modified - (1)', 'Deleted - (1)', and a 'Diff Only' button. The table compares two configuration files: 'Config_forti_rulecom1.txt' and 'Config_1.txt'. The table has columns for 'Policy Name', 'Rule Name', and 'Compare'. The 'Compare' column contains icons representing the status of each rule: a red icon for added rules, a blue icon for modified rules, and a green icon for deleted rules.

Policy Name	Rule Name	Compare	Policy Name	Rule Name
2	36	Added	-	-
4	45	Modified	-	45
5	-	Deleted	-	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

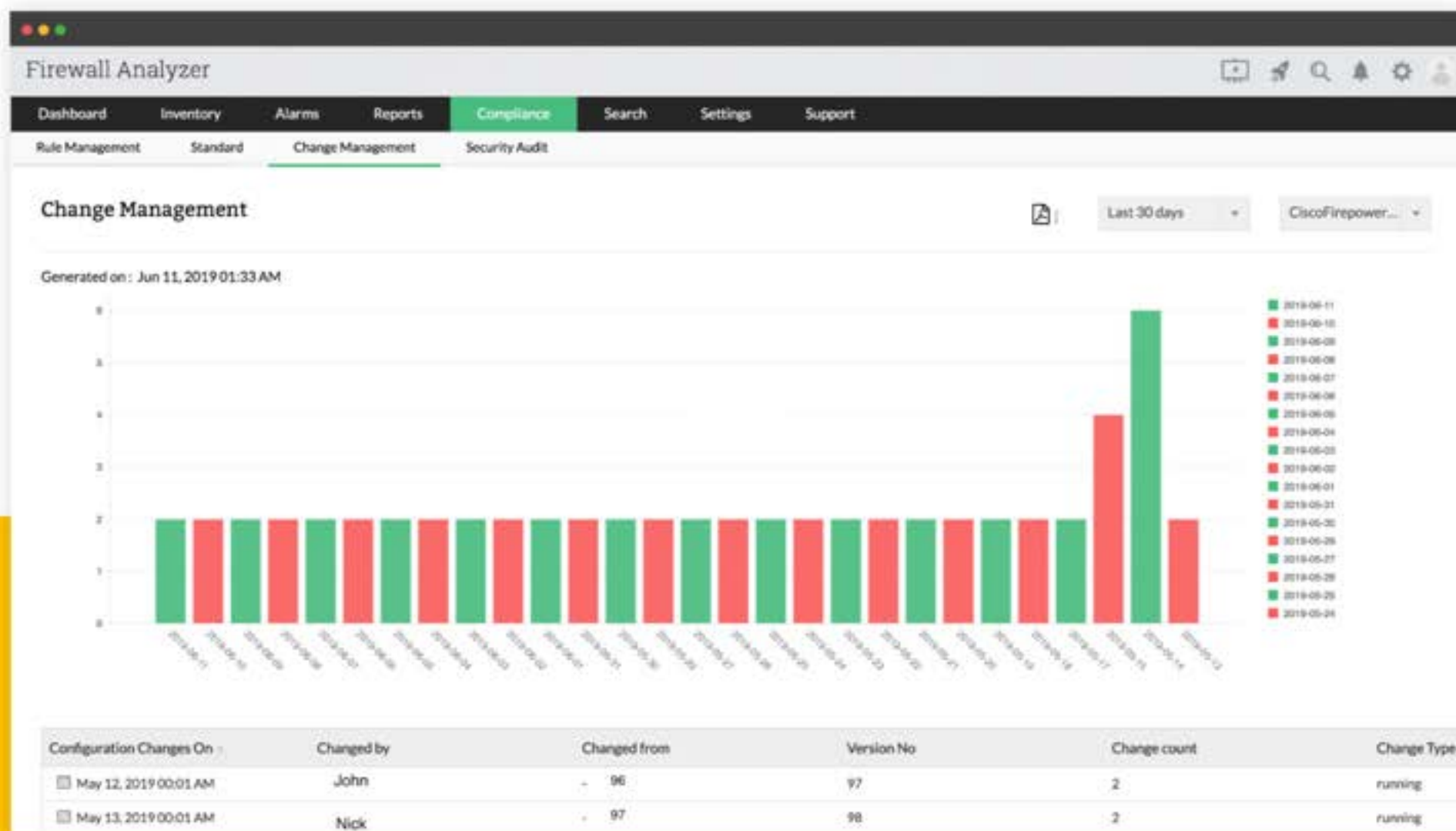
Rule Number/ID	Schedule Name	Schedule Type	Days of week	Time	Start Time	End Time
ruleexp3	non-recurring	onetime	2020/12/29 09:00-2020/12/31 23:45 2021/01/01 00:00-2021/01/02 23:45			
ruleexp2	weeklyschedule	recurring	sunday 09:00-12:00 monday 09:00-18:00			
ruleexp1	dailyschedule	recurring	daily 00:00-13:45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



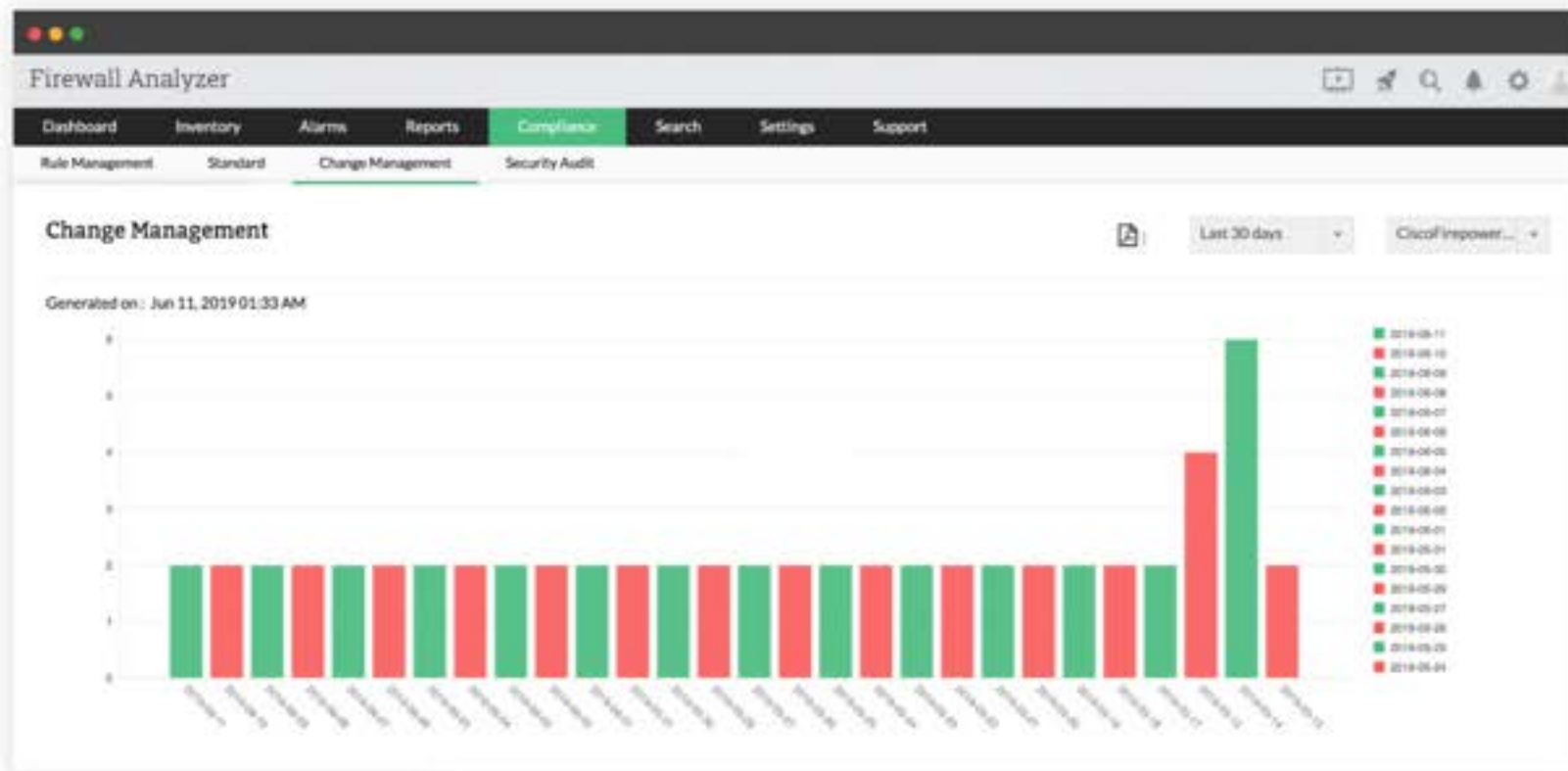
Significance of Change Management

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



- 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	3	running

BurbankSFR Added - (0) Modified - (2) Deleted - (0) Diff Only All Lines

```
11 enable password 8Ry2Yjyt7RRXU24 encrypted enable password 8Ry2Yjyt7RRXU24
12 enable https false
```


Configuration Comparison Using Diff-View

The screenshot displays a configuration comparison tool for Fortigate1. The interface is split into LHS (Left Hand Side) and RHS (Right Hand Side) configuration views. The LHS configuration type is 'Running' and the RHS configuration type is also 'Running'. The diff view shows a side-by-side comparison of configuration lines, with changes highlighted in color: green for added lines, blue for modified lines, and red for deleted lines. The diff view shows 10 added lines, 16 modified lines, and 10 deleted lines. The 'Diff View' button is highlighted in green.

Line	LHS Configuration	RHS Configuration
5	config system global	config system global
6	set access-banner disable	set access-banner disable
7	set admin-httpd-pki-required disable	set admin-httpd-pki-required disable
8	set admin-lockout-duration 80	set admin-lockout-duration 82
9	set admin-lockout-threshold 3	set admin-lockout-threshold 4
10	set admin-maintenance enable	set admin-maintenance enable
11	set admin-port 80	set admin-port 8080
12	set admin-scp enable	set admin-scp enable
13	set admin-server-cert "self-sign"	set admin-server-cert "self-sign"
14	set admin-sport 443	set admin-sport 443
15	set admin-ssh-port 22	set admin-ssh-port 22
16	set admin-ssh-v1 disable	set admin-ssh-v1 disable
17	set admin-https-port 22	set admin-https-port 22
18	set admin-https 3	set admin-https 3
19	set anti-replay strict	set anti-replay strict
20	set auth-cert "self-sign"	set auth-cert "self-sign"
21	set auth-http-port 2000	set auth-http-port 2000
22	set auth-https-port 2000	set auth-https-port 2000
23	set auth-keepalive disable	set auth-keepalive disable
24	set auth-policy-exact-match enable	set auth-policy-exact-match enable
25	set av-fallopem-pass	set av-fallopem-pass
26	set av-fallopem-session disable	set av-fallopem-session disable
27	set batch-credit enable	set batch-credit enable
28	set clog-save automatic	set clog-save automatic
29	set check-protocol-header base	set check-protocol-header base
30	set check-reset-range disable	set check-reset-range disable
31	set cli-vert-msg disable	set cli-vert-msg disable
32	set daily-restart disable	set daily-restart disable
33	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

The screenshot displays a configuration diff tool for FortiGate1. The interface is split into two columns: LHS (Left Hand Side) and RHS (Right Hand Side). The LHS column shows configuration type 'Running' and 'Select Config' set to '1'. The RHS column shows configuration type 'Running' and 'Select Config' set to '2'. The diff view shows 33 lines of configuration. At the top, a summary bar indicates: Added - (4), Modified - (16), Deleted - (10). A green 'Diff Only' button and an 'All Lines' button are also visible. The diff view uses color-coding: green for added lines, red for deleted lines, and blue for modified lines. The following table summarizes the changes shown in the diff view:

Line	Configuration	Change Type
5	config system global	Added
6	set access-banner disable	Added
7	set admin-http-ssl-required disable	Added
8	set admin-lockout-duration 60	Modified
9	set admin-lockout-threshold 2	Modified
10	set admin-maintainer enable	Added
11	set admin-port 90	Modified
12	set admin-ssl enable	Added
13	set admin-ssl-cert "self-sign"	Added
14	set admin-ssl-port 443	Added
15	set admin-ssl-port 22	Added
16	set admin-ssl-v1 disable	Added
17	set admin-ssl-v2-port 23	Modified
18	set admin-timeout 5	Added
19	set anti-reply strict	Added
20	set auth-cert "self-sign"	Added
21	set auth-http-port 1000	Modified
22	set auth-http-port 1000	Modified
23	set auth-keepalive disable	Added
24	set auth-policy-exact-match enable	Added
25	set av-fallop-pass	Added
26	set av-fallop-session disable	Added
27	set batch-conn enable	Added
28	set cfg-save automatic	Added
29	set check-protocol-header lower	Added
30	set check-reset-range disable	Added
31	set cli-ssl-req disable	Added
32	set daily-restart disable	Added
33	set detection-summary enable	Added

- 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

The screenshot displays the 'Firewall Analyzer' web interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Alarms', 'Reports', 'Compliance' (highlighted), 'Search', 'Settings', and 'Support'. Below this, a secondary menu shows 'Rule Management', 'Standard' (highlighted), 'Change Management', and 'Security Audit'. The main content area is titled 'Compliance Standards' and features a dropdown menu set to 'Zoho-CP-R80.10' with buttons for 'Update Data', 'Edit Setting', and 'Edit Widget'.

Four compliance standard cards are shown:

- SANS on 2019-02-18 06:26**: 50% Compliant. Recommendation: Your Organization is under threat. Failed Count 3: 4 Enable Logging, 11 Insecure Services, 15 Block ICMP Unwanted Traffic.
- NIST on 2019-01-30 04:49**: 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.
- PCI DSS on 2019-02-18 06:26**: 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.
- ISO on 2019-01-30 04:49**: 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.

Each card includes a progress indicator, a note that some requirements need to be manually verified, and a 'more...' link.

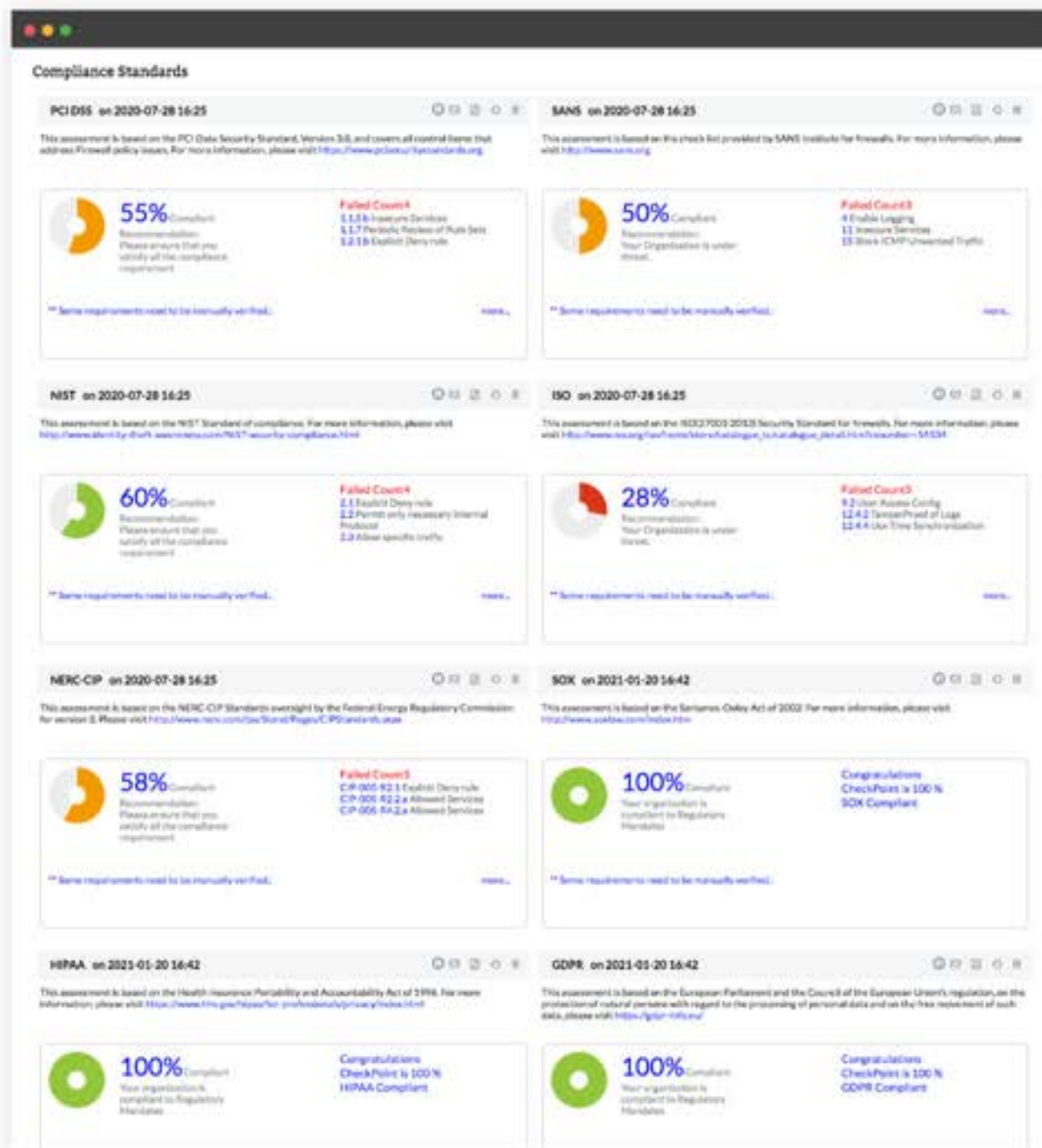
Stay compliant with out-of-the-box compliance reports

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



- 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 21:14:12

Security Audit Summary

ManageEngine performed a security audit of the FortiGate Fortigate1 device on Mon Feb 27 21:14:12 (ST 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 unencrypted and shared. ManageEngine recommends that all unencrypted services should be replaced with encrypted secure alternatives.

ManageEngine analyzed 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. Security Audit

- 2.1. Introduction
- 2.2. Clear-Text Telnet Service Enabled
- 2.3. Access Allowed To Clear-Text Protocol Services
- 2.4. Clear-Text HTTP Service Enabled
- 2.5. Access Allowed To Potentially Dangerous Services
- 2.6. Firewall Policy Does Not End with Deny All And Log
- 2.7. A Dictionary-Based SNMP Community String Was Configured
- 2.8. Rule Permits Packets To Any Service
- 2.9. Dictionary-Based SNMP Trap
- 2.10. Clear-Text SNMP In Use
- 2.11. No Post Logon Banner Message
- 2.12. Access Allowed To Potentially Unnecessary Services
- 2.13. Potentially Unused Network Interfaces
- 2.14. Conclusions
- 2.15. Recommendations

3. Security Best Practices

- 3.1. Introduction
- 3.2. Software
- 3.3. Services
- 3.4. Interfaces
- 3.5. Filtering

2.2. Clear-Text Telnet Service Enabled

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.

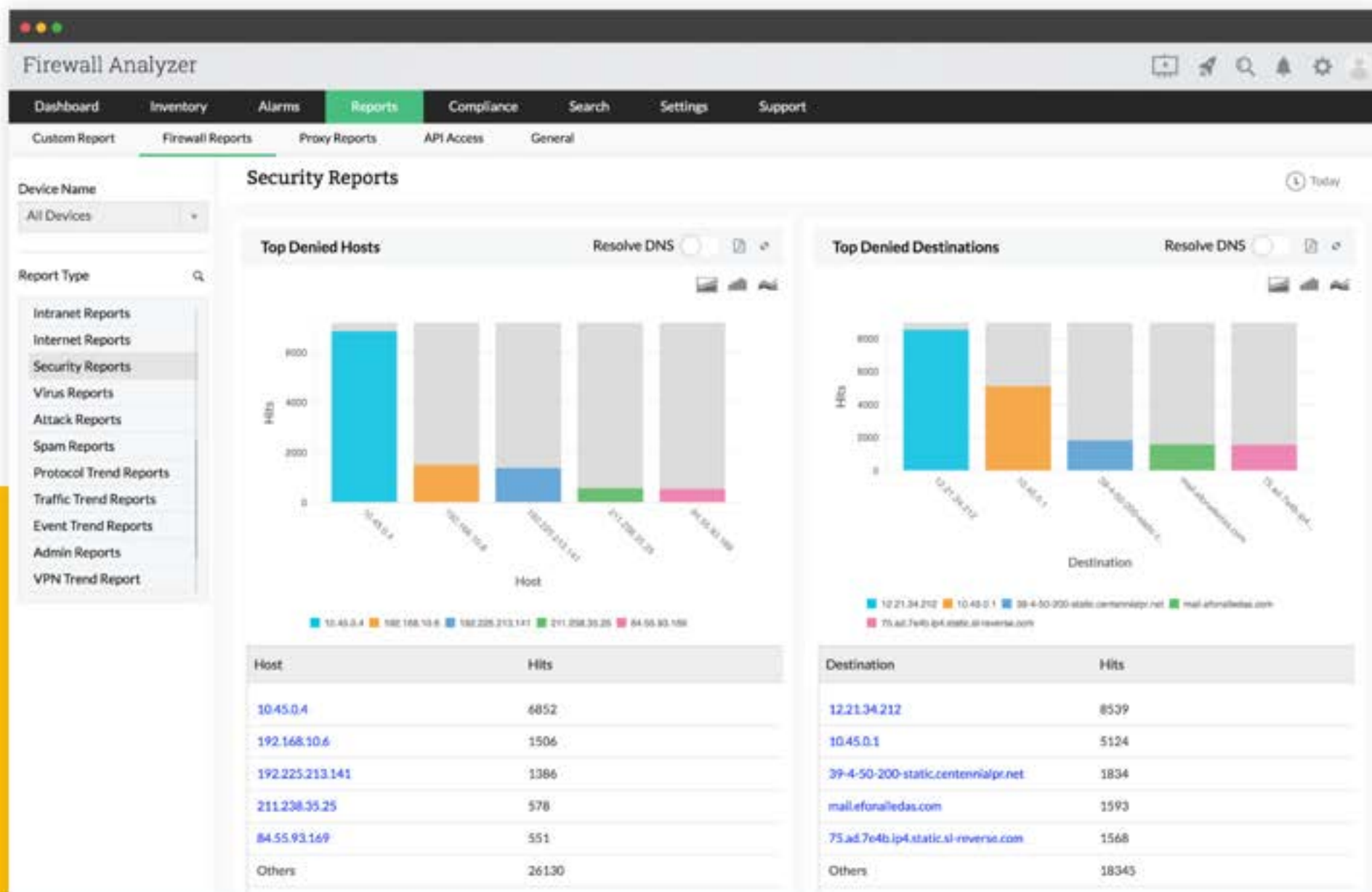
2.2.4. Recommendation

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:

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

Log Management



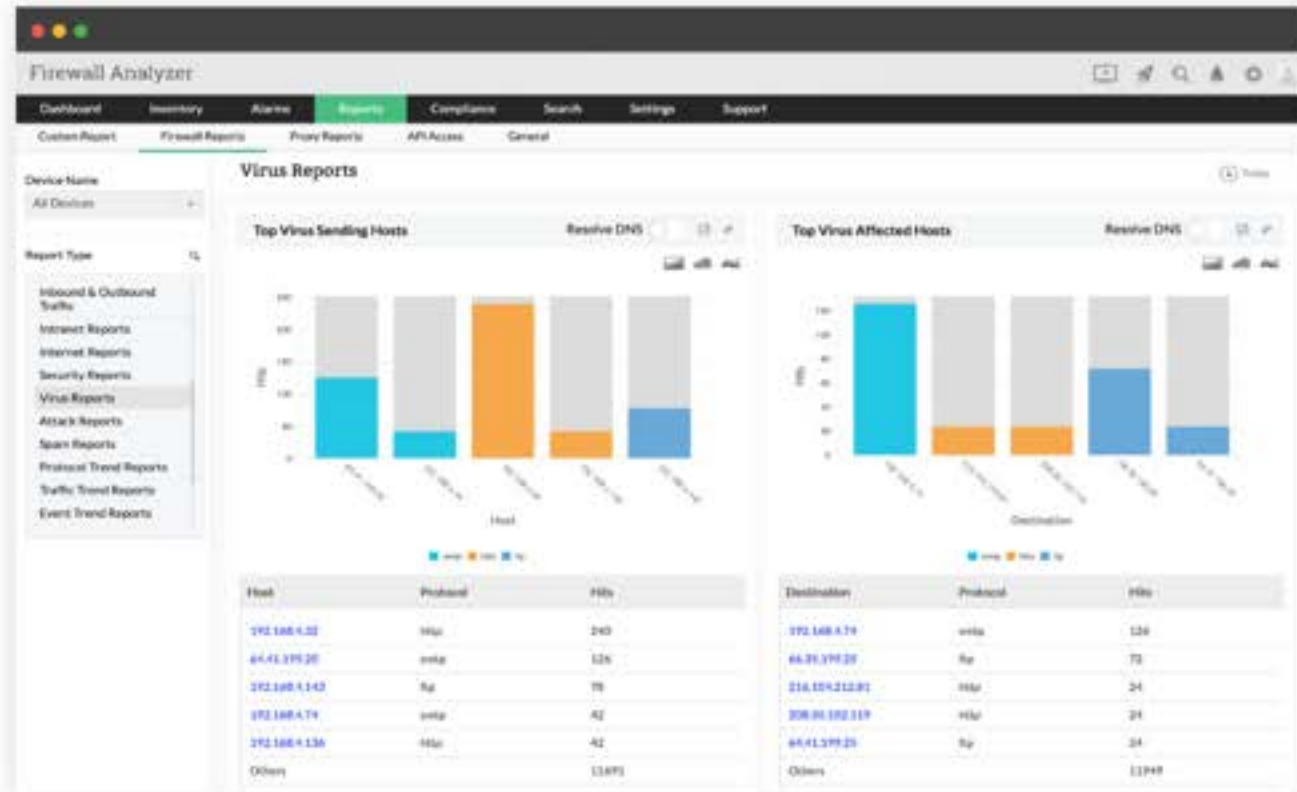
Log Management is critical for network security

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.

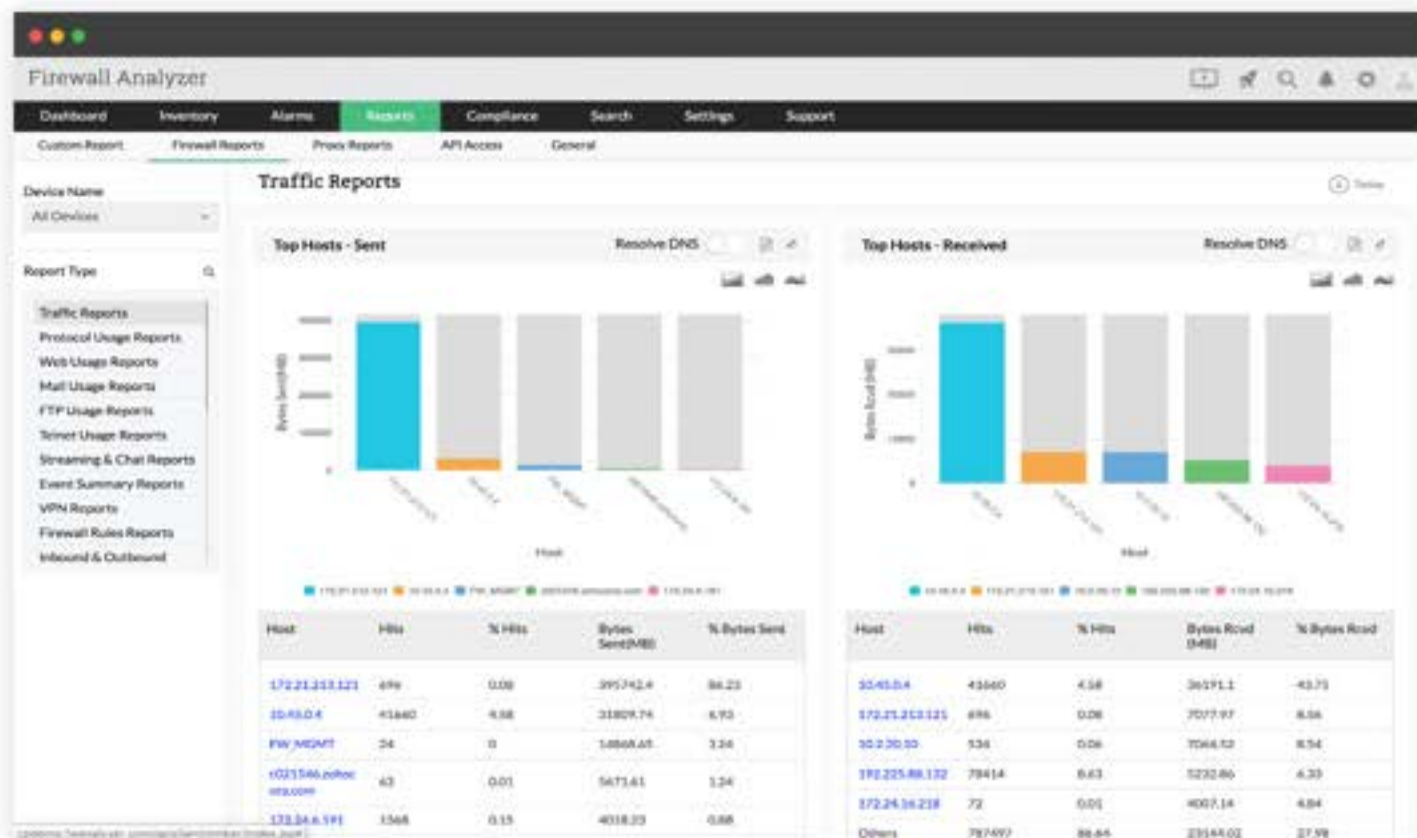
Security Analytics



- 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.

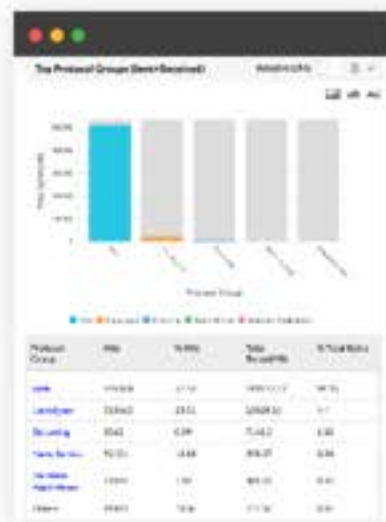


Traffic Analytics

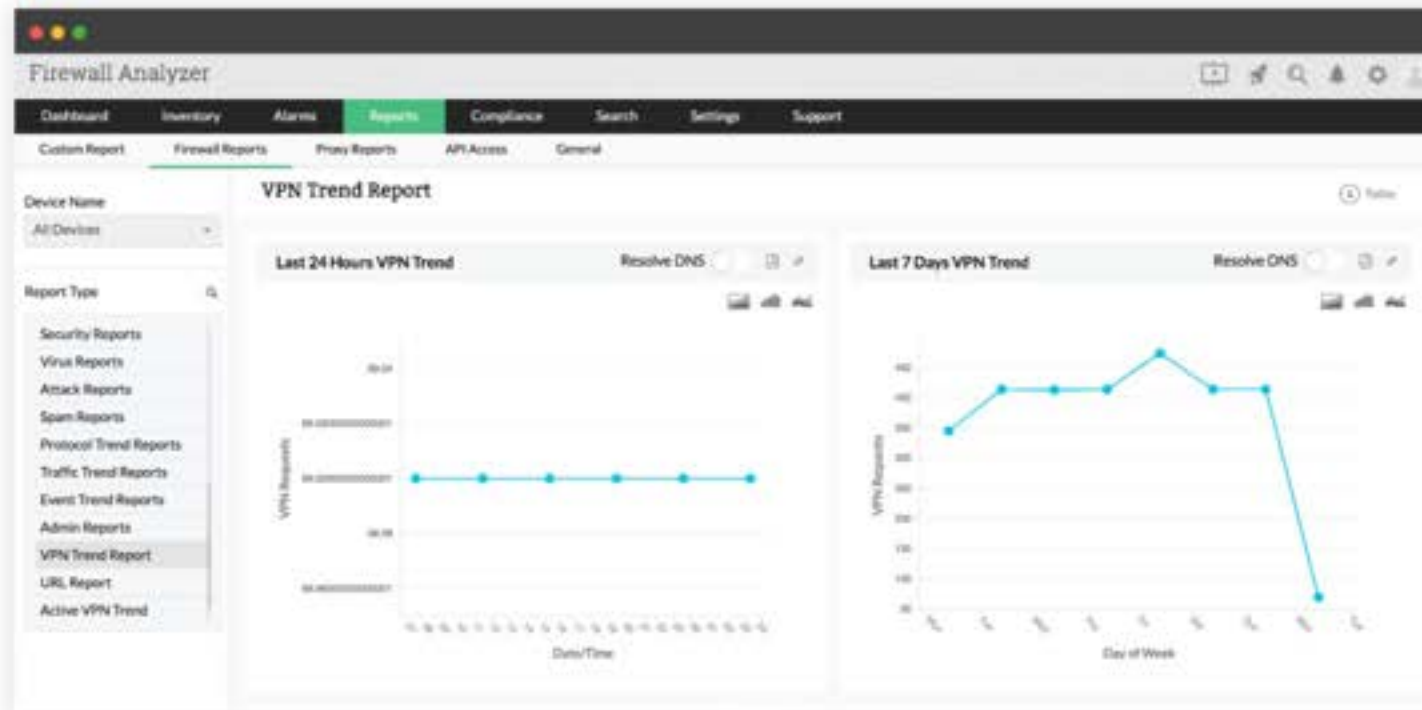


Firewall Analyzer's traffic reports help answering the following questions

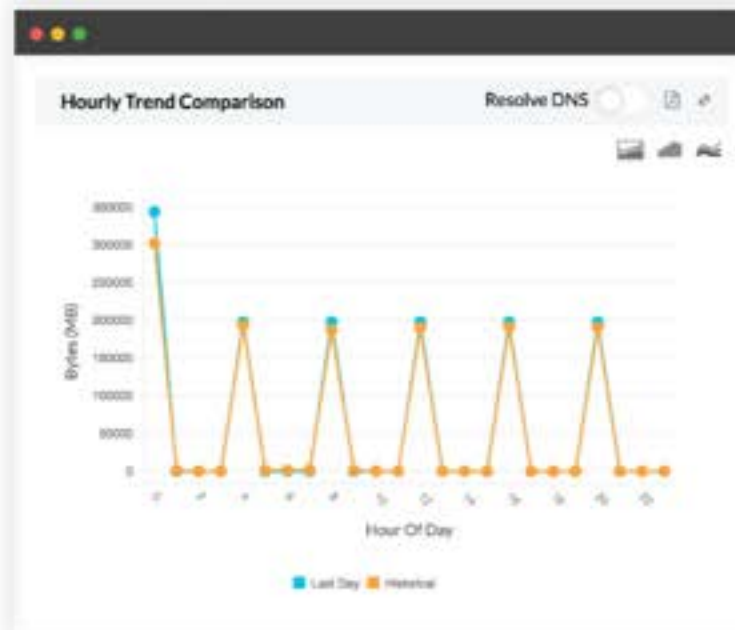
- Who is sending, receiving the traffic?
- Which host is sending, receiving the traffic?
- What is the traffic share of various protocol groups?
- What is the event severity pattern due to the traffic?



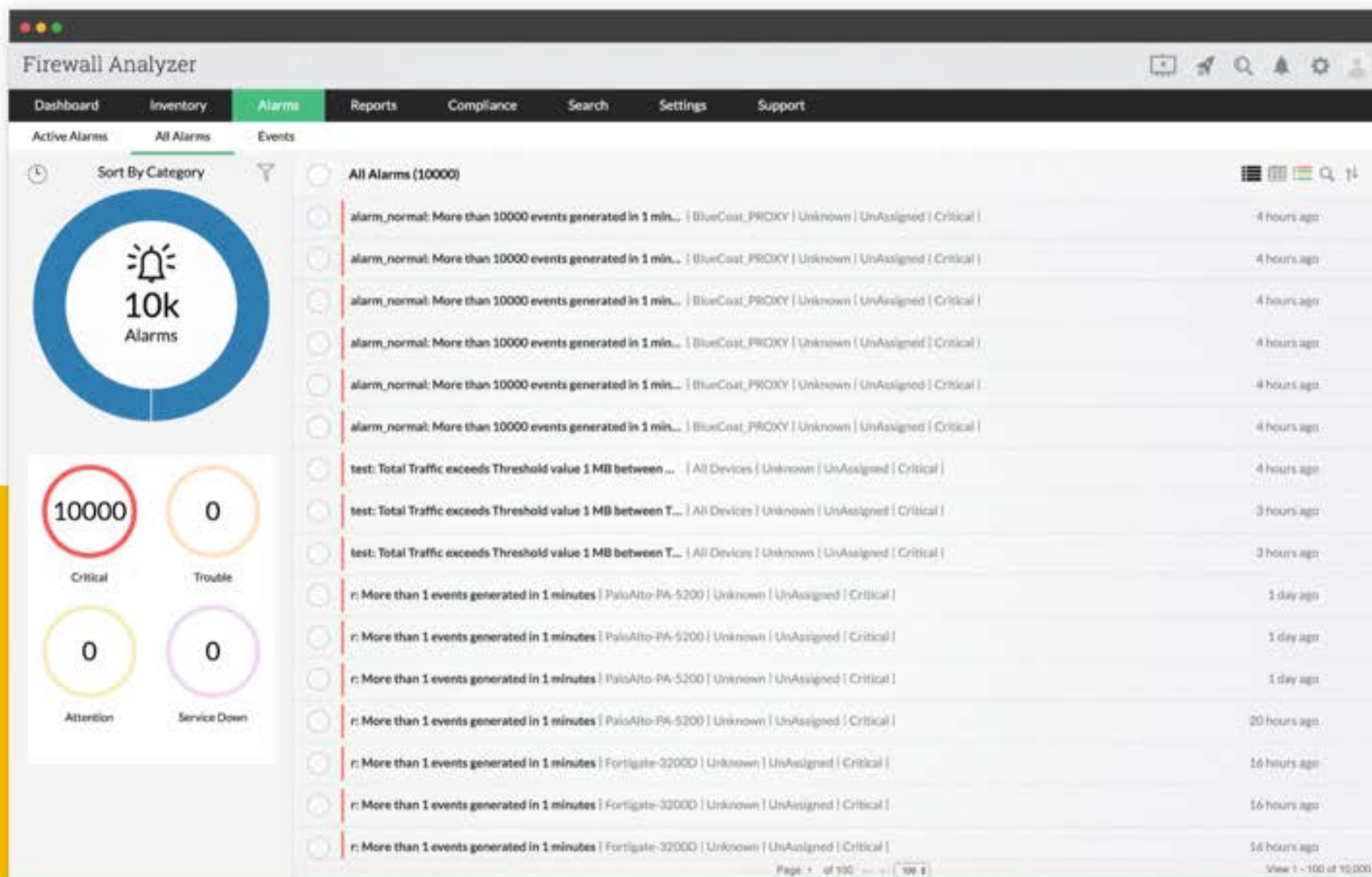
Trend Analysis



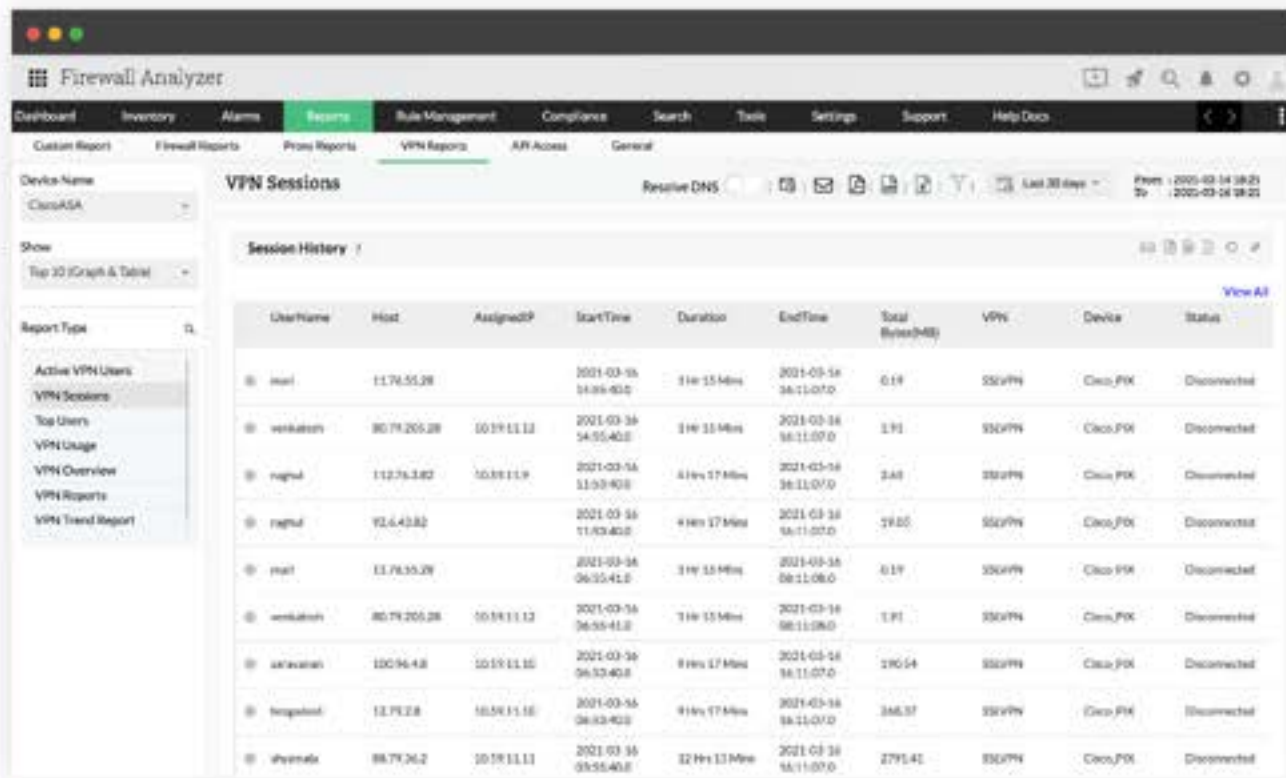
- Determine peak bandwidth usage trend across different protocols and time stamps.
- Troubleshoot links and identify security risks by analysing the event trend report.
- Identify live VPN connections and VPN related security risks using the VPN trend report.



Other significant features



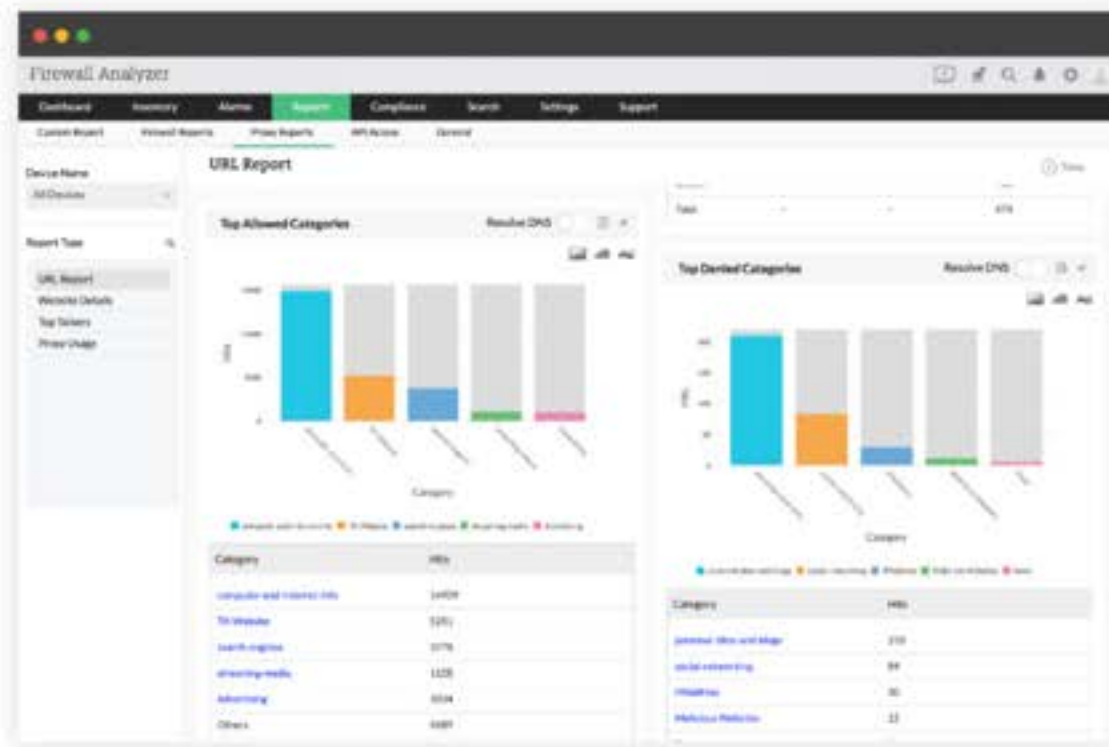
VPN Reports



- 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



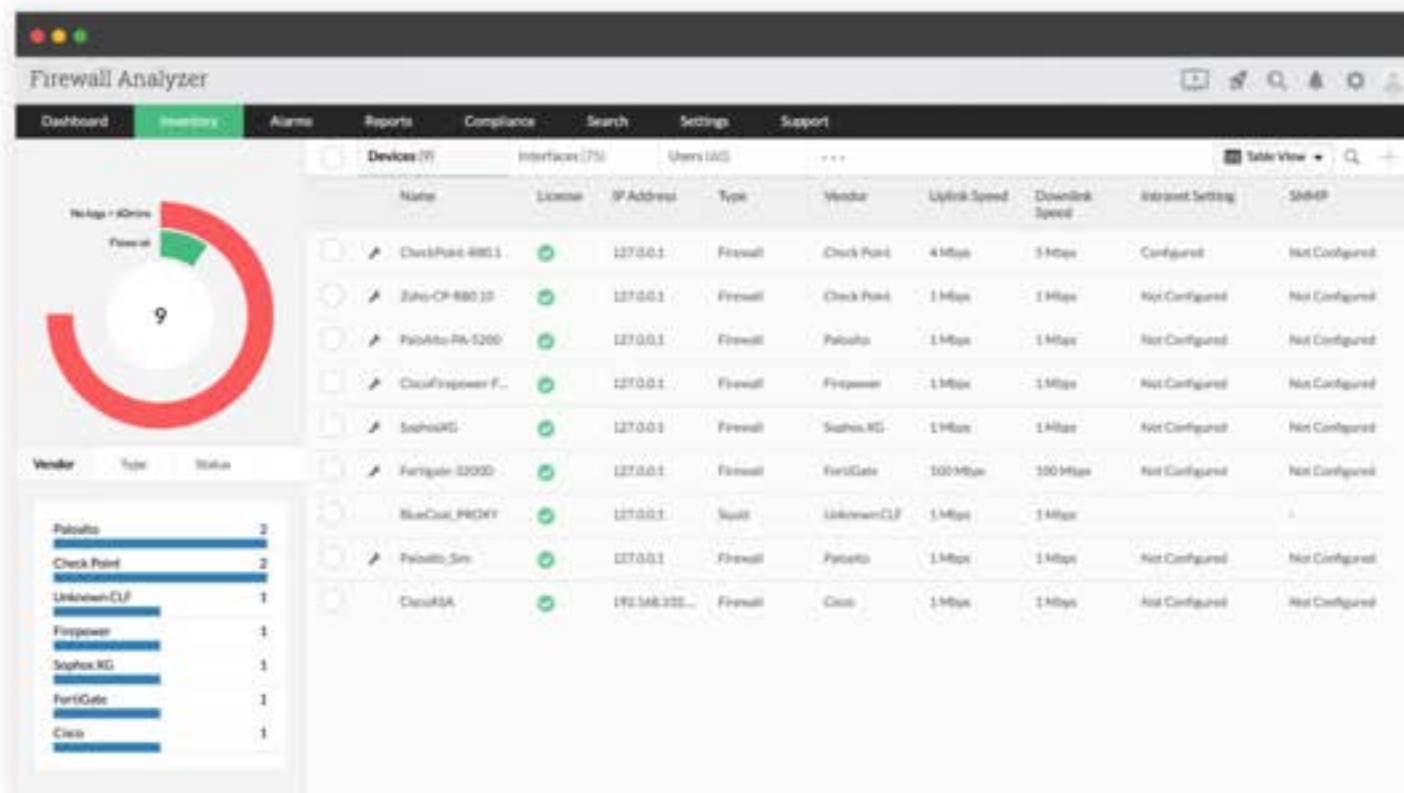
Proxy Report



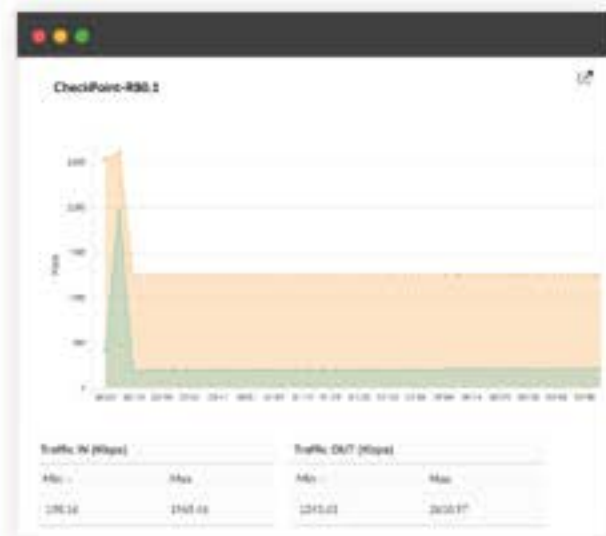
- Collect and archive the proxy server logs, analyzes them, and generate useful corporate internet access information reports.
- Generate proxy usage and proxy virus reports
- Get the list of URLs accessed using the proxy server



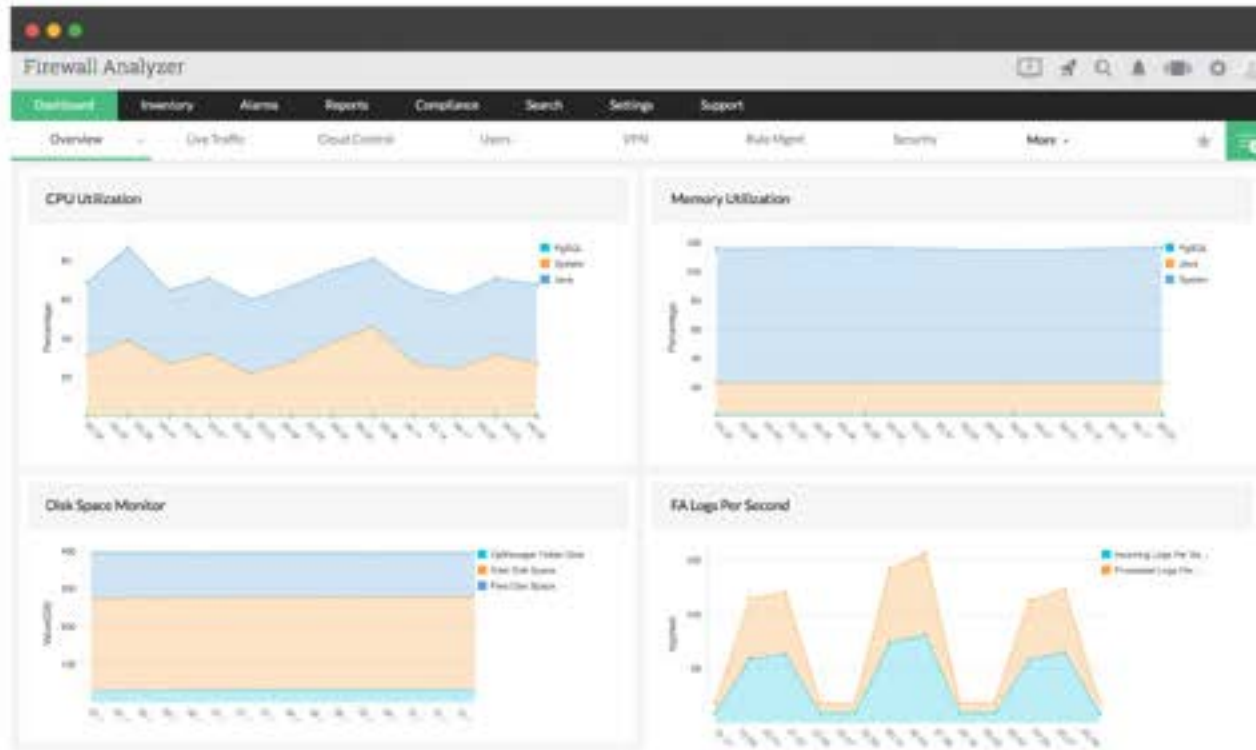
Inventory report



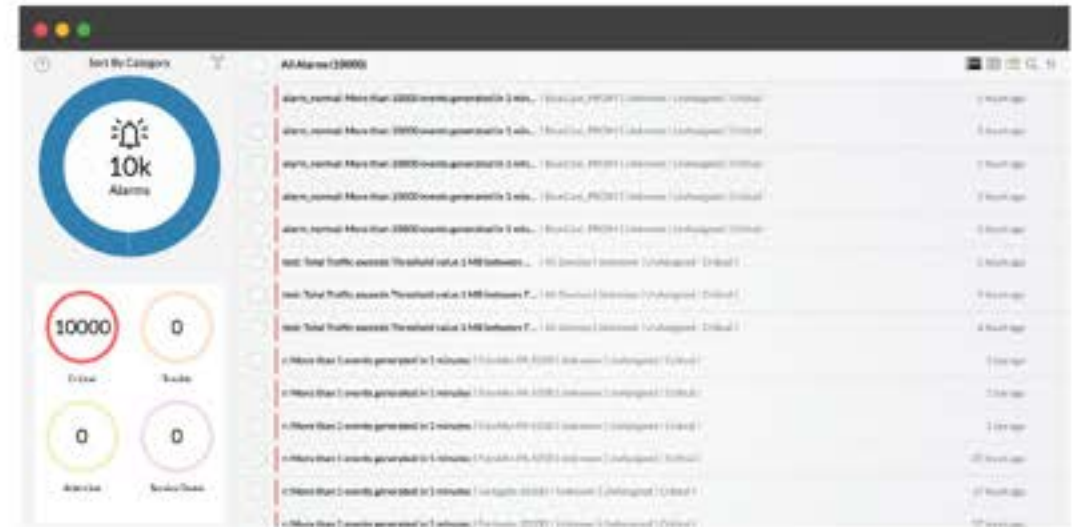
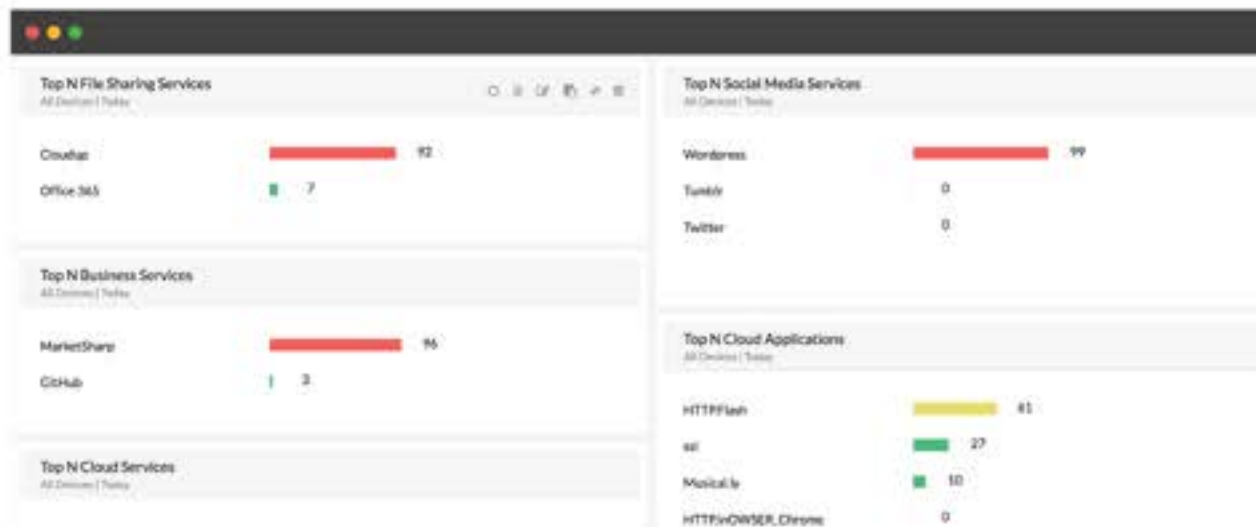
- Get a complete picture of everything that's happening on individual firewalls.
- Gain visibility to interfaces that are under the configured firewall devices.
- Get an overview of all the users that have accessed the internet through individual firewall devices.
- Monitor rules and cloud services accessed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



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 notified directly to your mail or phone.



Forensic Log Analysis & Custom Reports

The screenshot shows the 'Firewall Analyzer' search interface. It includes a navigation bar with 'Dashboard', 'Inventory', 'Alarms', 'Reports', 'Compliance', 'Search', 'Settings', and 'Support'. Below the navigation bar, there are tabs for 'Aggregated Search', 'RAW Search', and 'RAW Settings'. The main area is divided into 'Available Devices' and 'Selected Devices' sections, both with search boxes. A 'Search Type' dropdown is set to 'Raw Firewall Logs'. There are several checkboxes for log types: 'Raw VPN Logs', 'Raw Virus/Attack Logs', 'Traffic logs', 'Raw Device Management Logs', and 'Raw Denied Logs'. Under 'Criteria', there are two radio buttons: 'Match all the following' and 'Match any of the following'. Three criteria are listed: 'Protocol is HTTP', 'User is Jon', and 'Attack is ARP poisoning'. A 'Generate' button is at the bottom.

The screenshot shows the 'Search Report' interface with the 'Raw Logs' tab selected. It displays a table with the following columns: Date/Time, Host, User, Protocol, Destination, Virus/Attack, Severity, Duration, Sent, and Receive. The table contains three rows of log data.

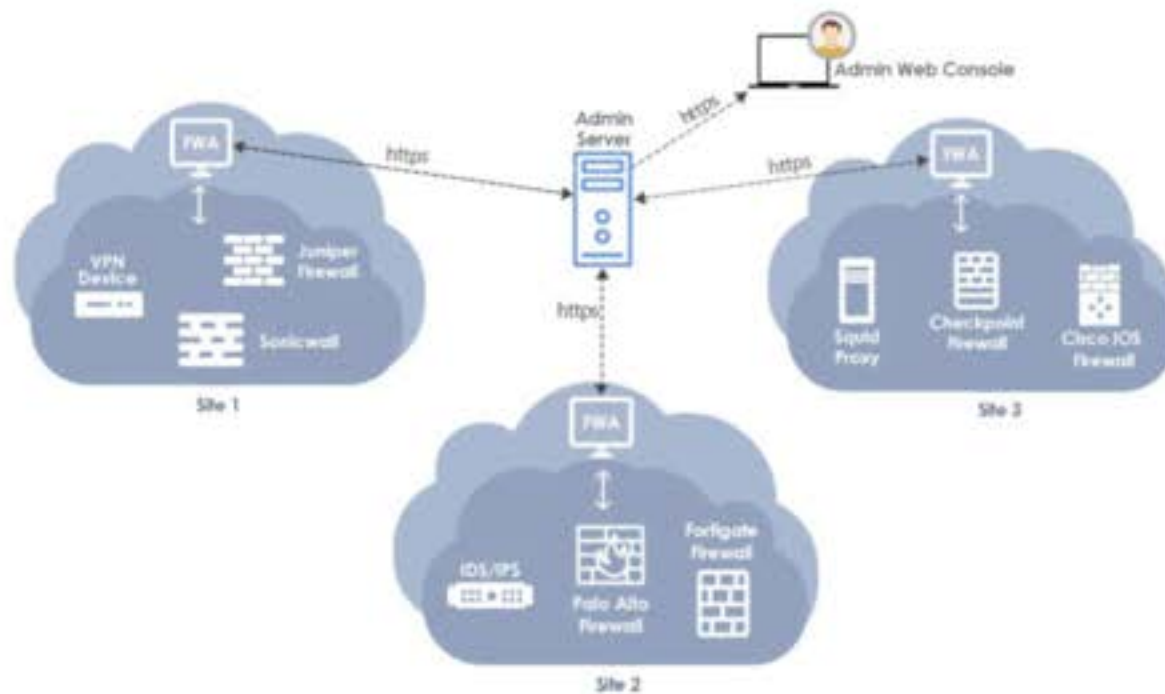
Date/Time	Host	User	Protocol	Destination	Virus/Attack	Severity	Duration	Sent	Receive
11 Jun 2019 06:46:33	192.168.1.31	Krista	HTTP	20.136.9.203	null	Unknown	1 Secs	0 KB	0 KB
11 Jun 2019 06:46:33	192.168.1.30	John	FTP	12.183.124.41	null	Unknown	2Mins 2 Secs	0 KB	4.08 KB
11 Jun 2019 06:46:33	192.168.1.89	Walter	malware	44.43.178.12	null	Unknown	16 Mins 1 Secs	0 KB	4.08 KB

The screenshot shows the 'Search Report' interface with the 'Raw Logs' tab selected. It displays raw log data for a specific entry. The log entry is: 'Paloalto_Sm_0018010214461TRAFFIC:srcD_192.168.1.42,104.20.25.250,192.168.1.42,104.20.25.250,Rule_89,Chris_HTTP,headers:User-Agent:Newsworld,LOG-FWD,17014.1.375.2.375.2,0=40001,udp,allow,4790.197576,79519,17,81,Information Technology@364809298,0x0'.

- 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.

The screenshot shows the 'Add Report Type' dialog box. It includes a 'Report Name' field and a 'Report based on' dropdown menu. There are checkboxes for 'Graph & Table', 'Graph', and 'Table'. The 'Graph Settings' section includes a 'Graph Type' dropdown, 'X-axis' and 'Y-axis' dropdowns, a 'Track' dropdown, and 'Grouping Criteria' and 'Order by' dropdowns. There are 'Cancel' and 'Ok' buttons at the bottom.

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

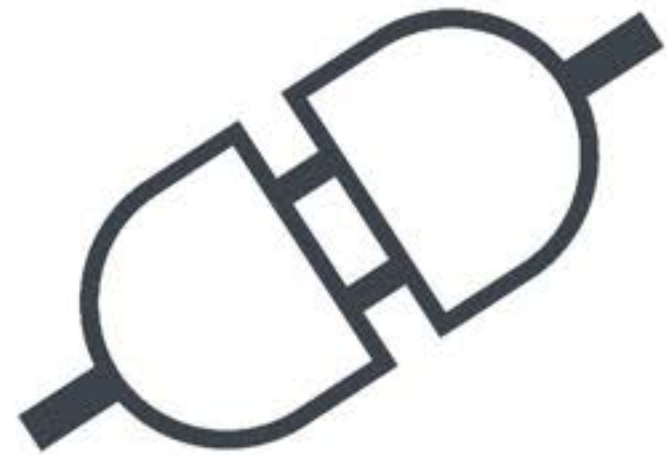
24x5 technical support
for customers to gain
maximum use of the
product!



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



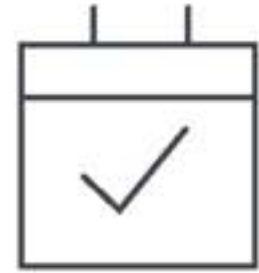
What makes us stand out?



Multi firewalls supported



Real time security alerts



Out-of-the-box reports



Highly scalable

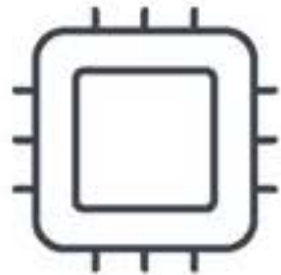


Economical

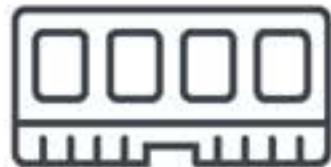


24*5 technical support

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