ManageEngine

Firewall Analyzer v12

Política de firewall, configuración y software de análisis de logs.

– ¿Qué es?

Firewall Analyzer es un software de análisis de políticas, monitoreo de configuraciones y generación de informes de log para que los administradores de seguridad controlen los cambios de políticas, optimicen el rendimiento del firewall y mantengan los estándares de cumplimiento.

Detecte y prevenga de forma proactiva las amenazas a la seguridad de la red, aproveche al máximo Firewall Analyzer con las siguientes funciones.

Gestión de reglas

Gestión de cambios

Informes de cumplimiento

Auditorías de seguridad

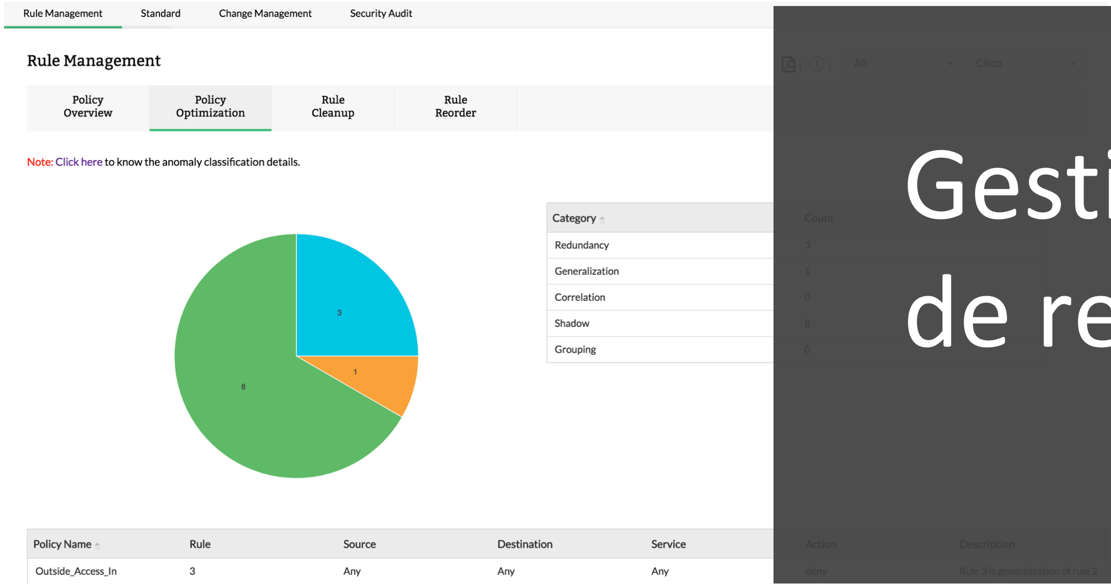
Gestión de logs

Gestión de alarmas

¡Por estas razones lo necesita!

- Simplifique las políticas de firewall, optimice las reglas y mejore el rendimiento del firewall.
- Mantenga un registro de todos los cambios de configuración al automatizar el control de cambios.
- Adhiérase a los estándares de cumplimiento e identifique las brechas de seguridad con los informes de cumplimiento out-of-the-box
- Identifique y prevenga las amenazas a la seguridad de la red al monitorear los logs de seguridad y el uso de Internet de los empleados.
- Recopile fácilmente los incidentes de seguridad de los logs sin procesar y realice análisis forenses para detectar amenazas.
- Reciba notificaciones sobre incidentes anómalos relacionados con la seguridad y el ancho de banda directamente en su correo o teléfono.

Gestión de reglas



Rule Management

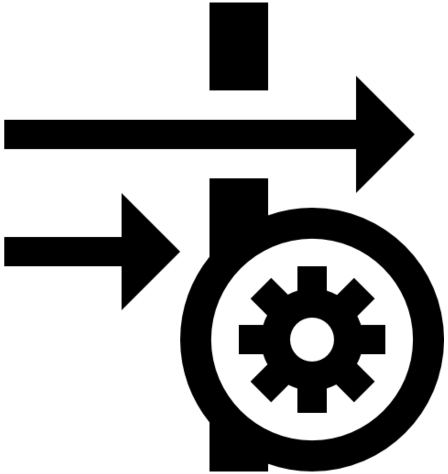
Note: Click here to know the anomaly classification details.

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

La importancia de la gestión de reglas

El rendimiento de cualquier firewall depende en gran parte de las reglas y políticas. Si las reglas no se gestionan correctamente, su red podría quedar vulnerable ante los ataques.



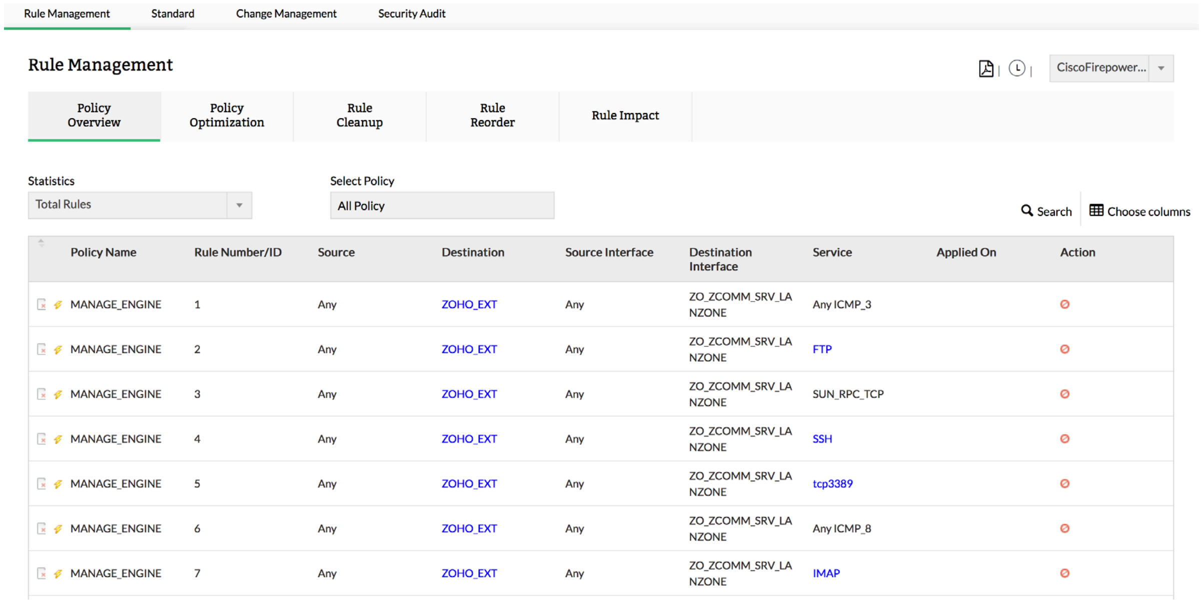
- Obtenga visibilidad completa sobre todas las reglas escritas en su firewall.
- Mejore el rendimiento del firewall identificando y eliminando las anomalías de las reglas.
- Optimice el rendimiento de las reglas organizando las reglas de manera correcta.
- Determine si una nueva regla propuesta va a afectar negativamente al conjunto de reglas existente.
- Identifique las reglas no utilizadas y elimínelas regularmente.

Resumen de la política

Obtenga visibilidad de todas las reglas escritas en un firewall específico.

Obtenga detalles completos de las reglas enumeradas, incluido el número de regla, el origen, el destino, la interfaz y el tipo de servicio.

Filtre fácilmente las reglas usando varios criterios de filtro.

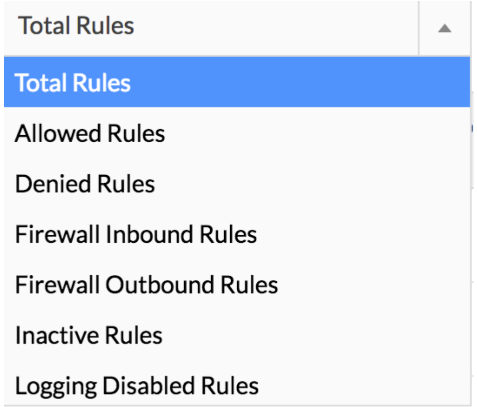


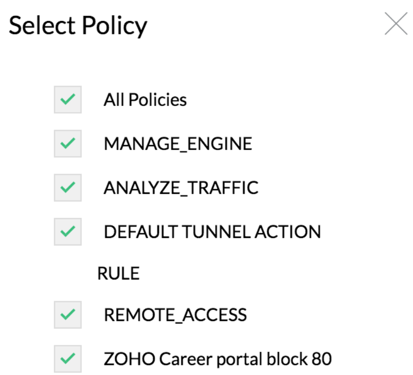
Rule Management

Statistics: Total Rules

Select Policy: All Policy

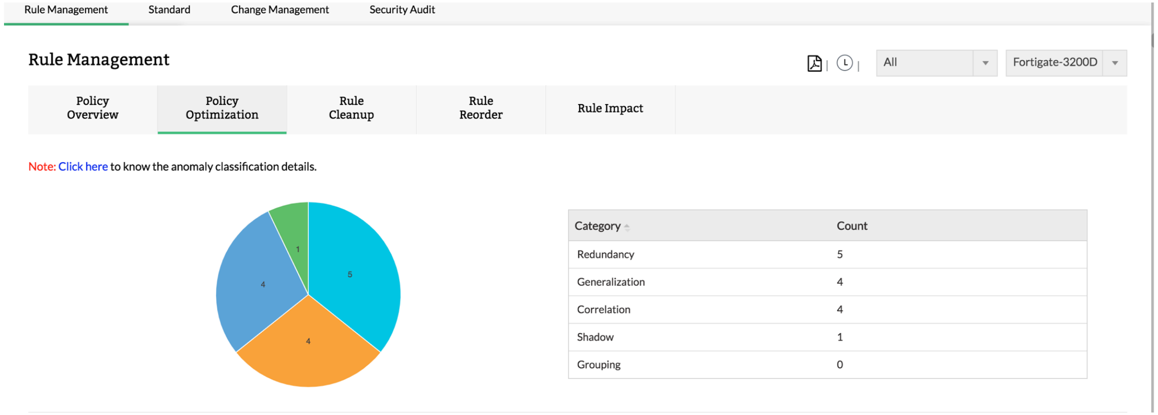
Policy Name	Rule Number/ID	Source	Destination	Source Interface	Destination Interface	Service	Applied On	Action
MANAGE_ENGINE	1	Any	ZOHO_EXT	Any	ZO_ZCOMM_SRV_LANZONE	Any ICMP_3		⊗
MANAGE_ENGINE	2	Any	ZOHO_EXT	Any	ZO_ZCOMM_SRV_LANZONE	FTP		⊗
MANAGE_ENGINE	3	Any	ZOHO_EXT	Any	ZO_ZCOMM_SRV_LANZONE	SUN_RPC_TCP		⊗
MANAGE_ENGINE	4	Any	ZOHO_EXT	Any	ZO_ZCOMM_SRV_LANZONE	SSH		⊗
MANAGE_ENGINE	5	Any	ZOHO_EXT	Any	ZO_ZCOMM_SRV_LANZONE	tcp3389		⊗
MANAGE_ENGINE	6	Any	ZOHO_EXT	Any	ZO_ZCOMM_SRV_LANZONE	Any ICMP_8		⊗
MANAGE_ENGINE	7	Any	ZOHO_EXT	Any	ZO_ZCOMM_SRV_LANZONE	IMAP		⊗




Select Policy

- ☑ All Policies
- ☑ MANAGE_ENGINE
- ☑ ANALYZE_TRAFFIC
- ☑ DEFAULT TUNNEL ACTION RULE
- ☑ REMOTE_ACCESS
- ☑ ZOHO Career portal block 80

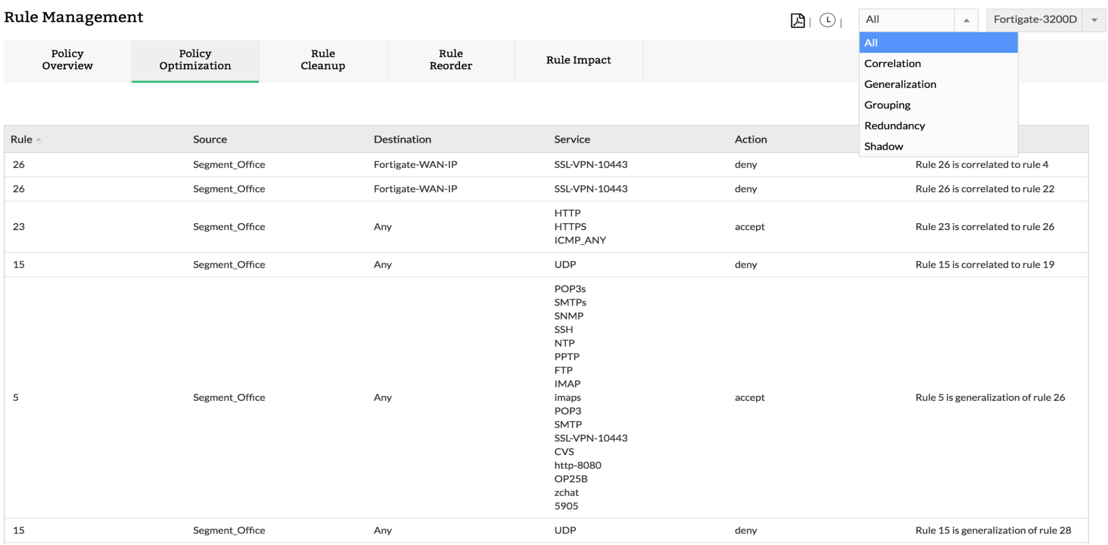
Optimización de la política



Rule Management

Note: Click here to know the anomaly classification details.

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



Rule Management

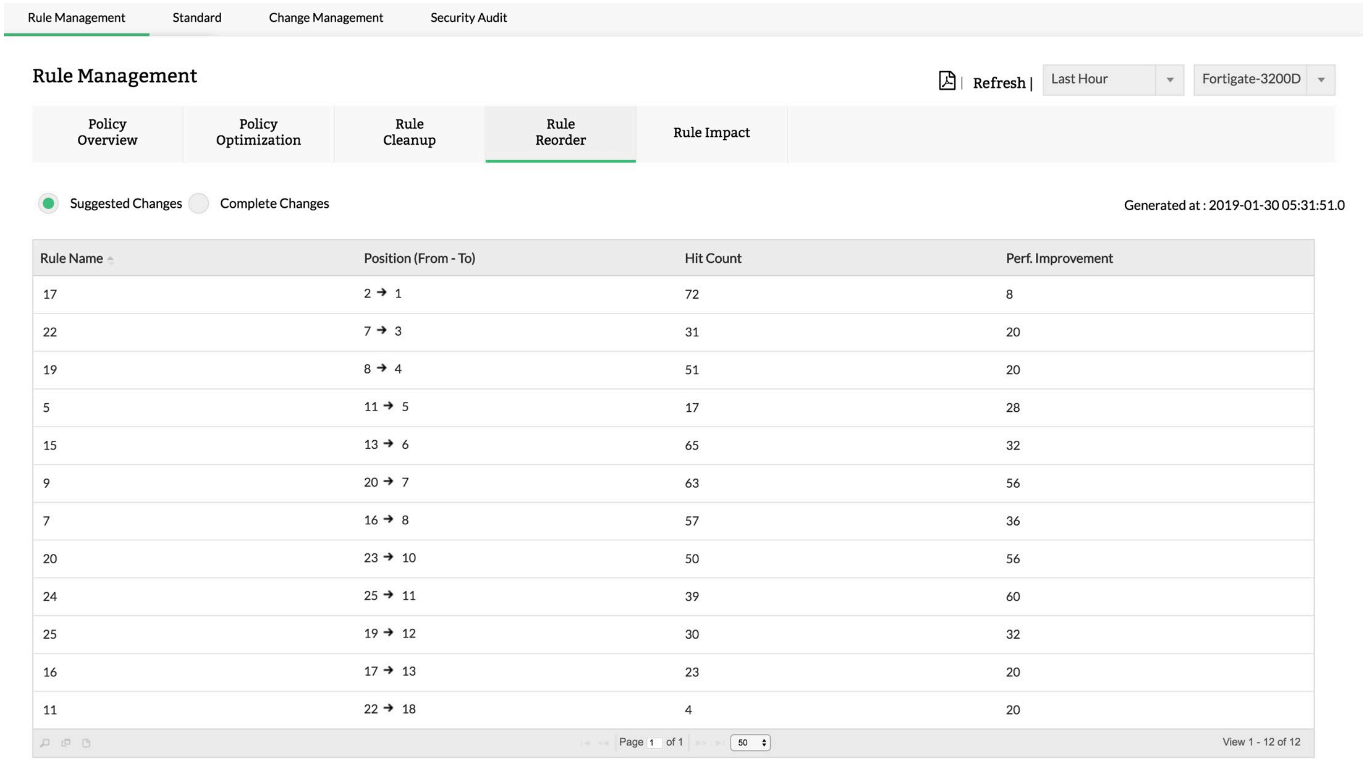
Rule	Source	Destination	Service	Action	
26	Segment_Office	Fortigate-WAN-IP	SSL-VPN-10443	deny	Rule 26 is correlated to rule 4
26	Segment_Office	Fortigate-WAN-IP	SSL-VPN-10443	deny	Rule 26 is correlated to rule 22
23	Segment_Office	Any	HTTP HTTPS ICMP_ANY	accept	Rule 23 is correlated to rule 26
15	Segment_Office	Any	UDP	deny	Rule 15 is correlated to rule 19
5	Segment_Office	Any	POP3s SMTPs SNMP SSH NTP PPTP FTP IMAP imaps POP3 SMTP SSL-VPN-10443 CVS http-8080 OP25B zchat 5905	accept	Rule 5 is generalization of rule 26
15	Segment_Office	Any	UDP	deny	Rule 15 is generalization of rule 28

Identifique las anomalías que afectan negativamente el rendimiento del firewall.

Obtenga detalles completos de los diferentes tipos de anomalías. Identifique las reglas que tengan anomalías de seguimiento, redundancia, generalización, correlación y agrupación.

Filtre fácilmente las anomalías usando varios criterios de filtro.

Sugerencia de reordenamiento de reglas



Rule Management

Last Hour | Fortigate-3200D

● Suggested Changes ○ Complete Changes

Generated at : 2019-01-30 05:31:51.0

Rule Name	Position (From - To)	Hit Count	Perf. Improvement
17	2 → 1	72	8
22	7 → 3	31	20
19	8 → 4	51	20
5	11 → 5	17	28
15	13 → 6	65	32
9	20 → 7	63	56
7	16 → 8	57	36
20	23 → 10	50	56
24	25 → 11	39	60
25	19 → 12	30	32
16	17 → 13	23	20
11	22 → 18	4	20

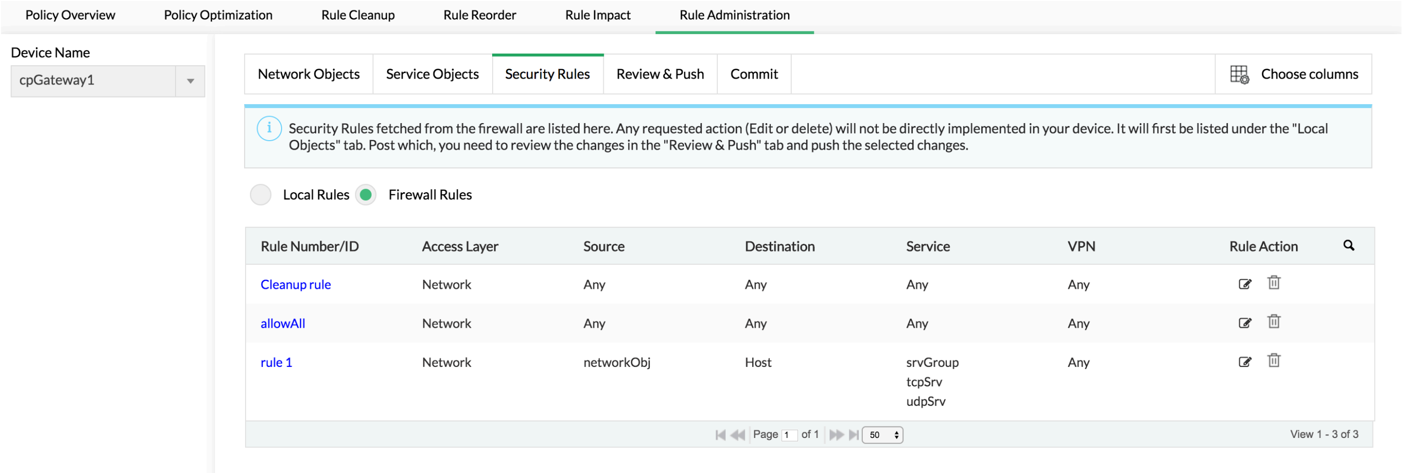
Page 1 of 1 | 50 | View 1 - 12 of 12

Obtenga información sobre cómo organizar las reglas de firewall para maximizar la velocidad.

Estime cuál es la mejora del rendimiento para un cambio de orden sugerido correlacionando el número de aciertos de la regla con la complejidad y las anomalías de la regla.

Exporte el reordenamiento sugerido y analícelo sin conexión.

Administración de reglas



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.

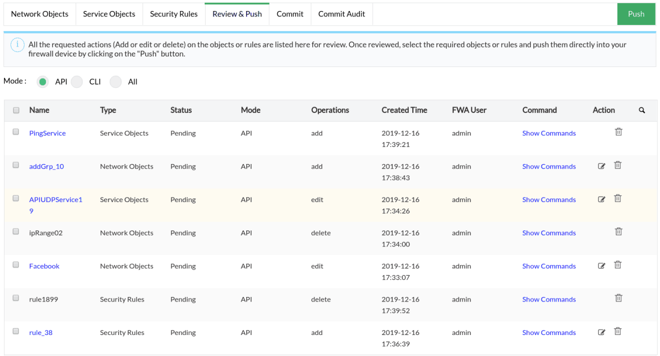
○ Local Rules ● Firewall Rules

Rule Number/ID	Access Layer	Source	Destination	Service	VPN	Rule Action
Cleanup rule	Network	Any	Any	Any	Any	✎ 🗑
allowAll	Network	Any	Any	Any	Any	✎ 🗑
rule 1	Network	networkObj	Host	srvGroup tcpSrv udpSrv	Any	✎ 🗑

Page 1 of 1 50 View 1 - 3 of 3

Agregue, modifique y elimine reglas y objetos de red, analice las implicaciones de un cambio propuesto y envíe los cambios directamente al firewall.

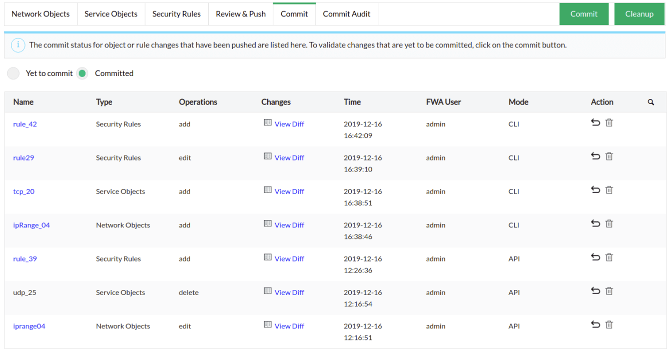
Simplifique la gestión de políticas de firewall automatizando el proceso de administración de reglas de firewall.



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	🗑
□	addGrp_10	Network Objects	Pending	API	add	2019-12-16 17:38:43	admin	Show Commands	✎ 🗑
□	APIUDPService19	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	✎ 🗑



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.

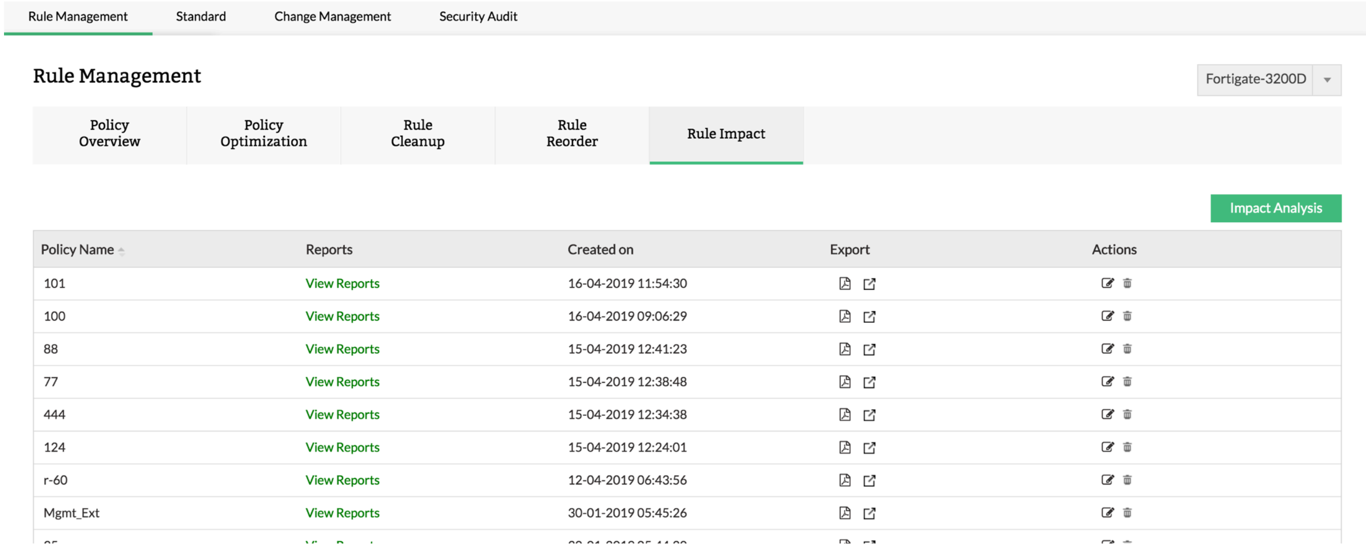
○ Yet to commit ● Committed

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	↶ 🗑
tcp_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	↶ 🗑
udp_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	↶ 🗑

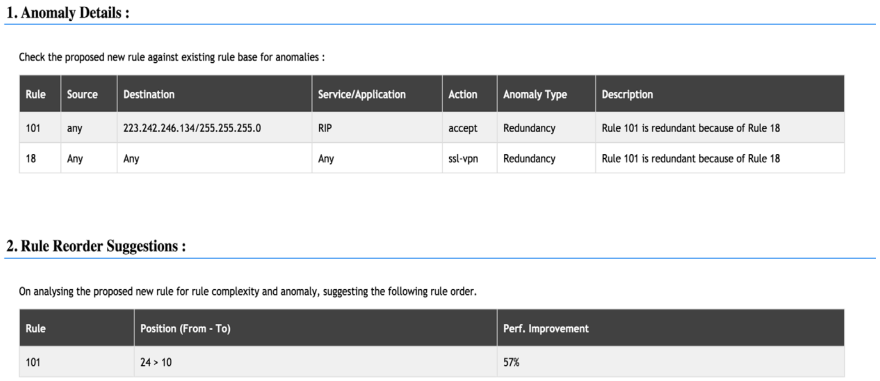
Análisis del impacto de las reglas

Analice detalladamente el impacto de una nueva regla propuesta y determine si la nueva regla propuesta afectará negativamente al conjunto de reglas existente.

Utilice el análisis de impacto para identificar las amenazas, comprender los riesgos, determinar las anomalías y optimizar la nueva regla propuesta.



Policy Name	Reports	Created on	Export	Actions
101	View Reports	16-04-2019 11:54:30		
100	View Reports	16-04-2019 09:06:29		
88	View Reports	15-04-2019 12:41:23		
77	View Reports	15-04-2019 12:38:48		
444	View Reports	15-04-2019 12:34:38		
124	View Reports	15-04-2019 12:24:01		
r-60	View Reports	12-04-2019 06:43:56		
Mgmt_Ext	View Reports	30-01-2019 05:45:26		



1. Anomaly Details :

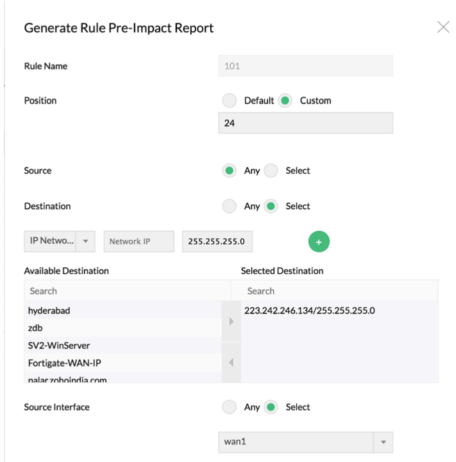
Check the proposed new rule against existing rule base for anomalies :

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

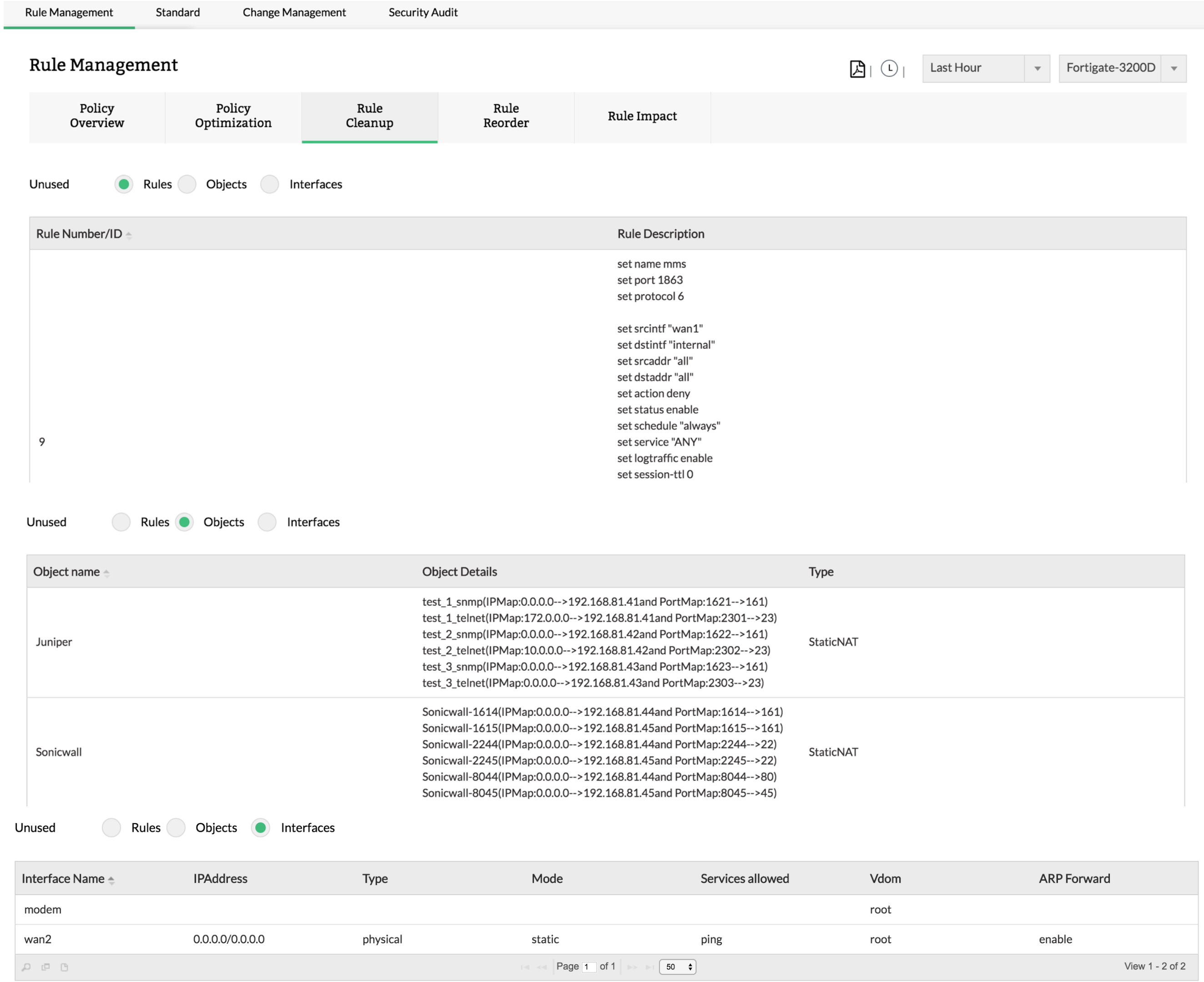
IP Netwo... | Network IP | 255.255.255.0 | +

Available Destination: hyderabad, zdb, SV2-WinServer, Fortigate-WAN-IP, palar.zohoindia.com

Selected Destination: 223.242.246.134/255.255.255.0

Source Interface: ○ Any ● Select
wan1

Limpieza de reglas



Unused ● Rules ○ Objects ○ Interfaces

Rule Number/ID	Rule Description
9	set name mms set port 1863 set protocol 6 set srcintf "wan1" set dstintf "internal" set srcaddr "all" set dstaddr "all" set action deny set status enable set schedule "always" set service "ANY" set logtraffic enable set session-ttl 0

Unused ○ Rules ● Objects ○ Interfaces

Object name	Object Details	Type

Juniper	test_1_snmp(IPMap:0.0.0.0-->192.168.81.41and PortMap:1621-->161)
	test_1_telnet(IPMap:172.0.0.0-->192.168.81.41and PortMap:2301-->23)
	test_2_snmp(IPMap:0.0.0.0-->192.168.81.42and PortMap:1622-->161)
	test_2_telnet(IPMap:10.0.0.0-->192.168.81.42and PortMap:2302-->23)
	test_3_snmp(IPMap:0.0.0.0-->192.168.81.43and PortMap:1623-->161)
	test_3_telnet(IPMap:0.0.0.0-->192.168.81.43and PortMap:2303-->23)
		StaticNAT

Sonicwall	Sonicwall-1614(IPMap:0.0.0.0-->192.168.81.44and PortMap:1614-->161)
	Sonicwall-1615(IPMap:0.0.0.0-->192.168.81.45and PortMap:1615-->161)
	Sonicwall-2244(IPMap:0.0.0.0-->192.168.81.44and PortMap:2244-->22)
	Sonicwall-2245(IPMap:0.0.0.0-->192.168.81.45and PortMap:2245-->22)
	Sonicwall-8044(IPMap:0.0.0.0-->192.168.81.44and PortMap:8044-->80)
	Sonicwall-8045(IPMap:0.0.0.0-->192.168.81.45and PortMap:8045-->45)
		StaticNAT

Unused ○ Rules ○ Objects ● Interfaces

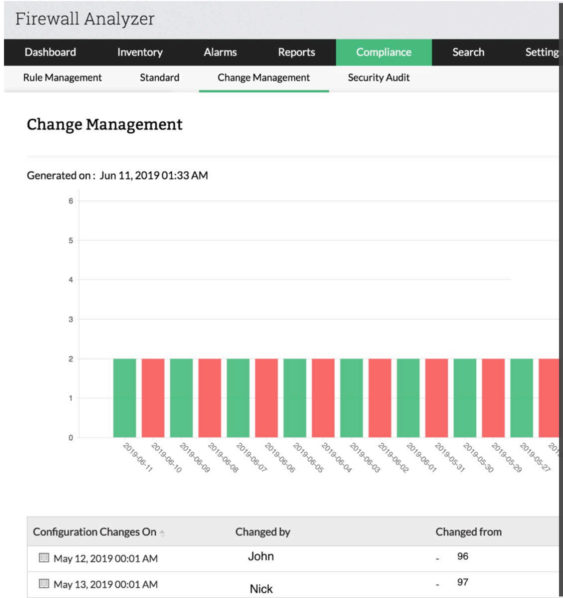
Interface Name	IPAddress	Type	Mode	Services allowed	Vdom	ARP Forward
modem					root	
wan2	0.0.0.0/0.0.0.0	physical	static	ping	root	enable

Page 1 of 1 50 View 1 - 2 of 2

Reduzca las amenazas de seguridad al identificar las reglas, objetos e interfaces de firewall no utilizados.

Obtenga un resumen general de alto nivel de cuáles reglas, objetos e interfaces se pueden eliminar o desactivar.

Gestión de cambios de configuración



Change Management

Generated on : Jun 11, 2019 01:33 AM

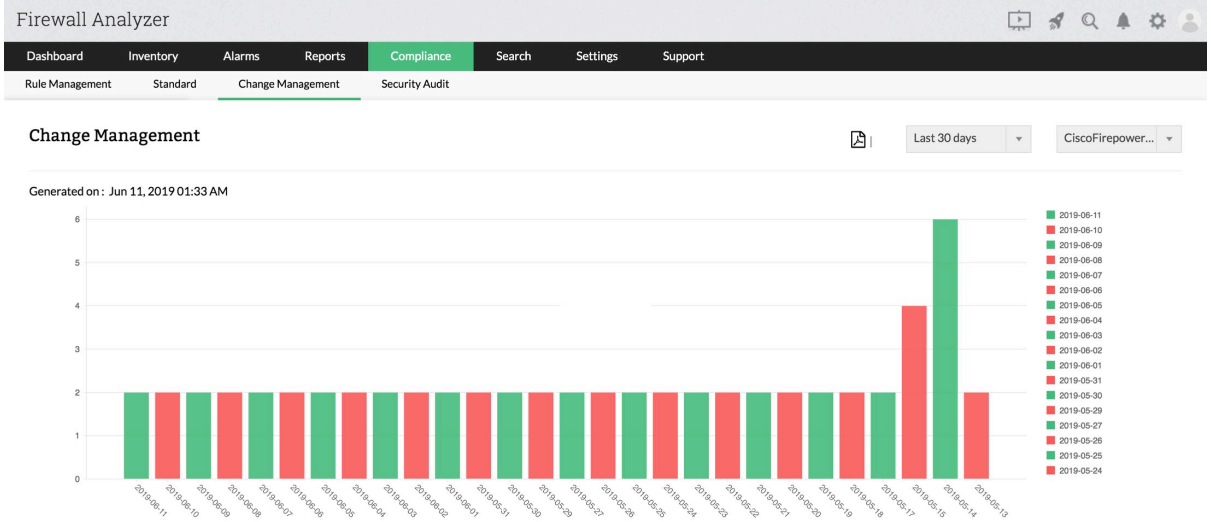
Configuration Changes On	Changed by	Changed from	Version No	Change count	Change Type
May 12, 2019 00:01 AM	John	- 96	97	2	running
May 13, 2019 00:01 AM	Nick	- 97	98	2	running

Importancia de la gestión de cambios

¡Es importante controlar los cambios de manera automática para obtener una mejor visibilidad de la configuración y seguridad de su firewall!

- Elimine el control de cambios manual.
- Proteja su red monitoreando los cambios realizados en la configuración del firewall.
- Las notificaciones de cambios le ayudan a mantenerse alerta.

Control de los cambios de configuración



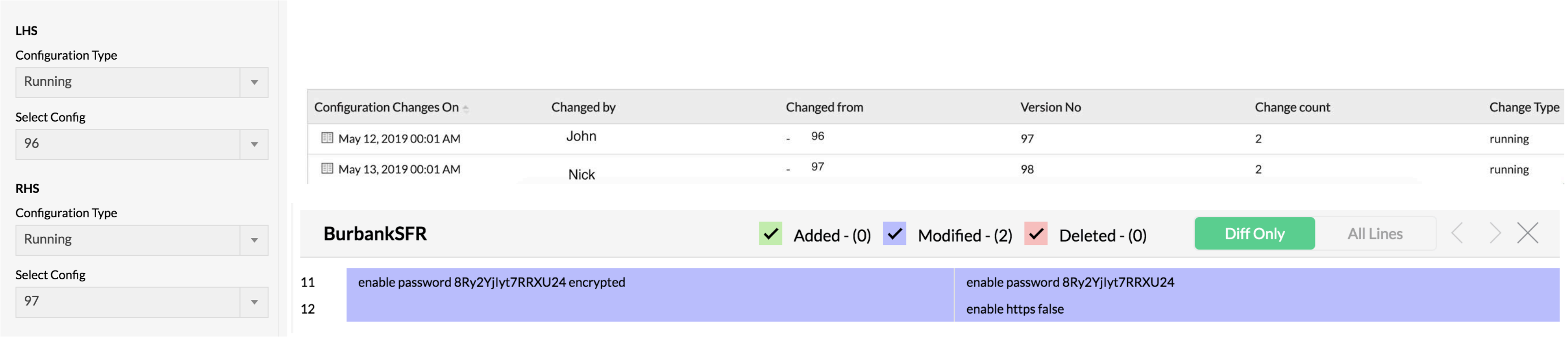
Change Management

Generated on : Jun 11, 2019 01:33 AM

Automatice el control de cambios de configuración en todos sus dispositivos de firewall.

Controle el "qué", "quién" y "cuándo" de los cambios de configuración.

Reciba notificaciones de cambios directamente en su correo.



LHS

Configuration Type: Running

Select Config: 96

RHS

Configuration Type: Running

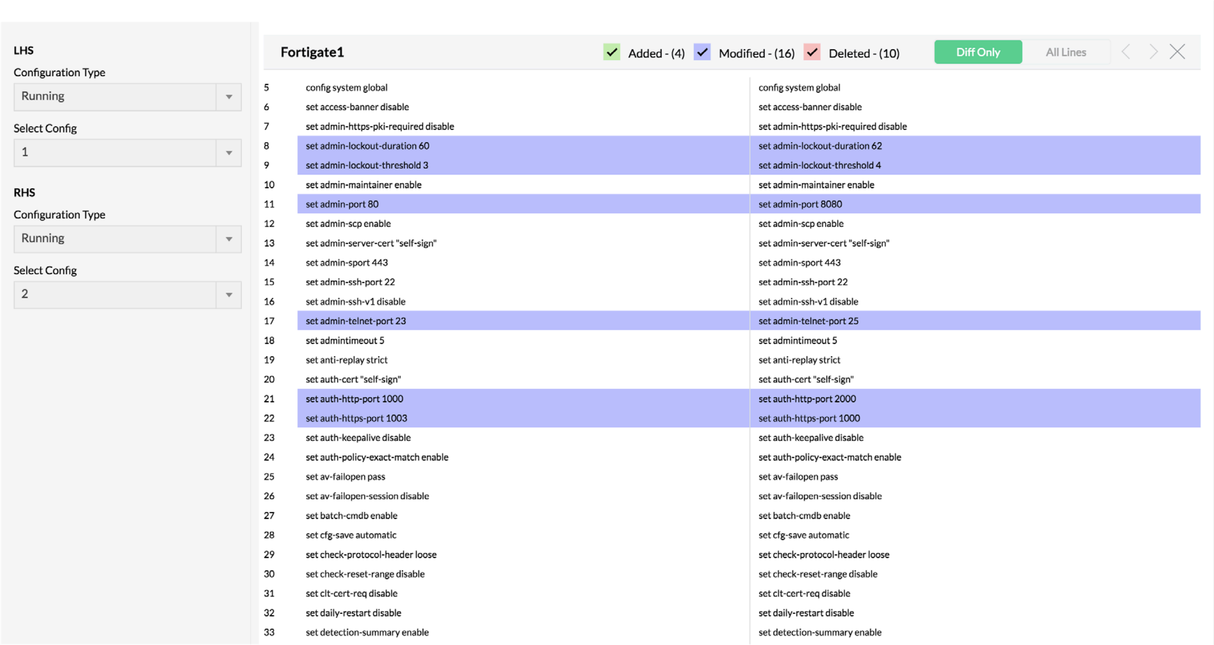
Select Config: 97

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 ✓ Added - (0) ✓ Modified - (2) ✓ Deleted - (0)

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

Comparación de configuración usando la vista de diferencias [diff]



LHS

Configuration Type: Running

Select Config: 1

RHS

Configuration Type: Running

Select Config: 2

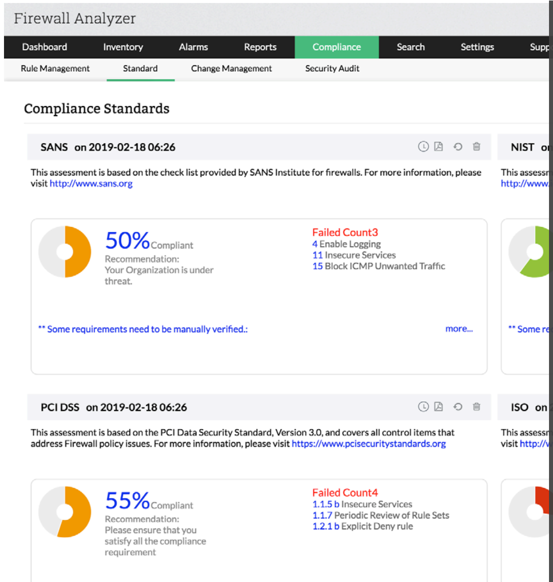
Fortigate1 ✓ Added - (4) ✓ Modified - (16) ✓ Deleted - (10) Diff Only All Lines

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-failopen pass	set av-failopen pass
26	set av-failopen-session disable	set av-failopen-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 clt-cert-req disable	set clt-cert-req disable
32	set daily-restart disable	set daily-restart disable
33	set detection-summary enable	set detection-summary enable

Compare los cambios de configuración entre dos configuraciones, una al lado de la otra, usando la vista de diferencias [diff view].

Identifique fácilmente los cambios entre los archivos de configuración usando una representación de cambios codificada por colores.

Vea las adiciones en verde, las eliminaciones en rojo y las modificaciones en azul.



Firewall Analyzer

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

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

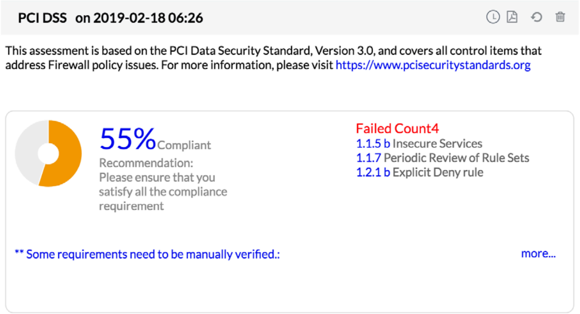
Auditoría de cumplimiento y seguridad

Cumpla con los informes de cumplimiento out-of-the-box

¡Siga las prácticas estándar y aplique políticas de seguridad internas / externas para evitar problemas legales implementando una gestión de cumplimiento adecuada!

- Cumpla con los requisitos reglamentarios PCI-DSS, ISO 27001, NIST, NERC-CIP, SANS.
- Identifique las brechas de configuración y manténgase protegido.
- Genere informes sobre el estado de cumplimiento de los dispositivos de firewall.

Informe de cumplimiento



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

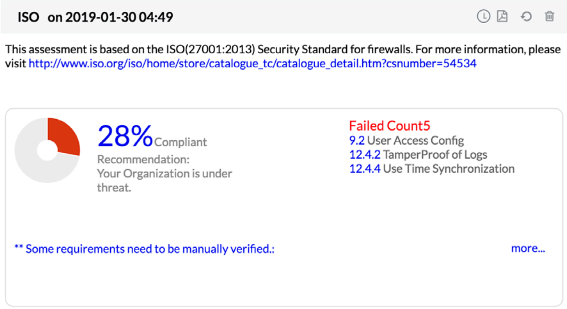
Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count4

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

** Some requirements need to be manually verified.:

more...



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

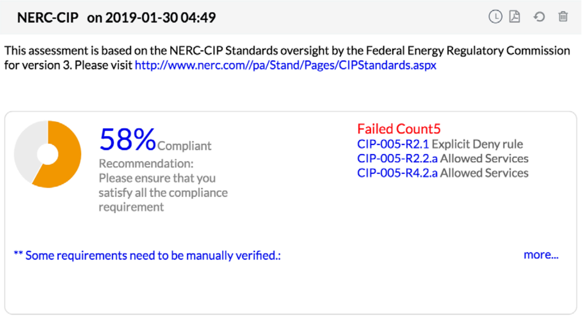
Recommendation: Your Organization is under threat.

Failed Count5

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

** Some requirements need to be manually verified.:

more...



NERC-CIP on 2019-01-30 04:49

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

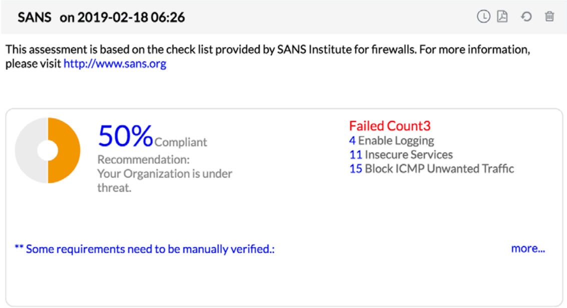
Recommendation: Please ensure that you satisfy all the compliance requirement

Failed Count5

CIP-005-R2.1 Explicit Deny rule
CIP-005-R2.2.a Allowed Services
CIP-005-R4.2.a Allowed Services

** Some requirements need to be manually verified.:

more...



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

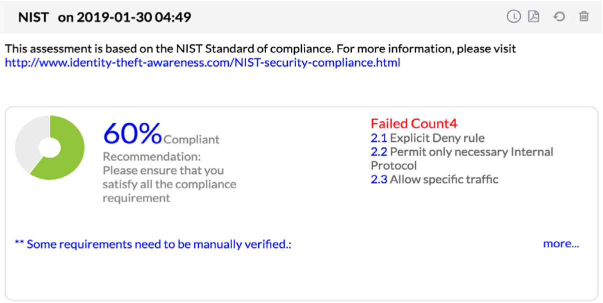
Recommendation: Your Organization is under threat.

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...

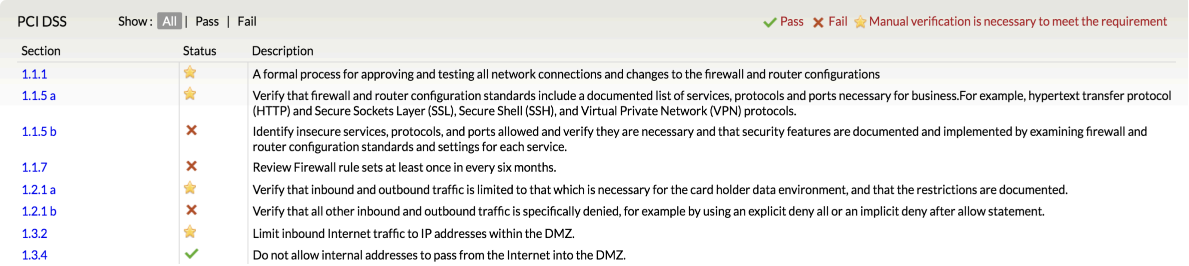
Proteja los datos de los titulares de tarjetas de manera efectiva al cumplir con PCI-DSS.

Domine la gestión de la seguridad de la información, cumpliendo con ISO 27001.

Asegúrese de que su infraestructura de TI crítica esté protegida cumpliendo con el mandato NERC-CIP.

Identifique las brechas de seguridad de la información verificando con el informe SANS.

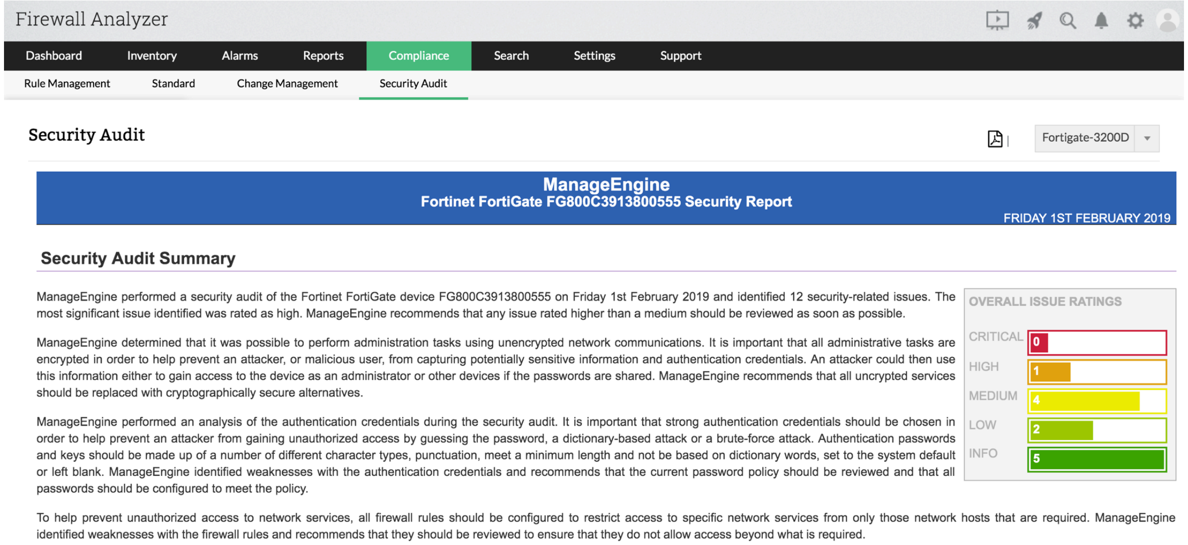
Revise los estándares del NIST con los informes de cumplimiento del NIST.



PCI DSS   Show : All | Pass | Fail   ✓ Pass ✗ Fail ☆ Manual verification is necessary to meet the requirement

Section	Status	Description
1.1.1	☆	A formal process for approving and testing all network connections and changes to the firewall and router configurations
1.1.5 a	☆	Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business.For example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.
1.1.5 b	✗	Identify insecure services, protocols, and ports allowed and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.
1.1.7	✗	Review Firewall rule sets at least once in every six months.
1.2.1 a	☆	Verify that inbound and outbound traffic is limited to that which is necessary for the card holder data environment, and that the restrictions are documented.
1.2.1 b	✗	Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit deny all or an implicit deny after allow statement.
1.3.2	☆	Limit inbound Internet traffic to IP addresses within the DMZ.
1.3.4	✓	Do not allow internal addresses to pass from the Internet into the DMZ.

Auditorías de seguridad



Security Audit

ManageEngine
Fortinet FortiGate FG800C3913800555 Security Report
FRIDAY 1ST FEBRUARY 2019

Security Audit Summary

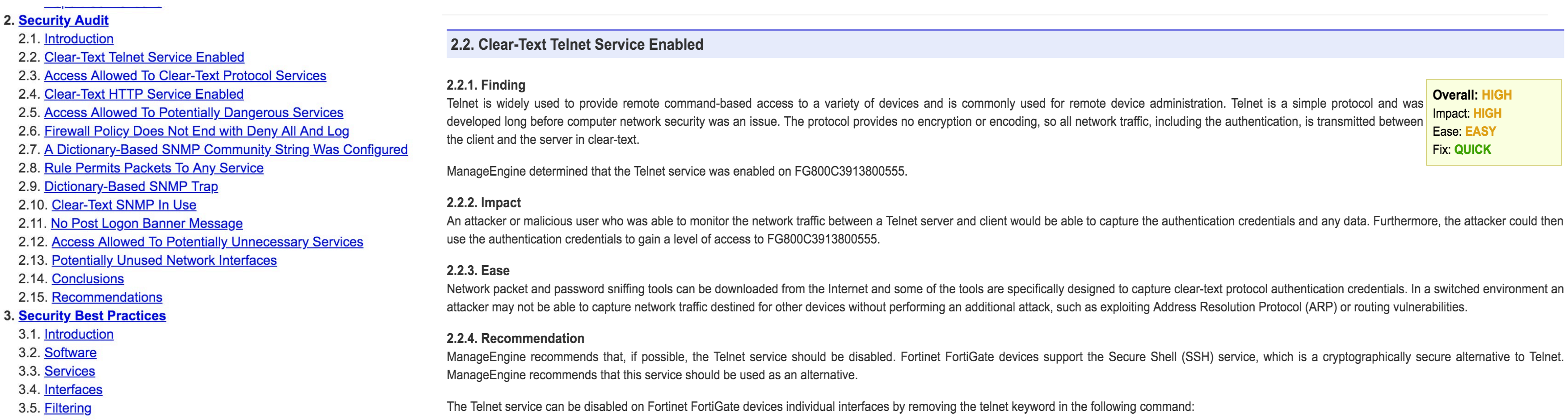
ManageEngine performed a security audit of the Fortinet FortiGate device FG800C3913800555 on Friday 1st February 2019 and identified 12 security-related issues. The most significant issue identified was rated as high. ManageEngine recommends that any issue rated higher than a medium should be reviewed as soon as possible.

ManageEngine determined that it was possible to perform administration tasks using unencrypted network communications. It is important that all administrative tasks are encrypted in order to help 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 shared. ManageEngine recommends that all uncrypted services should be replaced with cryptographically secure alternatives.

ManageEngine performed an analysis of the authentication credentials during the security audit. It is important that strong authentication credentials should be chosen in order to help prevent an attacker from gaining unauthorized access by guessing the password, a dictionary-based attack 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 weaknesses with the authentication credentials and recommends that the current password policy should be reviewed and that all passwords should be configured to meet the policy.

OVERALL ISSUE RATINGS	
CRITICAL	0
HIGH	1
MEDIUM	4
LOW	2
INFO	5

To help prevent unauthorized access to network services, all firewall rules should be configured to restrict access to specific network services from only those network hosts that are required. ManageEngine identified weaknesses with the firewall rules and recommends that they should be reviewed to ensure that they do not allow access beyond what is required.



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.

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

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.

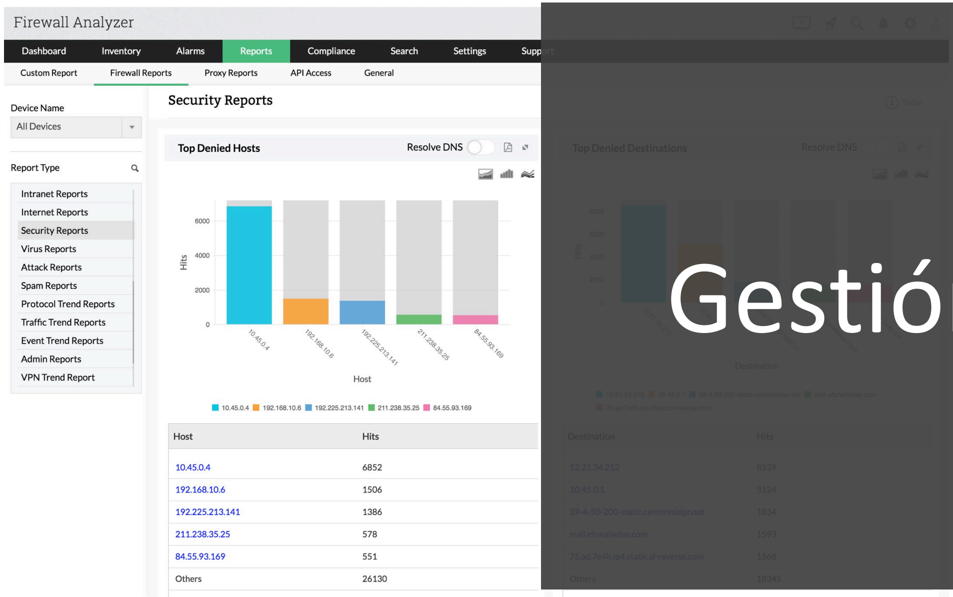
The Telnet service can be disabled on Fortinet FortiGate devices individual interfaces by removing the telnet keyword in the following command:

Realice auditorías de seguridad en el entorno de configuración de su firewall y obtenga informes detallados sobre las brechas de seguridad.

Determine la criticidad de las brechas de configuración y también la facilidad de ataque.

Obtenga recomendaciones sobre las mejores prácticas de la industria.

Gestión de logs



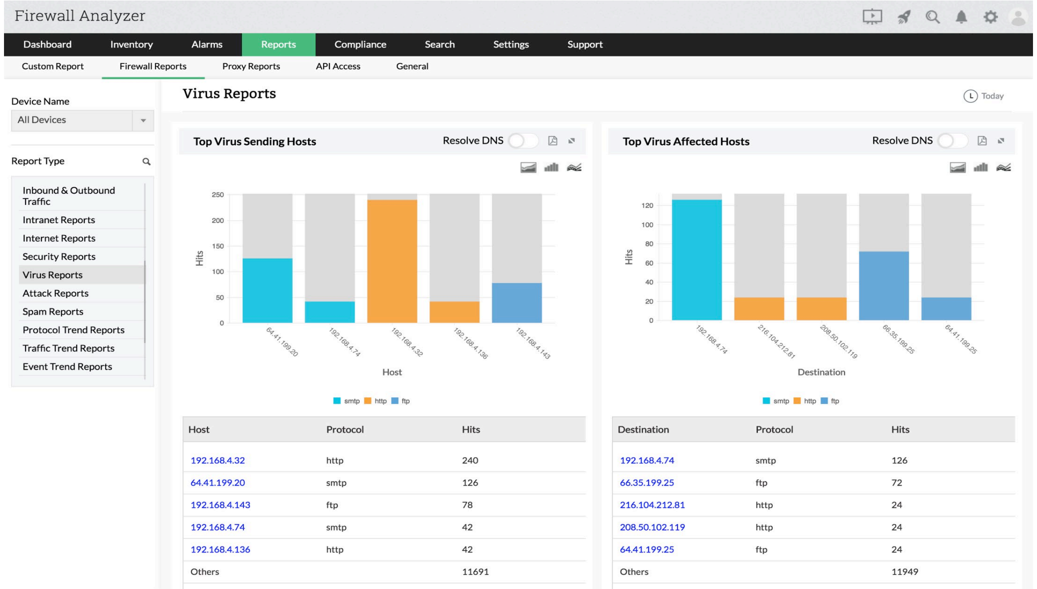
Host	Hits
10.45.0.4	6852
192.168.10.6	1506
192.225.213.141	1386
211.238.35.25	578
84.55.93.169	551
Others	26130

La gestión de logs es crucial para la seguridad de la red

Analizar los datos de syslog lo ayudará a identificar y prevenir las amenazas de seguridad en tiempo real

- El análisis de seguridad ayuda a identificar las amenazas internas y externas.
- El análisis de tráfico ayuda a gestionar el ancho de banda.
- Las alertas basadas en logs ayudan a solucionar los problemas instantáneamente.

Análisis de seguridad



Virus Reports

Top Virus Sending Hosts

Host	Protocol	Hits
192.168.4.32	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		11691

Top Virus Affected Hosts

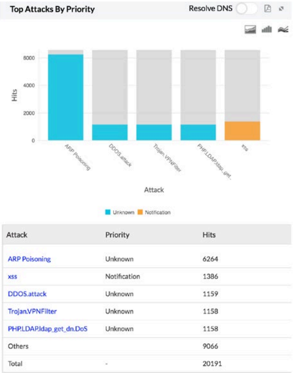
Destination	Protocol	Hits
192.168.4.74	smtp	126
66.35.199.25	ftp	72
216.104.212.81	http	24
208.50.102.119	http	24
64.41.199.25	ftp	24
Others		11949

Genere informes detallados sobre las posibles amenazas de seguridad para la red.

Solucione y resuelva los problemas de seguridad más rápido identificando y analizando logs relacionados con virus.

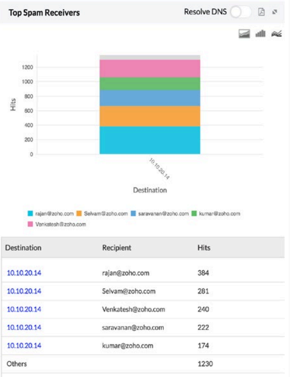
Obtenga información para identificar y contrarrestar los ataques a la red.

Obtenga información detallada sobre la actividad de spam y controle el spam en toda la red.



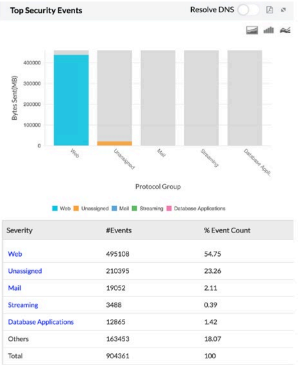
Top Attacks By Priority

Attack	Priority	Hits
ARP Poisoning	Unknown	6264
xss	Notification	1386
DDOS.attack	Unknown	1159
Trojan.VPNFilter	Unknown	1158
PHP.LDAP.ldap_get_dn.DoS	Unknown	1158
Others		9066
Total	-	20191



Top Spam Receivers

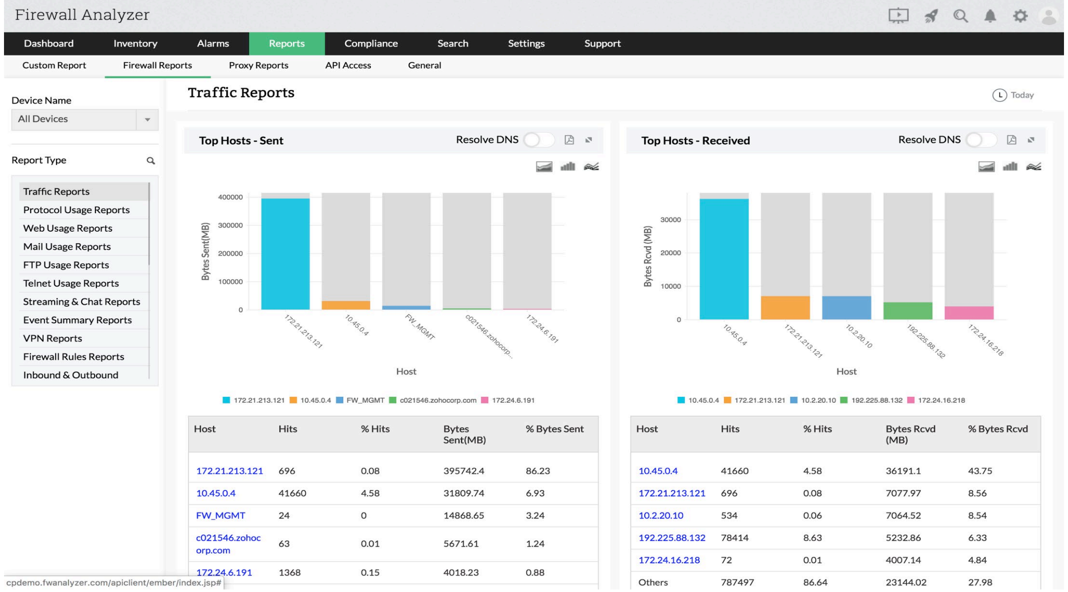
Destination	Recipient	Hits
10.10.20.14	rajan@zoho.com	384
10.10.20.14	Selvam@zoho.com	281
10.10.20.14	Venkatesh@zoho.com	240
10.10.20.14	saravanan@zoho.com	222
10.10.20.14	kumar@zoho.com	174
Others		1230



Top Security Events

Severity	#Events	% Event Count
Web	495108	54.75
Unassigned	210395	23.26
Mail	19052	2.11
Streaming	3488	0.39
Database Applications	12865	1.42
Others	163453	18.07
Total	904361	100

Análisis de tráfico

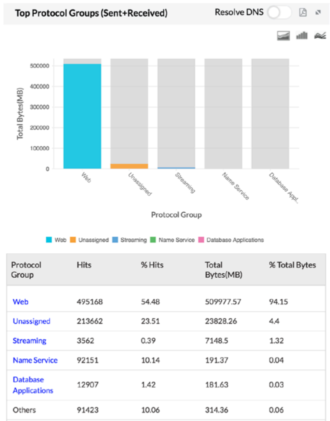


Host	Hits	% Hits	Bytes Sent(MB)	% Bytes Sent
172.21.213.121	696	0.08	395742.4	86.23
10.45.0.4	41660	4.58	31809.74	6.93
FW_MGMT	24	0	14868.65	3.24
c021546.zohocorp.com	63	0.01	5671.61	1.24
172.24.6.191	1368	0.15	4018.23	0.88

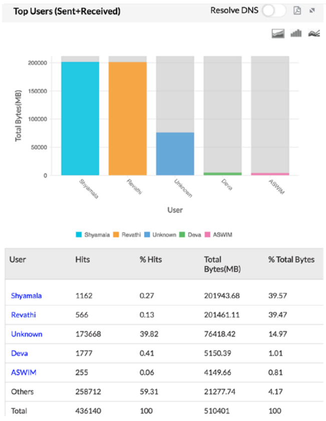
Host	Hits	% Hits	Bytes Rcvd (MB)	% Bytes Rcvd
10.45.0.4	41660	4.58	36191.1	43.75
172.21.213.121	696	0.08	7077.97	8.56
10.2.20.10	534	0.06	7064.52	8.54
192.225.88.132	78414	8.63	5232.86	6.33
172.24.16.218	72	0.01	4007.14	4.84
Others	787497	86.64	23144.02	27.98

Los informes de tráfico de Firewall Analyzer ayudan a responder las siguientes preguntas

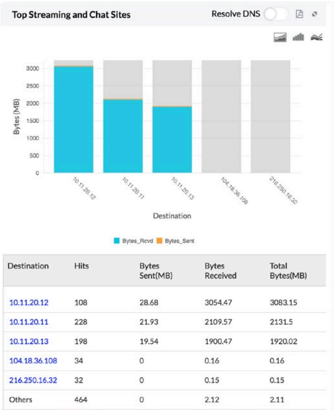
- ¿Quién está enviando, recibiendo el tráfico?
- ¿Cuál host está enviando, recibiendo el tráfico?
- ¿Cuál es la cuota de tráfico de varios grupos de protocolos?
- ¿Cuál es el patrón de gravedad de los eventos debido al tráfico?



Protocol Group	Hits	% Hits	Total Bytes(MB)	% Total Bytes
Web	495168	54.48	509977.57	94.15
Unassigned	213662	23.51	23828.26	4.4
Streaming	3562	0.39	7148.5	1.32
Name Service	92151	10.14	191.37	0.04
Database Applications	12907	1.42	181.63	0.03
Others	91423	10.06	314.36	0.06

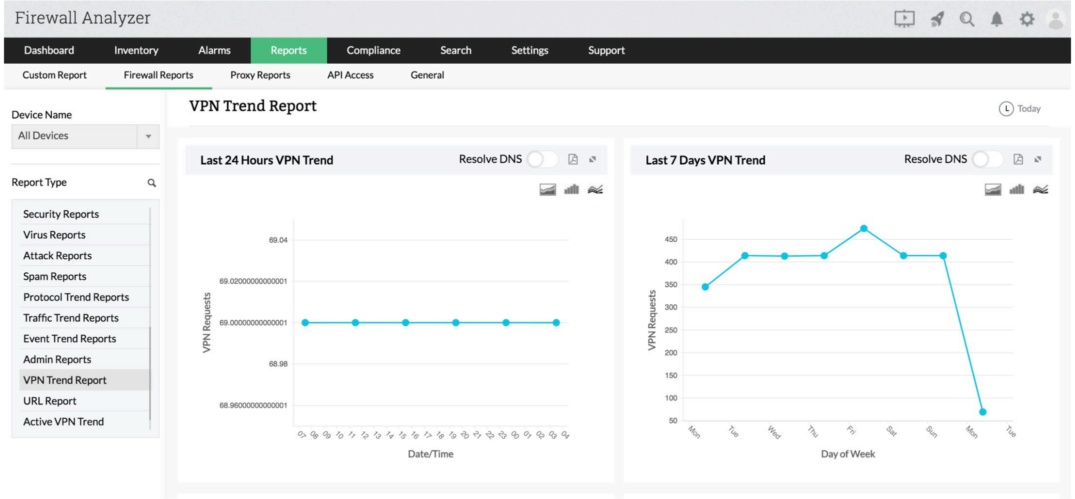


User	Hits	% Hits	Total Bytes(MB)	% Total Bytes
Shyamala	1162	0.27	201943.68	39.57
Revathi	566	0.13	201461.11	39.47
Unknown	173668	39.82	76418.42	14.97
Deva	1777	0.41	5150.39	1.01
ASWIM	255	0.06	4149.66	0.81
Others	258712	59.31	21277.74	4.17
Total	436140	100	510401	100



Destination	Hits	Bytes Sent(MB)	Bytes Received	Total Bytes(MB)
10.11.20.12	108	28.68	3054.47	3083.15
10.11.20.11	228	21.93	2109.57	2131.5
10.11.20.13	198	19.54	1900.47	1920.02
104.18.36.108	34	0	0.16	0.16
216.250.16.32	32	0	0.15	0.15
Others	464	0	2.12	2.11

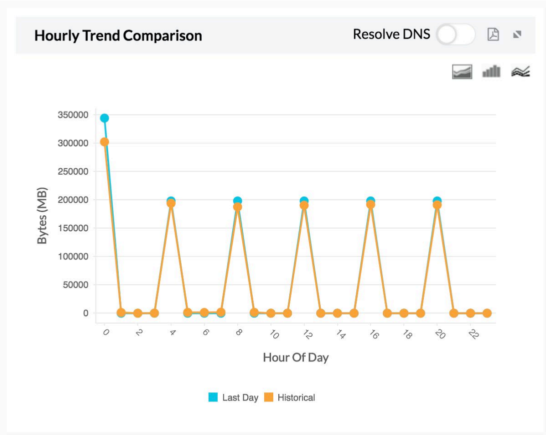
Análisis de tendencias

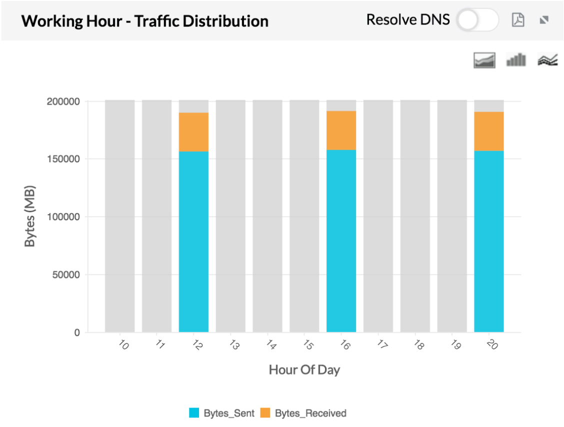


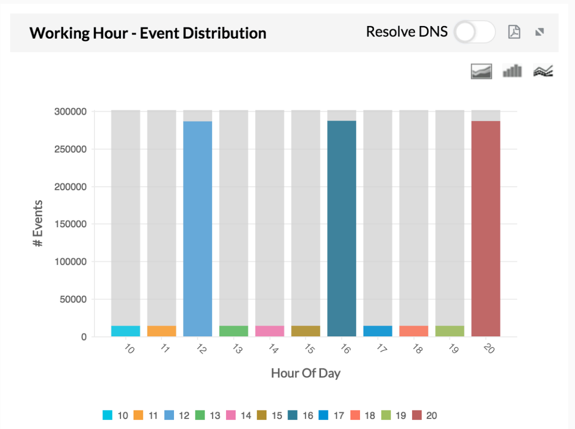
Determine la tendencia de uso de ancho de banda máximo en diferentes protocolos y marcas de tiempo.

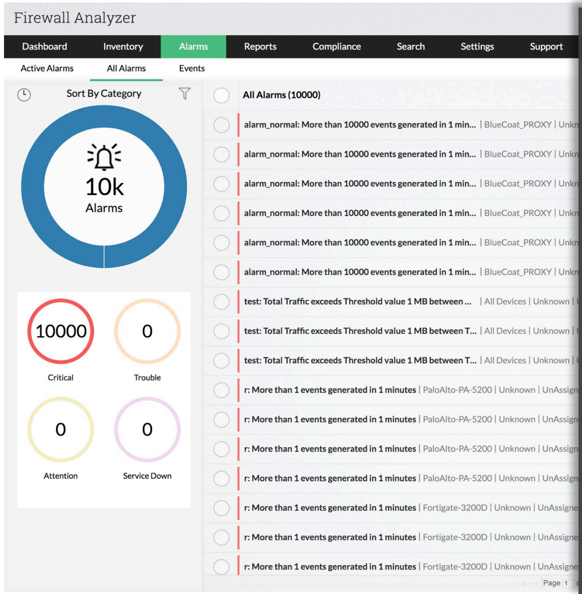
Solucione los problemas de conexión e identifique los riesgos de seguridad analizando el informe de tendencias de eventos.

Identifique las conexiones VPN activas y los riesgos de seguridad relacionados con la VPN utilizando el informe de tendencias de VPN.









Firewall Analyzer

All Alarms (10000)

alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unkn

alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unkn

alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unkn

alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unkn

alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unkn

alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unkn

test: Total Traffic exceeds Threshold value 1 MB between ... | All Devices | Unknown |

test: Total Traffic exceeds Threshold value 1 MB between T... | All Devices | Unknown |

test: Total Traffic exceeds Threshold value 1 MB between T... | All Devices | Unknown |

r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssign

r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssign

r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssign

r: More than 1 events generated in 1 minutes | PaloAlto-PA-5200 | Unknown | UnAssign

r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigne

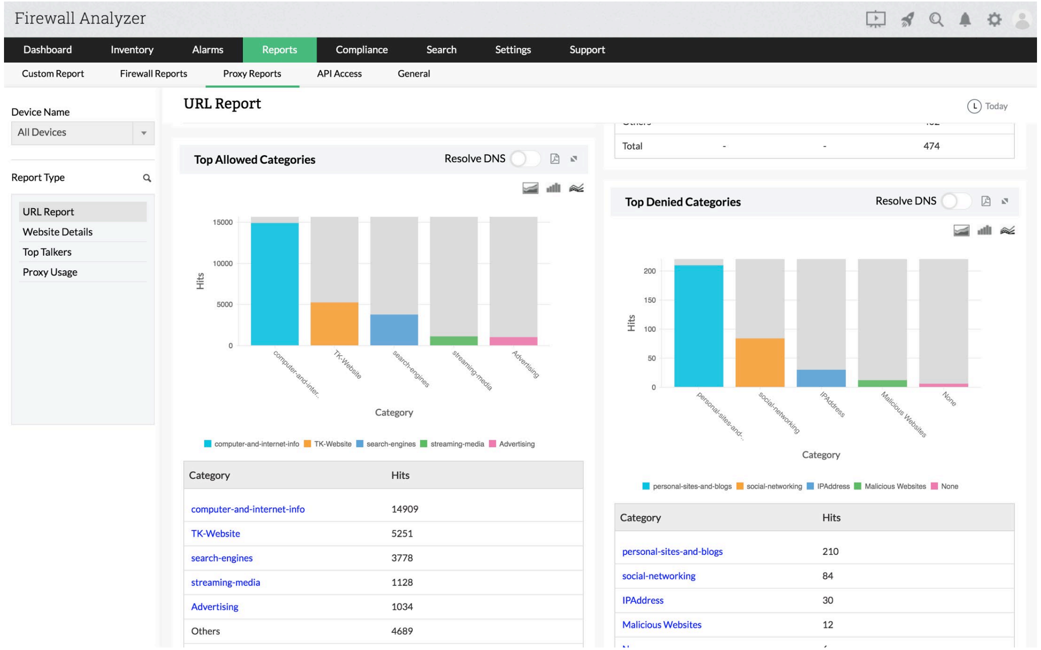
r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigne

r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigne

Page 1

Otras funciones destacadas

Informe de VPN y proxy



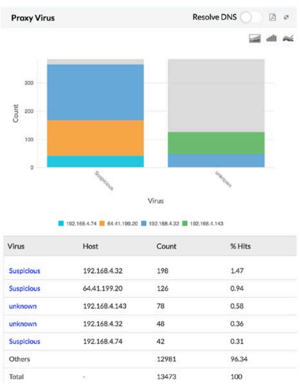
Total	-	-	474

Category	Hits
computer-and-internet-info	14909
TK-Website	5251
search-engines	3778
streaming-media	1128
Advertising	1034
Others	4689

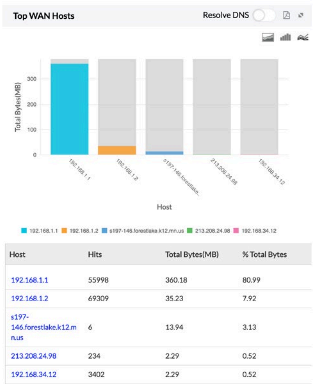
Category	Hits
personal-sites-and-blogs	210
social-networking	84
IPAddress	30
Malicious Websites	12

Identifique a los usuarios conectados a su VPN, el tráfico que consumen y también los inicios de sesión de VPN fallidos.

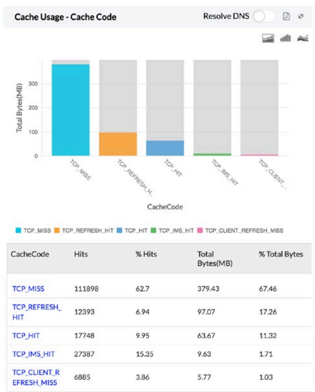
Recopile y archive los logs del servidor proxy, analícelos y genere informes útiles con información corporativa de acceso a Internet.



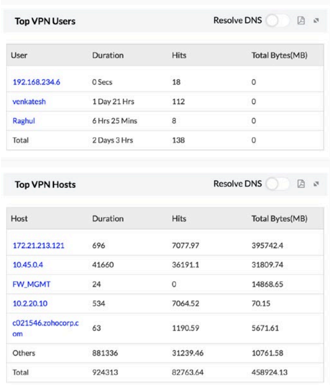
Virus	Host	Count	% Hits
Suspicious	192.168.4.32	198	1.47
Suspicious	64.41.199.20	126	0.94
unknown	192.168.4.143	78	0.58
unknown	192.168.4.32	48	0.36
Suspicious	192.168.4.74	42	0.31
Others		12981	96.34
Total	-	13473	100



Host	Hits	Total Bytes(MB)	% Total Bytes
192.168.1.1	55998	360.18	80.99
192.168.1.2	69309	35.23	7.92
s197-146.forestlake.k12.mn.us	6	13.94	3.13
213.208.24.98	234	2.29	0.52
192.168.34.12	3402	2.29	0.52

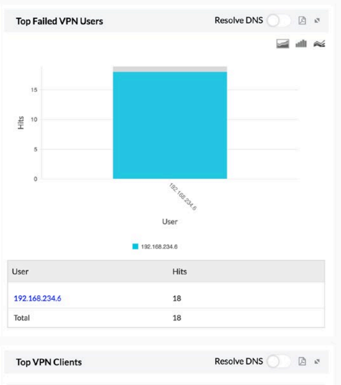


CacheCode	Hits	% Hits	Total Bytes(MB)	% Total Bytes
TCP_MISS	111898	62.7	379.43	67.46
TCP_REFRESH_HIT	12393	6.94	97.07	17.26
TCP_HIT	17748	9.95	63.67	11.32
TCP_IMS_HIT	27387	15.35	9.63	1.71
TCP_CLIENT_REFRESH_MISS	6885	3.86	5.77	1.03



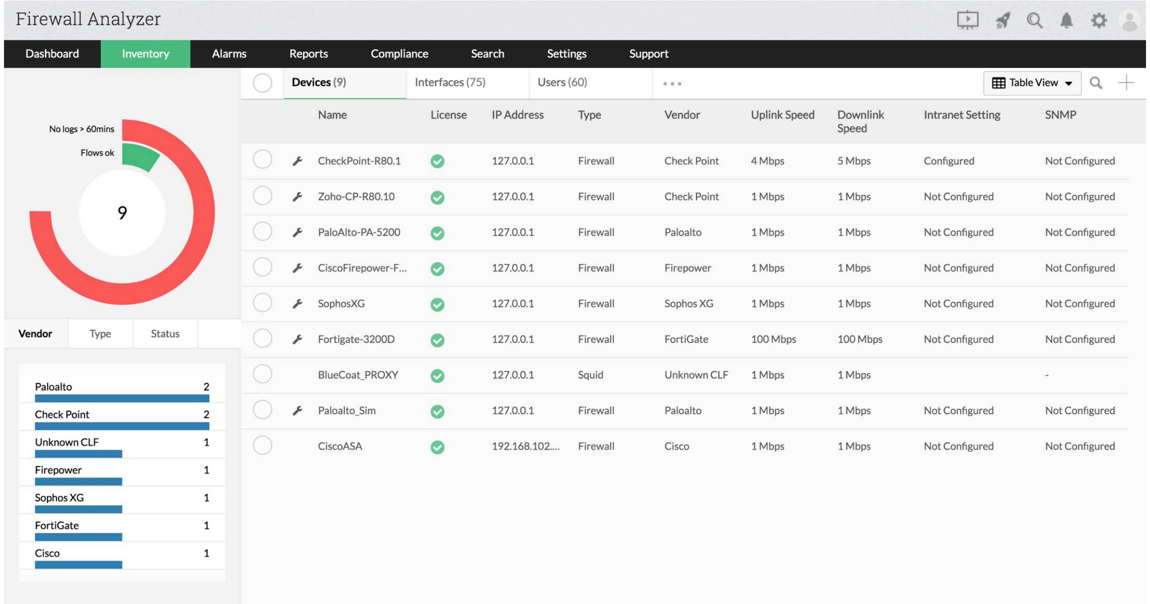
User	Duration	Hits	Total Bytes(MB)
192.168.234.6	0 Secs	18	0
venkatesh	1 Day 21 Hrs	112	0
Raghul	6 Hrs 25 Mins	8	0
Total	2 Days 3 Hrs	138	0

Host	Duration	Hits	Total Bytes(MB)
172.21.213.121	696	7077.97	395742.4
10.45.0.4	41660	36191.1	31809.74
FW_MGMT	24	0	14868.65
10.2.20.10	534	7064.52	70.15
c021546.zohocorp.com	63	1190.59	5671.61
Others	881336	31239.46	10761.58
Total	924313	82763.64	458924.13



User	Hits
192.168.234.6	18
Total	18

Informe de inventario



		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	✓	192.168.102....	Firewall	Cisco	1 Mbps	1 Mbps	Not Configured	Not Configured

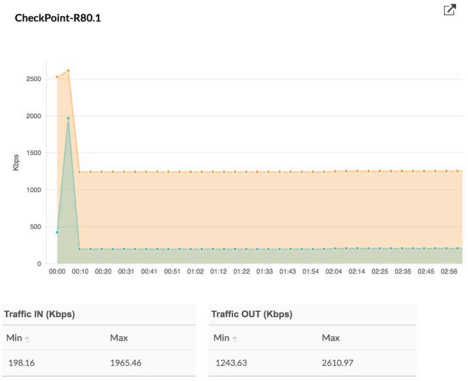
Paloalto	2
Check Point	2
Unknown CLF	1
Firepower	1
Sophos XG	1
FortiGate	1
Cisco	1

Obtenga una imagen completa de todo lo que sucede en los firewalls individuales.

Obtenga visibilidad sobre las interfaces que se encuentran en los dispositivos de firewall configurados.

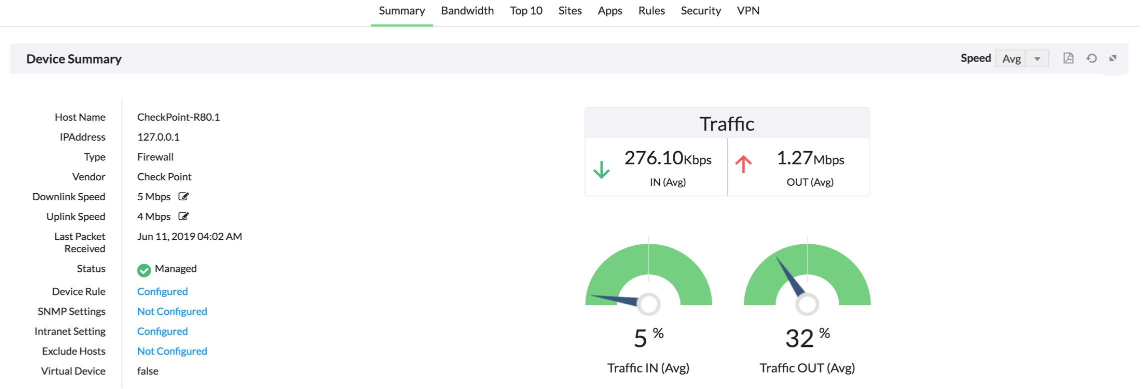
Obtenga un resumen general de todos los usuarios que han accedido a Internet a través de dispositivos de firewall individuales.

Monitoree las reglas y los servicios en la nube a los que se accede con un dispositivo de firewall específico.



Traffic IN (Kbps)	
Min	Max
198.16	1965.46

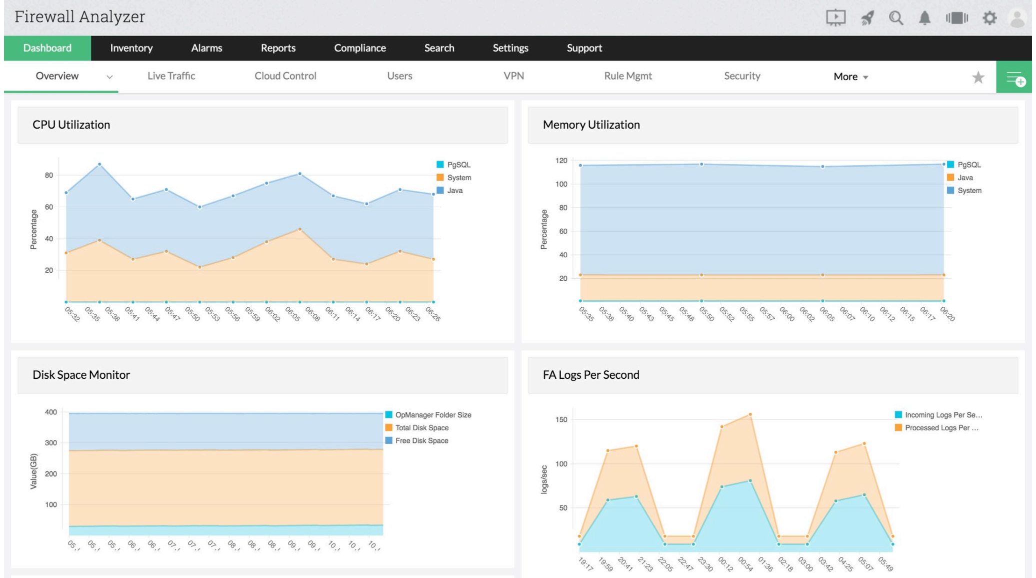
Traffic OUT (Kbps)	
Min	Max
1243.63	2610.97



Device Summary

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

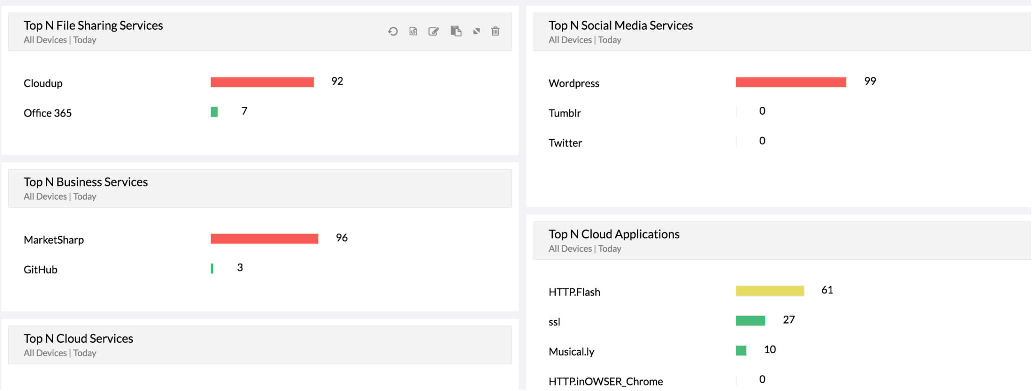
Dashboard, monitoreo en la nube y alarmas



Obtenga una imagen de alto nivel de todo lo que sucede en su entorno de firewall.

Mantenga un control estricto de todos los servicios en la nube que se ejecutan en su red.

Active alertas basadas en umbrales (tanto de tráfico como de seguridad) y reciba notificaciones directamente en su correo o teléfono.



Top N File Sharing Services
All Devices | Today

Cloudup	92
Office 365	7

Top N Business Services
All Devices | Today

MarketSharp	96
GitHub	3

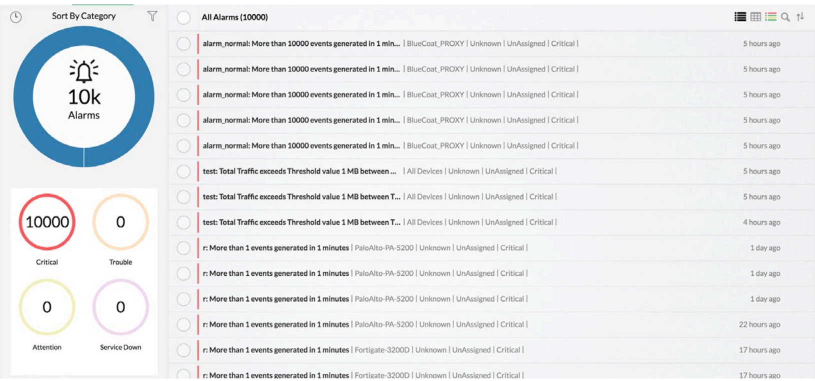
Top N Cloud Services
All Devices | Today

Top N Social Media Services
All Devices | Today

Wordpress	99
Tumblr	0
Twitter	0

Top N Cloud Applications
All Devices | Today

HTTP.Flash	61
ssl	27
Musical.ly	10
HTTP.inOWSER_Chrome	0



All Alarms (10000)

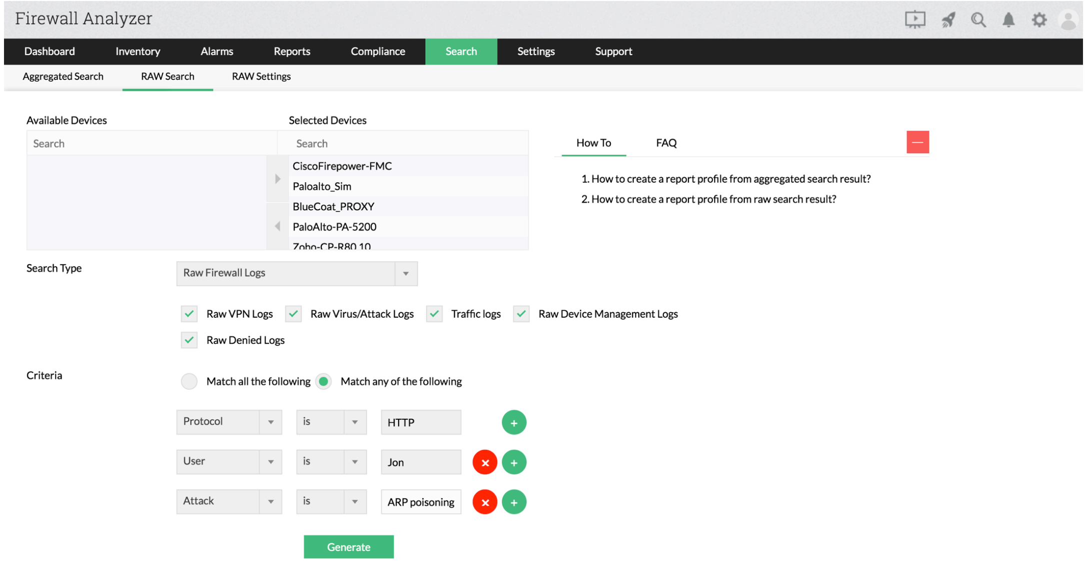
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical | 5 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical | 5 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical | 5 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical | 5 hours ago
alarm_normal: More than 10000 events generated in 1 min... | BlueCoat_PROXY | Unknown | UnAssigned | Critical | 5 hours ago
test: Total Traffic exceeds Threshold value 1 MB between ... | All Devices | Unknown | UnAssigned | Critical | 5 hours ago
test: Total Traffic exceeds Threshold value 1 MB between T... | All Devices | Unknown | UnAssigned | Critical | 5 hours ago
test: Total Traffic exceeds Threshold value 1 MB between T... | All Devices | Unknown | UnAssigned | Critical | 4 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 | 22 hours ago
r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigned | Critical | 17 hours ago
r: More than 1 events generated in 1 minutes | Fortigate-3200D | Unknown | UnAssigned | Critical | 17 hours ago

Análisis forense de logs e informes personalizados

Busque en los logs de Firewall sin procesar para identificar cuál entrada de log causó la actividad de seguridad.

Los logs archivados se pueden importar y los incidentes de seguridad se pueden recopilar buscando en los logs sin procesar.

Genere informes personalizados basados en criterios específicos. Elija los subinformes que desea incluir en el informe personalizado, los parámetros exactos que se incluirán e incluso el diseño del gráfico que se generará.



Available Devices: Search

Selected Devices: Search
- CiscoFirepower-FMC
- Paloalto_Sim
- BlueCoat_PROXY
- PaloAlto-PA-5200
- Zoho-CP-R80.10

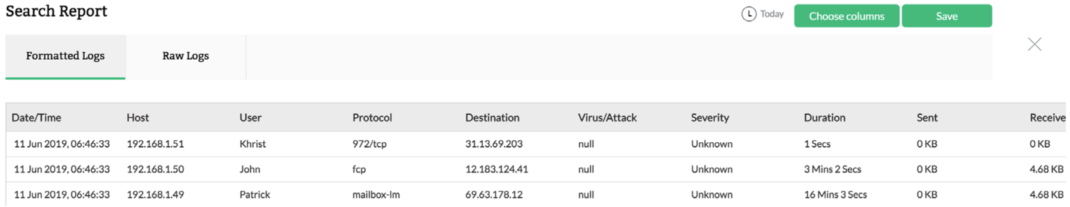
1. How to create a report profile from aggregated search result?
2. How to create a report profile from raw search result?

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

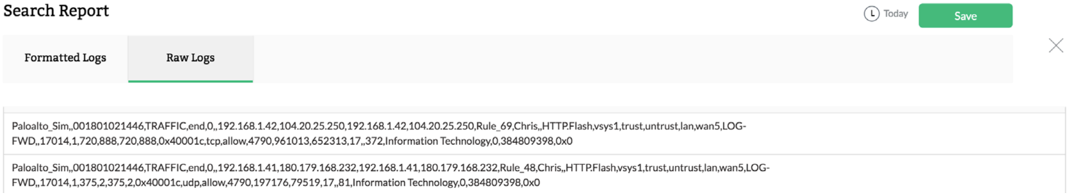
Protocol	is	HTTP
User	is	Jon
Attack	is	ARP poisoning



Search Report

Formatted Logs | Raw Logs

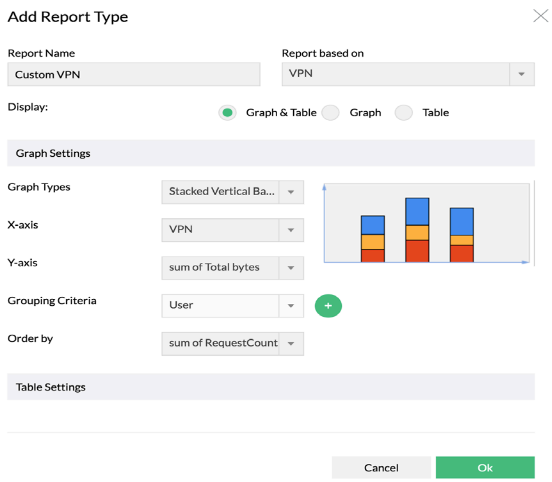
Date/Time	Host	User	Protocol	Destination	Virus/Attack	Severity	Duration	Sent	Receive
11 Jun 2019, 06:46:33	192.168.1.51	Khrist	972/tcp	31.13.69.203	null	Unknown	1 Secs	0 KB	0 KB
11 Jun 2019, 06:46:33	192.168.1.50	John	fcp	12.183.124.41	null	Unknown	3 Mins 2 Secs	0 KB	4.68 KB
11 Jun 2019, 06:46:33	192.168.1.49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



Search Report

Formatted Logs | Raw Logs

```
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,,HTTP.Flash,vsys1,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,,HTTP.Flash,vsys1,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
```



Add Report Type

Report Name: Custom VPN

Report based on: VPN

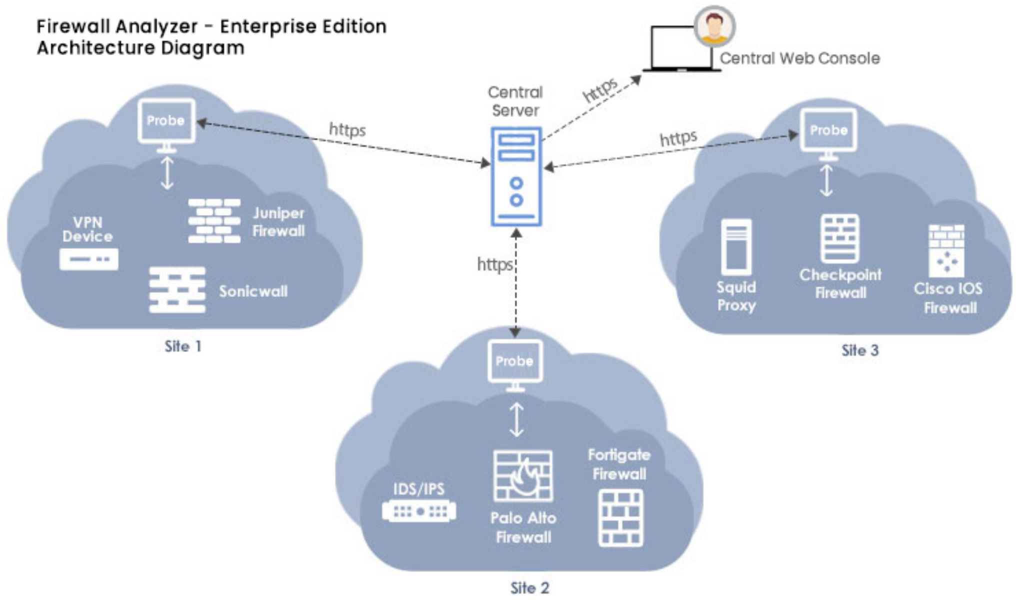
Display: ● Graph & Table ○ Graph ○ Table

Graph Settings

Graph Types	Stacked Vertical Ba...
X-axis	VPN
Y-axis	sum of Total bytes
Grouping Criteria	User
Order by	sum of RequestCount

Table Settings

Beneficios de usar Firewall Analyzer



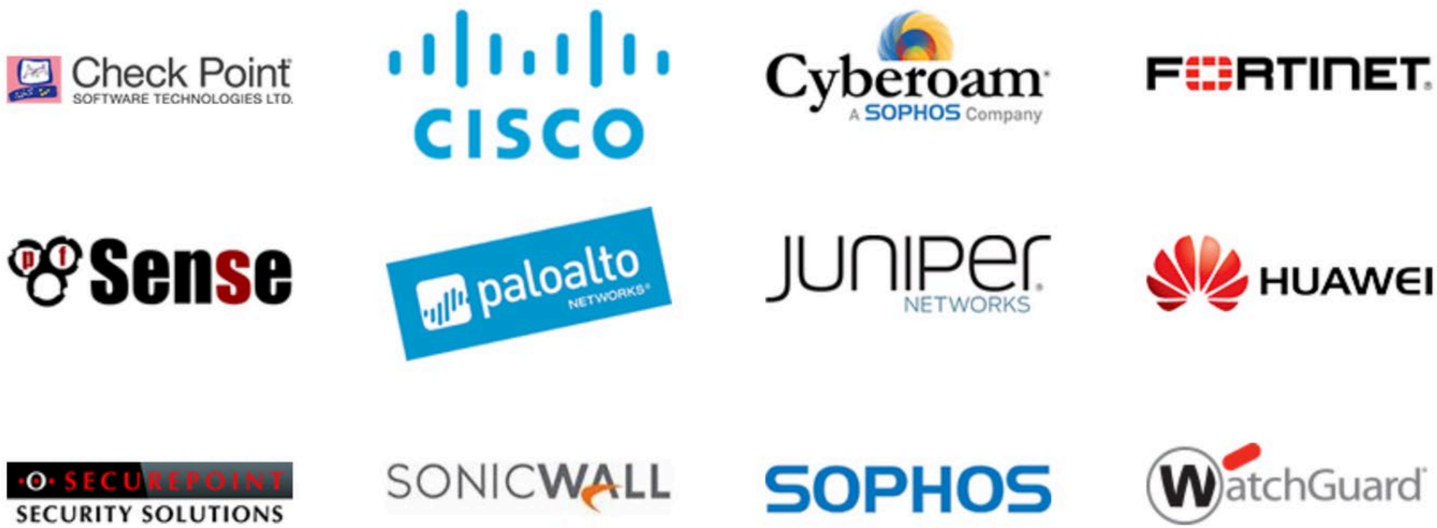
Monitoreo empresarial

Monitoree los firewalls distribuidos geográficamente desde una ubicación centralizada.

Escale fácilmente hasta 1200 dispositivos de seguridad.

Soporte multi firewall

Admite más de 50 proveedores de firewall y 200 dispositivos


Check Point SOFTWARE TECHNOLOGIES LTD.
CISCO
Cyberoam A SOPHOS Company
FORTINET
pfSense
paloalto NETWORKS
JUNIPER NETWORKS
HUAWEI
SECUREPOINT SECURITY SOLUTIONS
SONICWALL
SOPHOS
WatchGuard

Soporte técnico 24*5

¡Soporte técnico 24x5 para que los clientes aprovechen al máximo el producto!

Se integra perfectamente con toda su infraestructura de red

Integracion estrecha con:

- **OpManager:** Monitoreo de redes y servidores
- **NetFlow Analyzer:** Monitoreo del ancho de banda
- **Network Configuration Manager:** Gestión de cumplimiento, configuración y cambios de red
- **OpUtils:** Gestión de puertos de switch y direcciones IP

¿Qué nos hace destacar?

Soporte multi firewall

Alertas de seguridad en tiempo real

Informes out-of-the-box

Altamente escalable

Económico

Soporte técnico 24*5

Requisitos mínimos del sistema

Procesador Pentium Dual Core de 1 GHZ o equivalente

1 GB de RAM

1 GB de almacenamiento

PostgreSQL / MSSQL

Windows / Linux

Los requisitos de espacio en disco y tamaño de RAM dependen de la cantidad de dispositivos que se analizan y la cantidad de dispositivos que envían información de log a Firewall Analyzer.

Consulte: https://www.manageengine.com/latam/firewall/

Gracias

¡Tenga una mejor experiencia de gestión de firewall!

Contacto:

Para precios y más: latam-sales@manageengine.com

Para obtener más información, visite: www.manageengine.com/latam/firewall/