

Firewall Analyzer v12

Solution de politique, de configuration et d'analyse des journaux du pare-feu.



– Qu'est-ce que c'est?

Firewall Analyzer est un logiciel d'analyse des politiques, de contrôle de la configuration et de création de rapports sur les journaux, destiné aux administrateurs de la sécurité. Il leur permet de suivre les modifications apportées aux politiques, d'optimiser les performances du pare-feu et de maintenir les normes de conformité.

Détectez et prévenez de manière proactive les menaces à la sécurité du réseau. Exploitez au mieux Firewall Analyzer grâce aux fonctionnalités suivantes !



Gestion des règles

Gestion des modifications



Rapports de conformité

Audit de sécurité



Gestion des journaux

Gestion des alarmes



Voici pourquoi vous en avez besoin!

- Rationaliser les politiques de pare-feu, optimiser les règles et améliorer les performances du pare-feu.
- Conserver un enregistrement de toutes les modifications de configuration en automatisant le suivi des modifications.
- Respecter les normes de conformité et identifier les failles de sécurité grâce à des rapports de conformité prêts à l'emploi.
- Identifier et prévenir les menaces à la sécurité du réseau en surveillant les journaux de sécurité et l'utilisation d'Internet par les employés.
- Rechercher sans effort les incidents de sécurité à partir des journaux bruts et effectuer des analyses forensiques pour identifier les menaces.
- Recevoir des notifications sur les incidents de sécurité et de bande passante anormaux directement sur votre messagerie ou votre téléphone.

Rule Management Standard Change Management Security Audit

Rule Management

Policy Overview **Policy Optimization** Rule Cleanup Rule Reorder

Note: [Click here](#) to know the anomaly classification details.

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

Policy Name	Rule	Source	Destination	Service
Outside_Access_In	3	Any	Any	Any

Gestion des règles

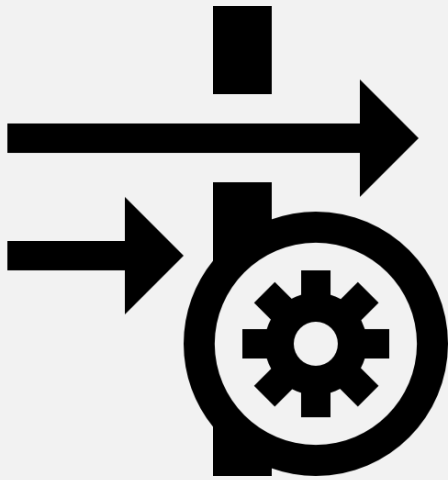
Count

Action Description

0/0 Rule: To prevent actions of rule 2

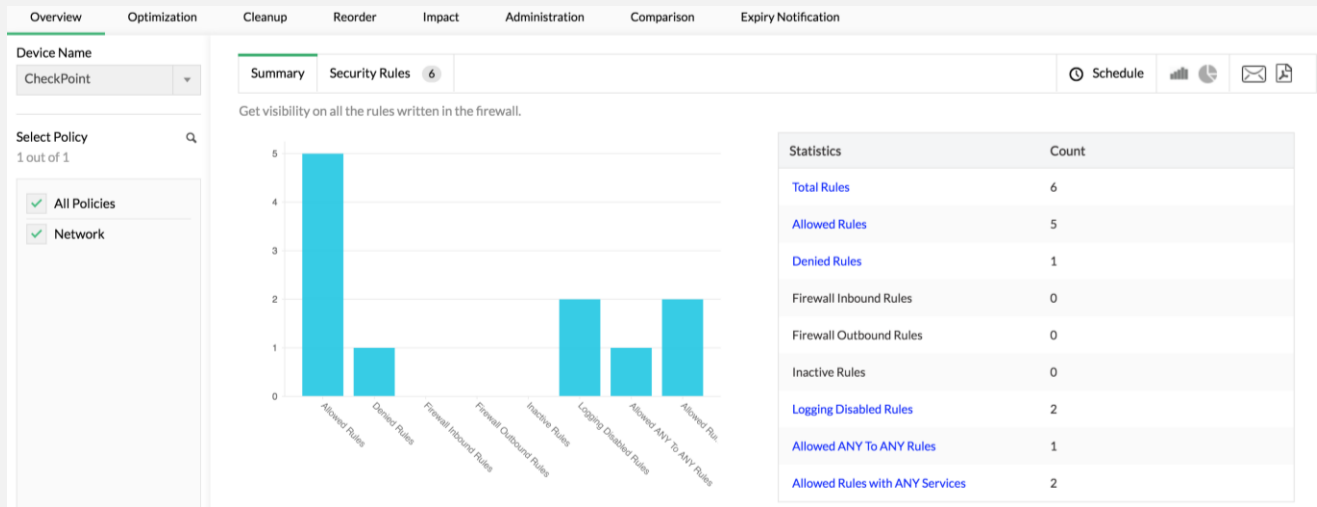
L'importance de la gestion des règles

Les règles et les politiques sont au cœur des performances de tout pare-feu. Si les règles ne sont pas gérées correctement, cela peut rendre votre réseau vulnérable aux attaques.



- Obtenez une visibilité complète de toutes les règles écrites dans votre pare-feu.
- Améliorez les performances du pare-feu en identifiant et en supprimant les anomalies des règles.
- Optimisez les performances des règles en les plaçant dans le bon ordre.
- Déterminez si une nouvelle règle proposée va avoir un impact négatif sur l'ensemble des règles existantes.
- Identifier les règles inutilisées et les supprimer régulièrement.

Aperçu des politiques



Obtenez une visibilité sur toutes les règles écrites dans un pare-feu spécifique.

Obtenez des détails complets sur les règles répertoriées, notamment le numéro de la règle, la source, la destination, l'interface et le type de service.

Filtrez facilement les règles en fonction de plusieurs critères de filtrage.

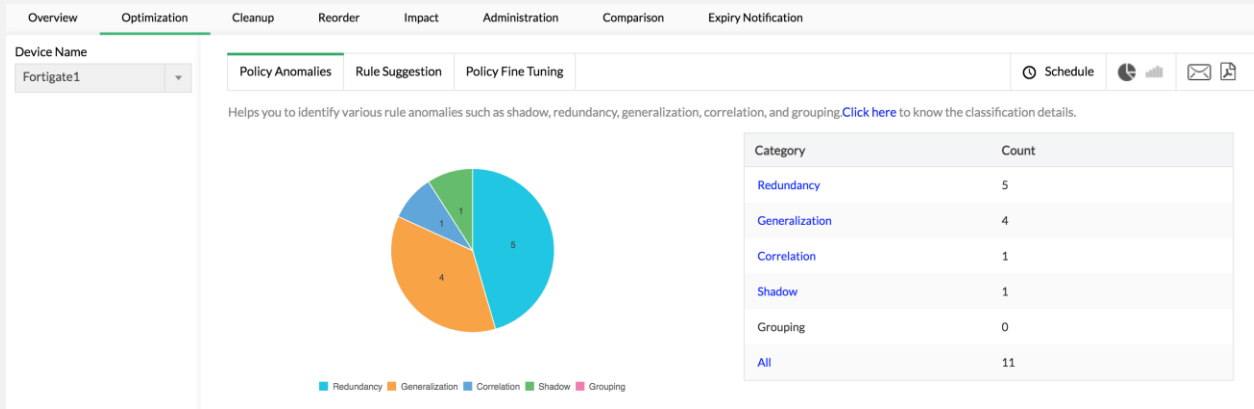
Overview Optimization Cleanup Reorder Impact Administration Comparison Expiry Notification

Device Name
Fortigate1

All 11

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

Optimisation des politiques



Identifiez les anomalies qui ont un impact négatif sur les performances du pare-feu.

Obtenez des détails complets sur les différents types d'anomalies. Déterminez les règles qui présentent des anomalies de type ombre, redondance, généralisation, corrélation et regroupement.

Device Name: CheckPoint

Select Time: Today

Policy Anomalies Rule Suggestion Policy Fine Tuning

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

Fine Tune

Filtrez facilement les anomalies en fonction de plusieurs critères de filtrage.

Réduire les règles trop permissives en recevant des suggestions de règles.

Ajustez les règles du pare-feu pour une performance maximale

Nettoyage des règles

Overview Optimization Cleanup Reorder Impact Administration Comparison Expiry Notification

Device Name
CheckPoint

Unused Rules 6 Unused Objects Unassigned Interfaces 5 Unassigned Objects 11

Schedule

Helps you identify the rules which have not been triggered for a given time period From : 2021-02-14 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,intcp,customUdp,UdpService Action=permit	🗑️
wireless to external	Source=Wireless Destination=InternalNetwork Service=ServiceGrp,syslogPort,UdpService Action=permit	🗑️

View 1 - 6 of 6

Réduisez les menaces de sécurité en identifiant les règles, objets et interfaces de pare-feu inutilisés.

Obtenez un aperçu de haut niveau des règles, objets et interfaces qui peuvent être supprimés ou désactivés.

Device Name
CheckPoint

Unused Rules 6 Unused Objects Unassigned Interfaces 5 Unassigned Objects 11

Schedule

Helps you identify the unassigned interfaces in your network.

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

Device Name
CheckPoint

Unused Rules 6 Unused Objects Unassigned Interfaces 5 Unassigned Objects 11

Schedule

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

Suggestion de réorganisation des règles

Overview Optimization Cleanup **Reorder** Impact Administration Comparison Expiry Notification

Device Name
FirePower

Select Time
Last 30 days

Suggested Changes **21** Complete Changes **48**

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

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

Obtenez des informations sur la façon d'organiser les règles de pare-feu pour maximiser la vitesse.

Estimez l'amélioration des performances pour un changement d'ordre suggéré en mettant en corrélation le nombre d'occurrences de règles avec la complexité des règles et les anomalies.

Exportez les suggestions de réorganisation et analysez-les hors ligne.

Analyse de l'impact des règles

Overview Optimization Cleanup Reorder **Impact** Administration Comparison Expiry Notification

Device Name
CiscoASA

Rule Impact 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		

Réalisez une analyse d'impact détaillée pour une nouvelle règle proposée et déterminez si la nouvelle règle proposée aura un impact négatif sur l'ensemble des règles existantes.

Utilisez l'analyse d'impact pour identifier les menaces, comprendre les risques, déterminer les anomalies et optimiser la nouvelle règle proposée.

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

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

Generate Rule Pre-Impact Report

Rule Name: 101

Position: Default Custom

24

Source: Any Select

Destination: Any Select

IP Network: Network IP 255.255.255.0

Available Destination: Search hyderabad zdb SV2-WinServer Fortigate-WAN-IP nalar.mobi@infia.com

Selected Destination: Search 223.242.246.134/255.255.255.0

Source Interface: Any Select

wan1

Administration des règles

Overview Optimization Cleanup Reorder Impact Administration Comparison Expiry Notification

Device Name: Fortigate1

Network Objects Service Objects Security Rules Review & Push Commit Choose columns

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_GET FTP_PUT RDP	

Ajoutez, modifiez et supprimez des règles et des objets réseau, analysez les implications d'un changement proposé et repoussez les changements directement dans le pare-feu.

Simplifiez la gestion de la politique du pare-feu en automatisant le processus d'administration des règles du pare-feu.

Network Objects Service Objects Security Rules Review & Push Commit Commit Audit

All the requested actions (add or edit or delete) on the objects or rules are listed here for review. Once reviewed, select the required objects or rules and push them directly into your firewall device by clicking on the "Push" button.

Mode: API CLI All

Name	Type	Status	Mode	Operations	Created Time	FWA User	Command	Action
pingService	Service Objects	Pending	API	add	2019-12-16 17:39:21	admin	Show Commands	
adkSrg_10	Network Objects	Pending	API	add	2019-12-16 17:38:43	admin	Show Commands	
APIUserService19	Service Objects	Pending	API	edit	2019-12-16 17:34:26	admin	Show Commands	
ipRange02	Network Objects	Pending	API	delete	2019-12-16 17:34:00	admin	Show Commands	
Facebook	Network Objects	Pending	API	edit	2019-12-16 17:33:07	admin	Show Commands	
rule1899	Security Rules	Pending	API	delete	2019-12-16 17:39:52	admin	Show Commands	
rule_38	Security Rules	Pending	API	add	2019-12-16 17:36:39	admin	Show Commands	

Network Objects Service Objects Security Rules Review & Push Commit Commit Audit

The commit status for object or rule changes that have been pushed are listed here. To validate changes that are yet to be committed, click on the commit button.

Yet to commit Committed

Name	Type	Operations	Changes	Time	FWA User	Mode	Action
rule_42	Security Rules	add	View Diff	2019-12-16 16:42:09	admin	CLI	
rule29	Security Rules	edit	View Diff	2019-12-16 16:39:10	admin	CLI	
ftp_20	Service Objects	add	View Diff	2019-12-16 16:38:51	admin	CLI	
ipRange_04	Network Objects	add	View Diff	2019-12-16 16:38:46	admin	CLI	
rule_39	Security Rules	add	View Diff	2019-12-16 12:26:36	admin	API	
vtp_25	Service Objects	delete	View Diff	2019-12-16 12:16:54	admin	API	
ipRange04	Network Objects	edit	View Diff	2019-12-16 12:16:51	admin	API	

Comparaison des règles

Overview Optimization Cleanup Reorder Impact Administration **Comparison** Expiry Notification

Compare Policies

📘 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

Compare

FortiGate ✔ Added - (1) ✔ Modified - (1) ✔ Deleted - (1) Diff Only All Policies ✉ 📄 ⏪ ⏩ ✕

Config_forti_rulecom1.txt			Config_1.txt		
Policy Name	Rule Name	Compare	Policy Name	Rule Name	
2	-	36			
4	-	45		45	
5			-	1001	

Suivre les modifications apportées aux règles de pare-feu dans le pare-feu





Gardez un œil sur toutes les modifications apportées à la configuration des règles du pare-feu.




Comparez les modifications de configuration entre :

1. Deux fichiers de configuration, qui peuvent être téléchargés manuellement.
2. Un fichier de configuration spécifique (pris manuellement) et la dernière configuration.
3. Les versions spécifiques de la configuration récupérées directement par Firewall Analyzer.

Notification d'expiration de la règle

Overview Optimization Cleanup Reorder Impact Administration Comparison Expiry Notification





All Scheduled Rules Active Rules Upcoming Rules Expired Rules Recurring Rules     10.59.10.165


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			


Suivre l'état des règles de pare-feu et être informé des règles qui ont expiré.

Liste de toutes les règles de pare-feu pour lesquelles une planification quelconque a été définie.





Énumérer toutes les règles de pare-feu actives pour lesquelles une planification a été définie.

All Scheduled Rules Active Rules Upcoming Rules Expired Rules Recurring Rules     10.59.10.165


Show: All Active Rules Rules which are active for next 24 Hrs 

Rule Number/ID	Schedule Name	Schedule Type	Days of week	Time	Start Time	End Time	Expiry Mail ID
<input type="checkbox"/>  ruleexp1	dailyschedule	recurring	daily 00:00-13:45 02:45-23:45				-

Cataloguer toutes les règles dont l'activation est prévue dans le futur.

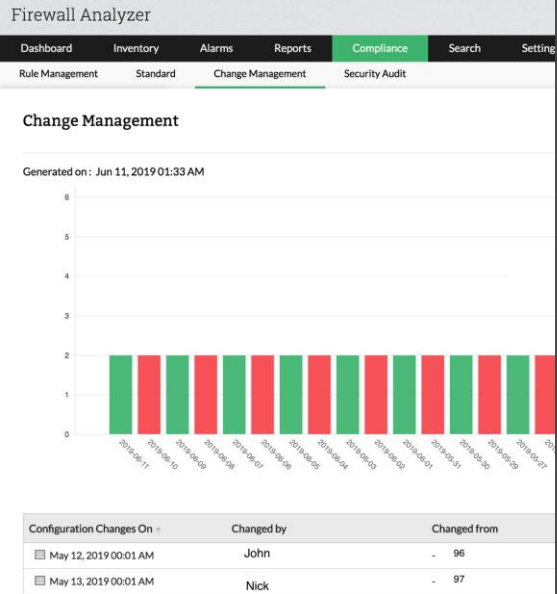
All Scheduled Rules Active Rules Upcoming Rules Expired Rules Recurring Rules     10.59.10.165

Show: All Expired Rules Rules Expired in the last 24 Hrs

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			

Enregistrer toutes les règles qui ont expiré

Répertorier toutes les règles qui sont réactivées et certifiées sur une base régulière.



Gestion des modifications de configuration

Version No	Change count	Change Type
97	2	running
96	2	running

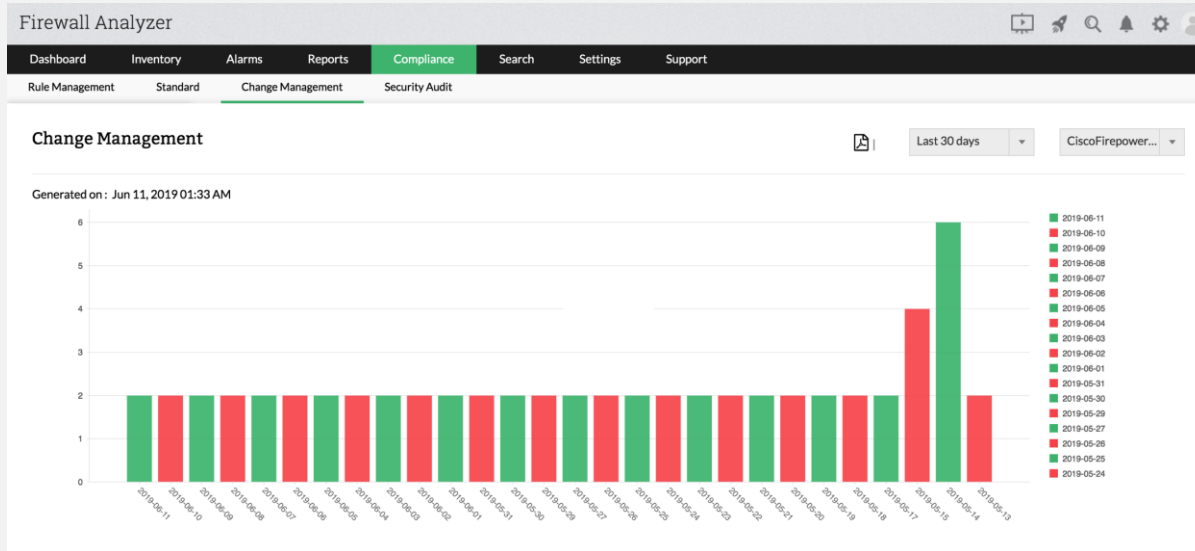
L'importance de la gestion des modifications

Le suivi automatisé des modifications est essentiel pour obtenir une meilleure visibilité sur la configuration et la sécurité de votre pare-feu !



- Éliminez le suivi manuel des modifications.
- Sécurisez votre réseau en surveillant les modifications apportées à la configuration du pare-feu.
- Les notifications de modifications vous aident à rester vigilant.

Suivi des modifications de configuration



Automatisez le suivi des modifications de configuration dans tous vos dispositifs de pare-feu.

Suivez le "quoi", le "qui" et le "quand" des modifications de configuration.

Recevez des notifications de modification directement dans votre courrier électronique.

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
<input type="checkbox"/> May 12, 2019 00:01 AM	John	- 96	97	2	running
<input type="checkbox"/> May 13, 2019 00:01 AM	Nick	- 97	98	2	running

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

11	enable password 8Ry2Yjlyt7RRXU24 encrypted	enable password 8Ry2Yjlyt7RRXU24
12		enable https false

Comparaison des configurations à l'aide de Diff-View

Fortigate1 ✓ Added - (4) ✓ Modified - (16) ✗ Deleted - (10) Diff Only All Lines < > ✕

5	config system global	config system global
6	set access-banner disable	set access-banner disable
7	set admin-https-pki-required disable	set admin-https-pki-required disable
8	set admin-lockout-duration 60	set admin-lockout-duration 62
9	set admin-lockout-threshold 3	set admin-lockout-threshold 4
10	set admin-maintainer enable	set admin-maintainer 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-telnet-port 23	set admin-telnet-port 25
18	set admintimeout 5	set admintimeout 5
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 1000	set auth-http-port 2000
22	set auth-https-port 1003	set auth-https-port 1000
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-fallopen pass	set av-fallopen pass
26	set av-fallopen-session disable	set av-fallopen-session disable
27	set batch-cmdb enable	set batch-cmdb enable
28	set cfg-save automatic	set cfg-save automatic
29	set check-protocol-header loose	set check-protocol-header loose
30	set check-reset-range disable	set check-reset-range disable
31	set cit-cert-req disable	set cit-cert-req disable
32	set daily-restart disable	set daily-restart disable
33	set detection-summary enable	set detection-summary enable

Comparez les modifications de configuration entre deux configurations, côte à côte, à l'aide de Diff-View.

Identifiez facilement les changements entre les fichiers de configuration à l'aide d'une représentation des modifications par code couleur.

Visualisez les lignes ajoutées en vert, les lignes supprimées en rouge et les lignes modifiées en bleu.

Firewall Analyzer

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

Rule Management Standard Change Management 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 Count 3
4 Enable Logging
11 Insecure Services
15 Block ICMP Unwanted 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 Count 4
1.1.5 b Insecure Services
1.1.7 Periodic Review of Rule Sets
1.2.1 b Explicit Deny rule

**Audit de conformité
et de sécurité**

NIST on 2019-01-30 04:49

This assessment is based on the NIST Standard of compliance. For more information, please visit <http://www.nist.gov>

60% Compliant
Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count 3
2.2.1 Insecure Services
2.2.2 Insecure Services
2.2.3 Insecure Services

** Some requirements need to be manually verified.

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/standards/standards_detail.htm?number=14324

28% Compliant
Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count 5
9.2 User Access Control
12.4.2 Implementation of patch
12.4.4 Use Third-Party Products

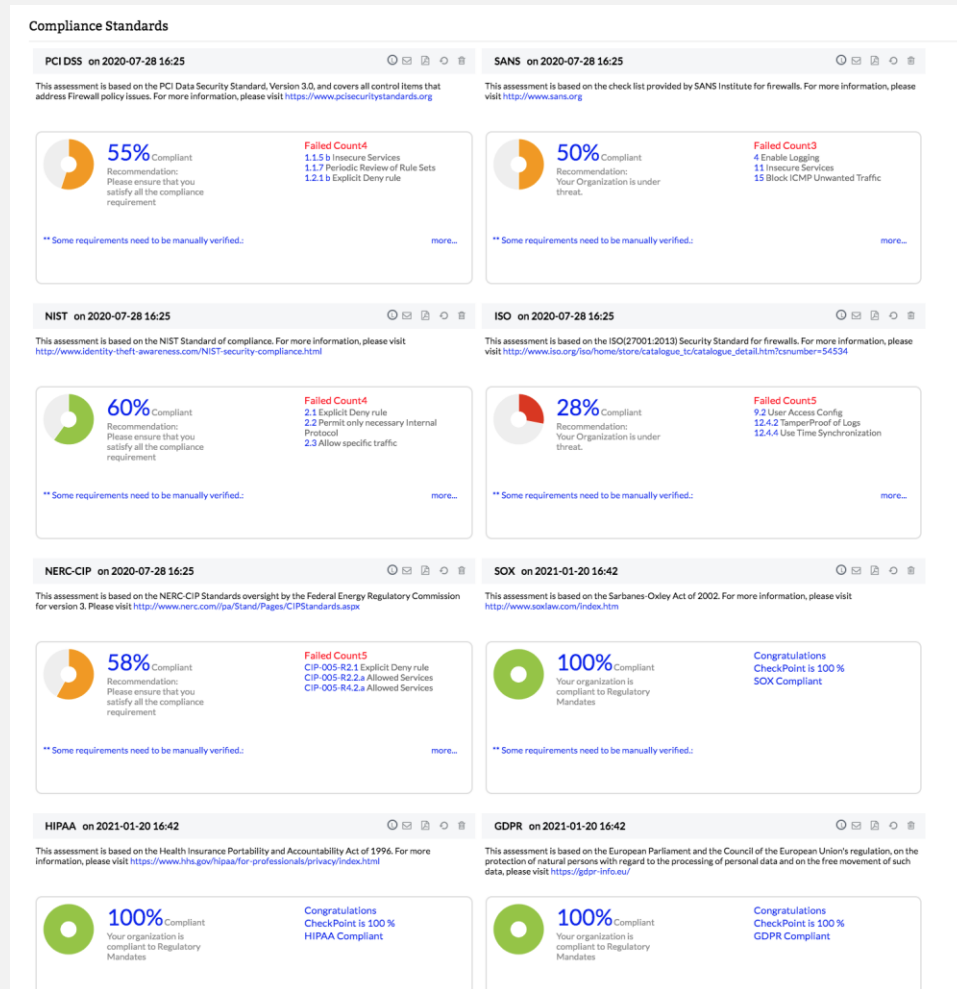
Restez conforme avec des rapports de conformité prêts à l'emploi

Suivez les pratiques standard et appliquez les politiques de sécurité internes/externes pour éviter les problèmes juridiques grâce à une bonne gestion de la conformité!



- Restez en conformité avec les normes PCI-DSS, ISO 27001, NIST, NERC-CIP, SANS, SOX, HIPAA et les mandats réglementaires GDP.
- Identifiez les failles de configuration et restez en sécurité.
- Générez des rapports sur l'état de conformité des dispositifs de pare-feu.

Rapport de conformité



Sécurisez efficacement les données de vos titulaires de cartes en vous conformant à la norme PCI-DSS.

Maîtrisez la gestion de la sécurité des informations en restant conforme à la norme ISO 27001.

Assurez-vous que votre infrastructure informatique critique est sécurisée en vous conformant au mandat du NERC-CIP.

Vérifiez les failles de sécurité de l'information en vous appuyant sur le rapport SANS.

Vérifiez les normes NIST avec les rapports de conformité NIST.

Vérifiez la conformité à SOX, HIPAA et GDPR avec des rapports prêts à l'emploi.

Audit de sécurité

The screenshot shows the 'Firewall Analyzer' interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Alarms', 'Reports', 'Compliance' (highlighted), 'Search', 'Settings', and 'Support'. Below this, there are sub-menus for 'Rule Management', 'Standard', 'Change Management', and 'Security Audit'. The main content area displays a 'Security Audit' report for 'Fortigate-3200D'. The report header is blue and contains the text: 'ManageEngine Fortinet FortiGate FG800C3913800555 Security Report' and 'FRIDAY 1ST FEBRUARY 2019'. Below the header is a 'Security Audit Summary' section. It contains three paragraphs of text and a bar chart titled 'OVERALL ISSUE RATINGS'. The bar chart shows the following counts: CRITICAL (0), HIGH (1), MEDIUM (4), LOW (2), and INFO (5).

Effectuez des audits de sécurité sur la configuration de votre pare-feu et obtenez des rapports détaillés sur toutes les failles de sécurité.

Identifiez la criticité des failles de configuration et obtenez également la facilité d'attaque.

Obtenez des recommandations sur les meilleures pratiques du secteur.

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

Firewall Analyzer

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

Custom Report Firewall Reports Proxy Reports API Access General

Device Name
All Devices

Report Type

- Intranet Reports
- Internet Reports
- Security Reports**
- Virus Reports
- Attack Reports
- Spam Reports
- Protocol Trend Reports
- Traffic Trend Reports
- Event Trend Reports
- Admin Reports
- VPN Trend Report

Security Reports

Top Denied Hosts

Resolve DNS

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

Resolve DNS

Destination	Hits
12.21.34.212	8539
10.45.0.1	2124
39-4-50-200-etc.com	1824
mail.efonaleda.com	1293
75.ad.7e4b.ip4.com	1288
Others	18345

Gestion des journaux

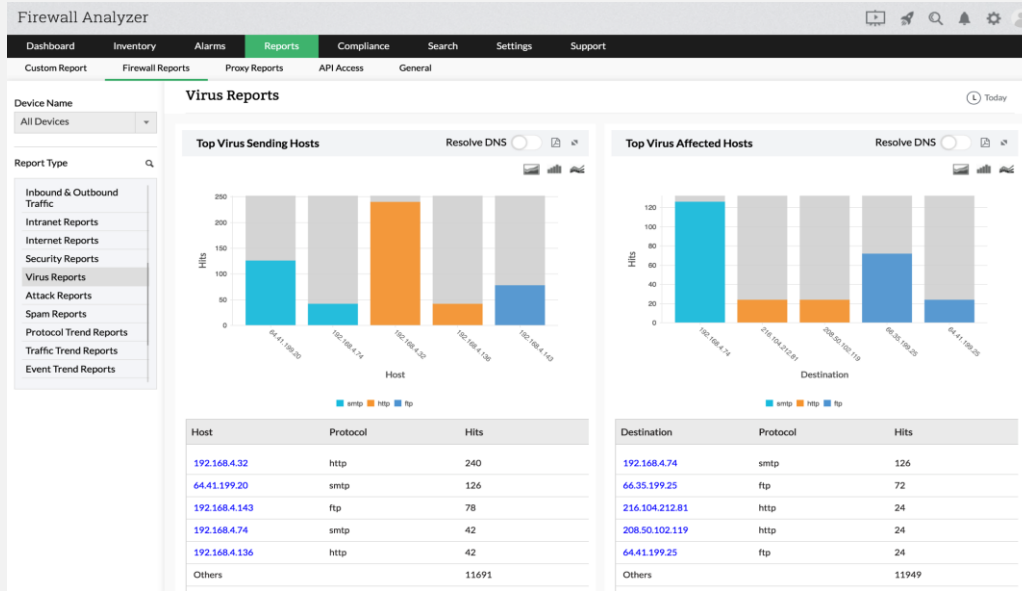
La gestion des journaux est essentielle pour la sécurité des réseaux

L'analyse des données syslog vous aidera à identifier et à prévenir les menaces à la sécurité en temps réel.



- les menaces internes et externes.
- L'analyse du trafic permet de gérer la bande passante.
- Les alertes basées sur les journaux permettent de prendre des mesures correctives instantanées.

Analyses de sécurité

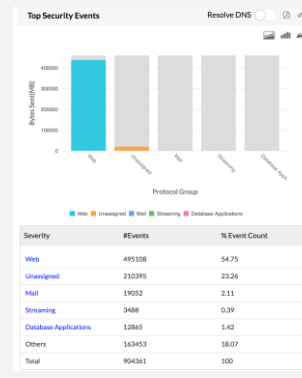
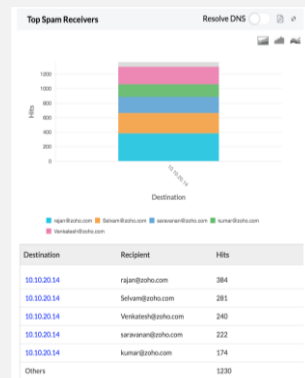
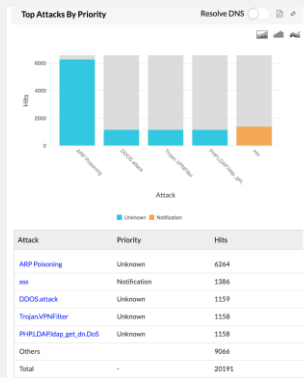


Générez des rapports détaillés sur les éventuelles menaces pour la sécurité du réseau.

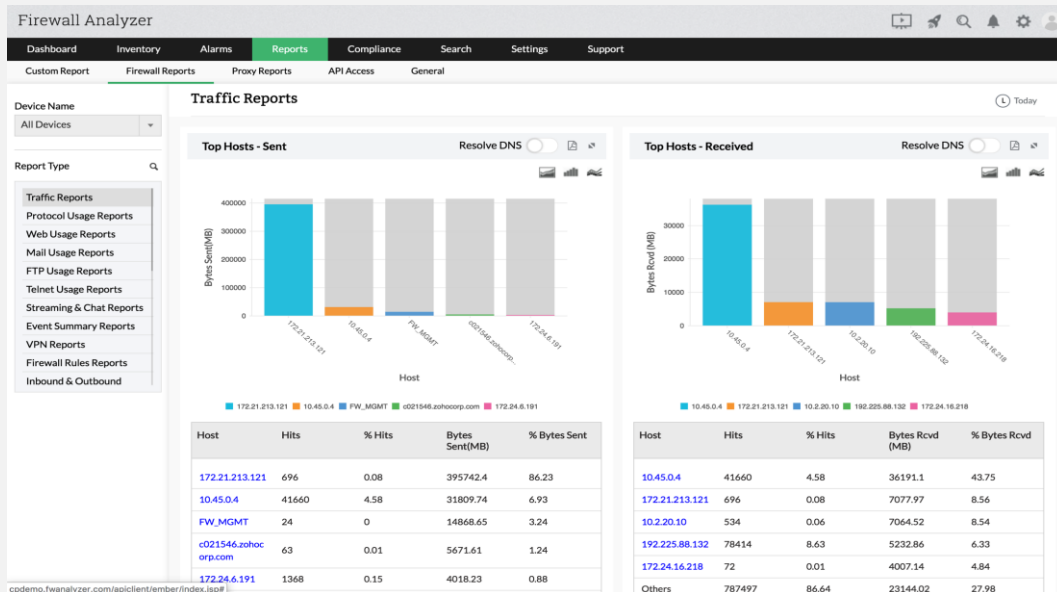
Dépannez et résolvez plus rapidement les problèmes de sécurité en identifiant et en analysant les journaux relatifs aux virus.

Obtenez des informations pour identifier et contrer les attaques du réseau.

Obtenez des informations détaillées sur l'activité du spam et contrôlez le spam sur le réseau.

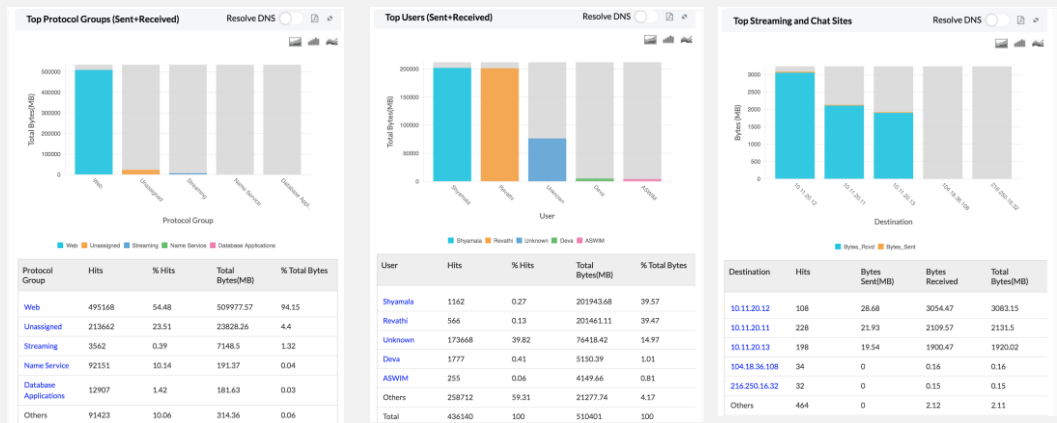


Analyses de trafic

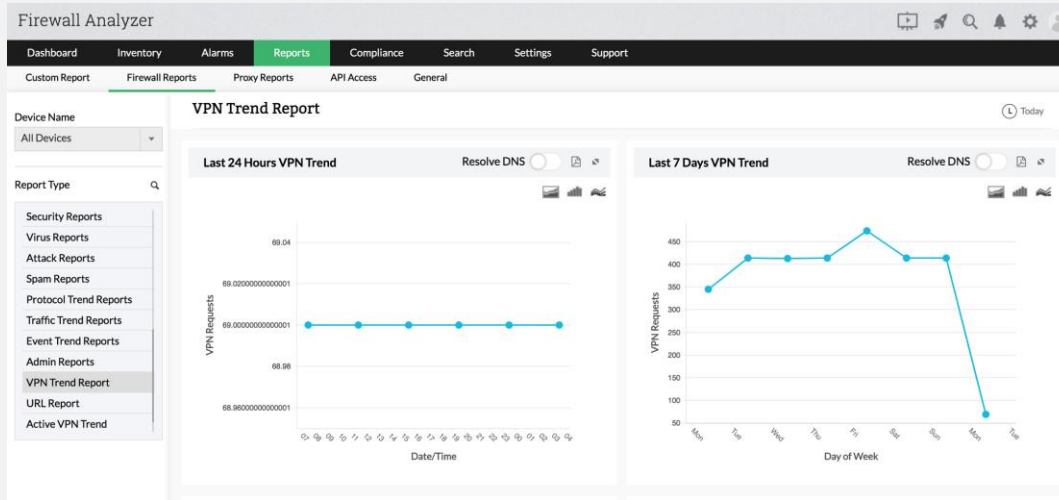


Les rapports de trafic de Firewall Analyzer permettent de répondre aux questions suivantes

- Qui envoie et reçoit le trafic ?
- Quel hôte envoie ou reçoit le trafic ?
- Quelle est la part de trafic des différents groupes de protocoles ?
- Quel est le modèle de gravité des événements dus au trafic ?



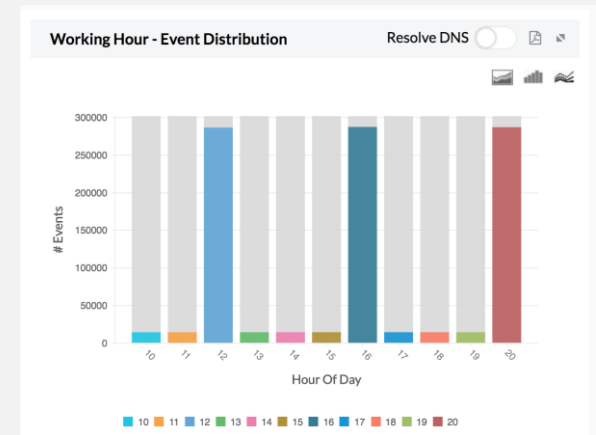
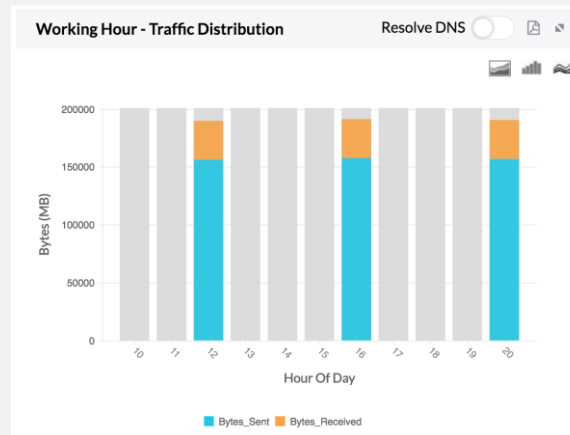
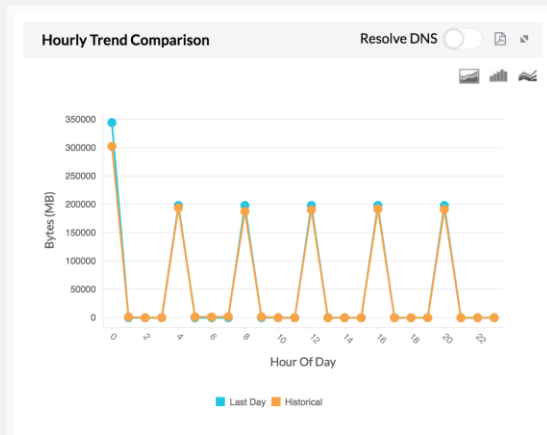
Analyses des tendances

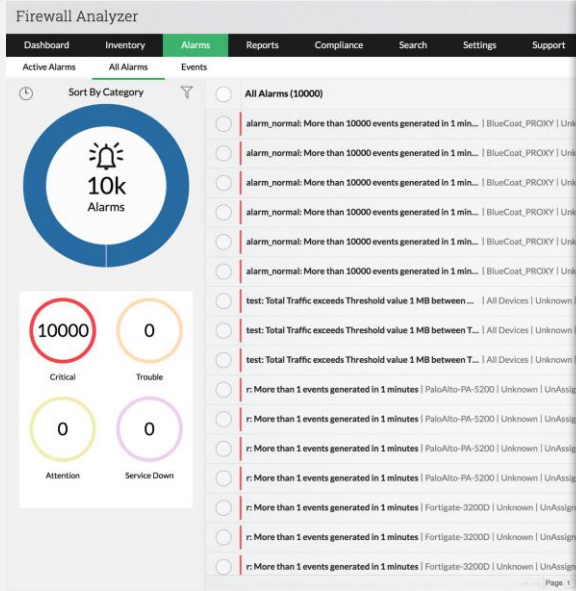


Déterminez la tendance de l'utilisation maximale de la bande passante pour différents protocoles et horodatages.

Dépannez les liens et identifiez les risques de sécurité en analysant le rapport de tendance des événements.

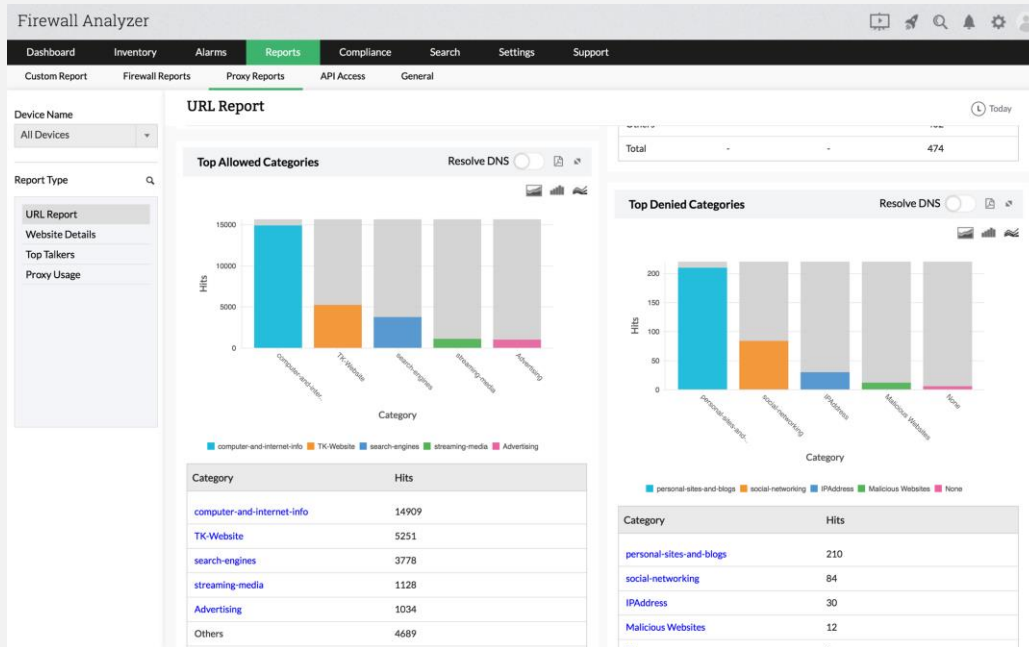
Identifiez les connexions VPN en direct et les risques de sécurité liés au VPN en utilisant le rapport de tendance VPN.





Autres fonctionnalités importantes

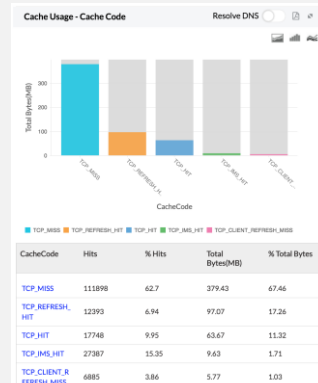
Rapport Proxy



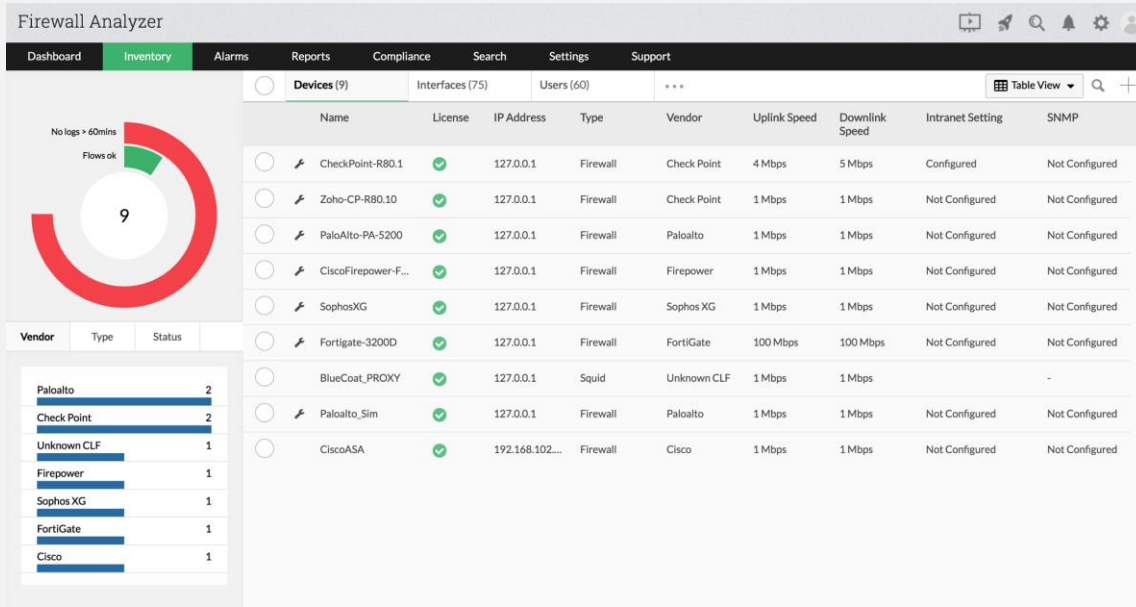
Collectez et archivez les journaux du serveur proxy, analysez-les et générez des rapports d'informations utiles sur l'accès à l'Internet de l'entreprise.

Générez des rapports sur l'utilisation du proxy et les virus du proxy

Obtenez la liste des URLs accédées en utilisant le serveur proxy



Rapport d'inventaire



Obtenez une image complète de tout ce qui se passe sur les pare-feu individuels.

Obtenez une visibilité sur les interfaces qui se trouvent sous les dispositifs de pare-feu configurés.

Obtenez une vue d'ensemble de tous les utilisateurs qui ont accédé à Internet par le biais de dispositifs de pare-feu individuels.

Surveillez les règles et les services en cloud auxquels vous avez accès sous un dispositif de pare-feu spécifique.

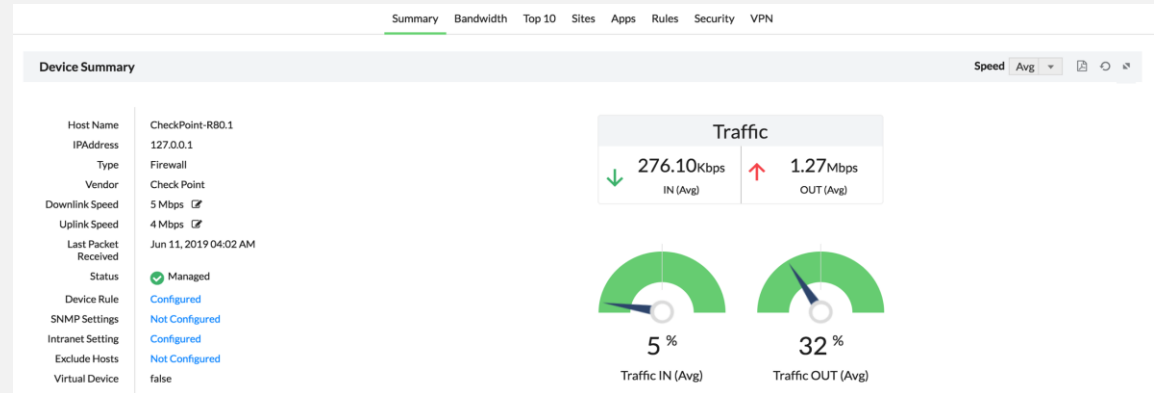
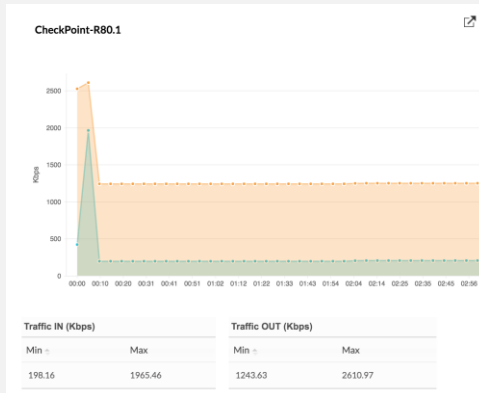
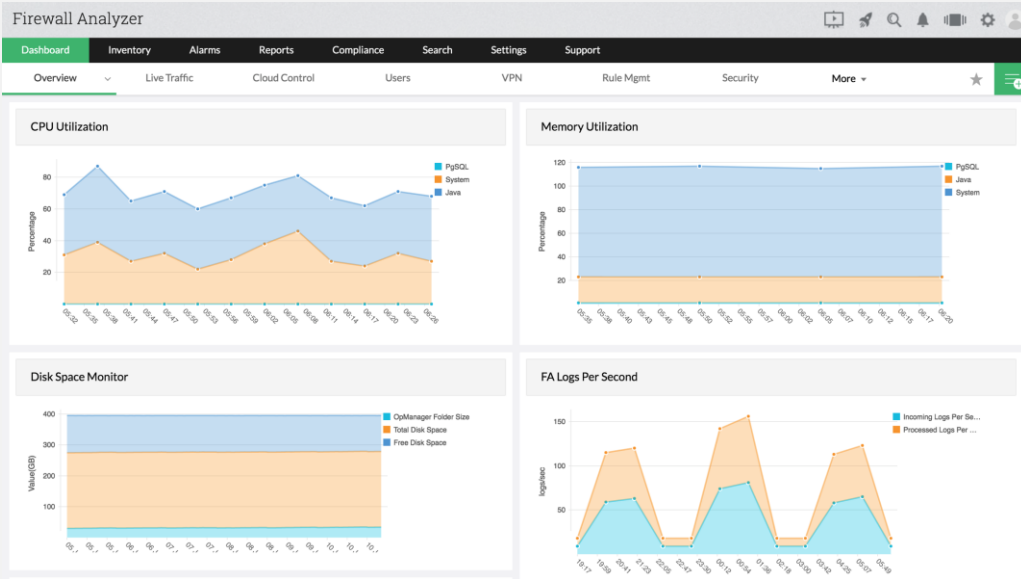


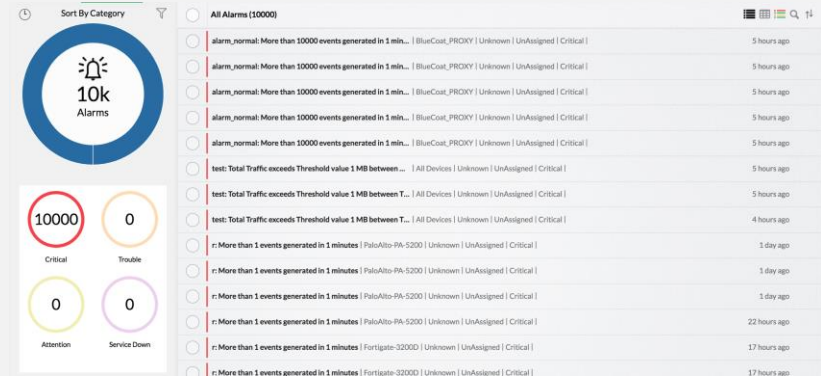
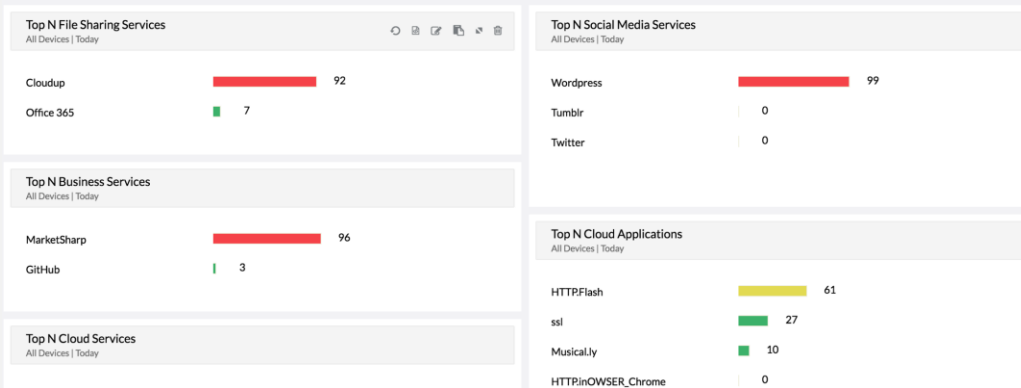
Tableau de bord, supervision du cloud et alarmes



Obtenez une image de haut niveau de tout ce qui se passe dans votre écosystème de pare-feu.

Gardez un œil sur tous les services de clouds exécutés sur votre réseau.

Déclenchez des alertes basées sur des seuils (trafic et sécurité) et recevez des notifications directement sur votre messagerie ou votre téléphone.



Analyse forensique des journaux et rapports personnalisés

The screenshot shows the 'Firewall Analyzer' interface with the 'Search' tab selected. The 'RAW Search' sub-tab is active. On the left, there are sections for 'Available Devices' and 'Selected Devices'. The 'Selected Devices' list includes 'CiscoFirepower-FMC', 'Paloalto_Sim', 'BlueCoat_PROXY', 'PaloAlto-PA-5200', and 'Ztehn-CP-RR1 10'. Below this, the 'Search Type' 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', all of which are checked. Under 'Criteria', the option 'Match any of the following' is selected. Three criteria are defined: 'Protocol is HTTP', 'User is Jon', and 'Attack is ARP poisoning'. Each criterion has a red 'X' and a green '+' button. A 'Generate' button is at the bottom.

Effectuez des recherches dans les journaux bruts de Firewall pour identifier l'entrée exacte qui a causé l'activité de sécurité.

Les journaux archivés peuvent être importés et l'exploration des incidents de sécurité peut être effectuée en recherchant les journaux bruts.

Générez des rapports personnalisés basés sur des critères spécifiques. Choisissez les sous-rapports que vous souhaitez inclure dans le rapport personnalisé, les paramètres exacts sur lesquels portera le rapport, et même la disposition du graphique à générer.

The screenshot shows the 'Search Report' page with the 'Raw Logs' tab selected. A table displays the search results with the following columns: Date/Time, Host, User, Protocol, Destination, Virus/Attack, Severity, Duration, Sent, and Receive.

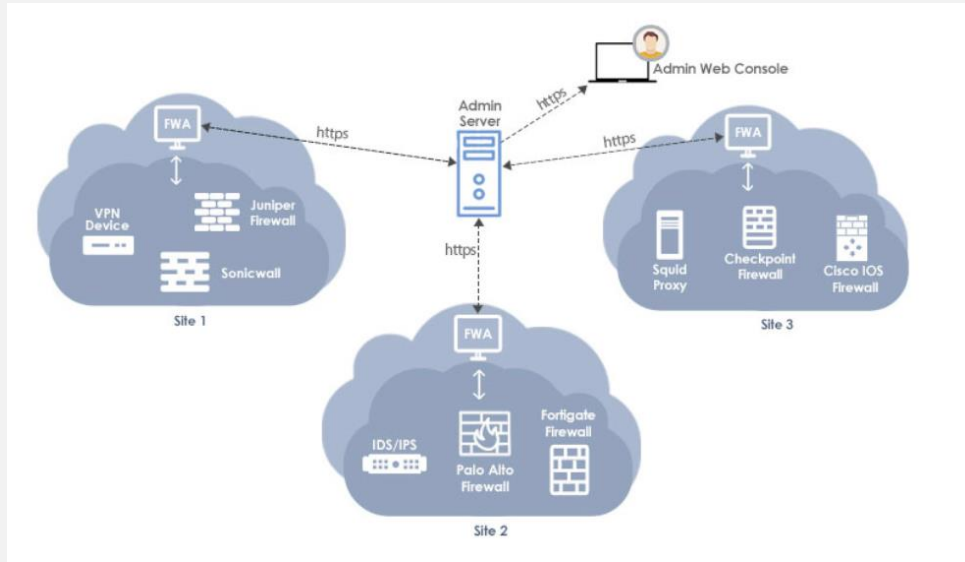
Date/Time	Host	User	Protocol	Destination	Virus/Attack	Severity	Duration	Sent	Receive
11 Jun 2019, 06:46:33	192.168.1.51	Khrist	972/tcp	31.13.69.203	null	Unknown	1 Secs	0 KB	0 KB
11 Jun 2019, 06:46:33	192.168.1.50	John	fcp	12.183.124.41	null	Unknown	3 Mins 2 Secs	0 KB	4.68 KB
11 Jun 2019, 06:46:33	192.168.1.49	Patrick	mailbox-lm	69.63.178.12	null	Unknown	16 Mins 3 Secs	0 KB	4.68 KB

The screenshot shows the 'Search Report' page with the 'Raw Logs' tab selected. A table displays the search results with the following columns: Date/Time, Host, User, Protocol, Destination, Virus/Attack, Severity, Duration, Sent, and Receive.

Date/Time	Host	User	Protocol	Destination	Virus/Attack	Severity	Duration	Sent	Receive
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,HTTPFlashvsys1,trust,untrust,lan,wan5,LOG-FWD,17014.1.720.888,720.888,0x40001c,tcp,allow,4790,961013.652313,17,372,Information Technology,0.384809398,0x0									
Paloalto_Sim_001801021446,TRAFFIC,end,0,192.168.1.41,180.179.168.232,192.168.1.41,180.179.168.232,Rule_48,Chris,HTTPFlashvsys1,trust,untrust,lan,wan5,LOG-FWD,17014.1.375.2.375.2,0x40001c,udp,allow,4790,197176,79519,17,81,Information Technology,0.384809398,0x0									

The screenshot shows the 'Add Report Type' dialog box. It has a 'Report Name' field with 'Custom VPN' and a 'Report based on' dropdown with 'VPN' selected. The 'Display' section has three radio buttons: 'Graph & Table' (selected), 'Graph', and 'Table'. The 'Graph Settings' section includes a 'Graph Types' dropdown with 'Stacked Vertical Ba...' selected, an 'X-axis' dropdown with 'VPN' selected, a 'Y-axis' dropdown with 'sum of Total bytes' selected, a 'Grouping Criteria' dropdown with 'User' selected, and an 'Order by' dropdown with 'sum of RequestCount' selected. There is a small bar chart preview showing three bars with stacked segments. At the bottom, there are 'Cancel' and 'Ok' buttons.

Avantages de l'utilisation de Firewall Analyzer



Supervision de l'entreprise

Surveillez les pare-feu géographiquement distribués à partir d'un emplacement centralisé.

Possibilité d'évoluer en douceur jusqu'à 1200 dispositifs de sécurité.

Prise en charge de plusieurs pare-feu

Prend en charge plus de 50 fournisseurs de pare-feu et 200 dispositifs



Tarification abordable

Abonnement annuel :

- Supervision d'un seul pare-feu à partir de 395\$.
- Le pack de 20 dispositifs (édition Enterprise) à partir de 8 395\$.



Assistance technique 24x5

Assistance technique 24x5 pour
les clients afin d'obtenir une
utilisation maximale du produit !



Intégration transparente à l'ensemble de votre infrastructure réseau

Intégration complète

- **OpManager:** Supervision du réseau et des serveurs
- **NetFlow Analyzer:** Supervision de la bande passante
- **Network Configuration Manager:** Configuration du réseau et gestion de la conformité
- **OpUtils:** Gestion des adresses IP et des ports de commutation



Qu'est-ce qui nous distingue ?



Prise en charge de
plusieurs pare-feu



Alertes de sécurité
en temps réel



Rapports prêts
à l'emploi



Hautement
évolutif

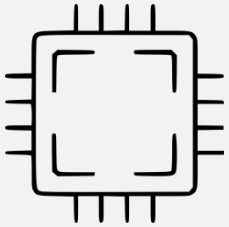


Économique

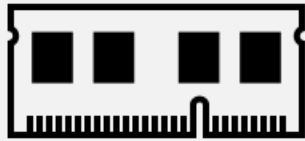


Support
technique 24x5

Configuration minimale requise



Processeur
Pentium Dual
Core 1 GHZ ou
équivalent



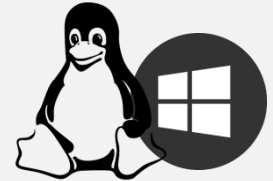
1 GO RAM



1 GO Stockage



PostgreSQL/MSSQL



Windows/Linux

L'espace disque et la taille de la mémoire vive requis dépendent du nombre de dispositifs analysés et du nombre de dispositifs envoyant des informations de journal à Firewall Analyzer.

Merci

Profitez d'une meilleure expérience de gestion du pare-feu !



Contact:

Pour toute requête technique: fwanalyzer-support@manageengine.com

Pour les tarifs et autres: sales@manageengine.com

Pour en savoir plus, visitez <https://www.pgsoftware.fr/siem/firewall-analyzer>