Jurnal Komunikasi Sains dan Teknologi
Vol. 3, No. 2, Desember 2024, pp. 319~327
ISSN: 2964 - 5077, DOI: 10.61098/jkst.v3i2.193

Implementasi dan Perancangan Sistem Kontrol Akses Terminal Access Controller Pada Perangkat Jaringan Switch

Javier Aditama[1], Sarwo[1](✉)
[1] BINUS Online Learning, Universitas Bina Nusantara, Jakarta, Indonesia
Javier.Aditama@binus.ac.id, sarwo@binus.ac.id

Informasi Artikel

Sejarah Artikel:

Disubmit 12 November 2024
Direvisi 17 November 2024
Diterima 05 Desember 2024

Kata Kunci:

Network Security,
Terminal Access Controller Access-Control System,
Autentikasi,
Otorisasi,
Akuntansi

ABSTRAK

Dalam jaringan yang besar dan kompleks, penerapan layanan AAA terpusat menjadi semakin penting. Layanan ini tidak hanya meningkatkan keamanan tetapi juga menyederhanakan pengelolaan akses pengguna dan memastikan bahwa kebijakan keamanan dapat diterapkan secara konsisten di seluruh jaringan.. Organisasi yang mengadopsi layanan AAA terpusat dapat lebih mudah mengelola akses pengguna, mengidentifikasi dan menanggapi ancaman keamanan, dan memastikan bahwa kebijakan dan prosedur keamanan diterapkan secara konsisten di seluruh infrastruktur jaringan mereka. Penelitian ini berfokus pada penerapan Terminal Access Controller Access-Control System (TACACS) sebagai layanan terpusat untuk Autentikasi, Otorisasi, dan Akuntansi (AAA) pada perangkat jaringan switch di PT XYZ.. Hasil penelitian menunjukkan bahwa penerapan TACACS di PT XYZ berhasil meningkatkan keamanan akses, memastikan pencatatan yang komprehensif, dan memberikan kontrol yang lebih baik atas aktivitas pengguna di jaringan. Sebagai kesimpulan, TACACS merupakan solusi yang efektif dalam memperkuat keamanan dan manajemen akses di perangkat jaringan yang terhubung di PT XYZ.

Corresponding Author:

Sarwo
BINUS Online Learning, Universitas Bina Nusantara, Jakarta, Indonesia
Email: sarwo@binus.ac.id

1. Pendahuluan

Di era digital ini, keamanan jaringan dan manajemen akses menjadi hal yang krusial bagi PT.XYZ untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi. Metode autentikasi yang kuat dan otorisasi berbasis peran memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sumber daya tertentu. Segmentasi jaringan membatasi dampak pelanggaran keamanan dengan mengisolasi berbagai bagian jaringan, sementara kontrol akses terpusat menyederhanakan manajemen akses pengguna. Aktivitas jaringan dicatat dan diaudit secara rutin untuk mendeteksi anomali, dan program kesadaran dan pelatihan keamanan siber dilakukan untuk meningkatkan kesadaran pengguna. Di era digital yang semakin maju, keamanan jaringan dan manajemen akses telah menjadi prioritas utama bagi organisasi dan perusahaan.

Manajemen akses dan keamanan jaringan sangat penting untuk melindungi data pribadi dari serangan siber dan memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem. Langkah-langkah keamanan yang tepat dapat membantu organisasi menghindari masalah seperti pencurian data, gangguan operasional, dan kerugian finansial. Manajemen akses juga membantu mematuhi hukum, mengurangi biaya pemulihan setelah serangan, dan menjaga nama baik perusahaan. Pada dasarnya, manajemen akses dan keamanan jaringan sangat penting untuk melindungi aset digital dan memastikan kelangsungan bisnis. Layanan Autentikasi, Otorisasi, dan Akuntansi (AAA) memainkan peran penting dalam memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sumber daya jaringan dan melacak aktivitas mereka untuk tujuan audit dan kepatuhan. AAA tidak hanya mengidentifikasi pengguna yang sah tetapi juga mengontrol apa yang dapat mereka lakukan setelah masuk ke jaringan dan mencatat semua aktivitas mereka

untuk analisis lebih lanjut. Implementasi AAA terpusat, seperti yang disediakan oleh protokol TACACS (Terminal Access Controller Access-Control System), memungkinkan organisasi untuk mengelola keamanan jaringan secara lebih efisien dan konsisten.

TACACS (Terminal Access Controller Access-Control System) adalah protokol jaringan yang menyediakan layanan Autentikasi, Otorisasi, dan Akuntansi (AAA) terpusat bagi pengguna yang mengakses jaringan. Protokol ini sangat penting untuk mengelola akses pengguna dan keamanan jaringan, terutama di lingkungan perusahaan atau dengan penyedia layanan internet yang memerlukan kontrol akses yang ketat.[1] TACACS, terutama versi yang lebih baru seperti TACACS+, menyediakan enkripsi penuh untuk semua komunikasi antara klien dan server, memastikan bahwa data sensitif seperti kata sandi tidak dikirimkan dalam teks biasa. Dengan model klien-server, TACACS memungkinkan perangkat jaringan seperti router dan switch untuk mengirim permintaan autentikasi, otorisasi, dan akuntansi ke server pusat yang mengelola proses ini. Penggunaan enkripsi dan komunikasi yang aman mengurangi risiko intersepsi data oleh pihak yang tidak berwenang. Switch adalah perangkat jaringan yang menghubungkan perangkat dalam jaringan area lokal (LAN) dan mengelola komunikasi data secara efisien. Beroperasi pada lapisan data-link (Lapisan 2) model OSI, switch mengarahkan lalu lintas data berdasarkan alamat MAC perangkat. Fungsinya termasuk meneruskan bingkai data, mempelajari dan menyimpan alamat MAC, memfilter bingkai untuk mengirimkannya ke port yang benar, dan melakukan segmentasi jaringan untuk meningkatkan efisiensi dan mengurangi tabrakan data.[2]

Dalam jaringan yang besar dan kompleks, penggunaan layanan AAA terpusat menjadi semakin penting. Hal ini tidak hanya meningkatkan keamanan tetapi juga menyederhanakan manajemen akses pengguna dan memastikan bahwa kebijakan keamanan dapat diterapkan secara konsisten di seluruh jaringan. Dengan meningkatnya ancaman serangan keamanan siber, layanan AAA terpusat seperti yang disediakan oleh TACACS telah menjadi komponen penting dalam strategi keamanan jaringan modern. Organisasi yang mengadopsi layanan AAA terpusat dapat lebih mudah mengelola akses pengguna, mengidentifikasi dan menanggapi ancaman keamanan, dan memastikan bahwa kebijakan dan prosedur keamanan ditegakkan secara konsisten di seluruh infrastruktur jaringan mereka. Dengan menerapkan langkah-langkah keamanan tingkat lanjut dan manajemen akses, PT.XYZ berkomitmen untuk melindungi data dan infrastruktur jaringannya dari berbagai ancaman. Sistem yang kuat dan prosedur yang ketat membantu memastikan bahwa semua pengguna jaringan dapat bekerja dan belajar di lingkungan yang aman dan terlindungi. Melalui upaya ini, PT.XYZ tidak hanya menjaga keamanan informasi tetapi juga mendukung misi pendidikan dan penelitiannya dengan menyediakan akses yang andal dan aman. TACACS (Terminal Access Controller Access-Control System) adalah protokol jaringan yang menyediakan layanan Autentikasi, Otorisasi, dan Akuntansi (AAA) terpusat bagi pengguna yang mengakses jaringan. Protokol ini sangat penting untuk mengelola akses pengguna dan keamanan jaringan, terutama di lingkungan perusahaan atau penyedia layanan internet yang memerlukan kontrol akses yang ketat.

Penelitian diawali dengan telaah pustaka untuk memperoleh pemahaman mendasar tentang Switch, TACACS, dan praktik terbaik dalam penerapan TACACS pada perangkat jaringan. Tahap ini sangat penting untuk membangun kerangka teoritis dan memandu aspek praktis penelitian. Pendekatan studi kasus kemudian diterapkan dalam lingkungan produksi Universitas Telkom. Metode pengumpulan data meliputi observasi langsung, wawancara dengan personel TI, dan analisis dokumentasi yang relevan. Pendekatan ini memastikan bahwa penelitian didasarkan pada aplikasi dan tantangan di dunia nyata. Langkah selanjutnya melibatkan penerapan TACACS sebagai layanan Autentikasi, Otorisasi, dan Akuntansi pada perangkat jaringan Switch. Proses ini meliputi pemasangan dan konfigurasi TACACS, serta integrasinya dengan infrastruktur yang ada, untuk memastikan operasi yang lancar dalam lingkungan jaringan. Bersamaan dengan TACACS, Google Authenticator diimplementasikan sebagai solusi Kode Akses untuk masuk ke perangkat jaringan Switch. Proses ini meliputi pemasangan Google Authenticator, konfigurasinya untuk penggunaan jaringan, dan integrasinya dengan infrastruktur saat ini untuk meningkatkan langkah-langkah keamanan. PuTTY diimplementasikan sebagai perangkat lunak untuk mengakses perangkat jaringan Switch dari jarak jauh. Langkah ini penting untuk memungkinkan manajemen jaringan jarak jauh yang aman dan efisien. PuTTY adalah perangkat lunak emulator terminal populer yang sering digunakan untuk koneksi jaringan yang aman seperti SSH (Secure Shell), Telnet, rLogin, dan sesi serial. PuTTY dikembangkan sebagai perangkat lunak sumber terbuka dan tersedia secara gratis, mendukung berbagai sistem operasi, termasuk Windows, Unix, dan Linux. Sebagai emulator terminal, PuTTY menyediakan lingkungan terminal yang memungkinkan pengguna berinteraksi dengan sistem operasi lain.[3].

Efektivitas dan efisiensi penggunaan TACACS dalam mengamankan perangkat jaringan Switch dievaluasi. Evaluasi difokuskan pada kecepatan pemantauan, responsivitas terhadap perubahan, dan penggunaan sumber daya, yang memberikan wawasan tentang kinerja sistem. Terakhir, data yang dikumpulkan selama fase implementasi dan evaluasi dianalisis. Analisis ini bertujuan untuk mengidentifikasi keberhasilan

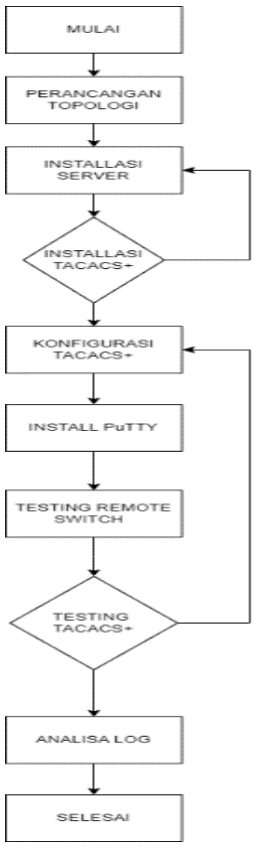
dan tantangan yang dihadapi, serta untuk mengembangkan rekomendasi untuk perbaikan di masa mendatang dalam implementasi TACACS dan langkah-langkah keamanan terkait. Bagian metodologi penelitian menguraikan prosedur pengujian untuk metode yang disebutkan sebelumnya. Pengujian fungsionalitas dilakukan pada TACACS dalam perangkat jaringan Switch, pengujian konektivitas antara server TACACS dan Switch, pengujian pengumpulan data antara TACACS dan User Login, dan pengujian pemantauan sistem pada Dasbor TACACS. Pengujian ini penting untuk memvalidasi efektivitas solusi yang diimplementasikan.

2. Method

2.1. Design Penelitian

Dalam penelitian ini, metode yang digunakan untuk desain dan pengembangan adalah metode waterfall. Model ini sering dianggap sebagai salah satu pendekatan tradisional dalam pengembangan sistem dan perangkat lunak. Metode waterfall dicirikan oleh proses yang berurutan, di mana setiap tahap pengembangan diselesaikan satu demi satu, dari tahap awal hingga tahap akhir. Setiap fase dalam model waterfall harus diselesaikan sepenuhnya sebelum beralih ke fase berikutnya, memastikan bahwa semua aspek dari setiap fase terpenuhi sebelum melanjutkan.

2.2. Research Process



Gambar 1. Research Process

Berikut penjelasan lebih rinci dari setiap langkah dalam diagram alur untuk menginstal dan mengonfigurasi server menggunakan TACACS+:

1. Start: Langkah awal ini menandai dimulainya seluruh proses instalasi dan konfigurasi. Pada tahap ini, semua persiapan awal dilakukan, termasuk memastikan bahwa semua perangkat keras dan perangkat lunak yang diperlukan tersedia dan siap digunakan.
2. Topology Design: Pada langkah ini, perencanaan terperinci mengenai struktur jaringan yang akan digunakan dilakukan. Ini termasuk memetakan perangkat seperti router, switch, server, dan klien.
3. Server Installation: Setelah menyelesaikan desain topologi, langkah selanjutnya adalah memasang server yang akan mengelola autentikasi dan akses jaringan. Server harus dipasang dengan sistem operasi yang kompatibel dan harus memiliki spesifikasi yang memadai untuk menangani beban kerja yang diharapkan.

4. TACACS+ Installation: TACACS+ (Terminal Access Controller Access-Control System Plus) adalah protokol yang digunakan untuk menyediakan layanan autentikasi, otorisasi, dan akuntansi untuk akses jaringan.
5. TACACS+ Configuration: Setelah instalasi, TACACS+ harus dikonfigurasi untuk memenuhi kebutuhan spesifik jaringan. Konfigurasi ini mencakup pengaturan kebijakan autentikasi (siapa yang dapat mengakses jaringan), otorisasi (apa yang dapat dilakukan oleh pengguna yang diautentikasi), dan akuntansi (mencatat aktivitas pengguna untuk keperluan audit dan pelaporan). File konfigurasi biasanya menentukan pengguna, grup pengguna, dan hak akses terkait.
6. PuTTY Installation: PuTTY adalah aplikasi klien terminal yang digunakan untuk mengakses perangkat jaringan dari jarak jauh. Pada langkah ini, PuTTY diinstal pada komputer administrator.
7. Remote Switch Testing: Setelah PuTTY terinstal, langkah selanjutnya adalah menguji akses jarak jauh ke switch jaringan. Hal ini dilakukan dengan menggunakan PuTTY untuk terhubung ke switch dan memastikan bahwa administrator dapat mengakses dan mengelola switch dari jarak jauh. Pengujian ini penting untuk memastikan bahwa koneksi jaringan dan autentikasi berfungsi dengan benar..
8. TACACS+ Testing: Setelah pengujian koneksi jarak jauh berhasil, konfigurasi TACACS+ diuji untuk memastikan bahwa sistem autentikasi dan otorisasi berfungsi seperti yang diharapkan.
9. Log Analysis: Pada tahap ini, log yang dihasilkan oleh TACACS+ dan perangkat jaringan dianalisis untuk memastikan bahwa semua operasi berjalan lancar dan untuk mengidentifikasi serta menyelesaikan masalah yang mungkin timbul.
10. Finish: Ini adalah langkah terakhir dari proses, di mana semua langkah sebelumnya telah selesai, dan sistem siap digunakan.

Table 1. Comparison of TACACS+ with Other Software

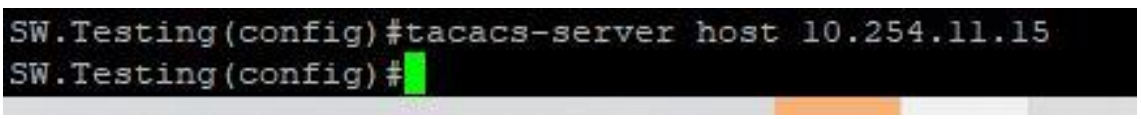
Aspek	TACACS+	RADIUS	Diameter
Transport Protocol	TCP	UDP	TCP/SCTP
Data Security	Encrypts entire payload	Encrypts only password	Supports
AAA Modularity	AAA Modularity	Separate (authentication, authorization, accounting)	Not separated (authentication and authorization combined)
Complexity	More complex	Lighter and faster	Very complex
Vendor	Proprietary (Cisco)	Vendor-neutral	Vendor-neutral
Fungsi	Network administration access	Remote access, WiFi, VPN	LTE, 5G, complex applications

3. Result and Discussions

3.1. Implementasi

TACACS+ (Terminal Access Controller Access-Control System Plus) adalah protokol keamanan yang menyediakan kontrol akses dan autentikasi untuk jaringan. Berikut adalah langkah-langkah dan perintah untuk menginstal dan mengonfigurasi server TACACS+ pada perangkat berbasis Linux. Proses ini melibatkan penginstalan paket TACACS+, konfigurasi file, dan menjalankan layanan TACACS+.
Berikut ini adalah implementasi pada perangkat jaringan Switch yang akan menginstal konfigurasi TACACS:
Konfigurasi TACACS pada Switch melalui CLI sebagai berikut :

1. Pertama masuk ke mode konfigurasi, langkah selanjutnya adalah menambahkan server TACACS yang akan digunakan untuk otentikasi dan dapat melakukannya dengan menggunakan perintah tacacs-server host, diikuti dengan alamat IP server TACACS yang dikonfigurasi sebelumnya.



Gambar 2. Konfigurasi sistem

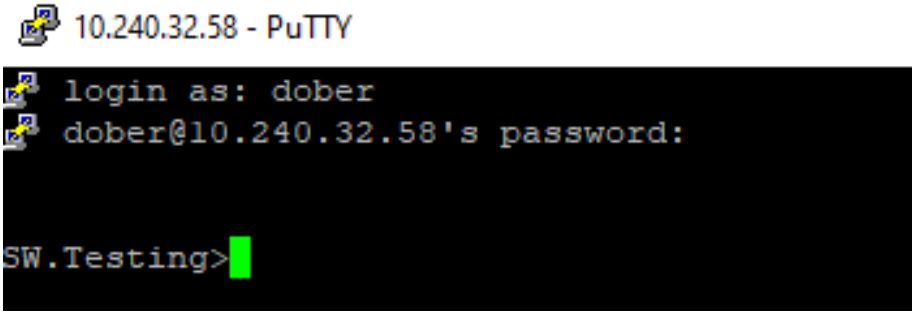
2. Selanjutnya, tambahkan encryption key yang akan digunakan untuk mengamankan komunikasi antara switch dan server TACACS. Perintah untuk menambahkan kunci enkripsi adalah sebagai berikut
3. tambahkan configuration berikut :

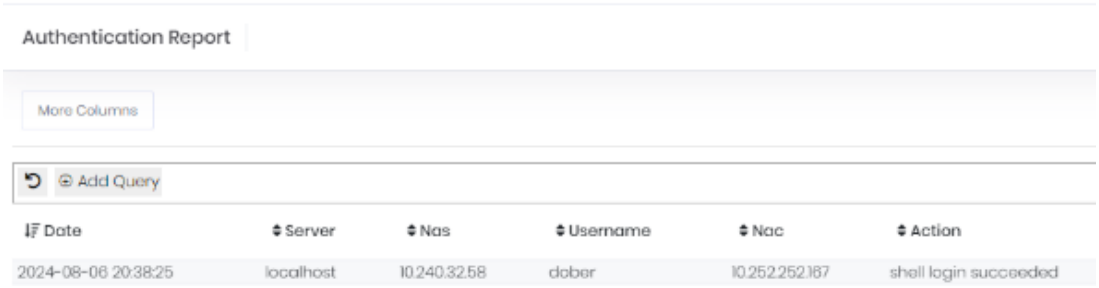
```
SW.Testing(config)#aaa new-model
SW.Testing(config)#aaa authentication login default local group tacacs+
SW.Testing(config)#$nable default local group tacacs+ enable
SW.Testing(config)#aaa authorization config-commands
SW.Testing(config)#aaa authorization exec default local group tacacs+
SW.Testing(config)#aaa authorization commands 1 default local group tacacs+
SW.Testing(config)#aaa authorization commands 15 default local group tacacs+
SW.Testing(config)#aaa accounting exec default start-stop group tacacs+
SW.Testing(config)#aaa accounting commands 1 default start-stop group tacacs+
SW.Testing(config)#$nds 15 default start-stop group tacacs+
SW.Testing(config)#
```

Gambar 3. Konfigurasi sistem 2

Secara keseluruhan, konfigurasi ini menyiapkan perangkat jaringan untuk menggunakan server TACACS+ untuk autentikasi, otorisasi, dan akuntansi. Hal ini meningkatkan keamanan dengan memastikan bahwa semua akses dan perintah dikontrol dan dicatat oleh server.

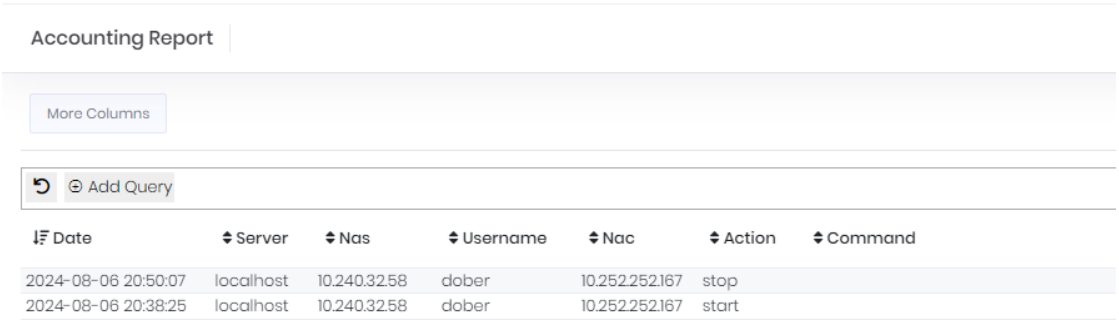
1. Jika TACACS berhasil dijalankan, maka akan muncul tampilan seperti berikut, di sini menggunakan username dober sebagai test untuk masuk ke switch yang telah dikonfigurasi sebelumnya
2. Untuk melihat log autentikasi yang mencatat semua percobaan login yang dilakukan. Di sini, Anda dapat melihat detail seperti siapa yang mencoba login, kapan, dan apakah login berhasil atau gagal.





Gambar 4. Melihat Log

3. Untuk melihat aktivitas pengguna yang login, termasuk waktu login, perintah yang dijalankan, dan tindakan lain yang diambil selama sesi login..



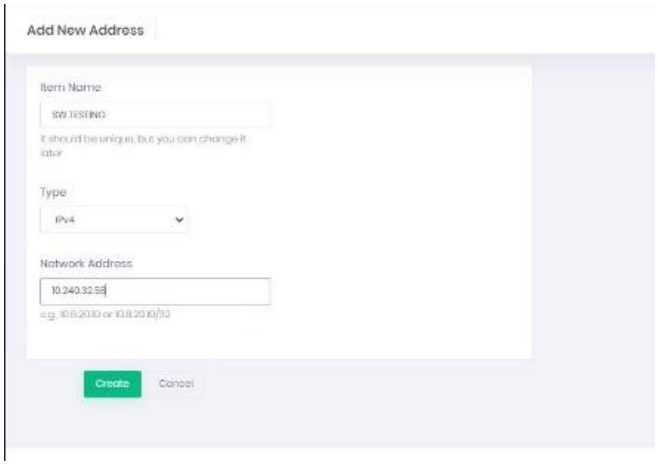
Gambar 5. Sesi Login

4. Untuk melihat aktivitas pengguna yang login semua perintah konfigurasi yang dijalankan dapat dilihat di Authorization Report,

Gambar 6. Authorization Report

TACACS Configuration pada Switch melalui GUI

1. Masukkan alamat, lalu klik tambah baru dan isi identitas sakelar sesuai kebutuhan.

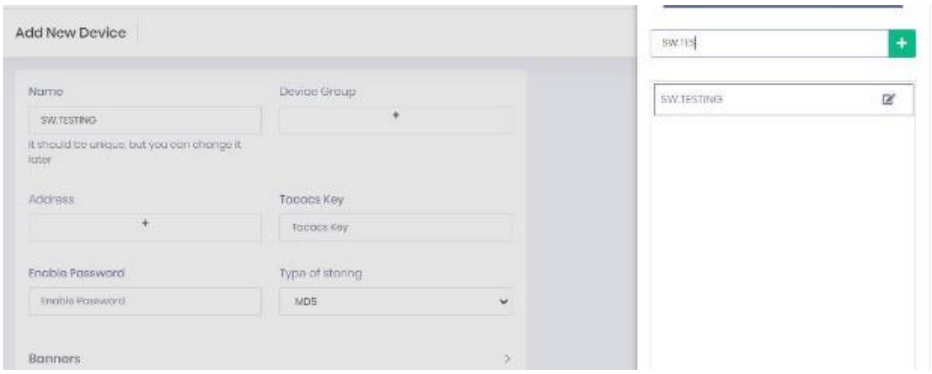


Gambar 7. Alamat GUI

2. Setelah alamat ditambahkan, cari nama switch yang telah dibuat sebelumnya

Gambar 8. View Setelah Login

3. Setelah identitas switch berhasil dibuat, masuk ke Menu Devices lalu isi nama dan Device Group yang sudah dibuat sebelumnya.

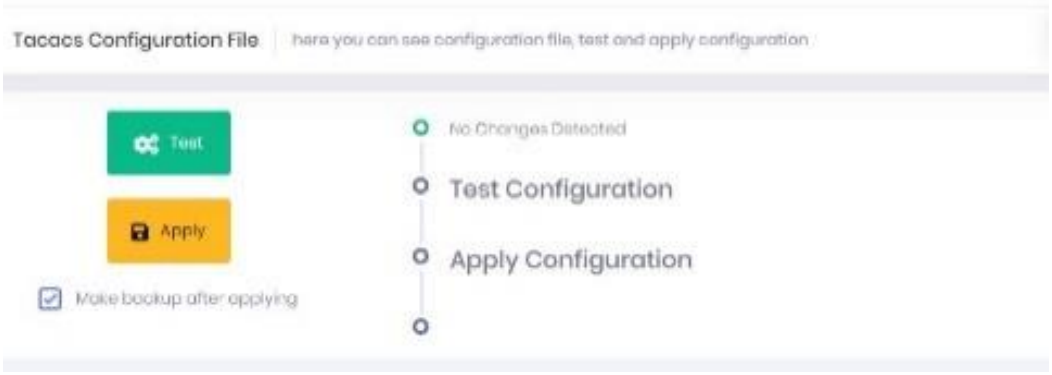


Gambar 9. Nama dan Device Group

4. Setelah Device berhasil di registrasi, klik tombol simpan yang ada di pojok kanan atas Menu

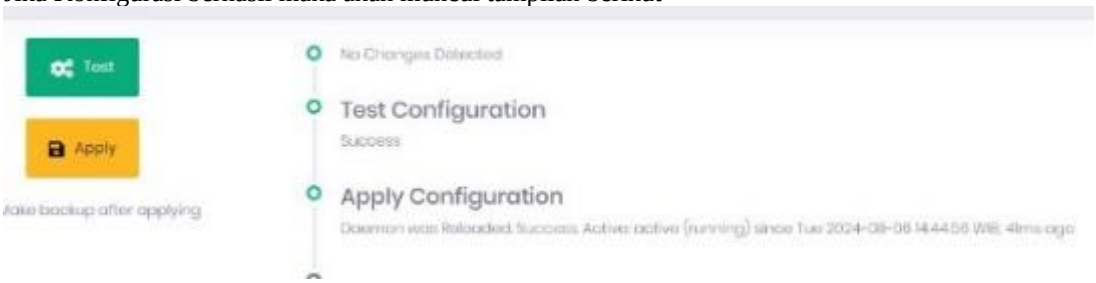
Gambar 10. Tanda Berhasil Registrasi

5. Jika berhasil disimpan, masuk ke Menu Uji & Terapkan untuk memverifikasi konfigurasi.



Gambar 11. Verifikasi Konfigurasi

6. Jika Konfigurasi berhasil maka akan muncul tampilan berikut



Gambar 12. Konfigurasi sukses

3.2. Evaluasi

Pengujian blackbox adalah teknik pengujian perangkat lunak yang mengevaluasi fungsionalitas sistem dari perspektif pengguna akhir, tanpa memerlukan pengetahuan apa pun tentang struktur internal, kode sumber, atau logika pemrograman. Dalam pendekatan ini, penguji bertindak sebagai pengguna akhir, dengan fokus semata-mata pada bagaimana perangkat lunak berperilaku berdasarkan masukan yang diberikan dan keluaran yang dihasilkan. Singkatnya, pengujian blackbox secara efektif memastikan bahwa perangkat lunak memenuhi spesifikasinya dan memenuhi persyaratan pengguna akhir, tanpa memerlukan pengetahuan terperinci tentang implementasi aplikasi. Metode ini sering diterapkan di seluruh tahap pengembangan perangkat lunak, khususnya dalam pengujian fungsional, pengujian regresi, dan pengujian penerimaan pengguna.

Table 2. TACACS GUI Login Menu Testing

No	Test	Test Type	Testing Steps	Result	Status
1	Login Page	Successful Login	Enter a username and password	User successfully login TACACS GUI	Successful
		Unsuccessful Login	Enter wrong username and password	User fails to login	Unsuccessful

Dari tabel pengujian kotak hitam untuk fungsi Login dapat disimpulkan bahwa pengujian ini membuktikan bahwa pengguna yang berhasil login ke dalam sistem sudah terdaftar terlebih dahulu, sedangkan pengguna yang gagal login belum terdaftar.

Table 3. TACACS Device Menu Testing

No	Test	Test Menu	Test Steps	Result	Status
1	Menu Devices	Add Devices	Click "Add Devices" in the Devices Menu	Add Devices" menu should show fields to complete.	Successful
		Search Devices	Enter the device name devices	The device list only show matching devices.	Successful
		Edit Devices	Click the "Edit"	The updated device information	Successful
		Delete Devices	Click the "Delete" icon	The deleted device should be removed	Successful
2	Menu Devices Group	Add Devices Group	Click the "Add" button.	The new group should appear in the list	Successful
		Search Devices Group	Search the Group name	The group list only show groups matching	Successful
		Edit Devices Group	Click the "Edit"	updated group name	Successful
		Delete Group	Click the "Delete"	The deleted group removed	Successful

Table 4. TACACS User Menu Testing

No	Test	Test Menu	Test Steps	Result	Status
1	Menu TACACS User	Add Users	Click the "Add" button.	The new user should appear in the list	Successful
		Search Users	Enter the user's	only show users matching	Successful
		Edit Users	Click the edit icon	A form to edit the user's	Successful
		Delete Users	Click the delete icon	A confirmation prompt	Successful
2	Menu Users Group	Add User Group	Click the "Add" button.	A form to add a new user group	Successful
		Search Users Group	Enter the user group name	group list should be filtered	Successful
		Edit Users Group	edit icon	Edit the user group details	Successful
		Delete Users Group	Delete icon to remove	A confirmation prompt	Successful

Table 6. Testing the Reports Menu

No	Test	Menu Tested	Testing Steps	Result	Status
1	Reports	Authentication	Test by logging	displays a successful login report	Successful
		Authorization	Test by entering command	The system displays	Successful
		Accounting	Test by entering command	The system displays	Successful

4. Conclusion

Penerapan TACACS+ pada perangkat switch jaringan di PT XYZ telah terbukti meningkatkan keamanan jaringan dengan memastikan bahwa hanya pengguna terverifikasi yang dapat mengakses dan mengelola perangkat. Sistem ini memungkinkan pencatatan autentikasi setiap kali pengguna mencoba mengakses switch, memastikan setiap upaya akses dapat dilacak dan diverifikasi, sehingga mencegah akses yang tidak sah. Selain itu, TACACS+ mencatat setiap tindakan pengguna yang melibatkan perubahan atau konfigurasi tambahan pada switch, meminimalkan risiko kesalahan atau perubahan konfigurasi yang mencurigakan. Sistem ini juga mencatat semua aktivitas pengguna setelah mereka memperoleh akses,

memberikan kontrol yang lebih baik atas penggunaan perangkat, serta memastikan siapa yang melakukan tindakan tertentu dan kapan tindakan tersebut dilakukan.

Daftar Pustaka

[1]. Cisco. (n.d.). *What is network switching?* Retrieved from https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html
[2]. Dutcher, W. (1997). TACACS, RADIUS secure servers. *PC Week, 14*(44), 151-153.
[3]. PuTTY. (n.d.). *PuTTY: A free SSH and telnet client*. Retrieved from https://www.putty.org/
[4]. TechTarget. (n.d.). *What is a network switch?* Retrieved from https://www.techtarget.com/searchnetworking/definition/network-switch
[5]. Cisco. (n.d.). *What is an unmanaged switch?* Retrieved from https://www.cisco.com/c/en/us/products/switches/what-is-an-unmanaged-switch.html
[6]. Cisco. (n.d.). *What is a managed switch?* Retrieved from https://www.cisco.com/c/en/us/products/switches/what-is-a-managed-switch.html
[7]. Cisco. (n.d.). *Power over Ethernet (PoE)*. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/power-over-ethernet-poe/nb-06-power-over-ethernet.html
[8]. IETF. (1993). *RFC 1492: An access control protocol, sometimes called TACACS*. Retrieved from https://datatracker.ietf.org/doc/html/rfc1492