GEBYAR

BULETIN EDISI 38/MARET 2017

AUTO-ID

UNTUK KALANGAN SENDIRI

PROTEKSI PERANGKAT IOT & MOBILE PADA TITIK UJUNG JARINGAN (EDGE)

ARUBA CLEARPASS UNIVERSAL PROFILER

LPR

LICENSE PLATE RECOGNITION

Tips & Info

8 TIPS UNTUK MENINGKATKAN KEAMANAN PERANGKAT IOT

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)
Dea Putty N(Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR
Usadi Sastra Atmadja

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Irvan Kurniawan
Deny Irawan

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

CONTENT

RALAT

Pada AUTO-ID edisi 37/DESEMBER 2016, dalam rubrik **Corporate Info** :

- Halaman 19, keterangan mengenai nama yang tertulis ".. Bapak **Stevan Looho** ..." seharusnya ialah ".. Bapak **Stefan Looho** ..."
- Halaman 20, keterangan yang tertulis ".. 9 staff yaitu :Masa jabatan 15 tahun diberikan kepada :" seharusnya hanya ".. 9 staff yaitu :"
- Halaman 20, keterangan mengenai status jabatan yang tertulis ".. dibekali oleh **CEO Kompas Gramedia** .." seharusnya adalah ".. dibekali oleh **mantan CEO Kompas Gramedia** .."
- Halaman 20, keterangan mengenai nama yang tertulis ".. Bapak **Stevan Looho** ..." seharusnya ialah ".. Bapak **Stefan Looho** ..."
- Halaman 21, keterangan mengenai training "Network Fundamental.." yang tertulis ".."
  - Zebra WLAN Enterprise Solutions - WiNG 5.8 Firmware
  - Azara (Zebra's AZARA Cloud WiF-Fi) – Zebra's Powerfull New Cloud Management Platform"

  seharusnya tertulis ".."
  - Pengenalan basic tentang design CCTV pada jaringan
  - Basic penggunakan perangkat hikvision (hardware maupun software)
  - Fokus bagaimana merancang solusi untuk customer menggunakan Hikvision"

Dengan demikian kesalahan telah diperbaiki.
Salam,
Pemimpin Redaksi

EDITORIAL

Pembaca yang budiman dan pelanggan yang terhormat,

Salam sejahtera, Puji syukur pada Tuhan yang Maha Esa, Kita semua dapat memasuki satu tahun yang baru lagi di 2017 dan terbit cetak kembali Bulletin Gebyar Auto-ID untuk edisi volume yang ke-38/2017. Dan tak terasa sudah 25 tahun pula, ACS Group berkiprah dan berkarya dalam bidang Teknologi Informasi di Indonesia dan menjadi trend setter khususnya dalam hal teknologi AUTO-ID, RFID dan Wireless LAN.

Internet of Things (IoT) telah menjadi topik yang hangat untuk dibicarakan akhir-akhir ini karena IoT tidak hanya menjadi suatu konsep yang mempengaruhi hidup manusia tetapi bagaimana IoT bisa membantu memudahkan kehidupan manusia. Ketersediaan broadband Internet yang semakin meningkat, disertai biaya koneksinya yang semakin murah, begitu juga harga alat pengembangan teknologinya, menjadikan IoT sebagai sesuatu yang mudah diterapkan dan sempurna untuk digunakan.

Internet of Things adalah konsep dasar yang menghubungkan perangkat apapun satu sama lain, mulai dari peralatan sehari-hari hingga perangkat teknologi informasi terbaru saat ini, Dengan penerapan IoT diharapkan dapat membantu meningkatkan kenyamanan dan keamanan lingkungan, mengurangi limbah dan meningkatkan penggunaan energi se-efisien mungkin.

Topik IoT selama beberapa tahun menjadikan kita berusaha untuk memahami bagaimana IoT mempengaruhi kehidupan. Kita juga harus berusaha untuk memahami peluang dan tantangan apa saja yang bisa kita ambil dan selesaikan. Karena semakin banyak perangkat mulai bergabung dengan IoT. Untuk itu, bagaimana pengaturan dan perlakuan terhadap masuknya perangkat-perangkat IOT khususnya pada jaringan sistem informasi di lingkungan enterprise akan dibahas dalam edisi bulletin kali ini.

Selain itu adapula sedikit pembahasan mengenai LPR (License Plate Recognition) yang mana merupakan salah satu fitur smart camera untuk mengenali plat nomor kendaraan dari vendor teknologi Hikvision. Hikvision merupakan produsen Smart IP Camera yang telah berkiprah di Indonesia dalam bisnis perangkat pendukung sistem keamanan sejak tahun 2001.

Dan melengkapi edisi 38 ini seperti biasa kami menghadirkan rubrik-rubrik yang menarik seperti produk baru, principal dan corporate info, serta tips dan trik.

Terima kasih dan selamat membaca!

Salam Redaksi,
Irvan Kurniawan
Enterprise IT Solutions - Manager
PT. Autojaya Idetech
PT. Solusi Periferal

PROTEKSI PERANGKAT IOT & MOBILE PADA TITIK UJUNG JARINGAN (EDGE)

Kehadiran perangkat-perangkat Internet of Things (IoT) yang terhubung ke jaringan sistem informasi perusahaan membawa tantangan baru khususnya bagi tim Teknologi Informasi di organisasi perusahaan atau enterprise. Di satu sisi tentunya akan memberi manfaat yang besar dari penerapan IoT misalnya dengan terwujudnya smart building atau smart office yakni bangunan atau perkantoran yang cerdas dengan dukungan teknologi informasi yang memberikan efisiensi yang optimal terhadap pemanfaatan sumber daya energi contohnya listrik dan air sehingga menghemat biaya operasional dan terciptanya keamanan, kesehatan serta keselamatan kerja yang pada akhirnya meningkatkan produktivitas.

Namun dibalik kehadiran dari banyaknya perangkat-perangkat IoT baru yang tidak dikenal sebelumnya pada jaringan sistem informasi di lingkungan perusahaan juga menimbulkan potensi risiko adanya celah-celah pada jaringan sistem informasi yang dapat disusupi oleh pihak-pihak yang tidak bertanggung jawab yang dapat mengakibatkan terjadinya penyadapan data, pembobolan data, hingga tidak beroperasinya jaringan sistem informasi perusahaan atau dikenal dengan istilah Denial of Service (DoS) menyebabkan terhentinya operasional perusahaan akibat dari serangan keamanan data pada perangkat-perangkat baru ini.

Saat ini kehadiran dari perangkat-perangkat mobile seperti smartphone, tablet dan handheld terminal baik dari para karyawan, tamu-tamu yang berkunjung dan mitra kerja yang menetap untuk beberapa waktu lamanya, serta para eksekutif yang mana perangkat-perangkat tersebut menyertai mereka dalam lingkungan perusahaan dimana dikenal dengan istilah Bring Your Own Device (BYOD) juga ditambah penerapan teknologi IoT dengan perangkat-perangkat yang membutuhkan akses ke pusat sumber data melalui jaringan sistem informasi tentunya secara signifikan menghadirkan satu tantangan baru bagi departemen tim sistem informasi dan komunikasi (ICT) dan para Pimpinan Direksi, diantaranya beberapa hal berikut ini:

A. Keterbatasan visibilitas - Apakah mengetahui apa yang ada di jaringan?

Keamanan jaringan sistem informasi dimulai dengan memahami apa sebenarnya yang ada di jaringan tersebut. Perangkat-perangkat seperti ponsel pintar yang tidak dikelola (unmanaged smartphone), perangkat endpoint yang berada di titik terujung (Edge) dari koneksi perangkat jaringan dimana mungkin terdapat perangkat yang tidak diperbolehkan (rogue endpoint) dan perangkat IoT merupakan potensi ditingkat permukaan paling awal dilakukannya suatu serangan (attack) pada jaringan dan tentunya akan mengancam (threaten) keamanan sistem informasi perusahaan.

Gambar 1. Kemampuan untuk Visibilitas perangkat

Kemampuan untuk melihat apa sebenarnya yang ada di jaringan tentunya akan memberikan team IT pemahaman yang lebih baik tentang bagaimana jaringan yang sedang mereka gunakan dan dengan apa. Team IT seharusnya mampu mengidentifikasi dan mengetahui profil dari setiap perangkat yang terhubung ke jaringan, terlepas dari mana perangkat itu terhubung. Dan sekarang ini, banyak perangkat IoT yang terhubung ke jaringan sistem informasi perusahaan yang tidak diketahui dan semakin deras membanjiri jaringan tersebut, dan

aksesnya masuk melalui media kabel dan nirkabel. Semua perangkat yang akan akses ke jaringan sistem informasi seharusnya dapat diketahui profile-nya, misalnya apa jenis perangkatnya? apakah laptop, desktop, ponsel atau perangkat tertentu lainnya? Kemudian bagaimana cara konektivitas-nya: apakah aksesnya melalui media kabel, melalui jaringan nirkabel atau melalui lokasi remote dengan VPN (Virtual Private Network)? Dan ditentukan kategorinya, apakah akses jaringan akan secara otomatis langsung diberikan atau ditolak berdasarkan jenis perangkat, status kepemilikan, serta sistem operasinya.

B. Kekhawatiran baru mengenai jaringan kabel

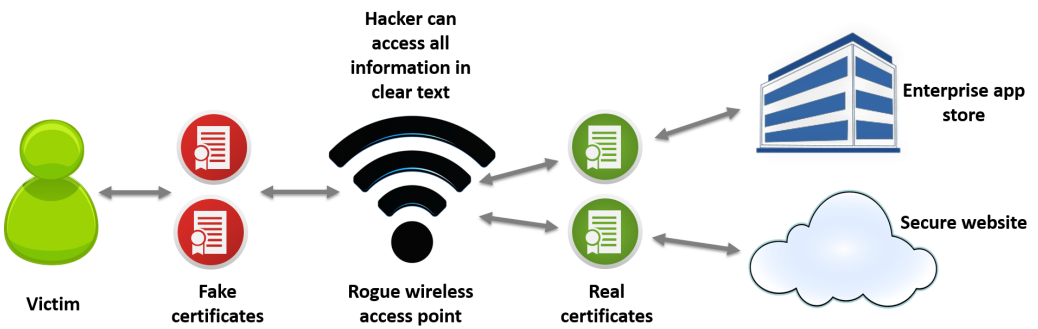
Pada beberapa perusahaan dan industri saat ini, jumlah perangkat IoT yang terhubung ke jaringan umumnya melalui koneksi kabel dan terus bertambah mulai dari kisaran 35% hingga lebih dari 50%, sebagai contoh perangkat motion-detector, peralatan medis, perangkat pengendali proses di pabrik, dan beberapa perangkat lainnya. Sedangkan jenis perangkat IoT yang terhubung ke jaringan umumnya adalah non-user dan secara kuantitas banyak pula jumlahnya serta tersebar di berbagai lokasi, dan menariknya lagi adalah harus terhubung dengan pusat data untuk menginformasikan berbagai hal baik itu alarm, alert ataupun sensor.

Topik diskusi mengenai kontrol akses jaringan (NAC) sebagian besar sebelumnya lebih berkutat pada bagaimana cara mengamankan jaringan nirkabel karena pada saat itu sebagian besar perangkat yang terhubung adalah melalui jaringan nirkabel. Memastikan bahwa setiap sesi koneksi jaringan nirkabel harus aman menjadi persyaratan utama jaringan nirkabel dimana potensi Eavesdropping pada jaringan nirkabel dan pengguna yang tidak diketahui dapat saja melakukan akses dari mana saja selama dalam jangkauan perangkat access point dan broadcast jaringan nirkabel yang tidak aman. Eavesdropping adalah tindakan melakukan intersepsi secara real-time yang tidak diotorisasi pada jaringan. Tindakan ini umumnya dilakukan untuk mencuri data yang dikirim melalui jaringan tanpa dienkripsi terlebih dahulu.

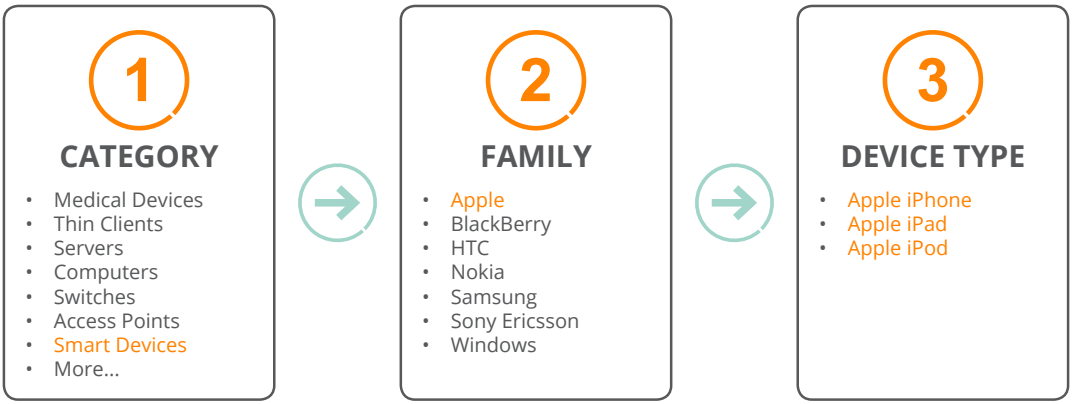
C. Infrastruktur jaringan kabel tradisional tidak optimal untuk penerapan IoT

Pada penerapan perangkat switch yang lama yang terhubung dengan switch ini adalah perangkat-perangkat yang tidak mobile seperti PC desktop, printer dan lain-lain sedangkan konektivitas untuk perangkat IoT belum dipertimbangkan untuk perangkat switch model lama ini. Dan yang berada dibelakang switch ini adalah perangkat firewall dan tim IT-lah yang perlu memastikan bahwa parameter yang diterapkan haruslah kuat.

Dengan masuknya perangkat IoT, maka infrastruktur jaringan kabel sekarang ini haruslah



Gambar 2. Eavesdropping on enterprise apps



Gambar 3. Pengelompokan perangkat endpoint dalam Category, Family dan Device Type

secerdas perangkat jaringan nirkabel yaitu mengenai cara akses untuk masuk ke dalam suatu jaringan.

Untuk dapat akses ke jaringan nirkabel, setiap perangkat nirkabel membutuhkan otorisasi terlebih dahulu sehingga dapat diketahui profil perangkat dan bagaimana hak aksesnya. Sehingga setiap perangkat yang masuk ke dalam jaringan dapat di-identifikasi dengan baik. Hal ini juga seharusnya diterapkan pada perangkat switch sekarang ini yaitu wajib memiliki fitur keamanan dan manajemen jaringan yang cerdas serta terintegrasi sehingga semua perangkat dapat terhubung dengan aman dan mulus (seamlessly).

D. Melindungi jaringan membutuhkan alur kerja yang automasi (*automated workflows*)

Dengan hadirnya ratusan hingga ribuan perangkat mobile yang tidak dapat dikenali dan perangkat IoT yang terhubung ke jaringan sistem informasi perusahaan setiap harinya, adalah sangat tidak tepat jika harus secara manual menetapkan dan menegakkan kebijakan policy account pada setiap perangkat satu per satu. Seluruh proses haruslah dapat dilakukan secara automasi untuk mengurangi risiko dan meminimalkan efforts yang tidak perlu dari team IT.

Pada perangkat yang statis dan perangkat infrastruktur harus di-profile-kan dan diperiksa secara otomatis untuk melihat apakah adanya perubahan yang mencurigakan. Jika ada perangkat yang bertindak mencurigakan, harus pula secara otomatis dapat dilakukan karantina (quarantined) sampai ancaman (threat) tersebut dapat dinilai bagaimana penanganannya.

E. Butuh biaya mahal untuk selalu ada di posisi depan dari para hacker

Tampaknya kita sering mendengar tentang terjadinya pembobolan data atau data *breaches* secara besar-besaran hampir setiap harinya.

Hal Ini menimbulkan biaya yang mahal dan juga memakan waktu bagi perusahaan untuk berinvestasi dalam hal keamanan data dan sepertinya hampir mustahil untuk menjaga keamanan jaringan agar selalu berada di depan para hacker dengan mengandalkan usaha dan

inovasi sendiri.

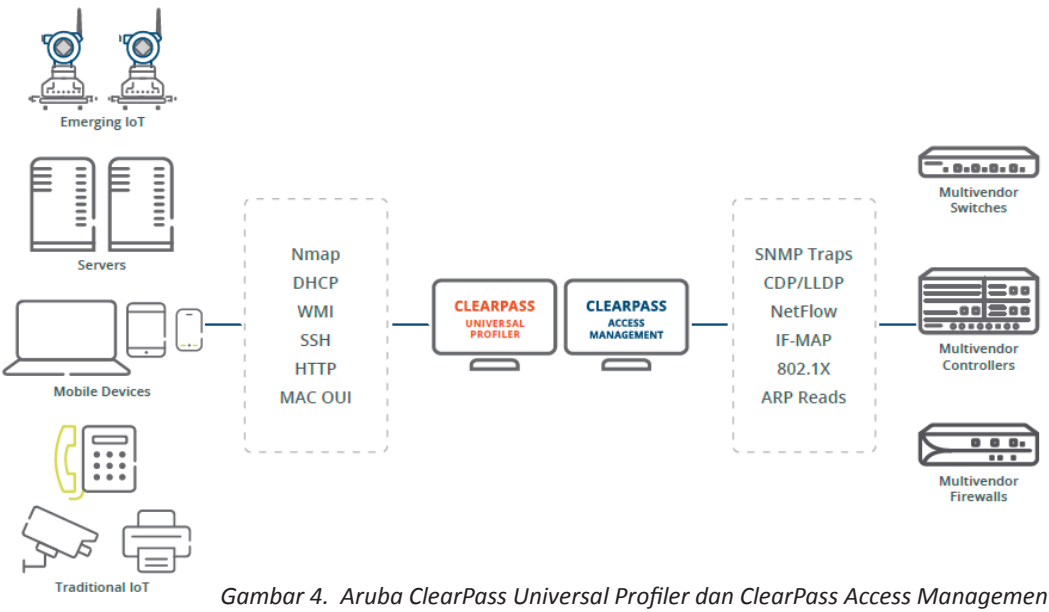
Tim IT membutuhkan perangkat yang dapat mengamankan dan mengatur perangkat-perangkat IoT tersebut misalnya secara otomatis dapat mengidentifikasi kehadiran perangkat baru, mengetahui profil perangkat, mengotentikasi perangkat, dan menerapkan suatu kebijakan untuk perangkat tersebut selama berada dalam jaringan perusahaan yang disebut dengan istilah policy.

Aruba Networks yang kini telah menjadi bagian dari perusahaan Hewlett Packard Enterprise company menjawab tantangan ini dengan pendekatan empat langkah untuk konektivitas perangkat IoT at the edge atau pada titik ujung dari jaringan sistem informasi. Ke-empat langkah tersebut yakni dengan melakukan identifikasi terhadap apa yang ada di jaringan, menghubungkan perangkat-perangkat mobile dan perangkat IoT dengan perangkat switch yang cerdas, kemudian melindungi jaringan dengan automated policy management, dan terus berinovasi melalui mitra ekosistem untuk memberikan keamanan yang end-to-end.

Berikut pendekatan 4-langkah dari Aruba Networks untuk mengamankan konektivitas perangkat IoT CONNECTIVITY AT THE EDGE

1. Mengidentifikasi dan profiling terhadap perangkat multi-vendor yang tidak dikenal pada jaringan kabel dan jaringan nirkabel

Mengingat bahwa keamanan jaringan dimulai dengan mengetahui apa yang ada di jaringan, adalah penting bagi organisasi dan perusahaan untuk dapat mengidentifikasi dan melakukan profil terhadap semua perangkat yang terhubung dalam jaringan. Produk ClearPass dari Aruba Networks menawarkan kelebihan yang unik dibandingkan dengan produk lainnya yang ada saat ini, yakni agentless profiling dalam melakukan identifikasi profile pada perangkat tanpa perlu agent yang di-



Gambar 4. Aruba ClearPass Universal Profiler dan ClearPass Access Management

Gambar 5. Aruba ClearPass Policy Manager

install pada perangkat endpoint.

Produk Profiling ini dapat diperoleh pada suatu perangkat yang standalone berdiri sendiri ataupun dalam satu perangkat dengan solusi penegakan kebijakan (policy enforcement) yang sangat komprehensif. Kedua solusi tersebut memungkinkan untuk terus dapat mengidentifikasi endpoint, baik terhadap perangkat jaringan yang non-AAA (Authentication Authorization Accounting) ataupun perangkat AAA serta dapat diaktifkan pada jaringan kabel dan jaringan nirkabel - baik melalui alamat IP (Internet Protocol) dinamis ataupun statis. Dengan tampilan visual dashboard yang komprehensif membuatnya mudah untuk melihat jumlah total endpoint, dan mengetahui jumlah endpoint berdasarkan kategori, family dan jenis perangkatnya.

Aruba ClearPass Universal Profiler adalah perangkat standalone virtual appliance yang dapat digunakan dan berjalan dalam hitungan menit, serta dirancang untuk organisasi yang belum siap untuk solusi NAC (Network Access Control) yang lengkap, misalnya pada lokasi remote area atau pada lokasi daerah yang dibatasi dimana NAC belum diterapkan. Aruba ClearPass Universal Profiler adalah jawaban dan kemudahan serta biaya yang efektif untuk dapat mengidentifikasi dan melakukan profil terhadap perangkat apa saja yang ada di jaringan sistem informasi.

Sedangkan produk *Aruba ClearPass Policy Manager* tersedia dalam bentuk perangkat virtual dan physical appliance yang meliputi fungsi:

- Profiling yang komprehensif,
- Policy enforcement atau penegakan kebijakan akses baik pada perangkat non-AAA dan perangkat AAA yang akan akses melalui jaringan kabel dan jaringan nirkabel,
- Fungsi pengaturan terhadap akses tamu yang masuk jaringan,
- BYOD onboarding terhadap perangkat-perangkat pribadi pengguna untuk akses pada jaringan
- Kemampuan melakukan penilaian terhadap endpoint (endpoint assessment capabilities),
- Reporting atau laporan yang dapat disesuaikan,
- Built-in third party security yakni beberapa fungsi keamanan andal yang telah tersedia.
- Berorientasi pada kemudahan bagi pengguna dengan solusi yang terintegrasi.

2. Menghubungkan perangkat IoT dengan automated intelligence

Dengan penerapan smart building berarti bahwa bisnis saat ini membutuhkan infrastruktur kabel yang lebih cerdas. Hal ini menjadi tambahan terbaru pada perangkat dalam ArubaOS-Switch yang dirancang untuk memberdayakan dan mengamankan intelligent edge, yakni perangkat-perangkat IoT yang berada di titik ujung dari jaringan, yang memang perangkat switch ini dioptimalkan untuk perangkat mobile dan

perangkat IoT. Peningkatan ini memungkinkan unified role-based access baik pada jaringan nirkabel dan jaringan kabel yakni suatu kemampuan untuk mengidentifikasi dan menetapkan suatu role yang tepat untuk perangkat IoT yang telah terhubung dengan jaringan untuk mendapatkan prioritas dalam menjalankan aplikasi bisnis yang critical serta mengamankan jaringan.

Perangkat switch Aruba layer 3 juga memiliki kemampuan akan user-based dan port-based terhadap lalu lintas data pada jaringan kabel yang di-tunneling ke perangkat Mobility Controller sehingga policies atau kebijakan mengenai akses jaringan dapat diterapkan, beberapa layanan canggih dapat diperpanjang, dan lalu lintas data dapat dienkripsi untuk mengamankan jaringan LAN.

Dalam rangka memenuhi permintaan akan pertumbuhan yang cepat pada perangkat-perangkat IoT dan perangkat-perangkat yang terhubung di perusahaan yang terdistribusi lokasinya, perangkat switch Aruba 2540 serta perangkat switch Aruba lainnya merupakan perangkat switch yang cost-effective untuk mendukung fitur Zero Touch Provisioning dan juga fitur optional cloud-based management yang memungkinkan perusahaan menyederhanakan dan memangkas penyebaran jaringan serta biaya manajemennya.

Gambar 6. Perangkat switch Aruba automatic intelligence

3. Melindungi jaringan dengan smart policies

Setelah memiliki visibilitas terhadap perangkat, maka dibutuhkan kebijakan yang cerdas terhadap perangkat yang akan masuk dalam jaringan.

Mengapa dikatakan kebijakan yang cerdas atau smart policy? Karena perangkat-perangkat yang ada demikian banyak ragamnya dari berbagai vendor pembuatnya dan mungkin saja digunakan oleh user yang berbeda keperluannya dan mungkin masih ditambah lagi dengan waktu pada jam-jam tertentu yang bervariasi metode dan lokasi akses-nya. Kemampuan untuk menyaring parameter-parameter yang sangat variatif dan demikian dinamis ini membutuhkan Policy atau kebijakan yang tepat dan cerdas untuk dapat diterapkan terhadap perangkat saat akses di jaringan.

Tentu saja semuanya membutuhkan suatu enforcement policy atau penerapan kebijakan yang tepat dan dapat secara otomatis dapat diterapkan workflow-nya. Dengan Aruba ClearPass Policy Manager dapat membantu Anda untuk melihat apa yang ada di jaringan dan kemudian menegakkan kebijakan yang seharusnya pada perangkat (enforce policies) dan membuat alur kerja otomatis (automated workflows) di beberapa perangkat multi-vendor baik pada infrastruktur kabel maupun infrastruktur nirkabel. Perangkat ClearPass memiliki kemampuan profiling pada perangkat mobile dan perangkat IoT, penegakan kebijakan policy enforcement, pengaturan akan akses para tamu, penanganan BYOD onboarding, dan banyak hal lainnya yang selama ini sulit untuk dilakukan, perlindungan terhadap ancaman juga ditingkatkan, dan yang terpenting adalah pengalaman user yang merasakan kemudahan penggunaannya.

Dan dengan fokus baru untuk mengamankan infrastruktur jaringan kabel, maka pada fitur OnConnect dari ClearPass menggunakan existing protokol perangkat switch yang telah ada, untuk membantu mengamankan dan mengunci port-port yang rentan seperti pada port-port di ruang konferensi, pada perangkat IP phone, dan perangkat printer. Karena selama ini port-port tersebut adalah non-user port dimana berpotensi disusupi oleh pihak yang tidak bertanggung-jawab dan langsung mendapat akses ke jaringan.

4. Mempercepat inovasi untuk meningkatkan keamanan jaringan Edge

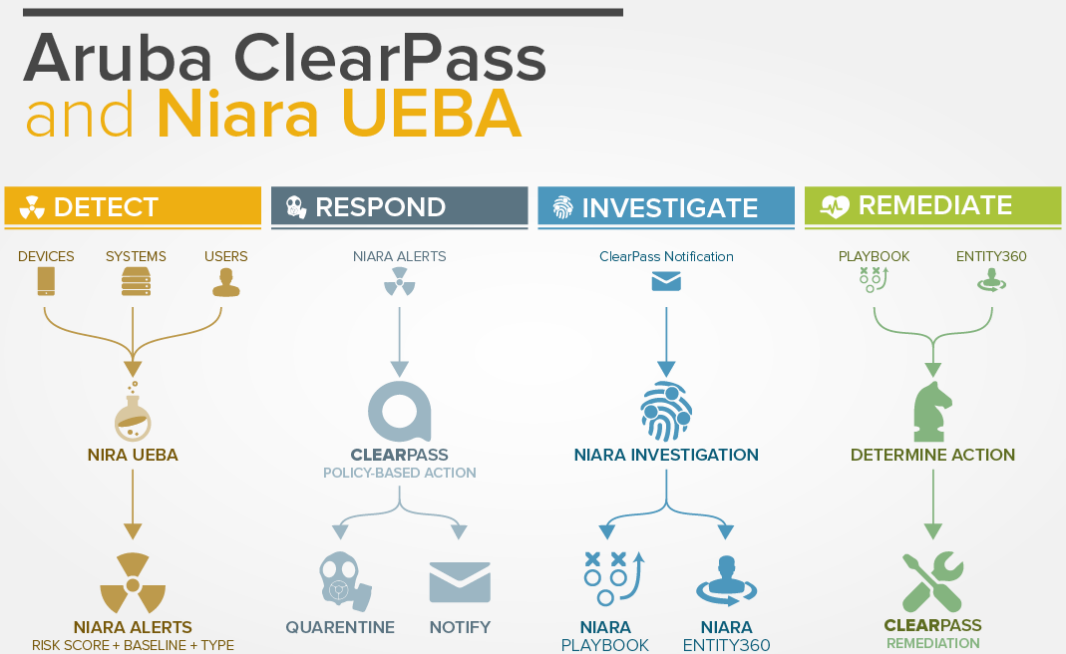
Ekosistem teknologi Aruba mencakup solusi keamanan dari industri terkemuka yang terintegrasi dengan ClearPass Exchange untuk

memastikan end-to-end keamanan di jaringan edge dan core. Berikut kemitraan Aruba dengan mitra yang fokus akan keamanan pada IoT, seperti:

- *Niara* menggunakan pola dari lalu lintas data perangkat yang terhubung dengan jenis perangkat untuk mengidentifikasi perilaku yang mencurigakan dan kemudian meminta perangkat Aruba ClearPass untuk menghapus perangkat dari jaringan atau tidak dapat akses ke jaringan lagi.
- *Attivo* memungkinkan untuk membuat suatu "fake virtual" perangkat IoT dimana ada orang yang mencoba untuk menggunakan perangkat palsu untuk menyerang jaringan. Setelah perangkat virtual melihat adanya perilaku yang tidak diinginkan, maka selanjutnya meminta pada perangkat Aruba ClearPass untuk menarik perangkat tersebut dari jaringan sehingga tidak dapat aktif lagi.

Sebagai organisasi perusahaan yang mulai menerapkan IOT dalam operasional, orientasi dan manajemen akan perangkat IOT menjadi penting bagi keberhasilan. Perusahaan membutuhkan strategi untuk mengamankan dan menghubungkan perangkat mobile dan perangkat IOT yang berada di edge jaringan untuk mendapatkan nilai dan efisiensi sekaligus menjaga jaringan dan aset perusahaan yang aman.

Demikian pendekatan 4-langkah Aruba Networks untuk konektivitas IOT menangani tantangan dalam mengidentifikasi apa yang ada di jaringan, menghubungkan perangkat melalui infrastruktur kabel dan nirkabel yang cerdas, melindungi jaringan dengan automated policy management, dan menggunakan ekosistem mitra Aruba untuk meningkatkan keamanan end-to-end serta menjaga tetap terdepan dalam menghadapi potensi risiko keamanan jaringan.



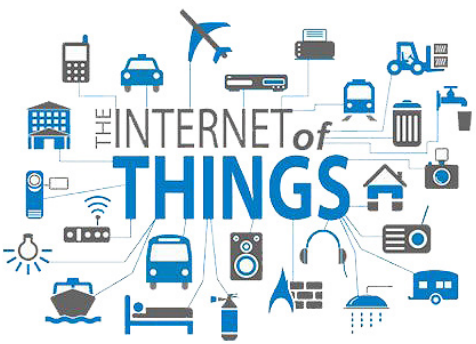
Gambar 7. Kolaborasi Aruba ClearPass dan Niara UEBA terhadap perangkat IoT

ARUBA CLEARPASS
UNIVERSAL PROFILER

Virtual appliance dari Aruba HPE yang memiliki kemampuan melakukan identifikasi terhadap semua perangkat yang terhubung pada jaringan kabel dan jaringan nirkabel.

Overview

Semua perangkat teknologi informasi yang terhubung ke jaringan mempunyai potensi atau rawan diserang (attack point), dengan mengetahui apa saja perangkat yang berada di jaringan merupakan langkah awal dalam mengamankan jaringan data. Tidaklah dapat diterima jika untuk mengetahui jumlah total keseluruhan perangkat yang berada dalam jaringan saja hanya dengan perkiraan atau estimasi! Demikian pula, bagaimana mengetahui apakah perangkat-perangkat tersebut adalah perangkat laptop yang dapat di-manage, smartphone yang tidak di-manage ataupun perangkat IoT (Internet of Thing)?



Mengingat bahwa jumlah perangkat IoT diharapkan akan terus tumbuh ke dalam jumlah miliaran, maka pengetahuan mengenai apa saja perangkat yang berada di jaringan merupakan tantangan terbesar bagi tim Informasi dan Teknologi (IT).
Kehadiran perangkat-perangkat IoT sudah demikian derasnya membanjiri jaringan enterprise, dimana perangkat IoT tersebut ada yang dikembangkan oleh team IT, ada juga merupakan bagian dari fasilitas gedung atau bahkan dibawa dari rumah oleh karyawan. Dengan pemahaman akan apa saja perangkat-perangkat tersebut dan bagaimana perangkat-perangkat tersebut digunakan menjadi hal yang kritikal. Karena pada hari-hari ini, para hacker masih terus saja mencari-cari cara guna mengeksploitasi kerentanan jaringan data. Mengetahui perangkat apa yang seharusnya berada di jaringan dan perangkat apa yang tidak diperbolehkan di jaringan sangat diperlukan untuk kepatuhan compliance baik dari sisi internal dan eksternal.
Aruba menghadirkan ClearPass Universal Profiler yang dirancang untuk secara otomatis memberikan visibilitas yang detil terhadap semua perangkat yang terhubung dalam jaringan, bahkan terhadap perangkat jaringan seperti controller dan switch. Pada layar utamanya terdapat dashboard untuk melihat category dan family dari perangkat-perangkat dan atribut individu perangkat dari semua perangkat yang terhubung di jaringan. Menariknya, tidak perlu agent pada perangkat endpoint, tanpa menginvestasikan perangkat kontrol akses jaringan (NAC) ataupun memerlukan perangkat solusi policy management seperti umumnya saat implementasi untuk kebutuhan ini. Dan jika persyaratan mengenai keamanan berubah, sangatlah mudah untuk bermigrasi dari pure profiling ke policy and enforcement solution yang lebih komprehensif bila diperlukan. Ini adalah sesuatu yang dalam kompetisi pasar teknologi informasi belum dapat tawarkan saat ini.

Key Benefits

- **Secara otomatis dapat mencari semua perangkat-perangkat IoT baik perangkat yang managed maupun perangkat yang unmanaged**

- **Kemampuan memonitor terhadap perangkat jaringan kabel dan perangkat jaringan nirkabel dari multi-vendor network**
- **Menggunakan active dan passive profiling methods seperti DHCP, SNMP dan lainnya**
- **Dapat mengetahui apa saja perangkat yang baru saja terhubung dan yang sudah tidak terhubung dengan jaringan**
- **Built-in profile update terhadap perangkat baru ataupun terhadap perangkat yang tidak diketahui**
- **Low cost untuk memulai implementasinya dan dapat disesuaikan dengan skala jaringan dalam perkembangannya**
- **Kemudahan dalam memulai profiling perangkat dan juga untuk penerapan policy enforcement nantinya jika diperlukan**

Real-Time Discovery & Fingerprinting

ClearPass Universal Profiler memiliki kemampuan untuk melakukan identifikasi terhadap semua perangkat pada jaringan secara otomatis dengan memanfaatkan DHCP, SNMP dan metode lainnya baik pada jaringan kabel dan jaringan nirkabel, dengan set-up yang minimal dan dalam lingkungan jaringan yang multi-vendor. Pada saat initial discovery, Universal Profiler mengidentifikasi setiap perangkat baru dan juga atribut yang berubah pada perangkat existing.

Belumlah pernah sebelumnya untuk mengumpulkan semua informasi dari perangkat yang terhubung dengan jaringan dan mengetahui mengenai kategori perangkat, produsen atau manufacturer, metode koneksi, jenis OS dan versinya, serta alamat IP dengan begitu mudahnya tanpa Universal Profiler. Dengan memiliki visibilitas yang diperlukan untuk keamanan jaringan dan optimalisasi terhadap kinerja jaringan memberi dampak bagi bisnis enterprise terus berkembang pesat dan memberikan pengalaman penggunaan yang aman dan handal akan product Universal Profiler ini.

Visibilitas Yang Terpusat Dari Satu Lokasi

ClearPass Universal Profiler hadir dalam web-based interface yang intuitif dimana sangat mudah dalam mengelolanya dan menampilkan informasi mengenai total perangkat serta dapat melihat perangkat berdasarkan :

- Kategori
- Nama host
- Informasi mengenai vendor perangkat, dan
- Mengetahui status perangkat apakah sedang online atau off.

Grafik visual yang tersedia memudahkan untuk melacak apa yang ada di jaringan dan

Gambar 1. Granular device discovery, categorization and visibility

memungkinkan untuk melihat lebih detail mengenai atribut perangkat tertentu. Dengan fleksibilitas koneksi ClearPass Universal Profiler dapat di akses dari mana saja, baik dari kantor maupun saat berada di luar atau dalam perjalanan. Juga terdapat opsi pilihan untuk penyaringan atau filtering yang memungkinkan untuk menemukan satu perangkat yang memerlukan perhatian khusus, misalnya perangkat tersebut sedang tidak dalam jaringan, atau perangkat tersebut menunjukkan perilaku yang mencurigakan terkait dengan keamanan jaringan. Dan dapat pula mengetahui lebih jauh mengenai suatu perangkat IoT baru yang terhubung ke port kabel di lokasi cabang atau remote. Cukup dengan satu perangkat ClearPass Universal Profiler saja sudah dapat mencari dan mengetahui informasi dan keberadaan perangkat dalam jaringan tanpa perlu menggunakan beberapa tool yang rumit dan sulit.

Profiling Merupakan Titik Awal Keamanan

Memeriksa unsur kerentanan sangatlah penting dan bahkan kritikal untuk mengidentifikasi adanya celah keamanan dalam perangkat server dan sumber daya lainnya dalam sistem informasi, melakukan identifikasi terhadap semua perangkat yang berbasis alamat IP (Internet Protocol) adalah hal yang critical dari sudut pandang keamanan, dan untuk keperluan audit serta kepatuhan akan persyaratan (compliance requirement). Dengan melakukan Profiling akan mendapatkan informasi perangkat yang detail tentu akan membuat suatu perbedaan, karena mempunyai visibilitas akan perangkat sehingga memudahkan dalam menerapkan policy kebijakan dari perangkat firewall, perangkat SIEM (Security information and event management), perangkat UBA (user behavior analytics) dan beberapa perangkat solusi lainnya.

Pada saatnya jika membutuhkan kontrol akses jaringan yang lebih komprehensif, Aruba HPE telah menyiapkan pula rencana jalur migrasi secara mudah dari perangkat ClearPass Universal Profiler ke perangkat ClearPass Policy Manager (CPPM) guna memastikan bahwa penegakan kebijakan policy akses jaringan secara otomatis akan mudah diterapkan untuk keamanan akses secara real-time. Dengan demikian maka perangkat-perangkat yang terkelola (managed device), perangkat-perangkat unmanaged dan perangkat-perangkat IoT dapat diperbolehkan ke jaringan dan dapat ditentukan apakah berdasarkan kategori-nya, versi OS-nya, kepemilikannya, ataupun atribut lainnya sebagai parameter.

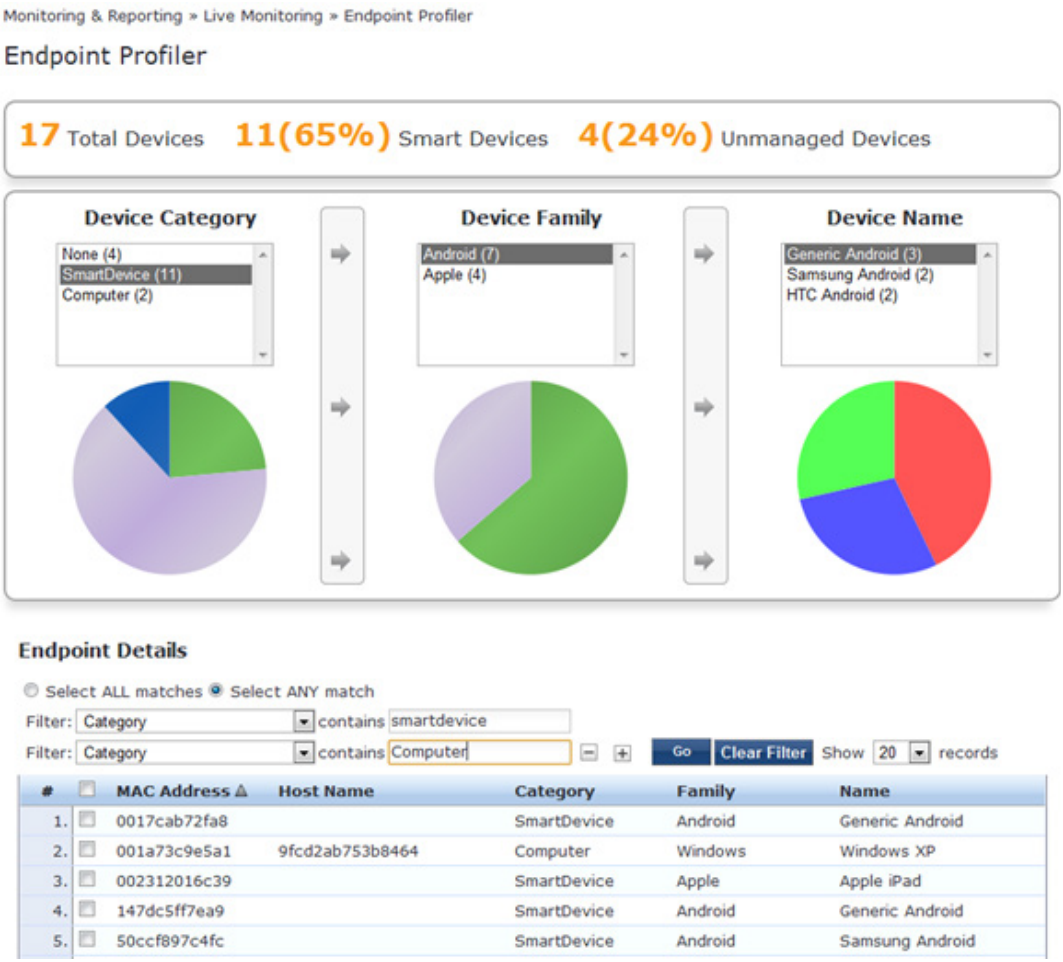
Key Features

- **Identifikasi terhadap semua perangkat IP-enabled, seperti: laptop, smartphone, switch, controller, router**
- **Kemudahan dalam melihat attribut per perangkat seperti:**
  - **Type printer, HVAC sensor, laptop, IV Pump, dan lain-lain**
  - **Model name**
  - **MAC address**
  - **IP address**
  - **NIC vendor**
  - **Jenis Operating System dan version number**
  - **Associated switch port**
  - **VLAN**
- **Web-based dashboard: Visibilitas yang dinamis, reporting dan admin access dalam beberapa tier**
- **Kemudahan dalam mengetahui jumlah total perangkat: dapat berdasarkan category, family, dan spesifik nama vendor**
- **Continuous insight: mengetahui semua perangkat yang terhubung dan terdapat profiling sepanjang waktu**
- **Kompilasi mengenai konektivitas perangkat: mengetahui informasi seperti IP subnet, perangkat jaringan kabel ataupun perangkat jaringan nirkabel**
- **Administrasi yang simple: kemudahan dalam monitoring mengenai heath metric terhadap semua titik profiler**
- **Vendor-agnostic: dibangun untuk dapat bekerja dalam perangkat multi-vendor baik pada jaringan kabel dan jaringan wireless network**

- **Tidak perlu agent ter-install: karena memanfatkan DHCP, SNMP dan method lainnya**

Produk Aruba ClearPass Universal Profiler berbasis subscription license yang sudah termasuk didalamnya dukungan support teknis, lisensi tersedia dalam per 100 perangkat. Saat ini, ClearPass Universal Profiler hanya tersedia dalam format virtual appliance dan platform yang didukung adalah VMware ESX. Dan appliance-nya berdasarkan jumlah kapasitas perangkat yang di-discover dalam jaringan, ada tiga sizing untuk virtual appliance-nya, yakni:

- Up to 2,000 devices
- Up to 20,000 devices
- Up to 100,000 devices



Gambar 2. Dashboard Aruba HPE ClearPass Universal Profiler

CASE STUDY

Keamanan pada jaringan wireless sering menjadi dilema karena penerapan keamanan yang tinggi berarti harus mengorbankan kenyamanan user dimana user akan dihadapkan dengan berbagai otentikasi, banyaknya SSID dengan sekuriti yang berbeda, sampai cara melakukan koneksi yang tidak mudah untuk orang awam seperti menggunakan username, certificate, dan lain-lain. Menjadi faktor utama disini adalah bagaimana caranya keamanan jaringan nirkabel dapat tetap tercapai dengan sesedikit mungkin mengorbankan kenyamanan user.

Pada tahun 2012 salah satu customer kami produsen Semen nasional yang memiliki pabrik di kota-kota besar seperti Sumatera Barat, Sulawesi Selatan dan Jawa Timur. Mereka mulai menyadari akan hal ini dan membutuhkan solusi untuk hal tersebut dan memilih Aruba (HPE) Clearpass Policy Manager sebagai solusinya dimana mereka menjadi yang pertama di Indonesia yang menerapkan fitur ini dan berhasil. Clearpass Policy Manager atau CPPM memberikan security dari sisi dalam pada sebuah konektivitas. Sebuah point of view yang sering terlewat oleh kita dimana pengamanan bukan hanya dengan menggunakan firewall untuk mengamankan user dari serangan luar perusahaan tetapi juga dari sisi dalam baik melalui akses kabel maupun nirkabel dari dalam perusahaan.

CPPM diterapkan untuk melakukan otentikasi, otorisasi, dan akunting terhadap semua konektivitas user. Dari saat pertama user mencoba melakukan koneksi, CPPM-lah yang bertanggung jawab mengotentikasi semua user ini dimana uniknya, CPPM dapat menerapkan otentikasi secara fleksibel terhadap berbagai macam jenis perangkat yang berbeda-beda.

Otentikasi yang fleksibel sangat dibutuhkan karena perangkat di dalam sebuah jaringan yang ingin terkoneksi sangat beragam jenisnya mulai dari perangkat laptop atau desktop milik perusahaan dan milik pribadi dengan beragam operating system dan karateristik. Perangkat gadget pun sangat beragam dengan variasi OS, jenis perangkat, manufaktur dan jenis perangkat yang juga tidak kalah penting membutuhkan akses adalah perangkat yang sering disebut non-user device atau perangkat yang tidak dioperasikan oleh orang secara langsung seperti printer, scanner, fax, dan lain-lain. Dimana perangkat ini menjadi masalah dalam hal keamanan karena tidak dapat mendukung tingkat keamanan otentikasi yang ingin kita terapkan.

Keamanan selalu menjadi masalah dalam hal implementaasi karena sifatnya yang selalu bertolak belakang dengan kenyamanan, semakin aman sebuah jaringan biasanya harus disertai dengan berkurangnya kenyamanan. Dengan CPPM, proses pengenalan siapa atau apa yang ingin terhubung (visibilitas terhadap user) dilakukan secara smart di back-end sehingga user secara tidak sadar sedang di profiling yang selanjutnya oleh CPPM diperlakukan secara berbeda tergantung dari tingkat keamanan yang perlu diterapkan terhadap user yang beragam tersebut dan pada akhirnya menerapkan beberapa jenis rule yang berbeda-beda pula tergantung seberapa tinggi tingkat keamanan yang harus diterapkan ini. Uniknya semua ini dapat dilakukan hanya dengan menggunakan 1 buah SSID sehingga user baik staff maupun manajer terkoneksi ke SSID yang sama tetapi bisa mendapatkan level keamanan yang berbeda.

Fitur mengenali siapa user yang terkoneksi inilah yang menjadi utama dalam fitur CPPM dan untuk memperkuat fitur ini, CPPM juga dilengkapi dengan berbagai fitur lainnya seperti Onboard sebagai automatic RADIUS configurator, fitur Onguard untuk melakukan Network Access Control, dan yang terakhir adalah fitur advance guest access.

PERESMIAN GEDUNG
SERVICE CENTER ACS GROUP

ACS Group

terus mengembangkan diri sejalan dengan terus bertumbuhnya jumlah customer yang telah bekerjasama dengan ACS Group karena komitmen yang telah kami berikan serta kepercayaan yang telah customer berikan kepada kami.

Untuk meningkatkan dukungan pelayanan after sales service bagi pelanggan setia kami, pada hari Rabu tanggal 1 Februari 2017 kami telah meresmikan sebuah "GEDUNG SERVICE CENTER" 4 lantai milik ACS Group sendiri. Letak gedung masih satu kompleks dengan kantor pusat ACS Group di Jl. Gunung Sahari Raya No 60-63 Blok E3 - Jakarta Pusat.

Acara peresemian gedung baru ini dibuka oleh bapak Ir. Indra Tjahjadi selaku Managing Director ACS Group. Sebagai ucapan syukur atas Anugerah Tuhan yang sudah diberikan kepada ACS Group acara peresmian ini dibawa dalam doa bersama para staff yang dipimpin langsung oleh bapak Stefan Looho sebagai komisaris ACS Group. Acara peresmian ini juga ditandai dengan pemotongan nasi tumpeng yang dilakukan oleh bapak Johanes Looho selaku komisaris ACS Group.

Repair room yang sudah dilengkapi dengan layar monitoring progress repair dan penempatan unit product yang akan diservice dan ruang penempatan unit product yang selesai service.

Ruang meeting bertempat di lantai III dan lantai IV digunakan sebagai ruang kerja para staf departemen Enterprise Bussiness Solution(EBS).

Seminar & Gathering
ACE Banten

Asosiasi Chief Engineering(ACE) Banten mengadakan Seminar & Expo pada tanggal 14 Desember 2016 lalu di Hotel ALLIUM, Tangerang - Banten. Para peserta seminar yang hadir pada acara ini adalah Anggota Engineer Hotel seluruh Banten. ACS Group bersama Brother Indonesia ikut serta berpartisipasi dengan membuka booth dan memperoleh kesempatan untuk memberikan presentasi produk printer Brother pada acara ini. Acara ini dibuka oleh Agus Salim selaku ketua ACE Banten.

Agus Salim, Ketua ACE Banten (kiri) bersama Ketua PHRI Banten dan GM Hotel Allium (bd)

Para sales dari Brother dan ACS Group bekerjasama memberikan penjelasan kepada para peserta seminar yang menghampiri booth Brother.

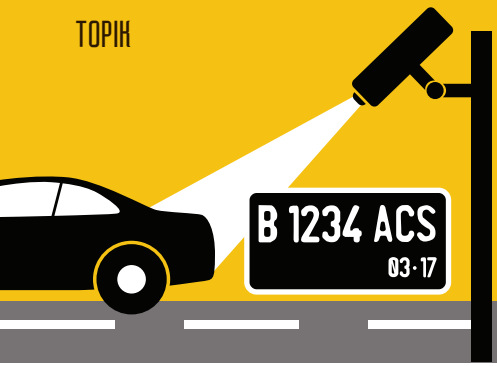
Nanda Pranawa, Sales Corporate - Brother, menyampaikan presentasi produk solusi printer Brother.

7th Anniversarry & Gathering
HUT Professional IT - Bali

Dalam rangka HUT Professional IT - Bali yang ke 7, pada pada tanggal 25 Februari 2017 para pengurus PROFIT IT-Bali mengadakan acara 7th Anniversarry & Gathering dengan thema "WORK SMART PLAY SMART" bertempat di Harris Hotel & Residence Sunset Road, Kuta - Bali dihadiri kurang lebih 250 anggota. Pada acara ini ACS Group bekerjasama membuka booth dengan PT. Sistech Kharisma(disti produk Aruba Networks) dan PT. Avnet Datamation Solution(disti Fortinet).

[1]Acara dibuka oleh Arya Sumerastha selaku COO Profit IT. [2]ACS Group ambil bagian dalam memberikan presentasi produk, untuk presentasi produk HP Aruba Networks disampaikan oleh Karel Martinus Widjaja, Product Manager - Hewlett Packard Enterprise dan [3]presentasi produk solusi security Fortinet dibawakan oleh staff ACS Group sendiri yaitu Jemis Pangaribuan, Technology Development Manager.

Para pengunjung yang mendatangi booth ACS Group untuk mendapatkan pengetahuan/ jawaban atau solusi yang dapat diterapkan di perusahaan mereka dan kunjungan ke booth ini menjadi lebih banyak setelah kedua presenter menyampaikan presentasi mereka.



LPR
License Plate Recognition

Hikvision sebagai produsen Camera Smart IP telah berkiprah di Indonesia dalam bisnis perangkat pendukung keamanan yang dimulai sejak tahun 2001. Meski belum terlampau lama namun sepak terjang keberadaan produknya telah didahului di pasaran Eropa kemudian area Asia. Alasan mengincar pasar Eropa lebih dahulu karena negara-negara di Eropa telah mature, meski lebih baik dari sisi teknologi terapan, namun bukan berarti minim dari kejahatan.

Dengan begitu, industri camera smart IP di Indonesia akan lebih bervariatif dan konsumen dapat memilah mana yang diperlukan. Dengan cara penjualan seperti ini Hikvision sebagai pemegang lisensi teknologi tentu tidak merasa berkeberatan karena dengan cara seperti ini juga akan menambah benefit bahwa produk teknologi yang diproduksi digunakan secara masal dan masif.

Terdapat beberapa aplikasi yang menjadi keunggulan dari camera smart IP Hikvision, salah satu yang dibahas saat ini adalah LPR.

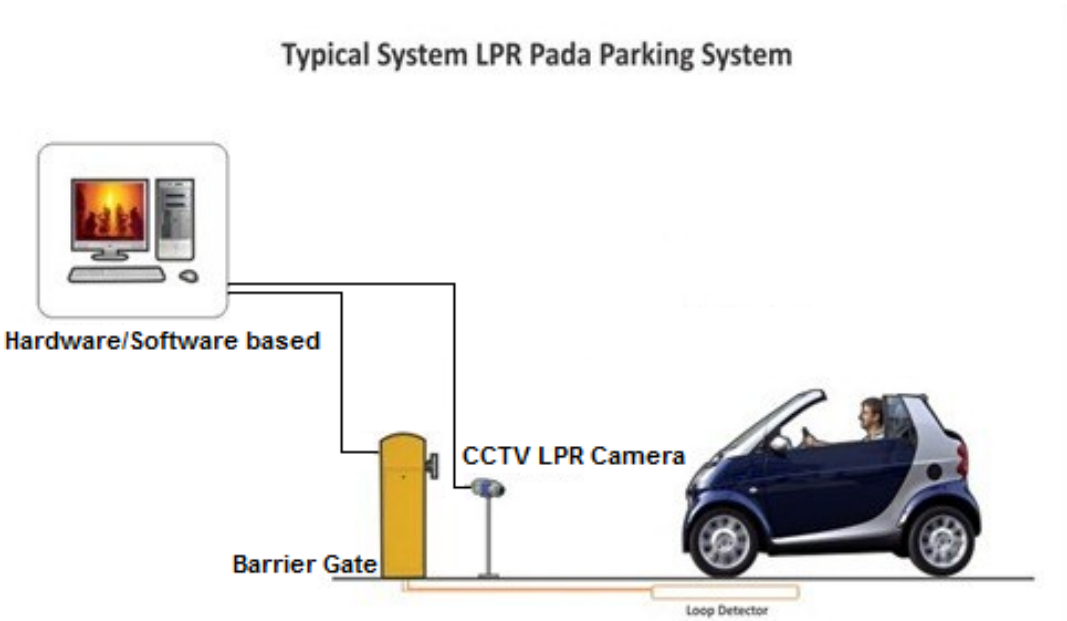
Gambar 1. Hasil gambar LPR pada camera Hikvision

LPR (License Plate Recognition) adalah salah satu fitur CCTV untuk mengenali plat nomor kendaraan. Adapun penggunaan LPR diantaranya adalah sebagai berikut:

- Identifikasi plat nomor kendaraan secara otomatis
- Sistem parkir otomatis dimana pintu garasi/ gerbang dapat terbuka secara otomatis hanya dengan mengenali plat nomor penghuni.
- Otomatisasi sistem Parkir pertokoan. Dengan LPR sistem dapat mencatat plat nomor mobil yang masuk secara otomatis.
- Access Control komplek perumahan atau apartment yang memungkinkan hanya kendaraan penghuni yang dapat masuk komplek.

Pada Camera Smart IP Hikvision aplikasi yang dibenamkan langsung dan tidak menggunakan software pihak ketiga seperti yang ada pada kebanyakan CCTV, Hikvision membenamkan aplikasi ini langsung di dalam unit. Aplikasi ini digunakan sebagai pendeteksi nomor polisi kendaraan bermotor dan mampu menangkap nomor kendaraan meskipun dalam kecepatan tinggi hingga 200km/ jam.

Perlu diketahui juga bahwa kemampuan rekam ditentukan dengan scanning area serta jarak zoom atau maksimum megapixel, semakin jauh atau semakin detail maka Hikvision mampu membuat unit dengan spesifikasi yang diinginkan. Inilah yang menarik bahwa, seperti apapun keinginan konsumen maka Hikvision bisa mewujudkan karena teknologi yang dimiliki secara terapan bisa diaplikasikan hanya saja dikompensasi dengan harga yang juga relatif mahal atau murah tergantung dengan spesifikasi yang diinginkan.



Gambar 2. Parking system dengan LPR Camera

Sepak bola Teknologi Passion

"Bagi Sales & Marketing Director ACS Group, Bapak Ir. Aryanto Hartanto, tiga hal ini yang merupakan beberapa rahasia beliau dalam jenjang kariernya yang sukses selama 25+ tahun. Pengalaman seorang yang akrab dipanggil Pak Ar ini merupakan cerita yang berbuah nilai-nilai positif bagi kalangan partners dan corporate. Bagaimana cara beliau berhasil melewati perubahan trend teknologi? Tips apa yang bisa dibagikan kepada para pembaca? Yuk kita simak di wawancara Kolom Insprasi berikut ini."

Ceritakan perjalanan karier Anda dari asal mulanya hingga sampai sekarang.

Saya mulai bekerja di Autojaya Januari 1996, sebagai seorang Sales Executive. Pada awalnya fokus hanya menjual solusi Cabling & Networks Devices. Masuk tahun ke 4 (tahun 2000) business-direction berubah, management menginstruksikan saya untuk fokus menjual solusi AIDC (solusi Bar Code). Saat sedang seru-serunya berjualan solusi Cabling & Networks, saya mengikuti arahan management dan mulai belajar menjual solusi Bar Code. Berkat bimbingan manajemen dan semangat kerja sama tim yang sangat memotivasi saya, tidak terasa 20 tahun sudah saya berkarya dan berkembang di perusahaan ini.

Apa yang membuat Anda gemar dengan sektor Teknologi-Informatika-Komunikasi (TIK)?

Saya menyenangi Teknologi Informasi dan Telekomunikasi karena alasan yang sederhana. Bagi saya teknologi khususnya teknologi informasi dan komputer itu keren banget. Mungkin karena doktrin dari Ayah saya yang seorang insinyur teknik mesin yang gemar teknik elektro, dan ditambah dahulu hobi saya nonton filem 'science fiction'..hehe. Selain itu , teknologi adalah buah pikiran manusia yang bermanfaat bagi kehidupan.

Sepanjang pengalaman kerja Anda, project mana yang paling berkesan dan mengapa?

Tidak ada proyek yang paling berkesan. Semua proyek yang saya dapatkan dan saya kerjakan, saya syukuri dan nikmati prosesnya. Tentunya semakin

besar dan kompleks suatu proyek semakin seru untuk dimenangkan dan dikerjakan. Jujur dan tekun adalah kunci keberhasilan. Pada tahun 2000 ada satu account retail yang dihibahkan kepada saya untuk dikelola, dan diawali dengan masalah besar. Dimana 25% dari 70 unit produk yang dibeli, mengalami kerusakan padahal umur produk baru 3 bulan. Pelanggan kecewa dan menuntut pertanggung jawaban. Saat yang sulit, namun dengan spirit 'tidak lari dari permasalahan', dukungan 'principal' dan tim Engineer yang mumpuni, permasalahan bisa ditangani. Namun, kekecewaan tidak langsung terobati. Saat sulit belum berlalu. Trauma mengakibatkan Pelanggan memilih produk kompetitor untuk tahapan kebutuhan berikutnya. Namun dengan tekun kunjungan demi kunjungan tetap dilakukan, dan walhasil , puji syukur, hingga detik ini Pelanggan tersebut menjadi salah satu Pelanggan yang paling loyal dan rutin belanja produk dan solusi kami setiap tahunnya.

Anda sudah bekerja di ACS Group lebih dari 20 tahun. Apa yang Anda suka dengan perusahaan ini?

Yang membuat saya kerasan disini adalah: kami diberi kesempatan, ruang gerak dan dibimbing untuk berkembang saling bahu membahu dalam suasana kekeluargaan. Tempat kerja benar2 menjadi rumah kedua bagi saya. Saya sangat beruntung bisa selama ini berkarya disini.

Karakteristik apa yang Anda cari ketika merekrut orang ke dalam tim Anda?

Jujur, memiliki passion untuk berkembang dan belajar.

Kami dengar Anda penggemar sepak bola dan Liverpool FC. Apa yang anda suka dengan tim julukan The Reds ini?

Saya bermain sepak bola sejak kelas 1 SD. Saat ini masih gemar bermain, 1 minggu 1 kali kami bermain fustsal. Bermain sepak bola itu menyenangkan dan keren. Kerja sama tim kunci kemenangan indah. Saat terciptanya gol, seluruh anggota tim akan meledak gembira dan merayakannya. Penghargaan pun diberikan kepada seluruh anggota tim. Saatnya kalah, kita saling menguatkan. Benar bahwa saya penggemar Liverpool FC , itu dimulai pada awal masa kuliah (tahun 1986). Saat itu saya dan Ayah senang nonton siaran langsung liga Inggris di TV. Ayah saya penggemar Arsenal – The Gunners. Saya pikir tidak seru kalau sama club kesayangannya. Saya cari club rival yang paling tidak disuka beliau, yaitu Liverpool FC. Maka sejak itu saya jadi pembela LFC. Haha…memory yang indah.

Full Name : Arijanto Hartanto
City of Residence : Tangerang Selatan, BSD
Current jabatan : Sales & Marketing Director
Hobbies : Futsal, Traveling, denger musik, nonton liga Inggris.

Education

S1 Itenas Bandung - Teknik Elektro

Work experience

PT. Masaro Oktober 1993 – November 1995 Teknisi dan Sales; PT. Autojaya Idetech , Jan 1996 hingga kini

Family

Menikah, 1 orang putra 13 tahun

Seluruh Staff dan Management
ACS Group mengucapkan

Selamat Hari Raya

Nyepi

Tahun Baru Saka 1939

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

KOLOM KETAWA

SIAPA TAKUT!

Kamirun pulang sendirian sehabis begadang di kampung sebelah. Saat itu tepat malam Jum'at kliwon, yang menurut banyak orang dianggap sebagai malam paling seram. Jalanan memang terlihat gelap, tanpa ada penerangan lampu, apalagi hujan turun rintik-rintik menambah suasana mencekam.

Kebetulan di jalan yang gelap itu, Kamirun harus melewati kuburan yang angker, banyak orang telah melihat penampakan saat melewati jalan itu terutama di malam Jumat. Benar saja, baru melangkah sebentar, tiba-tiba muncul hantu kuntilanak tepat di depannya. Meski merasa terkejut, namun Kamirun tidak merasa takut. Dia justru meledek kuntilanak itu.

Kamirun: "Hmm.. sudah pakai baju putih kumal lagi. Enggak pernah dicuci, barangkali ya Mbak? Padahal Mbak kan wanita, seharusnya malu?"

Kuntilanak merasa malu dan ngeloyor pergi karena merasa gagal membuatnya takut.

Melihat Kuntilanak dipermalukan, hantu pocong melompat ke depan si Tukimin. Namun, dia terkejut karena bukannya kabur, malah tertawa ngakak.

Kamirun: "Ya, ampun. Ini lagi.. Hantu kok payah banget. Sudah tahu jalan di sini mulus dan diaspal, kenapa harus lompat-lompat?"

Pocong pun tersipu malu dan melompat pergi.

Melihat keberanian Kamirun, hantu yang lain mulai merasa penasaran dan jadi kepo. Semua hantu penghuni makam mulai dari sundel bolong, pocong, tuyul, suster ngesot, genderuwo, hingga nenek gayung serempak menampakkan diri di depan si Kamirun. Namun hasilnya sangat mengecewakan para hantu, karena Kamirun masih lempeng, tanpa ekspresi rasa takut sama sekali.

Kamirun: "Percuma saja kalian mau jungkir balik untuk menakutiku, enggak ngaruh kok. Kalian kudu tahu kalau di dunia ini enggak ada yang bisa buat aku takut! Oke?!! " katanya sambil tertawa ngakak.

Kumpulan hantu itu pun menyerah, satu persatu mereka kembali bobok manis di dalam kuburan.

Tiba-tiba dari kejauhan terdengar suara teriakan seorang wanita yang memanggil Kamirun.

Perempuan: "Mas!! Kemana aja sih dari maghrib begadang enggak pulang-pulang? Awas ya, kalau pulang aku kemplang kepalamu sampai peyang!"

Kamirun tiba-tiba pucat, lalu segera lari bersembunyi di balik batu nisan.

Tuyul: "Eh, bro.. Hati-hati kepalaku terinjak, tahu?"

Kamirun "Psst.. Jangan berisik dong. Jangan sampai aku ketahuan kalau sembunyi di sini bisa bahaya."

Tuyul pun jadi kepo: "Memangnya, siapa yang nyari Bang, sampai gemeteran begitu?"

Kamirun: "Istriku, tau!"

Tuyul pun terjengkang: Ternyata!

ZEBRA VC80
Vehicle Mount Mobile Computer

Produk solusi untuk sektor industri : Warehouse, Manufaktur, Distribusi, dan Transportasi & Logistik.

VC80, merupakan produk yang didesain secara compact dan mudah untuk di-install di forklift, clamp truk, Crane dan banyak lagi. Produk yang super rugged ini tahan terhadap debu dan air dengan rating segel IP66 dan didukung full Windows untuk mampu beroperasi di area indoor maupun ouutdoor. Dapat beroperasi pula di area cold storage sampai suhu di -30° karena produk ini memiliki smart sensor suhu yang secara otomatis dapat mengontrol heater dan kecepatan untuk pemanasan touchscreen, board elektrik dan baterai.

ZEBRA MC36
Mobile Computer

Produk solusi untuk sektor industri : Transportasi dan Mobilitas di lapangan(Field Mobility)

MC36 hadir dengan ukuran layar 4.3” WVGA color sehingga mudah dibaca bahkan di luar ruangan sekalipun, produk ini diperkuat oleh processor 1.3 GHz quad core dengan operating system AndroidTM 4.4.2 KitKat yang memudahkan penggunaannya bagi para user. MC36 dengan rating segel IP65 merupakan produk rugged, tahan terhadap debu dan cipratan air/ basah serta tahan terhadap benturan pada kejatuhan berjarak 1.2M. MC36 memiliki pula dual slot kartu SIM untuk konektivitas jaringan yang berbeda bagi para pekerja yang melakukan perjalanan ke beberapa wilayah agar tetap terkoneksi dengan jaringan untuk aktivitas pekerjaannya secara online.

Honeywell
PD43 & PD43c Thermal Printer

Produk solusi untuk sektor industri : Distribution Center, Warehouse, Pelayanan Penumpang di Bandara.

Printer label PD43 dirancang super compact dan handal untuk memberikan kinerja dalam pencetakan label untuk ukuran lebar mulai dari 19 mm(0.75”) sampai118 mm (4.65”). Printer berbahan chasis metal yang rugged, dilengkapi display color dengan 10 bahasa untuk melakukan set-up dan juga support untuk comprehensive printer command language termasuk ZSim2. PD43 dapat menjalankan aplikasi di dalam printer, control peripheral sehingga mudah digunakan tanpa terhubung dengan PC.

ARUBA CLEARPASS POLICY MANAGER

Produk solusi RFID untuk sektor industri : Seluruh sektor Industri

ClearPass Policy Manager Aruba akan memberikan peran dan access control pada jaringan sehingga perusahaan dapat memastikan akses terpercaya ke jaringan dan aplikasi bisnis mereka baik untuk karyawan, kontraktor bahkan para tamu yang terhubung melalui kabel, nirkabel maupun VPN. Clearpass sudah di built-in dengan context-based policy engine RADIUS, dan didukung oleh protokol TACACS +, device profiling & comprehensive posture assessment dan pilihan untuk mengakses tamu yang masuk ke jaringan serta kelebihan-kelebihan dari fitur lainnya yang membuat ClearPass tak tertandingi sebagai dasar untuk keamanan jaringan dalam organisasi apapun. Memiliki cakupan keamanan yang lebih luas, menggunakan firewall, EMM dan existing solusi lainnya.

PRODUCT HIGHLIGHT

TRAINING
Extreme Networks Certified Expert Certification

Congratulation untuk Dasa Aprily Ardy & Junior Silalahi, pada tanggal 21 November hingga 2 Desember 2016 lalu mereka telah mengikuti training sekaligus mengikuti ujian di Extreme Networks - Singapura dan berita baiknya mereka berhasil lulus dengan memperoleh sertifikat peringkat Excelent.
Extreme Networks merupakan perusahaan penyedia layanan dan solusi networking yang telah bekerjasama dengan ACS Group.
Lulusnya kedua engineer kami ini patut disyukuri dan hal ini menjadi value added bagi ACS Group untuk terus memberikan dukungan secara maximal bagi seluruh para pelanggan setia kami. Dan ACS Group juga akan terus meningkatkan kapasitas & transfer knowledge bagi para staffnya.

Berfoto bersama trainer Alvin, Dasa Aprily Ardy (no 3 dari kiri) & Junior Silalahi (no 7 dari kiri).

SEMINAR
HP Aruba Conference

Irvan Kurniawan-Enterprise IT Solutions Manager, Adrian Dewantoro - Branch Manager Semarang dan Ricky Efraim Lie-Technology Services, selama 3 hari berturut-turut mengikuti seminar HP Aruba Conference bertempat di Marina Bay Sands, Singapura. Pada seminar ini mereka memperoleh transfer knowledge berkaitan dengan mobility, security dan GenMobile yg ada di Asia Pasifik, info Peluncuran Program Mitra baru dan berbagai info lainnya.

TRAINING
Product Update Zebra Technology

Pada tanggal 24 Februari 2017 bertempat di Gedung ACS Group Jl. Gunung Sahari Raya, para sales ACS Group mendapatkan training product update dari Zebra Technology. Para sales dibekali berbagai info produk baru, spesifikasi dan penerapan solusinya di lapangan.
Training disampaikan oleh Lie Kiat Chia - Zebra EMC Knowledge Worker, Portfolio Asia Pasific.

8 TIPS UNTUK MENINGKATKAN KEAMANAN PERANGKAT IOT

Kehadiran perangkat Internet of Things (IoT) sudah demikian derasnya dan terus bertumbuh, perangkat IoT dengan teknologi canggih dan terintegrasi ini menyisakan ruang untuk ancaman keamanan yang potensial seperti hacker dan malware. Berikut sedikit tips untuk meningkatkan keamanan perangkat IoT yang terhubung dengan koneksi internet, yakni:

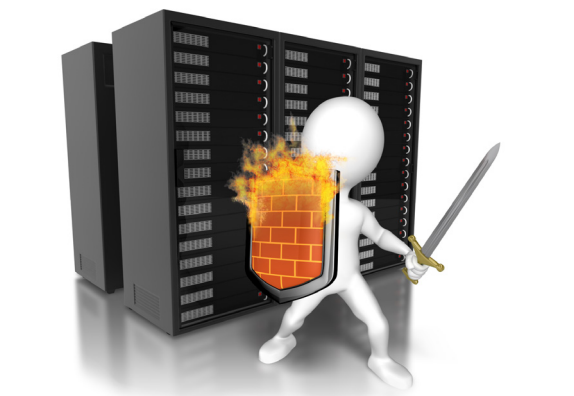
1. **Mengetahui perangkat apa yang terhubung.**
   Sebelum dapat mengamankan perangkat, sebaiknya tahu perangkat apa yang rentan terhadap serangan. Kemampuan untuk mengidentifkasi perangkat yang terhubung merupakan langkah awal dari pengamanan.

2. **Lindungi semua perangkat dan account dengan password yang kuat.**
   Setiap perangkat IoT dengan account berbasis internet harus dilindungi dengan nama pengguna yang kuat dan password yang mencakup kombinasi dari huruf, angka, dan simbol. Hindari menggunakan password yang sama untuk beberapa account. Karena jika berhasil diretas maka akan memiliki akses yang lebih luas ke perangkat.

3. **Hindari menggunakan koneksi internet yang tidak aman.**
   Jangan menggunakan koneksi internet yang tidak aman karena dapat membuat perangkat rentan terhadap hacking dan serangan. Untuk meningkatkan keamanan jaringan, buatlah password yang kuat untuk koneksi internet dan update secara berkala.

4. **Buat Jaringan yang terpisah untuk perangkat IoT.**
   Banyak perangkat router sekarang ini yang memungkinkan untuk mengatur beberapa segmen atau kelompok jaringan. Lakukan konfigurasi router untuk membuat setidaknya satu jaringan yang terpisah untuk perangkat IOT. Karena semakin banyak segmen dalam jaringan, semakin sulit bagi hacker untuk mengakses semua perangkat dan informasi.

5. **Pasang Firewall.**
   Firewall membantu mencegah hacker, virus, dan worm yang menyerang perangkat yang terhubung melalui Internet dengan melalui lalu lintas jaringan yang tidak seharusnya. Beberapa sistem menawarkan fungsi firewall secara default, yang sudah cukup untuk banyak pengguna. Untuk perlindungan tambahan, install perangkat firewall yang menawarkan fungsi keamanan yang lebih, atau lakukan konfigurasi perangkat firewall yang lebih advanced untuk keamanan jaringan yang lebih luas dan yang lebih baik.

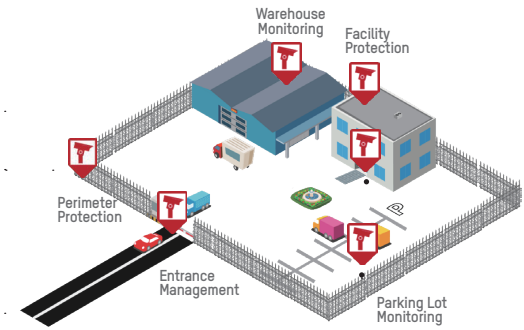


6. **Segera lakukan Patch akan Security Update.**
   Beberapa perangkat pintar secara rutin merilis update sistem yang menangani masalah pengguna dan kelemahan keamanan. Dengan menginstal update yang telah tersedia membantu untuk tetap terlindungi. Periksalah situs web masing-masing produsen perangkat untuk update fitur keamanannya. Bahkan beberapa perangkat bahkan memiliki fungsi pengaturan yang memungkinkan instalasi update secara otomatis.

7. **Lepaskan koneksi perangkat ketika tidak digunakan.**
   Matikan semua perangkat pintar bila tidak digunakan, pastikan port perangkat ke jaringan tidak dalam keadaan aktif sehingga menciptakan hole atau celah lubang keamanan yang dapat disusupi oleh hacker. Beberapa perangkat switch pintar saat ini, sudah dapat melakukan verifikasi suatu perangkat sebelum masuk ke jaringan.

HIKVISION

A PERFECT SYSTEM
DEVOTED TO PRODUCTIVITY AND PARKING SECURITY
SMART INDUSTRIAL PARKS SOLUTION



smart solution 2.0

INDUSTRIAL PARKS

Hikvision Indonesia

www.hiikvision.id

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

PRODUCT

- Bar Code (Label) Printers
- Bar Code Scanners
- Rugged Mobile Computers
- RFID Tags and RFID Readers
- Enterprise Wireless LAN
- Enterprise Wireless Broadband
- Security Networks
- Security System (CCTV, Access Control, Alarm System)
- IP PBX
- Consumable: Customize Label and various Thermal Ribbon

PROFESSIONAL SERVICES

- Wireless RF Site Survey and Wireless RF Performance Audit
- Installation and Commissioning
- Hardware Repair (On Call) and Maintenance Contract
- 24 x 7 Support Ready (with SLA and annual contract)
- Manage Services
- Application Software Package, such as:
  - Asset Management and Tracking System (AMTS)
  - Document Asset and Tracking System (DATS)
  - Mobile Meter Reading Solution (MMR)
  - Agro Data Integration System (ADIS)
  - Stability Program System (Stab-Pro)
  - Gate Access System - Vehicle(GAS-V)
  - STOCK KEEPER
  - PRODUCTION TRACKING

INDUSTRY SOLUTION

- Manufacturing
- Transportation & Logistics
- Retail & E-commerce
- Fast Moving Consumer Goods
- Hospitality
- Financial Services
- Education & Healthcare
- Agriculture & Mining

BUSINESS PARTNERS

ZEBRA PREMIER SOLUTION PARTNER · Honeywell PERFORMANCE PARTNER PROGRAM PLATINUM LEVEL · POINT Mobile · SEAGULL SCIENTIFIC · wavelink · IBM
brother at your side · FARGO Part of HID Global · Seuic · aruba a Hewlett Packard Enterprise company · FORTINET · Alcatel·Lucent Enterprise
hp Networking · Cambium Networks · Extreme networks · AXIS COMMUNICATIONS · HIKVISION · TelView

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

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(H); 8556278
Fax : +6231-8556279

Denpasar
Jl. Gatot Subroto I – XI, No 18
Denpasar Bali 80239
Telp : +62361-419284 (H)
Fax : +62361-424775