International Journal
of Applied Information Technology

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

Implementation of Management and Network Security Using Endian UTM Firewall

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

[a,b,c] *Diploma of Computer Engineering, Telkom University, Indonesia*

ARTICLE INFO

Received June 7, 2017
Revised July 26, 2017
Accepted August 8, 2017
Available online August 14, 2017

Keywords
Management Networks, Network Security, UTM, Endian, DMZ

ABSTRACT

Internet is a source of information which is widely used today. However, the mode of internet abused becomes more various and unavoidable. The internet abused can be done from external or internal networks. Unified Threat Management (UTM) is one of a good solution to secure 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 are 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.

* Corresponding author at:
Diploma of Computer Engineering, Telkom University,
Jl. Telekomunikasi No. 1, Terusan Buah Batu, Bandung, 40257
Indonesia.
E-mail address: fikrimarifin25@gmail.com

ORCID ID:
Second Author: 0000-0003-4387-6128

https://doi.org/10.25124/ijait.v1i02.874
Paper registration number IJAIT000010206 2017 © 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 (Intrusion Prevention System), 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, IPSec, 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] [10].

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 the router can be seen as shown in Figure 1 [4].

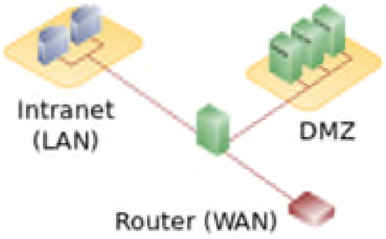


Figure 1 DMZ Server

The interconnected network on Figure 1, then will be implemented in one small company and it will be tested with several scenarios such as testing the inter-network connectivity testing, DHCP testing, and firewall testing and also the testing of several threats which will be addressed by Snort [9].

2. Discussion

UTM Endian serves as the center of the network, all types of data traffic are regulated through the port inter-zone rule in Endian, also the accessing internet can be set using a proxy as the user needed. Generally, the network topology that implements Endian can be seen in the Figure 2 below. However, the implementation of endian in this company will be assign as a picture shown in the Figure 4.

The UTM Endian is design as a firewall system that used to protect the corporate intranet. *Firewall* can be used to authenticate the user from outside network, verify the level of access authority, and then redirect the user to program, data or requested services. Besides protecting the enterprise network from the external network, the firewall can also be used to protect LANs from unauthorized internal access [5]–[8].

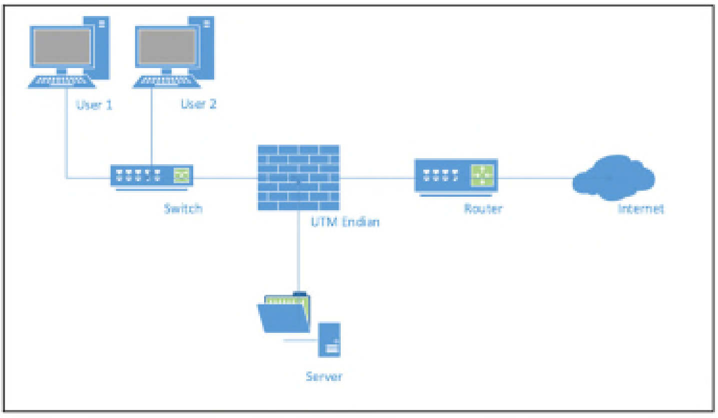
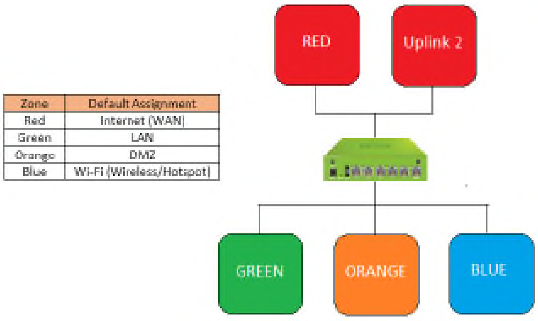


Figure 2 Implementation of Endian Network

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 3 Implementation of Endian Network

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

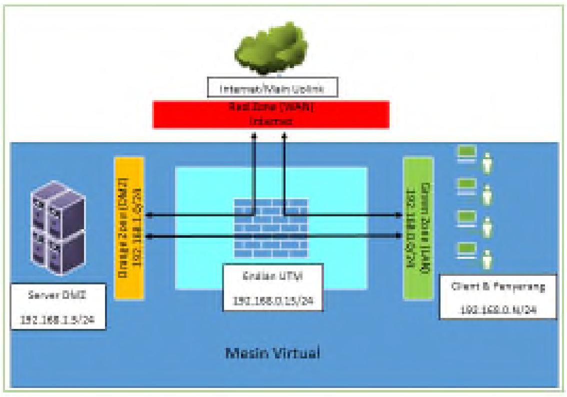


Figure 4 Network Topology

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 for this implementation 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 according with the endian topology.
2. Installation Endian UTM.
3. Perform the basic configuration of Endian.
4. DHCP Configuration.
5. Configure Content Filtering.
6. Configure port access restrictions on inter-zone.
7. Enabling IPS features on Endian UTM.
8. Simulate attacks such as port scanning and DDoS.

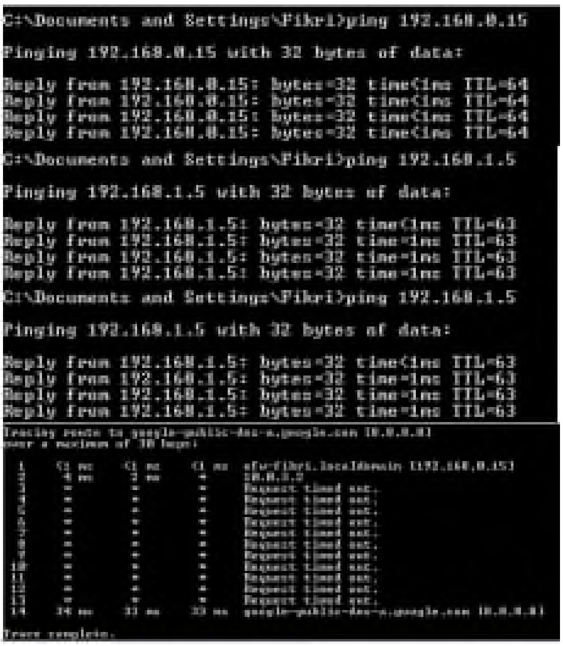
After doing the configuration, then do a ping test between the networks, ping the endian to internet, ping the endian to client, ping the endian to server, ping client to server, ping client to internet and trace the route Client to Internet. The next step we will testing the network using several scenarios.

3. Result

At this stage, we do some test to the implemented networks. 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 5 is the trace route of the connectivity testing.

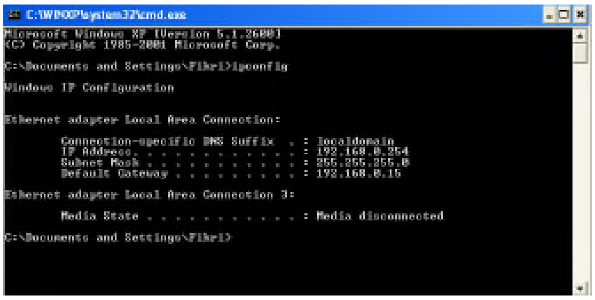


```
C:\Documents and Settings\Fikri>ping 192.168.0.15

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     3 ms     *     10.0.2.2
  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 5 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 6 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\Fikri1>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\Fikri1>
```

Figure 6 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 7 and 8 is the figure of sport category that will be blocked if the user list's it to the list of blocking content.

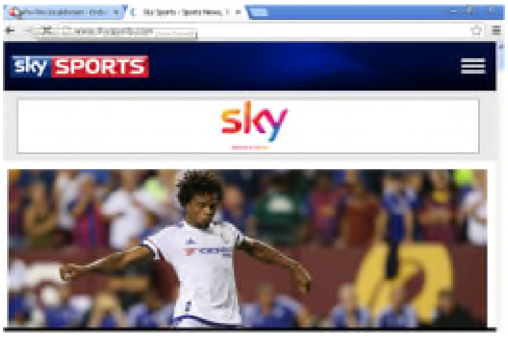
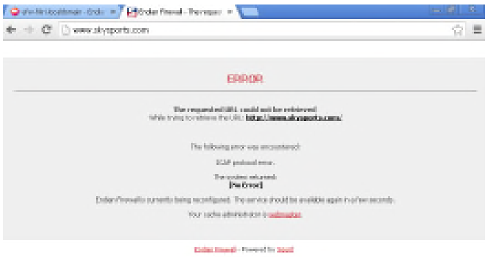


Figure 7 Site of Sport Categories Before Content Filtering



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.

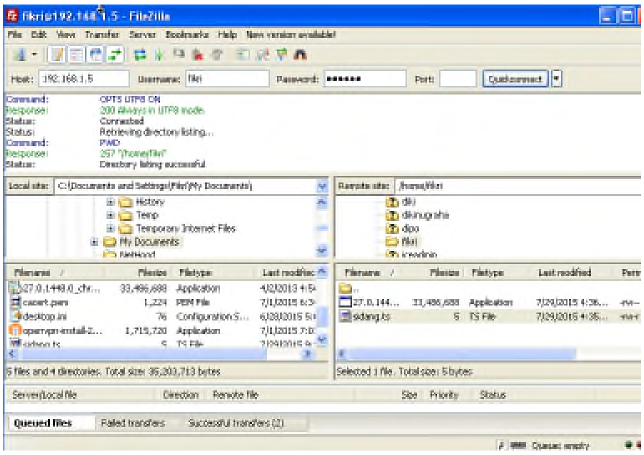
Your cache administrator is webmaster.

Endian Firewall - Powered by Squid

Figure 8 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 9 show that the client (green zone) is able to access the FTP server (orange zone). Figure 10 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 11 shows that the green zone cannot access port 21 (FTP) on the orange zone.


fikri@192.168.1.5 - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!

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

```
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

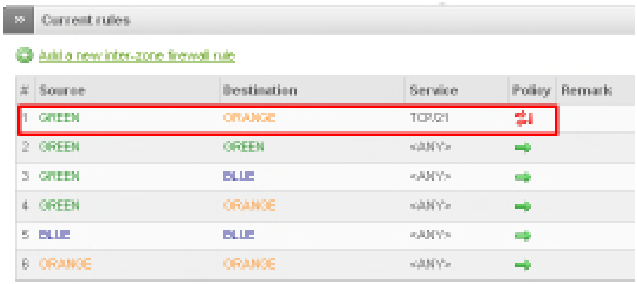
Filename	Filesize	Filetype	Last modified
27.0.1448.0_chr...	33,486,688	Application	4/2/2013 4:5
cacert.pem	1,224	PEM File	7/1/2015 6:3
desktop.ini	76	Configuration S...	6/28/2015 5:0
openvpn-install-2...	1,715,720	Application	7/1/2015 7:0
sidang.ts	5	TS File	7/29/2015 9:

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

Filename	Filesize	Filetype	Last modified	Perr
..				
27.0.144...	33,486,688	Application	7/29/2015 4:36...	-rw--
sidang.ts	5	TS File	7/29/2015 4:35...	-rw-r

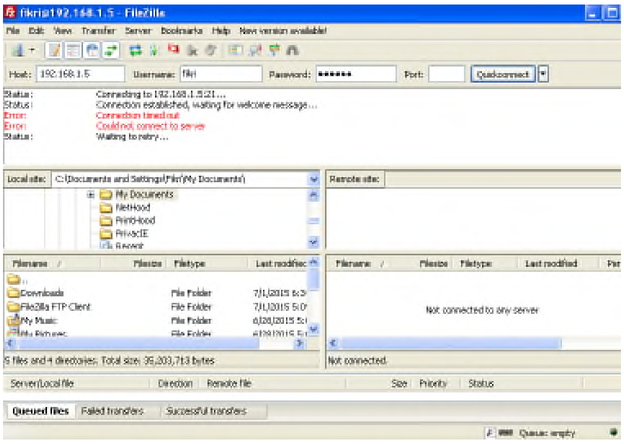
Selected 1 file. Total size: 5 bytes

Figure 9 Green Zone Port 21 on Orange Zone



#	Source	Destination	Service	Policy	Remark
1	GREEN	ORANGE	TCP/21	⇄	
2	GREEN	GREEN	<ANY>	➡	
3	GREEN	BLUE	<ANY>	➡	
4	GREEN	ORANGE	<ANY>	➡	
5	BLUE	BLUE	<ANY>	➡	
6	ORANGE	ORANGE	<ANY>	➡	

Figure 10 Blocking Port FTP on Orange Zone


fikri@192.168.1.5 - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!

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

```
Status:    Connecting to 192.168.1.5:21...
Status:    Connection established, waiting for welcome message...
Error:     Connection timed out
Error:     Could not connect to server
Status:    Waiting to retry...
```

Local site: C:\Documents and Settings\Fikri\My Documents\ — Remote site:

Filename	Filesize	Filetype	Last modified
..			
Downloads		File Folder	7/1/2015 6:3
FileZilla FTP Client		File Folder	7/1/2015 5:0
My Music		File Folder	6/28/2015 5:
My Pictures		File Folder	6/28/2015 5:

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

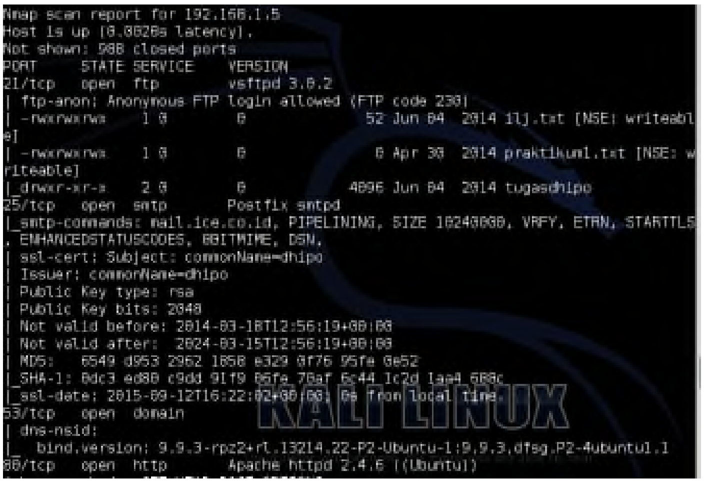
Not connected to any server

Not connected.

Figure 3 FTP Service on The Blocking Hit

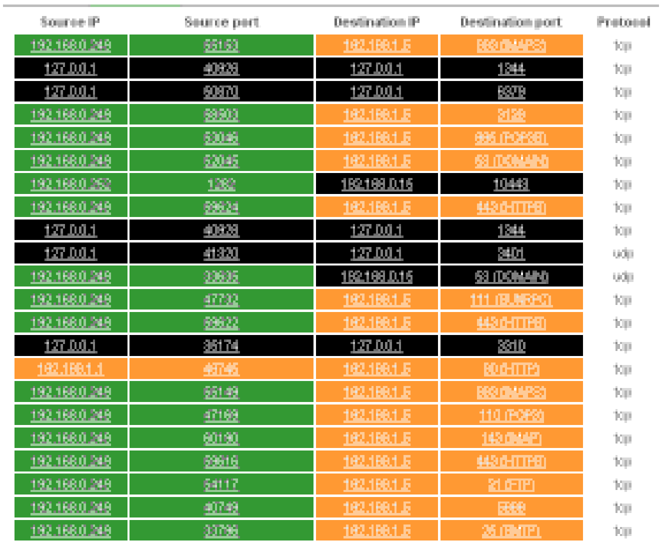
3.3.3. Testing the Report an IPS attacked

Figure 12 shows a report about simulation attack done by Platform Kali Linux. Port scanning attack is successful, but IPS failed to get a log of port scanning. This is because port scanning is not listed in the IPS rules. However, this attack was detected in the status menu connections on Figure 13.



```
Nmap scan report for 192.168.1.5
Host is up (0.0026s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rwxrwxrwx    1 0        0              52 Jun 04  2014 1lj.txt [NSE: writeabl
e]
| -rwxrwxrwx    1 0        0               0 Apr 30  2014 praktikum1.txt [NSE: w
riteable]
|_drwxr-xr-x    2 0        0            4096 Jun 04  2014 tugasdhipo
25/tcp   open  smtp       Postfix smtpd
|_smtp-commands: mail.ice.co.id, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS
, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=dhipo
| Issuer: commonName=dhipo
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2014-03-18T12:56:19+00:00
| Not valid after:  2024-03-15T12:56:19+00:00
| MD5:   6549 d953 2962 1058 e329 0f76 95fe 0e52
|_SHA-1: 0dc3 ed80 c9dd 91f9 05fe 70af 6c44 1c2d 1aa4 600c
|_ssl-date: 2015-09-12T16:22:02+00:00; 0s from local time.
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.9.3-rpz2+rl.13214.22-P2-Ubuntu-1:9.9.3.dfsg.P2-4ubuntu1.1
80/tcp   open  http       Apache httpd 2.4.6 ((Ubuntu))
```

Figure 4 Port Scanning Attacked



Source IP	Source port	Destination IP	Destination port	Protocol
192.168.0.249	55153	192.168.1.5	993 (IMAPS)	tcp
127.0.0.1	40928	127.0.0.1	1344	tcp
127.0.0.1	60870	127.0.0.1	6379	tcp
192.168.0.249	59503	192.168.1.5	3128	tcp
192.168.0.249	53046	192.168.1.5	995 (POP3S)	tcp
192.168.0.249	52045	192.168.1.5	53 (DOMAIN)	tcp
192.168.0.252	1282	192.168.0.15	10443	tcp
192.168.0.249	59624	192.168.1.5	443 (HTTPS)	tcp
127.0.0.1	40928	127.0.0.1	1344	tcp
127.0.0.1	41320	127.0.0.1	8401	udp
192.168.0.249	33635	192.168.0.15	53 (DOMAIN)	udp
192.168.0.249	47732	192.168.1.5	111 (SUNRPC)	tcp
192.168.0.249	59622	192.168.1.5	443 (HTTPS)	tcp
127.0.0.1	36174	127.0.0.1	8310	tcp
192.168.1.1	48746	192.168.1.5	80 (HTTP)	tcp
192.168.0.249	55149	192.168.1.5	993 (IMAPS)	tcp
192.168.0.249	47169	192.168.1.5	110 (POP3)	tcp
192.168.0.249	60130	192.168.1.5	143 (IMAP)	tcp
192.168.0.249	59616	192.168.1.5	443 (HTTPS)	tcp
192.168.0.249	54117	192.168.1.5	21 (FTP)	tcp
192.168.0.249	30749	192.168.1.5	5666	tcp
192.168.0.249	33796	192.168.1.5	25 (SMTP)	tcp

Figure 5 Port Scanning Attacked Detection

Besides port scanning attacks, we also conducted testing of DDoS (Distributed Denial of Service) attack. DDoS attacks successfully attacked server but likewise as the previous test, the attacks cannot be seen on IPS logs. This is because the attacked did not listed on IPS rules. When the attack was checked via the status menu connections, there is only one connection ICMP (Internet Control Message Protocol) conducted an attacker on the server.

3.4. Conclusion

The conclusion of implementation network management using Endian Topology and feature DHCP is work done smoothly. The implementation of the proxy on filtering contents is successfully good on doing the filter. Also the blocking port from the inter-zone is running well but unfortunately, the IPS feature is failed to detect the attacks which is carried out due to the limitation number of snort rules. Besides that, in the future, this endian topology can be implemented in many areas which need securing small topology server.

Bibliography

[1] Anonim, "Produk Unified Threat Management," 2011. [Online]. Available: http://netsolution.co.id/unified-threat-management.htm. [Accessed 27 June 2015].

[2] Anonim, "Endian UTM," [Online]. Available: http://www.endian.com. [Accessed 27 June 2015]

[3] T. Zeller, "New versions of the Endian and Sophos UTM solutions," 2014. [Online]. Available: http://www.admin-magazine.com/Archive/2014/20/New-versions-of-the-Endian-and-Sophos-UTM-solutions. [Accessed 27 June 2015].

[4] Anonim, "DMZ," [Online]. Available: http://www.proweb.co.id/articles/support/dmz.html. [Accessed 30 June 2015].

[5] I. A. Dhotre, Information Security, Technical Publication, 2009.

[6] M. Sanusi, The Genius: Hacking untuk membobol Facebook & Email, Jakarta: PT. Elex Media Komputindo, 2010.

[7] W. Komputer, Tutorial 5 Hari: Belajar Hacking dari Nol, Semarang: Penerbit ANDI, 2010.

[8] J. Enterprise, Membuat Jaringan Internet Wireless Tanpa Bantuan Teknisi, Jakarta: PT. Elex Media Komputindo, 2009.

[9] E. S. Mulyanta, Pengenalan Protokol Jaringan Wireless Komputer, Yogyakarta: Penerbit ANDI, 2005.

[10] S. Laverty, "Endian Firewall Hardware Requirements," [Online]. Available: Endian Firewall Hardware Requirements. [Accessed 27 June 2015].