GEBYAR

BULETIN EDISI 39/JUNI 2017

# AUTO-ID

UNTUK KALANGAN SENDIRI

# MENGATASI PERKEMBANGAN CYBER THREATS DENGAN ADVANCED THREAT PROTECTION SYSTEM

## One Stop Shopping Services

Solusi teknologi baru dari
**Extreme Networks – Connect Beyond The Network**

**Tips & Trik** : Tips Mengamankan Jaringan Perusahaan Pada Pengguna dan Perangkat.

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**
Usadi Sastra Atmadja

**DESAINER**
Oscar Budi Trianto

**KONTRIBUTOR (PENULIS)**
Dasa Aprily Ardy
Taufiq Rahman
Tju Hansel
Irvan Kurniawan

**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

**Follow us on social media**

- autojayasolusi
- @barcoderfid
- @autojayasolusi
- https://goo.gl/Z8f47A
- https://goo.gl/uJJflx

# CONTENT



# EDITORIAL

Pada awal pertengahan bulan Mei 2017 yang lalu, dunia dihebohkan dengan kehadiran ransomware tipe baru yang sering disebut dengan nama WannaCry. Ransomware ini menyerang ratusan organisasi di belasan negara di dunia dan cukup membuat kerepotan dalam penanganannya. Hal yang membuat ransomware ini cukup unik dalam penanganannya dikarenakan sifatnya yang berbeda dari ransomware/malware yang sudah dikenal sebelumnya, ransomware WannaCry ini tidak membutuhkan interaksi user/korban dalam penyebarannya dan tipenya yang termasuk sebagai Zero-day Threats (unknown). Atau beberapa minggu sebelumnya ada peristiwa salah satu perusahaan telekomunikasi terbesar di Indonesia mengalami serangan atas website-nya, mengakibatkan tidak bisa diaksesnya website perusahaan telekomunikasi tersebut selama beberapa jam.

Beberapa contoh kejadian di atas adalah bukti bahwa dewasa ini ancaman serangan keamanan jaringan sangatlah berkembang, kompleks, terstruktur dan masif baik dari sisi teknologi, mekanisme dan bahkan teknik penyebarannya. Paradigma lalu tentang ancaman keamanan jaringan mungkin hanyalah berpusat pada lembaga keuangan, dipatahkan dengan adanya serangan ransomware WannaCry, yang dengan tidak kenal ampun menginfeksi bermacam sektor organisasi, bahkan lembaga pelayanan publik. Ini membuktikan perlunya solusi teknologi keamanan jaringan di semua segmen organisasi, baik kecil, menengah maupun organisasi yang besar.

Menyambung bahasan keamanan jaringan pada bulletin terdahulu tentang “Next-Generation Security for Enterprise Network”, di bulletin edisi kali ini yang kami beri judul “Mengatasi Perkembangan Cyber Threats dengan Advanced Threat Protection System” mencoba untuk menjelaskan fenomena perkembangan ancaman keamanan jaringan yang terjadi dan teknologi apa yang dibutuhkan untuk mengatasinya.

**Dasa Aprily Ardy**
**Technology Development Supervisor**

PT. Autojaya Idetech
PT. Solusi Periferal

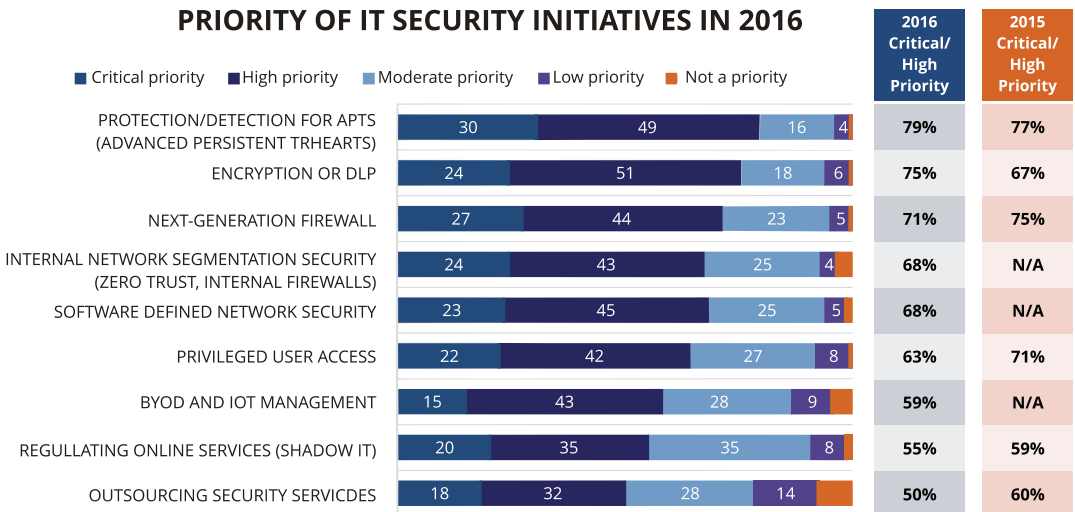
# MENGATASI PERKEMBANGAN CYBER THREATS DENGAN ADVANCED THREAT PROTECTION SYSTEM

Di jaman sekarang ini, dimana ancaman terhadap keamanan jaringan semakin berkembang dan kompleks setiap harinya, dibutuhkan satu teknologi yang kompleks pula untuk melawannya. Dimana muncul paradigma baru yang tadinya mungkin hanya mengamankan di salah satu titik dalam suatu jaringan, contoh: aspek end-client atau user-nya, menjadi bagaimana mengamankan aspek-aspek baik itu perangkat maupun user-nya secara menyeluruh di dalam jaringan perusahaan kita.

Salah satu fitur teknologi dalam pencegahan ancaman keamanan jaringan yang semakin kompleks itu diantaranya melebur fungsi firewall konvensional dan aplikasi antivirus ke dalam satu perangkat gateway di dalam jaringan, dimana perangkat tersebut akan memindai baik trafik transfer file maupun trafik mail attachment yang ada terhadap berbagai bahaya yang dapat mengancam keamanan jaringan perusahaan itu sendiri. Dan teknologi ini terus berkembang dengan fitur-fitur baru seperti URL *filtering*, *application control*, *anti-spam*, *anti-phishing* hingga ke spesifik mengamankan asset jaringan perusahaan seperti web maupun *database server*. Dari teknologi-teknologi baru pengamanan keamanan jaringan inilah muncul juga istilah-istilah baru.

> *"Did You Know: The top three industries affected by cyber attacks are Public Sector, Information Technology and Financial Services."*

Saat ini, salah satu istilah dalam industri keamanan



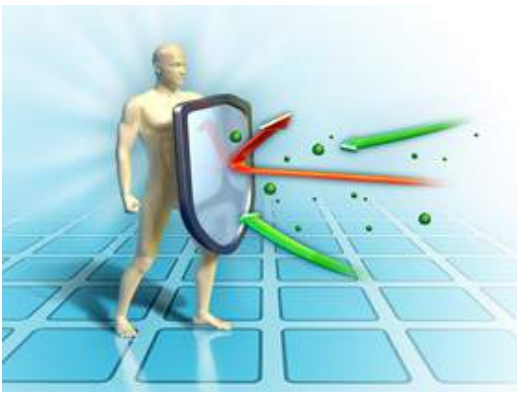

*Gambar 1. IT Security Priority, IDG Research 2016*

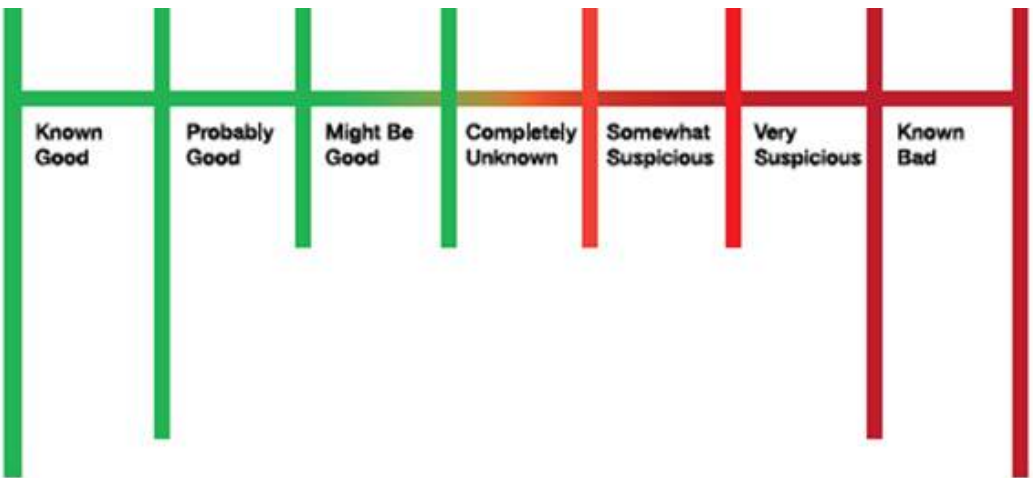
jaringan yang sedang hype namun yang paling tidak dipahami adalah ***Advanced Persistent Threat*** (APT), yang secara umum definisinya adalah ancaman akses yang tidak sah terhadap suatu jaringan secara terus menerus, dengan tujuan utamanya yaitu untuk mencuri informasi berharga. Dalam menanggulangi APT, dibutuhkan ketelitian maupun kejelian kita dalam mengamankan perangkat dan asset jaringan perusahaan, karena sifatnya yang dalam suatu waktu menggabungkan serangan terhadap sektor-sektor tertentu hingga eksploitasi bermacam *vulnerabilities* baik di sisi teknis maupun manusianya di dalam suatu organisasi, sehingga mengakibatkan kesulitan dalam mendeteksi maupun mencegahnya. Dan hal ini menjadi sulit untuk kita kategorikan terhadap istilah keamanan jaringan konvensional yang sudah umum sebelumnya, dimana sebelumnya kita hanya fokus terhadap satu titik ancaman keamanan tertentu di dalam suatu jaringan.

Dalam mengatasinya, yaitu melakukan pendekatan tradisional dengan mengintegrasikan berbagai macam vendor keamanan jaringan yang terbaik di segmen fiturnya, ibarat menjalankan sebuah kota dengan satuan polisi yang terbaik di spesialiasi unit masing-masing, tiap unit mempunyai kemampuan yang tinggi dalam mengatasi sebuah kejahatan, namun tanpa komunikasi maupun koordinasi diantara mereka. Dengan pendekatan di atas, ancaman keamanan yang spesifik terjadi mungkin dapat di atasi dengan efektif, namun tidak halnya untuk ancaman yang terkoordinasi dan secara terus menerus mengancam dalam suatu waktu yang bersamaan, karena tidak adanya integrasi sistem secara keseluruhan yang baik.

## Mencegah 'Known' Threats

Dengan mekanisme yang sama seperti sistem immune tubuh kita, dimana dalam tubuh manusia terdapat banyak lapisan pertahanan yang bekerjasama melawan gangguan yang tidak diinginkan ke dalam tubuh, begitu pula halnya dengan sistem keamanan jaringan modern yang ada saat ini, mempunyai konsep pertahanan berlapis- lapis dalam mencegah ancaman keamanan jaringan yang mungkin terjadi.






*Gambar 2. Known vs Unknown Threats*

*"Did You Know: 23% of recipients now open phishing messages and 11% click on attachments."*

Sebuah analogi yang dapat menjelaskan kesamaan antara sistem immune tubuh dan software antivirus adalah proses vaksinasi terhadap pathogen yang telah diketahui/known, dimana pathogen/virus komputer dideteksi dan dianalisis oleh pihak eksternal yang kemudian membuat sebuah vaksin/antivirus signature untuk mengatasinya. Vaksin/antivirus signature inilah yang akan digunakan kembali ketika terjadi infeksi pathogen/virus komputer yang sama di kemudian hari.

Namun tentu mekanisme itu akan berbeda apabila menyangkut gangguan pada jaringan komputer, dimana '*signature*' yang dimaksud sebelumnya juga bisa merujuk kepada pola akan prilaku akses jaringan yang mencurigakan dibanding hanya sebagai sebuah potongan code yang berbahaya. Namun, hasil akhirnya tetap sama, gangguan maupun ancaman yang sudah diketahui '*signature*'-nya tetap dapat dicegah sebelum terjadi.

## Mendeteksi '*Unknown*' *Threats*

Untuk kedua mekanisme baik immune tubuh dan jaringan perusahaan yang dijelaskan sebelumnya, gangguan dari ancaman yang belum dikenal atau belum ada vaksin/antivirus sayangnya tidak dapat dihindarkan, dan efek gangguan yang dihasilkannya tergantung dari seberapa cepat dan efektif gangguan itu dideteksi, dikarantina lalu diberantas.

Sama seperti sistem kekebalan tubuh manusia yang setiap waktu secara terus menerus mengawasi gangguan yang mungkin masuk ke dalam tubuh, begitu juga seharusnya dengan jaringan perusahaan, harus tetap waspada terhadap perilaku akses jaringan yang tidak biasa ataupun *malicious code*. Untuk melakukan ini, jaringan perusahaan harus mengandalkan perangkat teknologi yang tidak hanya melakukan analisa perilaku akses jaringan namun juga dapat melakukan sandboxing.

*"Did You Know: In 60% of cases, attackers are able to compromise an organizations within minutes."*

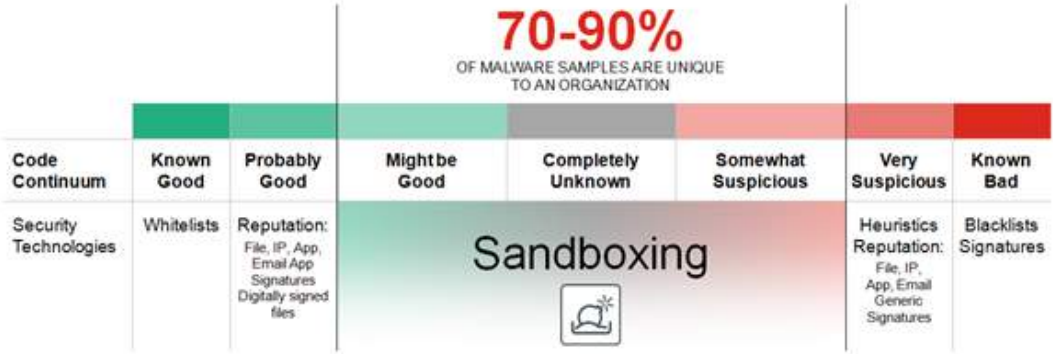
Dengan monitoring secara terus menerus dan juga membandingkan perilaku akses jaringan dengan parameter dasar 'normal' yang ada, dimungkinkan untuk mendeteksi lebih awal akan tanda-tanda dari sebagian besar gangguan ancaman jaringan. Dikombinasikan dengan *database* pengetahuan yang terperinci tentang bagaimana beberapa ancaman terjadi, dapat mendeteksi secara akurat dan cepat untuk sebagian besar ancaman yang sama sekali tidak dikenal sebelumnya.

Mendeteksi sebuah *malicious code* yang tidak dikenal sebelumnya (belum ada signature antivirus/ penanganan) yang mungkin saja merupakan sebuah ancaman keamanan jaringan, baiknya dilakukan dengan 2 cara.

**Langkah pertama**, meskipun *malicious code* tersebut mungkin adalah dalam 'bentuk' yang baru, namun biasanya terdapat parameter-parameter *coding* yang sudah umum digunakan dan dapat dikenali melalui teknik *deep packet inspection* dengan '*signature*' yang *up-to-date*. Namun lain halnya untuk *malicious code* yang memang benar-benar baru baik secara coding maupun bentuknya (biasa disebut *zero-day threats*), langkah terbaik yang dapat dilakukan saat ini adalah dengan menggunakan perangkat keamanan jaringan yang dikenal dengan sebutan sandbox. Sandbox digunakan bertahun-tahun oleh tim peneliti ancaman keamanan jaringan, hanya saja baru-baru ini teknologi sandbox diperkenalkan untuk digunakan dalam lingkungan keamanan jaringan perusahaan. Ide dasar dari teknologi sandbox ini adalah menyediakan lingkungan terisolasi yang aman, dimana nantinya digunakan untuk menguji setiap file mencurigakan yang akan memasuki jaringan. File seperti ini di-*execute* tanpa harus membahayakan jaringan utama operasional perusahaan itu sendiri. Proses ini dapat di-monitor dan hasilnya menentukan apakah file yang dicurigai tersebut benar-benar sebuah ancaman keamanan atau tidak.

*"Did You Know: 75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours)."*

**Langkah yang kedua** adalah dengan tidak membiarkan teknologi sandbox tertipu oleh teknik-teknik menghindari deteksi seperti *logic bombs*, *rootkits* atau *bootkits* dan lainnya. Sadar akan meningkatnya penggunaan teknologi sandbox di dalam suatu jaringan perusahaan, membuat para




*Gambar 3. Verizon Data Breach Investigations Report, April 2016*

penjahat dunia maya untuk lebih mengembangkan berbagai teknik menghindari deteksi yang lebih kompleks, sebagian besar memanfaatkan kelemahan dari teknologi sandbox dimana lingkungan virtual yang ada di sandbox tidak sama dengan kondisi operasional jaringan sebenarnya. Mereka mengeksploitasi kelemahan sandbox itu dengan mengembangkan *malware* yang lebih canggih yang akan aktif apabila dijalankan di kondisi operasional jaringan sesungguhnya, sehingga sandbox tidak dapat mendeteksinya di awal. Satu-satunya cara untuk membalikkan teknik tersebut adalah melalui *advanced code emulation analysis*, dimana instruksi berbahaya terhadap keamanan jaringan seperti itu dapat dikenali/dideteksi, bahkan sebelum instruksi code tersebut dijalankan.

## Meminimalisir Dampak Dari '*Unknown*' *Threats*

Apabila kita mendeteksi adanya gangguan pada jaringan dari ancaman yang tak dikenal, ada 2 hal yang bisa kita lakukan:

- Segmentasi Area
  Untuk membatasi potensi kerusakan dari gangguan tersebut, segeralah lakukan segmentasi (karantina) terhadap area yang terdeteksi ancaman. Perkecil ruang geraknya agar tidak menginfeksi/memasuki sumber daya jaringan yang lain.
- Proses Analisa (Transisi dari '*unknown*' menjadi '*known*')

Setelah dibatasi ruang geraknya, gangguan ancaman tersebut haruslah dianalisa lebih lanjut untuk mengetahui potensi dampak dan resiko yang ditimbulkan, hingga proses dimana akhirnya gangguan tersebut menjadi '*known*' oleh perangkat-perangkat jaringan lainnya.

Di akhir dari kedua proses di atas, ancaman yang tidak dikenal tersebut haruslah di "ingat" oleh sistem jaringan kita sebagai database "*immune*" dalam penanganan ancaman gangguan yang sama di kemudian hari.

## Solusi Dari Fortinet

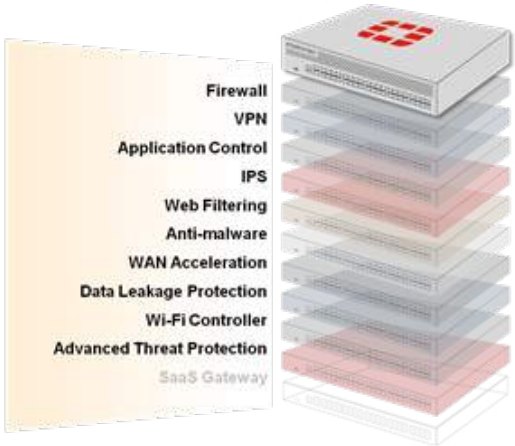
Fortinet sebagai salah satu vendor keamanan jaringan yang ternama, mempunyai 2 kelebihan unik dibanding competitor di segmen marketnya. Yang pertama adalah keunikan dari perangkat lunak Operating System-nya yang menjadi inti dari semua segmen produk dari Fortinet, kesatuan Operating System inilah yang mampu memberikan respons keamanan berlapis, integrasi, kolaborasi serta otomasi di setiap lini keamanan di dalam jaringan dalam menghadapi gangguan ancaman keamanan yang terus berkembang dan semakin kompleks setiap harinya.


Kelebihan Fortinet dibanding kompetitor yang

kedua adalah FortiGuard, yang merupakan sebuah jaringan riset global untuk ancaman keamanan jaringan, menyediakan "vaksin" bagi *known* maupun *unknown zero-day threat* di seluruh dunia selama 24 jam, 365 hari secara *realtime*. Sebagai member dari Cyber Threat Alliance dan lembaga-lembaga riset *threat* lain, Fortinet dengan FortiGuard-nya bertukar informasi akan segala ancaman keamanan jaringan baik yang *known* ataupun *unknown* yang sedang maupun akan terjadi di jaringan global dunia, sehingga respons dan efektivitas penangangan terhadap ancaman keamanan yang ada menjadi lebih cepat dan terotomasi secara pintar.

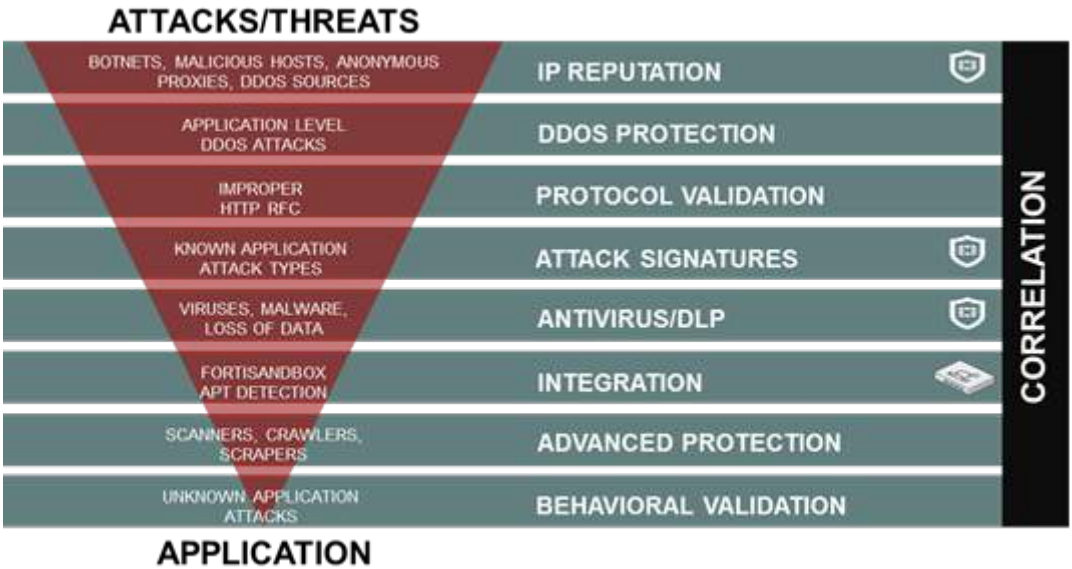
Atas ancaman *Advanced Persistent Threat* yang sudah kita bahas sebelumnya, Fortinet mempunyai solusi *Advanced Threat Protection system*, dimana kerangka solusi ATP dari Fortinet sebagai berikut:

- **Aspek LAN/WAN/Internet/Cloud via FortiGate**
  Di aspek ini identik dengan filtering terhadap semua trafik Ingress/Egress/Internal di dalam jaringan. Fortinet dengan FortiGate-nya, mempunyai peran sentral sebagai firewall, *next generation firewall*, internal segmentation firewall maupun unified threat management dalam mem-filter semua trafik tersebut. Ada 3 hal yang membuat FortiGate lebih unggul dibanding competitor dan menjadi yang teratas dalam laporan Gartner di segmen UTM (Unified Threat Management) selama tiga tahun berturut-turut.
  1. Perlindungan tanpa henti
     FortiGate bersama FortiGuard dalam hal layanan keamanannya mendapat peringkat teratas dari berbagai lembaga independen seperti NSS Labs dan Top Virus Bulletin Reactive & Proactive AntiMalware.
  2. Kemudahan monitoring dan konfigurasi
     Dengan sistem operasi FortiOS dan FortiView, melakukan konfigurasi hingga monitoring terhadap semua trafik jaringan yang terjadi menjadi sangat mudah.
  3. Performa yang tidak tertandingi
     Dengan *processor* FortiASIC-nya, yang dibuat secara khusus untuk menangani algoritma jaringan, membuat performa *throughput* dalam hal proses filtering konten maupun paket deep inspection jauh mengungguli kompetitornya.




*Gambar 4. FortiGate Security Features*

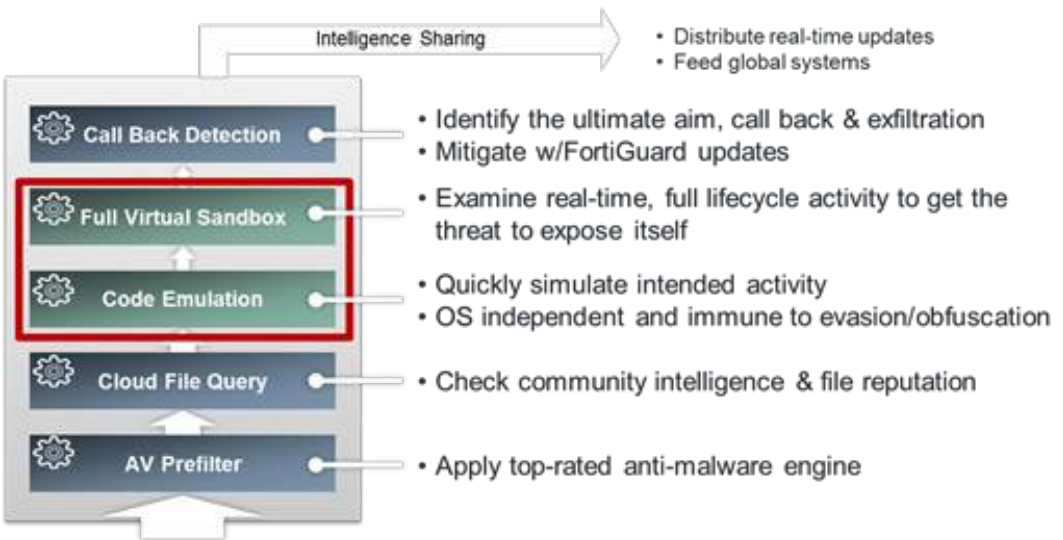
- **Aspek Email Server via FortiMail**
  Berbicara tentang trafik *email* dewasa ini tidak hanya mengenai clean dan unclean (*spam*) *email*, tetapi sudah menjadi media *virus/malware/phising/worms/spyware* yang paling populer penyebarannya saat ini. Dan ironisnya, menurut laporan dari Verizon tentang Data Breach Investigation pada April 2016 lalu, 30% dari pengguna email di seluruh dunia membuka link tautan *phishing site* dan 11%-nya meng-klik attachment yang ada.
  *FortiMail* melindungi data sensitif perusahaan dan membuat semua konten email bebas dari *spam/virus/malware* dan sejenisnya, sehingga produktivitas operasional karyawan juga akan meningkat.
- **Aspek Web Server via FortiWeb**
  Baru-baru ini *service provider* terbesar di Indonesia mengalami serangan pada halaman websitenya, gangguan tersebut mungkin tidak mengalami kerugian besar dalam hal materi/biaya pemulihannya, tetapi kerugian yang paling tidak bisa dhitung nilainya adalah reputasi perusahaan itu sendiri, karena celah keamanan yang bisa di-exploit pada aplikasi *web server*-nya. FortiWeb berfungsi melindungi *web* dan aplikasi *server* dari kemungkinan celah keamanan yang dapat di-*exploit* penyerang. Dengan mekanismenya




*Gambar 5. All Layers Protection dari FortiWeb*

yang melindungi di semua lapisan keamanan dari aplikasi maupun *web server*, dapat meminimalisir semua gangguan ancaman keamanan yang mungkin terjadi.

- **Aspek *Network* Sandbox via FortiSandbox**
  Elemen yang menjadi sentral dari kerangka *advanced threat protection system* dari Fortinet ini bertugas menganalisa setiap perilaku aktivitas jaringan secara dinamis, tidak hanya berpaku pada atribut-atribut statis saja, dalam mengidentifikasi yang tadinya sebagai *unknown threat/malware*.




*Gambar 6. Komponen Kunci dari FortiSandbox*

- **Aspek End Points via FortiClient**
  Terkadang kita melupakan aspek paling penting yang menjadi tujuan utama awal dari sebuah serangan yang terjadi, yakni aspek *end-points* (PC's/ /Smartphones/Tablets).
  FortiClient memberikan perlindungan terhadap ancaman *known* maupun unknown baik ketika *end-points* berada di 'dalam' maupun di 'luar' jaringan perusahaan, hingga menyediakan konektivitas yang aman di semua *device*.


*Gambar 7. FortiClient End-Points Protection*

Berintegrasi satu sama lain di dalam jaringan, kelima aspek produk ini membentuk *platform* Fortinet *Advanced Threat Protection*, yang secara cerdas dan kolaboratif bertugas untuk menangani 3 poin penting dalam menghadapi *advanced persistent threat* yang sudah kita ulas sebelumnya, yaitu:

1. Mencegah ancaman yang sudah diketahui/*known* masuk ke dalam jaringan.
2. Mendeteksi ancaman yang belum diketahui/ *unknown*, seandainya ancaman tersebut berhasil masuk ke dalam jaringan.
3. Mengurangi dampak dari setiap pelanggaran keamanan (*known*/*unknown*) yang terjadi dan memastikan bahwa hal serupa dapat dicegah di kemudian hari.


*Gambar 8. Kerangka Advanced Threat Protection Fortinet*

**Prevent**

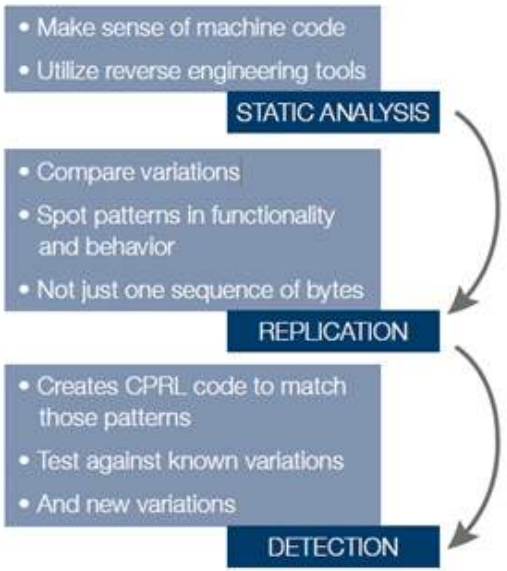
Langkah pertama dalam pencegahan a*dvanced persistent threat* adalah *identity control*, dimana harus dipastikan bahwa pengguna maupun perangkat yang tervalidasi dengan benar yang dapat masuk dan mengakses sumber daya jaringan yang ada.

Selanjutnya adalah teknologi pencegahan terpadu dari Fortinet, yang terdiri atas *antivirus*, *anti-phishing*, URL *filtering*, *intrusion prevention*, *application control* dan *endpoint control*. Komponen-komponen di atas menjadi bagian dari solusi *Advanced Threat Protection* dari Fortinet, dengan *engine* dari *antivirus* sebagai bagian yang paling critical disini.

Sebelumnya, mendeteksi signature dari sebuah *threat* pada dasarnya dilakukan dengan membandingkan ke *fingerprint database* dari sebuah *known malware*, dan sifatnya reaktif. Ini artinya, ancaman tersebut akan bisa dideteksi dan dicegah ketika menemukan signature yang sama persis dengan *fingerprint database malware* yang dimaksud, tapi ketika ancaman itu merupakan suatu coding yang benar-benar baru (*unknown*), otomatis ancaman itu akan lewat proses pendeteksian secara konvensional tersebut.

Fortinet mempunyai patent yang dinamakan *Compact Pattern Recognition Language* (CPRL), dimana teknologi ini berkerja secara proaktif

mendeteksi *signature threat* melalui *metode deep inspection*, yang caranya jauh melebihi pendeteksian secara konvensional. Hasil dari proses CPRL ini dapat mendeteksi 50.000 lebih varian malware baik *known* maupun *unknown*.




*Gambar 9. Compact Pattern Recognition Language (CPRL)*

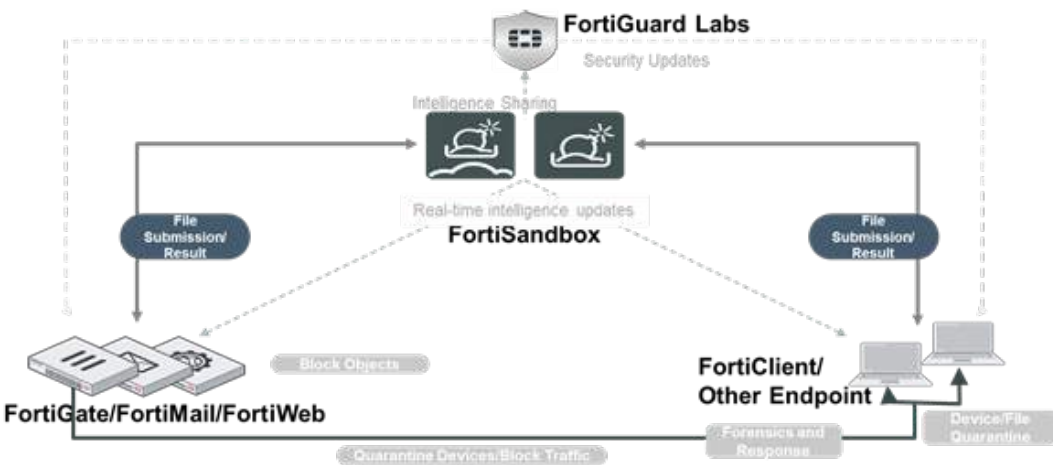
Dengan diterapkannya teknologi CPRL di semua lini produk dari Fortinet, indikasi ancaman *known* maupun *unknown* mayoritas dapat segera dihentikan, terlepas dari sisi sektor mana serangan itu datang, apakah *via email*, *web browsing*, *transfer* file bahkan USB *drive* yang sudah terinfeksi, semuanya dapat dikenali dan dicegah untuk masuk ke dalam jaringan.

**Detect**

Untuk membatasi kerusakan dari sebuah ancaman yang belum dikenal sebelumnya, dimana tidak ada *signature antivirus* ataupun *intrusion prevention* yang efektif saat ini, sistem pada jaringan kita haruslah waspada terhadap perilaku jaringan yang tidak biasa maupun *code-code* berbahaya setiap saat, kondisi ini dapat diatasi dengan sistem keamanan berlapis dari FortiGate dan FortiSandbox.

FortiSandbox merupakan perangkat *multi-layer* sandbox dengan fitur-fitur *pre-filtering* seperti *antivirus* yang sangat komprehensif, proses CPRL, dan akses cloud terhadap FortiGuard Labs, lembaga riset global untuk ancaman keamanan jaringan. Dan apabila tidak dapat diatasi oleh proses pre-filtering di atas, sampel-nya akan dilewatkan ke *virtual code emulation environment* di FortiSandbox, untuk dieksekusi, dalam menentukan apakah sampel file tersebut benar-benar berbahaya atau tidak.

Apabila sampel itu memang merupakan *code*




*Gambar 10. Bagaimana Kerangka ATP Fortinet Bekerja*

berbahaya, FortiSandbox akan membuat *signature* sementara terhadap sampel file itu dan meneruskannya ke semua komponen di dalam kerangka Fortinet *Advanced Threat Protection* (FortiGate/FortiMail/FortiWeb/FortiClient), dan *parallel* meng-*upload signature* tersebut secara detil ke FortiGuard Labs untuk dianalisa lebih lanjut dan juga pendistribusian global produk Fortinet di seluruh dunia.

## Mitigate

Ada beberapa proses yang akan dilakukan oleh FortiSandbox ketika ada indikasi keberadaan *malware* di dalam jaringan.

- ***Containment***
  Pada proses ini erat kaitannya dengan segmentasi jaringan, FortiGate dengan NGFW dan FortiGuard *services*-nya menyediakan baik segmentasi fisik maupun fungsional di setiap perangkatnya, dengan beragam pilihan interface berkecepatan tinggi dan akselerasi hardware melalui desain customisasi ASIC-nya. Dengan FortiOS sebagai perangkat lunaknya, segmentasi dapat dilakukan pada FortiGate berdasarkan beberapa kriteria seperti identitas pengguna, aplikasi yang digunakan, lokasi maupun jenis perangkatnya. Dengan cara ini, indikasi keberadaan *unknown malware* oleh FortiSandbox diteruskan ke FortiGate untuk disegmentasi di titik awal indikasi itu berada.
  Dalam hal known *malware*, FortiGate akan langsung melakukan segmentasi jaringan maupun karantina terhadap host yang dicurigai terinfeksi *malware* dan menginformasikannya kepada IT Security Manager agar dapat ditindaklanjuti lebih lanjut.
- **Analysis dan Memory**
  Di saat yang sama, analisa dilakukan secara menyeluruh terhadap *malware* sehingga yang tadinya *unknown* menjadi *known threats*. FortiSandbox lalu meng-*update knowledge* dari insiden ini ke FortiGuard dimana nantinya akan didistribusikan ke jaringan produk-produk Fortinet di seluruh dunia dalam bentuk *signature update*. Proses ini untuk mencegah terjadinya insiden *malware* yang sama di kemudian hari.

## Kesimpulan

Dengan persepsi yang sama tentang bagaimana sebuah obat mungkin tidak bisa secara 100% menyembuhkan infeksi penyakit yang menyerang tubuh manusia, begitu halnya pula dengan perlombaan yang terjadi antara penjahat dunia maya dengan mereka yang bertugas mengamankan data yang paling berharga di suatu organisasi, perlombaan tersebut tidak akan pernah selesai, dan takkan pernah ada pemenang di kedua belah pihak. Dengan diiringi kemajuan perkembangan teknologi di masing-masing pihak yang semakin hari menjadi semakin canggih, biasanya pihak yang 'bertahan' lah dalam hal ini IT Security Manager yang lebih membutuhkan semua pertolongan kemajuan teknologi yang ada.
Solusi *Advanced Threat Protection* sistem dari Fortinet dengan kerangka kombinasi dan kolaborasi yang unik, sifatnya yang semi-otomatis dalam mendeteksi segala ancaman, serta menyediakan sistem keamanan yang berlapis di semua elemen keamanan jaringan, pihak yang 'bertahan' dapat sedikit lebih diunggulkan dalam perlombaan tersebut.


*For Your Knowledge – WannaCry Ransomware*

Pada tanggal 12 Mei 2017 yang lalu, dunia dihebohkan dengan kehadiran Ransomware WannaCry yang menyerang ratusan organisasi di belasan negara. Ransomware ini mengeksploitasi *vulnerabilities protocol* SMBv1 yang ada pada OS Windows yang belum di-*patch*, mengenkripsi dokumen dan file pribadi dan menuntut "tebusan" berupa uang sekitar 300 USD dalam bentuk mata uang Bitcoin agar si korban dapat membuka file-file dan dokumennya kembali.
Ransomware WannaCry ini cukup membuat kerepotan karena sifatnya yang unik. Yang pertama,

ransomware ini tidak memerlukan interaksi *user* dalam penyebarannya, berbeda dengan ransomware terdahulu yang memerlukan campur tangan *user* (meng-klik tautan web atau file dalam email) dalam menginfeksi komputer korbannya. Dan keunikkan yang kedua karena sifatnya yang termasuk dalam *zero-day threat* (*unknown*), belum ada "vaksin" *signature*-nya.

Di hari yang sama pula sistem *Advanced Threat Protection* dari Fortinet menganalisa perilaku dari ransomware tipe baru ini dan dengan meyakinkan memblokir atas serangan unknown ransomware ini.

- FortiGate IPS mem-block vulnerabilities SMBv1 dengan mengeluarkan signature IPS dibulan yang sama Microsoft mengeluarkan Security Patch-nya (Maret 2017).
- FortiSandbox mendeteksi perilaku yang tak biasa atas *unknown* ransomware ini.
- FortiGuard AV mengeluarkan *signatures* dari ransomware ini.
- FortiWeb mengidentifikasi situs yang menjadi target dan dengan efektif memblokir ataupun mengizinkan aksesnya.
- FortiMail dengan AV signature dari FortiGuard memblokir akses ransomware via trafik email.
- FortiClient memblokir dititik awal ransomware memulai serangannya.

*/ Penulis : Dasa Aprili Ardy (ardy@acsgroup.co.id)


Seluruh Staff dan Management ACS Group Mengucapkan

Selamat Hari Raya

Idul Fitri 1438 H

Mohon Maaf Lahir dan Batin

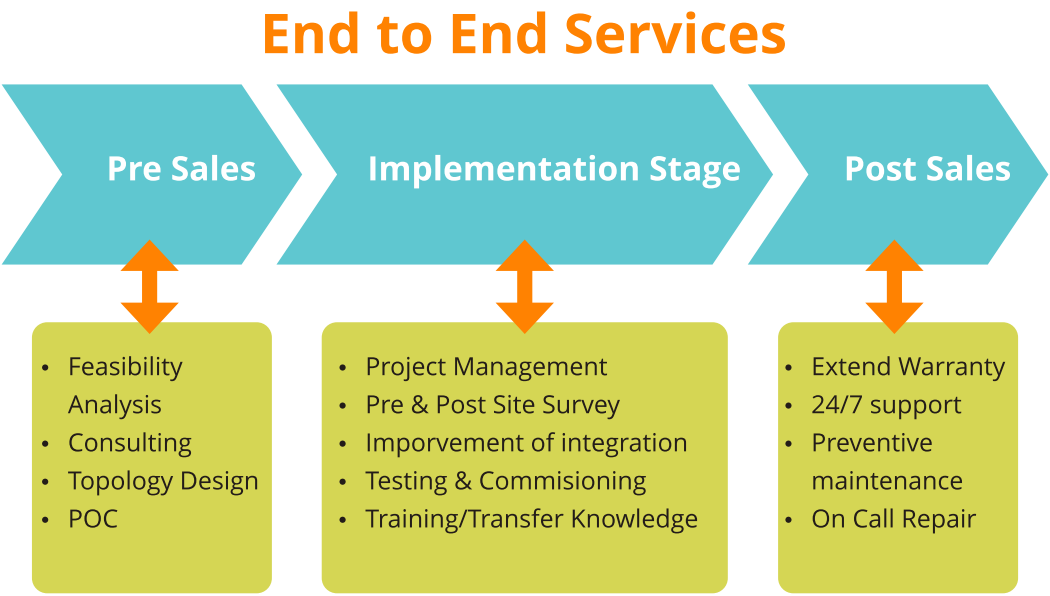
# ONE STOP SHOPPING SERVICES

Pada bulletin kami sebelumnya kami pernah membahas pentingnya suatu services dalam implementasi enterprise karena dalam pelaksanaannya membutuhkan suatu planning yang terencana, urutan kerja yang sistematis dan konsep yang sesuai dengan teknologi yang akan diterapkan.
Disamping itu juga melanjutkan topik utama kami yang sudah Anda baca yang membahas tentang *Advanced Threat Protection* System dari Fortinet yang mana solusi ini merupakan integrasi dari FortiGate, FortiMail, FortiWeb, FortiSandbox dan FortiClient. Implementasi dari solusi tersebut sangat membutuhkan keahlian khusus serta sertifikasi oleh principal yang concern terhadap hal tersebut yaitu Fortinet.

Untuk itu bagi perusahaan yang merencanakan untuk menerapkan Advanced Threat Protection System dari Fortinet dengan suatu *environment* yang kompleks, ingin terintegrasi dengan alat keamanan lainnya dan membutuhkan keamanan yang handal, serta kemudahan dalam hal instalasi, integrasi dan maintenance, maka kami ACS Group sebagai Fortinet Premium Partner siap untuk membantu Anda secara *end to end services*.

## A. PRE SALES

Agar tepat guna dalam penerapan Advanced Threat Protection sistem tentunya tak lepas dari perencanaan yang baik pada tahap awal.

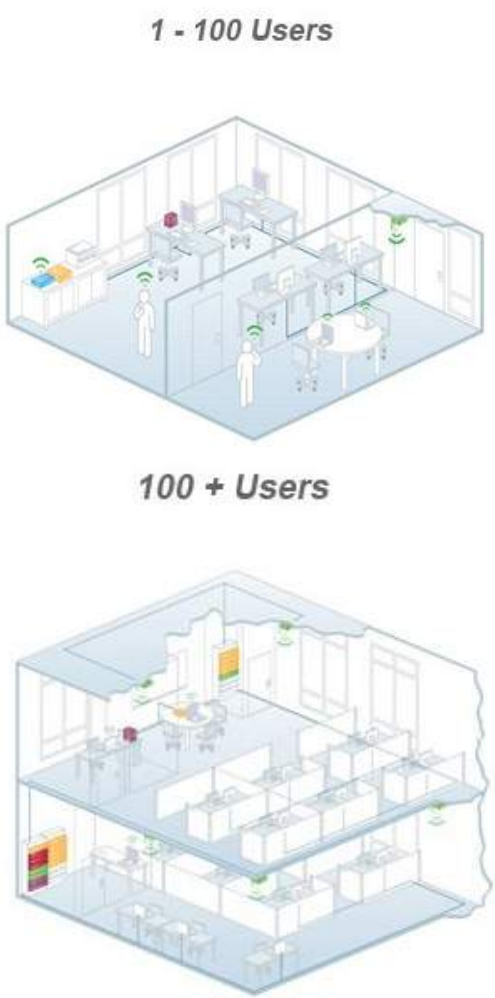



*Gambar 1. ACS Group Profesional Services.- End to End Services*

Berikut ulasan dari kami mengenai metodologi perencanaan kapasitas (*Planning Capacity*) :

1. Tentukan kapasitas yang ingin dicapai.
   *Advanced Threat Protection* sistem harus terlebih dahulu dimulai dengan mendefinisikan tujuan kapasitasnya. Tujuan kapasitas ini meliputi dua bagian, yang merupakan faktor kunci yang diperlukan dalam menentukan skala kapasitas yang benar dan menghasilkan desain proyek yang akan diimplementasikan, yaitu:
   A. Berapa jumlah total perangkat yang digunakan (*total number of devices*) : seringkali ini hanya diukur dengan jumlah user, atau jumlah "pengguna" di dalam suatu *environment*. Kadang-kadang, masing-masing user dapat mengandung lebih dari satu klien (yaitu, satu laptop dan satu *smartphone* Wi-Fi), artinya seseorang dapat saja membawa lebih dari 2 gadget. Hal ini penting karena setiap MAC *address* dari perangkat akan mengkonsumsi *airtime*, IP address, dan sumber daya lainnya dari jaringan.
   B. Minimum *bandwidth* per perangkat (*minimum bandwidth per device*) : Hal ini penting untuk dicapai mengingat nantinya akan adanya campuran antara data, suara, dan aplikasi video yang akan digunakan di dalam ruangan.

   Berikut adalah beberapa contoh statement yang jelas mengenai tujuan kapasitas yang lengkap dan apa yang mau dicapai:
   - "Setiap ruangan ada 30 staff yang masing-masing staff membutuhkan 2Mbps *throughput simetris*".
   - "*Auditorium/meeting room* menampung 500 orang. Masing-masing orang memiliki sebuah laptop yang membutuhkan minimal 350 Kbps untuk data dan sebuah handset suara yang membutuhkan minimal 128Kbps".
   - "Lantai *trading* harus melayani 800 orang, setiap orang membutuhkan minimal 512Kbps."




*Gambar 2. Kapasitas pengguna WLAN tidak diukur hanya dari kapasitas user di ruang tersebut*

Setiap skenario dalam perencanaan penerapan jaringan harus jelas dan terukur. Jangan lupa juga untuk mempertimbangkan kebutuhan kapasitas di masa depan. Mungkin saja jumlah user dalam suatu ruangan kantor akan berubah, namun dapat dipastikan bahwa jumlah radio 802.11 tentunya akan meningkat di masa depan.

Pastikan juga untuk mempertimbangkan lamanya pemakaian atau penggunaan sebenarnya dari setiap jenis perangkat yang digunakan pada saat menetapkan tujuan kapasitas. Dalam banyak kasus, belum tentu setiap perangkat memerlukan akses sampai pada kapasitas maksimum secara bersamaan (kecuali kalau memang ada aplikasi yang secara spesifik yang membutuhkan hal ini, seperti *interactive learning systems*/sistem pembelajaran interaktif pada lembaga pendidikan).

2. Tentukan berapa banyak pengguna di waktu yang bersamaan secara serentak (*concurrent user*)
   Langkah berikutnya adalah tentukan berapa jumlah maksimal *client* yang secara simultan sedang melakukan transmisi data yang dapat ditangani/di-handle. Tujuannya adalah untuk mengetahui batas praktis untuk jumlah perangkat client yang dapat mengirimkan secara simultan pada sebuah jaringan.
3. Perkirakan berapa total kapasitas bandwidth yang akan diimplementasikan.
   Gunakan matrix dari Fortinet atau software sederhana yang dapat melakukan kalkulasi untuk memperkirakan jumlah *bandwidth* pada suatu jaringan sesuai dengan kebutuhan *bandwidth* pada masing masing perusahaan dan juga sesuai dengan kebutuhan *bandwidth* aplikasi yang digunakan. Dengan menggabungkan antara aplikasi yang digunakan dan *bandwidth* yang ingin dicapai, kita dapat membuat ukuran sederhana yang memungkinkan dengan cepat dan menentukan sejumlah perangkat berdasarkan model atau tipe yang cocok.
4. Topology Design.
   Setelah mengetahui kebutuhan bandwidth maka langkah selanjutnya mendesign topologi *Advanced Threat Protection system* agar kita mengetahui overview design bagaimana konektivitas dan integrasi dengan perangkat lainnya dalam suatu network. Mengapa hal ini dibutuhkan ? karena *starting* pembuatan BOM (*Bill Of Material*) suatu solusi harus diawali oleh topologi design agar komponen-komponen pendukung dan korelasi komponen dengan perangkat lainnya terdefinisi dengan jelas dan nyata.
5. POC (*Proof of Concept*)
   Setelah tahapan yang ke 4, maka tahapan selanjutnya adalah POC yang berarti suatu langkah nyata dalam merealisasikan dari suatu metode atau gagasan tertentu untuk menunjukkan kelayakannya, dengan cara mendemokan atau menunjukan fakta-fakta yang nyata yang pada prinsipnya dengan tujuan untuk memverifikasi bahwa beberapa konsep atau teori tersebut memiliki potensi praktis yang dapat dibuktikan sendiri oleh pelanggan.
   Nah dengan POC tersebut tentunya pelanggan dapat dengan mudah mengevaluasi hasil dan bukti nyata yang ditunjukan dari topology design dan konsep teknis yang disodorkan oleh kami, konsep biasanya tersebut bisa 100% atau kurang lengkap sesuai sesuai kebutuhan yang ada tetapi paling tidak ada gambarang yang lebih melengkapi sebelum dilakukan keputusan

## B. IMPLEMENTASI

Agar suatu rencara dapat berlangsung dengan baik, tuntas serta efective, maka harus dilalui tahap implementasi dan sebaiknya lakukan point point berikut ini.

1. Project Management.
   Inti dari project manajement itu adalah untuk mengatur siapa melakukan apa dan kapan? hal ini sangat penting untuk mengatur dan memperkirakan waktu memulai dan akhir dari suatu project dan jangan lupa pula unsur unsur lain seperti *Initiating*, *Planning*, *Executing*, *Monitoring* dan *Controlling*, serta *Closing* agar *project* dapat selesai dalam rentang waktu yang direncanakan.
2. Re-Survey.
   Aktivitas ini diperlukan dalam rangka untuk memastikan ulang agar tidak ada hal hal yang tertinggal dan *re-survey* adalah salah satu cara untuk menutup hal tersebut, karena semakin komplek suatu *project* diperlukan pemastian kelengkapan secara ketat dan berulang, sedikit saja suatu komponen terlewatkan

akan mempengaruhi keseluruhan *project* dan mengakibarkan usaha usaha yang lebih lama, mahan dan *effort* yang luar biasa besar.

3. Improvement of Integration.
   Yang paling *critical* adalah di titik ini, karena membuat *device* agar dapat "berbicara" dengan *lainnya* dan dapat berperilaku sesuai dengan maunya "r*ule of the game*" tidak mudah, membutuhkan waktu yang *relative* panjang, memerlukan usuha usaha yang tekun dan diperlukan trial & *error* yang berulang ulang, hanya *partner* yang memiliki jam terbang yang dapat melakukan hal ini.

4. Testing & Commissioning.
   Dengan adanya pelaksanaan *commissioning* akan didapatkan kepastian hasil suatu pekerjaan atau dengan kata lain dengan adanya *commissioning* engujian atau melakukan pengujian operasional suatu pekerjaan secara real / nyata maupun secara simulasi untuk memastikan bahwa pekerjaan tersebut telah dilaksanakan dan memenuhi semua kebutuhan yang telah sepakati antara pelaksana kerja dan *customer*.

5. Training & Transfer Knowledge.
   Tentunya hal yang lazim bagi pelanggan mendapat pelatihan untuk pemakaian alat yang di *invest* sesuai kebutuhan *customer*, hal ini juga untuk kebutuhan operasional dilapangan agar lebih mudah penggunaannya dan melakukan *troubleshooting* jika ditemukan masalah di kemudian hari, semakin mandiri suatu pelanggan dalam mengoperasikan alat maka sebenarnya semakin baik karena *customer* yang paling dekat dengan operational dan pengguna akhir sedangkan *vendor* sifatnya *backup*.

## C. POST SALES


| Online Support | Onsite Support | Customers Training |
|---|---|---|
| Pengaduan ataupun diskusi bisa kami lakukan secara *Online* dengan menggunakan Telepon, email serta media *online* lainnya | Jika permasalah tidak bisa diselesaikan dengan *Online*, tim *engineering* kami akan mengunjungi kelapangan | Melakukan kegiatan pelatihan baik secara *Online* maupun *onsite*. |
| Solusi kami berikan secara Online dan remote *Desktop* ( melakukan *remote* PC/laptop pelanggan oleh *engineer* ACS Group) | *Preventive Maintenance* atau kunjungan rutin untuk melakukan pengecakan dan perawatan | Membantu pelanggan bisa melakukan tindakan pertama jika terjadi permasalahan |

*/ Penulis : Taufiq Rahman (taufiq.rahman@acsgroup.co.id)

Member Gathering
## HITA & ACS GROUP

Pada tanggal 15 Maret 2017 Asosiasi para staf IT Hotel (HITA) yang ada di Surabaya bekerjasama dengan ACS Group mengadakan acara Gathering yang berlangsung di Hotel Swiss-Belinn Tunjungan, Surabaya.

Pembentukan HITA (Hotel Information Technology Association) di Indonesia bertujuan memajukan informasi teknologi (IT) dunia perhotelan. Agar para tenaga IT khususnya yang bekerja di dunia perhotelan dapat mengembangkan dan berbagi informasi serta update teknologi di industri ini.

Acara ini diawali dengan kata sambutan oleh [1]**Tiara Matius** - Ketua HITA Jawa Timur dan [2]**Boedijanto Linardi** - Branch Manager ACS Group cabang Surabaya.



Para engineer [3]**Ricky Efraim Lie** & [4]**Wahyu Dwi Chandra** memberikan presentasi tentang product solution yang dapat diimplementasikan di dunia perhotelan. Bukan hanya product solution tetapi juga professional services yang kita presentasikan juga oleh engineer [5]**Feri Setiawan Adinata**, solusi ini menjadi salah satu product concern kami untuk menunjang kelangsungan operasional dalam suatu perusahaan.

Kami juga mempresentasikan mengenai success story dari product solution yang telah diimplementasikan oleh beberapa Hotel di Bali, yang kita tahu pulau Dewata merupakan pusat industri Hotel/Hospitality di Indonesia. Acara ini dibawakan oleh [6]**Dea Restu Putty N** - Account Executive ACS Group, Bali.


Workshop
## Security Without Compromise

ACS Group bersama FORTINET, AVNET dan Professional IT Bali bekerjasama menyelenggarakan Workshop dengan thema "Security Without Compromise" bertempat di Padma Resort Legian - Kuta, Bali pada tanggal 18 Maret 2017.


Acara dibuka oleh [1]**A.A Ngurah Mahendra** sebagai Branch Manager ACS Group Bali dan [2]**Armika Jaya** sebagai Chairman Profit IT Bali.


Presentasi mengenai Fortinet profile, Fortinet Product update serta Security Solution disampaikan oleh [3]**Halim Sutrisna** - Fortinet Channel Account Manager Indonesia Area. Gambaran tentang produk Fortinet seperti apa dapat anda baca pada topik utama kami pada bulletin ini.


Live demo untuk produk FORTINET dibawakan oleh engineer [4]**Dasa Aprily Ardy** sebagai Technology Development Supervisor.

Dan pada di sesi ini mendapatkan response yang baik dari para pengunjung yang hadir.

Workshop
## Fortinet Untuk Sektor Edukasi

ACS Group cabang Semarang bekerjasama dengan Avnet, Fortinet, Helios dan Aruba HP menjangkau dunia pendidikan khususnya seluruh perguruan tinggi yang ada di Yogyakarta dan sekitarnya dengan menyelenggarakan workshop dengan tema "Penerapan Teknologi Informasi & Komunikasi di Perguruan Tinggi". Acara ini diadakan tanggal 22 Maret di The Alana Hotel dengan tujuan untuk memberikan solusi teknologi tepat guna mengenai enterprise wireless network dan pengamanannya di sektor pendidikan, dan solusi teknologi ini juga akan membekali para mahasiswa saat mereka terjun ke dunia pekerjaan mereka.

Acara workshop dibuka oleh [1]**Adrian Dewantoro** - Branch Manager ACS Group Semarang. Disamping itu juga memberikan presentasi tentang Asset Management "How to Manage & Monitoring your Asset"



[2]**Halim Sutrisna** - Fortinet Channel Account Manager Indonesia Area memberikan presentasi tentang produk Fortinet Firewall serta live demo-nya.


Dilanjutkan presentasi tentang HPE Aruba Networks Solution dan Live Demo-nya yang dibawakan oleh engineer [3]**Ricky Efraim Lie**.

Info Professional Services disampaikan oleh [4]**Ihdi Arwan** - Technology Services

Antusiasnya para peserta mengunjungi booth ACS Group.

Gathering
## KOMITKABE

KOMITKABE (Komunitas IT Karawang – Bekasi) mengadakan Gathering tahunan yang dilaksanakan di Hotel Harper Purwakarta pada tanggal 25-26 Maret 2017 lalu.

Event IT Community Gathering 2017 ini dihadiri 96 orang praktisi IT yang mewakili 63 perusahaan baik local maupun multi nasional yang tersebar dari kawasan Purwakarta, Cikampek, Karawang, Cikarang sampai Bekasi.

ACS Group bersama Honeywell ikut berkontribusi dalam acara ini sebagai salah satu sponsorsip, mendapatkan slot presentasi yang dibawakan oleh [1]**Suprianto Kusman** - Branch Manager ACS Group Cikarang dan [2]**Irfan Mulyana** - Honeywell Enterprise IT Solutions Manager.



Pengunjung yang mendatangi booth mendapatkan pengetahuan/jawaban atau solusi yang dapat diterapkan di perusahaan mereka.

Seller Conference

## Hemat Biaya Operational dengan Printer Barcode Honeywell

Bertempat di Plaza Agro - Kuningan Jakarta Selatan, ACS Group dan Honeywell bersama LAZADA INDONESIA(E-Commerce) mengadakan acara Seller Conference dengan thema "Hemat Biaya Operational Dengan Printer Barcode Honeywell" pada tanggal 30 Maret 2017. Acara ini diadakan dengan tujuan untuk open minded bagi para seller mengenai Honeywell PC43t.


Acara dibuka oleh [1]**Christofel Champ** - Lazada Indonesia - Seller Experience Senior Associate dan mempresentasikan perihal cost menggunakan printer konvesional dengan printer label barcode.
ACS Group diwakili oleh [2]**Ramdany Tobing** memberikan presentasi ACS Group company profile dan solusi product printer honeywel PC43t dilanjutkan oleh [3]**Shalina Alatas** dari Honeywell yang memaparkan solusi produk dan Company profile Honeywell.

Demo Product PC43t dihadapan para seller oleh team Engineer Acsgroup Nopah H. Dan dibantu oleh team Honeywell Bpk. Hanif Bastian.

Workshop

## ClearPass Airwave Aruba

ACS Group bersama Helios & Aruba mengadakan acara workshop dengan thema "Profile Your Way to Protecting IoT Network and Maintening The Risk" pada tanggal 5 April 2017. Acara workshop ini membahas tentang produk ClearPass dari Aruba yang memberikan keuntungan seperti visiibility, policy control & workflow automation serta pembahasan lainnya.


Acara workshop ini dibuka oleh [1]**Arijanto Hartanto** - Sales Director ACS Group.
Pembahasan produk Clearpass dari Aruba di presentasikan oleh [2]**Ricky Efraim Lie**.


Pada acara ini juga diadakan diskusi panel yang dipandu oleh [3]**Liem Sony Santoso** dibantu oleh [4]**Irvan Kurniawan**.

Workshop
## RFID Smart CCTV


Untuk menjangkau customer di area Cikarang dan sekitarnya ACS Group bersama Honeywell & Hikvision mengadakan acara Kupas Tuntas dengan thema "Solusi RFID di Finished Goods Manufactured & Solusi Smart IP CCTV di Area Manufaktur" pada tanggal 12 April 2017. Acara ini membahas update product solution dari Honeywell, solusi RFID yang sedang berkembang dan sudah diimplementasikan di beberapa customer serta solusi Smart IP CCTV Hikvision untuk pengamanan di area manufaktur.


Acara ini dibuka oleh [1]**Suprianto Kusman** - Branch Manager ACS Group Cikarang.


Para Pembicara di acara ini:

1. Heru H Sukiyanto - Honeywell Channel Business Manager
2. Didi Kartasasmita - Honeywell Senior Solution Architec
3. Heru Wahyudi - ACS Sales General Manager
4. Yolanda Roring - Hikvision Channel & Sales Manager
5. Wawan Wahyudin - ACS Account Executive
6. Eko Purnomo - Hikvision Pre-Sales Manager

Acara ini juga diisi dengan testimoni yang dibawakan oleh [2]**Hidayat Gafur** - PPIC Head PT. SHOWA INDONESIA MANUFACTURING, tentang manfaat dan dampak dari solusi produk RFID yang sudah diterapkan di area gudangnya.

Live Demo produk RFID yang dilakukan oleh staf ACS Group Harry Sugiarto & Denny Irawan.

Live Demo produk Hikvision IP CCTV yang dilakukan oleh staf ACS Group Edward Nawar & Rijallulaah Ayatullaah.


**Live Demo RFID**

Workshop
## RFID Smart CCTV


AVNET Datamation Solutions mengadakan acara CYBERSECURITY DAY 2017 pada tanggal 17 Mei 2017 bertempat di Mandarin Oriental Hotel, Jakarta. ACS Group ikut ambil bagian dalam acara ini dan mendapat kesempatan membuka booth untuk produk Fortinet sekaligus slot waktu untuk mempresentasikan produk security ini.

Para peserta yang mengunjungi booth Fortinet dan mendapatkan penjelasan yang bermanfaat bagi perusahaan mereka.

# Solusi Teknologi Baru dari Extreme®

Connect Beyond the Network

Extreme Networks didirikan oleh Gordon Stitt, Herb Schneider dan Stephen Haddo ck pada tahun 1996 di California, AS, dengan kantor pertamanya berlokasi di Cupertino, yang kemudian pindah ke Santa Clara.

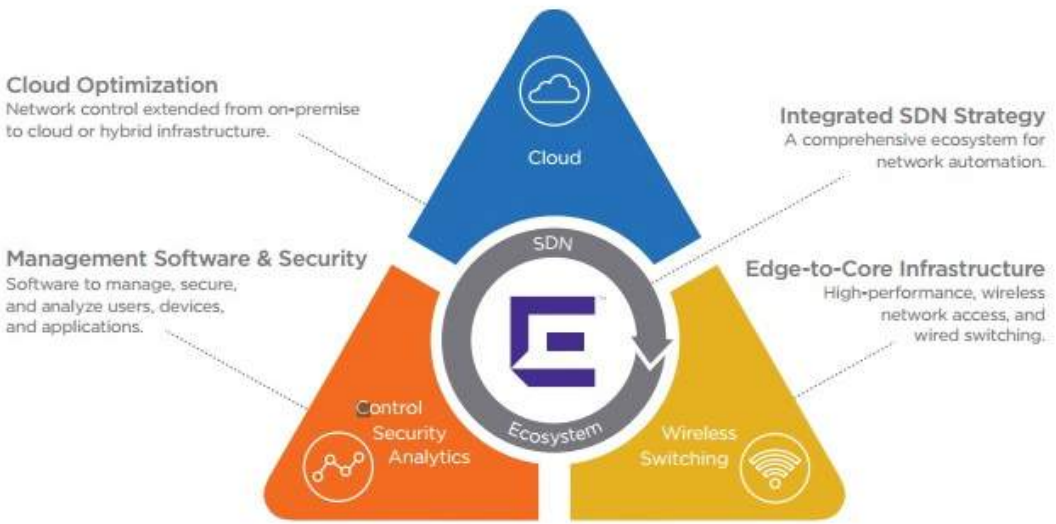
Misi dari Extreme Networks adalah memberikan kinerja yang tinggi, teknologi jaringan Layer 3 IP/ Ethernet, termasuk Quality of Service dan resiliency, dengan skala dan kecepatan perpindahan Gigabit Ethernet yang muncul.

Produk Extreme Network ditargetkan untuk perusahaan yang sedang membangun dan menyelenggarakan internet broadband. Produk pertama Extreme Networks adalah tombol Summit1 gigabit, yaitu perangkat switching 6 Port Ethernet Layer 3 yang menampilkan Dual GBIC SX 1000SX. Produk ini dikirim pada tahun 1997 dan memenangkan penghargaan 'Best of Show' di ajang pameran industri Networld + Interop pada tahun 1997. KTT ini juga dinobatkan sebagai 'Best of the Best Grand Winner' untuk acara tersebut. Extreme Networks meraih penghargaan Best of Show di Networld + Interop lima t ahun berturut-turut, 1997 sampai 2001.

## Extreme Solutions: Beyond Hardware

Extreme Networks telah dikenal lebih dari 20 tahun yang lalu yang paling banyak menawarkan Komprehensif, akses jaringan berkinerja tinggi dan produk switching. Tapi jika Anda masih berpikir "perangkat keras" dan saat mendengar "Extreme," sudah waktunya untuk berpikir ulang.

Terinspirasi oleh visi Extreme tentang kemampuan jaringan untuk menggerakkan koneksi yang



dapat meningkatkan bisnis Anda, Extreme telah melengkapinya pada satu set perangkat lunak dan sistem operasi untuk mengendalikan kebijakan dari satu simpul ke setiap perangkat di seluruh perusahaan. Platform analisis mengkorelasikan penggunaan dengan kinerja jaringan dan intelligent control plane kami untuk beradaptasi secara real-time.

Extreme telah berevolusi melampaui hardware menjadi salah satu supplier software driven terkemuka. Solusi jaringan berarti Extreme bisa mengantarkan infrastruktur TI yang cepat, tangguh dan dapat menyesuaikan diri dengan tuntutan dari sisi pengguna, aplikasi dan ancaman keamanan - dari kabel ke nirkabel, desktop ke pusat data.

## Extreme Resmi mengakuisisi Zebra WLAN

Tahun 2016 lalu Extreme Networks mengumumkan telah sepakat untuk mengakuisisi bisnis Zebra WLAN. Bisnis WLAN gabungan akan menjadi penyedia terbesar ketiga di target pasar gabungan dan pangsa pasar terbesar keempat. Extreme akan mengakuisisi pelanggan, channel partner, personil dan aset teknologi dari Zebra. Akuisisi ini tentunya akan memperkuat posisi terdepan Extreme di pasar ini dan memperluas perusahaan ke pasar vertikal baru yang kritikal, dengan menghadirkan solusi jaringan berbasis kabel dan nirkabel, dengan layanan pelanggan bagi industri terdepan(industry leading).

## Teknologi Extreme

A. ExtremeWireless WiNG

Dunia sekarang menuntut konektivitas tanpa batas. Solusi ExtremeWireless WiNG akan memaksimalkan keterlibatan pelanggan dan memberikan kualitas pengalaman yang luar biasa ke dunia ritel, perhotelan, transportasi & logistik serta industri lainnya.

- WiNG Access point
- WiNG Controllers
- Airdefense

Produk WiNG adalah produk Zebra hasil akuisisi yang masih dijual oleh Extreme.

B. ExtremeWireless

Menawarkan akses Wi-Fi high density yang tak ada bandingannya. Itulah sebabnya Extreme Networks dinobatkan sebagai “Penyedia Wi-Fi Resmi untuk NFL.” Ini berarti menghubungkan organisasi Anda dengan para karyawan, mitra dan pelanggan ke mana pun mereka pergi, memberikan pengalaman yang lebih baik, hubungan yang lebih kuat, dan hasil bisnis yang dipercepat. Terdiri dari :

- Access Point
- Virtual Appliances

C. ExtremeSwitching

Inti dari setiap jaringan yang mudah beradaptasi adalah platform switching yang fleksibel, aman dan efisien. ExtremeSwitching disini menyediakan platform yang legendaris untuk cakupan kinerja dan komprehensif mereka from edge-to-core(sisi ke ujung).

- Multi-Rate
- Standalone Solutions
- Modular
- Dan lain-lain

D. ExtremeCloud

- Cloud-Based Network Management

E. Dan produk Extreme lainnya

*/ Penulis : Tju Hansel ( tju.hansel@acsgroup.co.id )

# Kreativitas Teknologi Informasi

34 tahun sudah Jono Sutanto bergelut di bidang IT Technology, tidak mudah baginya untuk melalui semuanya itu untuk mencapai kariernya sampai saat ini, ada banyak hal yang harus dan sudah dilaluinya. Sosok beliau yang tenang, inspiratif dan tanggap sanggup melalui segala tantangan dan permasalahan yang dihadapi sehingga menambah wawasan, kekuatan dan kebijakan-kebijakan yang tepat guna yang pernah diambilnya bagi perusahaan dimana beliau bekerja. Dan tanpa disangkal semua itu adalah Anugerah Tuhan.

Jono Sutanto adalah alumni ITB lulusan tahun 1983 dengan mengambil jurusan yang cukup menantang yaitu Fisika Teknik. Pada tahun yang sama awal kariernya dimulai saat bergabung dengan PT. Gunung Sewu Kencana sebagai staff IT. Hanya setahun di perusahaan yang lama beliau bergabung ke PT. Syslog Infostem Ofimat di perusahaan inilah Jono Sutanto yang akrab dipanggil pak Jono mulai menapaki kariernya sampai ke jenjang Managing Director.

**Bagaimana perjalanan karier seorang Jono Sutanto hingga sekarang ini berikut kutipan yang disampaikan ke meja redaksi :**

Bidang Teknologi Informasi merupakan hal sangat menantang, dimana perkembangannya sangat cepat dari waktu ke waktu.

Pada tahun 80an, dengan teknologi Informasi yang terbatas kita tertantang untuk mengembangkannya menjadi suatu solusi yang efektif, khususnya untuk menggantikan hal klerikal yang memakan waktu pada saat itu. Dibutuhkan kreativitas untuk menghasilkan suatu solusi yang tepat guna, karena keterbatasan perangkat yang ada pada saat itu. Keterbatasan yang dimaksud adalah antara lain kapasitas storage yang hanya 2MB, dengan memory hanya 128 KB, serta development tool yang terbatas hanya dapat menampung 10 digit numeric.

Pada tahun 2000an sampai saat ini, perkembangan Teknologi Informasi sudah melompat sedemikian rupa, sehingga Kreativitas yang dilakukan di masa lalu dengan segala keterbatasan yang ada, sudah dapat dijawab langsung, sehingga tantangannya juga berubah.

Itulah situasi yang akan kita hadapi dari waktu ke waktu, dimana satu hal yang tidak pernah berubah adalah keberhasilan penerapan teknologi informasi harus selalu disesuaikan dengan budaya yang berkembang pada suatu lingkungan, maksudnya tujuan akhir maka harus selalu melalui suatu proses penyesuaian, karena penerapan teknologi informasi hanya berhasil apabila penerapannya dipahami oleh seluruh penggunanya, jadi bukan hanya jadi suatu symbol belaka.

**Tahun 2014, tepatnya di bulan Januari beliau bergabung dengan ACS Group menjabat sebagai salah satu Director hingga saat ini. Berikut kesan yang disampaikan selama bergabung di ACS Group :**

Tantangan yang kami hadapi untuk memberikan suatu solusi yang tepat pada setiap pelanggan kami membutuhkan kerjasama yang baik dari seluruh jajaran di ACS group, mulai dari meramu peralatan teknologi yang ada, merangkainya serta membuktikan kepada pelanggan kami bahwa solusi tersebut dapat diterapkan secara efisien dan affordable, karena penerapan teknologi tidak

selalu plug and play, manakala di setiap pelanggan memiliki kondisi dan keterbatasan yang berbeda-beda.

Hal inilah yang paling berkesan dalam diri saya, dimana kerja sama yang baik akhirnya dapat memberikan solusi terbaik untuk pelanggan kami, sehingga kami semua selau bersyukur pada apa yang telah kami capai, tanpa merasa ada orang/bagian yang lebih super dari yang lain.

**34 tahun tentunya bukan waktu yang sebentar bagi sosok yang gemar berolah raga dan berwisata ini memiliki banyak pengalaman yang telah didapatinya.**

**Tidak sedikit orang berpindah karier dari satu bidang dimana dia mulai berkarier ke bidang yang lain/berbeda hanya dengan alasan yang klasik yaitu mencari pengalaman yang berbeda. Namun tidak dengan Jono Sutanto, dia tetap berkarier di bidang yang sama di sektor Teknologi-Informatika-Komunikasi (TIK). Berikut kesan beliau :**

Teknologi Informatika & Komunikasi merupakan alat yang dapat membantu kita mempercepat dan mengefisiensikan pekerjaan kita sehari-hari, sehingga kita dapat berkolaborasi dalam segala kegiatan kita agar dapat mencapai tujuan kita bersama, tanpa dibatasi waktu maupun jarak serta cuaca yang ada di sekitar kita.

Semua Ide dan kreativitas setiap jenis teknologi informasi dapat mengubah kwalitas kerja dan kwalitas hidup manusia, asalkan dirangkai dengan baik sesuai dengan fungsi dan keterbatasan nya. Manusia dalam hal ini sebagai pengendali dari setiap solusi yang tercipta.

Mana terpikirkan 30 tahun yang lalu bahwa koneksi internet dapat menghubungkan kita sedemikian sehingga kita dengan sangat cepat mendistribusikan informasi ke seluruh dunia dengan sangat cepat dan akurat.

**ACS Group adalah perusahaan yang membidangi AUTO ID & Enterprise Security Solution, apa pesan yang disampaikan untuk bidang ini bagi sektor Industri di Indonesia ke depannya?**

Teknologi Auto ID dan Security, pada awalnya merupakan barang yang cukup mahal, sedemikian sehingga penggunanya hanya kalangan tertentu yang mempunyai apresiasi tinggi terhadap efektivitas pelaksanaan operasi hariannya. Tetapi dengan berjalannya waktu teknologi tersebut semakin diterima pasar dan harganya pun semakin affordable.

Teknologi Auto ID dan security merupakan jawaban atas kondisi bisnis yang makin ketat dari waktu ke waktu, walaupun penerapannya harus disesuaikan dengan kondisi dari masing-masing entitas bisnis, oleh sebab itu dibutuhkan teknologi partner ACS, yang sudah berpengalaman lebih dari 25 tahun di bidang ini.

Jono Sutanto
Director

## Zebra
## FX7500 Fixed RFID Reader

**Produk solusi untuk sektor industri :** Warehouse, Manufaktur, Retail, dan Transportasi.

FX7500 Fixed RFID Reader merupakan teknologi radio RFID yang canggih dengan kecepatan baca lebih cepat, lebih akurat, dan memiliki kinerja yang lebih konsisten bahkan di lingkungan yang menantang. Radio baru dipasangkan dengan arsitektur jaringan berbasis Linux yang lebih fleksibel yang mengintegrasikan alat dan interface open-standar yang diperlukan untuk penerapan yang cepat dan mudah dengan aplikasi RFID dan back-end.

## Zebra
## BARCODE PRINTER ZT230

**Produk solusi untuk sektor industri :** Retail, Healthcare, Manufaktur, Transportasi.

Barcode Printer yang dihadirkan untuk menggantikan produk printer Zebra S4M yang lama, dengan fitur desain hemat, body metal, setup yang mudah dan kemudahan dalam layanan & pemeliharaan. Printer dengan ukuran yang ramping sehingga tidak memakan tempat, disamping itu printer ini memiliki kecepatan 6”/152mm per second dan memiliki kapasitas ribbon sampai dengan 450 meter.


## Zebra
## TC 51
## TOUCH COMPUTER

**Produk solusi untuk sektor industri :** Retail, Warehouse, Manufaktur,

TC51 memiliki fitur prosesor hexa-core prosesor 1,8 GHz 64-bit dapat menjalankan kegiatan bisnis. Konsumsi daya yang lebih baik dan penghematan tenaga untuk processor hingga 15% lebih sedikit serta running aplikasi dengan kecepatan hingga 5 kali lebih cepat. Produk ini dilengkapi dengan ultra-high Resolution Photos 13 MP, produk yang memiliki kemampuan untuk mengcapture secara otomatis sehingga dapat mengcapture secara bersamaan seperti keseluruhan teks, no telp, gambar, tanda tanggan, check box dan tampilan lainnya.

## Fortinet Advanced Threat Protection Framework

memberikan end-to end perlindungan di seluruh rantai serangan, untuk keamanan tanpa ada kompromi. Fortinet terdiri dari tiga elemen, bekerja secara bergandengan tangan yaitu :

- Mencegah Serangan
- Mendeteksi dan Menganalisis Ancaman
- Mengurangi Dampak dan Meningkatkan Perlindungan

Terbagi menjadi:

1. FortiGate
2. FortiSandbox
3. FortiMail
4. FortiClient
5. FortiSwiitch
6. Dan lain-lain

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

PRODUCT HIGHLIGHT

## Honeywell
## ScanPal EDA50K

**Produk solusi untuk sektor industri :** Distribution Center, Jasa & Pengiriman, Logistik & Transportasi

Produk Enterprise Digital Assistant (EDA) dengan kinerja berkecepatan tinggi dan smooth, memiliki fitur prosesor quad-core 1,2 GHz dan RAM 2 GB serta mampu membaca barcode 1D & 2D. Konektivitas jaringan yang sangat baik mendukung banyak jaringan di area yang luas, dengan konektivitas Wi-Fi 2,4 GHz dan dual band 5 GHz. Dirancang agar dapat digunakan dengan tangan kiri atau kanan, dengan pegangan tangan yang melengkung dan ergonomis, sehingga mengurangi kelelahan dalam waktu lama, dan memberikan pengalaman pengguna yang lebih nyaman.

## Point Mobile
## PM80
### SMART BEYOND RUGGED ENTERPRISE MOBILITY

**Produk solusi untuk sektor industri :** Warehouse, Retail, Manufaktur, Transportasi & Logistik.

PM80 adalah terminal mobile full touch yang memiliki ukuran screen 5” dengan Qualcomm Snapdragon yang memiliki Quad-Core 1.4 GHz. PM80 juga dilengkapi dengan fitur 4GLTE dan IEEE 802.11 a/b/g/n, pemindai laser bar code 2D dan Bluetooth v4.0. Terminal mobile ini disamping hadir dengan OS Android sekarang ini sudah hadir dengan Windows 10 IoT dan produk ini dapat bertahan hingga 1,5 m (5ft) bersamaan dengan perlindungan terhadap air dan debu karena memiliki rating IP67.

# KOLOM KETAWA

## PENGACARA DAN PETANI TUA

Seorang pengacara kota besar pergi berburu burung di sebuah pedesaan. Dia menembak dan menjatuhkan seekor burung, tetapi jatuh ke dalam ladang petani yang dikelilingi pagar. Ketika pengacara tersebut naik melewati pagar, seorang petani tua mendekat dan bertanya kepadanya apa yang sedang dilakukannya?

Si pengacara menjawab, “Saya menembak seekor burung dan terjatuh di ladang ini, dan sekarang saya akan mengambilnya kembali.”

Petani tua itu menjawab, “Ini ladang milik saya, dan Anda tidak boleh masuk ke sini.”

Pengacara yang marah itu berkata, “Saya adalah salah satu pengacara terbaik di Indonesia, dan jika Anda tidak membiarkan saya mendapatkan burung itu, saya akan menuntut Anda dan mengambil semua yang Anda miliki.”

Petani tua itu tersenyum dan berkata, “Rupanya, Anda tidak tahu bagaimana kami menyelesaikan perselisihan di kampung ini. Kami menyelesaikan perselisihan kecil seperti ini dengan ‘Aturan Tiga Tendangan’.”

Pengacara tersebut bertanya, “Apa itu Aturan Tiga Tendangan?”

Petani tersebut menjawab, “Karena perselisihan terjadi di tanah saya, saya harus melakukannya terlebih dahulu. Saya menendang Anda tiga kali dan kemudian Anda menendang saya tiga kali dan seterusnya bolak-balik sampai salah satu mengatakan menyerah.”

Pengacara tersebut dengan cepat memikirkan aturan yang diajukan dan memutuskan bahwa dia dapat dengan mudah memenangkan pertandingan itu. Dia setuju untuk mematuhi adat setempat.

Petani tua itu perlahan mendekat dan langsung menemui sang pengacara. Tendangan pertamanya, sepatu botnya yang berat masuk ke dalam pangkal paha pengacara dan membuat pengacara tidak bisa berdiri!

Tendangan kedua tepat di perut dan mengirim makanan terakhir yang dimakan pengacara itu keluar dari mulutnya. Pengacara itu berada di posisi hendak berdiri saat tendangan ketiga petani menghujam ke wajahnya sampai mulutnya keluar darah segar. Akhirnya, dengan tenaga yang tersisa, si pengacara berusaha untuk berdiri.

Sambil mengusap wajahnya dengan lengan bajunya, dia berkata, “Baiklah, Pak Tua. Sekarang giliranku.”

Petani tua itu tersenyum dan berkata, “Nah, saya menyerah deh, silahkan Anda bisa mendapatkan burungnya.”

## ACS GROUP OUTING 2017 – GARUT

Pada tanggal 5 Mei - 7 Mei 2017 Seluruh ACS Group mengadakan acara outing bersama ke kota Garut. Di kota ini kami melakukan kunjungan ke beberapa tempat wisata Candi Cangkuang, Darajat Pas, Kebun Mawar, dan Penangkaran Elang.

## MEETING
## Branch Manager ACS Group

Pada tanggal 3 Mei 2017 bertempat di kantor pusat ACS Group - Gunung Sahari, kegiatan tahunan ini kembali diadakan, dimana semua manager yang ada di Jakarta dan seluruh cabang-cabang bersama para Director melakukan sharing bersama untuk membahas permasalahan di lapangan dan menyatukan langkah-langkah kerja yang perlu diambil untuk persiapan pencapaian target yang ditetapkan bersama di akhir tahun.

## TRAINING
## CAMBIUM NETWORKS CERTIFICATION

Bertempat di Gadjah Mada University Club (UC) engineer kami dari cabang Semarang, Iqbal Istiqobudi mendapatkan training bersertifikat untuk product Cambium Networks. Selama 2 hari training engineer dibekali dengan konsep dasar bagaimana mengoptimasi Wireless, memilih Antenna terbaik, Site Survey via Link Planner & BOM untuk Project dan pelajaran lainnya untuk diterapkan dalam pekerjaannya.

## ARUBA OLYMPIC BOOTCAMP

Aruba Networks mengadakan acara Olympic Bootcamp di Indoluxe Hotel, Yogyakarta, acara ini berlangsung dari tanggal 10-12 April 2017 lalu dikuti oleh semua partner & distributor yang ada di seluruh Indonesia. ACS Group diwakili oleh Liana Andari dari team sales Jakarta dan Iqbal Istiqobudi engineer cabang Semarang.

## Zebra Technologies
## APAC Channel Partner Summit 2017


Pada tanggal 27-28 April 2017 Zebra Technologies mengadakan Zebra Technologies APAC Channel Partner Summit 2017 yang diadakan di Tokyo Hilton Bay, Jepang dengan thema "Visibility that's Visionary". Acara ini dihadiri kurang lebih 300 peserta dari seluruh partner Zebra Technologies yang ada di Asia Pacific, ACS Group diwakili oleh Indra Tjahjadi & Arijanto Hartanto. Pada Conference ini dipaparkan mengenai Pencapaian bisnis Zebra di tahun 2016, Sales Growth APAC 8% di 2016. Membahas trend technology khusus utk menyikapi IoT, Cloud and Mobility dlm menunjang peningkatan kualitas visibility dari system informasi suatu Entreprise. Juga dibahas technology terbaru Zebra yang akan diluncurkan, khususnya untuk mobile computer hampir semua product terbaru akan berbasis Android.

## HPE ARUBA BOOTCAMP

Pada tanggal 16-19 Mei 2017, Helios mengadakan acara HPE Aruba Boothcamp bertempat di Aston Sentul Bogor - Jawa Barat, Engineer ACS Group Empianus Eko Putra dan Ridwan David Deden bersama dengan utusan partner lainnya mengikuti Aruba Bootcamp Training ini. Adapun materi yang mereka dapatkan antara lain : WLAN Controller Initial Setup, AP Configuration, Authentication sampai ke tingkat Advance, Firewall Policies dan pengetahuan lainnnya.

## HONEYWELL CONFERENCE 2017

Bertempat di Bangkok Marriott Marquis Queen's Park - Thailand, Honeywell menyelenggarakan conference dengan thema "ReImagination 2017", acara yang berlangsung selama dihadiri kurang lebih 200 peserta dari seluruh partner yang ada di ASEAN, Australia dan New Zealand. ACS Group sendiri diwakili oleh Arijanto Hartanto dan Heru Wahyudi.

# Tips Mengamankan Jaringan Perusahaan Pada Pengguna dan Perangkat.

Beberapa waktu lalu dunia *security* cukup dihebohkan dengan kemunculan *ransomware* yang memakan banyak sekali korban. Serangan itu cukup menarik karena biasanya *ransomware* menyerang dengan menggunakan perantara *trojan* tetapi *ransomware* dengan *codename WannaCry* ini menyerang dengan memanfaatkan *security hole* pada OS yang sebenarnya sudah "*out of date*" atau sudah tidak diberikan *patching* baru oleh manufakturnya. Hal ini dimanfaatkan oleh para *hacker* karena OS yang sudah *expired* seperti ini biasanya memiliki *security hole* yang terus terbuka tanpa ter-*update*. Selain dari standar prosedur yang biasa dilakukan seperti *patching*, pembatasan akses, upgrade OS, dan lain-lain.

Berikut sedikit informasi mengenai dua teknik keamanan yang cukup menarik untuk diterapkan.

## 1. Pembatasan terhadap *rogue* AP.

*Rogue* AP adalah perangkat *access point* yang digunakan di area kantor seperti umumnya tetapi bukan perangkat *access point* yang disediakan oleh kantor atau *access point* yang dibawa sendiri oleh karyawan untuk akses *internet* pribadi mereka. Yang paling umum adalah *access point* tipe SOHO yang biasa kita temui di toko-toko komputer yang dikoneksikan menggunakan kabel data ke *switch* atau *wall-plate port* yang kosong di area kantor atau bisa juga dengan menggunakan *access point* dengan memanfaatkan koneksi GSM seperti MiFi atau *tethering*. Dua hal ini sering menjadi masalah karena menjadi *backdoor* bagi jaringan perusahaan, seaman apapun *front door* kita amankan dengan *Firewall* tetapi jika *backdoor*-nya memiliki kelemahan maka bisa menjadi pintu masuk lain bagi *hacker*.

Jaringan *Wired* atau kabel untuk menghubungkan perangkat *access point* tersebut sering dilupakan oleh admin jaringan, biasanya pada jaringan *wired* ini cukup dikoneksikan maka akan langsung aktif, mendapat alamat IP, lalu dapat akses masuk dalam jaringan perusahaan. Untuk mengamankannya perlu menerapkan *security wired* yaitu 802.1X dengan RADIUS *Authentication* dimana setiap pengguna yang menggunakan kabel data terhubung ke perangkat *switch* harus melakukan *login* terlebih dahulu untuk memastikan bahwa pengguna tersebut memang seharusnya mendapatkan akses ke jaringan perusahaan.

Dari sisi jaringan *Wireless* LAN (WLAN), penerapan *Wireless* IPS atau WIPS juga sering dilupakan. Perangkat WLAN untuk kelas *Enterprise* biasanya memiliki fitur WiFi sensor *monitoring security* yang dapat diaktifkan untuk melakukan deteksi terhadap perangkat *Rogue* AP dan *Rogue* Client. Ketika ada pengguna yang membawa perangkat

*access point* yang tidak seharusnya atau melakukan *tethering*, perangkat *access point*-nya dan *client* akan diantisipasi oleh sensor ini sehingga *client* tidak dapat mengakses ke *rogue* AP atau istilah awam dengan melakukan *jamming* terhadap perangkat *access point* dan *client* yang tidak di-*authorize* penggunaannya.

## 2. Pengamanan pada perangkat.

Yang kedua dan tidak kalah pentingnya adalah pengamanan terhadap perangkat yang beraneka ragam di jaman IOT ini sangat banyak sekali jumlah dan jenisnya. Setiap orang dapat membawa banyak perangkat yang semuanya bisa mengakses jaringan perusahaan dimana belum tentu semuanya diperbolehkan untuk mengakses. Misalnya ada pengguna yang seharusnya menggunakan laptop operasional untuk pekerjaan sehari-harinya dapat juga membawa laptop pribadinya yang dihubungkan ke jaringan kantor. Berbeda dengan laptop operasional yang lebih dapat diatur dari sisi akses, keaslian *software*, *antivirus*, dan lain-lainnya, perangkat pribadi biasanya memiliki perhatian yang kurang dan tidak jarang menjadi sumber *virus* dan menjadi titik masuk atau *entry-point* bagi seorang hacker untuk menyebarkan *malware*-nya. Belum lagi jika berbicara perangkat lain seperti *smartphone*, *tablet*, *smartwatch*, *smartglass*, dan lain-lain.

NAC atau *Network Access Control* yang diintegrasikan dengan BYOD atau *Bring Your Own Device* dapat memberikan *visibility* terhadap siapa saja yang mengakses jaringan, menggunakan perangkat apa, kapan mengaksesnya, dimana mengakses-nya, dan bagaimana cara pengguna mengakses. *Visibility* terhadap hal tersebut sangat penting bagi administrator jaringan karena ini adalah modal awal untuk pengaturan dimana harus mengetahui terlebih dahulu tentang *background* penggunannya dalam jaringan perusahaan. Setelah BYOD berhasil mendapatkan *visibility* terhadap pengguna dan perangkat, selanjutnya NAC dapat melakukan pengaturan dan pembatasan akses terhadap pengguna dan perangkat. Penerapan akses terbatas terhadap perangkat misalnya pada pengguna yang sama ketika mengakses satu jaringan nirkabel (SSID) yang sama tetapi dari perangkat yang berbeda bisa diperlakukan secara berbeda. Jika aksesnya dari laptop operasional perusahaan, maka mendapatkan hak akses penuh (*full access*) dapat diberikan. Tetapi sebaliknya jika aksesnya dari perangkat laptop pribadi atau *smartphone* pribadi maka pengguna hanya dapat mengakses *internet* yang terbatas.

Pilihlah perangkat NAC yang dapat di-integrasikan dengan perangkat *server security* lainnya seperti misalnya penerapan *Mobile Device Management*, UTM (*Unified Threat Management*), *Firewall*, dan lain-lain. Hal ini bertujuan agar data collection dan penerapan *rule*-nya dapat diterapkan dengan lebih luas dan menyeluruh.

Semoga dengan Tips-and-Trick ini dapat membantu untuk memberikan pengamanan lebih terhadap jaringan data perusahaan dan menjaganya dari serangan threat atau potensi gangguan lainnya pada masa mendatang.

*/ Penulis : Irvan Kurniawan
(irvan.kurniawan@acsgroup.co.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 PLATINUM PLUS PERFORMANCE PARTNER Printer Specialist · POINTMobile · SEAGULL SCIENTIFIC · wavelink · IBM
brother at your side · FARGO · 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