Implementation of management and network security using Endian UTM Firewall

By Giva Andriana Mutiara

WORD COUNT 2304

TIME SUBMITTED 19-JUL-2017 11:25AM

PAPER ID 30597149

International Journal
of Applied Information Technology

http://journals.telkomuniversity.ac.id/index.php/ijait

Implementation of management and network security using Endian UTM Firewall.

Fikri Muhammad Arifin [a,*], Giva Andriana Mutiara [b], Ismail [c]

[a] Dept. of Applied Sciences, Telkom University, Indonesia
[b] Dept. of Applied Sciences, Telkom University, Indonesia
[c] Dept. of Applied Sciences, Telkom University, Indonesia

ARTICLE INFO

Received 30 August 2016
Revised 24 November 2016
Accepted 29 November 2016
Available online 2 December 2016

Keywords
lorem, ipsum, dolor, sit amet, duo

ABSTRACT

Internet is a source of information which is widely used today. Due to rapid technological development, the human need for the internet became a necessity. However, the mode of internet abused are becoming more various and unavoidably. The internet abused can be done from the external or internal networks. Unified Threat Management (UTM) is one of a good solution to securing the networks, because it has several security features such as firewall, proxy, Intrusion Prevention System (IPS) and several other security features in one package. Endian is an UTM distro which is an open source in large community. Besides having some security features, Endian also has some network management features such as DHCP, routing, and VPN. This research put Endian as the center of a network topology that connected to the internal network/LAN, DMZ Server, and Internet Network/WAN. The tests conducted in the form of implementation of DHCP feature, content filtering, port restrictions on inter-zone, and the response of the IPS features that exist on the Endian while receiving the attack. The results showed that Endian UTM is quite well in maintaining the security of the networks.

Acknowledgment

The authors would like to thank the Institute for Astronomy, ETH Zurich, Switzerland; the Space Science Center, Universiti Kebangsaan Malaysia; and the National Space Agency (ANGKASA) Malaysia research grant LL-2012-010, and University of Malaya's HIR grant

* Corresponding author at:
School of Applied Science, Telkom University,
Jl. Telekomunikasi No. 1, Terusan Buah Batu, Bandung, 40257
Indonesia.
E-mail address: sometone@tass.telkomuniversity.ac.id (First Author).

ORCID ID:
- First Author
- Second Author
- Third Author
- Fourth Author

http://dx.doi.org/10.1016/j.jvcir.2016.11.019
Paper_reg_number/_ 2016 © The Authors. Published by School of Applied Science, Telkom University.

1. Introduction

Nowadays, the internet service is very important in building an institutions or companies. Because both in terms of employment, learning, strengthening relationships with institutions or companies, also variety of services to the employees cannot be separated from the internet. Internet can be accessed anywhere, anytime and by anyone. So that, many people can abuse the internet, starts from doing the tapping, destruction, until IT data theft. The internet's abuse can be done in the internal and external network.

UTM *(Unified Threat Management)*, is the evolution of traditional firewall into integrated security products, which has the ability to perform the multiple security within a single device, such as firewalls, intrusion prevention network, gateway anti-virus (AV), gateway anti-spam, VPN, content filtering, load balancing, prevention data leakage, and reporting tools [1].

Endian, is an open source distro UTM on protection network security protection from viruses, malware, and other threats using UTM platform. Endian UTM provide security including web and email filtering, VPN, IPS, Bandwidth management, and other network security services. Endian UTM is one of an open source version available in the free version for community and a paid version also as enterprise. Only enterprise version of Endian offers a hardware device, a virtual network driver, professional support, hotspot features, as well as anti-spam and content filtering commercial grade. However, the community version also has a basic UTM functions, such as anti-virus, anti-spam, URL Filtering, IPSsec, Open VPN, and several other features [2]. The advantages of community version from Endian UTM than other open source UTM are no restriction on the number of connected client. Some other UTM open source does not have the features of IPSec and Open VPN [3].

DMZ, demilitarized zone, is an area that is used to interact with outsiders. In conjunction with a computer network, DMZ is a separate sub-network of sub-internal network for security purposes. DMZ server picture can be seen at figure 1 [4].

In this research, we implemented Endian, an open source UTM (unified threat management) distro with broad community support so it is suitable to be applied on an institutions or companies. This network interconnected with DMZ server, intranet and router as shown in figure 1 [5]–[8].

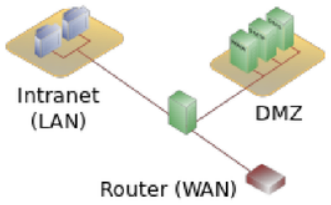


Figure 1 DMZ Server

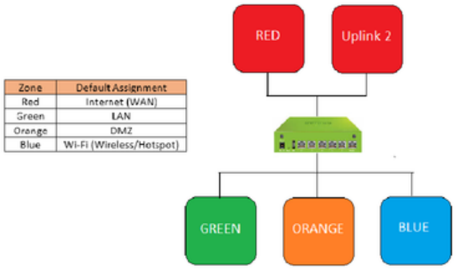
2. Discussion

Lorem ipsum dolor sit amet, duo equidem dolorum no. Mei no persius suscipiantur, cu facilisi volutpat hendrerit usu, est rebum offendit oportere ad. Ne possit suavitate quo, at pri eruditi phaedrum. An maiorum necessitatibus ius, libris persecuti vel eu. Tacimates vituperata instructior ne pri. Menandri consequuntur vis id, cu audire expetendis mei, an commodo fuisset nam.

His enim semper ei, brute posse ridens eam te, pro meis patrioque ea. Dicta consequuntur et vix, an ferri liberavisse reprehendunt vim (http://journals.telkomuniversity.ac.id/index.php/ijait). His ut clita feugiat. Ei has postea causae intellegat, mea vide mucius an. Nonumes blandit honestatis ne his, duo eu alia paulo clita, per ea fabulas postulant.

2.1. Architecture and Design Network

The architecture of endian network is implemented on figure 3, whereas each zone is connected via Endian UTM. The zones are divided into three zone; orange, green, blue zone. Unfortunately, this research did not implement VPN feature because it requires IP Public. Besides that, the blue zone is not implemented and the research only used virtual machines.



Zone	Default Assignment
Red	Internet (WAN)
Green	LAN
Orange	DMZ
Blue	Wi-Fi (Wireless/Hotspot)

Figure 2 Implementation of Endian Network

Design and implementation system of Endian will be implemented on the network topology can be seen at figure 4.

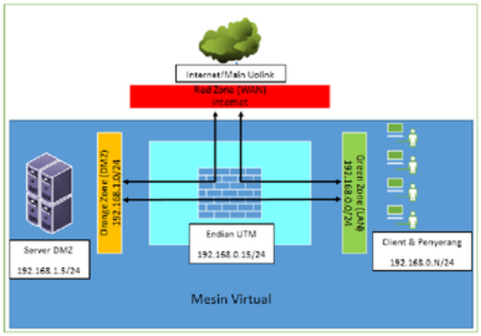


Figure 3 *Network Topology*

Figure 4 shows the topology of the network and the configurations of IP address described as:

1. Network interface which is connected to the internet only the network interface on Endian, so that all the internet will be centered with Endian
2. The attacker designed in the green zone
3. All access between zones (inter-zone) centered on Endian.

The minimal requirement of hardware system:

1. CPU and memory should be Intel x86 (32 bit), minimum speed 500MHz, RAM 256 MB.
2. Hard disk and optical drive. The type should be SCSI, SATA, SAS, or IDE. Endian need space at least 4 GB on hard disk. In addition, Endian needs an IDE, SCSI or USB CD-ROM to do the installation.

3. Network cards. Endian UTM compatible with almost all NIC (network interface card).

The implementation of the design of network topology is done on the virtual machine. The configuration of hardware system can be seen on table 1.

Table 1 Configuration of Hardware System

No	Operating System	Memory Capacity	Hard disk	NIC
1	Endian UTM	729 MB	8 GB	4 pieces PCnet-FAST III
2	Kali Linux	2048 MB	15 GB	Intel PRO/1000 MT Desktop
3	XP Client	256 MB	7 GB	PCnet-FAST III
4	Ubuntu Client	512 MB	7 GB	Intel PRO/1000 MT Desktop
5	Ubuntu Server	512 MB	8 GB	Intel PRO/1000 MT Desktop

The configuration and specification of software system can be seen on table 2.

Table 2 Configuration of Software System

No	Software	Detail Software	function
1	ISO	OS Endian, Ubuntu Server, Windows XP, Kali Linux	UTM, Server, Client, Penyerang
2	Virtual Machine	Oracle VM VirtualBox v4.3.6	Mesin Virtual
3	Aplikasi	Filezilla FTP, Mozilla Firefox	Media FTP dan Web Browser
4	Filezilla	Filezilla FTP Client	Media FTP

2.2. Procedure of Configuration

The stage of processing the implementation systems:

1. Implement the network topology on virtual machine in accordance with the endian topology.
2. Installation Endian UTM
3. Perform the basic configuration of Endian
4. Configure DHCP
5. Configure content filtering
6. Configure port access restrictions on inter-zone
7. Enabling IPS features on Endian UTM

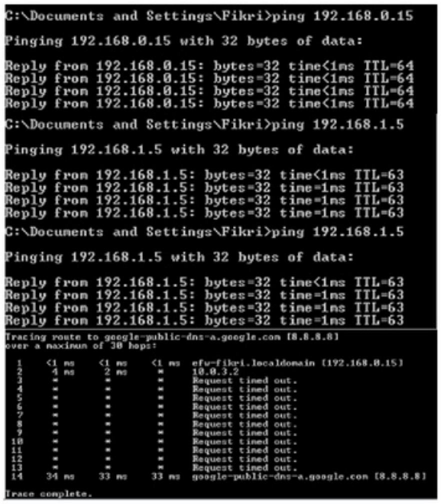
Simulate attacks such as port scanning and DDoS.

3. Result

At this stage, the testing is done by three scenarios. First scenario is testing the inter-network connectivity testing, the second scenario is DHCP testing, and the last scenario is firewall testing (URL filter and restrictions of access time) and also the testing of the threats addressed by snort.

3.1. Inter-Network Connectivity Testing

This test aims to determine the connection between the internal network, server, Endian UTM and the Internet. Testing is done by doing a ping from the server to the internal network users and also from the internal network to the internet. Figure 4 is the trace route of the connectivity testing.

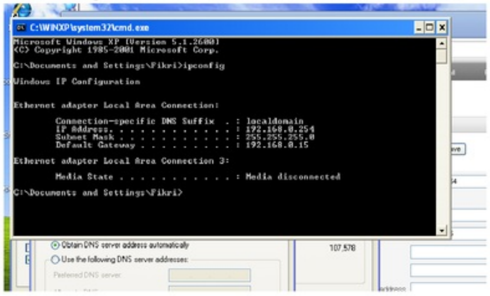


```
C:\Documents and Settings\Fikri>ping 192.168.0.15

Pinging 192.168.0.15 with 32 bytes of data:

Reply from 192.168.0.15: bytes=32 time<1ms TTL=64
Reply from 192.168.0.15: bytes=32 time<1ms TTL=64
Reply from 192.168.0.15: bytes=32 time<1ms TTL=64
Reply from 192.168.0.15: bytes=32 time<1ms TTL=64
C:\Documents and Settings\Fikri>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=63
Reply from 192.168.1.5: bytes=32 time=1ms TTL=63
Reply from 192.168.1.5: bytes=32 time=1ms TTL=63
Reply from 192.168.1.5: bytes=32 time=1ms TTL=63
C:\Documents and Settings\Fikri>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=63
Reply from 192.168.1.5: bytes=32 time=1ms TTL=63
Reply from 192.168.1.5: bytes=32 time=1ms TTL=63
Reply from 192.168.1.5: bytes=32 time=1ms TTL=63
Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  efw-fikri.localdomain [192.168.0.15]
  2     4 ms     2 ms     *     10.0.3.2
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    34 ms    33 ms    33 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.
```

Figure 4 Tracing of Connectivity Testing

3.2. DHCP Testing

This testing conducted to prove the DHCP feature of Endian. This testing can be done by select obtain an IP address automatically, so that the client gets an automatic IP from DHCP services on endian UTM. Figure 5 is one of the examples of a client who gets an automatic IP from DHCP service.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Fikri>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.0.254
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.15

Ethernet adapter Local Area Connection 3:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Fikri>
```

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:

Figure 5 DHCP Testing

3.3. Firewall Testing

Tests on the firewall as a security of the network is divided into several sections including testing a content filter, the restrictions port inter-zone on endian, and testing of report an IPS attacked.

3.3.1. Testing Content Filter

This testing is done to filter the content which is desired by the user. On this category there are two ways to block the site access. The first is blocking the content by category and the second is blacklist the feature. Figure 6 and 7 is the figure of sport category that will be blocked if the user list's it to the list of blocking content.

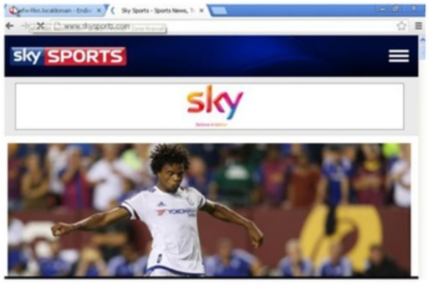
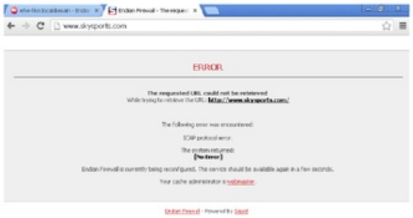


Figure 6 Site of Sport Categories before Content Filtering


www.skysports.com

ERROR

The requested URL could not be retrieved
While trying to retrieve the URL: http://www.skysports.com/

The following error was encountered:

ICAP protocol error.

The system returned:
[No Error]

Endian Firewall is currently being reconfigured. The service should be available again in a few seconds.

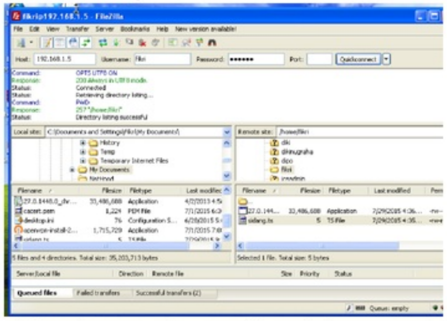
Your cache administrator is webmaster.

Endian Firewall - Powered by Squid

Figure 7 Site After Exposed Block by Content Filtering

3.3.2. *Testing the Restriction Port for Inter-Zone*

Port restriction is required in the construction of the network. Port restriction can be applied to the zone, IP address, or on the specific MAC address. Here is an example of restriction access on port 21 (FTP). Figure 8 show that the client (green zone) is able to access the FTP server (orange zone). Figure 9 show that the status of the access port 21 (FTP) of the orange zone is changed to blocked status for the access of the green zone. Figure 9 shows that the green zone cannot access port 21 (FTP) on the orange zone.


fikri@192.168.1.5 - FileZilla

Host: 192.168.1.5 Username: fikri Password: •••••• Port:

```
Command:    OPTS UTF8 ON
Response:   200 Always in UTF8 mode.
Status:     Connected
Status:     Retrieving directory listing...
Command:    PWD
Response:   257 "/home/fikri"
Status:     Directory listing successful
```

Local site: C:\Documents and Settings\fikri\My Documents\

Remote site: /home/fikri

Filename	Filesize	Filetype	Last modified
27.0.1448.0_dv...	33,486,688	Application	4/2/2013 4:5
cacert.pem	1,224	PEM File	7/1/2015 6:3
desktop.ini	76	Configuration S...	4/28/2015 5:
openvpn-install-2...	1,715,729	Application	7/1/2015 7:0

Filename	Filesize	Filetype	Last modified
..			
27.0.144...	33,486,688	Application	7/29/2015 4:36...
sidang.ts	5	TS File	7/29/2015 4:36...

5 files and 4 directories. Total size: 35,203,713 bytes

Selected 1 file. Total size: 5 bytes

File Edit View Transfer Server Bookmarks Help New version available!
Quickconnect
History
Temp
Temporary Internet Files
My Documents
NetHood
diki
dinugraha
dipo
fikri
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers (2)
Queue: empty

Lorem ipsum dolor sit amet, duo equidem dolorum no. Mei no persius suscipiantur, cu facilisi volutpat hendrerit usu, est rebum offendit oportere ad. His enim semper ei, brute posse ridens eam te, pro meis patrioque ea. Dicta consequuntur et vix, an ferri liberavisse reprehendunt vim. His ut clita feugiat. Duis albucius pro at. Ne ius animal legimus, qui ad salutatus persequeris. Ea qui consul voluptatum, affert dissentias vix ex. Ius alia quodsi id, eum ea nemore viderer constituto, novum ludus virtute ex mel. Cu ius noster nonumes, mel ea facer simul electram. Pri an dictas suscipiantur, eos cu mazim invidunt, sed ea euismod principes intellegat. Ei vis vivendo assueverit, nostro perfecto cum no, est consul mentitum rationibus ut. Usu modo aeterno accusam ea, sed ea debitis blandit. Mei semper similique no. Equidem habemus evertitur ei pro, sea te affert tempor dolorem, ut graeci nostrud pro.

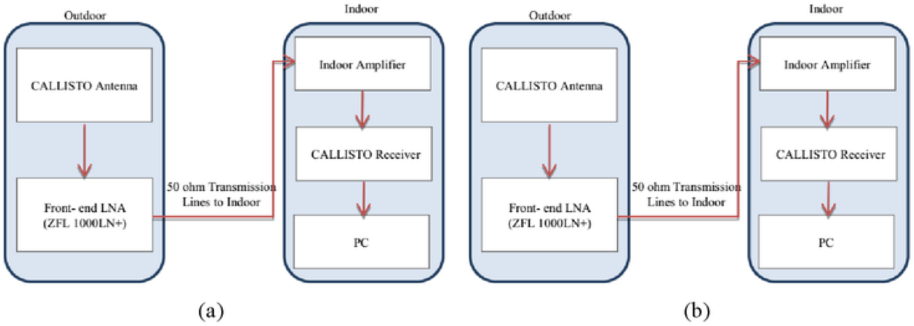


Figure 8 This is a sample of two images

Te nam definiebas reprehendunt interpretaris. Doming concludaturque in ius, convenire principes pertinacia an nam, duo falli tincidunt ut.

Lorem ipsum dolor sit amet, duo equidem dolorum no. Mei no persius suscipiantur, cu facilisi volutpat hendrerit usu, est rebum offendit oportere ad. His enim semper ei, brute posse ridens eam te, pro meis patrioque ea. Dicta consequuntur et vix, an ferri liberavisse reprehendunt vim. His ut clita feugiat. Duis albucius pro at. Ne ius animal legimus, qui ad salutatus persequeris. Ea qui consul voluptatum, affert dissentias vix ex. Ius alia quodsi id, eum ea nemore viderer constituto, novum ludus virtute ex mel. Cu ius noster nonumes, mel ea facer simul electram. Pri an dictas suscipiantur, eos cu mazim invidunt, sed ea euismod principes intellegat. Ei vis vivendo assueverit, nostro perfecto cum no, est consul mentitum rationibus ut. Usu modo aeterno accusam ea, sed ea debitis blandit. Mei semper similique no. Equidem habemus evertitur ei pro, sea te affert tempor dolorem, ut graeci nostrud pro. Te nam definiebas reprehendunt interpretaris. Doming concludaturque in ius, convenire principes pertinacia an nam, duo falli tincidunt ut.

Bibliography

[1] A. A. G. Agung, F. A. Yulianto, and W. Maharani, “Pengenalan Wajah Menggunakan Pseudo-2D Hidden Markov Model,” *J. Teknol. Inf.*, vol. 1, no. 1, pp. 26–31, May 2011.

[2] A. Kianpisheh, N. Mustaffa, P. Limtrairut, and P. Keikhosrokiani, “Smart Parking System Architecture Using Ultrasonic Detector,” *Int. J. Softw. Eng. It’s Appl.*, vol. 6, no. 3, 2012.

[3] Sharp, “GP2Y0A02YK0F,” 2006.

[4] A. M.-S. and R. N. Waltraud Grillitsch, “Successful Sharing of Project Knowledge: Initiation, Implementation and Institutionalisation,” *Electron. J. Knowl. Manag.*, vol. 5, no. 1, pp. 19–28, 2007.

[5] K. Tallent, “The role of CCTV in today’s parking access and revenue control systems.,” *J. Healthc. Prot. Manage.*, vol. 26, no. 1, 2010.

[6] N. Katira, L. Williams, E. Wiebe, C. Miller, S. Balik, and E. Gehringer, “On understanding compatibility of student pair programmers,” *ACM SIGCSE Bull.*, vol. 36, p. 7, 2004.

[7] “Wilson Wenas Gelisah akan Tragedi Sel Surya,” 2003. [Online]. Available: http://www.energi.lipi.go.id/utama.cgi?artikel&1080048809&10.

[8] P. Kesarwani and A. K. Misra, “Selecting Integrated Approach for Knowledge Representation by Comparative Study of Knowledge Representation Schemes,” *Int. J. Sci. Res. Publ.*, vol. 3, no. 2, pp. 1–5, 2013.

[9] T. G. Henkel and J. N. Wilmoth, “Factor Analysis of the Personal Profile System,” *J. Exp. Educ.*, vol. 60, no. 3, pp. 271–280, 1992.

[10] N. Asni, N. Wisna, and A. A. G. Agung, “Aplikasi Pencatatan Pembelian dan Persediaan pada Apotek Selamat Farma,” *J. Teknol. Inf.*, vol. 1, no. 5, pp. 184–188, May 2013.

[11] J. W. Wibowo, A. A. G. Agung, and R. B. K, “Aplikasi Pengelolaan Kas Kecil pada Unit Kemahasiswaan Politeknik Telkom,” *J. Teknol. Inf.*, vol. 1, no. 4, pp. 152–157, Nov. 2012.

Implementation of management and network security using Endian UTM Firewall

ORIGINALITY REPORT

14%

SIMILARITY INDEX

PRIMARY SOURCES

1	Submitted to Telkom University Your Indexed Documents	239 words — 11%
2	www.ida.gov.sg Internet	17 words — 1%
3	Pratondo, Agus, Chee-Kong Chui, and Sim-Heng Ong. "Integrating machine learning with region-based active contour models in medical image segmentation", Journal of Visual Communication and Image Representation, 2017. Crossref	12 words — 1%
4	m.migrationexpertzone.com Internet	10 words — < 1%
5	www.cognosec.com Internet	8 words — < 1%
6	www.knet.com.au Internet	8 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		