Penerapan Layanan dan Konfigurasi Perangkat Network Access Control untuk Keamanan Jaringan Pelanggan PT Datacomm Diangraha

1st Tareich Lazuardi Mufti
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
lzlazuardi@student.telkomuniversity.ac.id

2nd Henry Rossi Andrian
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
henryrossiandrian@telkomuniversity.ac.id

3rd Lisda Meisaroh
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
lisdameisaroh@telkomuniversity.ac.id

***Abstrak*— Keamanan jaringan telah menjadi perhatian utama bagi organisasi di era digital ini, dimana ancaman *cyber* semakin kompleks dan beragam. Implementasi *Network Access Control* (NAC) merupakan langkah strategis untuk meningkatkan keamanan jaringan internal pada sebuah organisasi. Tujuan utama dari implementasi NAC ini adalah untuk memastikan bahwa hanya perangkat yang memenuhi syarat dan standar keamanan yang dapat mengakses jaringan internal *customer*, guna mencegah akses tidak sah yang dapat mengancam integritas, kerahasiaan, dan ketersediaan data di dalam jaringan. Selain itu, implementasi NAC juga bertujuan untuk mengontrol dan memonitoring kondisi *user* yang yang mengakses jaringan internal perusahaan. Hasil dari implementasi dan pengujian ini diharapkan dapat memberikan kontribusi yang signifikan dalam meningkatkan keamanan dan stabilitas jaringan internal *customer*.**

Kata kunci*— *Network Access Control (NAC), Policy, Network Security

I. PENDAHULUAN

A. Latar Belakang

Dalam era digital yang berkembang pesat saat ini, perkembangan teknologi informasi telah menjadi salah satu pilar utama dalam mendukung berbagai aspek kehidupan sehari-hari. Namun, seiring dengan kemajuan tersebut, muncul pula tantangan baru seperti dalam hal keamanan *cyber*. Kejahatan *cyber* semakin canggih dan merugikan, mengancam setiap individu dan perusahaan yang mengandalkan teknologi informasi. Menyadari pentingnya perlindungan terhadap keamanan jaringan di tengah maraknya ancaman *cyber*, PT Datacomm hadir sebagai solusi terpercaya. Perusahaan ini menawarkan layanan keamanan jaringan yang komprehensif untuk membantu individu dan perusahaan melindungi aset digital mereka dari berbagai ancaman *cyber*.

Keamanan jaringan memiliki definisi yaitu tindakan untuk mengamankan serta mengurangi resiko gangguan terhadap *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan)[1]. Dalam laporan ini,berfokus pada aspek *integrity* yaitu dengan menerapan *network access control* (NAC) untuk memastikan bahwa data dan *resource network* pelanggan PT Datacomm hanya digunakan oleh pengguna yang sah dan hanya perangkat yang memenuhi kebijakan keamanan yang diizinkan untuk mengakses jaringan.

Penerapan NAC menjadi penting bagi *customer* PT Datacomm karena dapat memberikan kontrol dan visibilitas yang lebih baik terhadap perangkat yang terhubung ke jaringan. Dengan NAC, dapat memastikan bahwa hanya perangkat yang sesuai dengan standar keamanan yang dapat mengakses jaringan, sehingga dapat mengurangi risiko intrusi dan kebocoran data. Selain itu, NAC juga dapat membantu dalam memantau aktivitas perangkat di dalam jaringan dan melakukan tindakan perbaikan atau mitigasi jika terjadi potensi ancaman

B. Rumusan Masalah

Untuk implementasi *Network Access Control* (NAC), teknologi atau *software* yang akan digunakan adalah Forescout NAC, yang berbasis Virtual *CounterACT Enterprise Manager* (VCEM). Agar dapat mengakses jaringan, pengguna atau perangkat harus mematuhi kebijakan keamanan yang berlaku di Perusahaan *customers* PT Datacomm. Perangkat tersebut harus sesuai dengan standar perusahaan, yaitu sudah ter-*install agent* secure connector, antivirus (AV), dan NetBIOS domain yang sesuai dengan kebijakan yang berlaku.

Dengan menggunakan ForescoutNAC sebagai solusi implementasi *network access control*, diharapkan dapat memastikan hanya perangkat yang memenuhi persyaratan keamanan yang dapat terhubung ke jaringan perusahaan[2]. Hal ini bertujuan untuk meningkatkan keamanan jaringan dan melindungi aset-aset kritis perusahaan *customers* PT Datacomm.

C. Tujuan

Tujuan yang akan dicapai diantaranya sebagai berikut:

1. Memastikan hanya perangkat yang memenuhi syarat yang dapat mengakses jaringan internal *customer*.

2. Memberi visibilitas *agar dapat Memonitoring user-user* yang mengakses jaringan internal *customer*.

II. KAJIAN TEORI

A. *Network Access Control*

Network Access Control (NAC) merupakan salah satu pendekatan keamanan jaringan yang semakin banyak diadopsi oleh organisasi saat ini. NAC adalah teknologi keamanan jaringan yang memungkinkan *administrator* jaringan mengontrol dan mengamankan akses ke jaringan berdasarkan faktor-faktor seperti peran pengguna, lokasi, waktu, dan kepatuhan perangkat. NAC memberikan pengendalian akses yang lebih rinci dan lebih efektif, memungkinkan pengaturan *policy* akses yang lebih tepat dan meminimalkan risiko akses yang tidak sah atau tidak terotorisasi[3].

Meskipun demikian, seperti setiap solusi teknologi, NAC juga memiliki kelebihan dan kekurangan seperti berikut.

Kelebihan NAC:

1. NAC memberikan pengendalian akses yang lebih terperinci dan lebih efektif[4].
2. NAC memungkinkan pengaturan kebijakan akses yang lebih tepat dan meminimalkan risiko akses yang tidak sah atau tidak terotorisasi[4].

Kekurangan NAC:

1. Implementasi NAC dapat menjadi proses yang kompleks dan memerlukan perencanaan yang matang.
2. Implementasi NAC dapat melibatkan biaya yang signifikan untuk infrastruktur, perangkat lunak, dan personel yang dibutuhkan.

B. Keamanan *Cyber*

Keamanan *cyber* mengandalkan prinsip *Confidentiality, Integrity*, dan *Availability* (CIA Triad) untuk melindungi informasi dan sistem[1]. *Confidentiality* memastikan bahwa data hanya dapat diakses oleh pihak berwenang melalui enkripsi dan kontrol akses yang ketat. *Integrity* menjaga keabsahan dan keakuratan data dengan menggunakan *hashing* dan digital *signatures*. *Availability* memastikan sumber daya jaringan selalu dapat diakses dengan menggunakan redundansi dan perlindungan terhadap serangan *denial-of-service* (DoS)[1].

C. Autentikasi

Autentikasi adalah proses verifikasi identitas pengguna atau perangkat sebelum memberikan akses ke sistem atau data, menjadi langkah pertama dan penting dalam menjaga keamanan informasi. Metode autentikasi mencakup faktor pengetahuan (kata sandi atau PIN), faktor kepemilikan (token fisik seperti kartu pintar atau perangkat autentikasi berbasis hardware), dan faktor inheren (karakteristik biometrik seperti sidik jari, retina mata, atau wajah). Multi-factor Authentication (MFA) meningkatkan keamanan dengan menggabungkan dua atau lebih faktor dari kategori yang berbeda. Protokol seperti Kerberos, RADIUS, OAuth, dan SAML digunakan untuk mengelola dan memfasilitasi proses autentikasi dalam berbagai konteks jaringan dan aplikasi[5].

Autentikasi memberikan manfaat signifikan dengan memastikan hanya pengguna yang sah dapat mengakses sistem, mengurangi risiko akses tidak sah, dan memungkinkan pelacakan aktivitas pengguna[5]. Namun, tantangan yang dihadapi termasuk manajemen kompleks kata sandi, risiko keamanan terkait dengan biometrik, dan kebutuhan perangkat keras khusus untuk beberapa metode.

D. Virtual *Machine*

Virtual *Machine* (VM) adalah entitas yang memungkinkan perangkat keras fisik menjalankan beberapa sistem operasi sekaligus melalui *hypervisor* atau virtual *machine monitor* (VMM), yang menciptakan dan mengelola VM dengan membagi sumber daya fisik. *Hypervisor* terbagi menjadi Type 1 (*Bare Metal*), seperti VMware ESXi, dan Type 2 (*Hosted*), seperti Oracle VirtualBox[8]. VM meningkatkan efisiensi sumber daya, isolasi lingkungan, dan fleksibilitas pengelolaan sistem [9], memungkinkan beberapa VM berjalan terpisah satu sama lain di satu perangkat keras fisik.

III. METODE

Skenario pengujian *policy* NAC dilakukan untuk memastikan bahwa *policy* tersebut berfungsi dengan benar dan sesuai dengan spesifikasi yang ditetapkan. Tujuan dari skenario pengujian ini adalah untuk mengidentifikasi apakah *policy* NAC dapat diterapkan dengan efektif dan memberikan perlindungan jaringan yang sesuai.

Metode pengujian yang akan digunakan adalah sebagai berikut:

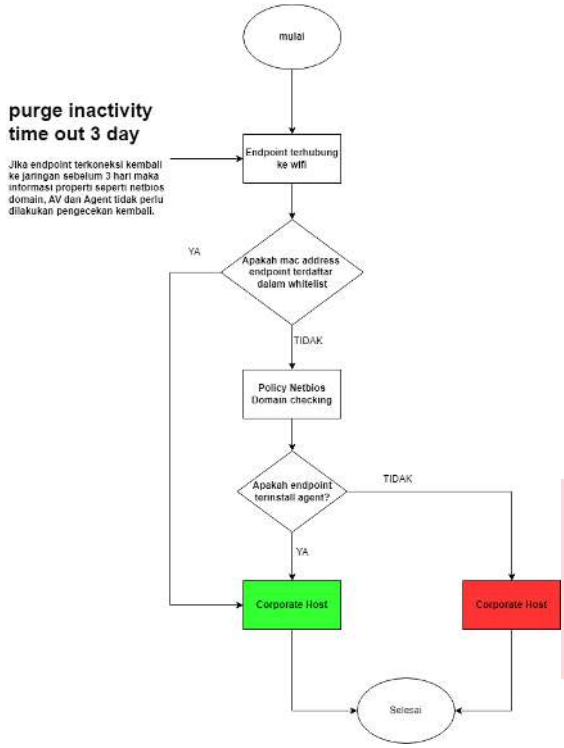
1. Beberapa laptop Windows dengan konfigurasi yang berbeda-beda akan digunakan dalam pengujian. Variasi konfigurasi laptop ini penting untuk menguji skenario yang lebih komprehensif, memastikan *policy* NAC dapat bekerja dengan baik pada berbagai jenis perangkat.
2. Laptop-laptop tersebut akan dihubungkan ke jaringan WiFi. Tim penguji akan mengamati dan mencatat bagaimana akses jaringan pada masing-masing laptop, termasuk apakah *policy* NAC dapat mengenali dan memberlakukan aturan akses yang sesuai.

Hasil pengujian yang diperoleh, baik berupa catatan observasi maupun data-data lain yang relevan, akan dicatat dengan seksama. Tim akan melakukan analisis mendalam terhadap data-data tersebut untuk memastikan bahwa *policy* NAC benar-benar bekerja sesuai dengan yang diharapkan.

IV. HASIL DAN PEMBAHASAN

A. Analisis Sistem

1. Gambaran Sistem Saat In



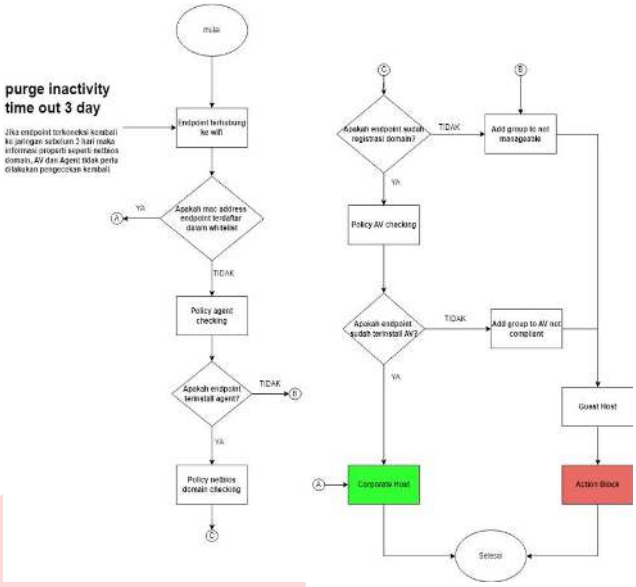
GAMBAR 1
Sistem Saat Ini

Berdasarkan sistem saat ini, *requirement* suatu *endpoint* dapat terkoneksi atau dapat mengakses jaringan *customer* yaitu dengan *policy* yang alurnya seperti berikut. Ketika *endpoint* terhubung ke WiFi, Forescout akan melakukan pengecekan apakah MAC address *endpoint* tersebut terdaftar dalam daftar *host corporate*. Jika iya, maka *endpoint* akan tetap dapat terhubung ke WiFi. Namun, jika tidak, maka *endpoint* tersebut akan melanjutkan ke pengecekan berikutnya, yaitu pengecekan NetBIOS domain. Dalam pengecekan NetBIOS domain, hanya *endpoint* dengan NetBIOS domain pelanggan Datacomm yang dapat terhubung ke WiFi.

2. Pengembangan Sistem

Pada sistem yang sebelumnya terdapat kelemahan atau isu, yaitu dalam beberapa kasus Forescout gagal untuk mendeteksi NetBIOS domain dari *endpoint*. Yang mana kasus tersebut menghambat pekerjaan user yang *device*-nya sudah memenuhi syarat namun terblokir karena Forescout gagal dalam mendeteksi informasi *endpoint*.

Maka dari itu, penulis menambahkan dua proses pengecekan pada Forescout yaitu pengecekan *agent* Secure Connector dan pengecekan Antivirus (AV). *Agent* Secure Connector pada pengembangan sistem ini adalah point utama agar memudahkan visibilitas dari Forescout dan wajib ter-*install* untuk semua *endpoint*. Dengan menambahkan pengecekan *Agent* Secure Connector, dapat membantu Forescout dalam mendeteksi informasi *endpoint* seperti NetBIOS domain dan mempercepat proses pengecekan. Selain itu, penambahan proses pengecekan Antivirus (AV) dapat menaikan tingkat keamanan sehingga proteksi bukan hanya di infra IT perusahaan.



GAMBAR 2
Pengembangan Sistem

B. Skenario Pengujian

Untuk memastikan keefektifan NAC, tim pengujian akan mengevaluasi berbagai konfigurasi perangkat dalam setiap skenario pengujian. Tabel berikut menyajikan rincian konfigurasi perangkat yang akan diuji pada masing-masing skenario:

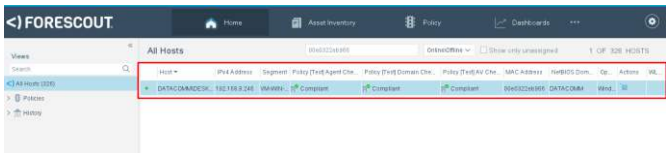
TABEL 1
Skenario Pengujian Sistem

Sequence Test	*End Point Type*	*Type Product*	*Compliance Expectation*	*AV Product*	*MAC Address Exception*	*Expectation Result*
1	*Laptop Corporate*	*Windows*	*Agent SC, Netbios, & AV*	*Avira & Windows Defender*	*no*	*All compliance passed. OK*
2	*Laptop Corporate*	*Windows*	*Agent SC, Netbios, & AV*	*Windows Defender*	*no*	*All compliance passed. OK*
3	*Laptop Corporate*	*Windows*	*Agent SC & AV*	*Avira & Windows Defender*	*yes*	*registered MAC address. Passed. OK*
4	*Laptop Guest*	*Windows*		*Windows Defender*	*no*	*Not comply, Blocked (Expected)*
5	*Laptop Guest*	*Windows*	*AV*	*Avira*	*no*	*SC & Netbios not comply, Blocked (Expected)*
6	*Laptop Guest*	*Windows*	*AV & Netbios*	*Windows Defender*	*no*	*Agent not comply Blocked (Expected)*

C. Hasil Pengujian

Untuk menganalisis kinerja dan kemampuan Forescout dalam menjalankan fungsi NAC, kami telah melakukan sejumlah pengujian. Dibawah ini menggambarkan hasil pengujian dan berisi *capture* sebagai *evidence* dari pengujian:

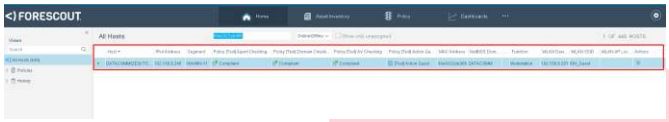
1. Skema pengujian 1



GAMBAR 3
Forescout Console Skema 1

Pada gambar 3, terlihat *endpoint* yang terdeteksi di console Forescout sudah *comply* baik *agent* secure connector, NetBIOS domain, dan juga AV (antivirus). Sehingga, *endpoint* tersebut tidak *terblock* oleh NAC.

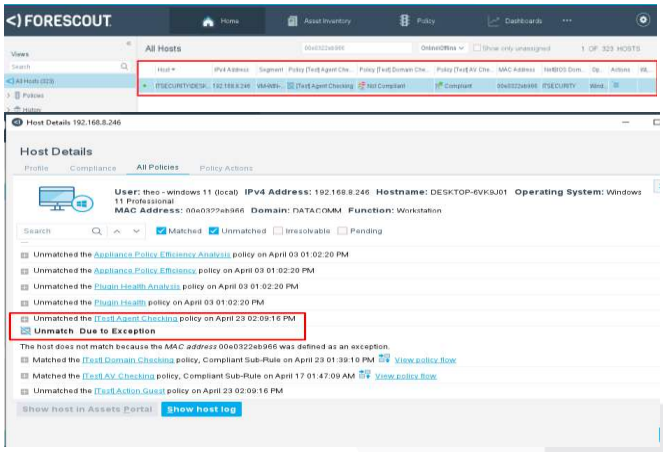
2. Skema pengujian 2



GAMBAR 4
Forescout Console Skema 2

Pada gambar 4, menunjukan *endpoint* yang terdeteksi di console Forescout sudah *comply* di semua *policy* NAC yang berlaku, sehingga tidak ada *block* kepada *endpoint* tersebut.

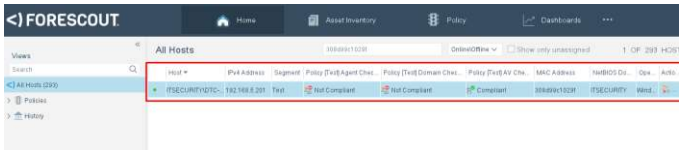
3. Skema pengujian 3



GAMBAR 5
Forescout Console Skema 3

Pada gambar 5, terlihat *endpoint* yang hanya kompatibel dengan antivirus saja, namun *mac dddress endpoint* tersebut ada dalam daftar pengecualian dengan keterangan "*unmatch due exception*", sehingga tidak diblokir oleh NAC.

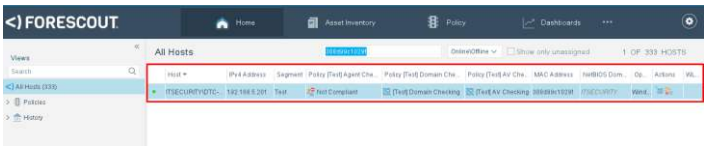
4. Skema pengujian 4



GAMBAR 6
Forescout Console Skema 4

Pada gambar 6, terlihat *endpoint* yang terdeteksi di Console Forescout tidak *comply* dengan *policy agent* Secure Connetor dan NetBIOS domain, sehingga diblokir oleh NAC.

5. Skema pengujian 5



GAMBAR 7
Forescout Console Skema 5

Pada gambar 7, terlihat *endpoint* yang terdeteksi pada Forescout console tidak *comply* dengan semua *policy* yang berlaku.

6. Skema pengujian 6

GAMBAR 8
Forescout Console Skema 6

Pada gambar 8, terlihat *endpoint* yang terdeteksi di console Forescout tidak *comply* pada *policy agent* secure connector sehingga *endpoint* tersebut terblokir.

D. Analisis Hasil Pengujian

Dari hasil pengujian, penulis mengidentifikasi beberapa temuan penting:

1. Keberhasilan *Blocking*
   Kebijakan NAC yang dikonfigurasi oleh penulis telah berhasil diterapkan dengan Forescout. Perangkat *non-compliant* dapat diblokir dan dibatasi aksesnya ke jaringan sesuai dengan *policy* yang ditetapkan.

2. Masalah dengan Metode *Blocking*
   Meskipun kebijakan NAC secara keseluruhan berhasil diterapkan, penulis mengalami masalah dengan tindakan pemblokiran (blocking) pada beberapa perangkat. Hal ini disebabkan oleh keterbatasan integrasi antara Forescout dan switch jaringan yang digunakan.

3. Keterbatasan Integrasi dengan *Switch*
   Penulis menemukan keterbatasan yaitu beberapa *switch* yang digunakan kurang didukung atau memiliki versi yang sudah *out of date* dan juga memiliki kendala *level* akses Forescout terhadap *switch* hanya sampai *read only*. Hal ini menyebabkan metode *WLAN block* yang digunakan oleh Forescout tidak dapat berjalan dengan baik.

4. Penggunaan Secure Connector
   Untuk mengatasi keterbatasan integrasi dengan *switch*, penulis memiliki metode alternatif dengan memanfaatkan

Secure Connector. Secure Connector memungkinkan Forescout untuk memerintahkan tindakan pemblokiran secara langsung ke perangkat *user* yang telah ter-*install* Secure Connector dengan menjalankan *script* berisi perintah pada sistem komputer.

V. KESIMPULAN

Berdasarkan hasil pengujian dan analisis, dapat disimpulkan bahwa implementasi *Network Access Control* (NAC) menggunakan Forescout telah mencapai sebagian besar tujuan yang diharapkan, yaitu:

1. Forescout telah mampu memastikan hanya perangkat yang memenuhi syarat yang dapat mengakses jaringan *internal customer*. *Policy* NAC yang dikembangkan berhasil diterapkan untuk mengidentifikasi dan memblokir perangkat yang tidak sesuai dengan standar yang ditetapkan.
2. Forescout NAC dapat memberikan visibilitas guna memonitoring *user-user* yang mengakses ke jaringan internal customer. Visibilitas yang mampu diberikan seperti NetBIOS domain, antivirus, *hostname*, dan Secure Connector.

Meskipun demikian, terdapat beberapa kendala terkait integrasi Forescout dengan perangkat *switch* jaringan yang digunakan, yang menyebabkan keterbatasan dalam metode pemblokiran yang dapat diterapkan.

REFERENSI

[1] Hafid Muhammad(1), Firjatullah Favian Zhuhri (2), and Pamungkaz Billyco Windy (3), “View of Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara,” JurnalPendidikan Tambusai. Accessed: Feb. 18, 2024. [Online]. Available: https://www.jptam.org/index.php/jptam/article/view/7858/6459

[2] A. Lakbabi, G. Orhanou, and S. El Hajji, “Network Access Control Technology—Proposition to Contain New Security Challenges,” *International Journal of Communications, Network and System Sciences*, vol. 05, no. 08, pp. 505–512, 2012, doi: 10.4236/ijcns.2012.58061.

[3] “What Is Network Access Control?”, Accessed: Jul. 02, 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

[4] Fortinet, “What Is Network Access Control (NAC)? ”.

[5] Wahyu Pratama Rifky, “IMPLEMENTASISISTEMAUTENTIKASIUSERMENGGUNAKANRADIUSSERVERDANACTIVEDIRECTORY,” *ressearchgate*, 2019.