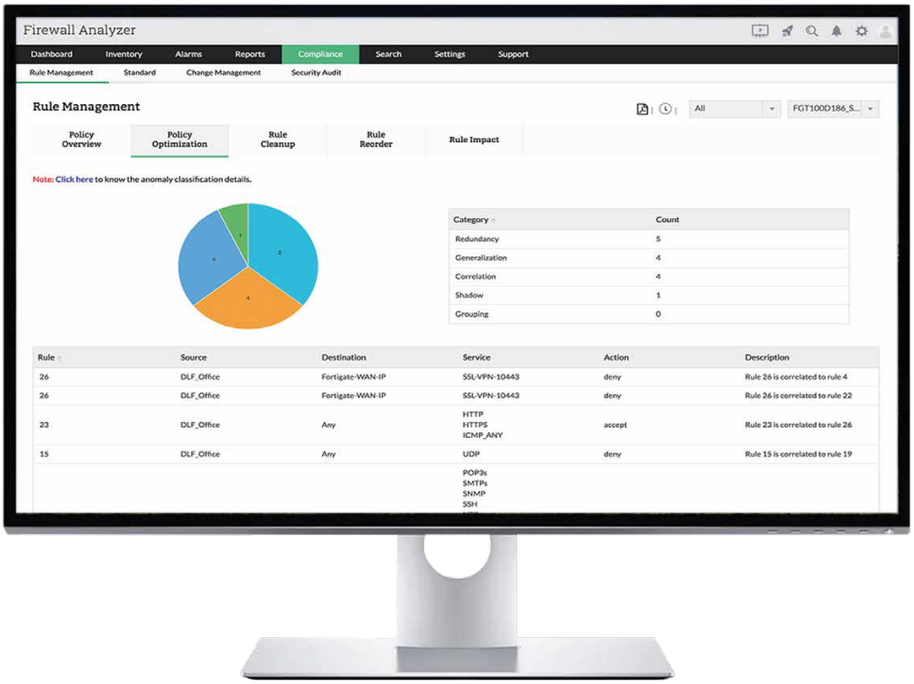
Analysieren Sie Ihre Firewall-Richtlinien und sichern Sie Ihr Netzwerk



Firewall Analyzer ist eine Log-Analyse- und Konfigurationsmanagement-Software für Firewalls. Sie bietet CLI-basierte Konfigurationsüberwachung und unterstützt die Protokolle Syslog, Telnet, SSH und SCP für die Sicherheits- und Traffic-Analyse. Sicherheitsadministratoren unterstützt Firewall Analyzer dabei, Richtlinienänderungen zu überwachen, die Performance der Firewalls zu optimieren und Compliance-Standards einzuhalten.

Firewall Analyzer auf einen Blick

- Analyse von Firewall-Richtlinien und -Regeln
- Vorschläge zur Optimierung der Firewall-Regeln
- Protokollierung von Konfigurationsänderungen
- Regelmäßige Sicherheitsaudits
- Berichte zur Internetnutzung
- Echtzeit-Warnung bei sicherheitsrelevanten Ereignissen
- Anzeige des aktuellen Sicherheitsstatus der Firewalls
- Regelmäßige Überprüfung aller Compliance-relevanten Aspekte
- Bandbreiten-Monitoring und Alarmierung bei Engpässen
- Sammeln, Korrelieren und Analysieren von Firewall-Logfiles

Firewall Analyzer unterstützt mehr als 50 Anbieter

Check Point	Paloalto	Cisco	Fortinet	Juniper	Sonicwall
WatchGuard	Huawei	pfSense	Cyberoam	Sophos	und weitere...

Technologiepartner von Firewall Analyzer

WatchGuard™ Check Point SOFTWARE TECHNOLOGIES LTD. paloalto NETWORKS®

Highlight-Features

Analyse der Firewall-Richtlinien

Analysieren Sie die Effizienz Ihrer Firewall-Regeln. Erhalten Sie detaillierte Berichte über alle abgelehnten, erlaubten, eingehenden, ausgehenden und inaktiven Regeln. Erkennen und protokollieren Sie Redundanzen, Generalisierungen, Korrelationen, Schatten- und Gruppierungsanomalien in Ihren Firewalls. Finden Sie heraus, ob sich eine neue Regel negativ auf das bestehende Regelset auswirken kann. Gewinnen Sie Einblicke, wie Sie die Leistung verbessern können, indem Sie die Reihenfolge der Regeln ändern.

Firewall-Compliance und -Auditierung

Automatisieren Sie das Erstellen von Auditberichten für eine kontinuierliche Compliance. Nutzen Sie die sofort einsatzbereiten Berichte zu gesetzlichen Vorschriften wie PCI-DSS, ISO 27001, NIST, SANS und NERC-CIP. Analysieren Sie Auswirkungen und Schweregrad von Schwachstellen mit Hilfe der Security Audit Reports.

Sofort einsatzbereite Berichte

Firewall Analyzer erstellt detaillierte Berichte, u. a. zu: Traffic, Protokoll-, Web-, E-Mail-, FTP- und Telnet-Nutzung, Streaming & Chat, Event-Übersicht, VPN, Firewall-Regeln, Change Management, Intranet, Internet, Sicherheit, Angriffe, Spam sowie Protokoll-, Traffic-, Event-, VPN-, Inbound- & Outbound-Traffic-Trends.

Konfigurations-Monitoring

Lassen Sie sich den vollständigen Audit-Trail aller Konfigurationsänderungen an Ihren Firewalls anzeigen. Erfahren Sie, wer welche Änderungen wann und warum vorgenommen hat. Erhalten Sie Echtzeit-Benachrichtigungen auf Ihrem Smartphone, wenn Änderungen vorgenommen werden. Stellen Sie sicher, dass alle Konfigurationen und nachfolgenden Änderungen an Ihren Firewall-Geräten erfasst und in der Datenbank gespeichert werden.

Sicherheitsanalysen

Identifizieren Sie Sicherheitsangriffe, Viren und andere Anomalien in Ihrem Netzwerk. Führen Sie forensische Analysen durch, um Bedrohungen zu erkennen. Erfahren Sie, welche Viren in Ihrem Netzwerk aktiv sind, einschließlich der betroffenen Hosts. Nutzen Sie die erweiterten Suchfunktionen, um komfortabel nach Sicherheitsvorfällen in den Rohdaten der Firewall-Logs zu suchen.

Monitoring von User-Aktivitäten und Bandbreite

Behalten Sie interne Bedrohungen im Blick, indem Sie die verantwortlichen Anwender, die besuchten Websites und die Websites, die das Netzwerk Angriffen ausgesetzt haben, analysieren und identifizieren.

Firewall Analyzer ist in 3 Versionen erhältlich

Standard

- Für bis zu 60 Geräte
- Unterstützt Sicherheitsgeräte verschiedener Hersteller
- Out-of-the-box-Monitoring für virtuelle Firewalls, Proxy-Server und VPN-Geräte
- Netzwerk-Traffic-Analyse
- Berichte zur Netzwerksicherheit
- Alarm-Management
- Forensische Analysen

Professionell

- Unterstützt bis zu 60 Geräte
- Alle Funktionen der Standard Edition +
- Firewall-Regel-Management
- Konfigurationsänderungs-Management
- Berichte zur Internetnutzung der Anwender
- Firewall-Security-Auditberichte
- Berichte zur Nutzung von Webanwendungen
- Diagnose der Firewall-Verbindungen
- Erweitertes Alarm-Management
- AD- & RADIUS-Benutzerauthentifizierung

Enterprise

- Unterstützt bis zu 1.200 Geräte
- Alle Funktionen der Professional Edition +
- Überwachung mehrerer Standorte
- Standortspezifische Berichte
- Rebranding des Web-Clients
- Kunden- und benutzerspezifische Ansichten

Systemanforderungen

CPU: mind. 1GHz Pentium Dual Core Prozessor oder gleichwertig

RAM-Größe: mind. 1 GB RAM

Festplatte: mind. 1 GB Festplattenspeicher

Betriebssysteme:

i) Windows: 8, 7, NT, 2000, XP, Vista, 2000 Server, 2003 Server, 2008 Server, 2012 Server, 2016 Server, 2016 Server

ii) Linux – Ubuntu, Fedora, OpenSuSE, CentOS, Red Hat RHEL, Mandriva, Debian, VMware

Webbrowser:

Internet Explorer 8 und höher, Firefox 4 und höher, Chrome 8 und höher

Datenbanken:

PostgreSQL, MS SQL 2000, MS SQL 2005, MS SQL 2008, MS SQL 2012

30 Tage gültige kostenlose Testversion downloaden

Kontakt

Tel.: +49 8139 9300-456

E-Mail: sales-ManageEngine@micronova.de

Ihr ManageEngine-Partner

MicroNova AG

Unterfeldring 6

D-85256 Vierkirchen