

ManageEngine Firewall Analyzer 7.5

ファイアウォール・UTM・プロキシサーバ ログ解析

製品概要

マルチベンダのファイアウォール・ログを一元管理し、ネットワークのセキュリティ強化を支援!

ManageEngine Firewall Analyzer (マネージエンジン ファイアウォール アナライザ、以下、Firewall Analyzer) は、マルチベンダのファイアウォールや UTM、プロキシサーバのログを収集・解析する、Web ベースのログ解析ツールです。多様なセキュリティレポート機能により、帯域使用状況やネットワークへの侵入の痕跡、トレンド情報から異常の兆候、ユーザのサイトアクセス状況などを容易に把握することができます。また、不正アクセス、ウイルス検知に関するアラート通知機能により、迅速なセキュリティ強化対策が可能です。マルチベンダの機器のログの一元的な管理で、ネットワーク管理者の負荷が大幅に軽減します。

特長

● マルチベンダのファイアウォール・UTM・プロキシサーバに対応

Firewall Analyzer は、Cisco ASA/PIX、Fortinet、Check Point、Juniper NetScreen、Palo-Alto、SonicWALL など 30 ベンダ以上の主要ファイアウォールのログ解析が可能です。Syslog/WELF 形式に対応しています。

● ログファイル管理

Syslog の受信 (Syslog サーバが製品に包含)、ログファイルのインポート、または、Check Point ファイアウォール用の LEA サーバ設定でログを取得します。受信したログデータの自動圧縮保存や保存したログファイルの読込が可能です。

● ログ解析・レポート機能

ネットワークごとの現在の状況把握に便利なライブレポートや、ホストごと/プロトコルごとのトラフィック使用量を表示するトラフィックレポートや Web 使用レポートなど、帯域分析に有効な情報を一覧やグラフでわかりやすく提供します。セキュリティ分析に有効なウイルスレポートや SSL-VPN など、各種 VPN 関連のレポート等も生成可能です。



[Firewall Analyzer ダッシュボード画面]

新機能

● Palo Alto、Blue Coat 機器向けのレポート強化【機能強化】

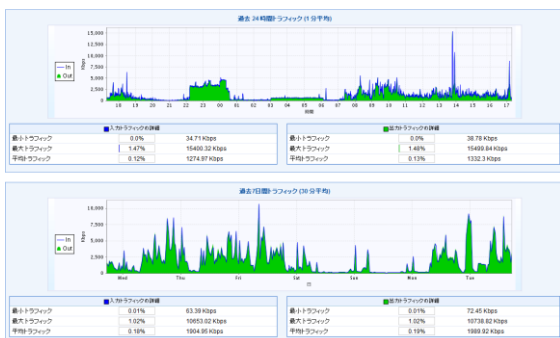
Palo Alto ファイアウォールのアプリケーション制御サービスが生成するログを解析することで、音声や動画等のリッチメディアデータを扱うアプリケーション (Skype、Facebook、YouTube 等) の帯域利用状況を把握できます。また、Blue Coat プロキシサーバのウイルスレポートに対応し、Blue Coat プロキシサーバがブロックしたウイルスとワームについてその回数を上位より表示することで送信元の追跡に役立ちます。

● SFTP (SSH File Transfer Protocol)、または SSH (Secure Shell)を用いた、リモートホストからのログインレポートに対応【機能強化】

暗号化したセキュアな通信を利用してリモートホストからログをインポートすることで、ログの盗聴や偽装・改ざんを防止します。

主な機能

ライブレポート



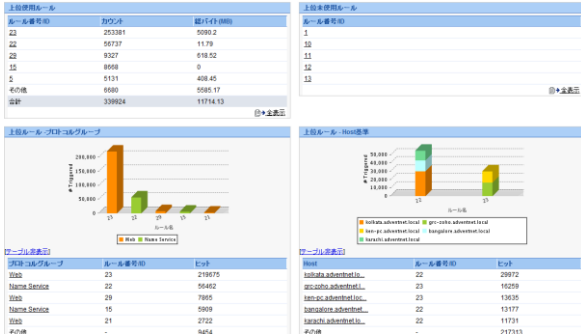
各インターフェースや機器全体の現在の帯域状況を表示します。SNMP でインターフェースの速度情報を取得し、帯域情報を計算します。最新のトラフィック状況を容易に把握可能です。

トラフィックトレンドレポート



どの時間帯にどの程度通信が発生しているか、過去のデータと比較して現在の状況を把握し、いち早く異常を検知します。ユーザグループごとの VPN トラフィック使用状況も把握可能です。

Firewall ルールレポート



ファイアウォールのルールを定期的に監視し、使用中のルールと未使用の(使用されていない)ルールのレポートを生成します。このレポートを基に不要なルールを管理することで、ファイアウォールの性能低下を防ぐことができます。

ログのインポート、カスタムレポートとスケジュール

ローカルホストのディレクトリ指定や、リモートホストからのFTP転送でログをインポート可能です。複数のログをインポートしている場合、特定の機器に対して条件を指定した独自のログレポートも生成できます。作成したレポートをPDF形式でサーバ上に保管できるほか、指定のメールアドレス宛に定期的な送信が可能です。

プロキシサーバレポート

Squid や Blue Coat、Microsoft ISA のプロキシサーバログに対応しており、ネットワーク内のトラフィックやユーザがアクセスした Web サイト等の外部ネットワークとの通信状況の詳細を提供します。

セキュリティレポート

ウイルスの種類や送信元、宛先等の情報を、セキュリティレポートやウイルスレポート、攻撃レポートとして提供します。ネットワークが受けているセキュリティ上の脅威を把握するのに有効です。

コンプライアンスレポート

コンプライアンスタブでは、Firewall ルール監視、セキュリティ監査、コンフィグレーション分析/変更管理などのコンプライアンス関連レポートをまとめて参照でき、機器の認証情報も管理できます。

アラート通知

しきい値を設定することで、ネットワーク異常の発生時や、ファイアウォールから一定時間ログを受信しない場合にアラートを生成して管理者に通知します。アラート通知と同時に、指定したスクリプト/バッチファイルの実行、メール通知や SNMP トラップ通知が可能です。ネットワーク異常の把握と対処の判断を迅速化します。

Edition と価格

Firewall Analyzer のライセンス体系は、レポート表示の対象とする機器数を基準にしています。

Edition		Professional Edition	Premium Edition	Distributed Edition	
対象		中小規模ネットワーク	中小規模ネットワーク	大規模ネットワーク	
構成		単一サーバ	単一サーバ	2 階層分散サーバ	
年間ライセンス料金 (消費税別、年間保守サポート付き)		¥ 68,000~	¥ 102,000~	¥ 1,190,000~	
機能	ログ解析 & レポート	ライブレポート、トラフィックトレンドレポート Firewall ルールレポート、プロキシサーバレポート セキュリティレポート、カスタムレポート・スケジュール	○	○	○
		Firewall 未使用ルール解析	×	○	○
	アラート	しきい値によるアラート生成 アラート管理、コマンド実行	○ ×	○ ○	○ ○
	コンフィグ変更管理のメール通知	×	○	○	
	ユーザ権限管理、VPN ユーザ管理	×	○	○	

動作環境

OS	CPU	メモリ	ディスク	解像度	ブラウザ
Windows XP / Vista / 7 / 2003 Server / Server 2008/2008 R2 (32bit/64bit)	Pentium Dual-Core 1GHz 以上 (32bit) / Xeon LV 2.8GHz 以上 (64bit)	1GB 以上	1GB 以上	1024×768 ピクセル以上	Internet Explorer 7.0 以上 Firefox 4.0 以上
Linux Red Hat Enterprise Linux 4 以上、Enterprise6.2、CentOS 6.2 (32bit/64bit)					

サポート対象のファイアウォール・UTM・プロキシサーバ

Alcatel-Lucent、Applied Identity、ARKOON Network Security、Sophos (Astaro)、Aventail、AWStats、Blue Coat、Check Point、Cimcor、Cisco ASA
Cisco Botnet、Cisco CSC-SSM、Cisco PIX、Cisco VDC、Cisco VPN、CyberGuard、FreeBSD、Funkwerk UTM、FortiGate family、FortiGate VDOM
Global Technologies、IPCop、Ingate、Inktomi、Juniper NetScreen、Microsoft ISA、McAfee、NetApp、NetASQ、NetFilter Netopia、Network-1
Palo-Alto、Recourse Technologies、Secure Point、Snort、St. Bernard Software、SonicWALL、Squid Project、TMG、WatchGuard、Zywall、3Com

(サポート対象機器の詳細は、右の URL をご参照ください。 http://www.manageengine.jp/products/Firewall_Analyzer/SupportedFW.html)

無料で製品を評価できます! Firewall Analyzer ダウンロード

- 本文中に記載されている会社、ロゴ、製品の固有名詞は各社の商号、商標または登録商標です。
- このリーフレットの記載内容は、2013 年 1 月現在のものです。記載されている内容は事前の予告なしに変更する場合があります。
- 製品に関するご質問、ご購入は、下記までお問い合わせください。

(C) ZOHO Japan Corporation. All rights reserved.

製品提供元

ゾーホージャパン株式会社

神奈川県横浜市神奈川区金港町 6-3 横浜金港町ビル 6 階
Tel:045-444-3881 (ManageEngine 営業担当)
<http://www.manageengine.jp/>
E-mail: jp-mesales@zohocorp.com



お問い合わせ先

販売元

株式会社EPコンサルティングサービス
ITソリューション事業部
高橋 道穂
03-4577-1718 (直通)
michiho.takahashi@epcs.co.jp