GEBYAR

BULETIN EDISI 60/SEPTEMBER 2022

AUTO-ID

UNTUK KALANGAN SENDIRI

ZERO TRUST CONCEPT FOR CYBER ATTACK SECURITY!

Hytera POC Solution

Tips & Info:
Mengamankan Jaringan dengan Solusi Network Access Control

MEDIA KOMUNIKASI PELANGGAN
ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

PEMIMPIN REDAKSI
Andre S.Kouanak

SEKRETARIS REDAKSI
Listya Kartikasari (Jakarta)
Indah Widiyanti (Cikarang)
Luh Wayan Sumariani (Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR
Arijanto Hartanto
Chandra Sari

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Empianus Eko Putra
Irvan Kurniawan

ALAMAT REDAKSI
Jakarta (HO)
Perkantoran Gunung Sahari Permai
#C03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.
Telp : +6221-4208221, 4205187
Fax : +6221-4207903, 4207904, 4205853

CONTENT

EDITORIAL

Pelanggan yang terhormat,

Puji syukur saya ucapkan kepada Tuhan Yang Maha Esa, atas berkat rahmat dan karuniaNya, sehingga kita semua dalam kondisi sehat, serta dalam lindunganNya.

Topik bulletin kali ini membahas seputar network security dengan menerapkan konsep **Zero Trust**. Dengan perkembangan teknologi informasi (TI) yang semakin pesat serta evolusi industry digital 4.0 yang telah memunculkan berbagai teknologi seperti *cloud computing, Artificial Intelligence* (AI), *Internet of Thing* (IoT), *Operational Technology* (OT), oleh sebab itu sangat penting dan perlu untuk melakukan pengamanan terhadap perangkat-perangkat tersebut dari pihak-pihak yang tidak bertanggung jawab, sehingga produktivitas perusahaan dan industri dapat berjalan dengan lancar dan aman.

Berbagai solusi yang bisa diterapkan diantaranya solusi **Zero Trust Network Access (ZTNA)** dari Fortinet dan solusi **Clearpass** sebagai *Network Access Control* (NAC) dari HPE Aruba, sehingga setiap perangkat dan pengguna yang terkoneksi ke jaringan yang seharusnya serta sesuai hak aksesnya. Produk-produk tersebut bisa terintegrasi dengan perangkat FortiGate Firewall Next Generation menghadirkan *deployment* yang cepat dan dengan biaya TCO (*Total Cost Ownership*) yang rendah serta mendukung opsi *cloud-based*, *on premise* serta SASE (*Secure Access Service Edge*). Dengan begitu keamanan akses jaringan dari dalam dan luar perusahaan tetap aman.

Selain pembahasan utama, ada pula berbagai topik lain yang menarik kita bahas seperti principal info, product highlight dan teknologi terbaru, serta tips & info dan info-info lainnya yang tentunya dapat bermanfaat bagi pembaca semua.

Akhir kata, penulis dan tim redaksi mengucapkan selamat membaca dan semoga bisa mengambil manfaatnya. Terima kasih dan salam sehat selalu.

Salam hangat,

Empianus Eko Putra

Enterprise Network and Security Specialist
PT. Autojaya Idetech
PT. Solusi Periferal

ZERO TRUST CONCEPT FOR CYBER ATTACK SECURITY!

by **Empianus Eko Putra,**
Enterprise Network and Security Specialist ACS Group

Teknologi Informasi merupakan suatu teknologi yang digunakan untuk mempermudah pekerjaan manusia mulai dari mengolah data, memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas. Informasi yang dimaksudkan adalah informasi yang akurat, relevan, dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan. Informasi ini bernilai strategis sehingga dapat digunakan dalam pengambilan keputusan.

Perkembangan teknologi informasi sangat dipengaruhi oleh kemampuan sumber daya manusia dalam memahami komponen teknologi informasi. Saat ini, perkembangan teknologi sudah sangat pesat, hal ini sangat menunjang pekerjaan baik itu di kantor maupun di area industri. Sehingga dapat mempermudah karyawan dalam mengolah data, dengan begitu bisa didapatkan informasi lebih cepat, tepat dan akurat. Semua informasi yang dihasilkan dalam suatu industri maupun perusahaan, tentunya disimpan dalam berbagai perangkat, baik itu pada *laptop, server on premis* maupun pada *server cloud* perusahaan.

Informasi yang dihasilkan dan disimpan dalam suatu perusahaan tentunya menjadi asset yang sangat kritikal karena menyangkut rahasia perusahaan, serta pengambilan keputusan kedepannya. Oleh sebab itu, perlu dilakukan pengamanan data–data tersebut dari pihak yang tidak bertanggung jawab seperti *Hacker* yang memungkinan untuk melakukan eksploitasi, mengunci maupun menjual data tersebut ke pihak luar.

Perkembangan teknologi di bidang digital informasi sudah memasuki era revolusi industri 4.0 di mana semua pekerjaan terutama sektor *manufacturing* dilakukan secara otomatis oleh *system* secara terpusat. Ini menjadi tantangan tersendiri bagi berbagai industri untuk mengamankan *system* tersebut dari *cyber attack*, khususnya divisi *information technology (IT)*. Kenapa ini menjadi tantangan tersendiri? Sebab perkembangan teknologi pastinya akan diikuti perkembangan *cyber attack* yang semakin modern dan canggih pula.

Bagaimana Cara Pengamanan Network dari Cyber Attack?

Cyber attack tentunya sejalan dengan bagaimana devices dan user terhubung ke *network* perusahaan dan sejauh mana perusahaan menerapkan pengamanan terhadap semua *devices* maupun user yang terkoneksi, dan bagaimana memberikan privilege terhadap user tersebut.

Salah satu metode untuk mengantisipasi *cyber attack* yaitu dengan menerapkan konsep ***Zero Trust*** dalam memberikan akses terhadap semua *devices/user* yang terkoneksi ke jaringan perusahaan.

Gambar 1. Network Visibility and Role Base

Apa itu Zero Trust?

Zero Trust adalah model keamanan jaringan yang didasarkan pada konsep bahwa tidak ada orang atau perangkat di dalam atau di luar jaringan organisasi yang boleh diberikan akses untuk terhubung ke sistem atau layanan TI hingga diautentikasi dan diverifikasi.

Model *zero trust* adalah konsep yang diperkenalkan oleh John Kindervag saat bekerja di Forrester Research pada tahun 2009. Prinsip dasar yang mendasari *zero trust* adalah **"Never Trust, Always Verify."** *Zero trust* menantang model keamanan berbasis perimeter tradisional di mana firewall melindungi jaringan perusahaan tepercaya dari internet yang tidak tepercaya.

Menurut data 2019 Forrester Research, Inc untuk mewujudkan *zero trust* information security ada lima langkah yang mesti dilakukan:

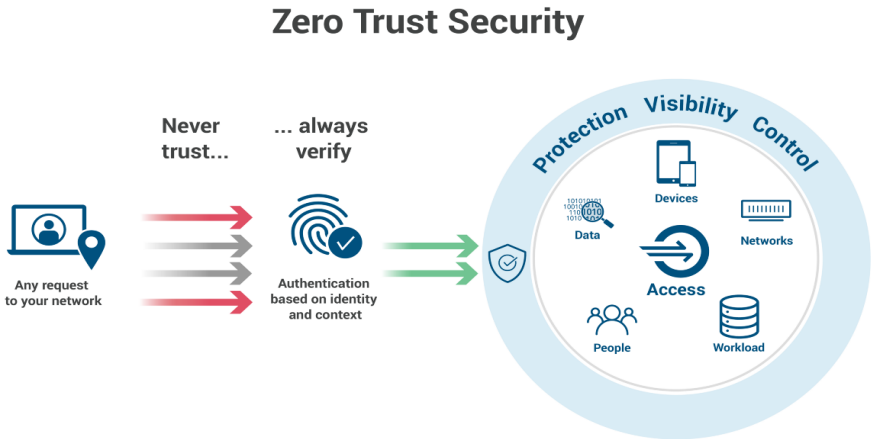
1. Identify your sensitive data

Anda tidak dapat melindungi apa yang tidak dapat anda lihat. *Zero trust* bekerja berdasarkan data untuk memastikan teknologi apa yang harus di investasi, agar sesuai dengan tujuan yang ingin dicapai, serta biaya yang dikeluarkan jadi tepat sasaran.

- Mengidentifikasi dan mengklasifikasikan data sensitif.
- Segmentasikan jaringan berdasarkan sensitivitas data. Mempelajari siapa, apa, kapan, di mana, mengapa, dan bagaimana data perusahaan Anda. Ini sangat penting untuk menciptakan arsitektur keamanan yang lebih kuat dan gesit.

2. Map the flows of your sensitive data.

Anda perlu memahami bagaimana data mengalir di jaringan Anda secara menyeluruh, sumber daya dan orang-orang yang menggunakannya. Serta libatkan banyak pemangku kepentingan untuk memetakan arus transaksi.



Gambar 2. Konsep Zero Trust Security

- Cari dan petakan semua jaringan yang bergantung dan objek sistem.
- Rancang aliran data yang lebih optimal jika perlu.
- Memanfaatkan data yang ada dan diagram aliran jaringan, seperti Data PCI standar keamanan.

3. Architect your Zero Trust microperi-meters.

Dasari rancangan jaringan *Zero Trust* Anda dengan alur transaksi di perluasan ekosistem bisnis Anda, serta bagaimana orang (karyawan, pelanggan) dan aplikasi mengakses data sensitif. Lalu tentukan dan optimalkan jalur transaksi yang menjadi ciri penggunaan data yang tepat dan tandai transaksi ketika seseorang berpotensi menyalahgunakannya.

- Tentukan mikroperimeter di sekitar data sensitif.
- Terapkan mikroperimeter dengan fisik atau kontrol keamanan virtual.
- Batasi dan tegaskan akses untuk mikroperimeter.
- Otomatisasikan basis aturan dan kebijakan.
- Gunakan alat kontrol audit dan perubahan.

4. Continuously monitor your Zero Trust ecosystem security analytics.

Catat dan periksa semua lalu lintas internal dan eksternal untuk aktivitas berbahaya dan area perbaikan:

- Evaluasi di mana analitik keamanan sudah diterapkan.
- Tentukan model penerapan terbaik untuk bisnis anda.
- Cari vendor yang akan mewujudkan jalur otomatisasi keamanan jaringan anda.

5. Embrace security automation and orchestration.

Tinggalkan operasi keamanan manual dan mulai untuk menerapkan keamanan secara otomatisasi.

- Bekerja dengan para pemimpin bisnis untuk menentukan kebijakan untuk otomatisasi.
- Menilai dan mendokumentasikan proses SOC Anda.

- Hubungi vendor analitik keamanan Anda untuk lihat opsi otomatisasi apa yang tersedia.
- Konfirmasikan bahwa otomatisasi keamanan dan vendor orkestrasi mendukung infrastruktur keamanan yang anda inginkan.

Model *zero trust* memindahkan keamanan dari kepercayaan tersirat yang didasarkan pada lokasi jaringan pengguna atau perangkat. Alih-alih, kepercayaan dievaluasi berdasarkan transaksi. Dengan *zero trust*, lokasi jaringan pengguna atau alamat IP tidak lagi menunjukkan implikasi kepercayaan. Sebaliknya, model *zero trust* membutuhkan kepercayaan secara eksplisit diturunkan dari kombinasi identitas dan berbasis konteks kontrol pada tingkat yang sangat terperinci yang memberikan akses berdasarkan prinsip keamanan dengan hak istimewa paling rendah dan perlu diketahui.

Zero trust dimulai dengan postur penolakan default untuk semua user dan devices — yaitu, nol kepercayaan. Dalam model tanpa kepercayaan, kapanpun pengguna atau perangkat meminta akses ke sumber daya, identitas mereka harus diverifikasi terlebih dahulu sebelum akses diberikan. Verifikasi tidak hanya didasarkan pada identitas pengguna dan/atau perangkat, tetapi atribut lainnya, termasuk konteks (seperti tanggal dan waktu), lokasi, dan postur keamanan perangkat.

Namun, akses bukanlah kesepakatan "satu dan selesai". Hanya karena pengguna atau perangkat telah diberikan akses ke sumber daya tidak berarti mereka dapat berkeliaran dengan bebas di jaringan. Akses diberikan dengan sangat tingkat granular. Akses hanya diberikan pada sumber daya yang dibutuhkan untuk melakukan fungsi tertentu untuk waktu yang terbatas dan bukan untuk keseluruhan jaringan. Elemen kunci dari model *zero trust* adalah bahwa kepercayaan harus dievaluasi kembali secara terus menerus. Jika ada perubahan atribut dari pengguna atau perubahan perangkat, kepercayaan dapat dicabut dan akses ke sumber daya juga akan dihapus. Untuk penerapan konsep *zero trust* ini, salah satu solusi yang bisa diimplementasikan yaitu ***Zero Trust Access* (ZTA)**.

ZTA dibangun di atas model *Zero Trust* dan berfokus untuk mengetahui dan mengendalikan siapa dan apa yang mengakses jaringan. *Role-based access control* (RBAC) adalah komponen penting dari ZTA. ZTA lebih khusus mengacu pada solusi di mana perhatian diberikan pada orang dan perangkat yang berada di jaringan. ZTA melibatkan kontrol akses berbasis peran, di mana pengguna hanya diberikan tingkat akses yang sesuai dengan peran mereka, tanpa kemampuan untuk melihat atau mengakses bagian lain dari jaringan.

Di bawah ZTA, manajemen memiliki kontrol dan visibilitas atas titik akhir pengguna untuk mendapatkan pengetahuan pasti tentang pengguna dan memberikan tingkat akses yang sesuai. ZTA juga mencakup perangkat yang mungkin memerlukan beberapa tingkat akses ke jaringan. Dalam pertumbuhan ekonomi Internet of Things (IoT), banyak perangkat seperti printer dan bahkan sistem akses pintu atau lift beroperasi pada koneksi jaringan. Namun, karena perangkat ini tidak mendapatkan akses melalui nama pengguna atau kata sandi, mereka dapat diberikan akses melalui solusi *network access control (NAC)*.

Di bawah model ZTA, perangkat tersebut akan kembali diatur dengan prinsip nol kepercayaan, dengan akses yang cukup diberikan hanya untuk memenuhi fungsinya.

Seiring perkembangan perangkat dan teknologi, selain mengetahui siapa dan apa yang terkoneksi di jaringan. Akses terhadap aplikasi yang digunakan dalam perusahaan juga perlu diamankan. Solusi yang bisa diterapkan adalah ***Zero Trust Network Access* (ZTNA).** ZTNA menawarkan solusi yang mengacu pada keamanan level akses aplikasi di mana tidak ada pengguna atau perangkat yang dipercaya untuk mengakses aplikasi kecuali mereka membuktikan kredensialnya. Elemen kunci dari konsep ZTNA adalah independensi lokasi pengguna. Di mana kebijakan akses aplikasi dan proses verifikasi diperlakukan sama baik

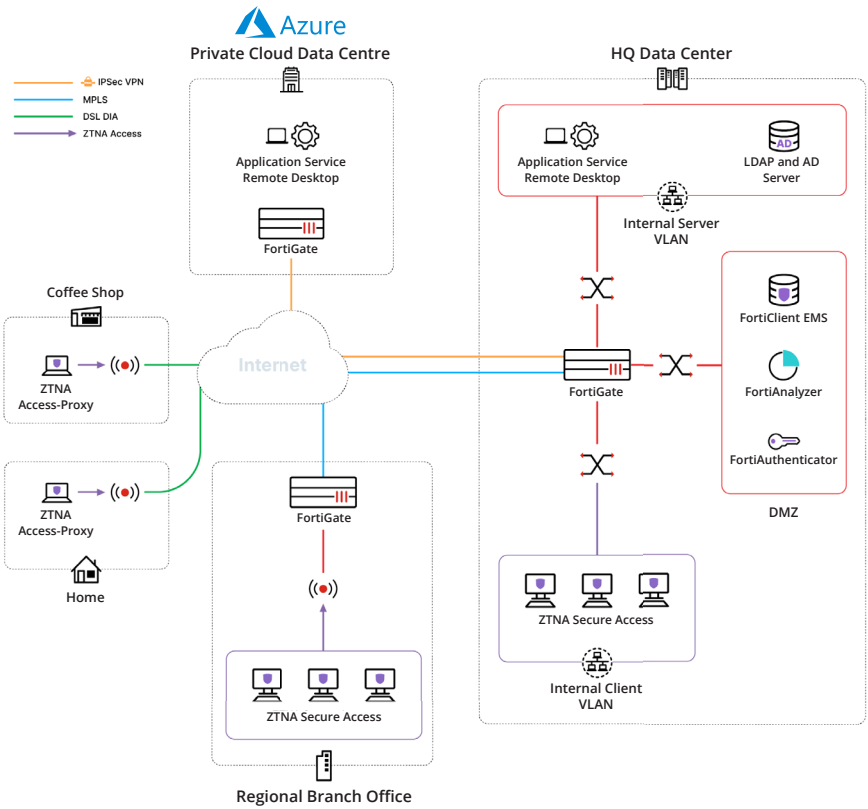
untuk pengguna yang berada di jaringan internal atau di luar jaringan. Untuk pengguna yang berada di luar jaringan, ZTNA menyertakan terowongan terenkripsi yang aman untuk konektivitas dari perangkat pengguna ke titik proxy aplikasi ZTNA. Titik Proxy aplikasi ZTNA memberikan manfaat lebih dari sekadar akses jarak jauh yang transparan dan aman. Dengan meletakkan aplikasi di belakang titik proxy, ZTNA akan menyembunyikan aplikasi tersebut dari internet. Dengan cara ini, ZTNA bisa meminimalkan serangan jaringan dari luar.

Lebih lanjut, ZTNA merupakan pengembangan prinsip ZTA yang mengontrol akses ke aplikasi untuk memverifikasi pengguna dan perangkat sebelum setiap sesi akses aplikasi untuk mengkonfirmasi bahwa mereka memenuhi kebijakan organisasi untuk mengakses aplikasi tersebut terlepas di mana pengguna atau aplikasi berada. Pengguna bisa saja berada pada jaringan perusahaan, bekerja dari rumah atau di tempat lain. Sedangkan aplikasi yang diakses bisa jadi berada di data center perusahaan, private atau public cloud.

ZTNA ini sendiri merupakan evolusi pengembangan dari akses jarak jauh VPN. Mengingat kompleksitas jaringan saat ini, ZTNA menawarkan keamanan yang lebih baik, kontrol yang lebih terperinci, dan pengalaman pengguna yang lebih baik dari pada VPN tradisional.

Selain itu, ZTNA juga mendukung otentikasi multi-faktor untuk mempertahankan tingkat verifikasi tertinggi.

Prinsip Konsep Zero Trust Network Access



Gambar 3. Design Topology Penerapan ZTNA

Model *zero trust* didasarkan pada lima prinsip dasar:

1. Setiap pengguna di jaringan selalu dianggap tidak aman.
2. Ancaman eksternal dan internal selalu ada di jaringan.
3. Lokalitas jaringan tidak cukup untuk menentukan kepercayaan dalam jaringan.
4. Setiap perangkat, pengguna, dan aliran jaringan diautentikasi dan disahkan.
5. Kebijakan harus dinamis dan dihitung dari sumber data sebanyak mungkin.

Manfaat Penerapan Zero Trust Network Access

Untuk mengatasi ancaman yang sudah semakin modern, perusahaan harus mulai beralih dari hanya perlindungan terhadap jaringan saja menjadi perlindungan yang menyeluruh terhadap aplikasi, data yang tersebar di seluruh environment perusahaan, *users*, *systems*, *devices*, dan sumber daya kritikal lainnya.

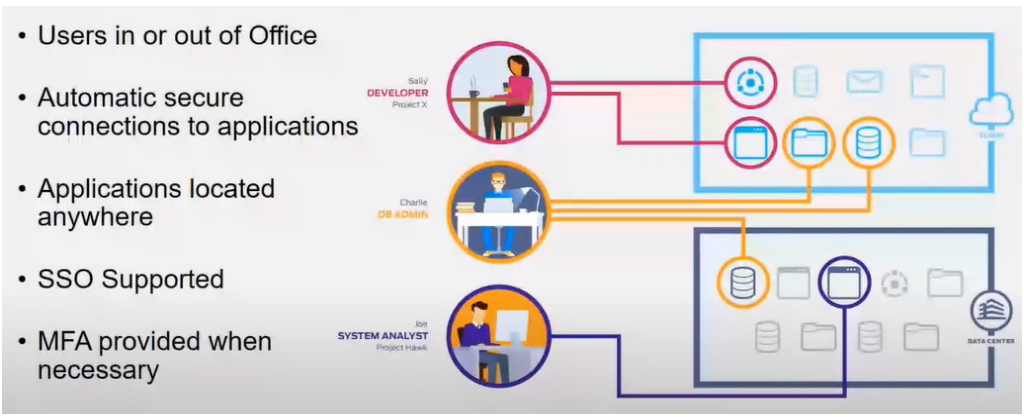
Strategi *zero trust* akan menyediakan secara komprehensif visibilitas dan perlindungan diseluruh *devices, users, endpoint, cloud, dan infrastructure* dengan pendekatan ***"never trust, always verify"*** untuk keamanan.

Reduces risk

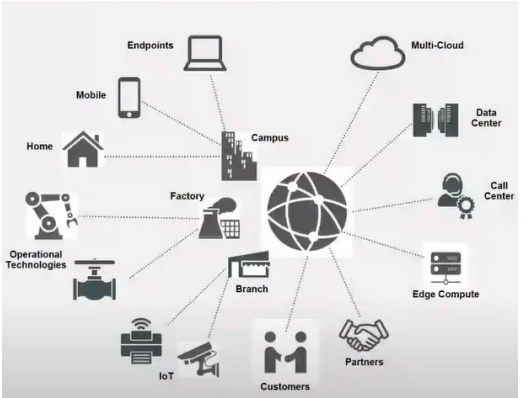
Saat Anda secara otomatis memberikan kepercayaan kepada siapapun, perangkat atau pengguna di jaringan Anda, Anda menempatkan perusahaan dalam risiko ketika salah satu hal tersebut dikompromikan, baik disengaja atau tidak disengaja. Model *zero trust* menghilangkan masalah kerentanan (*vulnerability)* dengan membatasi akses jaringan untuk pengguna, sekaligus secara intensif melakukan verifikasi identitas, sehingga mereka hanya memiliki akses ke data dan sistem yang sesuai dengan peran mereka atau posisi dalam organisasi.

Increases visibility

Anda tahu siapa dan apa yang terhubung ke jaringan setiap saat *(realtime)*. Visibility ini penting dalam menerapkan *security* dalam jaringan. Dengan mengetahui perangkat dan user yang terhubung dalam suatu jaringan, *privilege*, serta akses yang boleh diberikan terhadap user akan lebih mudah diterapkan.



Gambar 4. Controlling User Access



Gambar 5. Devices dan Users Visibility

Extends security

Keamanan jaringan dapat ditingkatkan dengan Menerapkan ZTNA. Tidak seperti *Virtual Private Network* (VPN), yang berfokus secara eksklusif pada lapisan jaringan, ZTNA naik satu lapisan, di mana secara efektif menyediakan keamanan aplikasi yang independen dari jaringan.

Zero Trust Network Access Use Case Fortinet

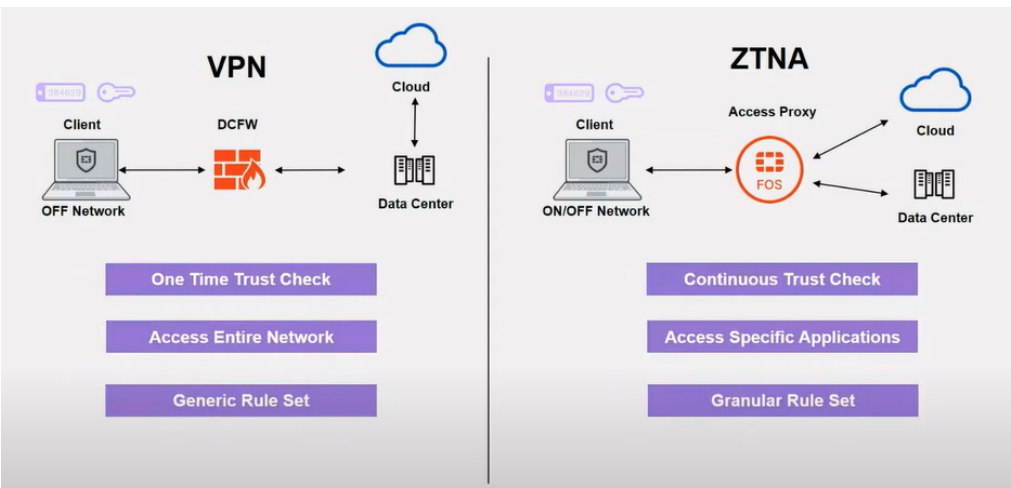
Solusi Fortinet *Zero Trust Network Access* menyediakan verifikasi berkelanjutan untuk semua pengguna dan perangkat saat mereka mengakses aplikasi dan data perusahaan.

IoT Endpoint and Device Protection

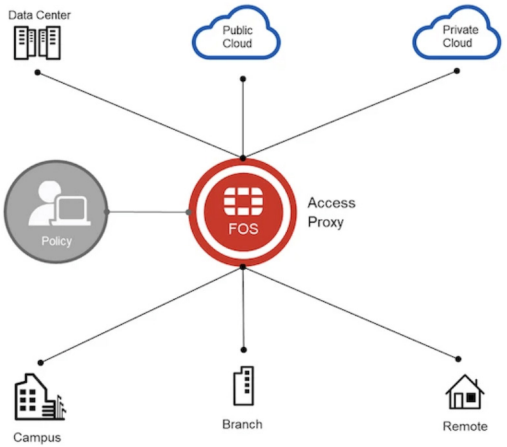
Diperlukan identifikasi dan keamanan untuk perangkat IoT yang tidak dikenal dan perangkat yang terhubung ke jaringan. Hal ini dapat dilakukkan dengan mengintegrasikan *visibility endpoint*, mengatur, dan melakukan pengamanan tingkat lanjut untuk memastikan perusahaan dalam kondisi aman.

Identity and Access Management

Diperlukan identifikasi dan verifikasi pengguna yang memasuki jaringan dengan keandalan tinggi. Otentikasi terpusat harus mencakup *Single Sign-On* (SSO), manajemen sertifikat, dan manajemen tamu. *Multi Factor Authentication* (MFA) mengkonfirmasi identitas dengan faktor kedua.



Gambar 6. Comparison Security Method VPN and ZTNA



Gambar 7. Identity Access Management

Remote Access and Application Access

Solusi Fortinet ZTNA memberikan akses per sesi ke aplikasi individual hanya setelah perangkat dan pengguna diverifikasi. Kebijakan ini juga diterapkan saat pengguna berada di jaringan baik itu di dalam atau pun di luar perusahaan, serta mengaktifkan model policy *zero trust* yang sama di mana pun lokasi pengguna.

Zero Trust Network Access Use Case Aruba Clearpass

Clearpass merupakan salah satu produk *zero trust security* Aruba yang dikenal dengan *network access control* (NAC) yang fokus untuk pengamanan akses / koneksi pengguna dan perangkat ke jaringan perusahaan baik lewat kabel, nirkabel, atau pun VPN, di manapun tidak terbatas lokasi pengguna. Semua pengguna dan perangkat mendapatkan kebijakan yang sesuai dengan peran saat terkoneksi. Secara umum *clearpass* melakukan tiga mekanisme yaitu identifikasi (autentikasi dan otorisasi), *action* (kebijakan) dan Proteksi (kontrol kebijakan dinamis).

Solusi *Aruba's zero-trust security* menyediakan perimeter keamanan yang menyeluruh. Mulai dari keamanan di dalam maupun di luar jaringan perusahaan termasuk keamanan untuk perangkat jarak jauh, seluler, dan IoT.

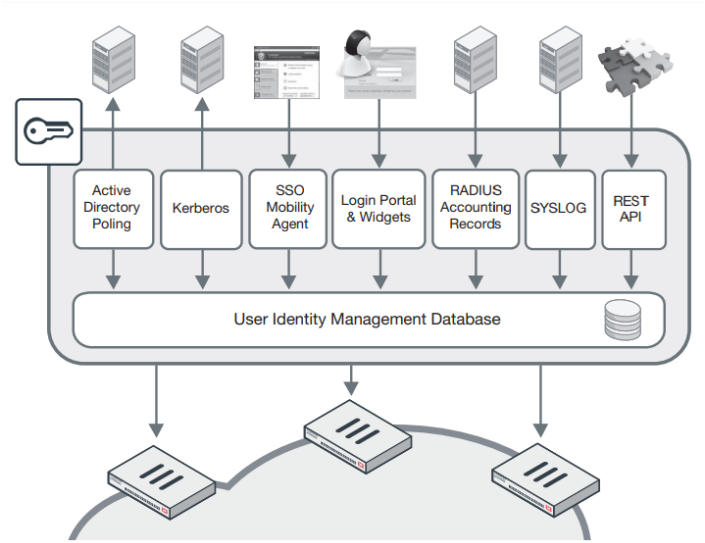
Aruba's zero-trust security solution menyediakan akses aman ke aplikasi dan sumber daya dengan kombinasi teknologi yang unik, termasuk 802.1X, MACSec, dan virtual private LAN service (VPLS), Virtual Extensible LAN (VXLAN), Dynamic Access Control.

Penerapan Industri Aruba Clearpass

Aruba's clearpass zero trust security solution sangat ideal untuk perusahaan, pendidikan, perawatan kesehatan, layanan keuangan dan sektor publik. Selain itu teknologi bisa diterapkan pada industri ritel, perhotelan dan transportasi.

Keuntungan Penerapan Teknologi Solusi Aruba's Zero Trust Security

- Keamanan akses jarak jauh ke sumber daya perusahaan untuk karyawan dan tamu.
- Kebijakan berbasis identitas, lokasi dan waktu untuk menerapkan pengamanan berdasarkan siapa dan apa yang diakses dari sumber daya perusahaan.
- Melindungi dari infeksi malware dan ancaman lainnya dengan hanya mengizinkan perangkat tepercaya mengakses sumber daya perusahaan. Juga, menghilangkan kebutuhan akan VPN dan infrastruktur keamanan mahal lainnya.
- Mengenkripsi komunikasi antara perangkat nirkabel dan pengontrol, melindungi dari penyadapan dan gangguan data.
- Menyediakan kemampuan untuk memperluas LAN di luar batas fisik bangunan ke pengguna atau perangkat jarak jauh.



Gambar 8. ZTNA Access Policy

Aruba ESP: Core Zero Trust Principles

Zero Trust sangat bervariasi tergantung pada domain mana keamanan sedang dipertimbangkan. Meski pun level aplikasi kontrol telah menjadi titik fokus dalam *zero trust*, sebuah strategi yang komprehensif juga harus mencakup keamanan jaringan dan semakin banyaknya perangkat yang terhubung, termasuk lingkungan kerja hybrid. Aruba ESP dengan Keamanan *Edge-to-Cloud* menggabungkan visibilitas yang komprehensif, memiliki segmentasi dan kontrol akses paling rendah, serta pemantauan berkelanjutan dan penegakan. Bahkan solusi VPN tradisional ditingkatkan dengan memastikan bahwa kontrol yang sama diterapkan ke kampus atau jaringan cabang, juga meluas ke lokasi terpencil dan pekerja lapangan.

Di era IoT, prinsip dasar keamanan jaringan yang baik seringkali sulit untuk diterapkan. Jika memungkinkan, semua perangkat dan pengguna harus diidentifikasi dan diautentikasi dengan benar sebelum memberikan mereka akses jaringan. Selain otentikasi, pengguna dan perangkat harus diberikan paling sedikit akses yang diperlukan untuk melakukan aktivitas bisnis penting mereka setelah mereka berada di jaringan. Ini berarti otorisasi sumber daya jaringan dan aplikasi setiap pengguna atau perangkat tertentu dapat diakses. Akhirnya, semua komunikasi antara pengguna akhir dan aplikasi harus dienkripsi.

Gambar 9. Core Zero Trust Principles

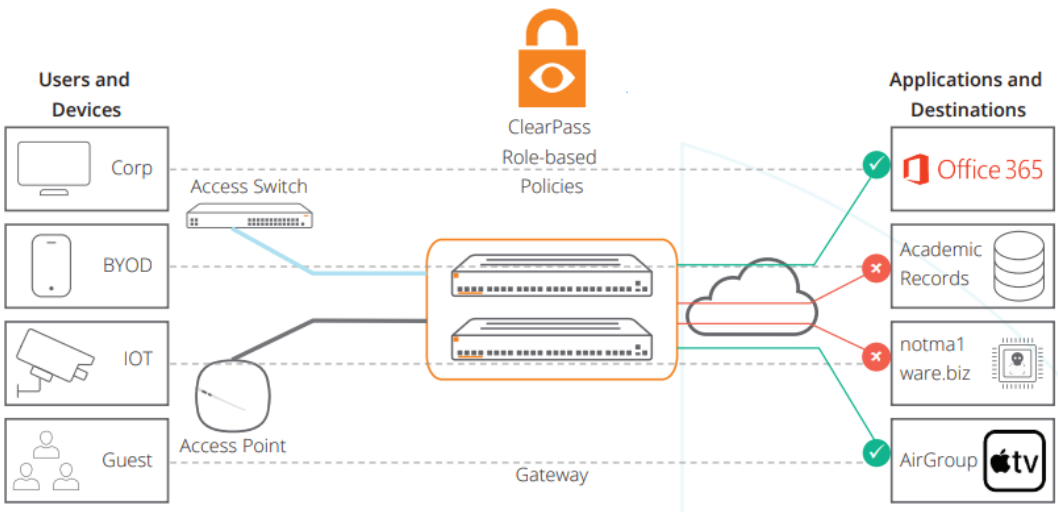
The Need For Comprehensive Visibility

Dengan peningkatan adopsi IoT, visibilitas semua perangkat dan pengguna di jaringan telah menjadi tugas yang semakin menantang. Tanpa visibilitas *zero trust* akan sulit untuk diterapkan. Otomatisasi, pembelajaran mesin berbasis *Artificial Intelligence* (AI), dan kemampuan untuk cepat mengidenfikasi jenis perangkat menjadi sangat penting.

Sebagai solusi manajemen jaringan berbasis cloud, Aruba Central mencakup visibilitas dan profil yang didukung AI dengan Wawasan Klien. *Client Insights* memanfaatkan infrastruktur asli telemetri dari *access point*, *switch*, dan *gateway* dari klien tanpa memerlukan instalasi fisik kolektor atau agen. Model klasifikasi berbasis *machine learning* (ML) digunakan untuk sidik jari, mengidentifikasi, dan secara akurat membuat profil berbagai macam klien, termasuk beragam perangkat IoT di seluruh infrastruktur kabel dan nirkabel. Untuk lingkungan yang tidak dikelola oleh Aruba Central atau untuk lingkungan dengan perangkat jaringan pihak ketiga, *ClearPass Device Insight* (CPDI) dapat dimanfaatkan untuk identifikasi dan profil klien berbasis ML.

Authentication

Setelah pengguna atau perangkat diketahui dan diprofilkan, langkah selanjutnya adalah untuk mengotentikasi identitasnya setiap kali terhubung ke jaringan. Dengan *ClearPass*, organisasi dapat menggunakan kabel atau nirkabel menerapkan penegakan standar 802.1X untuk otentikasi keamanan. *ClearPass* juga mendukung alamat MAC otentikasi untuk IoT dan perangkat non user device yang mungkin kurang dukungan untuk otentikasi menggunakan standar 802.1X. Untuk lingkungan yang berbasis koneksi kabel di mana RADIUS otentikasi tidak dapat diterapkan, ClearPass menawarkan alternatif menggunakan penegakan berbasis SNMP. Beberapa metode otentikasi dapat digunakan secara bersamaan pada berbagai kasus penggunaan termasuk dukungan untuk multifactor otentikasi berdasarkan waktu masuk, pemeriksaan postur, dan konteks lain seperti pengguna baru, perangkat baru, dan lainnya.



Gambar 10. Trust Enforced Dynamic Segmentation by Aruba Clearpass

Adopting "Least Access" And Identity-Based Access Control

Setelah visibilitas tersedia, menerapkan praktik terbaik *Zero Trust* terkait dengan "Akses Terkecil" dan kontrol akses berbasis identitas adalah langkah kritis berikutnya. Ini berarti menerapkan kebijakan kontrol akses yang hanya mengotorisasi akses ke sumber daya yang benar-benar diperlukan untuk perangkat atau pengguna tersebut.

***Aruba Dynamic Segmentation*,** memastikan bahwa pengguna dan perangkat secara otomatis diberi kebijakan kontrol akses yang tepat sehingga mereka hanya dapat berkomunikasi dengan tujuan yang konsisten dengan peran mereka. Segmentasi Dinamis yang mendukung dua penegakan model yaitu terpusat dan terdistribusi, memungkinkan teknologi informasi (TI) untuk menggunakan salah satu atau kedua model tersebut berdasarkan kebutuhan lingkungan. Dengan Segmentasi Dinamis terpusat, lalu lintas tetap aman dan terpisah dengan penggunaan terowongan GRE antara *access point* dan Aruba *Gateways* (atau *Mobility Controller*). Aruba ClearPass Manajer Kebijakan memungkinkan pembuatan akses berbasis peran kebijakan yang mengikuti pengguna di seluruh jaringan dan diterapkan secara seragam di seluruh koneksi nirkabel, kabel, dan VPN. Penegakan disediakan oleh *Firewall* Penegakan Kebijakan Aruba (PEF), *firewall* aplikasi lengkap yang tertanam di Aruba infrastruktur jaringan.

***Aruba Central NetConductor*,** memungkinkan segmentasi dinamis terdistribusi menggunakan protokol yang diadopsi secara luas seperti EVPN/VXLAN untuk menghasilkan *overlay* jaringan terdistribusi. Pusat NetConductor menawarkan layanan keamanan *cloud-native* untuk global manajemen kebijakan dan konfigurasi jaringan dengan sederhana antarmuka logika bisnis dan alur kerja intuitif.

Pengidentifikasi kebijakan global yang mencerminkan peran dan izin akses dari pengguna atau perangkat tertanam di *header* paket dan ditafsirkan sejalan oleh *switch* dan *gateway* Aruba CX untuk kebijakan pelaksanaan.

CONTINUOUS MONITORING AND ENFORCEMENT

Dengan kontrol akses berbasis peran untuk menerapkan granular segmentasi, pemantauan berkelanjutan terhadap pengguna dan perangkat di jaringan membuat praktik terbaik *Zero Trust* lainnya. Ini mengatasi risiko yang terkait dengan ancaman orang dalam, malware tingkat lanjut, atau ancaman terus-menerus yang telah menghindari tradisional pertahanan perimeter.

Threat Defense with IDS/IPS

Kemampuan pertahanan ancaman Aruba bertahan melawan segudang ancaman, termasuk *phishing*, penolakan layanan (DoS), dan serangan ransomware yang semakin meluas. Gateway SDWAN yang didukung melakukan deteksi intrusi berbasis identitas dan pencegahan (IDS/IPS), bekerja sama dengan *Aruba Central, ClearPass,* dan *Firewall* Penegakan Kebijakan. IDS/IPS berbasis identitas melakukan pemeriksaan lalu lintas berbasis pola dan *signature* pada LAN kantor cabang, serta lalu lintas SD-WAN mengalir melalui *gateway* untuk mengamankan jaringan.

360 Security Exchange

Dengan lebih dari 150 integrasi yang terdiri dari keamanan terbaik solusi yang mencakup Operasi dan Respons Keamanan (SOAR), *ClearPass* mampu menegakkan secara dinamis akses berdasarkan telemetri ancaman *real-time* yang berasal dari berbagai sumber. Kebijakan dapat dibuat untuk membuat keputusan kontrol akses berdasarkan peringatan yang datang dari *Next-Gen Firewalls* (NGFW), *Security Information and Event Management* (SIEM), dan banyak sumber lainnya. Tindakan *ClearPass* sepenuhnya dapat dikonfigurasi dari membatasi akses (mis. Internet saja), menghapus perangkat sepenuhnya dari jaringan untuk perbaikan.

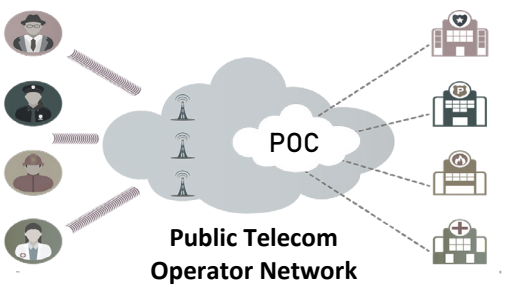
Hytera

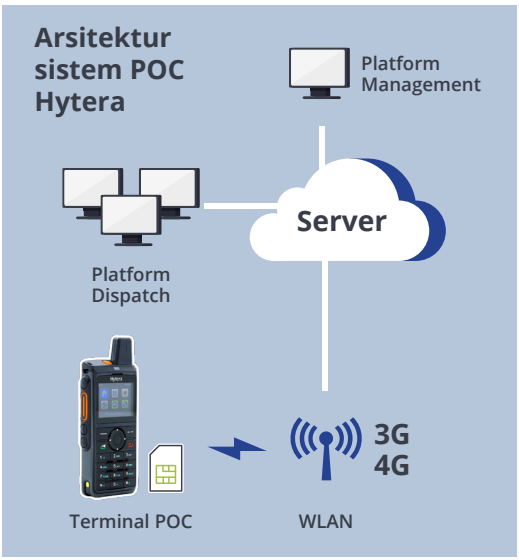
POC (Push-to-talk Over Cellular) Solution

Hytera adalah perusahaan pemimpin global dalam komunikasi radio dua arah, yang mengembangkan dan membuat solusi inovatif untuk menangani beragam situasi komunikasi. Hytera memiliki reputasi sistem yang berkualitas tinggi, andal, serta kaya fitur. Anda dapat menemukan Hytera di seluruh dunia, mulai dari metro Shenzhen hingga Pelabuhan Tanjung Priok, sampai bandara Balikpapan, jaringan kereta api, pusat konferensi, serta lokasi konstruksi.

POC (*Push-to-talk Over Cellular*)

Komunikasi *push-to-talk* (PTT) telah terbukti efisien dan dapat diandalkan di dunia bisnis selama puluhan tahun. Dengan pesatnya perkembangan jaringan broadband seluler, kini tuntutan dari pengguna PTT untuk layanan multimedia padat data makin tinggi, seperti gambar dan video yang tidak dapat dipenuhi oleh sistem radio narrowband lama. Memanfaatkan jaringan broadband yang sudah mapan, solusi *Push-To-Talk Over Cellular* (PoC) dari Hytera menyediakan suara PTT dan data bervolume besar dalam cakupan nasional tanpa perlu investasi tambahan dalam hal infrastruktur nirkabel.





Solusi Hytera HyTalk

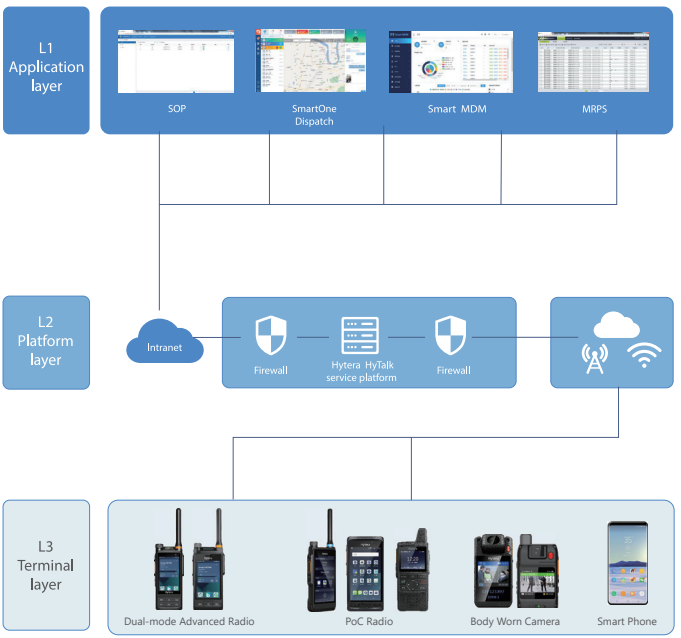
Solusi Hytera HyTalk terdiri dari platform layanan Hytera HyTalk, peralatan pengguna (radio PoC, ponsel pintar, dan lain-lain.), Platform Operasi Layanan (SOP), Platform Pengiriman (*SmartOne Dispatch*), Platform Manajemen Perangkat Seluler (*Smart* MDM), Sistem Perekaman dan Pemutaran Multimedia (MRPS). Solusi Hytera HyTalk dapat digunakan pada 3G publik, 4G, jaringan WLAN, serta jaringan LTE pribadi.

Radio PoC PNC380

Radio PoC Hytera PNC380 memadukan komunikasi instan dan aplikasi multimedia ke dalam satu perangkat. Melalui jaringan 2G, 3G, 4G, dan WLAN, perangkat ini menyediakan layanan data multimedia lengkap, seperti transmisi video 4G, berbagi lokasi, dan pesan instan. PNC380 masih mempertahankan tombol PTT berukuran besar yang berasal dari radio dua arah tradisional, PNC380 menawarkan komunikasi suara *one-to-one user* (satu ke satu) dan *one-to-many* (satu ke banyak) dalam seketika. Radio ini juga menghadirkan audio berkualitas *volume* tinggi namun jernih, tombol darurat khusus, serta baterai 4.000 mAh yang mampu bertahan seharian. Kokoh serta tahan lama, radio ini ideal untuk berbagai skenario aplikasi, seperti manajemen kota, keamanan properti, logistik, acara besar, kompleks industri, bandara, dan lapangan kerja Anda yang beragam.

Radio 5G PNC560

PNC560 memberikan dua hal terbaik kepada Anda yaitu radio PTT profesional dan ponsel cerdas produktivitas yang tangguh. Perangkat ini memberikan *mission-critical push-to-talk* (MCPTT) kepada Anda dengan jaringan 5G/LTE yang memiliki kecepatan super cepat dan latensi rendah, memungkinkan komunikasi dan kolaborasi tim dengan hanya perlu menekan tombol. PNC560 Berfungsi meningkatkan produktivitas Anda. Dengan desain dan spesifikasi tercanggih dalam industri radio seluler, PNC560 memungkinkan pengoperasian yang andal dan efisien untuk digunakan dalam beragam penggunaan di lapangan yang dapat Anda gunakan sebagai mitra paling terpercaya dalam menjalankan misi.



Aplikasi Industri

Dengan pesatnya perkembangan ekonomi sosial, konten pekerjaan sehari-hari dan lingkungan kerja pengguna industri semakin beragam dan rumit merupakan tuntutan terbaru dari pengguna PTT untuk semakin efisien.

Solusi Hytera HyTalk sangat cocok untuk mendukung industri:

- Perhotelan
- Katering
- Logistik
- Transportasi
- Layanan Komersil (Ojek Online)
- Properti, dan lain-lain.

Saksikan video podcast ACS Group yang membahas "ACS Group Cyber Security: NGFW To EDR | Eps. 12" di channel Youtube kami.

Scan this QRcode

SUBSCRIBE

PT Autojaya Idetech &
PT Solusi Periferal (ACS Group)

THINGS THAT WILL YOU DISCOVER.

- Podcast
- Case Study
- Product Highlight
- Unboxing & Tutorial

... etc.

Dan jangan lupa juga ikuti update-an info terbaru di instagram kami

@acsgroup.co.id Follow

New Product | Tips & Info | Quiz | etc

Training SAT PM75

22 Juni 2022

ACS Group sekali lagi diberikan kepercayaan oleh Alfamart untuk menyediakan produk Mobile Computer, yang sebelumnya telah sukses dengan unit Point Mobile PM80nya, kini diganti dengan unit terbaru yaitu Point Mobile PM75. Diharapkan nantinya dapat kembali sukses memenuhi kebutuhan operasional Alfamart.

Tentunya ACS Group bertanggung jawab untuk memberikan pelatihan, pembekalan dan pendampingan sebelum PM75 ini digunakan secara menyeluruh untuk kegiatan operasional Alfamart.

Team engineer Agung Atmoko dan Bimo Jati Utomo, dan Tju Hansel (Sales ACS Jakarta) telah memberikan training kepada 23 peserta dari team

IC (*Inventory Control*) Alfamart yang berlokasi di Bandar Djakarta Alam Sutera, Tangerang.

Kegiatan tersebut meliputi :

- Presentasi deskripsi produk Point Mobile PM75, unboxing unit beserta aksesori, menjelaskan fitur-fitur terbaru yang disematkan pada unit tersebut, serta tips penggunaan dan pemeliharaan.
- Tanya jawab terkait penggunaan PM75, *after sales services*, *issue* yang dihadapi user pada saat operasional, serta masukan dan harapan dari user kepada ACS Group kedepannya.

Hybrid Event

#FactoriesSecret

Securing Your OT Digitalization

20 Juli 2022

ACS Group kembali menyelenggarakan event dengan tema #FactoriesSecret "Securing Your OT Digitalization" secara Hybrid (Offline dan Online). Acara offline diadakan di Hotel Mercure Karawang Barat dan berkolaborasi dengan VST ECS (Platinum Distributor Fortinet) dan FORTINET Principle.

Acara yang dihadiri kurang lebih 50 orang peserta ini, terdiri dari para Praktisi IT (*Information Technology)* dan OT (*Operation Technology*) dari berbagai kota yaitu DKI Jakarta, Karawang, Bekasi serta Purwakarta.

Suprianto Kusman, ACS Group

Event dibuka oleh Branch Manager ACS Group Cikarang Suprianto Kusman. Beliau menyampaikan rasa bahagianya setelah 3 tahun lamanya akhirnya dapat berkumpul serta bertatap muka kembali dengan para customer dan menyampaikan pula tentang pentingnya Cyber Security untuk Area Operation di manufaktur.

Alan Rantelino, Fortinet

Dua pembicara lainnya di event ini antara lain dari Fortinet yaitu Alan Rantelino sebagai OT Business Development Manager dan dari VST ECS yaitu Charles sebagai Technical Consultant. Alan Rantelino mempresentasikan solusi dan penerapan Cyber Security di Operation Technology Manufacture yang relevan dengan

program pemerintah yaitu menuju Indonesia 4.0. Lebih detail Alan memaparkan teknologi ini sebagai solusi tepat guna untuk mengamankan mesin-mesin produksi yang telah terdigitalisasi dan sangat penting bagi kegiatan perusahaan. Karena begitu pentingnya Cyber Security untuk area OT, maka ada istilah "Loss of Information in IT and loss of life in OT".

Disamping itu Charles memaparkan pula secara teknis bagaimana implementasi Cyber Security dari Fortinet dapat saling terintegrasi dengan sistem kendali dari mesin-mesin existing seperti Scada, PLC, HMI, dan lain-lain yang ada di suatu perusahaan. Sebagai salah satu perusahaan Solution Provider ACS Group (*Indonesia's Trusted Professional IT Solution*), kami berkomitmen siap membantu kebutuhan dalam hal pengembangan digital transformation Industry 4.0 untuk semua perusahaan manufaktur, terutama pada Segmen Cyber Security. Fortinet adalah solusi yang tepat dimana semua yang dibutuhkan sudah ada di dalam satu platform Fortinet ini, *and only vendor recognized as a Leader across both SD-WAN and Netwrok Firewall.*

ACS Group x VSTECS x FORTINET selalu berusaha memberikan solusi serta support atau after sales yang terbaik untuk perkembangan IT dan OT di Indonesia secara umum dan khususnya perusahaan manufaktur.

Charles, VST ECS

Virtual Event

#IAmSecure

Securing your Infra to App at Cloud

24 Agustus 2022

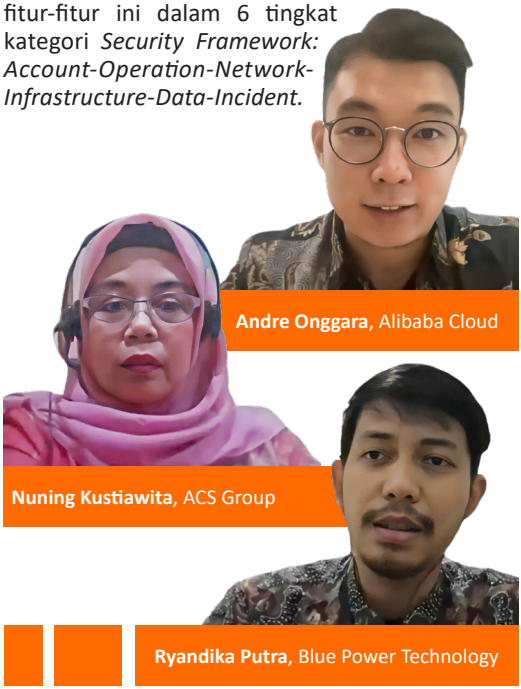
Era digitalisasi telah tiba di Indonesia dan *cloud technology* memainkan peran besar dalam transformasi ini. Pernyataan ini didukung oleh penelitian yang dilakukan oleh IDC pada tahun 2021, yang memprediksi meningkatnya kebutuhan pasar Indonesia akan *public cloud services*. Teknologi *Cloud Computing* menjadi salah satu solusi yang populer saat ini. Teknologi ini memungkinkan pelaku bisnis untuk menyewa tempat beserta jasa layanannya tanpa perlu memikirkan biaya *overhead* terselubung untuk pengelolaannya (*maintenance*). Keamanan juga merupakan suatu aspek penting yang disediakan *cloud provider* secara berlapis, baik dari segi fisik yang tercermin dari SLA, maupun digital.

ACS Group, bersama dengan Alibaba Cloud dan Blue Power Technology, mengadakan webinar #IAmSecure pada tanggal 24 Agustus 2022.

Pembicara pertama dalam event ini, Ibu Nuning Kustiawita selaku Sales Manager ACS Group, membawakan penyegaran materi webinar sebelumnya, #Cloudology, perihal keuntungan yang bisa didapatkan dari implementasi Cloud. Kemudian beliau menjelaskan faktor-faktor umum yang seringkali membuat pelaku usaha ragu-ragu dalam mengadopsi *cloud solution* dalam proses bisnisnya. Pengantar untuk *Shared Responsibility Model* juga disampaikan, yang kemudian dibahas lebih dalam oleh Bapak Andre Onggara selaku Channel Business Development dari Alibaba Cloud.

Unsur-unsur lain yang perlu diketahui *end-user* atau pelaku bisnis adalah manfaat fitur-fitur yang telah disediakan Alibaba Cloud. Dibutuhkan pengetahuan yang mumpuni perihal bagaimana suatu *attack surface* itu terbentuk dan pemilihan *partner*/vendor yang dapat memberikan konsultasi agar implementasi layer keamanan tepat guna. Komitmen Alibaba Cloud pada keamanan, spesifiknya pada pasar Indonesia, dibuktikan dengan berbagai sertifikasi *compliance* keamanan skala internasional dan tersedianya 3 Data Center yang sudah beroperasi di Indonesia. Alibaba Cloud juga memiliki *Scrubbing Center* yang independen yang dikhususkan untuk memitigasi ancaman DDoS yang marak terjadi akibat terbukanya akses jaringan perusahaan ke internet.

Bapak Ryandika Putra menutup sesi materi dengan pemaparan *instance-instance* atau produk yang tersedia di *console* Alibaba Cloud. Beliau membahas celah-celah serangan yang perlu diperhatikan pelaku usaha yang ingin dengan aman mengadopsi Cloud untuk server, ERP, aplikasi, penyimpanan data, *media content delivery*, dan lain-lain. Alibaba Cloud membungkus fitur-fitur ini dalam 6 tingkat kategori *Security Framework: Account-Operation-Network-Infrastructure-Data-Incident.*



Zebra Technologies

ET8X Series Rugged 2-IN-1 Windows Tablets

Industri : Transportation, Manufacturing & Field Mobility

Zebra ET8x Series merupakan tablet Windows 2-in-1 yang tipis, ringan dan rugged dibandingkan dengan tablet sejenis yang ada di pasaran. Tablet ini mendukung Wi-Fi 6E dan 5G atau 4G.

Screen 12 inci dengan rasio aspek 3:2 ini mudah dilihat baik di dalam maupun di luar ruangan, bahkan di bawah sinar matahari yang cerah. Layarnya dapat disentuh saat kondisi basah atau menggunakan sarung tangan. Produk ini dilengkapi dengan pemindai bar code serta Baterai PowerPrecision+ yang memberikan banyak informasi untuk kesehatan baterai yang dapat dilihat langsung pada tablet tersebut.

Zebra Technologies

L10 Rugged Tablet

Industri : Field Mobility, Warehouse Management, Transportation, & Manufacturing

Zebra Technologies mengeluarkan Tablet Rugged Android L10 untuk memenuhi kebutuhan pekerja di lapangan seperti di area minyak dan gas, pertambangan, telekomunikasi, konstruksi dan militer maupun di gudang dan pabrik. Tablet 10,1 inci ini memiliki 500 nit yang cerah dan mudah dilihat di hampir semua kondisi pencahayaan, bahkan dengan opsi layar View Anywhere® 1000 nit yang dapat dibaca di bawah sinar matahari langsung. L10 ini dapat meng-*capture* barcode 1D/2D serta memiliki ketahanan baterai sepanjang waktu dengan sekali pengisian daya, ditambah koneksi nirkabel yan cepat seperti WiFi, Bluetooth, seluler, GPS, dan NFC. Tahan terhadap air, debu, serta tahan benturan dan mampu beroperasi di suhu yang sangat panas, di bawah 0°, atau di lingkungan yang memiliki bahan berbahaya sekalipun.

Tanpa biaya tambahan, dengan *Push-to-Talk Express* pekerja Anda mendapatkan kemampuan *push-to-talk* instan melalui jaringan WiFi yang ada.

Zebra Technologies

ET4X Series Enterprise Tablets

Industri : Retail, Hospitality, Transportation, & Healthcare

Tablet ET4X Series dirancang sebagai produk yang tahan lama untuk bisnis dari dalam ke luar. Memiliki ukuran layar 8 inci atau 10 inci yang mudah dibawa-bawa serta dilengkapi kamera belakang ultra-detail yang dapat mengcapture foto sekaligus memindai barcode dalam segala kondisi. Tablet ini mendukung koneksi nirkabel terbaru dan tercepat — termasuk Wi-Fi 6 dan 5G. Anda dapat dengan mudah berkolaborasi dengan push-to-talk instan dan pesan teks yang aman melalui Workforce Connect PTT Pro opsional Zebra

Zebra Technologies

ET5X Series Tablet Computer

Industri : Retail, Manufacturing, Warehouse Management, Transportation, & Healthcare

Tablet Android™ ET5X Series adalah komputer tablet Zebra yang paling tipis dan paling ringan sehingga memudahkan para pekerja untuk melakukan pengambilan data, dan meningkatkan fleksibilitas kegiatan operasional. Tablet dengan model layar 8,4" dan 10.1" ini sudah dilengkapi pemindai bar code 1D/2D yang terintegrasi,

Dilengkapi pula dengan berbagai fitur untuk meningkatkan kapasitas, kecepatan, dan jangkauan jaringan WiFi dengan 2x2 *Multi-User*, *Multiple Input*, *Multiple Output* (MU-MIMO) yang memungkinkan Access Point dapat berkomunikasi dengan beberapa perangkat secara bersamaan.

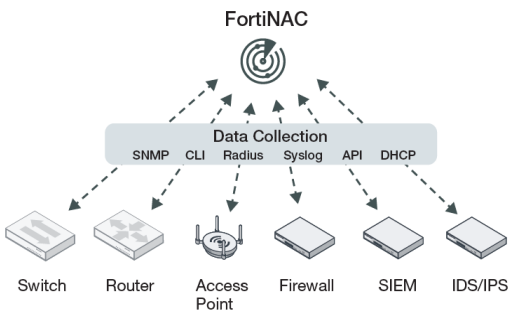
Produk yang rugged ini siap digunakan baik di dalam maupun di luar, tahan terhadap benturan, terkena hujan, salju, tumpahan cairan bahkan semprotan air yang kuat, debu, tahan suhu panas yang ekstrim serta mampu digunakan pada suhu di bawah 0°.

Fortinet

FortiNAC™

Industri : Semua industri.

Network access control (NAC) adalah solusi akses ke jaringan perusahaan dengan konsep *zero-trust* yang memberi visibilitas mengenai perangkat dan pengguna bahkan hingga terhadap perangkat *Internet of Things* (IoT) yang semakin meningkat perkembangannya. Dengan Solusi NAC, pengguna, aplikasi, atau perangkat yang mencoba mengakses jaringan harus diverifikasi terlebih dahulu, dan dengan mudah mengetahui apa dan siapa yang mengakses jaringan, serta bagaimana melindungi aset perusahaan baik di dalam maupun di luar jaringan.



FortiNAC™ adalah solusi modern dari Fortinet dalam *network access control* yang meningkatkan integrasi keamanan *Security Fabric* dengan visibilitas, kontrol dan respon secara automasi terhadap semua hal yang terhubung dengan jaringan. **FortiNAC™** menyediakan perlindungan terhadap IoT *threats*, meningkatkan kontrol terhadap perangkat *third-party*, dan orkestrasi respon secara automasi terhadap sejumlah *event* yang terjadi di jaringan.

- **Visibilitas pada setiap perangkat dan pengguna dijaringan** FortiNAC memberikan *profiling* yang detail terhadap perangkat menggunakan sejumlah informasi dan sumber-sumber *behavior* untuk mengidentifikasi secara akurat mengenai apa yang ada dalam jaringan.
- **Kontrol yang lebih lanjut terhadap *Third-Party Products* dalam jaringan** Dengan implementasi *micro-segmentation policies* dan perubahan

konfigurasi pada produk *switch* dan *wireless products* terhadap lebih dari 70 vendor, hal ini memperluas jangkauan *Security Fabric* dalam lingkungan jaringan yang heterogen.

- **Respon secara automatis terhadap *event*** yang terjadi di jaringan dengan cepat untuk mencegah serangan *threats* sebelum menyebar lebih luas. FortiNAC menawarkan secara luas sejumlah *policy* automasi yang akan secara langsung memicu perubahan konfigurasi terhadap observasi perilaku yang dipantau.

Fortinet

FortiAuthenticator™

User Identity Management and Single Sign-On

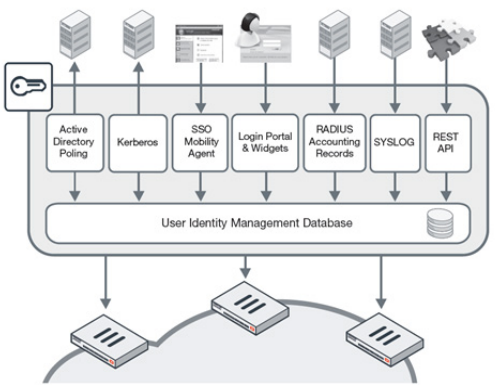
Industri : Semua industri.

Konsep *Zero Trust Access (ZTA)* adalah tersedianya akses yang aman terhadap setiap perangkat, pengguna, konteks, dan faktor-faktor lainnya yang harus diverifikasi terlebih dahulu dengan baik dan benar melalui proses otentikasi.

FortiAuthenticator adalah produk manajemen identitas dari Fortinet yang menyediakan kemampuan otentikasi yang handal dan otorisasi terhadap jaringan kabel dan jaringan nirkabel. Produk ini menyediakan akses yang aman bagi para pengguna, baik dari internal maupun eksternal, untuk mengakses aplikasi dan sumber daya lainnya yang terdapat dalam jaringan. Dilengkapi dengan opsi pilihan *two-factor authentication* menggunakan *token* dari Fortinet ataupun *token non*-Fortinet (RSA). Produk ini juga memanfaatkan **X.509 certificate** untuk proses ototentikasi yang handal sebagai persyaratan yang banyak diterapkan dalam lembaga *keuangan* dan *healthcare*.

Kapabilitas FortiAuthenticator meliputi:

- Kemampuan untuk mengidentifikasi pengguna jaringan secara transparan dan menegakkan kebijakan berbasis identitas pada jaringan perusahaan yang mendukung Fortinet
- Proses otentikasi *two-factor authentication* maupun OTP (*one-time password*) *authentication* yang aman dan lancar dengan FortiToken
- Manajemen sertifikat untuk penerapan keamanan terhadap jaringan nirkabel dan akses VPN
- Manajemen akses tamu untuk keamanan jaringan kabel dan jaringan nirkabel dalam organisasi perusahaan
- Kemampuan *Single Sign On* untuk jaringan internal dan cloud



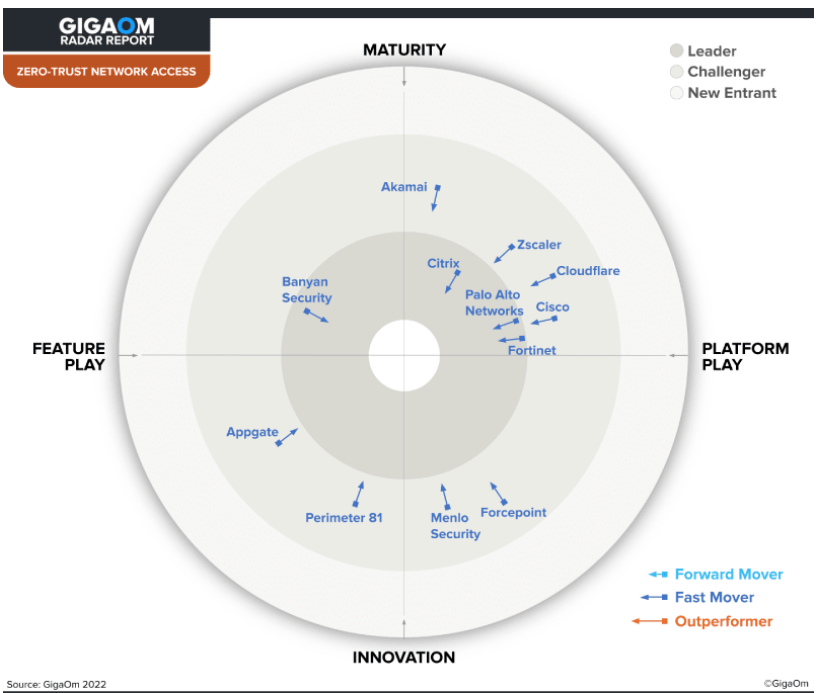
Untuk penjelasan lebih detail lagi anda dapat menghubungi fitur chat kami di www.acsgroup.co.id.

Fortinet diakui sebagai Leader dalam GigaOm Radar Report

Solusi ***Zero Trust Network Access*** **(ZTNA)** dari **Fortinet** diakui oleh **GigaOm Radar Report** sebagai pemimpin atau ***Leader*** radar dalam laporan terbaru 2022 ini. GigaOm adalah firma analis dan perusahaan media yang berfokus pada teknologi dimana GigaOm berevolusi dari *blog* yang menawarkan berita, analisis, dan opini tentang perusahaan rintisan, teknologi baru, dan topik terkait teknologi lainnya hingga menjadi satu-satunya perusahaan firma riset yang menyediakan *tools* mulai dari informasi hingga pengetahuan, pemecahan masalah sampai solusi, serta bagaimana menerapkannya.

Solusi ZTNA dari Fortinet yang universal terintegrasi dengan perangkat ***FortiGate Firewall Next Generation*** untuk menghadirkan *deployment* yang cepat dan biaya TCO (*total cost ownership*) terendah serta mendukung opsi *cloud-based*, *on-premise* serta SASE (*Secure Access Service Edge*). Universal ZTNA Fortinet memanfaatkan ***Fortinet Security Fabric*** untuk meningkatkan penerapan ZTNA dengan elemen keamanan seperti UEBA (*User and Entity Behavior Analytics*) atau MFA (*Multi-Factor Authentication*) dari Fortinet dan berbagai vendor pihak ketiga.

Fortinet juga diakui karena dukungan yang kuat untuk aplikasi *legacy*, seperti RDP, SSH, Telnet, FTP, SMB, dan protokol berbasis TCP lainnya, dan terus menambahkan dukungan protokol tambahan lainnya. Selain itu, kemampuan pemantauan sesi yang kuat juga tersedia dengan *tools Fortinet Security Fabric*.



Awards PT Autojaya Idetech

Di tahun 2021, ekonomi dan pergerakan kegiatan perusahaan masih mengalami hambatan karena pandemi yang masih melanda Indonesia. Namun atas berkat Tuhan, ACS Group masih diberikan kepercayaan oleh customer untuk bekerjasama dalam memberikan solusi tepat guna untuk efesiensi dan efektivitas kegiatan bisnis perusahaan mereka.

Hasil kerja keras dan kesungguhan dalam melayani para customer, ACS Group mendapatkan beberapa penghargaan yang diberikan oleh principal:

Zebra Technologies Award 2021
Strategic Win (EVM) Partner of The Year 2021.
PT. AUTOJAYA IDETECH in recognition of outstanding performance, achievements, and dedication to Zebra Technologies.

Zebra Technologies Award 2021
RFID Partner of The Year.
PT. AUTOJAYA IDETECH in recognition of outstanding performance, achievements, and dedication to Zebra Technologies.

Point Mobile Award 2021
Platinum Award Partner.
PT. AUTOJAYA IDETECH in recognition of outstanding performance, achievements, and dedication for Point Mobile.

Ingram Micro Award 2021, Top AIDC Partner 2021.
PT. AUTOJAYA IDETECH won the “Top AIDC Partner 2021” from Ingram Micro, the leading global IT distribution company.

BULAN MADU BERBINTANG

Sepasang suami istri yang baru saja menikah merayakan bulan madu mereka dengan mendaki gunung.

Setelah mencapai tempat yang dituju dan membangun tenda serta makan malam bersama mereka pun tertidur karena kelelahan setelah pendakian...

Sekitar pukul dua pagi, sang istri terbangun dan membangunkan sang suami dan berkata kepadanya:

I: Sayangku... Apakah kamu melihat bintang-bintang itu?

S: Ya tentu saja seperti kamu lihat kan?? ...

I: Apa yang kamu simpulkan sayang?

S: Yah, saya dapat katakan bahwa, dari sudut pandang astrologi, yang kita miliki di utara ada bintang yang disebut dalam bahasa Latin “ursa mayor” sebagai bintang yang paling terang. Dari sudut pandang teknis, setidaknya ada jutaan planet dan ribuan galaksi... Dari sudut pandang teologis, saya akan mengatakan bahwa Tuhan Maha kuasa karena telah menciptakan keindahan yang sempurna ini dan, dari dari sudut pandang logis, saya akan mengatakan bahwa ini adalah malam dan kita harus tidur lagi ya untuk lanjutkan perjalanan...

Sang istri menatapnya dengan rasa kasihan dan berkata:

I: Sayang! kamu tau nggak...

S: Nggak !!, ada apa sayang??

I: Ada yang curi tenda kita tauu...! (geram sang istri..)

KOLOM KETAWA

Tips & Info mengenai

Mengamankan Jaringan dengan Solusi Network Access Control (NAC)

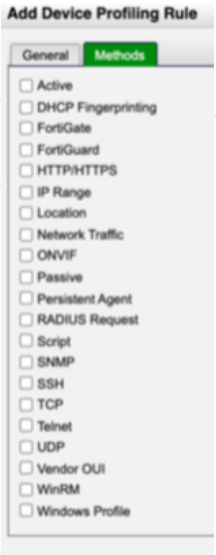
Pengamanan terhadap jaringan dimulai dengan bagaimana pengaturan terhadap perangkat dan pengguna yang akan terhubung dan mendapatkan akses sumber daya di jaringan. Dengan solusi *Network Access Control* maka perangkat dan pengguna akan diverikasi terlebih dahulu dengan melakukan proses **otentikasi dan otorisasi** saat akan masuk ke dalam jaringan.

Setelah proses ***authentication* dan *authorization*** itu, maka akan didapatkan **visibilitas** pada semua yang terhubung dalam jaringan. Visibilitas didapat dengan adanya kemampuan metode *discovery* terhadap pengguna, aplikasi dan perangkat. Teknik mendapatkan profil ini antara lain dengan metode DHCP Fingerprinting, protokol SNMP, RADIUS request dan sebagainya.

Dengan adanya visibiltas maka didapatkan **kontrol terhadap perangkat dan pengguna**, seperti: (1) Penolakan akses terhadap perangkat yang tidak aman atau yang *non-compliant*, (2) melakukan tindakan *quarantine* terhadap perangkat yang tidak aman, (3) Pembatasan akses (*restricted access*) terhadap perangkat yang tidak aman terhadap sumber daya jaringan, dan lain sebagainya.

Kontrol terhadap terhadap perangkat dan pengguna dapat ditegakkan karena penerapan manajemen kebijakan yang secara dinamis dan otomatis ***(dynamic policy management)***. Penegakan kebijakan *policy* tidak saja karena faktor dari perangkat dan pengguna semata tetapi memperhatikan konteks yang terjadi misalnya pada waktu (saat jam kerja, atau saat hari libur, dan sebagainya), lokasi (apakah akses dari dalam jaringan kantor, atau *remote access* dari luar jaringan kantor) dan kondisi kesehatan perangkat (perangkat sudah update versi OS, *anti-virus*, *patching*, dan lain-lain).

Manajemen akses jaringan untuk *guest* mengatur akses tamu yang berkunjung, seperti para mitra kontraktor yang memerlukan akses ke jaringan perusahaan serta pengguna khusus lainnya, yang hanya dilakukan untuk kebutuhan akses internet hingga untuk kolaborasi kerja bersama. Fitur *self-registration* diperlukan jika *admission* pengguna *guest* sehingga tidak menambah beban kerja bagi administrator jaringan atau staff *receptionist*.



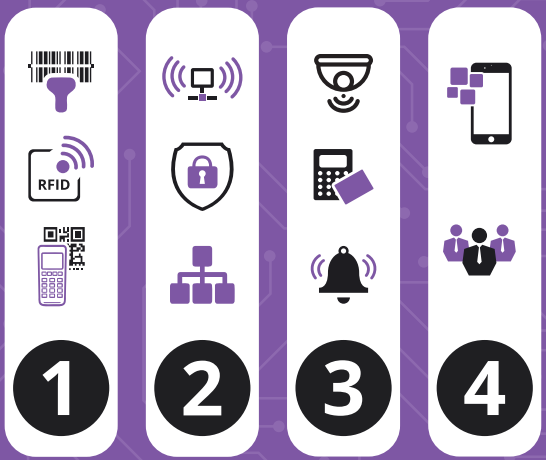
Setelah perangkat dan pengguna telah *compliant* dan berada dalam jaringan yang seharusnya dan akses yang diperlukan maka dilakukan pemantauan yang berlanjut dan deteksi kejanggalan perilaku dengan ***Policy lifecycle management*.** Pemantauan jaringan secara berkelanjutan dilakukan dengan mengevaluasi *endpoint* untuk memastikan profilnya. Perangkat akan dipindai ulang untuk memastikan tidak terjadi *spoofing MAC address* yang dapat mem-*bypass* keamanan akses jaringan.

Pemantauan dan pengawasan anomali dalam pola lalu lintas jaringan, Ketika *endpoint* disusupi atau terdeteksi sebagai ancaman, maka akan segera dilakukan respon terhadap insiden atau anomali yang terjadi untuk mencegah kemungkinan penyebaran serangan *threat* yang lebih meluas. Kejanggalan yang terjadi akan memicu **respon otomatis** untuk tindakan secara *real-time*.

*/ Penulis : Irvan Kurniawan (irvan@acsgroup.co.id)

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

CORE BUSINESS SOLUTIONS : 4 PILLARS



1 Automatic Identification & Data Capture (AIDC)
Barcode & RFID peripherals: printer, reader, and scanner | Enterprise Mobile Printer & Computer (handheld, vehicle mount, tablet, wearable).

2 IT Infrastructure
Network Devices (router, controller, wired/wireless)| Cloud Computing | Cyber Security (NextGen Firewall, Network Access Control Endpoint) | Data Center (Server, Storage, Hyper-Converge).

3 Enterprise Security System
Physical Access Control (Turnstile, Barrier Gate) | Enterprise IP Surveilance Cam & Alarm | Unified Command & Control Center solution.

4 Enterprise Business Solution
Enterprise Software and Manage Service.

BUSINESS PARTNERS

Alibaba Cloud · aruba a Hewlett Packard Enterprise company · BarTender by Seagull Scientific · BOSCH Invented for life · brother at your side
Cambium Networks · Extreme Connect Beyond the Network · FORTINET · Hewlett Packard Enterprise · HID
HIKVISION · HUAWEI · Hytera · ivanti · JANZ
NUTANIX YOUR ENTERPRISE CLOUD · POINTMobile · SAMSUNG · Seuic · ZEBRA

Jakarta (Head Office)
Perkantoran Gunung Sahari Permai #C03-05
Jl. Gunung Sahari Raya No 60-63 Jakarta 10610
Telp : +6221 - 4208221, 4205187
Fax : +6221 - 4207903, 4207904, 4205853

Jakarta (Service Center)
Perkantoran Gunung Sahari Permai Blok E No. 3
Jl. Gunung Sahari No. 60 - 63, Kemayoran, Kota Administrasi Jakarta Pusat, DKI Jakarta - 10610
Telp : +6221 - 4208221, 4205187
Fax : +6221 - 4207903, 4200651

Cikarang
Cikarang Square Blok E No 62, Jl. Raya Cikarang, Cibarusah Km 40, Cikarang Barat, Bekasi
Telp : +6221 - 29612366, 29612367
Fax : +6221 - 29612368

Semarang
Grand Ngaliyan Square Blok B No.18, Ngaliyan 50181, Semarang
Telp : +6224 - 76638092, 76638093
Fax : +6224 - 76638096

Surabaya
Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo 61254
Telp : +6231 - 8556277, 8556278
Fax : +6231 - 8556279

Denpasar
Ruko Grand Sudirman Agung Blok B No.29,
Jl. PB Sudirman, Dauh Puri Kelod,
Denpasar Barat, Denpasar - Bali 80114
Telp : +62361 - 4457859
Fax : +62361 - 4746526