JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620

Implementasi Network Attached Storage Synology dengan High Availability dan Akses Aman Melalui VPN dan Two Authentication di PT Mitra Tera Sinergi

M. Alfi Nurpiansyah[1,*], Taufik Asra[2]

[1,2]Fakultas Teknik dan Informatika, Teknologi Informasi, Univeristas Bina Sarana Informatika, Kota Jakarta Selatan, Indonesia
Email: [1*]alfinurpiansyah@gmail.com, [2]taufik.tas@bsi.ac.id
(*Email Corresponding Author: alfinurpiansyah@gmail.com)
Received: September 3, 2025 | Revision: September 22, 2025 | Accepted: September 22, 2025

Abstrak

Penelitian ini dilaksanakan di PT. Mitra Tera Sinergi yang sebelumnya menggunakan OwnCloud sebagai sistem penyimpanan data internal. Sistem tersebut hanya berjalan pada satu server tanpa dukungan High Availability (HA) dan diakses langsung melalui IP publik tanpa pengamanan yang memadai. Kondisi ini menyebabkan tingginya risiko terhadap downtime serta ancaman keamanan dari luar jaringan. Untuk menjawab permasalahan tersebut, penelitian ini mengusulkan implementasi sistem penyimpanan data berbasis Synology Network Attached Storage (NAS) yang dilengkapi dengan fitur High Availability melalui konfigurasi Synology High Availability (SHA), koneksi Virtual Private Network (VPN), serta autentikasi dua faktor (2FA) menggunakan Google Authenticator. VPN digunakan untuk mengamankan akses ke jaringan perusahaan dari luar, di mana hanya pengguna yang berhasil terhubung melalui VPN yang dapat mengakses sistem penyimpanan data internal. Sementara itu, 2FA berfungsi menambahkan lapisan keamanan ekstra pada proses login ke NAS, dengan mewajibkan pengguna memasukkan kode OTP yang dihasilkan dari aplikasi Google Authenticator. Sistem ini dijalankan pada dua server dengan mode aktif-pasif dan menggunakan IP virtual HA sebagai endpoint layanan. Hasil implementasi menunjukkan peningkatan signifikan dalam ketersediaan layanan, keamanan data, dan efisiensi manajemen jaringan internal.

Kata Kunci: OwnCloud, Synology NAS, High Availability, VPN, Two-Factor Authentication

Abstract

This research was conducted at PT. Mitra Tera Sinergi, which previously used OwnCloud as its internal data storage system. The system operated on a single server without High Availability (HA) support and was accessed directly via a public IP address without adequate security measures. This condition posed a high risk of downtime and external security threats. To address these issues, this study proposes the implementation of a data storage system based on Synology Network Attached Storage (NAS), equipped with High Availability through Synology High Availability (SHA) configuration, a secure connection via Virtual Private Network (VPN), and two-factor authentication (2FA) using Google Authenticator. VPN is used to secure remote access to the company network, allowing only users connected through VPN to access the internal data storage system. Meanwhile, 2FA adds an extra layer of protection during the NAS login process by requiring users to enter a One-Time Password (OTP) generated by the Google Authenticator app. The system is deployed on two servers in active-passive mode and uses a virtual HA IP as the service endpoint. The implementation results demonstrate significant improvements in service availability, data security, and internal network management efficiency.

Keywords*: OwnCloud, Synology NAS, High Availability, VPN, Two-Factor Authentication*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat mendorong setiap perusahaan untuk memiliki sistem penyimpanan data yang handal, aman, dan dapat diakses kapan saja. Data merupakan aset yang sangat penting bagi perusahaan, karena berisi informasi-informasi yang menunjang proses operasional, pengambilan keputusan, serta strategi bisnis jangka panjang. Oleh karena itu, pengelolaan data yang buruk atau sistem yang tidak andal dapat berakibat pada gangguan besar dalam aktivitas perusahaan, bahkan menimbulkan kerugian finansial dan reputasi.

PT. Mitra Tera Sinergi saat ini menggunakan sistem penyimpanan berbasis cloud (OwnCloud) tanpa dukungan fitur *High Availability* (HA), dan sistem keamanannya masih bergantung pada akses publik yang rentan terhadap gangguan serta ancaman siber. Sistem seperti ini memiliki sejumlah keterbatasan, terutama ketika terjadi gangguan teknis pada server utama yang menyebabkan akses data terputus. Selain itu, minimnya pengamanan pada akses luar jaringan internal menjadikan data perusahaan rentan terhadap akses tidak sah.

Untuk mengatasi permasalahan tersebut, diperlukan solusi penyimpanan data berbasis *Network Attached Storage* (NAS) dengan dukungan fitur *High Availability*, yang menjamin ketersediaan data secara terus-menerus meskipun terjadi kegagalan pada salah satu sistem, serta mampu mengurangi waktu *down time* atau bahkan mencegah terjadinya *down time* yang dapat mengganggu operasional perusahaan. NAS Synology dikenal sebagai solusi penyimpanan yang fleksibel, mudah dikelola, serta mendukung pengaturan HA yang efisien.

Selain ketersediaan data, aspek keamanan juga menjadi fokus utama, khususnya dalam hal akses dari luar jaringan kantor. Untuk memastikan koneksi jarak jauh tetap aman, sistem ini dirancang menggunakan *Virtual Private Network*

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620

(VPN) yang dikonfigurasi melalui perangkat MikroTik RouterOS. Melalui VPN, maka user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. "Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standar utama dalam VPN, sehingga dalam VPN selalu disertakan akan fitur utama yaitu enkripsi dan *tunnelling"* [1]. MikroTik mendukung berbagai protokol VPN seperti PPTP, L2TP/IPsec, dan SSTP, yang masing-masing memiliki karakteristik dan tingkat keamanan berbeda, sehingga dapat disesuaikan dengan kebutuhan dan kompatibilitas perangkat klien.

"Metode *Two factor authentication* merupakan pengamanan lapis kedua yang harus dilewati setelah memasukan username dan password" [2]. Sebagai tambahan lapisan pengamanan, sistem ini turut dilengkapi dengan *Two-Factor Authentication* (2FA) menggunakan aplikasi Google Authenticator, yang menambahkan verifikasi login berbasis kode waktu (*time-based OTP*). Kombinasi dari *High Availability*, VPN berbasis MikroTik, dan *Two-Factor Authentication* (2FA) ini bertujuan untuk membangun sistem penyimpanan data yang tidak hanya tersedia setiap saat, tetapi juga terlindungi dari berbagai ancaman keamanan.

Berdasarkan kondisi tersebut, penelitian ini merumuskan beberapa hal, yaitu bagaimana cara mengimplementasikan sistem penyimpanan data berbasis NAS Synology dengan High Availability di PT. Mitra Tera Sinergi, bagaimana merancang sistem akses yang aman ke data menggunakan NAS Synology dari luar kantor, serta langkah-langkah yang diperlukan untuk mengurangi waktu down time atau bahkan mencegah terjadinya down time dan kehilangan data akibat kegagalan sistem. Selain itu, penelitian ini juga membahas bagaimana cara mengintegrasikan sistem autentikasi dua langkah (2FA) untuk meningkatkan keamanan akses pengguna. Adapun tujuan dari penelitian ini adalah membangun sistem Network Attached Storage (NAS) Synology dengan fitur High Availability, serta merancang dan mengimplementasikan akses aman menggunakan VPN dan Two-Factor Authentication (2FA) di PT. Mitra Tera Sinergi.

2. METODOLOGI PENELITIAN

Penelitian ini merupakan penelitian terapan dengan pendekatan deskriptif studi kasus. Penelitian terapan dipilih karena berfokus pada penerapan langsung teknologi untuk menyelesaikan permasalahan nyata di PT. Mitra Tera Sinergi. Pendekatan deskriptif studi kasus digunakan untuk memberikan gambaran mendetail mengenai proses perancangan, implementasi, dan evaluasi sistem penyimpanan data berbasis Synology NAS dengan *High Availability*, Virtual Private Network (VPN), serta autentikasi dua faktor (2FA).

2.1 Teknik Pengumpulan Data

Data penelitian dikumpulkan dengan tiga metode utama:

a. Observasi : mengamati kondisi sistem penyimpanan data dan infrastruktur jaringan yang ada di PT. Mitra Tera Sinergi.
b. Wawancara : Wawancara dilakukan dengan bagian IT perusahaan untuk memperoleh informasi terkait kendala sistem saat ini dan kebutuhan terhadap sistem yang baru.
c. Studi Pustaka : Selain melakukan kegiatan di atas penulis juga mengumpulkan data melalui buku, jurnal yang berkaitan dengan judul yang diangkat sebagai referensi.

2.2 Model Pengembangan Jaringan

Model pengembangan jaringan yang digunakan dalam penelitian ini adalah topologi terpusat dengan pendekatan *high availability* pada dua server NAS Synology. Sistem ini dirancang untuk menjamin ketersediaan data secara berkelanjutan melalui mekanisme *failover* otomatis antar server. Selain itu, jaringan dikembangkan dengan penambahan layanan VPN sebagai jalur aman untuk akses data dari luar kantor, serta penerapan autentikasi dua faktor (2FA) menggunakan Google Authenticator untuk meningkatkan keamanan akses pengguna.

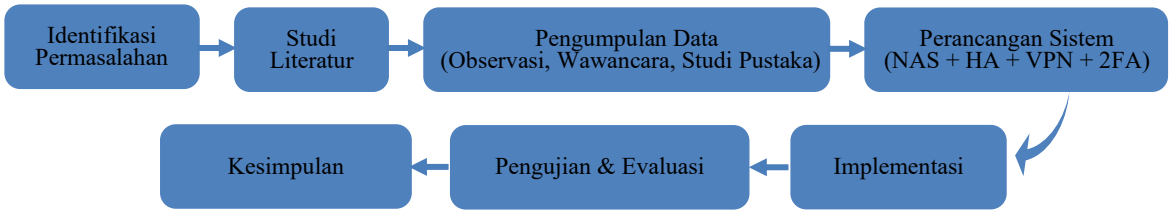
2.3 Ruang Lingkup

Ruang lingkup penelitian ini mencakup proses implementasi NAS Synology dengan fitur *High Availability* untuk meningkatkan ketersediaan data, serta mampu mengurangi waktu *down time* atau bahkan mencegah terjadinya *down time*. Dan juga perancangan sistem akses data yang aman dari luar kantor menggunakan VPN dan 2FA. Penelitian difokuskan pada lingkungan internal PT. Mitra Tera Sinergi, dengan batasan pada sistem penyimpanan dan mekanisme keamanan akses data.

2.4 Tahapan Penelitian

Tahapan penelitian ini disusun secara sistematis agar proses perancangan dan implementasi sistem dapat berjalan terarah. Setiap tahap saling berkesinambungan, dimulai dari identifikasi permasalahan hingga penarikan kesimpulan. Adapun alur tahapan penelitian ditunjukkan pada gambar berikut.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620



Gambar 1. Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

3.1 Hasil Implementasi Sistem

Pada bagian ini penulis memberikan solusi terhadap permasalahan yang dihadapi oleh PT. Mitra Tera Sinergi, khususnya untuk mengatasi keterbatasan pada sistem OwnCloud yang tidak mendukung fitur *high availability*, penulis mengusulkan penambahan dua server baru yang akan digunakan sebagai sistem penyimpanan berbasis NAS Synology. Kedua server ini akan dikonfigurasi dalam sistem *Synology High Availability* (SHA) dengan arsitektur *failover* aktif-pasif, di mana komunikasi *heartbeat* antar server dilakukan melalui koneksi AOC (*Active Optical Cable*) menggunakan port SFP+ agar proses sinkronisasi dan replikasi data tetap cepat dan stabil.

Untuk meningkatkan keamanan, akses ke sistem sistem penyimpanan Synology akan dilindungi menggunakan autentikasi dua faktor (2FA) dengan aplikasi *Google Authenticator* yang harus diunduh dan diaktifkan pada perangkat ponsel masing-masing pengguna. Selain itu, koneksi dari luar kantor hanya akan diizinkan melalui jalur VPN yang diaktifkan pada router distribusi, sehingga setiap koneksi eksternal tetap aman dan terenkripsi sebelum mengakses jaringan internal perusahaan.

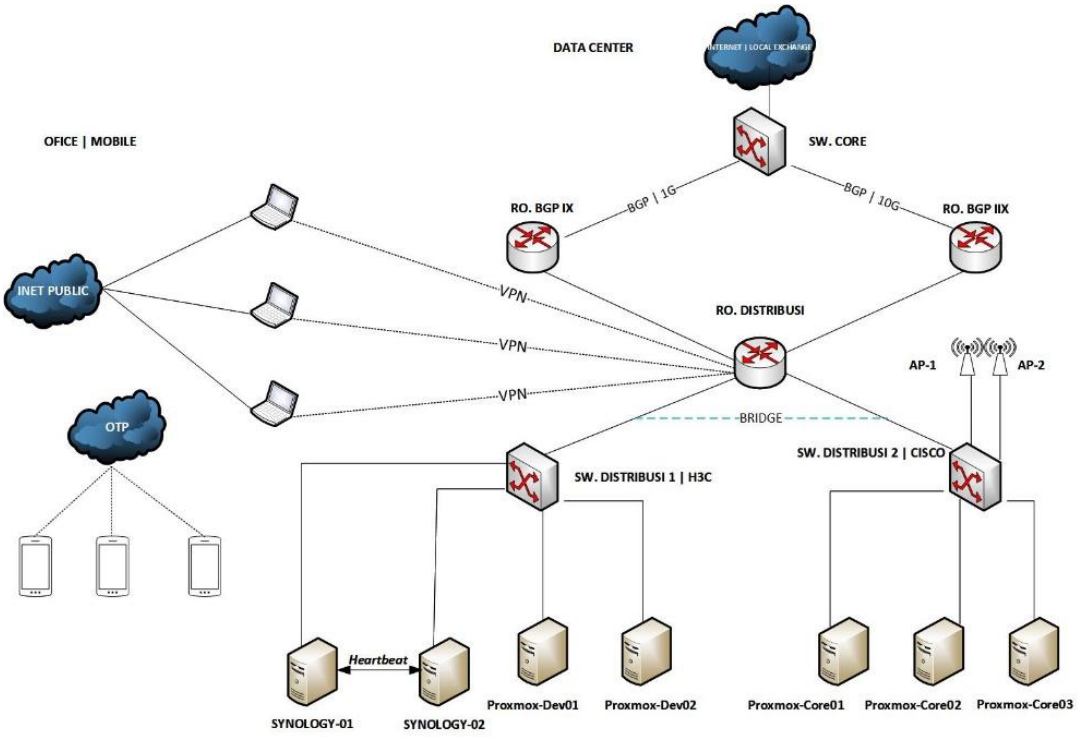
3.2 Topologi Jaringan

Topologi jaringan usulan di PT. Mitra Tera Sinergi mencakup penambahan dua server Synology yang dikonfigurasi dalam mode *High Availability* (HA) dan terhubung ke *Switch Distribusi* 01. Akses dari luar jaringan menggunakan VPN yang diaktifkan pada Router Distribusi, dan dengan penerapan autentikasi dua faktor (2FA) melalui aplikasi *Google Authenticator* yang di install pada ponsel setiap karyawan untuk meningkatkan keamanan.

3.3 Skema Jaringan

Skema jaringan usulan mencakup dua server Synology dalam konfigurasi *High Availability* (HA) sebagai sistem penyimpanan utama, terhubung melalui AOC untuk komunikasi *heartbeat* dan replikasi data. Keduanya terkoneksi ke *Switch Distribusi* 01. Akses pengguna luar atau public dilakukan melalui VPN yang dikonfigurasi pada Router Distribusi dengan Autentikasi Dua Faktor (2FA) menggunakan *Google Authenticator*. Pengguna mengakses layanan sistem penyimpanan melalui *IP Virtual HA*, bukan IP fisik masing-masing server, sehingga layanan tetap berjalan jika salah satu server mengalami gangguan atau bahkan *down*.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620



Gambar 2. Skema Jaringan Usulan PT. Mitra Tera Sinergi

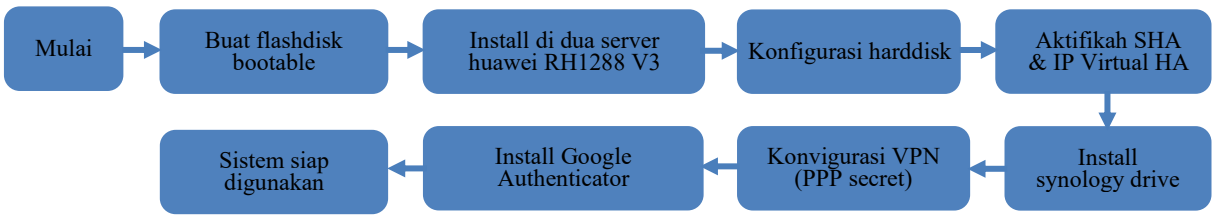
Sistem keamanan jaringan usulan mencakup penerapan VPN di Router Distribusi untuk mengamankan akses dari luar jaringan, sehingga hanya pengguna yang terhubung ke VPN yang dapat masuk ke sistem penyimpanan NAS Synology. Untuk memperkuat perlindungan, diterapkan Autentikasi Dua Faktor (2FA) menggunakan *Google Authenticator* pada setiap akses ke layanan penyimpanan NAS Synology.

3.4 Rancangan Aplikasi

NAS (*Network Attached Storage*) yang digunakan dalam rancangan sistem ini bertujuan untuk membangun solusi sistem penyimpanan internal yang satbil dan tetap berjalan maskipun salah satu server mengalamali gangguan atau *down*, dengan memanfaatkan fitur *Synology High Availability* (SHA). Penulis menggunakan dua unit server Huawei RH1288 V3 untuk implentasi di PT. Mitra Tera Sinergi sebagai perangkat NAS Synology model DS3622xs+ (kode 42218). Sistem operasi *DiskStation Manager* (DSM) versi 7.0.1 diunduh dari situs resmi Synology atau dan diinstal melalui *flashdisk bootable* ke kedua server.

Setelah instalasi selesai, dilakukan konfigurasi harddisk dan *volume storage*. Lalu dilakukan instalasi dan konfigurasi SHA (*Synology High Availability*) untuk menggabungkan kedua server menjadi satu klaster aktif-pasif, yang memungkinkan sinkronisasi data *real-time* dan menyediakan satu *IP Virtual HA* sebagai akses utama layanan penyimpanan. Selanjutnya, aplikasi Synology Drive diinstal sebagai layanan file sharing, dan dilakukan pembuatan akun pengguna di dalam sistem.

Akses dari eksternal difasilitasi melalui VPN yang dikonfigurasi di Router Distribusi menggunakan PPP *Secret*, dengan username dan password disamakan dengan yang ada di Synology. Untuk keamanan tambahan, setiap pengguna diwajibkan menginstal *Google Authenticator* di perangkat seluler masing-masing untuk verifikasi OTP saat login.



Gambar 3. Ilustrasi Rancangan Aplikasi PT. Mitra Tera Sinergi

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620

3.5 Manajemen Jaringan

Manajemen jaringan dalam sistem yang diusulkan bertujuan untuk memastikan ketersediaan layanan penyimpanan file secara aman, terpusat, dan mudah diakses baik dari dalam maupun luar jaringan perusahaan. Sistem NAS Synology yang diimplementasikan dalam mode *High Availability* (HA) memberikan solusi penyimpanan yang selalu aktif dan andal. Adapun strategi manajemen jaringan yang diterapkan adalah sebagai berikut:

a. Akses Jarak Jauh Aman
   Akses dari luar jaringan internal dilakukan melalui koneksi VPN yang dikonfigurasi pada router distribusi, hal ini menjaga keamanan lalu lintas data.
b. Manajemen Terpusat dengan IP Virtual HA
   Melalui fitur *Synology High Availability* (SHA), dua perangkat NAS digabungkan menjadi satu sistem logis dengan satu *IP virtual*. User hanya perlu terhubung ke *IP virtual* untuk mengakses layanan sistem penyimpanan, sehingga layanan tetap tersedia meskipun salah satu perangkat mengalami gangguan atau bahkan *down*.
c. Penyeragaman Akun dan Autentikasi Dua Faktor
   Akun pengguna pada sistem NAS dan akun VPN pada router dibuat dengan nama pengguna dan kata sandi yang sama, untuk memudahkan pengguna dalam mengingat kredensial akses mereka. Selain itu, setiap pengguna diwajibkan mengaktifkan autentikasi dua faktor (2FA) menggunakan aplikasi *Google Authenticator* di perangkat masing-masing untuk menambah lapisan keamanan saat mengakses layanan.

3.6 Hasil Pengujian Sistem

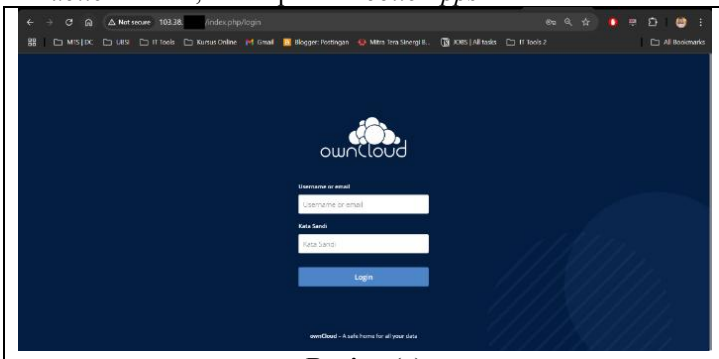
Pengujian jaringan dilakukan untuk mengevaluasi tingkat keamanan, ketersediaan layanan, serta keandalan akses terhadap sistem penyimpanan data perusahaan sebelum dan sesudah implementasi sistem yang diusulkan. Pengujian ini bertujuan untuk membandingkan kondisi sistem lama yang masih menggunakan OwnCloud tanpa sistem *redundansi* dan keamanan berlapis, dengan sistem baru berbasis NAS *Synology High Availability* (SHA), akses VPN, dan autentikasi dua faktor (2FA).

3.7 Pengujian Jaringan Awal (OwnCloud)

Pada tahap ini, dilakukan pengujian terhadap kondisi jaringan sebelum implementasi sistem baru. Sistem penyimpanan file masih menggunakan OwnCloud yang diakses langsung melalui IP publik tanpa perlindungan VPN maupun 2FA. Hasil pengujian menunjukkan beberapa kelemahan sebagai berikut:

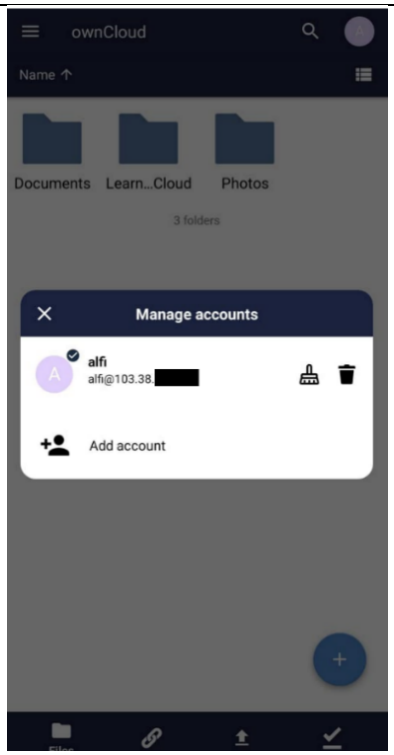
a. Risiko Keamanan Tinggi

Akses OwnCloud secara langsung melalui IP publik tanpa perlindungan VPN memungkinkan potensi serangan dari pihak luar seperti *brute force login*, *scanning port,* hingga *eksploitasi* kerentanan. Tidak adanya sistem keamanan berlapis menyebabkan sistem rentan terhadap ancaman. Berikut merupakan tampilan akses ke Owncloud langsung dengan *IP Public* via web, desktop dan *Mobile Apps*.



Bagian (a)

Bagian (b)



Bagian (c)

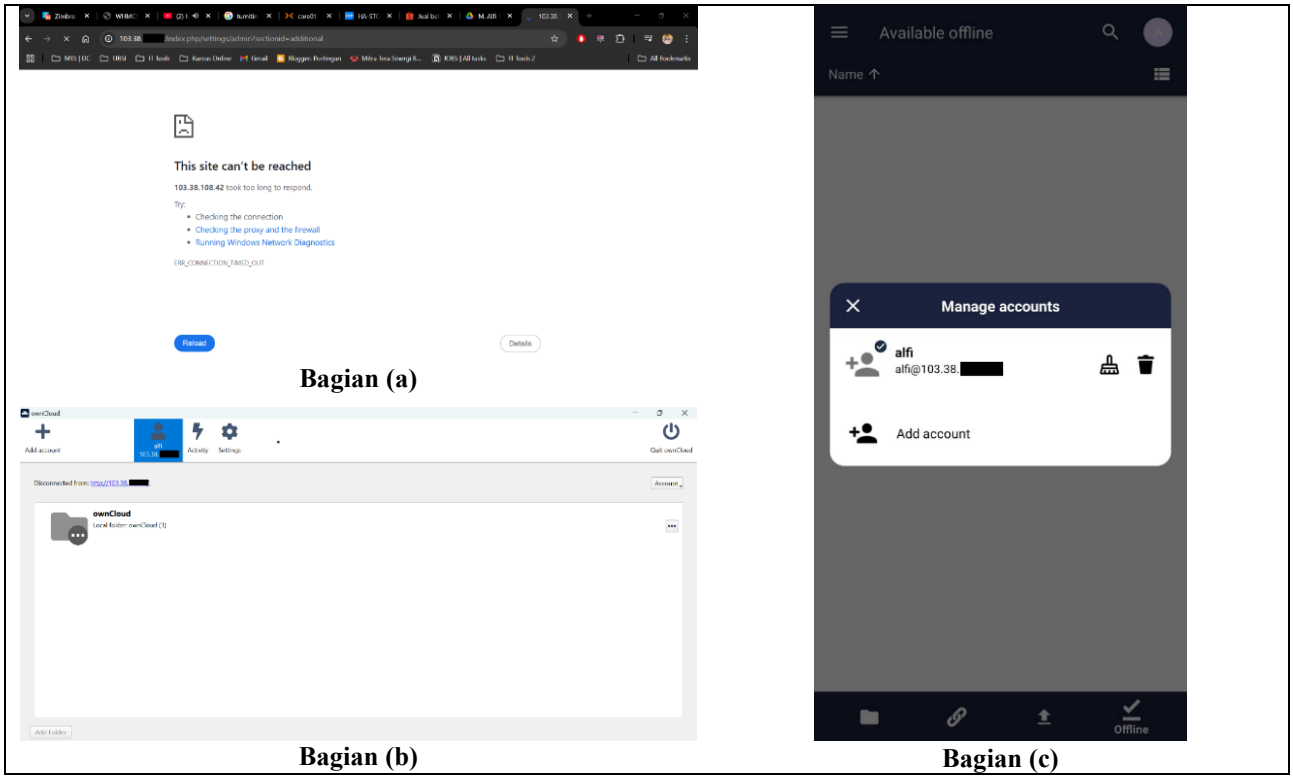
Gambar 4. Akses Publik Web Owncloud (a), Dekstop Owncloud (b), Mobile App Owncloud (c)

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620

Pada gambar 4 bagian a merupakan akses Owncloud dengan *IP public* via web, bagian b akses Owncloud dengan IP public via desktop, sedangkan bagian c merupakan akses Owncloud dengan IP public via mobile apps.

b. Tidak Tersedianya Redundansi Server

Jika server yang menjalankan OwnCloud mengalami gangguan atau down, maka seluruh layanan tidak dapat diakses. Hal ini menyebabkan sistem tidak memiliki toleransi terhadap kesalahan (fault tolerance). Berikut merupakan tampilan akses ke Owncloud langsung dengan IP Public via web, desktop dan Mobile App jika terjadi gangguan atau down di server Owncloud.



Gambar 5. No Akses Publik Web Owncloud (a), Dekstop Owncloud (b), Mobile App Owncloud (c)

Pada gambar 5 bagian a merupakan tampilan tidak bisa akses ke owncloud via web jika server owncloud down. Bagian b tampilan tidak bisa akses ke owncloud via dekstop jika server owncloud down denga nada tampilan disconnected. Pada bagian c tampilan tidak bisa akses ke owncloud via mobile apps jika server owncloud down dengan ada tampilan offline.

c. Ketiadaan Autentikasi Dua Faktor

Sistem login hanya bergantung pada kombinasi username dan password, yang meningkatkan risiko pembobolan akun apabila kredensial diketahui pihak tidak bertanggung jawab.

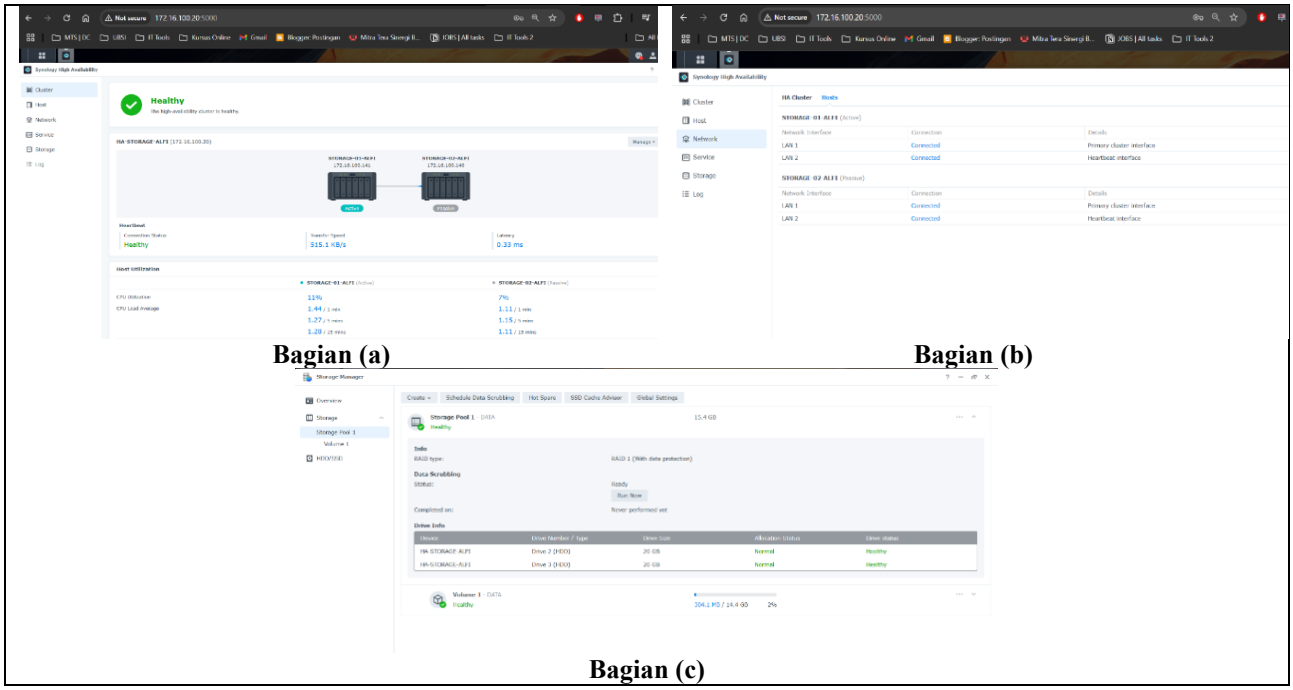
3.8 Pengujian Jaringan Akhir (NAS Synology)

Setelah implementasi sistem baru menggunakan Synology NAS dengan konfigurasi *High Availability* (SHA), sistem VPN di router distribusi, serta autentikasi dua faktor melalui *Google Authenticator*, dilakukan pengujian kembali untuk memastikan peningkatan performa dan keamanan. Hasil pengujian menunjukkan:

a. Redundansi Sistem melalui Implementasi *High Availability*

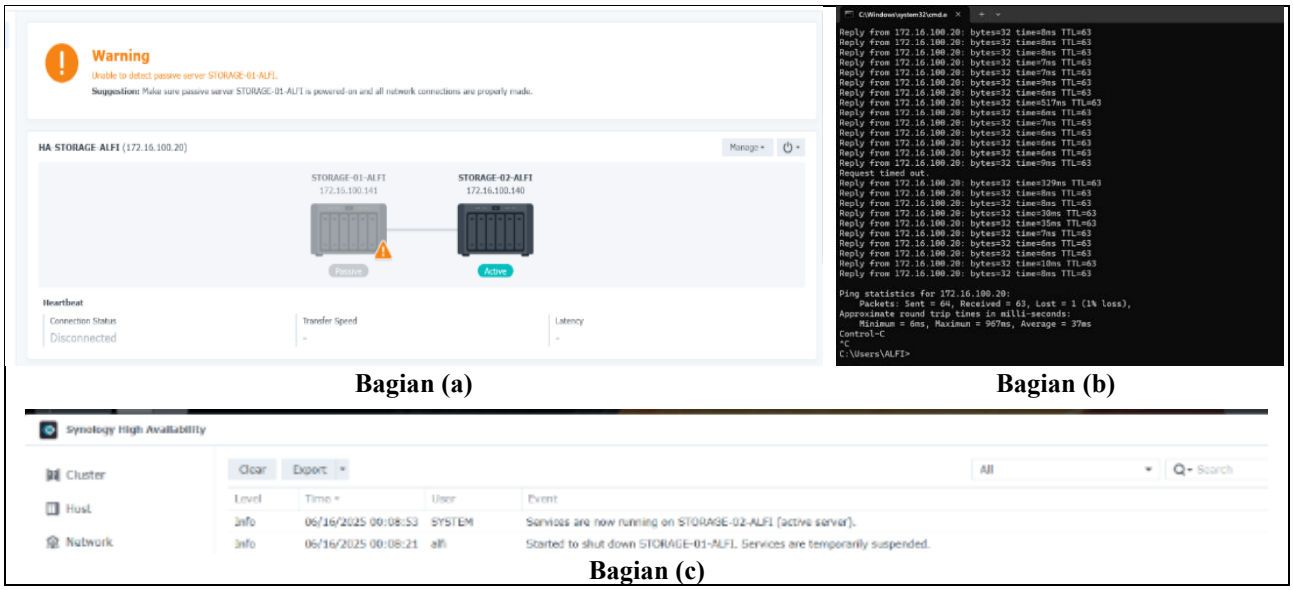
Setelah sistem Synology NAS dikonfigurasi dalam mode *High Availability* (HA), dilakukan pengujian untuk memastikan fitur failover berjalan dengan baik. Dalam konfigurasi ini, server pertama menggunakan *IP address* 172.16.100.141, sedangkan server kedua menggunakan *IP address* 172.16.100.140. Sistem SHA menghasilkan sebuah *IP Virtual High Availability* (IP HA) yang berfungsi sebagai titik akses utama, yaitu 172.16.100.20. IP virtual ini secara otomatis berpindah dari server aktif ke server cadangan saat terjadi gangguan, sehingga pengguna tetap dapat mengakses layanan penyimpanan.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620



Gambar 6. Tampilan utama SHA (a), Tampilan Network – Host SHA (b), Tampilan Storage Manager SHA (c)

Pada Gambar 6 bagian a menunjukkan tampilan SHA dengan status Healthy, menandakan kedua server berjalan normal. Node aktif menggunakan IP 172.16.100.141, node pasif 172.16.100.140, dan IP virtual SHA adalah 172.16.100.20. Pada bagian b terlihat pada LAN 1 di kedua server merupakan koneksi langsung ke switch, dan LAN 2 merupakan interface komunikasi heartbeat antar server. Pada Gambar bagian c terlihat setiap server dilengkapi dua hard disk berkapasitas masing-masing 20 GB (total 40 GB per server). Kedua hard disk tersebut dikonfigurasi dalam mode RAID 1 untuk keamanan data, sehingga kapasitas yang terbaca secara efektif menjadi 14.4 GB. Konfigurasi ini diterapkan pada kedua server, baik server 1 maupun server 2.



Gambar 7. Proses Failover pada sistem SHA (a), Uji Koneksi Ke IP Virtual HA (b), Log Failover (c)

Pada Gambar 7 bagian a menunjukkan proses failover pada sistem Synology High Availability (SHA). Terlihat bahwa server utama (STORAGE-01-ALFI) dengan IP 172.16.100.141 berada dalam kondisi tidak terdeteksi (disconnected), yang mengindikasikan bahwa server tersebut dalam kondisi off atau mengalami gangguan.

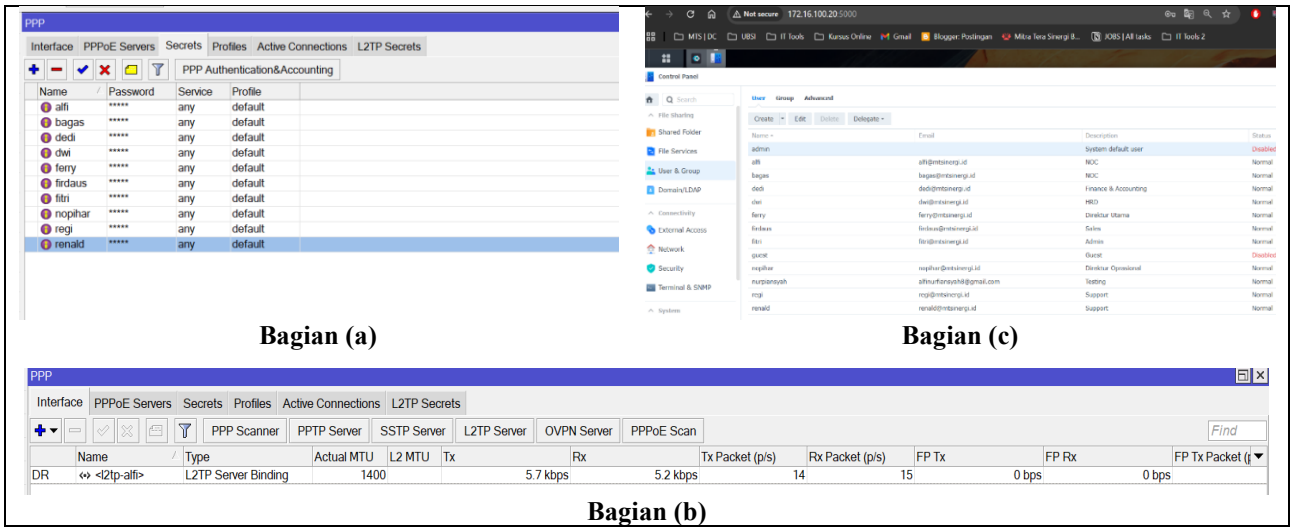
Sebagai respons otomatis, sistem SHA mengalihkan peran aktif ke server cadangan (STORAGE-02-ALFI) dengan IP 172.16.100.140, sehingga layanan tetap berjalan normal melalui IP virtual HA 172.16.100.20. Proses ini membuktikan bahwa mekanisme failover berjalan dengan baik untuk menjaga ketersediaan layanan secara terus-menerus.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620

Gambar 7 bagian b menunjukkan bahwa proses failover antar server umumnya dapat menghasilkan 1 hingga 5 kali Request Time Out (RTO), namun pada simulasi ini hanya terjadi 1 kali RTO. Hal ini menandakan bahwa perpindahan layanan berlangsung sangat cepat dan sistem dapat kembali stabil dalam waktu singkat. Pada gambar 7 bagian c merupakan tampilan log failover dari sebelum nya server STORAGE-01-ALFI active pindah ke server STORAGE-02-ALFI.

b. Akses Aman melalui VPN

Akses dari luar jaringan hanya dapat dilakukan melalui koneksi VPN yang telah dikonfigurasi di Router Distribusi dengan metode autentikasi menggunakan username dan password yang disamakan dengan akun NAS. Hal ini memastikan bahwa hanya pengguna yang sah dan terverifikasi yang dapat mengakses layanan dari luar jaringan internal.



Gambar 8. Konfigurasi VPN pada Router Distribusi (a), User aktif VPN di Router Distribusi (b), Konfigurasi User pada NAS Synology (c)

Pada Gambar 8 bagian a merupakan konfigurasi VPN yang di buat pada PPP Secrets Router Distribusi. Konfigurasi ini memuat user dan password karyawan untuk mengakses VPN. Pada Gambar 8 bagian b merupakan interface VPN yang aktif, yang sudah terhubung dari end device user ke arah Router Distribusi Pada gambar 8 bagian c merupakan konfigurasi sistem, username dan password yang digunakan untuk login ke NAS Synology diselaraskan dengan kredensial yang digunakan pada koneksi VPN. Pendekatan ini diterapkan untuk menyederhanakan proses autentikasi bagi karyawan, sekaligus memastikan konsistensi dan kemudahan dalam manajemen akses dengan hanya satu set akun per pengguna.

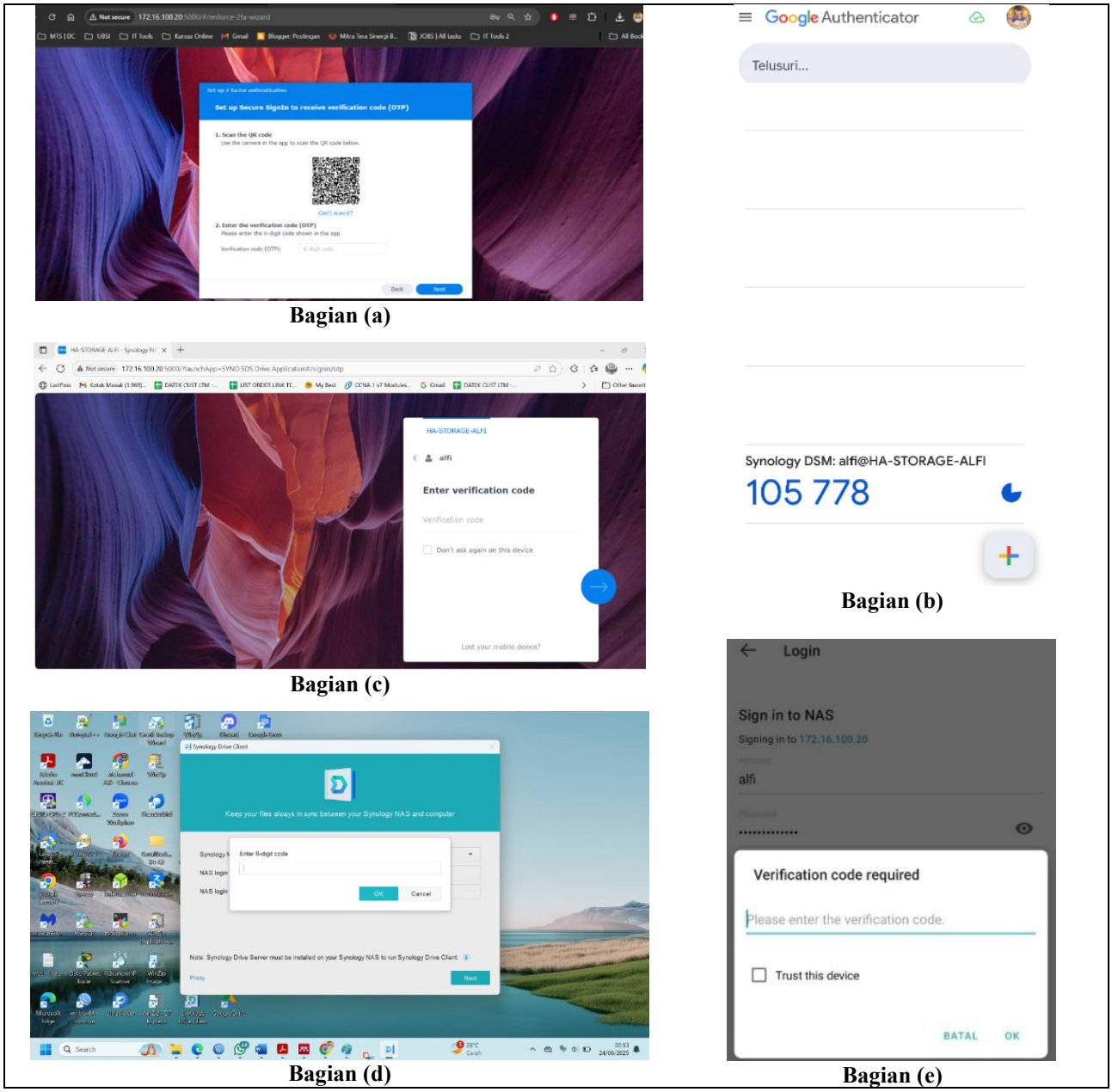
c. Autentikasi Dua Faktor untuk Keamanan Lebih

Untuk meningkatkan keamanan akses, setiap pengguna diwajibkan mengaktifkan autentikasi dua faktor (2FA) dengan aplikasi *Google Authenticator*. Proses login ke akun Synology tidak hanya membutuhkan *username* dan *password*, tetapi juga kode OTP yang bersifat dinamis dan berubah setiap 30 detik. Tahapan penerapan 2FA adalah sebagai berikut:

1. Menghubungkan akun NAS Synology dengan Google Authenticator, dilakukan dengan memindai barcode yang disediakan oleh sistem.
2. Google Authenticator menghasilkan kode OTP yang secara otomatis berubah setiap 30 detik.
3. Setiap kali login ke Synology Drive Client, baik melalui web, desktop, maupun mobile, pengguna harus memasukkan kode OTP tersebut setelah memasukkan *username* dan *password*.

Dengan mekanisme ini, keamanan akses meningkat karena meskipun *username* dan *password* diketahui pihak lain, akun tetap tidak dapat diakses tanpa kode OTP yang hanya tersedia di perangkat pengguna.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620



Gambar 9. Setup Kode OTP pada login NAS Synology (a), Gambar 20 Kode OTP pada Google Authenticator (b), Verfikasi kode OTP Synology Drive Client Web (c), Verfikasi kode OTP Synology Drive Client Dekstop (d), Verfikasi kode OTP Synology Drive Client Mobile App (e)

Pada Gambar 9 bagian a merupakan setup awal untuk mengkoneksikan antara account user NAS Synology dengan Google Authenticator. Yang mana dari Google Authenticator ini akan menscan barcode yang diberikan oleh NAS Synology. Gambar 9 bagian b merupakan kode OTP dari Google Authenticator yang sudah terhubung dengan NAS Synology. Pada Gambar 9 bagian c, d dan e merupakan tampilan Two-Factor Authentication (2FA), dimana user harus menginput kode OTP yang ada di Google Authenticator. Yang sebelum nya user sudah memasukan username dan password.

d. Penggunaan dan Pemantauan *Client Synology Drive*

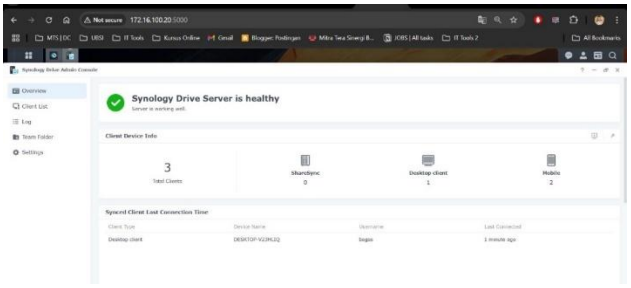
Synology Drive digunakan sebagai platform untuk berbagi dan menyinkronkan data antara server pusat dan perangkat klien di lingkungan perusahaan. Aplikasi ini diinstal pada perangkat masing-masing pengguna. Pengguna dapat mengakses dan mengelola file secara langsung dari perangkat masing-masing melalui koneksi aman VPN.

Melalui fitur *Synology Drive Admin Console*, administrator dapat memantau seluruh aktivitas klien secara terpusat. Informasi yang dapat dilihat meliputi:

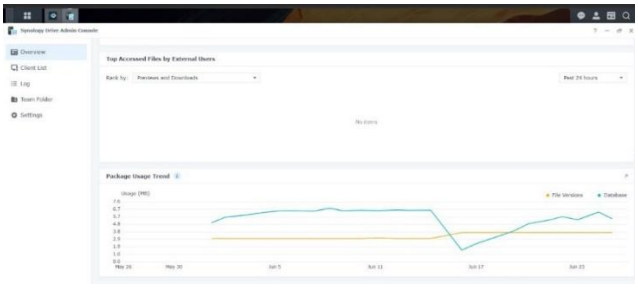
1. Jumlah Total Klien yang Terhubung
   Menampilkan jumlah keseluruhan perangkat klien yang telah terdaftar dan pernah terhubung ke layanan *Synology Drive*.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620

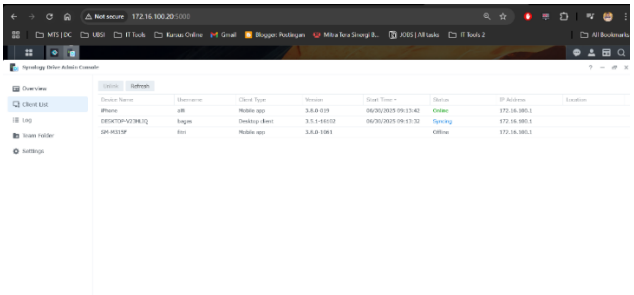
2. Status Koneksi Klien (Aktif/*Offline*)
   Menunjukkan apakah klien sedang aktif (*online*) atau tidak terhubung (*offline*) secara *real-time*.
3. Tipe Perangkat Klien
   Mengidentifikasi jenis perangkat yang digunakan oleh klien, seperti Dekstop Client atau Mobile App.
4. Nama Perangkat (Device Name)
   Menampilkan nama masing-masing perangkat yang digunakan untuk mengakses dan sinkronisasi data dengan Synology Drive.
5. Tampilan Synology Drive di Sisi Klien
   Synology Drive tersedia dalam bentuk aplikasi desktop untuk Windows/macOS serta aplikasi mobile untuk Android/iOS. Di sisi klien desktop, aplikasi ini menampilkan status sinkronisasi file secara langsung di *file explorer* dan mendukung pengaturan folder sinkronisasi khusus. Di sisi mobile, aplikasi Synology Drive memungkinkan pengguna untuk mengakses, mengunggah, dan menyinkronkan file secara langsung dari ponsel, lengkap dengan fitur pratinjau dan manajemen folder.



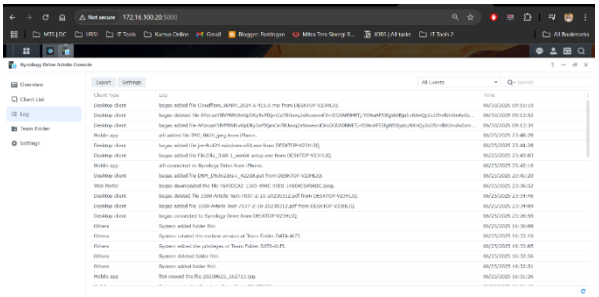
Gambar 10. Tampilam Overview 1 *Synology Drive Admin Console*



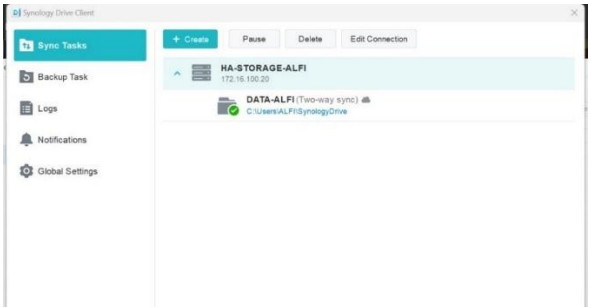
Gambar 11. Tampilam *Overview* 2 *Synology Drive Admin Console*



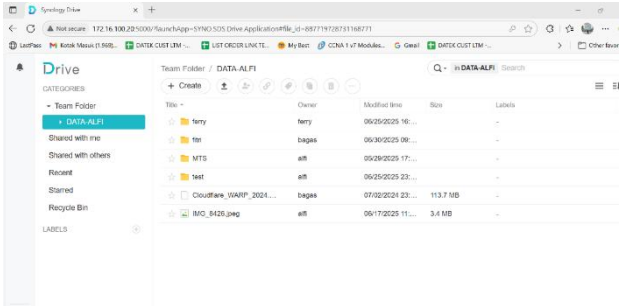
Gambar 12. Tampilam *Client List Synology Drive Admin Console*



Gambar 13. Tampilam Log *Synology Drive Admin Console*

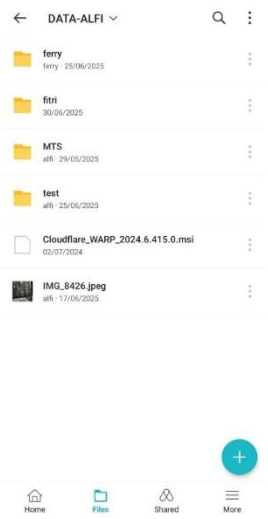


Gambar 14. Tampilam *Dashboard Synology Drive Client Desktop*



Gambar 15. Tampilam Dashboard *Synology Drive Client Web*

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620



Gambar 16. Tampilam Dashboard Synology Drive Client Mobile Apps

Pada Gambar 10 ditampilkan Synology Drive Admin Console pada menu *overview* yang menunjukkan total klien, meliputi *sharesync*, *desktop client*, dan *mobile*. Selanjutnya, Gambar 11 memperlihatkan menu *overview* yang menampilkan penggunaan *bandwidth*. Gambar 12 menunjukkan menu *client list* yang memuat informasi mengenai status pengguna, baik yang aktif, *offline*, maupun yang sedang melakukan sinkronisasi data dari perangkat ke server NAS Synology. Adapun Gambar 13 menampilkan menu *log* yang berisi riwayat aktivitas pengguna. Pada Gambar 14 ditunjukkan Synology Drive Client versi *desktop* yang menampilkan status koneksi ke server NAS Synology, *backup task*, *logs*, notifikasi, serta pengaturan umum (*global setting*). Sementara itu, Gambar 15 memperlihatkan tampilan Synology Drive Client versi *web* yang mencakup *team folder*, *shared with me*, *share with others*, *recent*, *starred*, dan *recycle bin*. Terakhir, Gambar 16 menyajikan tampilan Synology Drive Client versi *mobile* yang menampilkan daftar folder dan file dalam direktori *DATA-ALFI* beserta nama pengguna serta tanggal modifikasi terakhir.

4. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi sistem yang dilakukan di PT. Mitra Tera Sinergi, dapat disimpulkan bahwa penerapan sistem penyimpanan data berbasis NAS Synology dengan fitur Synology High Availability (SHA) berhasil menyediakan layanan dengan ketersediaan tinggi sehingga mampu meminimalisir risiko *down time* dan memastikan operasional tetap berjalan meskipun terjadi kegagalan pada salah satu server. Keamanan akses data juga meningkat melalui konfigurasi Virtual Private Network (VPN) pada router distribusi, yang memungkinkan pengguna mengakses data dari luar jaringan kantor secara lebih aman. Selain itu, risiko kehilangan data dapat diminimalisir melalui penerapan sistem redundansi dengan dua server yang saling mencadangkan, sehingga mendukung ketahanan data serta keberlangsungan layanan perusahaan. Upaya penguatan keamanan semakin ditingkatkan melalui penerapan autentikasi dua langkah (2FA) menggunakan aplikasi Google Authenticator, yang menambah lapisan perlindungan terhadap akses tidak sah pada sistem penyimpanan.

REFERENCES

[1] S. Dewi, "Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis," *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.

[2] L. Qadriah, S. Achmady, and Husaini, "Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentation (2FA)," *J. Sains dan Inform.*, vol. 9, no. November 2022, pp. 29–35, 2023, doi: 10.34128/jsi.v9i1.519.

[3] moeh, "Moehamad Ibnu Triwahyudi," vol. 11, pp. 55–64, 2022.

[4] W. Buana, A. Hariyandi, and F. Rezi, "Pengembangan Jaringan Local Area Network (Lan) Dan Wide Area Network (Wan) Pada Smkn 4 Padang Dengan Metode Research Dan Development," *JOISIE J. Inf. Syst. Informatics Eng.*, vol. 7, no. 1, pp. 120–134, 2023.

[5] P. P. Desmira, "ANALISIS OPTIMALISASI KINERJA JARINGAN MAN PADA LAYANAN INTERNET BERBASIS MIKROTIK DI PT. BINA TECHNINDO SOLUTION," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 8, no. 1, pp. 8–17, 2021, doi: 10.30656/prosisko.v8i1.2936.

[6] G. Syahputra, U. Erdiansyah, and H. T. Hidayat, "RANCANG BANGUN NAS SERVER DI LINGKUNGAN JURUSAN TIK PNL DALAM UPAYA MENGURANGI KETERGANTUNGAN TERHADAP JARINGAN

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 2 September 2025
Hal: 1242-1253
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i2.620

INTERNET," vol. 7, no. 1, pp. 49–52, 2024.
[7] D. Andana Haris Andana, Hansen Salim, and Joseph Kristianto, "Rancang Bangun NAS dengan SBC Raspberry Pi Sebagai Alternatif Penyimpanan Cloud Dengan Koneksi Internet," *Ranah Res. J. Multidiscip. Res. Dev.*, vol. 6, no. 5, pp. 1515–1528, 2024, doi: 10.38035/rrj.v6i5.954.
[8] S. Raharjo and F. Ekawati, "Optimasi Perlindungan Data Dari Serangan Siber Dengan Synology Untuk Kelangsungan Bisnis Perusahaan," *J. Ilmu Komput. JIK*, vol. 5, no. 1, pp. 39–45, 2022.
[9] I. M. Lina and G. R. Fernandes, "Natural : Jurnal Pelaksanaan Pengabdian Bergerak bersama Masyarakat Pengenalan NAS (Network Attached Storage) untuk Penyimpanan Data Terpusat pada Paguyuban Kebon Manggis Introduction to NAS (Network Attached Storage) for Centralized Data Storage at P," no. 1, 2025.
[10] I. Rusilpan, "78 Jurnal Teknik Informatika dan Sistem Informasi Implementasi Manajemen Backup Data Berbasis Strategi Backup Rule 3-2-1 Menggunakan NAS Synology Dan Autentikasi LDAP," vol. 10, no. 1, pp. 78–90, 2023.
[11] Hartati, Shinta Septiantina, Amelia Luthfi Kamil, and Farkhatus Solikhah, "Teknik Failover Clustering Sebagai Solusi High Availability," *Tematik*, vol. 8, no. 1, pp. 104–109, 2021, doi: 10.38204/tematik.v8i1.579.
[12] D. Darmadi and R. Susandi, "Pengujian Efektifitas Sistem Cluster Dengan Penerapan Hugh Availability Pada Server Virtual," *J. Anal. Res.*, vol. 1, no. 1, pp. 36–50, 2022.
[13] M. K. Wijaya, Z. Sari, and M. Faiqurahman, "Implementasi High Availability Cloud Storage Dengan Metode Replikasi dan Failover Pada Laboratorium Teknik Informatika," *J. Repos.*, vol. 2, no. 2, pp. 165–176, 2020, doi: 10.22219/repositor.v2i2.245.
[14] H. P. Fitrian *et al.*, "ANALISIS PENERAPAN TEKNOLOGI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI KEAMANAN DATA DI JARINGAN PUBLIK," vol. 9, no. 1, pp. 1559–1563, 2025.
[15] P. Harry, Amanda, Idan, Nabila, "ANALISIS MANAJEMEN TRAFIK JARINGAN PADA VIRTUAL PRIVATE NETWORK," vol. 9, no. 2, pp. 2310–2314, 2025.
[16] A. T. Atmoko, A. Surya Budiman, and N. Nuraeni, "Perancangan Dan Pengembangan Virtual Private Network (VPN) Menggunakan PPTP Pada PT Indobinatu Mitra Sejati Design and Development of Virtual Private Network (VPN) Using PPTP in PT Indobinatu Mitra Sejati," *Jtsi*, vol. 5, no. 1, pp. 160–170, 2024.
[17] H. Haeruddin and K. Kelvin, "Analisa Penggunaan VPN L2TP dan SSTP di Masa Pandemi Covid-19," *J. Ilmu Komput. dan Bisnis*, vol. 13, no. 1, pp. 105–114, 2022, doi: 10.47927/jikb.v13i1.279.
[18] I. K. Rahman and L. N. Harnaningrum, "Analisa Quality of Service (QoS) Pada Jaringan L2TP IPSec Dan Wireguard VPN untuk mengamankan VoIP," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 7, no. 1, pp. 10–20, 2024, doi: 10.31598/jurnalresistor.v7i1.1553.
[19] Aren Brayen Sangi, Ferdinan I. Sangkop, and Olivia Kembuan, "Perancangan Dan Implementasi Jaringan Internet Berbasis Mikrotik," *J. Penelit. Rumpun Ilmu Tek.*, vol. 2, no. 2, pp. 170–186, 2023, doi: 10.55606/juprit.v2i2.1938.
[20] R. Fauzi *et al.*, "Instalasi Mikrotik Pada Virtualbox Dan Pengkoneksian Antara Mikrotikdi Virtualbox Dengan Winbox Di Smk S Teruna Padang Sidempuan," *J. ADAM J. Pengabdi. Masy.*, vol. 2, no. 1, pp. 106–118, 2023, doi: 10.37081/adam.v2i1.1381.
[21] F. S. M. Angga Eko Bayu Arieska, "Pemanfaatan One-Time Password dan Algoritma Advanced Encryption Standard dalam Sistem Login Internet Kampus," *G-Tech J. Teknol. Terap.*, vol. 8, no. 1, pp. 186–195, 2024.
[22] M. A. Taqwim, A. Kusyanti, and R. A. Siregar, "Implementasi Algoritme Speck Untuk Enkripsi One-Time Password Pada Two-Factor Authentication," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 7, pp. 3103–3111, 2021.
[23] Yusuf Heriyanto, Anas Azhimi Qalban, and Iif Alfiatul Mukaromah, "Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik," *J. Innov. Inf. Technol. Appl.*, vol. 4, no. 2, pp. 142–150, 2022, doi: 10.35970/jinita.v4i2.1637.
[24] T. Aprilia *et al.*, "Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial," *Pengaruh Keamanan Two Factor*, vol. 2, no. 5, pp. 449–458, 2024.
[25] H. D. Lie and M. M. Engel, "Library Self Service System Using Nfc and 2Fa Google Authenticator," *J. Tek. Inform.*, vol. 3, no. 3, pp. 753–761, 2022.
[26] M. Anwar Fauzi, A. Id Hadiana, and F. Rakhmat Umbara, "Penambahan Fitur Multi-Factor Authentication Dalam Studi Kasus Sistem Informasi Rekam Medis Rumah Sakit," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 4, pp. 2938–2944, 2024, doi: 10.36040/jati.v7i4.7305.
[27] R. Y. A. Muhammad Rizqy Ath-Thaariq, Erna Kumalasari Nurnawati, "Perancangan Otentikasi One Time Password menggunakan Kode Unik via Email," *J. Din. Inform.*, vol. 12, no. 1, pp. 70–78, 2023.
[28] L. G. R. Semesta and S. Amini, "Implementasi One Time Password Dengan Algoritma Secure Hash Algorithm 512 (SHA-512)," *Skanika*, vol. 1, no. 3, pp. 1206–1211, 2018.
[29] D. Zaldiyanto, Subektiningsih, and I. R. Wulandari, "IMPLEMENTASI VPN MENGGUNAKAN PROTOKOL L2TP UNTUK," vol. 5, no. 4, pp. 387–395, 2024, doi: 10.47065/bit.v5i2.1770.
[30] J. Olbinson and Jonifan, "an Implementation of Two-Factor Authentication Technology Using Time-Based One Time Password (Totp) Method on Private Cloud Storage Website for Guidance and Counseling Teacher," *J. Inf. Technol. Its Util.*, vol. 5, no. 1, pp. 25–30, 2022, doi: 10.56873/jitu.5.1.3854.