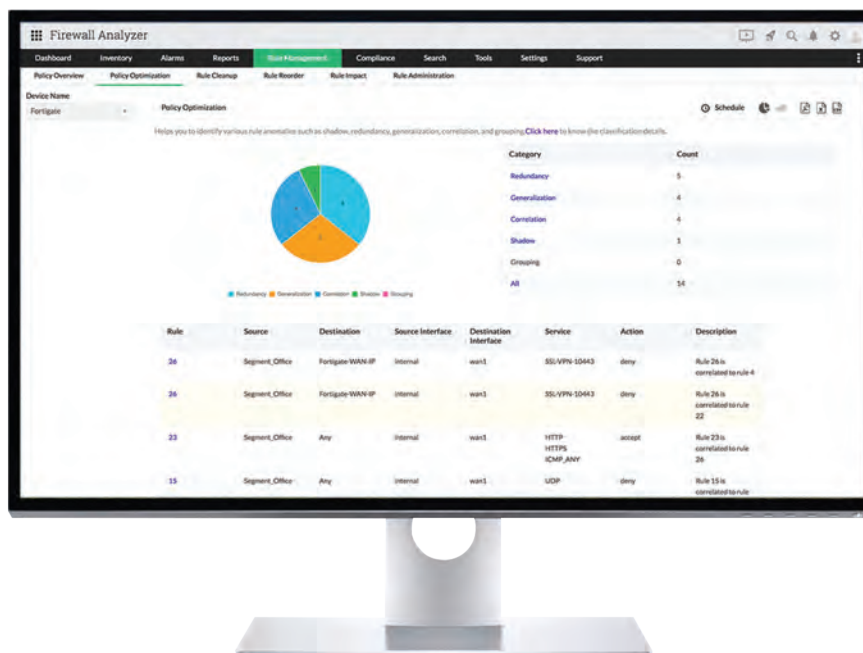


## Firewall Analyzer - Analysez votre stratégie de pare-feu et sécurisez votre réseau.



Firewall Analyzer est une solution d'analyse de politique et de rapport de configuration. Il offre une surveillance de la configuration basée sur la CLI et prend en charge les protocoles Telnet, SSH et SCP pour la sécurité et l'analyse du trafic. Il aide également les administrateurs de la sécurité à suivre les modifications de politique, à optimiser les performances du pare-feu et à maintenir les normes de conformité.

### Firewall Analyzer en résumé

- Fournit une analyse des politiques et règles de pare-feu
- Aide à automatiser l'administration des règles de pare-feu
- Suggère l'optimisation des règles de pare-feu
- Tient un journal des modifications de configuration
- Effectue des audits de sécurité périodiques
- Surveille l'utilisation d'Internet par les employés
- Alertes les événements de sécurité en temps réel
- Affiche l'état de sécurité actuel des pare-feu
- Effectue des contrôles de conformité d'audit réguliers
- Surveille et alerte lorsque la bande passante est dépassée
- Collecte, consolide et analyse les journaux du pare-feu
- Suit l'utilisation du VPN et génère des rapports VPN

### Firewall Analyzer prend en charge plus de 50 fournisseurs

Check Point	Paloalto	Cisco	Fortinet	Juniper	Sonicwall
WatchGuard	Huawei	pfSense	Cyberoam	Sophos	Et plus...

### Partenaires technologiques de Firewall Analyzer



# Principales fonctionnalités

## Analyse et administration des politiques de pare-feu

Gagnez en visibilité sur l'ensemble de votre set de règles. Détectez et enregistrez les anomalies de redondance, de généralisation, de corrélation, d'ombre et de regroupement dans votre pare-feu. Découvrez comment améliorer les performances en modifiant l'ordre des règles. Automatisez l'administration des règles de pare-feu et déterminez également si une nouvelle règle peut avoir un impact négatif sur l'ensemble de règles existant.

## Conformité et audit du pare-feu

Automatisez les rapports d'audit du pare-feu et assurez une conformité continue. Obtenez des rapports prêts à l'emploi sur les mandats réglementaires tels que PCI-DSS, ISO 27001, NIST, SANS et NERC-CIP. Analysez l'impact et la gravité des vulnérabilités grâce aux rapports d'audit de sécurité.

## Rapports prêts à l'emploi

Firewall Analyzer génère des rapports détaillés sur le trafic, l'utilisation du protocole, l'utilisation du Web, l'utilisation du courrier, l'utilisation du FTP, l'utilisation de Telnet, le streaming et le chat, le récapitulatif des événements, le VPN, les règles de pare-feu, la gestion des modifications, l'intranet, Internet, la sécurité, les attaques, le spam, la tendance du protocole, du trafic, des événements, des VPN, et le trafic entrant et sortant.

## Surveillance de la configuration

Affichez la trace complète de toutes les modifications appliquées à vos configurations de pare-feu. Découvrez qui a fait quels changements, quand et pourquoi. Recevez des alertes en temps réel sur votre téléphone mobile lorsque des changements se produisent. Assurez-vous que toutes les configurations et les modifications ultérieures apportées à votre pare-feu sont capturées périodiquement et stockées dans la base de données.

## Analyse de sécurité

Identifiez les attaques de sécurité, les virus et autres anomalies dans votre réseau. Effectuez une analyse forensique pour identifier les menaces. Sachez quels virus sont actifs sur votre réseau, y compris les hôtes concernés. Utilisez les capacités de recherche avancées pour rechercher sans effort les incidents de sécurité dans les journaux bruts du pare-feu.

## Activité des utilisateurs et surveillance de la bande passante

Gardez une trace des menaces internes en analysant et en identifiant les utilisateurs responsables, les sites Web visités et les sites Web qui ont exposé le réseau à des attaques.

## Firewall Analyzer est disponible en 3 éditions

### Standard

À partir de **395\$**

- Prend en charge jusqu'à 60 appareils
- Prise en charge des dispositifs de sécurité multi-fournisseurs
- Surveillance prête à l'emploi pour les pare-feu virtuels
- Serveurs proxy et périphériques VPN
- Analyse du trafic réseau
- Rapports de sécurité réseau
- Gestion des alertes
- Analyse forensique

### Professionnel

À partir de **595\$**

- Prend en charge jusqu'à 60 appareils
- Toutes les fonctionnalités de l'édition Standard +
- Gestion des règles de pare-feu
- Gestion des modifications de configuration
- Rapports d'activité Internet des employés
- Rapports d'audit de sécurité du pare-feu
- Rapports d'utilisation des applications Web
- Diagnostic de connexion au pare-feu
- Gestion avancée des alertes
- Authentification des utilisateurs AD & RADIUS

### Entreprise

À partir de **8395\$**

- Prend en charge jusqu'à 1200 appareils
- Toutes les fonctionnalités de l'édition professionnel +
- Surveille les emplacements multi-géographiques
- Rapports spécifiques au site
- Rebranding du client Web
- Vues spécifiques au client et à l'utilisateur

## Configuration minimale requise

**Processeur:** Processeur Pentium Dual Core 1 GHz ou équivalent

**Taille de la RAM:** 1 Go de RAM

**Disque dur:** 1 Go d'espace disque

### Système opérateur :

- i) Windows: 8, 7, NT, 2000, XP, Vista, 2000 Server, 2003 Server, 2008 Server, 2012 Server, 2016 Server
- ii) Linux - Ubuntu, Fedora, OpenSuSE, CentOS, Red Hat RHEL, Mandriva, Debian, VMware

### Navigateurs Web:

Internet Explorer 8 et versions ultérieures, Firefox 4 et versions ultérieures, Chrome 8 et versions ultérieures

### Base de données:

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

## Nos clients



**Essai gratuit de 30 jours**