Analisis dan Implementasi Kontrol Akses Jaringan dan Kebijakan pada PT. Asuransi Jiwa Sinarmas MSIG Tbk Menggunakan Sistem Genian NAC

Shesia Rizki Damara

Perangkat Lunak Sistem Informasi, Universitas Gunadarma
E-mail : shesiard@gmail.com

Abstrak

Kebocoran data perangkat internal perusahaan yang berisi informasi penting, merupakan masalah keamanan data dan jaringan komputer yang dapat terjadi. salah satu penyebabnya berasal dari kesalahan pihak internal (karyawan) organisasi/perusahaan tersebut dalam penggunaan perangkat dengan sistem BYOD (Bring Your Own Device) yang terhubung pada jaringan terpusat sehingga dibutuhkan Implementasi Kontrol Akses Jaringan pada PT. Asuransi Jiwa Sinarmas MSIG Tbk. dengan platform sistem Genian NAC yang didukung oleh teknologi 802.1X sebagai penyedia tiga fungsi penting dalam menjaga keamanan sistem yaitu Authentication, Authorization, Accounting tentunya mampu memaksimalkan sistem keamanan jaringan dengan cara menemukan, mengklasifikasikan, dan menerapkan kebijakan akses untuk pengguna, perangkat, sistem, dan aplikasi yang terhubung pada jaringan secara otomatis.

Kata Kunci: Network Access Control, IEEE 802.1X-EAP, IP Address Management.

Pendahuluan

Kebocoran data perangkat internal suatu organisasi/perusahaan yang berisi informasi penting merupakan masalah bagi keamanan data dan jaringan komputer yang dapat terjadi. hal tersebut dapat disebabkan oleh kesalahan pihak internal/karyawan dalam penggunaan perangkat dengan sistem BYOD (Bring Your Own Device) yang terhubung pada sistem jaringan perusahaan. [1] Implementasi Platform perangkat lunak Genian NAC menggunakan Sensor Jaringan berbasis layer 2 (dua) yang otomatis mengklasifikasikan pengguna dan perangkat yang terhubung dengan pengelompokan yang terstruktur berdasarkan kebutuhan bisnis perusahan, serta memiliki kecerdasan untuk menyajikan informasi secara langsung, mudah dipahami, dan dapat ditindaklanjut secara cepat. Dalam penggunaan fitur-fitur kontrol akses jaringan dengan Genian NAC, Administrator harus mengkonfigurasi sensor jaringan dalam mode aktif dan mengaktifkan kebijakan IPAM (IP Address Management).Manfaat Implementasi Kontrol Akses Jaringan dengan menggunakan Plaform Perangkat Lunak NAC di perusahaan PT. Sinarmas MSIG Tbk, antara lain: Mencegah terjadinya serangan terhadap server, Mengkontrol keamanan jaringan secara terpusat, Kontrol Aset manajemen dan kebijakan Teknologi Informasi pada sistem terpusat, Memudahkan Pencatatan laporan inventaris perangkat yang terkoneksi dengan jaringan sistem terpusat.

Security Policy

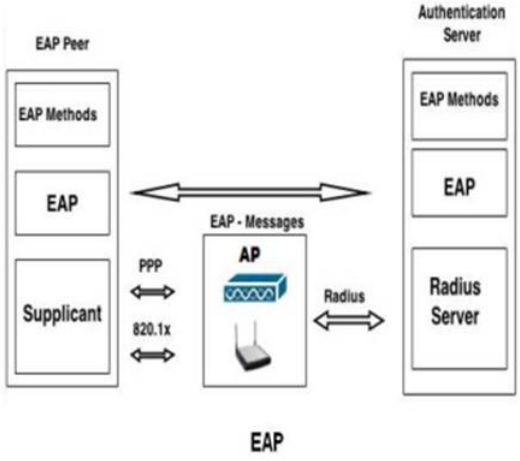
Security Policy (Kebijakan Keamanan) merupakan sebuah dokumen keamanan informasi yang berisi prinsip dan strategi tentang berbagai cara yang harus dilakukan untuk mengontrol serta mengatur tata cara mengamankan informasi.[2] Kebijakan keamanan organisasi yang dibangun dengan baik akan memberikan keberhasilan implementasi sistem terkait keamanan saat ini dan di masa depan. untuk meningkatkan keamanan bagi suatu organisasi adalah dengan memperkenalkan kebijakan tersebut kepada semua anggota staf tentang tugas dan tanggung jawab mereka yang berbeda Selama pengembangan sistem, hal tersebut bermanfaat untuk mengurangi risiko potensi pelanggaran keamanan melalui kesalahan manusia.

Protokol IEEE 802.1X – EAP

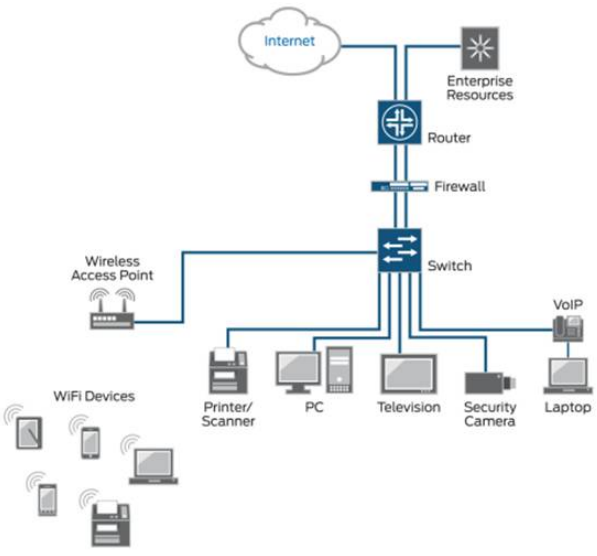
IEEE 802.1x (Institute of Electrical and Electronics Engineers) merupakan standar port jaringan berbasis kontrol akses. 802.1x yang memanfaatkan Protokol Authentication dengan varian yang diperluas untuk mengotentikasi akun pengguna atau terhadap otentikasi sistem eksternal melalui jaringan

DOI : http://dx.doi.org/10.32409/jikstik.19.3.67

kabel. [5] EAP (Extensible Authentication Protocol) bukan sebuah protokol, melainkan kerangka kerja (framework). Awalnya EAP dikembangkan untuk PPP (Point to Point Protocol).[3] EAP adalah persetujuan paket antara klien dan server. Struktur protokol 802.1x terdiri dari 3 komponen utama: a.Client/Supplicant, b.AP (Access Point) c.AS (Authentication Server). Gambaran EAP terdiri dari dua logic port: port terkontrol dan port tidak terkontrol. Jika pengguna telah dikenal/tervalidasi maka port terkontrol akan digunakan, tetapi ketika pengguna tidak tersertifikasi/tidak dikenal maka port tidak terkontrol digunakan untuk komunikasi seperti Gambar 1.



Gambar 1: *EAP Overview*



Gambar 2: Arsitektur NAC

Network Access Control

Network Access Control (NAC) merupakan solusi untuk keamanan jaringan komputer dengan beberapa kebijakan, termasuk pemeriksaan sebelum dan pasca masuk untuk endpoint. dimana user dan perangkatnya dapat mengakses ke suatu jaringan dan apa saja yang dapat diakses pada jaringan tersebut [4]. NAC dimulai dengan memeriksa apakah suatu perangkat diizinkan untuk terhubung ke jaringan. melalui teknologi yang dikenal sebagai 802.1X, yang menyediakan tiga fungsi penting yang disebut Authentication, Authorization, Accounting) [5]. Arsitektur NAC dapat dilihat pada Gambar 2. Beberapa solusi NAC [6] diantaranya adalah :

1. Cisco NAC Appliance.
2. ForeScout
3. Genian NAC
4. Packetfence

Bring Your Own Device

BYOD mendefinisikan tentang user (pengguna) yang memiliki kebebasan untuk menggunakan alat pribadi untuk mengakses informasi dan berkomunikasi melalui jaringan bisnis atau jaringan akademis [9]. kebijakan BYOD tidak hanya memungkinkan pengguna dapat mengakses data internal hanya di tempat organisasi tersebut, tetapi pengguna juga dapat mengakses data internal organisasi tersebut di luar lingkungan organisasi [10].

Tabel 1: Penelitian terkait implementasi NAC

No	Nama	Judul	Tahun	Analisis
1	Ali Latiful Apriantо dan Idris Winarno	Implementasi Network Access Control Pada Jaringan EEPIS	2015	Melakukan implementasi NAC dengan metode: *Filtering* Paket Data dengan *Snort* [4]
2	Musa Abubakar Muhammad dan Aladdin Ayesh	A Behaviour Profiling Based Technique for	2019	Musa Abubakar Muhammad dan Aladdin Ayesh[5]
3	M. Roopesh, G. Reethika, B.V. Srinath, dan A.Sarumathi	Network Access Control	2017	Membahas masalah dalam sistem keamanan dan solusi yang ditawarkan oleh produk NAC [7]
4	Agus Sulomo	Penerapan Pengamatan Network Access Control (NAC) untuk Autentikasi dengan Menggunakan Protokol 802.1X di Bank Indonesia	2018	Melakukan implementasi NAC pada layer 2 model OSI. Penerapan NAC ini meliputi pengecekan perangkat yang ingin terkoneksi ke dalam jaringan Bank Indonesia [8].

Metode Uji

Penelitian ini mengambil beberapa referensi penelitian sebelumnya yang berhubungan dengan penelitian ini termasuk jurnal-jurnal yang terdapat pada Tabel 1 State of Art / penelitian terkait implementasi NAC.

Pada Implementasi aturan kebijakan akses (Policy Access) jaringan kedalam Policy Server Genian NAC disusun terlebih dahulu list kepatuhan yang akan diterapkan sebagai kebijakan akses (Policy Access) pada sistem jaringan terpusat perusahaan. berikut list akses yang akan di implementasikan kedalam server kebijakan pada Genian NAC pada tabel 2.

Tabel 2: . List Kebijakan Genian NAC

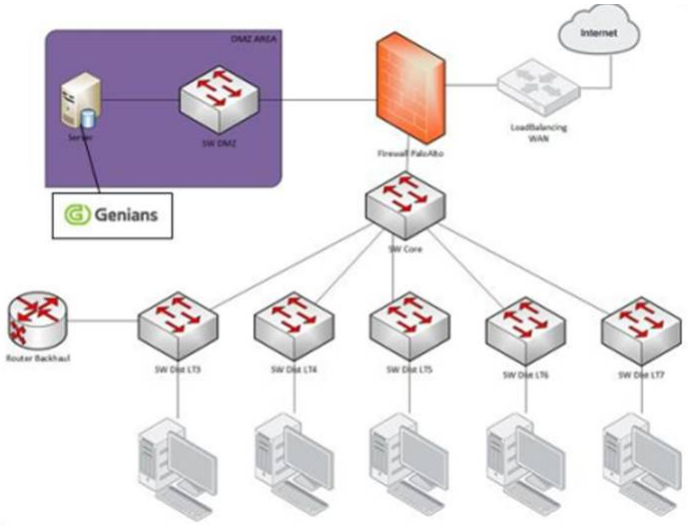
Group	Kondisi	*Policy Access*
Tamu	Akun tamu	Hanya Akses Internet
Semua Pengguna	Tidak terinstal Software Agent	Tidak ada akses jaringan
Semua Pengguna	Antivirus yang Tidak Sesuai Antivirus tidak berjalan Antivirus Tidak Terpasang Pemindaian Real-Time Antivirus Tidak Berjalan Antivirus sudah ketinggalan zaman	Tidak ada akses Jaringan, diizinkan mengakses Panda AV Server
Group IT	Setelah memenuhi kepatuhan	Akses Jaringan diizinkan
Tamu	Pengguna diharuskan memasukkan Nama Pengguna dan Kata Sandi untuk diautentikasi	Captive Web Portal (CWP) untuk Autentikasi Pengguna
Semua Pengguna	Penolakan Perubahan IP atau Konflik IP	Tidak Ada Akses Jaringan
Semua Pengguna	Wireless endpoint putus koneksi letika terhubung pada SSID luar(bukan SSID perusahaan)	Tidak Ada Akses Jaringan
Semua Pengguna	Ditemukan/terdeteksi Malware	Tidak Ada Akses Jaringan
Semua Pengguna	IP / MAC Node tidak diizinkan	Tidak Ada Akses Jaringan

Implementasi Platform sistem Perangkat Lunak Genian NAC sebagai Sistem Kontrol Akses Jaringan pada sistem jaringan Infrastruktur PT. Asuransi Jiwa Sinarmas MSIG Tbk. menggunakan teknologi Device Platform, dimana semua jenis perangkat keras dan perangkat lunak, atau kombinasi dari kedua jenis perangkat tersebut dapat menyajikan identitas perangkat yang paling akurat, kontekstual, dan informasi risiko pada jaringan untuk meningkatkan visibilitas dan mengamankan akses jaringan pada era IoT dimana DPI yang dapat dibagikan melalui Genians Cloud [10] yang menyajikan solusi keamanan berupa:

1. Kecerdasan berkelanjutaan pada Keamanan Cyber
2. Solusi Penting Keamanan Cyber
3. Kontrol Akses (Keamanan) Berlapis-Lapis
4. Interoperabilitas

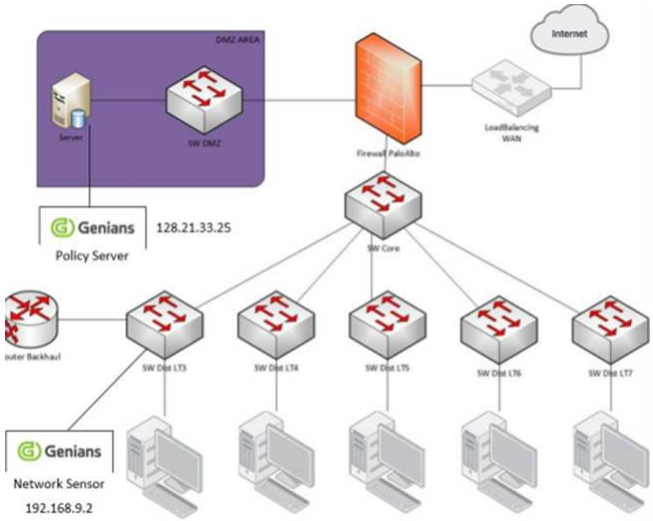
Konfigurasi jaringan yang digunakan sebagai model sistem adalah :

1. 1.Topologi Jaringan
   (a) Pada topologi fisik, Genian NAC diinstal pada 1 perangkat server yang mana perangkat tersebutt ada pada DMZ Area, yang terdapat pada Gambar 3.



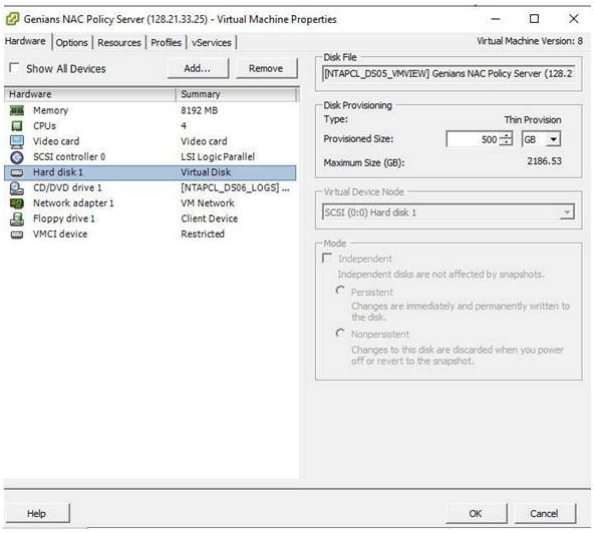
Gambar 3: Physical Diagram

   (b) Pada topologi logical, Genian NAC terletak pada 2 segmen, untuk Policy Server terletak pada segmen server, sedangkan network sensor ada pada segmen user dibawah Switch Core seperti Gambar 4.

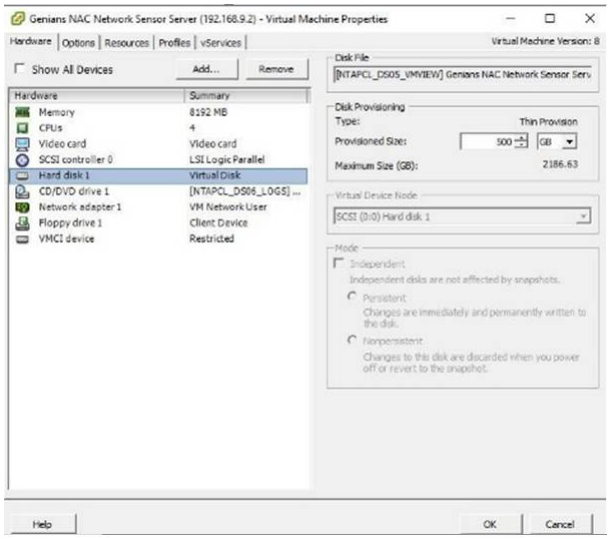


Gambar 4: Logical Diagram

2. Spesifikasi Genian NAC Spesifikasi Policy Server dan Network Sensor Genian NAC yang diinstal pada jaringan Infrastruktur Perusahaan terdapat pada Gambar 5 & Gambar 6.



Gambar 5: Policy Server



Gambar 6: Network Sensor

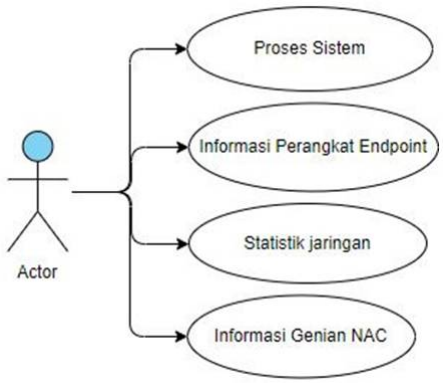


Figure 7: Use Case Sistem Diagram

Table 3: . Pengujian Sistem Genian NAC

No	Skenario Uji	Validasi Input	Pengujian	Hasil
1.	*Menu Dashboard*	Klik Mouse	Muncul tampilan seluruh proses yang sedang berjalan di sistem operasi sebagai bagan monitoring keseluruhan	Valid
2.	Menu Management	Klik Mouse	Muncul tampilan informasi detail (IP,MAC,DNS, dll) dari perangkat endpoint	Valid
3.	Menu *Log*	Klik Mouse	Muncul tampilan informasi statistik port untuk mempermudah evaluasi kinerja sistem	Valid
4.	Menu *Policy*	Klik Mouse	Muncul Tampilan informasi untuk penerapan Pollicy(kebijakan) yang diterapkan kepada akses jaringan dari perangkat *Endpoint*	Valid
5.	Menu *Preferences*	Klik Mouse	Muncul tampilan klasifikasi perangkat *endpoint* dan tampilan mengatur preferensi system perangkat endpoint sesuai kebijakan perusahaan	Valid
6.	Menu *System*	Klik Mouse	Muncul tampilan informasi seputar sistem Genian NAC dari sisi	Valid

Ruang Lingkup Uji

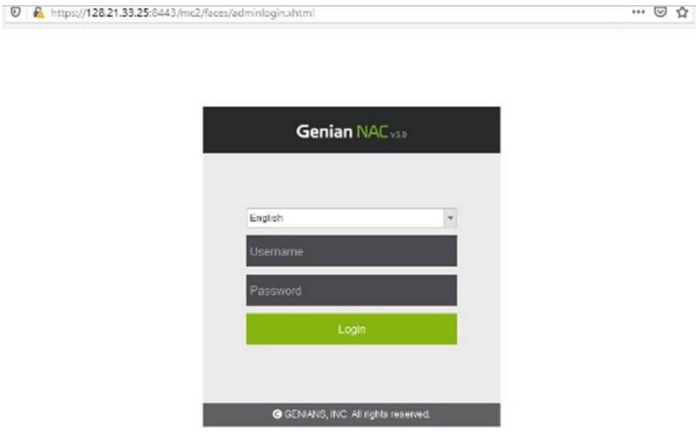
Untuk memastikan pengujian fungsi sistem Genian NAC dan beroperasi dengan baik ditunjukkan pada Gambar 7 terdapat satu actor yaitu IT-Security Administrator yang menjalankan system dan dapat mengakses seluruh menu proses sistem, detail informasi perangkat endpoint yang terhubung men-

gakses statistik jaringan, serta mengakses informasi seputar Genian Sistem dan pengembangan kerja sistemnya.

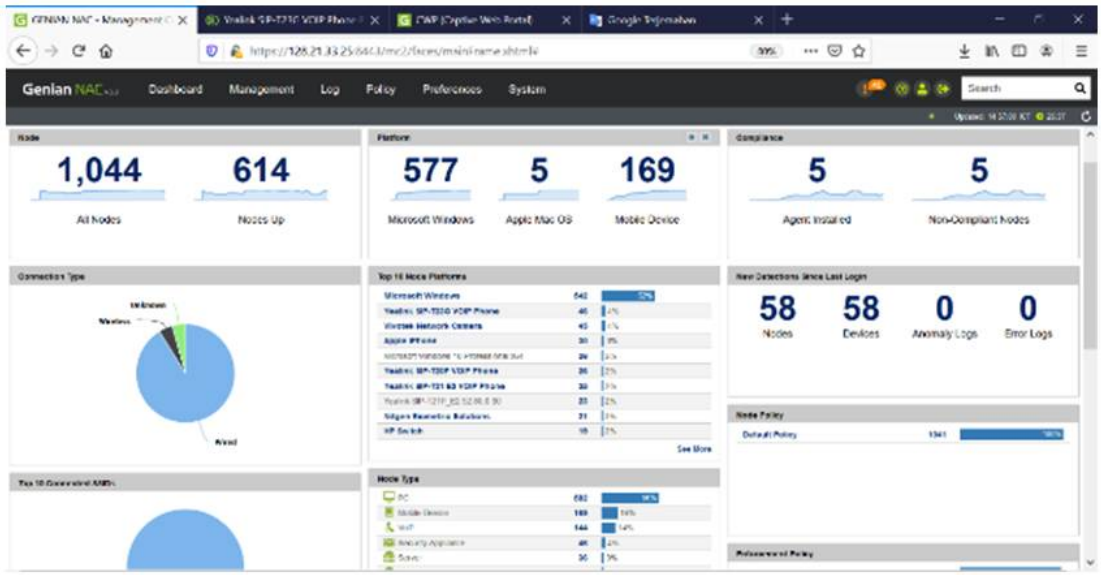
Kriteria yang digunakan untuk pengujian sistem Genian NAC didini menggunakan metode validasi untuk membuktikan validitas sistem yang akan digunakan oleh administrator IT-Security dalam mengelola sistem tersebut terdapat pada Tabel 3.

Hasil Analisa dan Implementasi

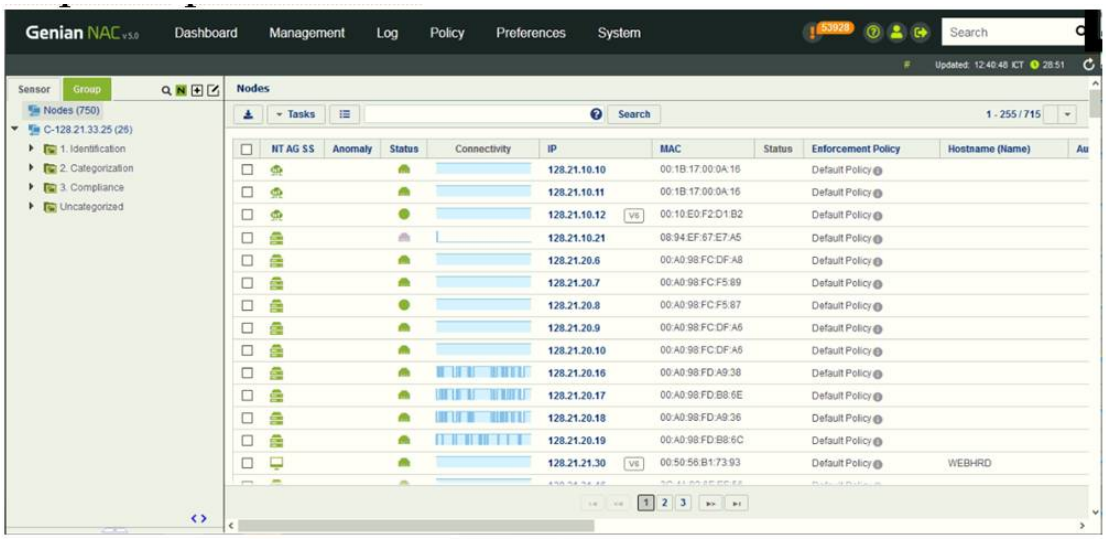
Proses monitoring guna implementasi Genian NAC pada PT Asuransi Jiwa Sinarmas MSIG Tbk. menggunakan cloud system yang dapat diakses melalui search engine dengan memasukkan alamat IP yang sudah diatur sebelumnya yaitu 128.21.33.25 setelah itu akan masuk kedalam halaman login sistem Genian NAC, lihat Gambar 8 dan aspek lainnya adalah :



Gambar 8: Halaman Login Genian NAC



Gambar 9: Halaman Dashboard Genian NAC



Gambar 10: Node Management

1. Dashboard

   Berfungsi untuk proses monitoring keamanan jaringan yang di dalamnya terdapat informasi seluruh perangkat endpoint yang terdeteksi oleh Genian NAC dan spesifikasi dari tipe perangkat, tipe koneksi, jenis OS, Compliance yang terhubung dengan jaringan terpusat (server Perusahaan) dan telah di scan oleh jaringan sensor Genian NAC, lihat Gambar 9.

2. Management

   Menu management ini digunakan untuk memonitor network assets berdasarkan alamat IP masing-masing perangkat yang terhubung pada jaringan terpusat perusahaan, lihat Gambar 10.

3. Log Menu ini digunakan untuk melihat semua informasi log yang terekam di dalam sistem Genian NAC, lihat Gambar 11.

4. Policy Menu pada halaman ini digunakan untuk membuat policy/kebijakan, membuat group tertentu, membuat schedule, dan sebagainya yang berlaku untuk perangkat endpoint, lihat Gambar 12..

5. Preferences Node Type di dalam menu preference berisi tentang Definisi/arti dari icon yang terdapat pada menu management > node , lihat Gambar 13.

6. System Session Sub menu Session di dalam sistem digunakan untuk melihat user yang telah login kedalam sistem Genian NAC, lihat Gambar 14.

7. License PT Asuransi Jiwa Sinarmas MSIG Tbk menggunakan 2 license untuk implementasi sistem Genian NAC ini, yaitu:

   (a) License Genians Tidak ada batas waktu, selama Genian tidak diinstall ulang, karena license ini menyangkut pada server ID, lihat Gambar 15

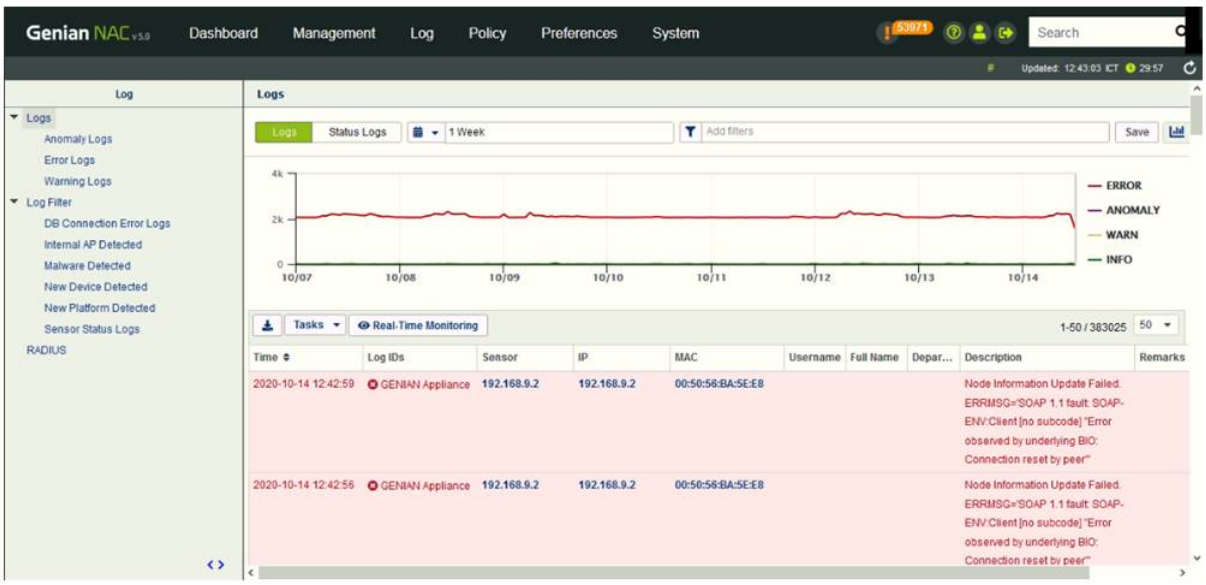
   (b) License Maintenance bersifat sementara, yakni pertahun. License ini untuk support langsung dari pihak Genian jika ada issue, dan juga untuk update firmware Genian NAC.

Genian Software

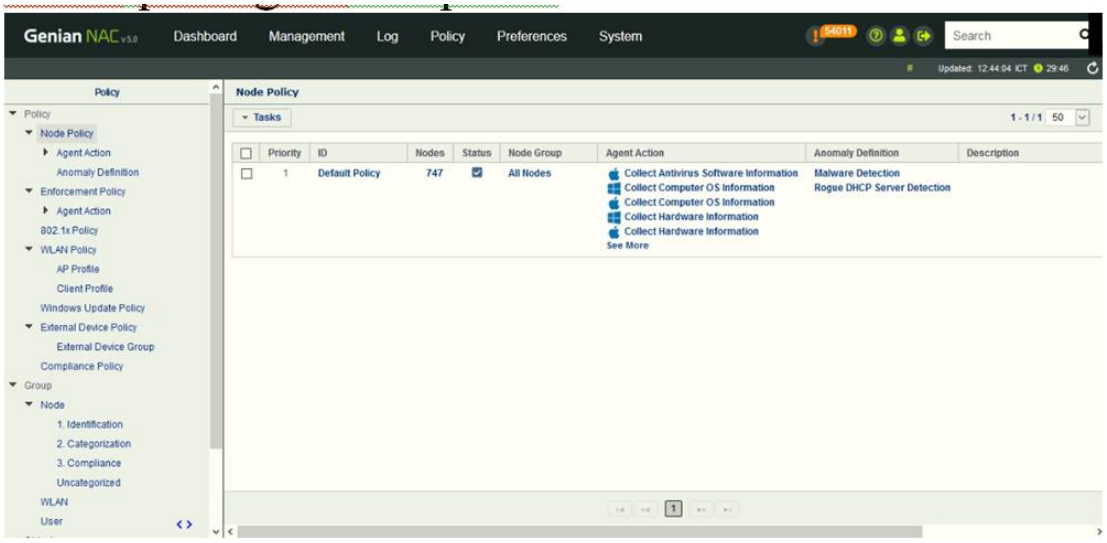
Genian agent dapat di unduh melalui menu ini, dan apabila ingin mengupdate firmware ke versi terbaru, dapat dilakukan dengan klik update from Genian Cloud, lihat Gambar 16.

Genian Data

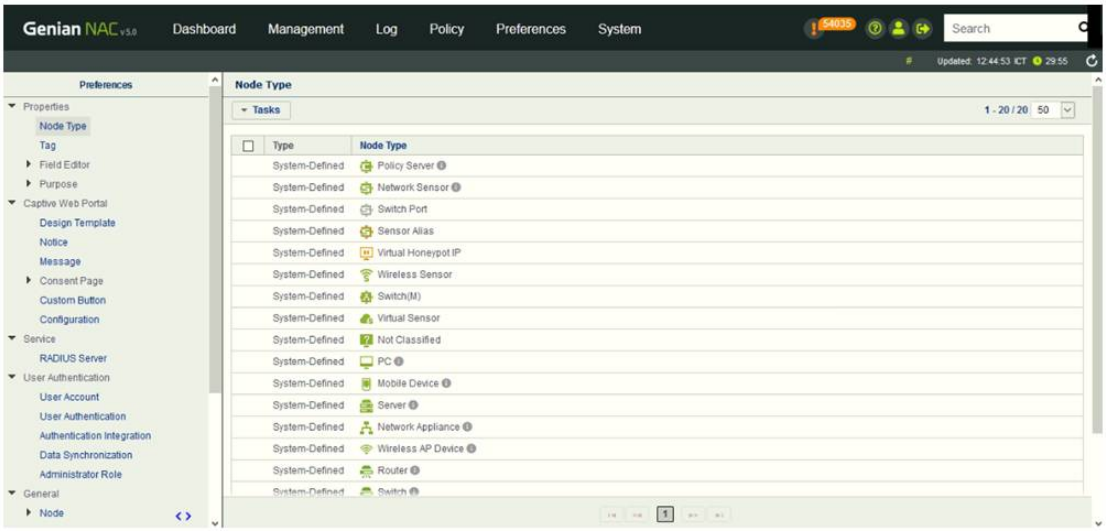
Halaman ini digunakan untuk mengupdate detail informasi perangkat yang bersumber dari server Genian, jika policy server Genian terkoneksi dengan internet, maka informasi berikut ini akan terupdate secara otomatis, lihat Gambar 17.



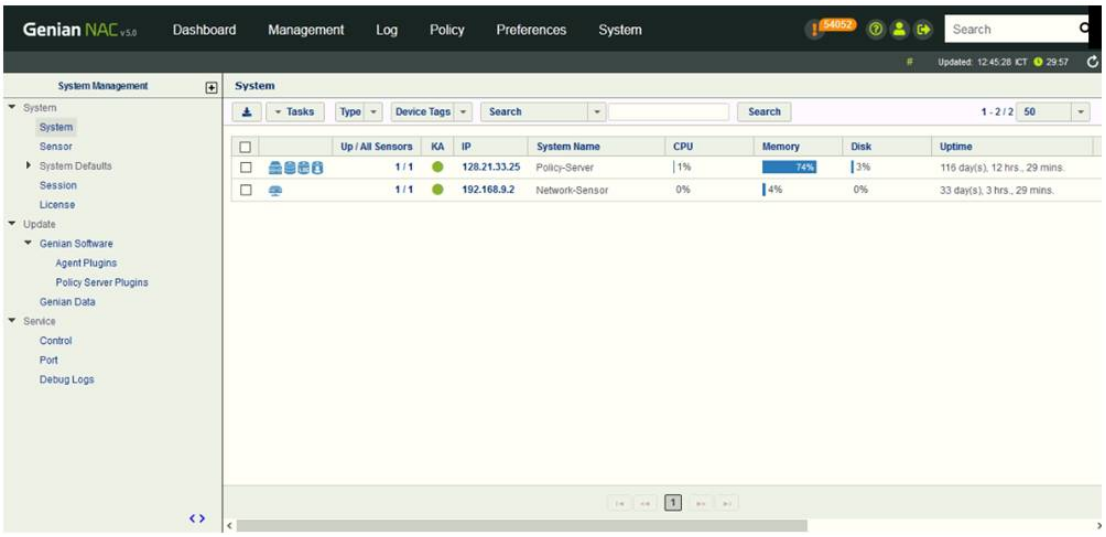
Gambar 11: Halaman Log



Gambar 12: Policy Node



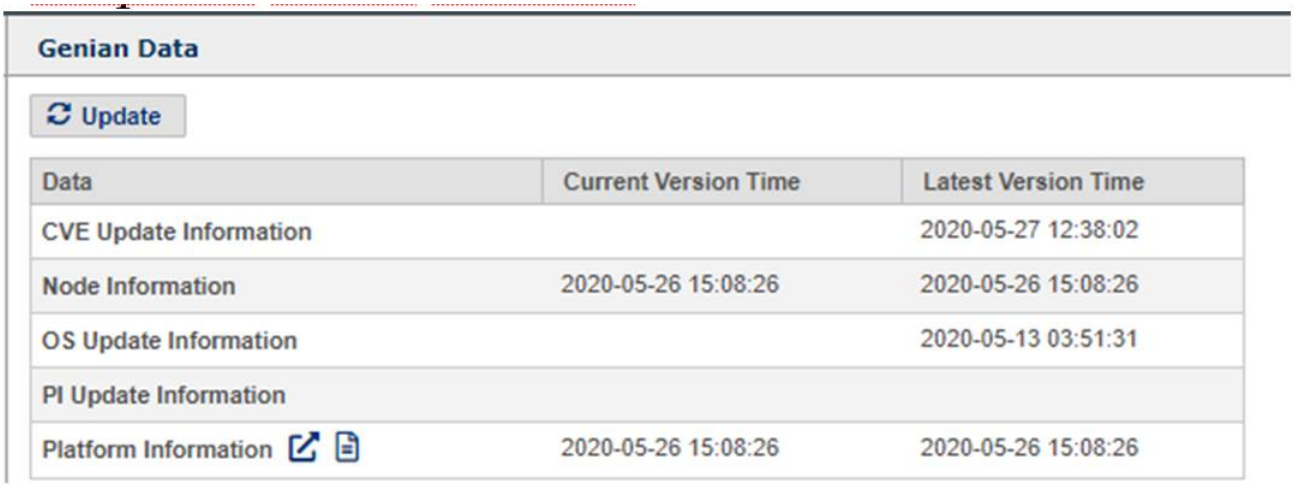
Gambar 13: Node Type Preference



Gambar 14: Session

Gambar 15: Licence Genians

Gambar 16: Genian Software



Gambar 17: Genian Data

Penutup

Mekanisme Kontrol Akses Jaringan menggunakan sistem Genian NAC berdasarkan analisa dan implementasi yang telah dilakukan, maka dapat ditarik kesimpulan :

1. Kontrol Akses Jaringan untuk manajemen kebijakan penggunaan perangkat jaringan komputer membawa manfaat bagi perusahaan terutama untuk mengontrol dan mengalokasikan penggunaan bandwidth seluruh staff yang mengakses sumber daya jaringan perusahaan

2. Genian Sistem didukung dengan protokol IEEE 802.1x-EAP yang yang memiliki faktor keamanan berupa Privasi, Identifikasi, Otentikasi, Autorisasi, Akuntabilitas guna menunjang aspek efisiensi dan efektifitas keamanan sistem perusahaan serta memudahkan klasifikasi hak akses bagi perangkat endpoint yang terhubung dengan akses jaringan perusahaan sehingga meminimalisir resiko keamanan jaringan terpusat.

3. Memudahkan network administrator untuk memonitor dan mengkontrol perangkat pengguna siapa saja yang terkoneksi serta mengatur hak akses dalam jaringan perusahaan guna kepentingan keamanan informasi, asset manajemen dan infrastruktur.

4. Genian NAC mengkategorikan seluruh perangkat endpoint berdasarkan grup tertentu. Sehingga apabila ditemukan perangkat pengguna yang tidak sesuai dengan kebijakan yang telah ditetapkan, maka Genian NAC memblokir IP Address perangkat tersebut secara otomatis. sehingga perangkat tersebut tidak dapat terhubung dengan akses internet jaringan perusahaan

Daftar Pustaka

[1] Anonim, “Genian NAC Admin Guide”, diakses daring pada http://docs.genians.com/release/en/deploy_overview.html, diakses 02 Februari 2020].

[2] D. Danchev, “Building and Implementing a Successful Information Security Policy”, E-Book WindowSecurity.com, diakses daring pada https://www. netsense/ downloads/ security-policy.pdf. , diakses 26 Februari 2020.

[3] Umesh Kumar, Praven Kumar and Sapna.Gambhir, “Analysis and Literature review of IEEE 802.x (Authentication) Protocols”, International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Volume-3, 2014.

[4] Ali Latiful Aprianto dan Idris Winarno, ”Implementasi Network Access Control pada Jaringan EEPIS”, Electronics Engineering Polytechnic Institute of Surabaya, 2015.

[5] M. Abubakar Muhammad and Aladdin Ayesh, ”A Behaviour Profiling Based Technique for Network Access Control Systems. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 23-30. The Society of Digital Information and Wireless Communications (SDIWC), ISSN: 2305-00, 2019.

[6] Asep M. Taufik, “Pembangunan Network Access Control untuk Authentikasi dan Security dengan menggunakan 802.1X Authentication. ISSN:2089-9033”, Edisi 1 Volume 1. Universitas Komputer Indonesia, Bandung, 2014.

[7] M. Roopesh, G. Reethika, B.V.Srinath, and A. Sarumathi, “Network Access Control”, International Journal on Computer Science and Engineering (IJCSE), ISSN:0975-3397, Vol.9 No.5, 2017.

[8] Agus Sulomo, “Penerapan Pengamanan Network Access Control (NAC) Untuk Autentikasi dengan menggunakan Protokol 802.1X di Bank Indonesia”, Universitas Mercubuana, Jakarta, 2018.

[9] Anonim, “Cisco Networking Academy course 2019/2020”, diakses daring pada https://static-course-assets.s3.amazonaws.com /ITN6/en/index.html#1.4.1.2, diakses 28 Februari 2020.

[10] Morufu Olalere, M. Taufik.Abdullah, Ramlan Mahmod and Azizol Abdullah,”A Review of Bring Your Own Device on Security Issues”, Volume: 5 issue: 2. Universiti Putra, Malaysia, 2015.

Halaman ini sengaja dikosongkan.