IMPLEMENTASI NETWORK ACCESS CONTROL MENGGUNAKAN PLATFORM FORESCOUT DI PT. XYZ

Muhamad Hadi Arfian.
Fakultas Ilmu Komputer Universitas Esa Unggul, Jakarta
Jalan Arjuna Utara No 9 Kebon Jeruk Jakarta 11510
muhamad.arfian@esaunggul.ac.id

Abstrak

Network technology is a system created to make it easier for humans to connect with each other. In the current era of globalization, the network system is a very vital asset that needs to be protected. All information in this case is company data, can be accessed easily through a network system. This study aims to assist companies in securing their network systems. Building Network Access Control (NAC) using a forescout platform will make it easier for a network administrator to control and monitor network conditions at PT. XYZ easily. The policy feature on this forescout platform combines various conditions for network security such as sorting the types of devices connected to the network system, forcibly closing applications that are included in the blacklist, turning on inactive antivirus and so on. System testing got good results in the form of forcibly closing applications that were included in the blacklist. The author uses the Network Development Life Cycle (NDLC) method through several stages, namely Analysis, Design, Simulation, Implementation, Monitoring and Management.

Keywords: NAC, Forescout, NDLC

Abstrak

Teknologi jaringan adalah sebuah sistem yang dibuat untuk memudahkan manusia untuk terhubung satu sama lain. Pada era globalisasi saat ini sistem jaringan merupakan sebuah aset yang sangat vital yang perlu dilindungi. Semua informasi dalam hal ini adalah data perusahaan, dapat diakses dengan mudah melalui sistem jaringan. Penelitian ini bertujuan untuk membantu perusahaan dalam mengamankan sistem jaringannya. Membangun *Network Access Control* (NAC) dengan menggunakan *platform* forescout akan memudahkan seorang *network 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 menyortir jenis perangkat yang terhubung ke sistem jaringan, menutup paksa aplikasi yang termasuk didalam *blacklist*, menghidupkan antivirus yang tidak aktif dan sebagainya. Pengujian sistem mendapat hasil yang bagus berupa ditutupnya secara paksa aplikasi yang termasuk didalam *blacklist*. Penulis menggunakan metode *Network Development Life Cycle* (NDLC) melalui beberapa tahapan yakni *Analysis, Design, Simulation, Implementation, Monitoring dan Management*.

Kata Kunci: NAC, *Forescout*, NDLC

Pendahuluan

PT. XYZ sebagai salah satu perusahaan yang terpercaya di Indonesia terus meningkatkan pelayanan dan pengembangan fasilitas teknologi informasi untuk menunjang setiap proses bisnis di lingkungan perusahaan. PT. XYZ berlokasi di Jl. Asia Afrika, Kecamatan Tanah Abang, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta Kode Pos 10270 dengan jumlah karyawan kurang lebih 250 orang yang bekerja dengan sistem *hybrid working*.

Seiring berkembangnya perusahaan maka bertambah pula jumlah *endpoint* di jaringan perusahaan. Kontrol dan pengidentifikasian terhadap pengguna, perangkat dan aktivitas yang ada di dalam jaringan perusahaan menjadi sulit dilakukan oleh *network administrator*. Sehingga tidak menutup kemungkinan akan ada aktivitas - aktivitas yang dapat mengganggu, mengambil, bahkan merusak data dan infrastruktur jaringan PT. XYZ.

Dengan adanya *Network Access Control*, user yang terkoneksi ke jaringan PT. XYZ akan menjadi terkontrol dan lebih aman, selain itu akan memudahkan bagi *network administrator* dalam melakukan *monitoring*, serta investigasi ketika terjadi hal-hal yang tidak wajar yang diakibatkan oleh perangkat user. selain itu, *network administrator* juga diberikan keamanan *endpoint* yang lengkap dan memungkinkannya dengan mudah menerapkan kebijakan keamanan bisnis ke infrastruktur teknologi informasi secara akurat dan otomatis.

Selain hal-hal yang disebutkan diatas, secara efektif *Network Access Control* juga dapat memerangi *worm, malware dan hacker*. Kemudian ia secara otomatis melindungi *vulnerability* jaringan dan membuat *virtual firewall* yang melindungi atau membuka zona jaringan tertentu. Terakhir, fitur *Network Access Control* memungkinkan tim *IT Security*, *IT Department*, dan *Help Desk* untuk memanfaatkan informasi jaringan yang luas melalui portal aset berbasis web.

Network Access Control

Network Access Control (NAC) adalah konsep pengendalian akses ke lingkungan melalui kepatuhan ketat dan implementasi kebijakan keamanan.
Tujuan digunakannya NAC adalah sebagai berikut:

- Mencegah/mengurangi serangan *zero-day*
- Menerapkan kebijakan keamanan di seluruh jaringan
- Menggunakan identitas untuk melakukan kontrol akses

Tujuan tersebut di atas dapat dicapai melalui penggunaan kebijakan keamanan terperinci yang kuat yang mendefinisikan semua aspek kontrol keamanan, penyaringan, pencegahan, deteksi, dan respon untuk setiap perangkat dari klien ke server dan untuk setiap komunikasi internal atau eksternal. NAC bertindak sebagai sistem deteksi dan respon otomatis yang dapat bereaksi secara real time untuk menghentikan ancaman saat terjadi dan sebelum menyebabkan kerusakan atau pelanggaran.
NAC dapat diimplementasikan dengan filosofi *pre-admission* atau filosofi *post-admission*, atau aspek dari keduanya. Filosofi *pre-admission* membutuhkan sistem untuk memenuhi semua persyaratan keamanan saat ini (seperti aplikasi patch dan pembaruan antivirus) sebelum diizinkan untuk berkomunikasi dengan jaringan. Filosofi *post-admission* memungkinkan dan menolak akses berdasarkan aktivitas pengguna, yang didasarkan pada matriks otorisasi yang telah ditentukan (Chapple et al., 2018)

Policy

Policy atau kebijakan menetapkan pedoman tentang bagaimana jaringan akan beroperasi dengan mempertimbangkan konfigurasinya. Kebijakan juga membuat aturan tentang bagaimana pengguna jaringan harus mengoperasikannya. Kebijakan menentukan hal-hal seperti alokasi sumber daya pada jaringan dan hak istimewa jaringan. Kebijakan memberikan pedoman tentang bagaimana melakukan sesuatu (Schmidt, 2018).
Berikut ini adalah beberapa skenario di mana kebijakan diimplementasikan:

- Menjaga dan membatasi individu yang memiliki akses ke jaringan dan sumber daya jaringan
- Mengawasi sumber daya jaringan
- Menggunakan peralatan atau perangkat elektronik (laptop, PC dan lain-lain) milik perusahaan dengan tanggung jawab
- Menerapkan protokol keamanan
- Melakukan pencadangan (*Backups*) secara berkala

Forescout

ForeScout Technologies adalah perusahaan swasta yang berbasis di Campbell, California, yang menjual perangkat keras dan peralatan virtual dari keluarga CounterACT. Meskipun ForeScout menawarkan *agent* opsional, pendekatan tanpa *client* 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 (Damara, 2020).

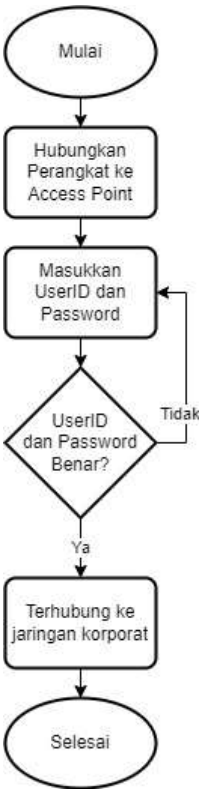
Metode Penelitian

Metodologi yang diterapkan dalam penelitian ini adalah metode Network Development Life Cycle (NDLC), yang terdiri dari *Analysis, Design, Simulation Prototype, Implementation, Monitoring, dan Management* (Mamay et al., 2022).

Analysis

Pada tahap ini dilakukan analisis terhadap perangkat dan sistem yang berjalan pada jaringan PT. XYZ. Analisis dilakukan dengan cara observasi untuk mengumpulkan data-data dan masalah yang dihadapi, dan memberikan usulan pemecahan masalah. Berdasarkan hasil observasi peralatan yang digunakan pada jaringan PT.XYZ ini menggunakan *switch* yang *manageable* di bagian *core maupun distribution* juga terdapat *access switch* dengan berbagai tipe yang terhubung langsung ke komputer user.

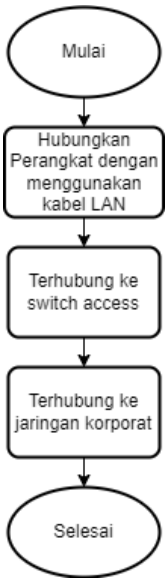
Untuk perangkat *wireless* LAN, PT. XYZ menggunakan access point dari Arubanetworks yang dikontrol menggunakan *Wireless* LAN *Controller*. Adapun Segmentasi IP PT.XYZ menggunakan VLAN dan membagi jaringan menjadi beberapa Segment.



Gambar 1

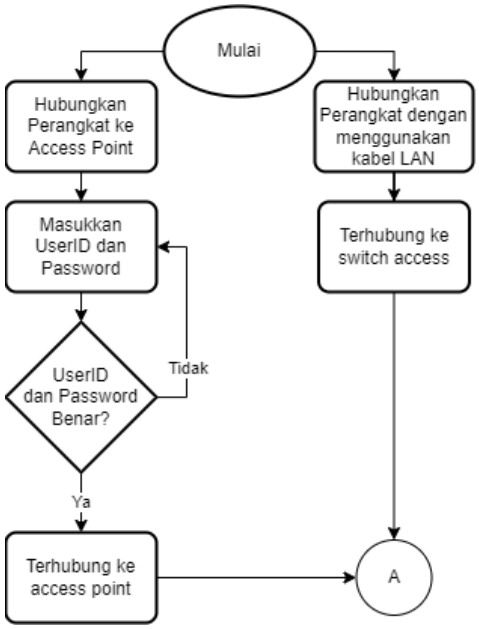
Flowchart koneksi *wireless* pada sistem berjalan

Gambar 1 menunjukan proses ketika seorang user di PT. XYZ ingin menghubungkan perangkat komputernya kedalam jaringan korporat melalui jalur nirkabel *(wireless).* User tersebut setelah memilih SSID *(Service Set Identifier) access point* maka diharuskan memasukkan user ID dan *password*. Jika user ID yang dimasukkan salah, maka harus mengulangi kembali. Jika user ID yang dimasukkan benar, maka user tersebut akan terhubung ke jaringan korporat. Hal yang berbeda dilakukan ketika user tersebut ingin menghubungkan ke jaringan korporat dengan menggunakan kabel LAN. Proses menghubungkan perangkat ke jaringan korporat PT. XYZ melalui jalur kabel bisa dilihat di gambar 2.

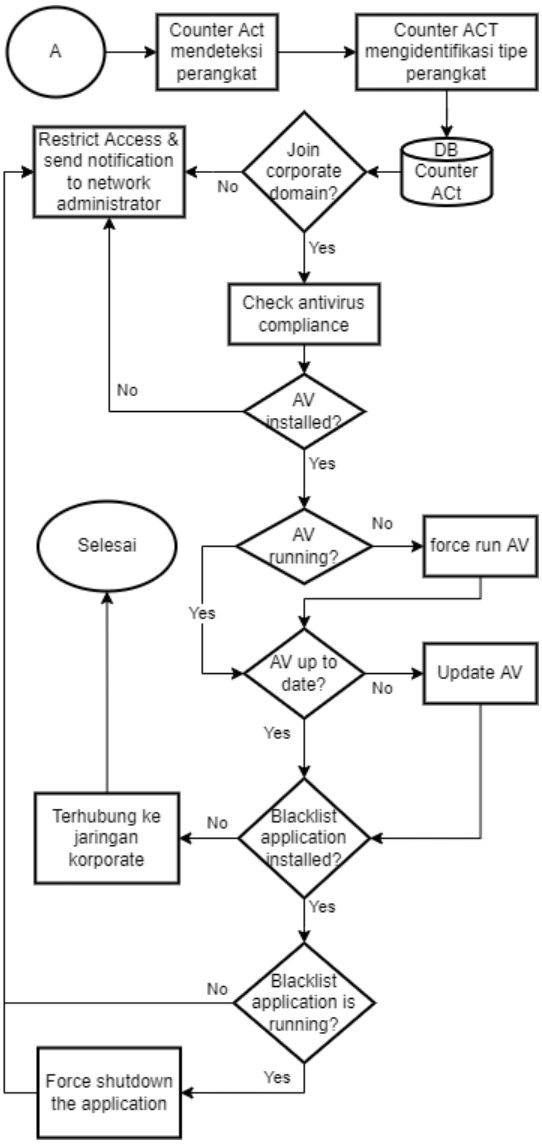


Gambar 2
Flowchart koneksi *wired* pada system berjalan

Sistem yang dikembangkan oleh penulis adalah dengan menambah sebuah server baru yang di install pada server VMware vSphere client yaitu software Forescout yang akan menjadi *inspector* terhadap proses koneksi perangkat ke jaringan korporat perusahaan. Jadi setelah perangkat user terkoneksi ke *access point* atau *switch*, maka Forescout akan langsung melakukan *discovery* terhadap perangkat tersebut seperti yang terlihat di gambar 3 dan 4.



Gambar 3
Flowchart system yang akan dikembangkan (1)



Gambar 4
Flowchart system yang akan dikembangkan (2)

Pada penelitian ini, solusi NAC yang digunakan adalah Forescout *virtual appliance* yang akan diinstal di atas *virtual machine*. Dibawah ini adalah persyaratan *virtual machine* yang dibutuhkan untuk menginstall forescout *software.*

Tabel 1
Tabel Spesifikasi kebutuhan VM

Memory	**CPU**	***Storage***	***OS & Other***
14 GB	6 vCPU	200 GB	Forescout installer comes with pre-hardened OS (LINUX, CentOS 7, 64 bit)

Berikut ini adalah beberapa hardware yang dibutuhkan. Kondisi terkini di PT. XYZ sudah terpasang *VMware HCI infrastructure, core switch, distribution switch, access point,* WLC dan juga *access switch* dengan tertata rapih dalam sebuah rak di ruang *data center*. Untuk itu penulis hanya akan melakukan installasi Forescout CounterACT *virtual appliance* pada VMware dan memasangkan 1

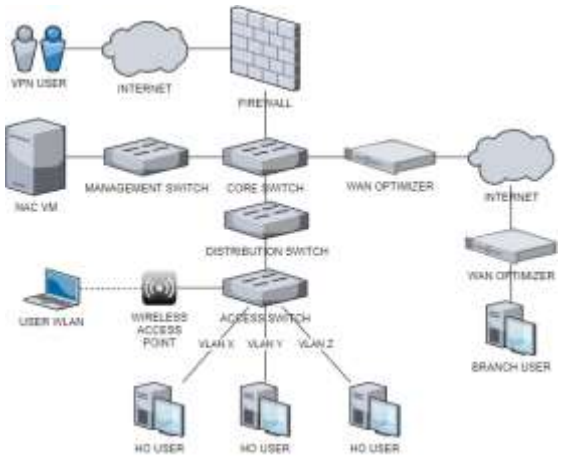
kabel UTP untuk dihubungkan ke laptop melalui *switch access*. Pada Tabel 2, merupakan daftar kebutuhan *hardware* yang dibutuhkan untuk menjalankan sistem.

Tabel 2
Tabel perangkat keras

No	Device	Fungsi	Jml	Ket
1	Cisco WS-C3850-48T-L	Core Switch	2	Sudah terpasang
2	Cisco WS-C3650-48TS-L	Distribution Swtich	2	Sudah terpasang
3	HP Procurve 2626-48	Access Switch	20	Sudah terpasang
4	Kabel UTP	Media koneksi dari switch ke perangkat	1 (dari port switch ke 1 laptop test)	CAT6 Flat Ethernet Patch Network LAN Cable RJ45
5	Aruba APIN0205	Access Point	15	Sudah terpasang
6	Aruba AC 7010	Wireless Lan Controller	1	Sudah terpasang
7	Laptop Dell 3400	Computer User	1	Sudah terintall OS windows

Design

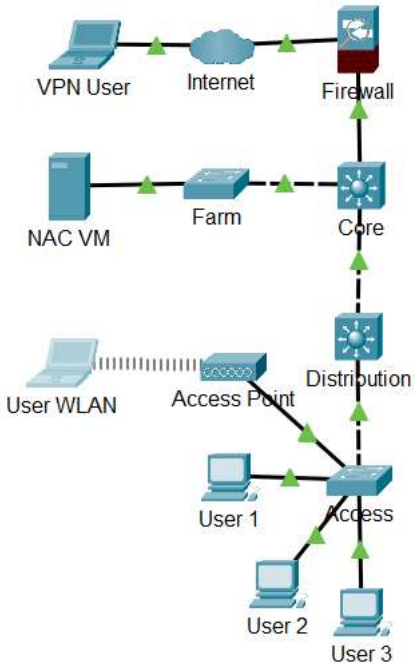
Desain yang dibangun melekat pada desain topologi PT. YXZ. *Existing* sistem ini berada di dalam data center yang di dalamnya terdapat server rak yang berisi berbagai server korporat. Topologi yang dibangun menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain.



Gambar 5
Logical Topologi PT XYZ

Simulation Prototype

Alur dari dari sistem topologi yang dibangun dibuat kedalam simulasi menggunakan *software* Packet Tracer sebelum melakukan implementasi pada jaringan secara langsung. Contoh simulasi bisa dilihat pada gambar 6 (Lammle, 2004).



Gambar 6
Simulation Prototype di aplikasi Packet Tracer

Implementation

Setelah melakukan analisis dan perancangan, selanjutnya adalah tahap implementasi. *Design* yang sebelumnya sudah dirancang dan disimulasikan akan dijalankan dan dilakukan pengujian. Sebelum melakukan pengujian ada beberapa tahapan yang harus dilakukan. Tahap pertama konfigurasi yang dilakukan pada ESXI *(VMware vSphere)* disesuaikan dengan sistem yang dibutuhkan oleh software yang akan dijalankan. Gambar 7 dibawah merupakan tampilan dari *VMware vSphere Client* yang menampilkan dimana server forescout berjalan.

Gambar 7
Tampilan *VMWare vSphere ESXI*

Kemudian setelah itu pada tahap yang kedua adalah memastikan bahwa *virtual switch* telah dikonfigurasi dengan benar untuk konektivitas jaringan ke *virtual machine* Forescout. Masuk ke

access/distribution switch, dapatkan hak istimewa maksimum dan lakukan perintah berikut dalam mode konfigurasi.

```
snmp-server community "snmp user" unrestricted
```

Gambar 8
Tampilan *snmp-server di switch*

Setelah itu lakukan konfigurasi SNMPv3 (gambar 9) dan konfigurasi SNMP Trap (gambar 10) seperti dibawah ini.

```
(Instant Access Point) (config)# snmp-
server host <IP-address> {version 3}
<name> udp-port <port> inform
(Instant Access Point) (config)# end
(Instant Access Point) # commit apply
```

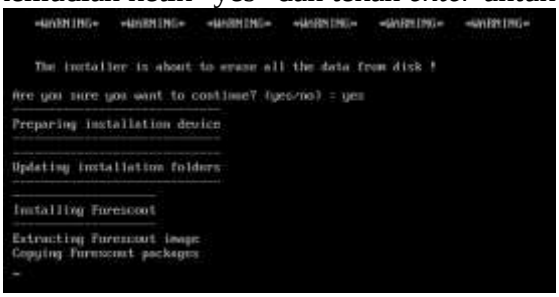
Gambar 9
Tampilan setting *snmp di wireless LAN controller*

```
hostname name
syscontact name
syslocation string
snmp-server community string
snmp-server enable trap
snmp-server engine-id engine-id
snmp-server host ipaddr version {3} string
[udp-port number]
snmp-server trap source ipaddr
snmp-server username [auth-prot {sha}
password priv-prot DES password
```

Gambar 10
Tampilan setting *snmp-trap di wireless LAN controller*

Installation

Sebelum melakukan instalasi, pastikan VM dikonfigurasi dengan spesifikasi yang benar. Lakukan boot ke VM dengan *file* ISO yang telah di-*mount* ke dalam VM. Pilih "Install CounterACT x.x.x-xx" dan tekan enter untuk memulai instalasi saat diminta di layar. Setelah ISO di-*boot*, layar instalasi akan ditampilkan. Kemudian ketik "yes" dan tekan *enter* untuk memulai instalasi.

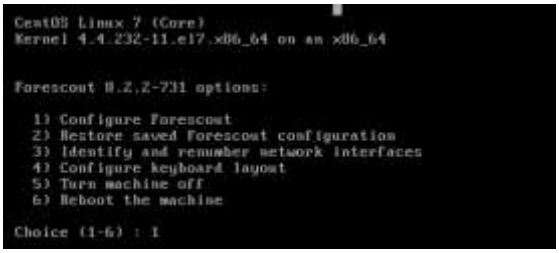


Gambar 11
Tampilan screen memulai proses instalasi

Setelah instalasi selesai tekan *enter* untuk *reboot*.

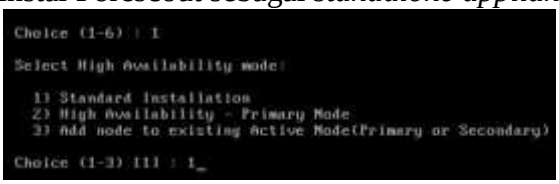
Gambar 12
Tampilan screen proses instalasi telah selesai

Konfigurasi
Setelah kita menyelesaikan tahap instalasi, kemudian kita masuk ke tahap konfigurasi. Pilih opsi 1 untuk mengonfigurasi Forescout.



Gambar 13
Tampilan screen memulai proses konfigurasi

Pilih opsi 1 lagi untuk menginstal Forescout sebagai *standalone appliance*

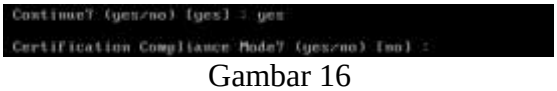


Gambar 14
Tampilan screen proses konfigurasi *high availability mode*

Ketik "yes" untuk melanjutkan pengaturan

Gambar 15
Tampilan screen Forescout *initial setup*

Masukkan "no" untuk mode *certificate compliance* (ini mengaktifkan mode FIPS secara *default* dan menonaktifkan akses shell, yang tidak diperlukan dalam penerapan ini)

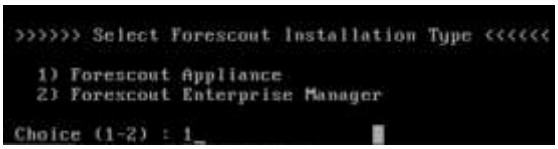


Gambar 16
Tampilan screen Forescout *certification compliance mode*

Pilih "no" untuk enkripsi disk (ini mengenkripsi *disk* tempat Forescout diinstal untuk perlindungan data, yang tidak diperlukan dalam penerapan ini)

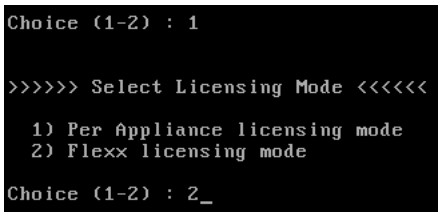
Gambar 17
Tampilan screen Forescout *enable disk encryption*

Pilih opsi 1 untuk menginstal *appliance*



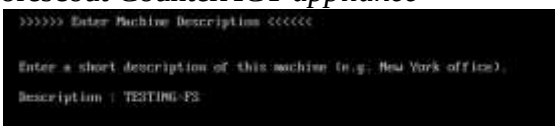
Gambar 18
Tampilan screen Forescout *installation type*

Pilih opsi 2 untuk Model Lisensi Flexx



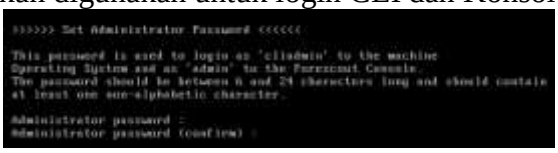
Gambar 19
Tampilan screen Forescout *licensing mode*

Masukkan deskripsi untuk Forescout CounterACT *appliance*



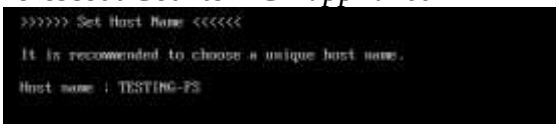
Gambar 20
Tampilan screen Forescout *enter machine description*

Masukkan kata sandi yang akan digunakan untuk login CLI dan Konsol



Gambar 21
Tampilan screen Forescout *set administrator password*

Masukkan nama *host* untuk Forescout CounterACT *appliance*

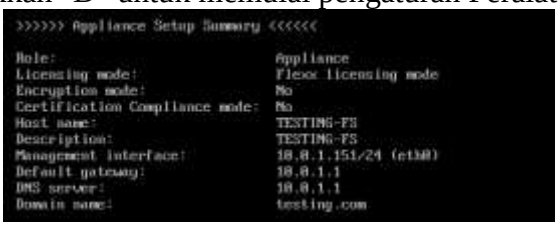


Gambar 22
Tampilan screen Forescout *set host name*

Masukkan informasi jaringan lainnya dan pastikan bahwa alamat IPv6 manajemen disetel sebagai tidak ada

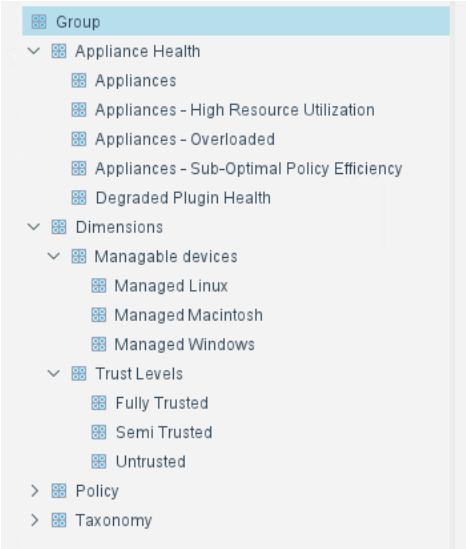
Gambar 23
Tampilan screen Forescout *configure network settings*

Setelah konfigurasi selesai, halaman ringkasan akan ditampilkan. Masukkan "T" untuk menguji pengaturan, jika tidak masukkan "D" untuk memulai pengaturan Peralatan.

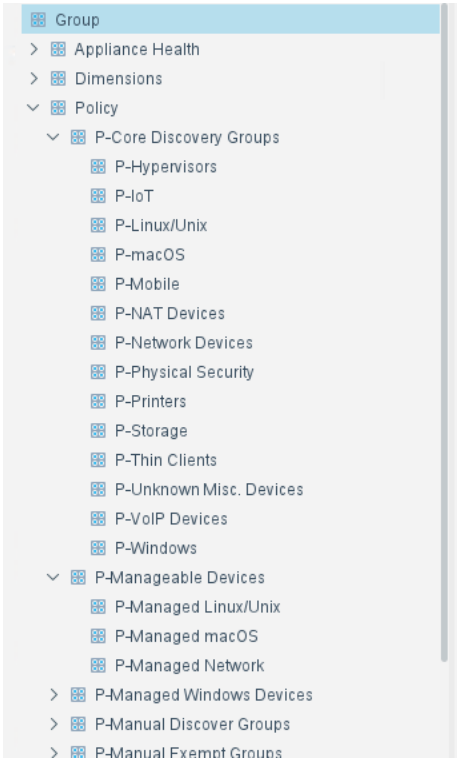


Gambar 24
Tampilan screen proses konfigurasi telah selesai

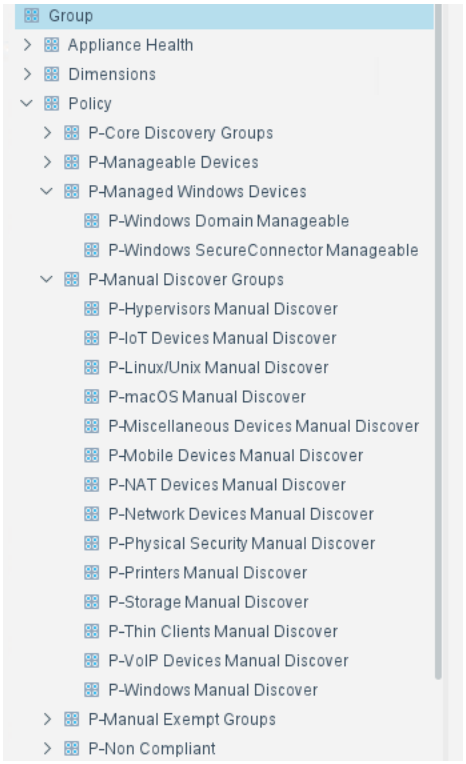
Administration
Bagian ini menunjukkan proses administrasi Forescout yang dilakukan pada GUI. Dalam proses ini juga dilakukan konfigurasi segmentasi jaringan, grup dan juga pembuatan *policy* yang akan dijalankan oleh Forescout.



Gambar 25
Tampilan screen *group manager 1*



Gambar 26
Tampilan screen *group manager 2*



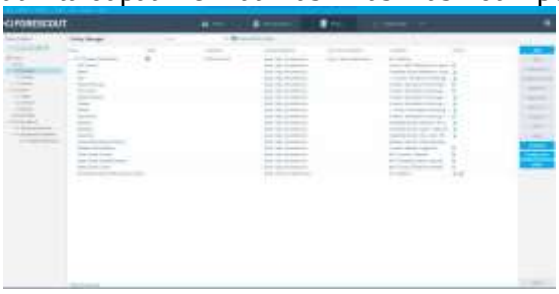
Gambar 27
Tampilan screen *group manager 3*

Gambar 28
Tampilan screen *group manager 4*

Gambar 29
Tampilan screen *group manager 5*

Monitoring

Tahapan monitoring dilakukan setelah semua konfigurasi yang ada di tahapan implementasi selesai dilakukan. Melakukan monitoring sekaligus melihat hasil dari konfigurasi yang dibuat apakah sesuai dengan fungsinya atau tidak. Gambar 30 merupakan tampilan depan dari *policy manager*. Dimana dari tampilan tersebut kita dapat melihat klasifikasi hasil dari policy yang diterapkan.



Gambar 30
Tampilan screen *policy manager 1*

Gambar 31
Tampilan screen *policy manager 2*

Gambar 32
Tampilan screen *policy manager 3*

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

Hasil dan Pembahasan
Pengujian sistem NAC ini dilakukan pada laptop user. Pertama dengan cara menyiapkan komputer user tersebut tanpa di masukkan kedalam domain korporat dimana *join domain* korporat ini merupakan syarat pertama yang harus dipenuhi oleh komputer user. Apabila komputer user ini tidak *join domain* korporat maka sistem forescout akan menolak akses pada komputer user tersebut, seperti pada gambar 13.

Gambar 33
Tampilan laptop yang memasuki vlan 180 (restricted)

Kemudian pada percobaan tahap kedua komputer user digolongkan oleh sistem NAC forescout bahwa komputer user tersebut tidak terinstall antivirus. Kondisi ini menjadi kondisi kedua yang diterapkan setelah kondisi pertama yaitu *join domain*.

Gambar 34
Tampilan laptop yang tidak terinstall antivirus

Setelah dilakukan instalasi oleh tim IT kemudian dihubungkan kembali ke jaringan kantor, terlihat bahwa tampilan di Forescout sudah berubah. Antivirus yang baru diinstall tadi langsung di *forced update* oleh Forescout dan statusnya sekarang *running and up to date*

Gambar 35
Tampilan laptop yang sudah terinstall antivirus

Percobaan yang terakhir adalah ditutupnya secara paksa aplikasi yang termasuk didalam *blacklist*. Pada gambar dibawah, terlihat bahwa Forescout laptop test menginstall *P2P application* yang termasuk kedalam *blacklist.*

Gambar 36
Tampilan laptop yang terinstall *blacklist application*

Kemudian secara otomatis Forescout mengirimkan request untuk *kill process* ke laptop user seperti terlihat pada gambar 37 dibawah.

Gambar 37
Tampilan Forescout *kill process blacklist application*

Setelah itu terlihat hasil seperti pada gambar 38 bahwa *P2P software* yang sedang berjalan tersisa 2 buah dari yang sebelumnya ada 5 buah di gambar 36.

Gambar 38
Tampilan Forescout *P2P Software running*

Kesimpulan

Dari hasil dan pembahasan maka dapat disimpulkan:

1) Impelementasi NAC Forescout membantu *network administrator* mengamankan jaringan komputer PT.XYZ dari perangkat komputer yang tidak sah.
2) Forescout memudahkan *network administrator* memonitor jaringan korporat dengan fitur *asset inventory*
3) *Policy* yang dikonfigurasi pada forescout bekerja dengan baik sehingga semua komputer user yang berada di jaringan korporat lebih terjaga dari virus dan *vulnerability*.

Adapun saran untuk pengembangan kedepannya yaitu:

a. Menambah kombinasi *policy* agar jaringan korporat semakin aman.
b. Menggunakan teknologi otentikasi lainnya seperti LDAP, Active Directory®, RADIUS®, Oracle® dan Sun.

Daftar Pustaka

Chapple, M., Stewart, G.M., Gibson, D. (2018). *CISSP® Certified Information Systems Security Professional Official Study Guide*. Eighth Edition. Sybex.

Damara, S.R. (2020). 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).* 373-381.

Lammle, T. (2004). *CCNA™: Cisco® Certified Network Associate Study Guide*. Sybex.

Schmidt, W. (2018). *A Comprehensive Beginners Guide to Learn About The CompTIA Network+ Certification from A-Z.* Independen Publisher.

Syani, M., Mahestro, R., Tresna, Firdaus, E.A., Nugraha, F.F. (2022). Penerapan Network Access Control Autentikasi Internal Network Security Protokol 802.1x. *Jurnal Nuansa Informatika, vol.16 (no.2).* 77-86.