JURNAL NUANSA INFORMATIKA
Volume 16 Nomor 2, Juli 2022
p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

PENERAPAN NETWORK ACCESS CONTROL AUTENTIKASI INTERNAL NETWORK SECURITY PROTOKOL 802.1 X

Mamay Syani[1], Rizqi Mahestro Tresna[2], Eryan Ahmad Firdaus[3], Fauzi Faisal Nugraha[4]
[1,2]Politeknik TEDC Bandung
[3]Universitas Galuh Ciamis
[4]Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Email: [1]msyani@poltektedc.ac.id, [2]rizqimahestrotresna@gmail.com,
[3]eryan.ahmad.firdaus@unigal.ac.id, [4]fauzi.kun@gmail.com

Abstrak

Jaringan merupakan sebuah sistem yang dibangun untuk memudahkan manusia dalam berbagi informasi. Bagi sebuah perusahaan pada era sekarang jaringan merupakan sebuah aset yang sangat vital yang perlu dilindungi. Semua data mengenai detail perusahaan dapat diakses dengan mudah melalui jaringan. Penelitian ini bertujuan untuk membantu perusahaan dalam mengamankan asetnya. Membangun Network Access Control (NAC) dengan menggunakan platform forescout akan memudahkan seorang administrator dalam mengontrol dan memonitoring kondisi jaringan di PT. XYZ dengan mudah, fitur policy pada platform forescout ini mengkombinasikan berbagai macam kondisi untuk keamanan jaringan seperti antivirus host intrusion dan network worm. Pengujian sistem mendapat hasil yang bagus dari total karyawan organik 139 karyawan dari data penggunaan aplikasi antivirus ada 162 antivirus yang terinstall pada device/pc yang berada pada jaringan. Penulis menggunakan metode Network Development Life Cycle (NDLC) melalui beberapa tahapan yakni Analysis, Design, Simulation, Implementation, Monitoring dan Management.

Kata Kunci : *NAC, forescout, policy, Antivirus, NDLC*

Abstract

The network is a system built to make it easier for humans to share information. For a company in today's era, the network is a very vital asset that needs to be protected all data regarding company details can be accessed easily through the network. This study aims to assist companies in securing their assets. Building a NAC using the forescout platform will make it easier for an administrator to easily control and monitor network conditions at PT. XYZ, the policy feature on this forescout platform combines various conditions for network security such as Antivirus host intrusion and network worms. The system test got good results from a total of 139 organic employees. From the data on the use of the Antivirus application, there were 162 antiviruses installed on the device/pc that was on the network. The author uses the NDLC method that goes through several stages of Analysis, Design, Simulation, Implementation, Monitoring and Managements.

Keywords : *NAC, forescout, policy, Antivirus, NDLC*

1. PENDAHULUAN

Perkembangan Teknologi Informasi dan Komunikasi sangatlah pesat dan beragam, untuk itu perlu sebuah perencanaan baik yang sesuai dengan kebutuhan dan juga teknologi yang ada saat ini serta yang akan datang. Dalam menggunaan teknologi sistem informasi menjadi kebutuhan manusia dan akan memberikan manfaat besar terhadap perubahan pada suatu struktur organisasi dan manajemen organisasi [2]. Penerapan Teknologi Informasi yang kurang tepat dan tidak melihat jauh ke masa depan serta

Terakreditasi SINTA 5

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

perencanaan yang tidak matang akan mengakibatkan pengeluaran anggaran yang tidak efisien.

PT. XYZ sebagai salah satu organisasi yang memegang peranan yang sangat penting di Indonesia dengan kegiatan usaha antara lain: sebagai penyedia tenaga listrik juga tidak lepas dari kebutuhan teknologi informasi yang bermutu dan tepat guna.

PT. XYZ berlokasi di Jl. Desa Cadas Sari, Kecamatan Tegal Waru, Kabupaten Purwakarta, Jawa Barat dengan jumlah karyawan *organik* 139 orang dan *Non-organik* 15 orang, jumlah tersebut belum termasuk dan tenaga bantu kantor lainnya. Karyawan *organik* tersebut setiap hari bekerja dengan menggunakan perangkat komputer/laptop.

Akses perpindahan data yang sangat cepat dapat menimbulkan kerugian bagi individu maupun korporat yang diakibatkan serangan virus. Tak jarang banyak karyawan yang kedapatan antivirus pada laptop yang digunakan statusnya *out-of-date.* Pada tanggal 20 Januari 2020 *user IT* mendapat laporan bahwa ada *device*/PC *client* yang terkena serangan, untuk mengantisipasi hal tersebut terjadi pada *PC* yang lain, maka dapat dilakukan beberapa upaya seperti berikut:

1.1. Distributed System

Sistem terdistribusi ialah sistem yang terdiri dari kumpulan mesin otonom yang dihubungkan dengan jaringan komunikasi dan dilengkapi sistem perangkat lunak untuk menghasilkan lingkungan komputasi yang terintegrasi dan konsisten. Sistem terdistribusi memungkinkan orang untuk bekerja sama dan mengkoordinasikan aktivitas mereka secara lebih efektif dan efisien. Tujuan utama dari sistem distribusi dapat diwakili oleh: berbagi sumber daya, keterbukaan, konkurensi, skalabilitas, toleransi kesalahan dan transparansi.[1]

1.2. Network Access Control (NAC)

NAC merupakan sebuah pendekatan dalam keamanan jaringan komputer yang berusaha untuk memadukan beberapa teknologi pengamanan jaringan, seperti *antivirus, host intrusion prevention*, dan autentikasi pada sistem serta keamanan jaringan lainnya. NAC menjadi solusi dalam keamanan jaringan komputer yang menggunakan beberapa protokol untuk mendefinisikan dan mengimplementasikan sebuah aturan yang mendeskripsikan cara untuk mengamankan sebuah akses ke dalam sebuah jaringan ketika sebuah alat mencoba untuk tersambung dalam suatu jaringan. NAC bertujuan untuk mengontrol akses dalam suatu jaringan dengan penerapan *policy* tertentu yang telah diatur sebelumnya. Dimana seorang administrator dapat menentukan segmen atau perangkat mana saja yang dapat mengakses suatu jaringan, dan apa yang dapat dilakukan perangkat tersebut dalam suatu jaringan. Sehingga jaringan tersebut terhindar dari serangan virus, *host intrusion* dan *network worm*. NAC mungkin mengintegrasikan proses remediasi otomatis (memperbaiki node yang tidak sesuai sebelum mengizinkan akses) ke dalam sistem jaringan, memungkinkan infrastruktur jaringan seperti *router*, *switch*, dan *firewall* untuk bekerja sama dengan *server* kantor belakang dan peralatan komputasi pengguna akhir untuk memastikan sistem informasi beroperasi dengan aman sebelum interoperabilitas diizinkan. Bentuk dasar NAC adalah 802.1X standar.[3]

1.3. ForeScout

ForeScout Technologies adalah perusahaan swasta yang berbasis di Campbell, California, yang menjual perangkat keras dan peralatan virtual

Terakreditasi SINTA 5

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

dari keluarga *Counter* ACT. Meskipun ForeScout menawarkan agen opsional, pendekatan tanpa clien memudahkan dukungan endpoint Windows, Mac OS X dan Linux. *Forescout* adalah *platform* yang menyediakan pemantauan dan mitigasi keamanan berkelanjutan. Hal ini memungkinkan organisasi TI untuk secara efisien menangani berbagai akses, kepatuhan titik akhir, dan tantangan manajemen ancaman bahkan dalam jaringan perusahaan yang kompleks, dinamis, dan luas saat ini.[4]

1.4. Protokol SNMP (Simple Network Management Protocol)

SNMP merupakan protokol yang digunakan secara luas untuk pengelolaan jaringan khususnya kegiatan monitoring jaringan. Berbagai perangkat mendukung protokol SNMP untuk kegiatan monitoring, mulai *dari Router, Switch, Firewall, Modem/ONT, Server*, Komputer (PC), *IP Cam, IP Phone* hingga *Hypervisor* seperti ESXi. SNMP menggunakan data-data yang didapat dari komunikasi UDP dengan *device/*peralatan yang masuk dalam jaringan tersebut. SNMP dapat meminta data atau melakukan *setting* kepada peralatan yang bersangkutan.[5]

1.5. LDAP *(Lightwieght Directory Access Protocol)*

LDAP adalah protokol yang digunakan untuk mengakses berbagai informasi dalam suatu direktori. LDAP dikembangkan atas dasar X.500 yang lebih mudah dan mendukung TCP/IP, walaupun penggunaannya belum luas tapi LDAP merupakan *Open Protocol* yang fleksibel karena dapat diimplementasikan untuk aplikasi seperti E-mail, Public Key dengan berbagai platform dan sistem operasi. LDAP merupakan bagian dari *Internet Protocol*, yang digunakan untuk mengakses suatu directory misalnya directory telepon, directory email suatu perusahaan dan lain sebagainya. LDAP ini tidak hanya membaca informasi, tetapi juga bisa menambah dan mengupdate informasi yang ada pada directory tersebut. LDAP juga sudah dilengkapi SASL (*Simple Authentication and Security Layer*) untuk memeriksa dan memastikan apakah suatu user berhak dan diperbolehkan masuk atau tidak. Karena itulah LDAP juga banyak digunakan untuk '*single sign on'*, yaitu dengan sekali sign-on, user dapat mengakses berbagai aplikasi yang telah disediakan[6].

2. METODE PENELITIAN

Metodologi yang diterapkan dalam penelitian ini adalah metode *Network Development Life Cycle* (NDLC), yang terdiri dari *Analysis, Design, Simulation Prototype, Implementation, Monitoring,* dan *Management*. Metode ini sangat cocok digunakan untuk menganalisis dan merancang penelitian yang bertemakan Jaringan. Kemudian Perspektif partisipan sangat penting untuk dapat memperoleh gambaran dari hasil penelitian yang diinginkan [7].

2.1. Analysis

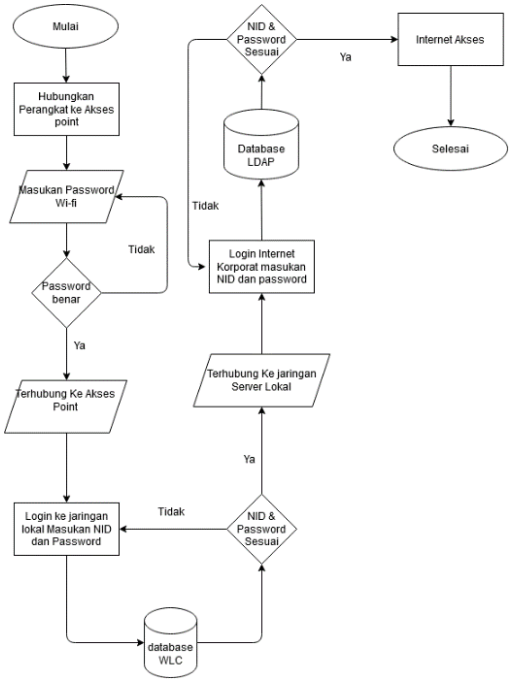
Pada tahap ini dilakukan analisis terhadap perangkat dan sistem yang digunakan pada jaringan saat ini. Analisis dilakukan dengan cara observasi untuk mengumpulkan data-data dan masalah yang dihadapi, dan memberikan usulan pemecahan masalah.

Berdasarkan hasil obeservasi peralatan yang digunakan pada jaringan PT.XYZ ini menggunakan peralatan yang *manageable*, seperti *Switch Cisco Catalyst* 3850 24 *Port* yang digunakan sebagai *Core Switch* dan *Cisco Catalyst* 2960-X *series* digunakan sebagai *Switch client* yang terhubung langsung ke PC *client*.[8]

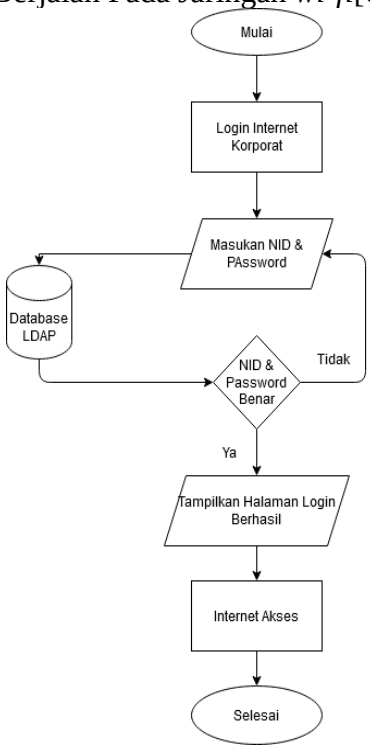
Terakreditasi SINTA 5

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

Adapun Segmentasi IP PT.XYZ menggunakan *VLAN* dan membagi menjadi beberapa *Segment.* Segmentasi ini akan memudahkan dalam epembagian *IP* sesuai kebutuhan masing-masing *IP* yang diperlukan.[9]

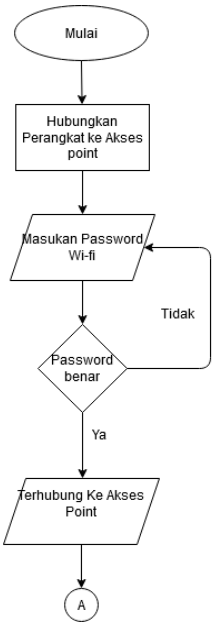


Gambar 1. *Flowchart* Sistem Yang Berjalan Pada Jaringan *wi-fi*[6]

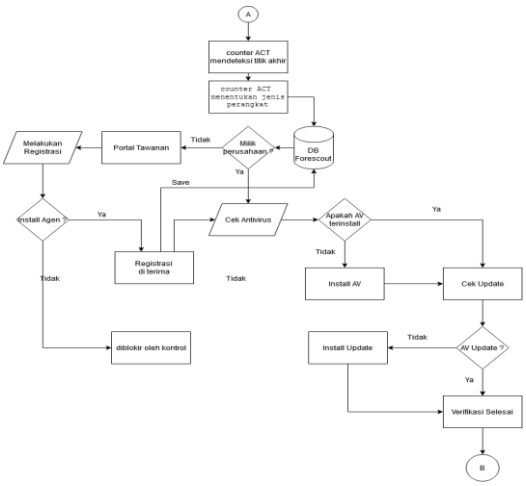


Gambar 2. *Flowchart* Yang Sedang Berjalan Pada Jaringan *Wired* [6]

Sistem yang dikembangkan adalah dengan menggabungkan sistem yang sedang berjalan seperti antivirus, autentikasi dan *host intrusion prevention*, dengan menambah sebuah *Server* baru yang di *install* pada *server VMware vSphere* yaitu *software Forescout.* Penelitian ini ditunjang dengan studi literatur pada jurnal, buku serta menggunakan penelitian terdahulu.[10]

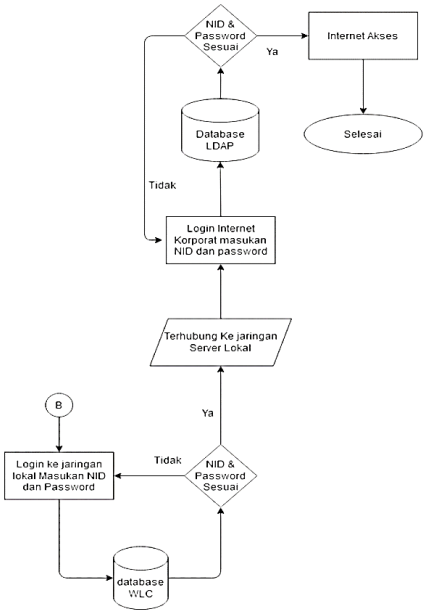


Gambar 3. *Flowchart* Sistem



p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

Gambar 4. *Flowchart* Sistem Yang Akan Dikembangkan [6]



Gambar 5. *Flowchart* Sistem Yang Akan Dikembangkan [5]

Hasil analisis yang dilakukan, sebelum melakukan implementasi ada beberapa *hardware* yang dibutuhkan. Kondisi saat ini di PT. XYZ sudah terpasang *server* HP Gen-9 dan untuk pengembangan yang akan dilakukan penulis hanya akan melakukan *upgrade* pada *server* yang sebelumnya terpasang dengan menambah kapasitas *harddisk*. Pada Tabel I, merupakan daftar kebutuhan *hardware* yang dibutuhkan untuk menjalankan sistem.[3], [11]

TABEL 1. Kebutuhan Perangkat Keras

No	Device	Fungsi	Jml	Keterangan
1	*Server* HP HPE Proliant Dl380 Gen9, *Server Rack-Mountable*, 16 GB Ram	*Server*	1	Sudah terpasang
2	HDD *Server* HPE 300GB 12G SAS 15K 2.5" SC ENT HDD PN 759546-00	Tempat penyimpanan Data/*File* system	4	Pengadaan/pasang baru
3	Kabel *UTP*	Untuk menghubungkan *server* dengan *switch*	2	CAT6 *Flat Ethernet Patch Network LAN Cable* RJ45
4	*Switch* Cisco Catalyst 3850 24 Port	*Terminal* SPAN	2	Sudah terpasang
5	*Switch* Cisco Catalyst 2960-x 24 Port	*Terminal*	25	Sudah terpasang

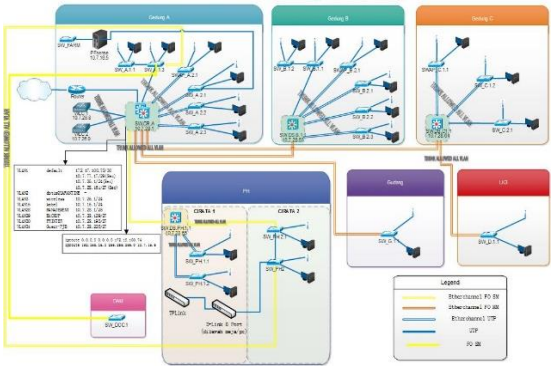
Untuk menjalankan sistem ini dibutuhkan beberapa perangkat lunak (*software*). Tabel II, merupakan kebutuhan *software* yang dibutuhkan sistem.

TABEL 2. Kebutuhan Minimal Perangkat Lunak

No	Nama Software	Jumlah	Keterangan
1	*ESXI 6.0*	1	
2	*VMware vSphere Client 6.0*	1	
3	*Forescout*	1	*Licence* 300 *Device*

2.2. Design

Desain yang dibangun melekat pada desain topologi



Gambar 6. *Logical* Topologi PT XYZ [5]

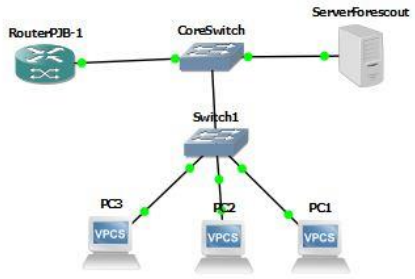
p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

Existing sistem ini berada di dalam *server* rak yang berisi berbagai *server* korporat. Topologi yang dibangun menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain.

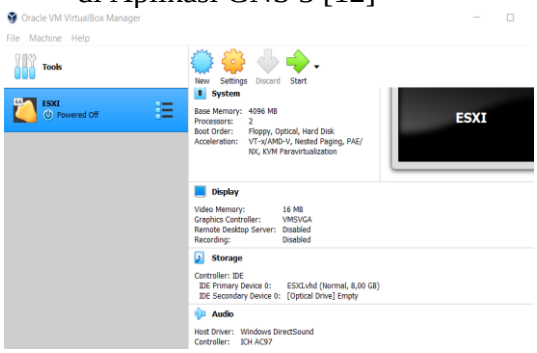
2.3. Simulation Prototype

Alur dari dari sistem topologi yang dibangun dubuat kedalam simulasi menggunakan *software* GNS3 dan *VirtualBox* sebelum melakukan implementasi pada jarinan secara langsung.[10]

Contoh simulasi bisa dilihat pada gambar 7 dan gambar 8.



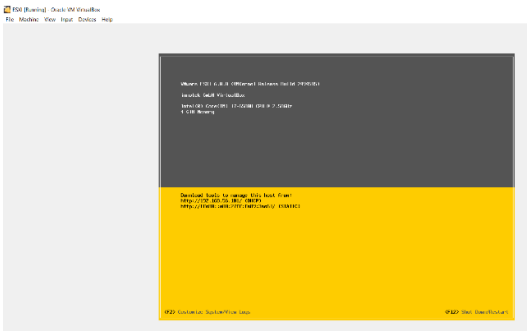
Gambar 7. *Simulation* Prototype di Aplikasi GNS 3 [12]



Gambar 8. *Simulation Prototype* di Aplikasi *Virtualbox* [10]

2.4. Implementation

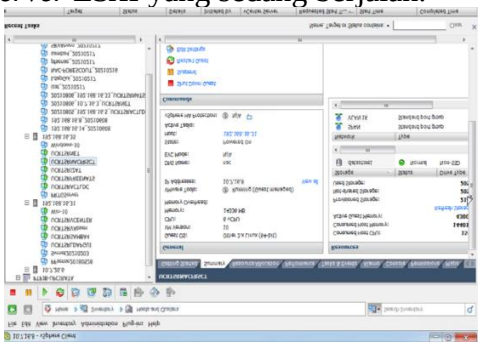
Setelah melakukan analisis dan perancangan, selanjutnya adalah tahap *implementasi*. *Design* yang sebelumnya sudah dirancang akan dijalankan dan dilakukan pengujian. Sebelum melakukan pengujian ada beberapa tahapan yang harus dilakukan.



Gambar 9. Tampilan *Software ESXI* 6.0 [11]

Tahap pertama konfigurasi yang dilakukan pada *ESXI* (*VMware vSphere*) disesuaikan dengan sistem yang dibutuhkan oleh *software* yang akan dijalankan.[10]

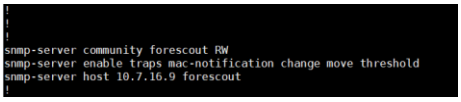
Pada gambar 9 adalah tampilan dari *server ESXI* yang sedang berjalan.



Gambar 10. Tampilan *Software ESXI* dari *VMSphere Client* [11]

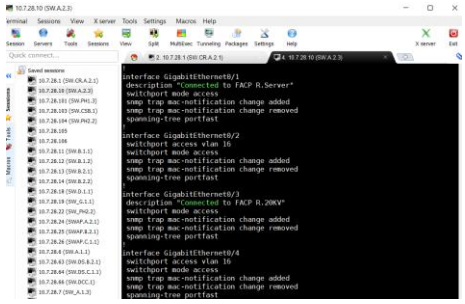
Pada gambar 10 merupakan tampilan dari *VMware vSphere Client* 6.0 yang menampilkan dimana *server forescout* berjalan.

Selanjutnya melakukan konfigurasi pada *core switch* dan *switch client* dengan menambahkan konfigurasi seperti pada gambar 11 untuk *Core Switch* dan gambar 12 untuk *Switch Client*.



Gambar 11. Konfigurasi *SNMP* Pada *Core Switch* [5]

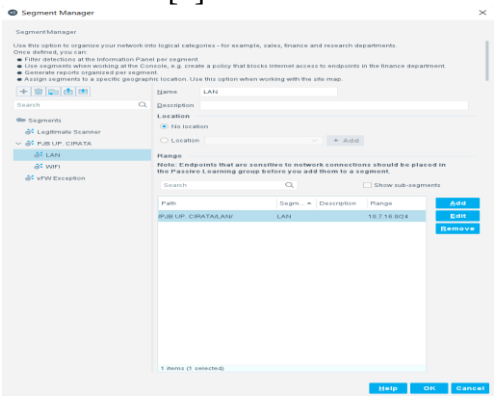
p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom



Gambar 12. Konfigurasi *SNMP* Pada *Switch Client* [5]

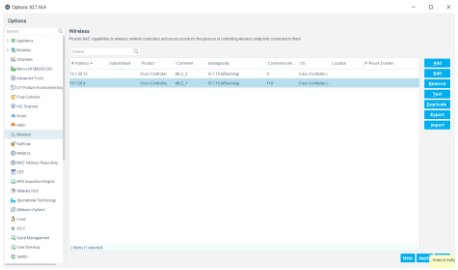
Selanjutnya pada gambar 13 merupakan tampilan login admin untuk memulai konfigurasi pada *software Forescout.*

Gambar 13. Login Admin Panel [4]

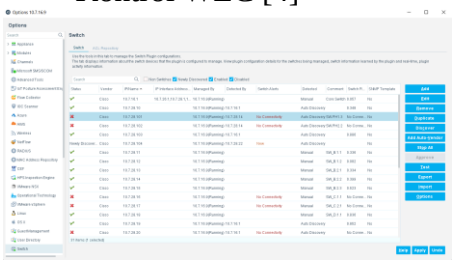


Gambar 14. Menambahkan Segmen Manager [4]

Pada gambar 14 adalah tampilan dimana administrator melakukan penambahan segmen jaringan pada *software forescout.*

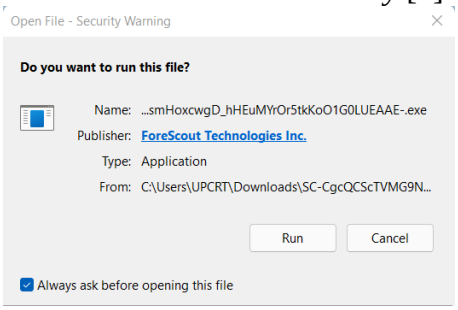


Gambar 15. Menambahkan Kontrol WLC [4]



Gambar 16. Menambahkan IP *Switch* Ke *Forescout* [4]

Gambar 17. Membuat *Policy* [3]



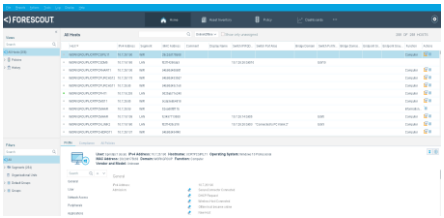
Gambar 18. *Install* SC *Forescout* Pada *PC Client* [4]

2.5. Monitoring

Tahapan monitoring dilakukan setelah semua konfigurasi dilakukan. Melakukan monitoring sekaligus melihat hasil dari konfigurasi yang dibuat apakah sesuai dengan fungsinya atau tidak pada gambar 18 merupakan tampilan depan. Dimana dari tampilan tersebut kita dapat melihat klasifikasi hasil dari *policy* yang diterapkan. [13], [14]

Terakreditasi SINTA 5

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom



Gambar 19. Halaman *Home Admin* [4]

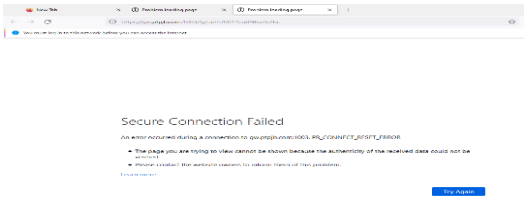
2.6. Management

Pada tahapan *management* yang dilakukan oleh *administrator* adalah menambah atau melakukan pembaruan terhadap *policy* yang dibuat pada saat implementasi. Memantau dan menjaga kondisi sistem beserta jaringan agar tetap dalam konsisi yang aman.

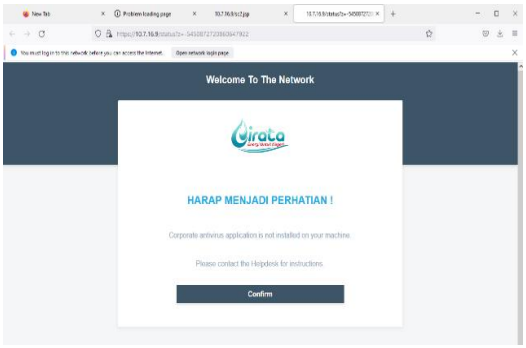
3. HASIL DAN PEMBAHASAN

Pengujian sistem *NAC* ini dilakukan langsung pada komputer client. Pertama dengan cara menyiapkan komputer client tersebut tanpa di *install SC* (*secure connectore)* dimana *SC* ini merupakan syarat pertama yang harus dipenuhi oleh komputer *client*. Apabila komputer *client* ini tidak terinstall *SC* ini maka sistem *forescout* akan

menolak akses pada komputer *client* tersebut, seperti pada gambar 20. [11]



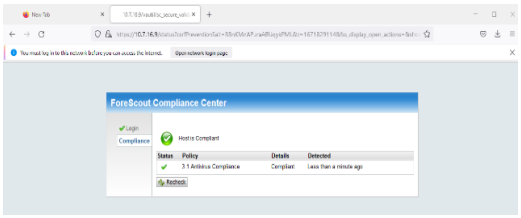
Gambar 20. Pengujian Tanpa Di *Install SC*[4]



Gambar 21. Pengujian pada *Client* Yang Tidak *install Antivirus* [4]

Pada gambar 21 komputer *client* mendapatkan notifikasi dari sistem *NAC forescout* bahwa *client* tersebut tidak terinstall antivirus. Kondisi ini menjadi kondisi kedua yang diterapkan setelah kondisi pertama yang berhubungan dengn *agent* yaitu *secure connectore*.

Pengujian selanjutnya adalah dilakukan pada komputer *client* yang sudah *terinstall SC* dan ter *install* antivirus. Hasilnya pada gambar 22. Komputer yang sudah memenuhi kriteria dinyatakan aman oleh sistem dan mendapatkan izin untuk bergabung ke jaringan *intranet*.

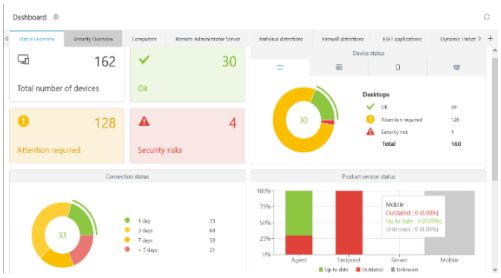


Gambar 22. *Compliance*

Pengujian berikutnya yaitu dilihat dari *dashboard* WEB antivirus korporat dengan melihat jumlah *host* yang sudah *install* antivirus apakah sudah mencapai 100%.

Pada gambar 23 merupakan hasil dari sistem *NAC* yang dibuat dengan jumlah *client* yang tersambung ke jaringan sudah lebih dari 100% ter *install* antivirus. Dari total jumalah karyawan *organik* 139 orang dan *non-organic* 15 orang yang memegang komputer/laptop.

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom



Gambar 23. *Dashboard Antivirus* [4]

4. KESIMPULAN

Dari hasil dan pembahasan maka dapat disimpulkan:

a. Sentralisasi pengamanan jaringan dapat bekerja dengan baik dan memberikan kemudahan kepada *administrator* untuk *management network*.
b. *Device/PC* yang tersambung kejaringan sudah diamankan dengan penerapan *policy*.
c. *Policy* yang dibangun pada *forescout* bekerja dengan baik sehingga semua komputer yang berada dijaringan lebih terjaga dari serangan *attacker*, virus dan *vulnerability.*

5. SARAN

Adapun saran untuk pengembangan kedepannya yaitu:

a. Penelitian kedepannya menambah kombinasi *policy* misalnya *device* korporat tidak di izinkan untuk download menggunakan software downloader dijaringan PT XYZ.
b. kedepannya selain implementasi *NAC* menggunakan *platform forescout* untuk menjaga kestabilan jaringan ditambah dengan implementasi *firewall* dan *Intrusion Prevention System*.[15]

DAFTAR PUSTAKA

[1] W. Jia and W. Zhou, “Distributed Network Systems : From Concepts to Implementations (Network Theory and Applications),” 2005.

[2] Firdaus, E. A., Maulani, S., & Dharmawan, A. B. (2021). Pengukuran Minat Baca Mahasiswa dengan Metode Clustering di Perpustakaan Akademi Keperawatan RS.Dustira Cimahi menggunakan Data Mining. Nuansa Informatika, 32-40.

[3] C. Fisher, “Network Access Control: Disruptive Technology?,” 2007. [Online]. Available: https://epublications.regis.edu/theses

[4] Shesia Rizki Damara, “Analisis dan Implementasi Kontrol Akses Jaringan dan Kebijakan pada PT. Asuransi Jiwa Sinarmas MSIG Tbk Menggunakan Sistem Genian NAC,” *Jurnal Ilmiah Komputasi*, vol. 19, no. 3, Sep. 2020, doi: 10.32409/jikstik.19.3.67.

[5] A. M. Fanggidae, H. Hermawan, and H. I. Pratiwi, “Sistem Monitoring Server Dengan Menggunakan SNMP,” *Widyakala Journal*, vol. 6, no. 2, p. 163, Sep. 2019, doi: 10.36262/widyakala.v6i2.218.

[6] Rudi Candra Satriawan, “PENGEMBANGAN Sistem Autentikasi Single Sign On Menggunakan Protocol Ldap (Lightweight Directory Access Protocol),” 2017.

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

[7] Trianto, W., Firdaus, E. A., & Suburdjati, B. A. (2021). Analisis Sistem Antrian Pendaftaran menggunakan Metode Queuing System di Puskesmas Kota Cimahi. Nuansa Informatika, 64-69.

[8] K. Evan, P. Wiguna, and I. P. Hariyadi, "Otomatisasi Keamanan Router Dan Switch Berbasis Cisco Menggunakan Ansible," 2020.

[9] S. Hidayatulloh, P. M. Ilham, and M. Lase, "Calculation Application for Subnetting IPv4 Address on Android," *Journal Of Informatics And Telecommunication Engineering*, vol. 4, no. 1, pp. 112–118, Jul. 2020, doi: 10.31289/jite.v4i1.3827.

[10] Herdiana, O., Maulani, S., & Firdaus, E. A. (2021). Strategi Pemasaran Produk Industri Kreatif menggunakan Algoritma K-Means Clustering Berbasis Particle Swam Optimization. Nuansa Informatika, 1-13.

[11] S. Varrette, M. Guzek, V. Plugaru, X. Besseron, and P. Bouvry, "HPC performance and energy-efficiency of Xen, KVM and VMware hypervisors," in *Proceedings - Symposium on Computer Architecture and High Performance Computing*, 2013, pp. 89–96. doi: 10.1109/SBAC-PAD.2013.18.

[12] J. C. Neumann, *The book of GNS3 : build virtual network labs using Cisco, Juniper, and more*.

[13] T. Habibullah and D. Arnaldy, "Implementasi Network Monitoring System Nagios dengan Event Handler dan Notifikasi Telegram Messenger," 2016.

[14] M. Syani and B. Saputro, "Mamay Syani, Bayu Saputro Implementasi Remote Monitoring Pada Virtual Private Server Berbasis Telegram Bot API (Studi Kasus Politeknik TEDC Bandung)."

[15] Tati Ernawati and Fikri Faiz Fadhlur Rachmat, "Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, pp. 180–186, Feb. 2021, doi: 10.29207/resti.v5i1.2825.