



Web Content Filtering

for Enterprise Networks Using Clear Packets FMS-Enterprise Gateway

State of the Art **Web Content Filtering, Security and Data Leak Protection** Solution Runs on Inexpensive Intel/AMD Server

1 Introduction

Clear Packets FMS-Enterprise Gateway has been designed for immediate and long-term network security. It is an integrated security which meets majority of security requirements for enterprises. The solution has major innovations in it which separates it from the many other solutions available in the market. The architecture of the system is based on modern day advanced router design concepts which enables it to deliver high performance with very little latency and meet scalability requirements of small and large networks. **The solution is so advanced that it even allows software upgrades during full load network operations without interrupting any network operations, also known as in-service-software-upgrade (ISSU).**

Unlike all other competitors which use rudimentary techniques of matching URL strings to block unwanted traffic, **Gateway harnesses power of modern 64-bit computing of Intel or AMD hyper-threading processors available in ordinary PCs to deliver almost 100 times better performance.**

A brief overview of major features available in the system is provided here:

1.1 Features

1.1.1 Web Filtering & Monitoring

- Ensure internet and the network is used for educational purposes only. Easily verify and audit automatically maintained simple to understand 24/7/365 network activity record. An ordinary PC can store internet access record for a full year.

- Quickly pinpoint any suspicious activity like P2P clients, rogue applications through accurate, up to the minute activity summary.
- Industry's most comprehensive SafeSearch enforcement for all major search engines so that only appropriate content is returned by Google, Yahoo, Live, MSN, AOL, Ask and Cuil. This is perhaps the most important safety feature which will become far more important going forward as search engines improve it further. More details are at: <http://www.clearpackets.com/files/ClearPacketsSafeSearchPDF.pdf>
- Block unwanted websites through a large black list websites for inappropriate content, harmful or attacking websites etc, which along with SafeSearch form a very powerful combination to ensure safe and appropriate internet environment for minors. Add your own websites to the blacklist.
- Real-time record of internet bandwidth usage for each user on daily, weekly and monthly basis to control excessive usage.
- Advanced internet access control option to allow access to specific websites for one set of users (example staff) but deny to others (students).
- Up to date list of 50 most accessed websites in real-time.

1.1.2 Virus, Worms, Malware/Spyware

- Automatically stops latest discovered viruses, worms and other malicious programs from entering your network via any of the methods as email, Web mail, HTTP (Web browsing or downloads), FTP downloads etc. using terminate-worms-on-the-wire technology.

1.1.3 Intrusion Detection & Protection

- Using latest data from best internet watchdogs like Storm Control Center, DShield, Emerging Threat, Shadow Server etc., blocks out more than 6 million known hackers, bots, intruders from getting into the network.
- Blocks any computer from inside the network from connecting to these networks for two-way protection. This is updated regularly and clients get automatic protection.

1.1.4 Application Control

- Stop specific groups of users from running any network application. For example, prohibit running FTP, HTTP, FTP, SSH, Streaming, SIP etc. for a set of users while permit others.
- Large number of predefined applications to choose from, or quickly define your own if needed.

1.1.5 Data Leak Protection

- Protect data from being stolen or leaked out through any of the network transport method - Web mail, HTTP upload, FTP, regular email etc.

- All document formats are accepted without requiring any changes to network or mail transfer agents.

1.1.6 Guest Access Rights Control

- Policy based control on resources accessible to guest users, management amount of bandwidth they can use, network applications they can run and internal servers they can access. This provided strong security against any visitors trying to get into unauthorized parts of internal network

1.1.7 Highly Available, Scalable and Low Latency System

- Very well designed system, automatically monitor heartbeat to auto restart for non-stop availability. Even allows in-service software upgrades (ISSU).
- Optional port bypass/link bypass hardware NIC for extreme conditions like power failure etc.
- Extensive load and stress tested system for graceful handling of overload conditions.
- Designed for scalability to easily cope with high load using minimal resources to deliver optimal performance.

1.1.8 Investment Protection

- System runs on ordinary PC or regular inexpensive Dell or HP servers which can be used for any other purpose in case of upgrades.

1.1.9 Easy to Deploy and Manage

- Layer-2 device (L2 operating mode) for easy deployment.

1.2 Out of the Box Available Reports

1.2.1.1 Internet Access Reports

1. Internet access activity report – 24 hours view of all network activity for all users, clearly identifying source, destination, time of activity, network protocol used, amount of data transferred, source and destination ports and brief explanation.
2. Internet access activity report can be generated for any user containing all information as in (1).
3. Internet access report based on matching of specified keywords – network activity matching specified keywords can be generated using specified keywords.
Example, administrator may specify keywords like gamble, proxy, porn, adult,

liquor, bomb and system would return all network activity matching any of these keywords in the accessed domain names.

4. Internet access log report to query for access activity for any user for any day in past.
5. Internet access activity based on amount of data received or transmitted.
6. Internet access activity report to a specific website. Example - report for access activity to website yahoo.com.
7. Internet access activity report for a specific user and a specific website. Example – report for access activity by userid john to website yahoo.com
8. Internet access activity to an IP address by all users or one specific user.
9. Internet access activity using only TCP or only UDP protocol.

1.2.1.2 Virus, Malware, Data Leak Protection and Blocked Service Reports

10. Report on virus, malware, IDS/IPS, filter hits – show all hits to virus/malware filters, intrusion filters, data leak protection filters for today.
11. Report on virus, malware, IDS/IPS, filter hits – show all hits to virus/malware filters, intrusion filters, data leak protection filters for any day in past (log reports).
12. Blocked/denied service use report – shows all blocked accesses to blocked websites, blocked accesses to intrusion detection filter blocked networks or websites, blocked application use attempts, blocked attempts to steal protected data for today.

1.2.1.3 Network Flow and Bandwidth Usage Reports

13. Bandwidth usage report – current value of daily, weekly and monthly internet bandwidth usage in mega bytes (MBytes). This is also available to individual users so they can find out how much bandwidth they have used up.
14. Monthly bandwidth usage log – monthly log of bandwidth usage in previous months. Can be sorted on daily, weekly, monthly usage, IP address, active flows or total flows.
15. Network flow report – real-time report on number of network flows currently active for a user as well as total flows created today. This is very useful for

- diagnostic purposes and detecting P2P and similar applications running on the network.
16. Fifty most visited websites – real-time list of 50 most visited websites.
 17. Up to 5000 latest access websites in auto scrolling list.
 18. System activity report – complete history of all activity carried out on system by the administrator to ensure system integrity. Maintained in encrypted and tamperproof format.
 19. User report showing their current authentication status to access internet (if authentication requirement is enabled), authentication status to be able to create data leak protection filters through Web browser interface.

1.2.1.4 Reports of Various Filters and Website Lists

20. List of all virus/malware filters.
21. List of all data leak protection filters.
22. List of all controlled applications.
23. List of all intrusion detection and protection filters.
24. List of all websites in each access blocked website group.
25. List of all websites in each access restricted website group.
26. List of all websites address by individual users to Whitelist if configured, including userid, the IP address of computer from which user carried out the addition and name of the website added to white list.

Summary

FMS-Enterprise Gateway is a state of the art integrated solution for Web content filtering, user internet bandwidth management, virus/malware/spyware filtering, data leak protection (DLP), intrusion detection/prevention (IDS/IPS) and application control. It is also a vital resource in helping customers meet regulatory compliance requirements by maintaining complete records of network activity for everyday. The system software has been designed with great thoughtfulness making it highly available (HA) and an extremely robust solution. Optional port bypass/ link bypass hardware NIC is available to all customers if they require it to ensure network availability in catastrophic events like power failure. System runs on general purpose PCs or inexpensive Dell/HP servers saving thousands of dollars for customers by eliminating custom hardware requirements and offering

great investment protection. For further product details visit <http://www.clearpackets.com>, email info@clearpackets.com or call 972-325-1966.

© 2008, Copyright Clear Packets, L.L.C.
All Rights Reserved.

This document may not, in whole or in part be reproduced, copied, translated, photographed or photocopied or changed or reduced to any electronic form or medium without explicit prior written consent from Clear Packets, LLC.

Trademarks

Clear Packets, Clear Packets logo and FMS-Enterprise Gateway are trademarks of Clear Packets, L.L.C. worldwide.