Pengamanan Layanan Private Cloud Storage Menggunakan HTTPS, IPTables dan SSTP

I Putu Hariyadi[1], Raisul Azhar[2]
[1,2]STMIK Bumigora; Jalan Ismail Marzuki Mataram,(0370) 634498
Jurusan Teknik Informatika, Nusa Tenggara Barat
: [1]putu.hariyadi@stmikbumigora.ac.id, [2]raisul.azhar@stmikbumigora.ac.id

Abstract

STMIK Bumigora is a computer college in the province of West Nusa Tenggara (NTB). The spread of data from 12 (twelve) sections on each staff computer or section head causes data search both within and between sections to be inefficient. The condition underlies the prototype development of Nextcloud-based Private Cloud Storage system as centralized data storage for each part. This system has been successfully created and tested and received a positive response for immediate implementation. But PusTIK as part of managing Information and Communication Technology (ICT) is still considering to delay implementation until security is done to access and transfer data between client to Private Cloud Storage Server. In addition there is also a need to remain able to access to Cloud Storage services from the Internet, especially when the academic community is on duty out of town or out of campus. The implementation of Secure Socket Tunneling Protocol (IPTables) and Secure Socket Tunneling Protocol (VPN) based Server Protocol Secure (HTTPS) and IPTables on Gateway Routers can help solve the problems encountered. Based on the analysis there is a known test results HTTPS can secure access and transfer data from client to Cloud Storage Server. While IPTables can protect Private Cloud Storage server from unwanted traffic so it can keep the service available. In addition, SSTP can bridge the need for access and security of communications to Private Cloud Storage service from the Internet.

Keywords: *Cloud Storage, HTTPS, IPTables, SSTP, Nextcloud*

1. PENDAHULUAN

STMIK Bumigora merupakan salah perguruan tinggi komputer yang terdapat di propinsi Nusa Tenggara Barat (NTB). Untuk mendukung kegiatan operasional institusi dan proses belajar mengajar baik di ruang kelas maupun laboratorium maka telah dibangun infrastruktur jaringan kampus baik menggunakan media kabel maupun nirkabel dan penyediaan koneksi *Internet* bagi civitas akademika. Dengan adanya infrastruktur jaringan kampus dan *Internet* membuat civitas akademika dapat melakukan aktivitas berbagi pakai file (*sharing*), korespondensi dan komunikasi baik dengan pihak internal maupun eksternal. Pengelolaan keseluruhan infrastruktur jaringan kampus dan operasional Teknologi Informasi dan Komunikasi (TIK) di STMIK Bumigora berada dibawah tanggungjawab bagian Pusat Teknologi Informasi dan Komunikasi (PusTIK).

Pada awalnya PusTIK memiliki permasalahan terkait manajemen data civitas akademika khususnya di bagian atau departemen yang terdapat pada struktur organisasi institusi. Terdapat 12 (duabelas) bagian atau departemen antara lain Administrasi Umum (ADUM), Keuangan, Akademik, Badan Perencanaan dan Pengembangan (BPP), Laboratorium, Badan Penjaminan Mutu (BPM), Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM), Lembaga Sertifikat Profesi (LSP), Perpustakaan, Program Studi dan Manajemen serta PusTIK. Permasalahan yang dihadapi meliputi tersebarnya data dari masing-masing bagian di setiap komputer staf atau kepala bagian yang menyebabkan pencarian data baik di dalam

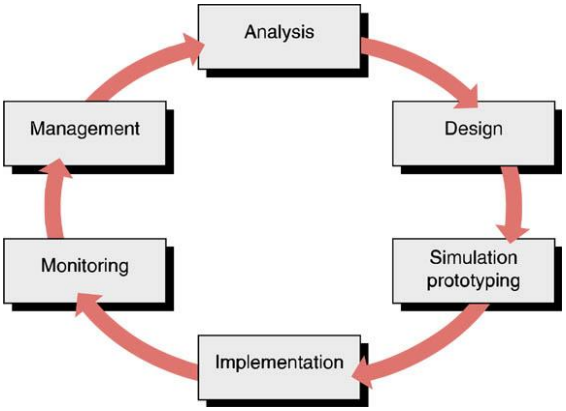
maupun antar bagian menjadi tidak efisien dan aktivitas *backup* untuk pengamanan data sulit dilakukan sehingga rentan terjadi kehilangan data sebagai akibat penyimpanan data yang tersebar. Kondisi tersebut memunculkan ide adanya suatu sistem penyimpanan terpusat yang dapat mengakomodasi struktur organisasi dari institusi sehingga dapat mempercepat pencarian data baik di dalam maupun antar bagian dan mempermudah aktivitas *backup* sehingga keamanan data tetap terjaga.

Dalam mewujudkan ide sistem tersebut, PusTIK telah membangun *prototype* dari sistem *Private Cloud Storage* berbasis *Nextcloud* sebagai penyimpanan data terpusat bagi setiap bagian. *Private Cloud* merupakan infrastruktur *cloud* yang ditujukan untuk penggunaan eksklusif oleh satu organisasi dengan beberapa konsumen sebagai contoh unit bisnisnya. *Private Cloud* dapat dimiliki, dikelola dan dioperasikan oleh organisasi, pihak ketiga, atau gabungannya serta dapat berada di dalam atau luar organisasi [1]. *Cloud Storage* adalah sistem yang menyediakan fungsi penyimpanan data di *cloud computing* dan dibentuk dari berbagai jenis perangkat penyimpanan dengan kapasitas besar serta program aplikasi [2]. *Nextcloud* merupakan perangkat lunak *open source* yang dapat digunakan untuk membangun server dengan layanan sinkronisasi file dan berbagi pakai file (*share*) serta dapat dikelola sendiri (*self-hosted*) [3]. Sistem ini telah berhasil dibuat dan diujicobakan ke beberapa bagian serta mendapat respon positif agar dapat segera diimplementasikan. Namun PusTIK masih mempertimbangkan untuk menunda implementasi sampai dilakukan analisa terkait aspek keamanan terutama akses dan transfer data antar client ke *ServerPrivate Cloud Storage*. Selain itu terdapat pula kebutuhan agar tetap dapat mengakses ke layanan *Cloud Storage* dari Internet terutama ketika civitas akademika sedang bertugas keluar kota atau diluar kampus.

HyperText Transfer Protocol Secure (HTTPS) dan *IPTables* dapat mengamankan akses dan transfer data pada *Server* yang memuat layanan *Private Cloud Storage* berbasis *Nextcloud*. HTTPS merupakan protokol komunikasi *Internet* yang digunakan untuk melindungi integritas dan kerahasiaan dari data antara komputer pengguna dengan situs [4]. Terdapat 3 (tiga) lapisan keamanan yang diproteksi ketika data dikirimkan melalui HTTPS yaitu *encryption*, *data integrity* dan *authentication* [4].Dengan diterapkannya HTTPS maka komunikasi antara *client* dengan *serverPrivate Cloud Storage*akan dienkripsi sehingga proses file transfer baik ketika proses unggah, unduh maupun otentikasi login pengguna layanan menjadi terproteksi. Proteksi ini sebagai bentuk perlindungan terhadap kerahasiaan data yang ditransmisikan di jaringan ketika memanfaatkan layanan *Cloud Storage*sehingga dapat meminimalkan dampak dari aktivitas *sniffing* seperti pencurian data oleh pengguna di jaringan. Sedangkan *IPTables* merupakanprogram *command line* yang digunakan oleh *system administrator* untuk melakukan pemfilteran paket yang disediakan oleh *kernel Linux 2.4.x*sehingga berfungsi sebagai *firewall*[5]. Penerapan *IPTables* dapat melindungi *server Private Cloud Storage* dari trafik yang tidak diinginkan. Selain itu penerapan *Secure Socket Tunneling Protocol (SSTP)* pada *Router Gateway* dapat menjembatani kebutuhan akses bagi civitas akademika yang sedang berada diluar kampus ke layanan *Private Cloud Storage* dari *Internet* melalui *Remote AccessVirtual Private Network (VPN)*sekaligus pengamanan komunikasinya.SSTP merupakan bentuk baru dari *VPN tunnel* yang menyediakan mekanisme untuk mengenkapsulasi trafik *Point-to-Point Protocol (PPP)* melalui jalur *Secure Socket Layer (SSL)* dari protokol HTTPS [6].

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah *Network Development Life Cycle (NDLC)*. NDLC terdiri dari 6 (enam) tahapan meliputi *analysis*, *design, simulation prototyping, implementation*, *monitoring* dan *management*, seperti terlihat pada gambar 1 [7].



Gambar 1 Network Development Life Cycle [7]

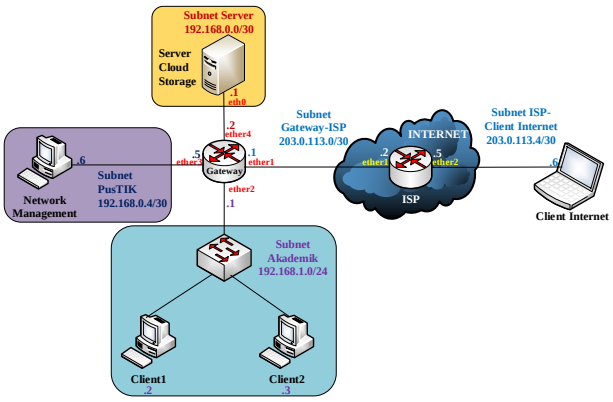
Dari 6 tahapan yang terdapat pada NDLC, peneliti hanya menggunakan 3 tahapan pertama yaitu *analysis*, *design* dan *simulation prototyping*.

2.1 Tahap Analysis

Pada tahap ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa terhadap topologi/jaringan yang sudah ada saat ini [8]. Sebelum dapat melakukan proses analisis maka terlebih dahulu dilakukan pengumpulan data menggunakan berbagai teknik meliputi observasi, wawancara dan dokumentasi.

2.2 Tahap Desain

Pada tahap ini dilakukan pembuatan rancangan jaringan ujicoba dan rancangan pengalamatan IP sertarancangan akun pengguna untuk ujicobapengaksesan ke *Private Cloud Storage*. Rancangan jaringan ujicoba untuk pengamanan layanan *Private Cloud Storage*, seperti terlihat pada gambar 2. Rancangan jaringan ujicoba ini terdiri dari 2 (dua) bagian yaitu *Local Area Network (LAN)* dan *Internet*. Koneksi LAN ke Internet dapat dilakukan melalui *router gateway*. Router gateway juga berfungsi sebagai *Virtual Private Network (VPN)Server* berbasis *Secure Socket Tunneling Protocol (SSTP)* untuk menerima *Remote Access* dari *Client Internet*. Pada LAN terdapat 3 (tiga) subnet yaitu *Server*, PusTIK dan Akademik.



Gambar 2 Rancangan Jaringan Ujicoba

Subnet *Server* terdiri dari 1 (satu) *server Cloud Storage.* Sedangkan pada subnet PusTIK terdapat 1 (satu) komputer yang difungsikan sebagai *network management*. Selain itu terdapat subnet Akademik yang terdiri dari 2 (dua) komputer *client* untuk ujicoba pengaksesan layanan *Cloud Storage* menggunakan rancangan akun pengguna, seperti terlihat pada gambar 4 dan aktivitas *sniffing*.Pada jaringan Internet terdiri dari 1 (satu) *router Internet Service Provider (ISP)* untuk menyediakan layanan Internet bagi LAN dan *Client Internet*. *Client Internet* digunakan untuk mensimulasikan pengaksesan layanan *Private Cloud Storage* melalui *Internet* oleh civitas akademika yang sedang berada diluar kampus. *Client Internet* terlebih dahulu harus melakukan koneksi VPN sebelum dapat mengakses layanan *Private Cloud Storage*.

Rancangan pengalamatan IP untuk jaringan ujicoba menggunakan 3 (tiga) alamat *network* yaitu 192.168.0.0/24 yang di*subnetting* sesuai dengan jumlah kebutuhan pengalamatan pada subnet *Server* (192.168.0.0/30) dan PusTIK (192.168.0.4/30), 192.168.1.0/24 untuk subnet akademik serta 203.0.113.0/24 yang di*subnetting* sesuai dengan jumlah kebutuhan pengalamatan pada *subnet Gateway-ISP*(203.0.113.0/30) dan *ISP-Client Internet* (203.0.113.4/30). Detail alokasi pengalamatan IP per perangkat, seperti terlihat pada tabel 1.

Tabel 1 Alokasi Pengalamatan IP

No.	Perangkat	Interface	Alamat IP	Gateway
1.	*Server Cloud Storage*	*Eth0*	192.168.0.1/30	192.168.0.2
2.	*Router Gateway*	*Ether1*	203.0.113.1/30	203.0.113.2
		Ether2	192.168.1.1/24	
		Ether3	192.168.0.5/30	
		Ether4	192.168.0.2/30	
3.	*Network Management*	*Local Area Connection*	192.168.0.6/30	192.168.0.5
4.	*Client1*	*Local Area Connection*	192.168.1.2/24	192.168.1.1
5.	*Client2*	*Local Area Connection*	192.168.1.3/24	192.168.1.1
6.	*Router ISP*	*Ether1*	203.0.113.2/30	
		Ether2	203.0.113.5/30	
7.	*Client Internet*	*Local Area Connection*	203.0.113.6/30	203.0.113.5

Rancangan akun pengguna untuk ujicoba pengaksesan ke layanan *Private Cloud Storage*, seperti terlihat pada tabel 2. Terdapat 4 (empat) akun yang dibuat untuk mewakili ujicoba dari bagian kepala bagian, staf dan dosen.

Tabel 2 Akun Pengguna *Private Cloud Storage*

No.	Username	Password	Deskripsi
1.	ka-pustik	pustik2017!	Digunakan untuk ujicoba akses oleh kepala bagian di bagian PusTIK melalui komputer *Network Management* yang terdapat di subnet PusTIK.
2.	ka-akademik	akademik2017!	Digunakan untuk ujicoba akses oleh kepala bagian di bagian Akademik melalui Client1 yang terdapat di subnet Akademik.
3.	staf-akademik	staf2017!	Digunakan untuk ujicoba akses oleh staf di bagian Akademik melalui Client2 yang terdapat di subnet Akademik.
4.	dosen	dosen2017!	Digunakan untuk ujicoba akses oleh dosen melalui *Remote Access VPN Connection* dari *Client Internet*.

2.3 Tahap Simulation Prototyping

Tahap *simulation prototyping* dibagi menjadi dua bagian yaitu konfigurasi dan ujicoba baik verifikasi konfigurasi maupun skenario.Konfigurasi dilakukan di keseluruhan perangkat yang terlibat yaitu *Server Private Cloud Storage*, *Router Gateway*, *Personal Computer (PC) Network Management*, *PC Client1*, *PC Client2* dan *Router ISP* serta *PCClient Internet*. Sedangkan ujicoba dibagi menjadi 2 (dua) jenis yaitu verifikasi konfigurasi dan ujicoba berbasis skenario. Verifikasi konfigurasi dilakukan pada seluruh perangkat meliputi verifikasi pengalamatan IP dan koneksi antar perangkat.Sedangkan ujicoba berbasis skenario terdiri dari 4 (empat) skenario yang digunakan untuk mengujicoba konfigurasi.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Konfigurasi

Konfigurasi dilakukan pada 7 (tujuh) perangkat jaringan. Pada *Server Private Cloud Storage* terdapat 4 (empat) bagian yang dikonfigurasi meliputiinstalasi *mod_ssl* sebagai modul dari *web server Apache* untuk menyediakan dukungan enkripsi SSL, membuat *self-signed SSLcertificate* dan *server key* secara bersamaan dengan masa berlaku 365 hari, menerapkan *SSL certificate*yang telah dibuat pada *web server Apache*, mengatur*firewall* berbasis*IPTables* untuk mengijinkan hanya *service HTTP* dan *HTTPS* yang dapat diakses oleh seluruh *PC Client* serta akses SSH hanya dapat diakses dari subnet PusTIK.Berikut adalah cuplikan hasil konfigurasi *directive* untuk penerapan sertifikat SSL pada *file/etc/httpd/conf.d/ssl.conf* dari *Apache*:

```
DocumentRoot
"/var/www/html/nextcloud"

ServerName
drive.stmikbumigora.local:443

SSLCertificateFile
/etc/ssl/certs/apache-
selfsigned.crt

SSLCertificateKeyFile
/etc/ssl/private/apache-
selfsigned.key
```

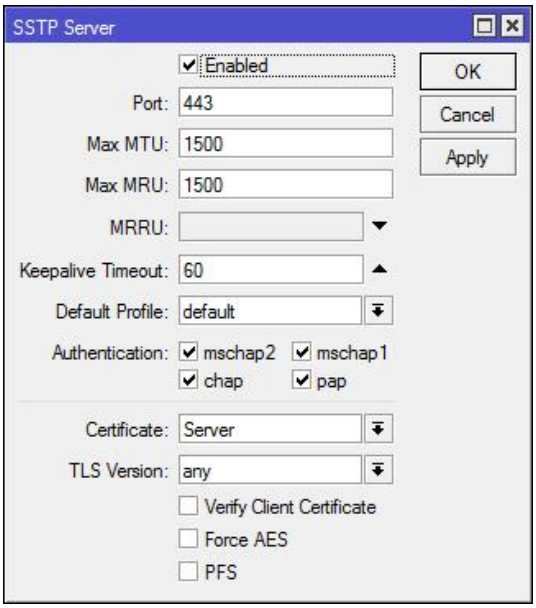
Sedangkan cuplikan dari hasil konfigurasi *IPTables*adalah sebagai berikut:

```
iptables -F

iptables -P INPUT DROP

iptables -A INPUT -m state --
state ESTABLISHED,RELATED -j
ACCEPT

iptables -A INPUT -m state --
state NEW -p tcp --dport 80 -j
ACCEPT

iptables -A INPUT -m state --
state NEW -p tcp --dport 443 -j
ACCEPT

iptables -A INPUT -s 192.168.0.6
-m state --state NEW -p tcp --
dport 22 -j ACCEPT

iptables -A INPUT -p icmp -j
ACCEPT

iptables -A INPUT -i lo -j ACCEPT
```

Kebijakan keamanan yang diterapkan menggunakan *IPTables*pada *Server Private Cloud Storage*adalah mengijinkan akses HTTP dan HTTPS serta *Internet Control Message Protocol (ICMP)* dari seluruh jaringan dan mengijinkan akses *Secure Shell (SSH)* hanya dari *PC Network Monitoring*.

Pada *router gateway*menggunakan *Mikrotik* dilakukan konfigurasi meliputi pembuatan *template Certificate Authority (CA)*, *Server* dan *Client Certificate*, *export certificate* yang telah dibuat yang digunakan oleh *PC Client Internet* yang bertindak sebagai *SSTP Client*, pengaktifan fitur *SSTP Server* dan pembuatan akun pengguna untuk koneksi dari *SSTP*

Client.Hasil pengaktifan *SSTP Server*, seperti terlihat pada gambar 3.



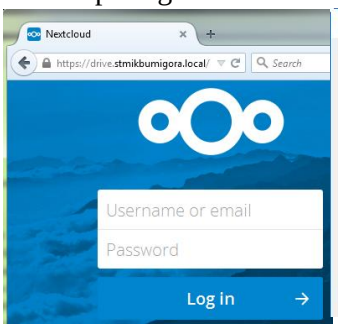
Gambar 3 Pengaktifan SSTP Server

Pada*PC Network Management*, *Client1* dan *Client2* serta *Client Internet* dilakukan pengaturan pengalamatan IP secara statik. Selain itu pada *Client Internet* juga dilakukan proses *import certificate* dan pembuatan *VPN Client Connection* sebagai sarana *remote access* ke *VPN Server* berbasis SSTP.

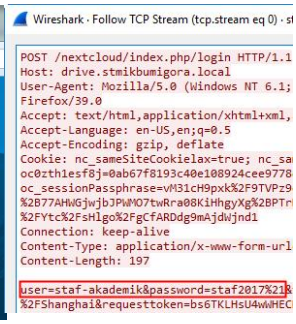
3.2 Hasil Ujicoba

Terdapat 4 (empat) skenario utama yang digunakan untuk mengujicoba konfigurasi yaitu mengakses layanan *Cloud Storage* menggunakan *HTTPS* dari *Client*, melakukan *sniffing* komunikasi*PC Client*ke *Server Private Cloud Storage* baik sebelum maupun sesudah penerapan HTTPS terkait proses otentikasi login maupun file transfer, koneksi *SSTP Client* ke *SSTP Server* dan verifikasi konfigurasi *IPTables* dengan melakukan *SSH* dari *Client Internet*.

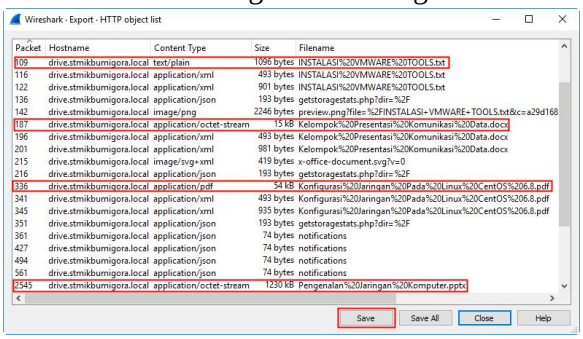
Hasil ujicoba pengaksesan layanan *Cloud Storage*dari salah satu *Client* yaitu dari *Client1* yang terdapat di subnet Akademik,seperti ditunjukkan pada gambar 4. Terlihat layanan *Cloud Storage* sukses diakses dari *PCClient1* dan secara otomatis di *redirect* menggunakan HTTPS. Sedangkan pada gambar 5 memperlihatkan hasil ujicoba *sniffing* menggunakan *wireshark* ketika *PC Client1* melakukan otentikasi login ke *Cloud Storage*sebelum menggunakan HTTPS. Terlihat akun untuk otentikasi login dari pengguna berhasil tersadap yaitu *username* "staf-akademik" dengan *password* "staf2017!".Begitu pula data pengguna dapat diekstrak berdasarkan hasil ujicoba *sniffing*file transfer menggunakan *wireshark*sebelum menerapkan HTTPS, seperti terlihat pada gambar 6.



Gambar 4Homepage Private Cloud Storage

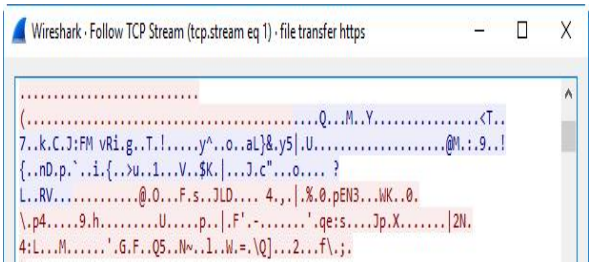


Gambar 5 Sniffing Login HTTP



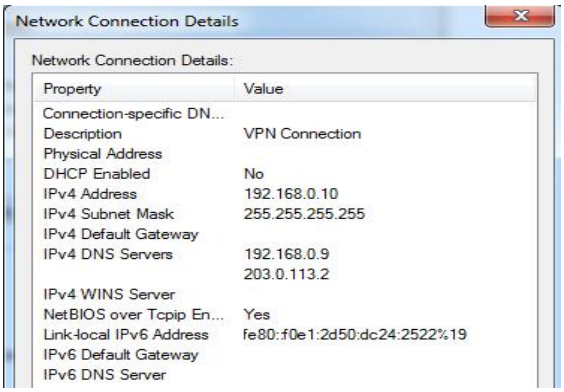
Gambar 7 Ekstrak File dari Capture Trafik HTTP

Sebaliknya sesudah menggunakan HTTPS, data akun login pengguna tidak dapat diketahui dan file transfer dari layanan *Cloud Storage* tidak berhasil diekstrak, seperti terlihat pada gambar 7.

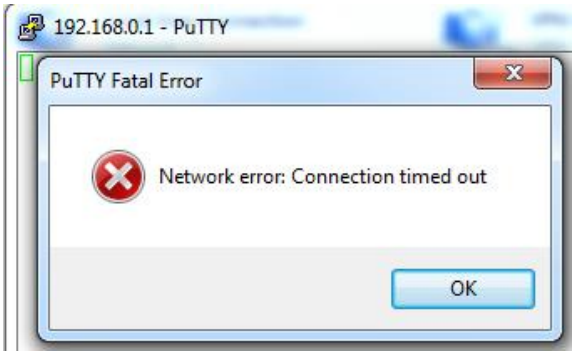


Gambar 7 Capture File Transfer Trafik HTTPS

Gambar 8memperlihatkan hasil ujicoba koneksi dari *SSTP Client*yaitu *PC Client Internet* ke *SSTP Server*yang telah berhasil dilakukan.Terlihat *PC Client Internet* memperoleh pengalamatan IP 192.168.0.10.



Gambar 8 Koneksi



Gambar 9 SSH Client

Sedangkan hasil ujicoba akses *SSH*dari *PCClient Internet*ke *Server Private Cloud Storage*, seperti ditunjukkan pada gambar 9.Terlihat koneksi SSH gagal dilakukan karena telah diterapkan pemfilteran menggunakan *IPTables* yang hanya mengijinkan akses SSH dari *PC Network Management*.

3.3 Analisa Hasil Ujicoba

Berdasarkan ujicoba yang telah dilakukan maka dapat diperoleh hasilanalisa sebagai berikut:

1. Akun untuk otentikasi login pengguna layanan *Private Cloud Storage* yaitu berupa *username* dan password dapat diketahui dari trafik HTTP yang di *capture* menggunakan *Wireshark* dengan memanfaatkan fitur *Follow TCP Stream.*
2. File yang ditransfer oleh pengguna layanan *Private Cloud Storage* berhasil diekstrak dari trafik HTTP yang di*capture* menggunakan *Wireshark* dengan memanfaatkan fitur *Export Object*.
3. Akun berupa *username* dan *password* untuk otentikasi login serta file yang ditransfer oleh pengguna layanan *Private Cloud Storage* tidak dapat diekstrak dari trafik HTTPS yang di*capture* menggunakan *Wireshark*.
4. Civitas akademika dapat mengakses layanan *Cloud Storage* yang terdapat di jaringan internal dari *Internet* dengan melakukan *Remote Access VPN*menggunakan SSTP.
5. *IPTables* dapat membatasi layanan yang dapat diakses pada *Server Private Cloud Storage* meliputi SSH yang hanya dapat diakses dari subnet PusTIK dan HTTP serta HTTPS dari keseluruhan jaringan sehingga dapat mengamankan *Server*.

4. KESIMPULAN

Berdasarkan konfigurasi dan ujicoba serta analisa terhadap hasil ujicoba yang telah

dilakukan maka dapat diambil kesimpulan sebagai berikut:

a. HTTPS dapat mengamankan akses dan transfer data dari client ke *Server Private Cloud Storage* melalui pengujian *sniffing* menggunakan *Wireshark*.
b. *IPTables* dapat melindungi *server Private Cloud Storage* dari trafik yang tidak diinginkan melalui pemfilteran paket sehingga dapat menjaga layanan tetap tersedia.
c. *Remote Access VPN* berbasis *SSTP* dapat menjembatani kebutuhan akses dan pengamanan komunikasi ke layanan *Private Cloud Storage* dari *Internet*.

5. SARAN

Adapun saran-saran untuk pengembangan penelitian ini lebih lanjut adalah sebagai berikut:

a. Mengembangkan *cloud storage* dengan fitur *high availability*melalui penerapan *clustering* agar layanan tetap beroperasi atau *zero downtime* ketika salah satu server yang mengelola layanan mengalami permasalahan.
b. Mengintegrasikan fitur otentikasi *cloud storage* dengan sistem otentikasi*single sign-on*sehingga civitas akademika dapat menggunakan akun yang samaseperti yang digunakan ketika mengakses layanan sistem informasi perguruan tinggi dan layanan *hotspot* kampus.
c. Menganalisa performansi dari teknik pengamanan *cloud storage* yang diterapkan.

DAFTAR PUSTAKA

[1] NIST. 2013. NIST Cloud Computing Standards Roadmap. https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf. Diakses pada tanggal 4Oktober 2017

[2] Kun, L dan Long-jiang D. 2012. Research on Cloud Data Storage Technology and Its Architecture Implementation. Procedia Engineering International Workshop on Information and Electronics Engineering. Volume 29. Hal. 133-137

[3] Nextcloud. 2017. Nextcloud 12 User Manual Introduction. https://docs.nextcloud.com/server/12/user_manual/index.html. Diakses tanggal 4 Oktober 2017

[4] Google. 2017. Secure your site with HTTPS. https://support.google.com/webmasters/answer/6073543?hl=en. Diakses tanggal 4 Oktober 2017

[5]Pablo Neira Ayuso. 2017. "The netfilter.org "iptables" project". https://www.netfilter.org/projects/iptables/index.html. Diakses tanggal 4 Oktober 2017

[6] Microsoft. 2007. SSTP Remote Access Step-by-Step Guide: Deployment. https://technet.microsoft.com/enus/library/cc731352(v=ws.10).aspx. Diakses tanggal 4 Oktober 2017

[7] James E.Goldman dan Phillip T. Rawles. 2004. The Network Development Life Cycle. http://higheredbcs.wiley.com/legacy/college/goldman/0471346403/lecture_slides/ch10.ppt?newwindow=true. Diakses tanggal 4Oktober 2017

[8] Deris Stiawan. 2009. Fundamental Internetworking Development & Life Cycle. http://unsri.ac.id/upload/arsip/network_development_cycles.pdf, Diakses tanggal 4Oktober 2017