OPEN SOURCE UTM ALTERNATIVE: ClearOS

Sedat Akleylek[1], Levent Emmungil[2], and Urfat Nuriyev[3]

[1]Ondokuz Mayıs University, Samsun and Middle East Technical University, Ankara, Turkey
[2]Ufuk University, Ankara, Turkey
[3]Ege University, İzmir, Turkey
[1]*akleylek@gmail.com*, [2]*emmungil@gmail.com*, [3]*urfat.nuriyev@ege.edu.tr*

Unified network security solutions are relatively new concept for computer networks' security market [2], [3], [4], [5]. As all data of the local network use one point as a gateway, the security solutions are placed in that point. Improvements of both hardware and software technologies lead us to the possibility of single-box solutions for all security needs.

Unified Threat Management (UTM) appliances are available for low-cost, reliable network security solutions [3], [5]. Today there are many UTM alternatives both for software and hardware solutions. Because this single appliance will be the most important factor for the network reliability it is very crucial to select, install and maintain the UTM device according to the need of the institution.

The aim of this paper is to introduce one of the UTM software alternative in the market; ClearOS, Open Source UTM solution [1].

Unified Threat Management (UTM) is one of the most important factors for network and security management. UTM is easy to manage, all in one network solution. Ease of use and extensive talents increases the importance and usage of the system. However there are many UTM alternatives in the market. The alternatives can be mainly distinguishes as hardware and software appliances. ClearOS, Endian, Untangle, ClearOS are some examples for the open source software UTM alternatives. In this paper, ClearOS UTM is analyzed in detail. It is freely available and all functions are active. Some software solutions have disabled some functions in the free versions [2].

ClearOS is a powerful network and gateway server designed for small organizations and distributed environments [1]. Though ClearOS comes with an extensive list of features and integrated services, the solution is easy to configure with the use of web-based interface. The list of features of ClearOS is listed below:

Directory Features

- *Integrated LDAP for User and Group Management*
- *User Security Certificate Manager*

ClearOS is integrated with user and group management. Users can be defined to the system in order to control the environment better. Access rights can be defined according to the user groups. The important point about the user and group management is; the web access control cannot be configured according to users if the ClearOS proxy is working in transparent mode.

Network Features

- *Multi-WAN*
- *VPN - PPTP, IPsec, OpenVPN*
- *DMZ and 1-to-1 NAT*
- *Stateful Firewall*
- *Local DHCP and DNS Servers*

Network features of ClearOS provide load balance and security for the organization. ClearOS can be combine many external connection and distribute to local area network. It is automatically provide fail over protection. Besides, integrated firewall protects the internal network from the external attacks. ClearOS also provides local DHCP server. The external connections can be configured inside the ClearOS i.e. it has PPPoE support for the connections.

Gateway Features

- *Antimalware - Antivirus, Antiphishing, Antispyware*
- *Antispam*
- *Bandwidth Management*
- *Intrusion Protection, Intrusion Prevention, Intrusion Detection*
- *Protocol Filtering including Peer-to-Peer Detection*
- *Content Filter*
- *Web Proxy*
- *Access Control*

ClearOS has the ability to provide a complete solution for virus protection, antispam, content filter, protocol filter etc. All files passed through the ClearOS are scanned with freely available open source antivirus software Clamav. As well as intrusion detection ClearOS also has intrusion prevention capabilities. Antipishing and antispam functions are also provided in this UTM. Bandwidth management is another module of the software. After combining all Internet connection in ClearOS it provides the management of the available bandwidth according to the protocol or devices. Web proxy feature is used to accelerate and secure the Internet connection of the local area network devices. The web usage features configured according to each user or group as well.

Server Features

- *Windows Networking with PDC Support*
- *File and Print Services*
- *Flexshares*
- *Groupware with Outlook Connector*
- *Mail Server - POP, IMAP, SMTP, Webmail, Retrieval*
- *Mail Filtering - Antispam, Antimalware, Greylisting, Quarantine*
- *Mail Archiving*
- *Database with MySQL*
- *Web Server with PHP Support*

ClearOS can be worked as a primary domain controller in windows network environment. Besides file and printer sharing are available in the system. Web based mail server is ready to setup in this UTM. Mysql database and web server are last but not least functions available in ClearOS.

Many available UTM hardware in the market does not have hard disc embedded, so it is not possible to have some applications such as web server, Mysql server, web proxy or file server [3], [4]. Software UTM alternatives are more flexible in this perspective. Besides most hardware appliance requires annual update fee whereas open source alternatives do not. As a result ClearOS is freely available, open source UTM alternative which is easy to install and manage.

References

[1] ClearOS (2009) Clear Foundation, available at http://www.clearfoundation.com/Software/overview.html

[2] Emmungil, L. (2008) Endian Birleşik Tehdit Yönetimi. 2. Özgür Yazılım Konferansı, Ankara

[3] Excitingip.com (2009) An Introduction to Unified Threat Management in Network Security, available at http://www.excitingip.com/553/unified-threat-management-network-security/

[4] Excitingip.com (2009) Hardware vs Sofware UTM and Open Source UTM, available at http://www.excitingip.com/563/hardware-vs-sofware-utm-open-source-utm/

[5] Unified Thread Management (2010) Wikipedia, available at http://en.wikipedia.org/wiki/Unified_threat_management