OPTIMASI KEAMANAN PADA JARINGAN MULTI-ENDPOINT ACCESS MENGGUNAKAN NETWORK ACCESS CONTROL BERBASIS CISCO ISE

Diky Kus Heryadi[1)], Ade Surya Budiman[2)]
[1] Teknik Informatika, Univ. Nusa Mandiri, Jl. Jatiwaringin No. 2, Jakarta Timur
[2] Teknologi Komputer, FTI, Univ. Bina Sarana Informatika, Jl. Kramat Raya No.98, Senen, Jakarta Pusat
Co Responden Email: ade.aum@bsi.ac.id

Article history
Received July 20, 2021
Revised August 11, 2021
Accepted Sept 27, 2021
Available online Oct 05 2021

Keywords
Network Security, Endpoint, Network Access Control, Cisco ISE

Abstract

Companies need to continue to improve the performance and performance of their computer networks, including the most important thing related to computer network security. PT Nusantara Compnet Integrator (Compnet) has a high density of access from endpoints to the corporate network. The addition of endpoints made the company's network became more congested and more vulnerable to security problems. As a result, it became more difficult to identify users, devices, and activities on the Compnet network, given that access to the Compnet network is without access control. The enhancement of Network security design is needed to identify and control the access to each endpoint on the company's networks. In this research, the implementation of the Network Access Control (NAC) was proposed to control the access to any of the endpoint. NAC will filter endpoints that do not belong to Compnet that are trying to connect via the Switch. The NAC used is based on the Cisco Identity Services Engine (ISE). From the test results, it is obtained that the optimization of the Compnet network security, in the form of better control of endpoints when accessing the Compnet network, through the authentication and verification process.

Riwayat
Diterima 20 Juli 2021
Revisi 11 Agustus 2021
Disetujui 27 Sept 2021
Terbit 05 Okt 2021

Kata Kunci
Keamanan Jaringan, Titik Akhir, Kontrol Akses Jaringan, Cisco ISE

Abstrak

Perusahaan perlu terus meningkatkan kinerja dan performa jaringan komputernya, termasuk yang paling utama adalah terkait dengan keamanan jaringan komputer. PT. Nusantara Compnet Integrator (Compnet) memiliki kepadatan akses yang cukup tinggi dari endpoints ke jaringan perusahaan. Pertambahan endpoints, mengakibatkan lalu lintas data pada jaringan Compnet menjadi padat dan lebih rentan dengan masalah keamanan. Imbasnya, membuat identifikasi terhadap pengguna, perangkat, dan aktivitas yang ada di dalam jaringan Compnet menjadi lebih sulit untuk dilakukan, mengingat akses ke jaringan Compnet tanpa adanya kontrol akses. Untuk menyelesaikan permasalahan tersebut dibutuhkan rancangan keamanan jaringan yang mampu mengidentifikasi dan mengendalikan akses terhadap setiap endpoint yang akan terkoneksi ke jaringan sehingga tidak sembarang endpoint dapat terkoneksi ke jaringan. Didalam penelitian ini, dilakukan perencanaan dan perancangan Network Access Control (NAC), sebagai mekanisme pengawasan dan pengendalian akses endpoints dalam jaringan Compnet. NAC akan melakukan filter terhadap endpoint yang bukan milik Compnet yang mencoba terkoneksi melalui Switch. NAC yang digunakan berbasis Cisco Identity Services Engine (ISE). Dari hasil pengujian, diperoleh optimasi keamanan jaringan Compnet, berupa kontrol terhadap endpoint yang lebih baik ketika akan mengakses jaringan Compnet, melalui proses otentikasi dan verifikasi.

PENDAHULUAN

Pada prinsipnya keamanan jaringan merupakan proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Dengan cara menghentikan akses dari pengguna yang tidak sah terhadap sistem jaringan komputer. Hal ini bertujuan untuk mengantisipasi resiko ancaman pada jaringan komputer (Ma'sum et al., 2017). Berkembangnya kebijakan terkait dengan *Bring Your On Device* (BYOD) disertai dengan pesatnya teknologi *Internet of Thing* (IoT), berdampak pada berubahnya bentuk jaringan komputer dan konsekuensi keamanan yang menyertainya (Fortinet, 2018). Kesulitan utama bagi kebanyakan perusahaan adalah bagaimana mengamankan *mobile endpoints* dan bahkan akan lebih sulit lagi ketika harus mengamankan perangkat-perangkat IoT, karena tidak ada atau kurangnya *built-in security* pada perangkat.

Permasalahan terkait bagaimana mengembangkan kendali akses (*access control*) merupakan aspek paling krusial apabila dikaitkan dengan keamanan dan kerahasiaan dalam teknologi jaringan termasuk diantaranya perangkat terkait dengan IoT (Ouaddah et al., 2017). Telah banyak upaya yang dilakukan terkait dengan penelitian untuk mengatasi beragam kebutuhan teknologi, yang bertujuan untuk mengintegrasikan objek cerdas (*smart objects*) seperti misalnya didalam IoT kedalam jaringan internet yang saat ini telah ada dan digunakan. Setiap perusahaan dengan *business core* yang berbeda, akan mengahadapi permasalahan terkait keamanan jaringan yang berbeda pula. Sebagai contoh kasus dalam penelitian diantaranya adalaha *Internet Service Provider* (ISP). ISP merupakan salah satu jenis perusahaan penyedia layanan yang menghadapi masalah yang besar dengan adanya penambahan atau pengembangan jumlah perangkat dalam jaringannya (Widyatmoko & Salamah, 2016). Sehingga, manajemen perangkat menjadi sebuah isu terkait keamanan yang perlu diatasi dengan baik. Sistem otentikasi dan otorisasi konvensional dimana setiap database user tersimpan di setiap perangkat tentu akan menjadi tidaklah efisien dalam manajemen perangkat. Sehingga, dapat menimbulkan permasalahan terkait hak akses, dan kontrol terhadap perangkat.

Menjaga validitas dan integritas data merupakan hal yang tidak dapat dikesampingkan dalam membangun infrastruktur jaringan komputer. Hal penting terkait keamanan yang tidak bisa dikesampingkan adalah mencegah penyusupan dari perangkat yang tidak terotentikasi dan terotorisasi. Perlu adanya kontrol terhadap akses dan pencatatan (*log*) terhadap setiap paket data yang memasuki jaringan (Arta et al., 2018). Untuk mengembangkan suatu jaringan yang aman, ada dua hal yang perlu dipertimbangkan yaitu: *confidentiality* dan *integrity* (Pawar & Anuradha, 2015). *Confidentiality* memiliki makna adanya kepastian bahwa *non-authenticated party* tidak dapat mengakses data. Sementara, *integrity* bermakna adanya jaminan bahwa data yang diterima oleh penerima data, tidak mengalami perubahan atau modifikasi setelah dikirim dari pengirim data. Dalam kasus lain, penambahan *node* atau *endpoint* pada jaringan suatu perusahaan meningkatkan tantangan dalam menjamin keamanan jaringan tersebut secara keseluruhan.

Dalam penelitian dengan mengambil studi kasus yang dilakukan di Universitas Padjajaran (Unpad), pertambahan *node* jaringan tersebut berimplikasi terhadap sulitnya *network administrator* dalam melakukan kontrol dan pengidentifikasian terhadap pengguna, perangkat dan aktivitas yang ada di dalam jaringan. Sehingga, tidak menutup kemungkinan aktivitas - aktivitas lainnya yang dapat mengganggu, mengambil, bahkan merusak data dan infrastruktur jaringan Unpad, mengingat akses ke jaringan Unpad sangat mudah, disamping adanya kelemahan-kelemahan pada aplikasi atau *software*. Selain itu juga, metode dan teknologi yang digunakan untuk aktivitas-aktivitas ilegal dalam teknologi informasi atau jaringan komunikasi terus berkembang dan adanya kebiasaan-kebiasaan yang yang salah dilakukan user seperti tidak mengupdate antivirus, membuka *attachment* yang berbahaya dan sebagainya. Mekanisme manajemen kontrol di jaringan Unpad diusulkan agar jaringan menjadi lebih optimal dan lebih aman. Diantaranya dengan pengimplementasian autentikasi pada jaringan (*network access control*) yang berjalan pada *media-access layer* (*layer 2* OSI) menggunakan IEEE 802.1x *authentication* dengan *MAC Address*. Mekanisme ini akan memvalidasi perangkat-perangkat seperti laptop, ponsel dan perangkat lainnya yang digunakan oleh *user*.

User yang terkoneksi ke jaringan Unpad 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 (Taufik, 2014).

Pemanfaatan Cisco ISE sebagai platform keamanan jaringan komputer juga menjadi titik fokus dalam penelitian dengan objek studi kasus PT. Lintasarta (Dali, 2017). Peningkatan dan perbaikan berkelanjutan terus dilakukan terhadap infrastruktur Teknologi Informasi di perusahaan tersebut, untuk mencegah dan melindungi aset perusahaan dan operasional perusahaan dari ancaman kejahatan *cyber* yang mempengaruhi kepuasan dan kepercayaan konsumen Lintasarta. Dengan penyampaian informasi dari setiap *user devices* kepada Cisco ISE melalui *Cisco AnyConnect*, akan lebih mudah dalam mengawasi dan mengendalikan keamanan jaringan jika ada kunjungan dari tamu ataupun vendor, yang kemudian mengakses jaringan internal Lintasarta.

Didalam penelitian ini, penulis mengambil studi kasus pada PT. Nusantara Compnet Integrator (Compnet). Permasalahan yang dihadapi perusahaan adalah padatnya *endpoint* yang melakukan akses ke jaringan Compnet. Seiring pertambahan *endpoints* jaringan, baik *endpoint* milik Compnet maupun *endpoint* yang bukan milik Compnet terhubung ke jaringan Compnet secara bersamaan sehingga akses menuju jaringan Compnet menjadi padat dari yang seharusnya hanya 10 pengguna yang diperbolehkan terkoneksi ke jaringan Compnet, menjadi 30 pengguna yang terkoneksi ke jaringan Compnet. Artinya, terdapat 20 pengguna yang seharusnya tidak diperbolehkan untuk terkoneksi ke jaringan Compnet. Hal tersebut membuat kontrol dan pengidentifikasian terhadap pengguna, perangkat dan aktivitas yang ada di dalam jaringan Compnet menjadi sulit dilakukan oleh network administrator. Sehingga tidak menutup kemungkinan aktivitas-aktivitas lainnya yang dapat mengganggu, mengambil, bahkan merusak data dan infrastruktur jaringan Compnet, mengingat akses ke jaringan Compnet sangat mudah tanpa adanya kontrol akses atau pembatasan akses.

Untuk menyelesaikan permasalahan tersebut dibutuhkannya suatu teknologi keamanan jaringan yaitu suatu *device* yang dapat melakukan pengidentifikasian dan kontrol akses terhadap setiap *endpoint* yang akan terkoneksi ke jaringan Compnet, sehingga tidak sembarang *endpoint* dapat terkoneksi ke jaringan Compnet. *Device* tersebut disebut dengan *Network Access Control* (NAC). Dari penelitian ini akan dilihat seperti apa pengaruh penggunaan NAC terhadap kepadatan akses seluruh *endpoint* ke jaringan Compnet. Dengan melakukan filter terhadap *endpoint* yang bukan milik Compnet yang mencoba terkoneksi melalui Switch, saat sebelum dan sesudah menggunakan NAC. Sehingga kedepannya tidak sembarang *endpoint* dapat terkoneksi ke jaringan Compnet. NAC yang digunakan oleh PT. Nusantara Compnet Integrator adalah *Cisco Identity Services Engine* (ISE).

Network Access Control (NAC) pada dasarnya adalah serangkaian proses pemeriksaan terhadap apa yang dihadapi oleh *host*, proses karantina dan proses perbaikan yang dihasilkan oleh suatu gangguan, hingga kendali terhadap bagaimana *host* meminta akses ke jaringan. Jika klien tidak menerima *patch* dari *Operating System* (OS) terbaru maupun *bug* yang terkait, bersamaan dengan sebuah definisi virus terbaru yang berjalan pada sistem itu, maka *client* tidak akan diizinkan untuk mengakses jaringan, meskipun akan dipindahkan baik ke VLAN maupun karantina (jaringan) sampai memenuhi persyaratan yang dinyatakan oleh jaringan (Roopesh et al., 2017). NAC tidak akan selalu mengizinkan akses terhadap jaringan yang diminta oleh staf, pengunjung selain staf, dan juga secara protektif mencegah ancaman terhadap keamanan jaringan meskipun memiliki wewenang untuk mengakses di mana saja jaringan mendukung peran *client*. Akses ke dalam jaringan dapat saja diterima, ditolak, serta mendukung identitas client ke *network cluster* tertentu. Hal yang mendasari penting adanya metode untuk melakukan validasi terhadap *patched and up to date-Operating System* adalah banyaknya kasus infeksi *malware* yang dimulai dari eksploitasi secara *remote* terhadap target yang memiliki kerentanan (*vulnerability*) pada OS maupun aplikasi lainnya (Miller, 2014). Dengan demikian, menjaga komponen *host* pada jaringan komputer merupakan aspek penting untuk mengurangi serangan terhadap jaringan komputer suatu perusahaan.

Salah satu perubahan utama dalam bidang telekomunikasi yaitu maraknya

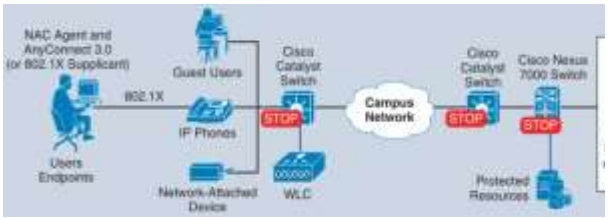
penggunaan jaringan *wireless*. Masalah yang akan dihadapi apabila menerapkan jaringan *wireless* yaitu isu tentang keamanannya. Jika ingin merancang suatu jaringan *wireless*, diharuskan juga merancang sistem keamanan yang efisien. Terkait penjelasan di atas, dirancanglah sistem otentikasi pada pengguna jaringan *wireless* dengan teknologi *Remote Authentication Dial-In User Service* (RADIUS) yang bertujuan melakukan otentikasi, otoritasi, dan pendaftaran akun *user* secara terpusat dalam mengakses jaringan (Darmadi, 2018). RADIUS bekerja menggunakan sistem *client-server* terdistribusi dengan *server*-nya yang menerapkan model protokol *AAA* (*Authentication, Authorization, Accounting*) untuk mengamankan jaringan dari pengguna yang tidak berhak. Model otentikasi yang digunakan yaitu PAP (*Password Authentication Protocol*) sehingga *user* hanya dapat menikmati jaringan ketika telah mempunyai *username* dan *password* dalam RADIUS *server*. RADIUS *server* telah mendukung *multi-user* dan *multi-roaming*, hal ini diharapkan mampu mempermudah *user* ketika melakukan perpindahan ke tiap *access point*/titik jaringan tanpa mendaftar ulang serta dapat memberi keamanan yang lebih baik dalam suatu jaringan komputer.

Cisco Identity Services Engine (ISE) merupakan platform manajemen keamanan dan komponen kunci dari arsitektur keamanan akses milik Cisco (Woland & Redmon, 2015). Perannya dalam jaringan memungkinkannya untuk menjadi titik penegakan keamanan jaringan. Cisco ISE bertindak sebagai platform kebijakan keamanan jaringan dan server RADIUS yang terpusat, memperluas fungsionalitas AAA ini ke semua perangkat jaringan. Saat pengguna atau *endpoint* mencoba mengakses jaringan, perangkat akses jaringan (*switch*) meneruskan semua parameter otentikasi yang relevan ke Cisco ISE. Cisco ISE merespons *switch* dengan kebijakan keamanan yang dihasilkan untuk diterapkan pada pengguna atau endpoint dengan menggunakan RADIUS *Attribute-Value Pairs* (AVPs). Cisco ISE merupakan sebuah "mesin kebijakan" (*policy engine*) yang memungkinkan NAC secara kontekstual melintasi jaringan kabel maupun nirkabel, dan memperluas konektivitas perangkat *mobile* (diantaranya dalam BYOD) (Rasner, 2015).

Cisco ISE secara garis besar memiliki fungsi dan manfaat berikut (Janoff & McGlothin, 2016):

a. Memungkinkan perusahaan skala besar (*enterprise*) untuk mengotentikasi dan mengotorisasi pengguna dan *endpoints* melalui jaringan kabel, nirkabel VPN, dengan kebijakan yang konsisten di semua bagian dari *enterprise* tersebut.
b. Mencegah akses jaringan dari pihak yang tidak terotorisasi sebagai usaha untuk melindungi aset perusahaan.
c. Menyediakan manajemen siklus hidup bagi non-staff/tamu (*guest lifecycle management*) secara lengkap, dengan cara mendayagunakan (*empowering*) *guest* yang merupakan tenaga pendukung (*sponsors*) untuk menjadi penyokong bagi korporasi (*on-board guest*), dengan demikian bisa mengurangi beban kerja Teknologi Informasi perusahaan.
d. Menemukan (*discover*), mengklasifikasikan dan mengendalikan *endpoints* yang terhubung ke jaringan, sehingga memungkinkan layanan yang tepat sesuai dengan jenis dari *endpoint*.
e. Memaksakan berlakunya kebijakan keamanan, dengan cara merintangi, mengisolasi dan memperbaiki perangkat yang tidak sesuai ketentuan (*non-compliant machines*) dalam suatu area karantina, tanpa perlu diperhatikan sepenuhnya oleh administrator jaringan.
f. Menawarkan konsol terintegrasi (*built-in console*) untuk mengawasi, melaporkan dan memecahkan permasalahan, dengan tujuan untuk membantu *helpdesk operators* dan administrator jaringan menjalankan jaringan secara baik.

Gambar 1 memperlihatkan hubungan antara *Network Access Control* (NAC) yang berada pada sisi *endpoints* dengan Cisco ISE pada suatu jaringan *Local Area Network* (LAN).



Gambar 1. Skema Penggunaan Cisco ISE-Based LAN (Janoff & McGlothin, 2016)

Cisco ISE dalam prakteknya – secara mekanisme - dapat diintegrasikan dengan *tool* yang dipakai untuk mengelola resiko keamanan cyber (*cyber risk security managament tools*), seperti Nessus Home (Roldán-Molina et al., 2017). Integrasi ini akan menilai tingkat kerawanan dan kerentanan (*vulnerability*) dari faktor risiko keamanan, apakah *low*, *medium*, *high* atau *critical*.

METODE PENELITIAN

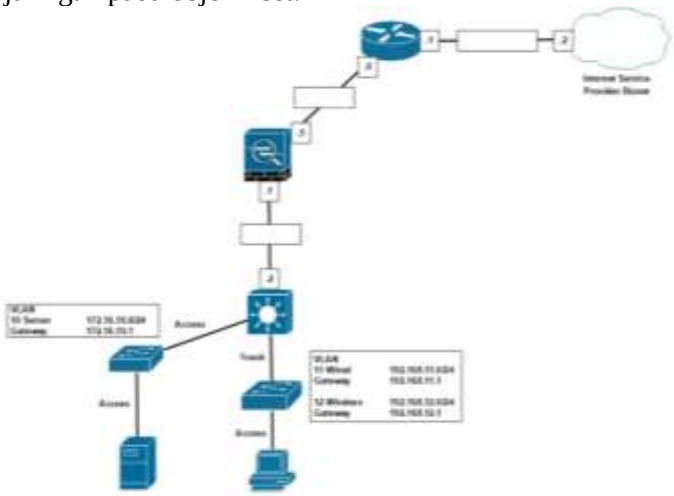
Mengacu kepada siklus pengembangan jaringan komputer dalam sebuah organisasi, penulis membagi penelitian ini kedalam beberapa tahapan yang terdiri dari analisa kebutuhan, desain, dan testing. Metode ini sebagian diantaranya diadopsi dari model Network Development Life Cycle (NDLC), sebagai metode dalam pengembangan jaringan komputer (Nugroho et al., 2021).

a. Analisa
   Penulis menganalisa kebutuhan yang dibutuhkan dalam mengontrol dan memonitor pengguna pada jaringan Compnet dan merancang jaringan baik *hardware* maupun *software* yang akan digunakan. Dalam tahapan analisa ini, penulis melakukan serangkaian pengujian jaringan awal untuk melihat secara objektif permasalahan yang terdapat pada objek penelitian.
b. Desain
   Penulis mendesain sistem yang dapat menyelesaikan masalah yang dihadapi perusahaan. Desain diperoleh dari pemilihan solusi terbaik dari permasalahan jaringan. Kegiatan yang dilakukan dalam tahap desain antara lain, menggambar skema jaringan dan topologi jaringan.
c. Implementasi
   Dalam tahap implementasi ini, penulis menggunakan *Cisco Switch* sebagai jembatan untuk *user* melakukan *authentication*, *Cisco Identity Services Engine (ISE)* sebagai *NAC*, *Microsoft Active Directory* sebagai *user identity database*, dan *DNS Server*.
d. Testing
   Penulis melakukan testing meliputi *user authentication* untuk melakukan kontrol dan pembatasan ketika akan masuk ke jaringan yang akan memanfaatkan fungsi dari *Switch*, *NAC*, dan *Active Directory*.

HASIL DAN PEMBAHASAN

Kondisi Awal Pada Jaringan (*Existing Network*)

Secara skematik, *existing network* pada objek riset diperlihatkan pada Gambar 2. Skema yang diperlihatkan pada Gambar 2 merupakana skema yang disederhanakan dari kondisi nyata jaringan, sehingga tidak memperlihatkan seluruh *device* yang terdapat pada jaringan sebenarnya. Beberapa IP Address juga tidak dipublikasikan, untuk melindungi jaringan pada objek riset.



Gambar 2. Skema *Existing Network*

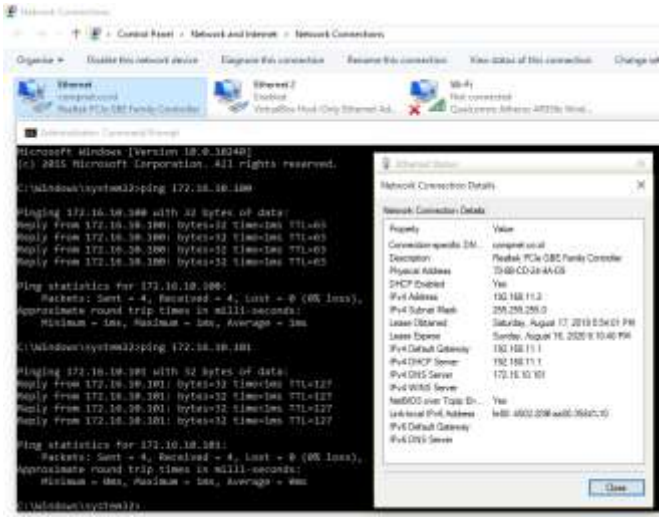
Pada kondisi awal, banyaknya *endpoint* baik yang merupakan milik Compnet maupun bukan milik Compnet yang terhubung ke jaringan Compnet secara bersamaan, menyebabkan akses menuju jaringan Compnet menjadi lebih padat dari yang seharusnya. Dengan pembatasan hanya 10 pengguna yang diperbolehkan terkoneksi ke jaringan Compnet, namun terdapat 30 pengguna yang terkoneksi ke jaringan Compnet. Hal ini berarti terdapat 20 pengguna yang seharusnya tidak diperbolehkan untuk terkoneksi ke jaringan Compnet. Dampaknya manajemen, kontrol, dan identifikasi terhadap pengguna *endpoint* yang ada di dalam jaringan Compnet menjadi sulit

dilakukan oleh *network administrator* akibat banyaknya pengguna *endpoint* yang tidak dikenal. Ditambah lagi dengan adanya aktivitas lain dari pengguna *endpoint* yang tidak dikenal tersebut yang tidak relevan dengan pekerjaan yang dapat mengganggu, mengambil, bahkan merusak data dan infrastruktur jaringan Compnet, mengingat akses ke jaringan Compnet sangat mudah tanpa adanya kontrol akses atau pembatasan akses.

Pengujian Jaringan Awal

Penulis melakukan pengujian dengan membandingkan jumlah pengguna yang masuk ke jaringan sebelum dan setelah implementasi *Network Access Control* dengan Cisco *ISE*. Dari hasil pengujian dinyatakan bahwa pengguna yang dikenal dan terverifikasi dapat masuk ke jaringan, sedangkan pengguna yang tidak dikenal dan tidak dapat diverifikasi tidak dapat masuk ke jaringan. Pengujian jaringan awal dilakukan menggunakan PC dan Cisco *Switch*. Windows PC mencoba untuk masuk ke jaringan sebelum dilakukan implementasi Cisco *ISE*. Tahapan untuk masuk ke jaringan adalah dengan menghubungkan PC ke salah satu *port* yang ada pada Cisco *Switch* menggunakan kabel UTP, hasilnya PC dapat masuk ke jaringan dengan mudah tanpa proses *user authentication*. Tahap pengujiannya adalah sebagai berikut:

a. PC tersebut telah penulis beri IP *address* beserta *gateway* secara *dynamic*. Selanjutnya, penulis melakukan uji konektivitas berupa pengiriman PING dari PC ke *Active Directory* dan Cisco *ISE*. Gambar 3 memperlihatkan detail koneksi dan pengujian perangkat pada jaringan. Terlihat bahwa pengiriman PING telah berhasil, yang menandakan bahwa PC dapat menjangkau jaringan internal PT. Nusantara Compnet Integrator.



Gambar 3. Uji Konektivitas Menuju Jaringan Internal

b. Apabila mengacu kepada *MAC Address Table* yang terdapat pada switch yang dipergunakan, *MAC address* dari PC tersebut akan terlihat yang menandakan bahwa PC sudah terhubung ke salah satu *port* yang ada pada Cisco *Switch* dan masuk ke jaringan PT. Nusantara Compnet Integrator. Dari perintah yang dimasukkan pada Switch, terlihat pada VLAN 11, terdaftar MAC Address dengan alamat 708b.cd24.4ad8 yang terhubung pada interface Fa1/0/2. Seperti yang diperlihatkan pada gambar 4.

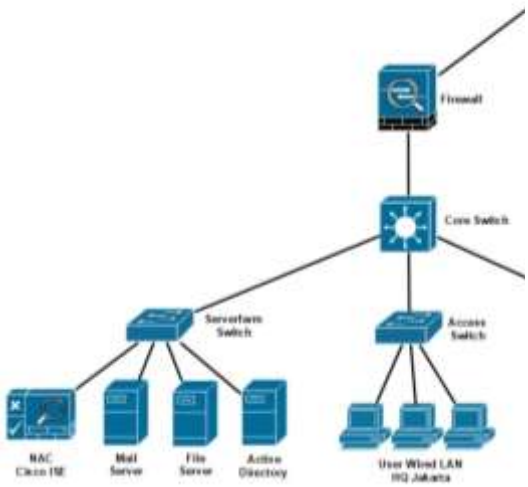
```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  11    708b.cd24.4ad8    STATIC      Fa1/0/2
```

Gambar 4. MAC address PC pada *MAC Address Table*

Rekomendasi Usulan Penelitian

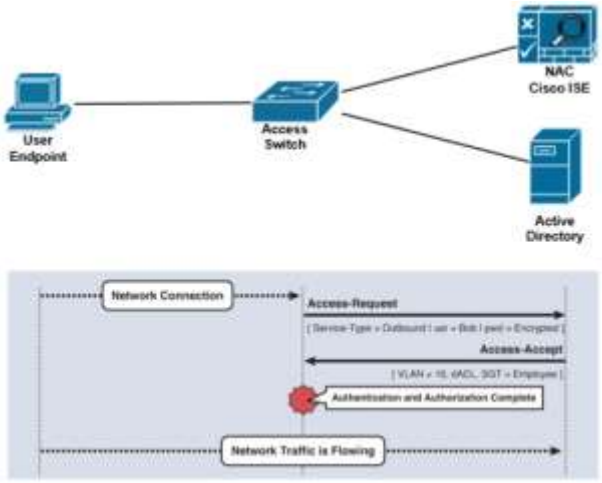
Rekomendasi usulan terhadap permasalahan pada objek riset penambahan perangkat Cisco ISE pada switch Serverfarm, serta penerapan teknologi NAC, dalam hal ini Cisco ISE yang dirancang untuk sebuah perusahaan atau institusi yang selektif dalam menentukan siapa yang diperbolehkan terkoneksi ke jaringan internal dan siapa yang tidak diperbolehkan. Usulan yang penulis berikan akan mengubah mekanisme akses

seluruh *endpoint* yang akan terkoneksi ke jaringan PT. Nusantara Compnet Integrator. Rancangan usulan yang digambarkan dalam gambar 5, akan merubah skema dari *exixting network*.



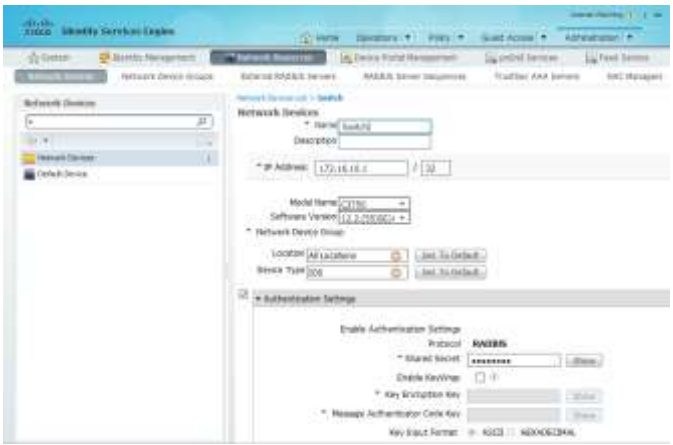
Gambar 5. Skema Jaringan Yang Direkomendasikan

Rekomendasi ini melibatkan penggunaan *802.1x authentication* yang diterapkan pada *endpoint user* ketika mencoba untuk terkoneksi ke jaringan. Sehingga *access switch* akan meminta identitas dari *endpoint user* tersebut. Mekanisme yang direkomendasikan ini, diadaptasikan dari panduan resmi *CCNP Security* (Woland & Redmon, 2015). *EndpointUser* akan memberikan informasi identitas yang diminta oleh *access switch* berupa *username* dan *password*. *Access switch* akan mengirimkan identitas tersebut menuju Cisco *ISE* untuk dilakukan verifikasi. Cisco *ISE* melakukan *query* ke *Active Directory* terhadap identitas yang diberikan apakah valid atau tidak. Apabila identitas yang diberikan valid, Cisco *ISE* akan memberikan *enforcement* kepada *access switch* untuk mengizinkan *user endpoint* tersebut untuk masuk kedalam jaringan PT. Nusantara Compnet Integrator. Namun, apabila identitas yang diberikan tidak valid, Cisco *ISE* akan memberikan *enforcement* kepada *access switch* untuk tidak mengizinkan *endpoint user* tersebut untuk masuk kedalam jaringan PT. Nusantara Compnet Integrator. Mekanisme otentikasi tersebut diperlihatkan dalam Gambar 6.



Gambar 6. Mekanisme Otentikasi Dengan NAC dan *Active Directory*

Penerapan NAC ini sekaligus juga melibatkan fitur keamanan berupa *Extensible Authentication Protocol* (EAP), *Protected EAP* (PEAP), dan penerapan *Authentication, Authorization, Accounting* (AAA). Integrasi dengan *Active Directory* perlu diterapkan agar Cisco *ISE* dapat melakukan *query* untuk memverifikasi identitas yang diberikan oleh pengguna yang mencoba masuk ke dalam jaringan. Disamping itu, konfigurasi *Authentication Policy* untuk menetapkan pengguna yang akan masuk ke jaringan harus menggunakan protokol Radius 802.1x. Konfigurasi umum Network Device pada Cisco ISE, diperlihatkan pada Gambar 7.



Gambar 7. Konfigurasi Network Device Pada Cisco ISE

Selanjutnya pada Access Switch, diterapkan konfigurasi otentikasi sebagai berikut:

```
aaa new-model
aaa authentication login default local
aaa authentication dot1x default group
radius
aaa authorization network default group
radius
aaa accounting update periodic 1440
aaa accounting dot1x default start-stop
group radius
aaa accounting network default start-
stop group radius
aaa accounting system default start-
stop group radius

aaa server radius dynamic-author
 client 172.16.10.100 server-key
xxxxxxx!
 auth-type any
aaa session-id common
authentication mac-move permit
ip routing
ip device tracking
dot1x system-auth-control

interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/2
 switchport access vlan 11
 switchport mode access
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
interface Vlan11
 ip address 192.168.11.1 255.255.255.0
ip http server
ip http secure-server

snmp-server enable traps snmp
authentication linkdown linkup
coldstart warmstart
snmp-server enable traps mac-
notification change move threshold

radius-server attribute 6 on-for-login-
auth
radius-server attribute 8 include-in-
access-req
radius-server attribute 25 access-
request include
radius-server attribute 31 mac format
ietf
radius-server dead-criteria time 5
tries 3
radius-server host 172.16.10.100 auth-
port 1812 acct-port 1813 key xxxxxxx!
radius-server deadtime 15
radius-server directed-request
radius-server vsa send accounting
radius-server vsa send authentication
end

interface FastEthernet 1/0/2
 switchport mode access
 authentication event fail action next-
method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate
server
 authentication timer inactivity server
 authentication violation restrict
 mab
 snmp trap mac-notification change
added
 snmp trap mac-notification change
removed
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Selanjutnya dilakukan konfigurasi pada Active Directory dan DNS Server yang dilakukan pada Server Manager pada bagian *Active Directory Domain Services* (ADDS). Terakhir, dilakukan konfigurasi pada masing-masing *endpoint* berupa pengaturan *Wired 802.1x* yang terdapat pada menu *Wired AutoConfig* pada *Service* (*local*).

Pengujian Jaringan Akhir

Pengujian jaringan akhir dilakukan menggunakan PC, Cisco *Switch*, Cisco *ISE*, dan *Active Directory*. Melalui PC, penulis mencoba untuk masuk ke jaringan setelah dilakukan implementasi Cisco *ISE*. Tahapan untuk masuk ke jaringan adalah dengan menghubungkan PC menggunakan kabel UTP ke salah satu *port* yang ada pada Cisco *Switch* yang telah diaktifkan fitur *authentication*.

Hasilnya PC yang dikenal atau terverifikasi dapat masuk ke jaringan dengan mudah dengan adanya proses *user authentication*. Sedangkan untuk PC yang tidak dikenal atau tidak dapat diverifikasi, akan ditolak oleh Cisco *Switch* untuk masuk ke jaringan. Tahapan pengujiannya adalah sebagai berikut:

a. PC dihubungkan ke *Switch* menggunakan kabel UTP dan secara otomatis akan muncul *pop-up* untuk proses *user authentication*. Penulis juga menguji coba pada *user* yang lain, untuk membuktikan hasil *log*, yang memperlihatkan lebih dari satu *user*. Selanjutnya diteruskan dengan pengisian *username* dan *password* yang sebelumnya telah dibuat pada *Active Directory*, seperti yang diperlihatkan didalam gambar 8.

Gambar 8. *User Authentication Prompt*

b. PC yang berhasil melalui proses *user authentication*, akan terlihat pada menu *Live Log* yang ada pada Cisco *ISE*. Pada Gambar 9, diperlihatkan *Live Log* beserta *overview* atau rincian data dari *user* yang berhasil memperoleh otentikasi dari proses sebelumnya yang menyatakan bahwa PC tersebut berhasil masuk dengan status "*Authentication Success*".

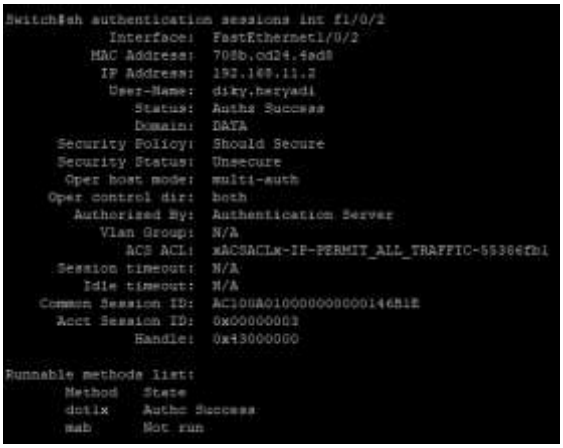
Gambar 9. *Live Log Cisco ISE*

c. PC yang berhasil melalui proses *user authentication* dan masih terhubung ke jaringan juga akan terlihat pada menu "*Show Live Authentications*" yang ada pada Cisco *ISE*. *User active session* atau deskripsi dari *user* yang masih terhubung ke jaringan atau memiliki sesi komunikasi yang aktif dengan jaringan, diperlihatkan dalam gambar 10.

Gambar 10. *User Active Sessions*

Menu *user active session* akan membantu *network administrator* untuk melakukan monitoring atau pengawasan *traffic* jaringan maupun tindakan pemutusan koneksi terhadap pengguna yang sedang terhubung ke jaringan PT. Nusantara Compnet Integrator, apabila diperlukan.

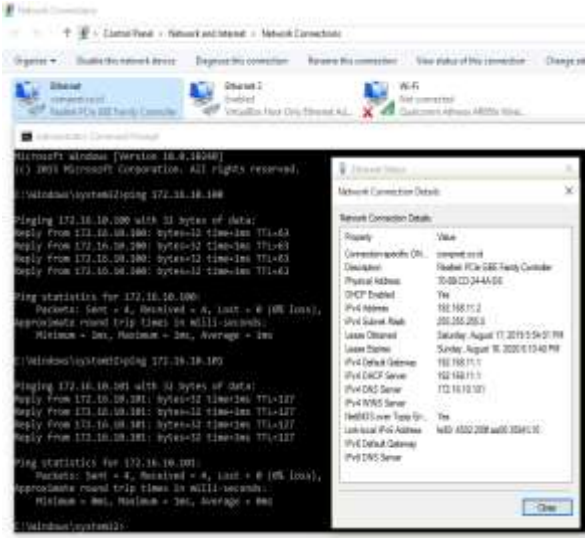
d. PC yang berhasil melalui proses *user authentication* bisa terlihat dari statusnya pada Cisco *Switch*, seperti yang diperlihatkan pada gambar 11. Terlihat juga *enforcement* berupa *ACL Permit All Traffic*, pada *Access Control Server* (ACS).



Gambar 11. *Authentication Session Success*

e. PC yang berhasil melalui proses *user authentication* dilakukan uji konektivitas berupa pengiriman PING dari PC ke *Active Directory* dan Cisco *ISE*, seperti yang diperlihatkan dalam gambar 12. Dari hasil pengujian PING tersebut, diperoleh *reply* yang berhasil diterima (sukses) yang menandakan bahwa PC dapat masuk dan menjangkau jaringan internal Compnet.

P ISSN : 2549-0710
E ISSN : 2722-2713



Gambar 12. PC berhasil melakukan PING ke Jaringan Internal

f. PC yang tidak berhasil melalui proses *user authentication*, akan terlihat pada Cisco *ISE* bahwa PC tersebut tidak berhasil masuk dengan status "*Authentication Failed*", seperti ditunjukkan pada gambar 13. Ini disebabkan oleh input *username* dan atau *password* yang salah. Pengujian ini dilakukan untuk memastikan setiap pihak yang ingin mengakses, memiliki *username* dan *password* yang benar dan valid. Pada Gambar 13 juga diperlihatkan *overview* dari kegagalan otentikasi tersebut.

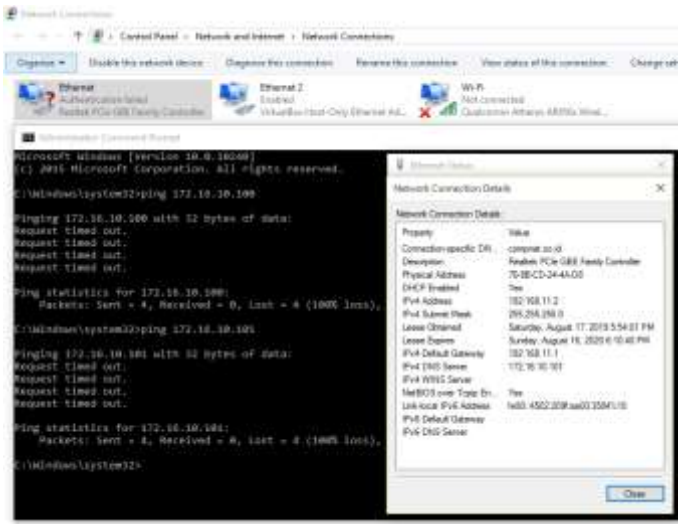
Gambar 13. *User Authentication Failed*

g. PC yang tidak berhasil melalui proses *user authentication* akan terlihat statusnya pada Cisco *Switch*. Terlihat juga dalam gambar 14, enforcement berupa *ACL Deny All Traffic* berupa kegagalan dalam sesi otentikasi untuk pengguna dengan alamat fisik (MAC Address 70-8B-CD-24-4A-D8.

```
Switch#sh authentication sessions int fl/0/2
            Interface:  FastEthernet1/0/2
          MAC Address:  708b.cd24.4ad8
           IP Address:  192.168.11.3
            User-Name:  70-8B-CD-24-4A-D8
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
        Oper host mode:  multi-auth
      Oper control dir:  both
         Authorized By:  Authentication Server
          Vlan Group:  N/A
             ACS ACL:  xACSACLx-IP-DENY_ALL_TRAFFIC-55586fb1
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  AC100A0100000000030028E968
      Acct Session ID:  0x00000008
               Handle:  0x64000003

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

Gambar 14. *User Failed* mendapatkan *ACL Deny All Traffic*

h. Pengujian terakhir untuk PC yang tidak berhasil melalui proses *user authentication* dilakukan uji konektivitas berupa pengiriman PING dari PC ke *Active Directory* dan Cisco *ISE*, hasilnya PING gagal yang menandakan bahwa PC dapat tidak dapat masuk dan menjangkau jaringan internal Compnet, seperti ditunjukkan dalam gambar 15.



Gambar 15. Uji Koneksi Yang Gagal ke Jaringan Internal

KESIMPULAN

Manajemen, kontrol, dan identifikasi terhadap pengguna yang ada di dalam jaringan PT. Nusantara Compnet Integrator tidak dapat dilakukan oleh *network administrator* untuk menghadapi banyaknya pengguna yang tidak dikenal. Hal ini menjadi titik sentral permasalahan jaringan komputer ketika begitu banyak *endpoint* yang terhubung ke suatu jaringan. Melalui implementasi Cisco *ISE*, administrator jaringan dapat dengan lebih efisien dalam mengelola dan melakukan kontrol akses terhadap pengguna yang akan masuk kedalam jaringan dengan memanfaatkan teknologi *RADIUS User Authentication.* Dengan demikian, user yang tidak dapat diverifikasi dari sisi *credential* tidak dapat terkoneksi dengan jaringan internal perusahaan. Disamping itu, *network administrator* dapat melakukan manajemen, kontrol, dan identifikasi pada seluruh pengguna jaringan kabel pada PT. Nusantara Compnet Integrator.

Pengaktifan fitur *Posturing* pada Cisco *ISE* bisa dipertimbangkan, untuk menambah unsur keamanan pada jaringan. Karena fitur *Posturing* pada Cisco *ISE* dapat melakukan pengecekan secara detail apakah PC dari pengguna yang akan masuk ke jaringan tersebut sudah memiliki *Antivirus* atau belum. Agar setiap pengguna yang akan masuk ke jaringan, diasumsikan telah terbebas dari virus karena telah memiliki *Antivirus*. Disamping itu, untuk meningkatkan produktifitas dari karyawan pengguna jaringan PT. Nusantara Compnet Integrator, penulis menyarankan perusahaan untuk melakukan instalasi *Web Proxy* agar dapat melakukan *filter* terhadap setiap situs web yang diakses oleh karyawan pengguna jaringan. Sehingga, segala aktivitas *web browsing* dari karyawan pengguna jaringan dapat dipastikan sudah sesuai dengan *bussiness relevance*.

REFERENSI

Arta, Y., Syukur, A., & Kharisma, R. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *IT Journal Research and Development*, *3*(1), 104. https://doi.org/10.25299/itjrd.2018.vol3(1).1346

Dali, F. (2017). Sistem Keamanan Jaringan Menggunakan Cisco AnyConnect Dengan Metode Network Access Manager. *Jurnal Ilmu Teknik Dan Komputer*, *Vol.X*(No. X), 1–7.

Darmadi, E. A. (2018). Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless. *Jurnal IKRA-ITH Informatika*, *2*(3), 9–16.

Fortinet. (2018). *The Evolution of Network Access Control (NAC): How IoT and BYOD Devices Have Changed NAC Solutions (White Paper)*. www.fortinet.com

Janoff, C., & McGlothin, B. (2016). *Cisco Compliance Solution for PCI DSS 2.0 Design Guide Summary* (3rd Editio). Cisco.

Ma'sum, M. S., Irwansyah, M. A., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *5*(1), 56–60.

Miller, L. C. (2014). *Cybersecurity For Dummies, Palo Alto Networks Edition* (R. Mengle (ed.); Palo Alto). John Wiley & Sons, Inc.

Nugroho, F. E., Daniarti, Y., & Rosidin. (2021). Rancang Bangun QOS (Quality of Service) Jaringan Wireless Local Network Menggunakan Metode NDLC (Network Development Life Cycle) di PT Trimitra Kolaborasi Mandiri (3KOM). *Jurnal Informatika (JIKA)*, *5*(1), 79–83.

Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and New Opportunities. *Computer Networks*, *112*(November 2016), 237–262. https://doi.org/10.1016/j.comnet.2016.11.007

Pawar, M. V., & Anuradha, J. (2015). Network Security and Types of Attacks in Network. *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)*, 503–506.

Rasner, B. G. (2015). *Cisco IT and the Identity Services Engine (White Paper)* (Issue 02/15). https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/cisco-it-and-ise.pdf

Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-

Fernandes, V. (2017). A Comparison of Cybersecurity Risk Analysis Tools. *Procedia Computer Science*, *121*, 568–575. https://doi.org/10.1016/j.procs.2017.11.075

Roopesh, M., Reethika, G., Srinath, B. V, & Sarumathi, A. (2017). Network Access Control. *International Journal on Computer Science and Engineering (IJCSE)*, *9*(05), 1–3.

Taufik, A. M. (2014). Pembangunan Network Access Control Untuk Autentikasi dan Security dengan Menggunakan 802 .1X Authentication. *Jurnal Ilmiah Komputer Dan Informatika (KOMPUTA)*, *1*, 1–7.

Widyatmoko, D., & Salamah, U. (2016). Implementasi Freeradius Berbasis Lightweight Directory Access Protocol Pada Management Infrastruktur Jaringan Internet Service Provider. *Jurnal Format*, *6*(2), 119–135.

Woland, A. T., & Redmon, K. (2015). *CCNP Security SISAS 300-208 Official Cert Guide*.