



Arsitektur *Zero Trust*

Definisi dan cara mencapainya





Contents

Apa itu arsitektur <i>zero trust</i>	3
Memahami segmentasi makro dan mikro.....	5
Mengapa Anda perlu keduanya.....	6
Cara mencapainya.....	7
Metodologi.....	7
Hal lainnya.....	12
Mengapa ALE?.....	12
Yang kami tahu pasti.....	13



Apa itu arsitektur *zero trust*?

Apa arti dari arsitektur *zero trust* (ZTA)? ZTA berarti setiap pengguna dan perangkat harus diautentikasi dan disahkan sebelum diizinkan akses ke data. Sebuah strategi yang 'tidak percaya pada siapa pun; autentikasi semuanya'.

Mari gunakan sebuah analogi.

Jika kita memisalkan keamanan tradisional sebagai benteng yang melindungi desa, kita akan membangun sebuah tembok benteng (atau disebut sebagai *firewall*) di sekitar desa (atau disebut sebagai perusahaan). Setiap hal yang datang dari luar benteng tidak dipercaya dan akan diteliti namun apa pun di dalam benteng secara implisit dipercaya dan diizinkan. Batas kepercayaan ini terlihat nyata dan implisit, tergantung Anda berada pada sisi benteng yang mana, karena selama Anda berada di sisi tembok yang 'tepat', maka tidak diperlukan pemeriksaan lebih lanjut. Jika menurut kita pendekatan ini dalam konteks hal jaringan perusahaan mungkin ada beberapa segmentasi dasar dalam bentuk VLAN, SSID, subjaringan atau antarmuka yang terikat pada *firewall*, tetapi segmentasi ini bersifat statis dan lebih berkaitan dengan skalabilitas dan pengelolaan jaringan daripada dengan keamanan.

Namun saat ini, pendekatan *firewall* (benteng) menjadi kurang efektif jika hanya sendiri, karena sejumlah alasan. Alasan yang pertama adalah mobilitas. Pengguna terhubung ke jaringan lain di luar perusahaan dan dapat membawa ancaman bersama mereka. Kedua, tamu belum tentu dapat dipercaya. Orang mungkin berpendapat bahwa bahkan karyawan (orang-orang yang berada di dalam benteng) tidak boleh dipercaya secara begitu saja. Ketiga, semakin banyak perangkat IoT yang ditambahkan ke jaringan. Perangkat IoT memunculkan risiko keamanan yang lebih tinggi karena bisa jadi tidak disetujui dan dikelola oleh TI dan biasanya tidak memiliki kapabilitas keamanan. Dengan pendekatan tradisional 'benteng/desa', '*firewall*/perusahaan', jika pengguna atau perangkat disusupi, tidak ada yang dapat menghentikan ancaman supaya tidak menyebar ke pengguna dan perangkat lain. Begitu Anda masuk, Anda bebas bergerak.

Dalam analogi benteng di atas, jika satu-satunya hal yang melindungi desa dari penyusup adalah tembok, maka pada hari para penyusup belajar memanjat tembok benteng — dan hari itu pasti datang — akan terjadi pembantaian.





Pertanyaannya adalah - apa yang bisa kita lakukan? Mari kita pikirkan hal ini dengan pendekatan 'tidak percaya pada siapa pun', atau '*zero trust*'.

Dalam *zero trust*, tidak ada pengguna atau perangkat yang dipercaya. Baik mereka di dalam ataupun di luar tempat, semua melalui pemeriksaan yang sama. Tidak ada yang namanya mempercayai pengguna internal. Setiap akses diautentikasi dan diotorisasi.

Dalam analogi benteng berarti bahwa selain adanya benteng yang melindungi desa dari ancaman luar, setiap rumah, setiap bangunan, juga memiliki keamanannya sendiri agar terlindungi dari risiko yang datang dari pelaku jahat yang tinggal di dalam benteng. Dalam konteks perusahaan, yang dikenal sebagai segmentasi mikro yang ditentukan perangkat lunak akan membawa perlindungan ini selangkah lebih maju. Selain benteng, dan keamanan di sekitar bangunan, kami juga memiliki penjaga keamanan pribadi yang mengikuti kita kemanapun kita pergi.

Dan kemanapun kita pergi, kita akan ditanyakan tentang paspor kita. Dalam jaringan Perusahaan, batas kepercayaan ini bersifat tidak jelas, terdistribusi dan bergerak. Batasan tersebut tidak terikat ke lokasi tertentu, *port switch*, atau VLAN. Hal ini tergantung pada antara lain identitas, perangkat, situasi, dan waktu terjadinya. Batasan ini ditentukan oleh perangkat lunak dan disesuaikan langsung dengan cepat. Dalam pendekatan ini, komponen perlu dikelola dan harus dapat bereaksi dan mengkonfigurasi ulang sesuai kebutuhan untuk merespons ancaman atau perubahan dalam alur kerja.



Memahami segmentasi makro dan mikro

Dalam arsitektur *zero trust* terdapat dua jenis segmentasi, yaitu segmentasi makro dan mikro. Dalam analogi kami, tembok benteng adalah segmentasi makro, dan penjaga keamanan pribadi adalah segmentasi mikro.

Dalam **segmentasi makro**, jaringan fisik dibagi menjadi segmen logis yang berbeda. Segmen ini bisa berupa VLAN, kombinasi VLAN dan VRF, bisa juga VPN jika berbicara tentang *Shortest Path Bridging* (SPB), MPLS, atau bahkan VXLAN atau terowongan GRE. Setiap lalu lintas antara pengguna atau perangkat di segmen yang berbeda dikendalikan oleh *firewall*. Semua perusahaan menggunakan segmentasi dalam beberapa bentuk atau jenis, namun tidak selalu untuk tujuan keamanan. Sering kali segmentasi semacam ini digunakan untuk skalabilitas, tujuan administratif atau organisasi. Jika dua perangkat dipetakan ke VLAN yang berbeda tetapi dua perangkat tersebut dapat berkomunikasi tanpa melalui *firewall*, maka perangkat-perangkat ini berada di segmen makro yang sama. Contoh khas dari segmentasi semacam ini adalah menjalankan telepon IP pada VLAN dan VRF terpisah yang secara logis diisolasi dari PC.

Pertanyaannya adalah bagaimana Anda memetakan pengguna atau perangkat ke segmen ini? Walau dapat dilakukan secara statis, dengan *switch port* atau SSID misalnya, cara ini sangat kuno. Cara tersebut terlalu kaku dan kurang cocok baik bagi pengguna seluler. Idealnya, Anda perlu memiliki sistem otentikasi yang ditentukan oleh perangkat lunak sehingga ketika pengguna atau perangkat terhubung dan mengautentikasi, mereka akan diberikan sebuah profil. Profil akan menempatkan pengguna atau perangkat di segmen yang tepat terlepas dari lokasi fisik, *switch port*, atau SSID.

Meskipun segmentasi makro tentu memiliki manfaat keamanan, dalam banyak kasus keamanan itu dilaksanakan untuk tujuan organisasi atau administratif. Misalnya, kamera dan kunci pintu berada di bawah kendali golongan keamanan akses, sedangkan

termostat berada di bawah kendali golongan perawatan gedung.

Segmentasi mikro membawa kita satu langkah lebih jauh. Tidak semua pengguna sama dan tidak semua pengguna memiliki kebutuhan yang absah untuk mengakses semua sumber daya. Profil yang sama yang memetakan pengguna ke segmen juga meliputi serangkaian kebijakan yang menambahkan kontrol terperinci atas hak pengguna/perangkat yang berbeda untuk peran yang berbeda seperti SDM versus Keuangan. Hal ini dikenal sebagai **akses berbasis peran**, dan secara langsung berhubungan dengan **prinsip hak istimewa terendah**. Jadi, meskipun kamera dan kunci pintu berada di segmen yang sama, keduanya tidak perlu menggunakan sumber daya yang sama. Kamera perlu berkomunikasi dengan perekam video dan kunci pintu berkomunikasi dengan servernya. Kamera tidak perlu berkomunikasi dengan kunci pintu seperti halnya kunci pintu tidak perlu berkomunikasi dengan kunci pintu lain. Izin terperinci ini diterapkan melalui kebijakan yang merupakan bagian dari profil dan diimplementasikan secara dinamis ke perangkat setelah autentikasi.

Segmentasi mikro perlu didefinisikan oleh perangkat lunak karena beberapa alasan. Baik pengguna maupun perangkat IoT bersifat tidak statis, mereka bergerak, terhubung, dan memutuskan sambungan, sehingga kebijakan tidak dapat diikat ke lokasi atau *port*. Faktanya, konfigurasi segmentasi mikro harus dinamis berdasarkan kombinasi beberapa faktor, termasuk namun tidak terbatas pada, identitas pengguna atau perangkat, waktu dan lokasi.

Secara ringkas, ketika komunikasi antara segmen yang berbeda dikendalikan oleh *firewall*, hal itu disebut dengan segmentasi makro. Ketika komunikasi dalam segmen yang sama dikendalikan oleh kebijakan *Network Access Control* (NAC) yang terkait dengan perangkat atau peran pengguna, hal itu disebut dengan segmentasi mikro.



Mengapa Anda perlu keduanya

Bagaimana jika Anda hanya menggunakan satu jenis segmentasi?

Mari kita lihat segmentasi makro. Jika hanya menggunakan pendekatan ini, masalah yang muncul adalah *firewall* menjadi terhambat karena semua lalu lintas harus melalui *firewall* untuk autentikasi dan otorisasi. Hal ini dapat menimbulkan masalah kinerja. Anda dapat memasang lebih banyak *firewall* pada lapisan distribusi, tetapi bisa menjadi sangat mahal dan belum tentu akan meningkatkan kinerja karena *firewall* bukanlah kecepatan kabel. Selain itu, sekarang ada beberapa titik penegakan kebijakan dan banyak tempat untuk menjaga agar kebijakan tetap mutakhir, sehingga sulit untuk dikelola.

Opsi lainnya, menggunakan segmentasi mikro saja, juga memiliki masalah. Jika penegakan kebijakan hanya dilakukan melalui kebijakan NAC, maka daftar kebijakan ini akan menjadi sangat panjang dan rumit, sehingga dapat menghabiskan batas kapasitas perangkat Anda.

Ringkasnya, lebih baik ada keseimbangan antara dua bentuk segmentasi ini. Biarkan *firewall* mengontrol setiap lalu lintas di antara segmen yang berbeda (vertikal) dan biarkan kebijakan NAC mengontrol lalu lintas dalam suatu segmen (lateral).

Dengan menggabungkan keduanya, Anda dapat menangani ancaman keamanan yang menyebar dari satu segmen keamanan ke segmen keamanan lainnya, serta ancaman yang bergerak secara menyamping di segmen yang sama. Dalam istilah yang lebih jelas, segmentasi mikro adalah sesuatu yang menghentikan penyerang yang telah berhasil merampas kamera, dari menggunakan pelanggaran sebagai titik pivot sampai merampas sumber daya lain seperti kunci pintu.

Tujuannya yaitu mengautentikasi setiap koneksi dan memberikan izin untuk setiap pengguna atau perangkat. Hal tersebut berarti menggunakan segmentasi untuk mencegah penyebaran ancaman melalui gerakan lateral, serta pemantauan dan karantina berkelanjutan terhadap setiap pengguna atau perangkat yang tidak sesuai.





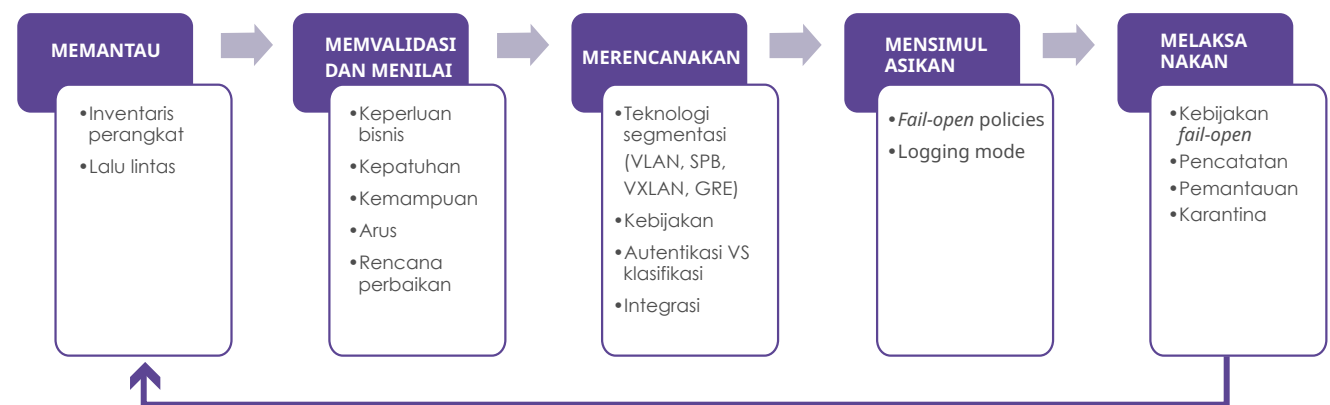
Cara mencapainya

Dalam situasi baru (*greenfield*), relatif mudah untuk membangun arsitektur *zero trust* menggunakan segmentasi mikro dari nol. Namun, dalam situasi lama (*brownfield*), memperkuat jaringan dengan segmentasi mikro dapat mengakibatkan pengguna, perangkat dan aplikasi dikunci dari jaringan karena autentikasi yang gagal atau kebijakan yang tidak lengkap. Sulit atau bahkan tidak mungkin bagi suatu perusahaan untuk melakukan migrasi dalam sekali jalan — dalam satu siklus penyegaran.

Dalam lingkungan *brownfield*, akan ada waktu di mana arsitektur *non-zero trust* dan *zero trust* akan hidup berdampingan, dan migrasi akan dilakukan oleh setiap lapisan atau setiap lokasi satu demi satu. Yang penting Anda memastikan bahwa elemen infrastruktur yang Anda terapkan, dan cara penerapannya, bersifat fleksibel dan mampu beroperasi dalam mode *zero trust* atau tersegmentasi mikro ketika elemen infrastruktur lainnya telah siap. Ini artinya infrastruktur tersebut perlu bekerja sama dengan komponen yang ada dan yang mendatang.

Metodologi

Terdapat lima langkah menuju arsitektur zero trust – memantau, memvalidasi dan menilai, merencanakan, mensimulasikan, dan melaksanakan.



Gambar 1 - Metodologi



Langkah 1: Memantau

Pertama, Anda perlu mulai memantau dan membangun peta serta inventaris mengenai setiap hal dalam jaringan Anda.

Untuk migrasi ke ZTA, kita perlu pengetahuan terperinci tentang aset (fisik dan virtual), subjek (termasuk hak pengguna) dan proses bisnis yang menyentuh atau menggunakan jaringan.

Pengetahuan yang tidak lengkap sering kali menyebabkan kegagalan di mana akses ditolak karena informasi yang tidak cukup. Hal ini menjadi masalah utama jika terdapat "TI bayangan" atau "IoT bayangan" yang tidak diketahui di dalam organisasi.

Mulai memantau perangkat dan arus lalu lintas. Buat laporan inventaris di mana semua perangkat yang terlihat di jaringan, dikategorikan menurut jenis perangkat, pabrikan, model, sistem operasi dan lainnya. Laporan ini juga harus menunjukkan di mana dan port switch atau SSID mana yang terakhir dilihat perangkat. Informasi ini dapat dikumpulkan dari elemen seperti alamat MAC, tanda DHCP dan agen pengguna HTTP.

Kebanyakan alat dari pihak ketiga hanya akan memberikan alamat IP, dan bukan jenis peralatan. Idealnya, kita mendapatkan alat untuk membuat inventaris IoT/ perangkat untuk memfasilitasi pembuatan profil NAC yang cepat dan mudah untuk setiap jenis perangkat.

Informasi lain yang diperlukan untuk membuat kebijakan adalah arus lalu lintas. Tergantung pada peralatan yang Anda miliki, Anda dapat memperoleh informasi ini dari alat pemantauan arus seperti sFlow, Netflow, atau Deep Packet Inspection (DPI).

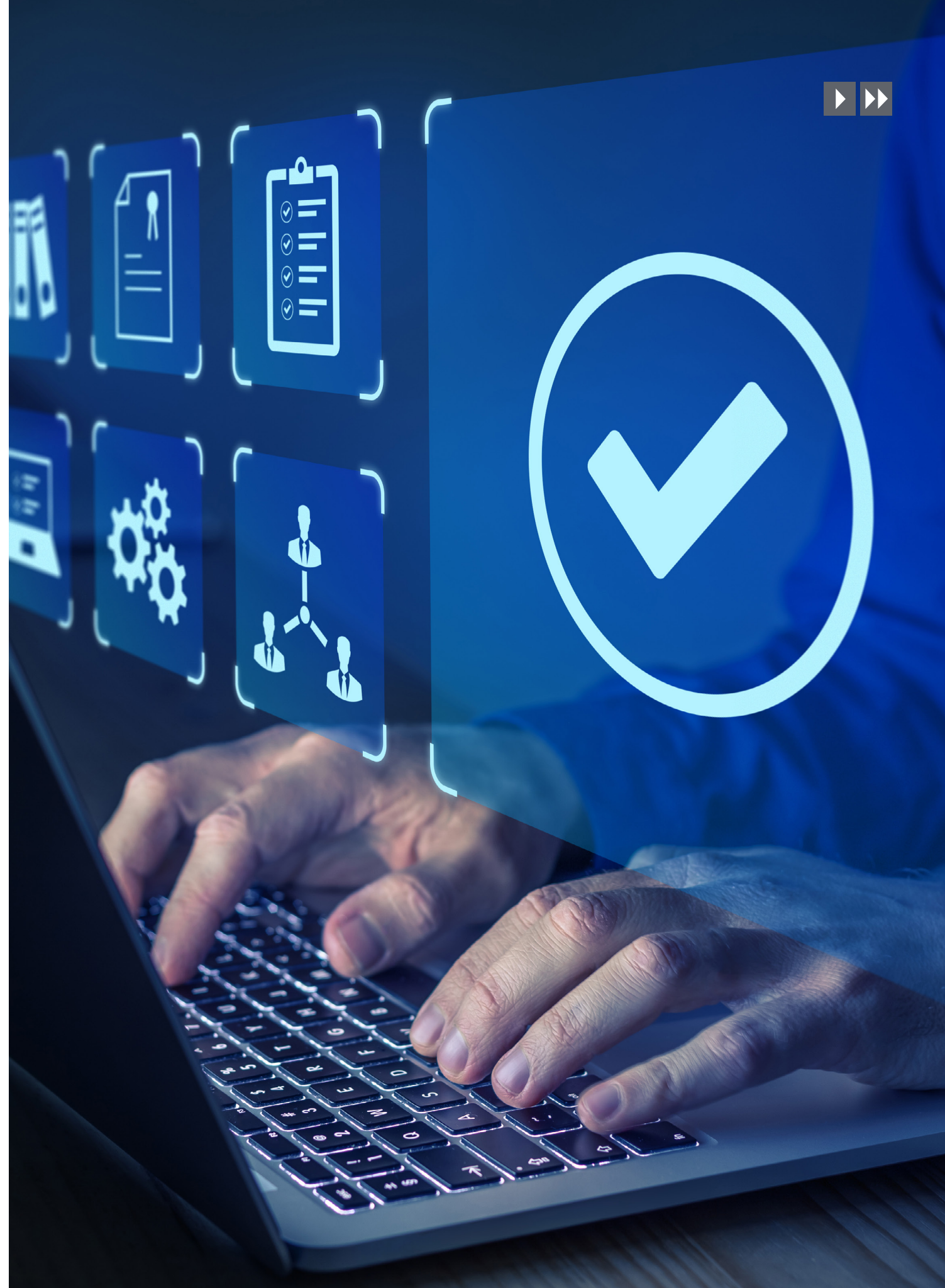
Proses ini berulang. Ketika Anda pertama kali mengaktifkan pemantauan, laporan mungkin akan tidak begitu berarti namun saat Anda lanjut ke langkah berikut, laporan tersebut akan menjadi lebih spesifik dan berguna. Informasi yang Anda kumpulkan dalam langkah ini akan menjadi kunci untuk langkah selanjutnya



Langkah 2: Memvalidasi dan Menilai

Langkah selanjutnya yaitu memvalidasi temuan ini. Nilai kebutuhan bisnisnya. Setiap IoT bayangan yang tidak dapat dijustifikasi harus dieliminasi karena hal tersebut meningkatkan permukaan serangan secara tidak perlu. Selebihnya, Anda perlu mengidentifikasi subjek (pengguna dan perangkat), arus lalu lintas dan alur kerja karena hal-hal tersebut perlu dipertimbangkan dalam kebijakan Anda. Sebagai contoh, siapa yang akan memiliki akses ke aset tertentu, dan apa yang akan mereka lakukan dengan aset tersebut. Terapkan prinsip hak istimewa terendah.

Segmentasi mikro bukan berarti melonggarkan kebijakan keamanan lainnya seperti kebijakan kata sandi, atau pembaruan *firmware*. Kemampuan setiap individu perlu dievaluasi. Apakah perangkat ini dapat mendukung autentikasi berbasis sertifikat? Apakah ada alat manajemen yang memungkinkan sertifikat tersebut untuk diterbitkan dan diterapkan? Apa saja arus lalu lintas yang dibutuhkan? Anda mungkin perlu memperoleh informasi ini dari pabrik, namun Anda juga harus membandingkannya dengan laporan analisis lalu lintas milik Anda sendiri. Jika Anda menemukan aset yang tidak sesuai dengan kebijakan perusahaan, Anda memerlukan rencana perbaikan untuk mematuhi, atau Anda perlu menerapkan kontrol tambahan.





Langkah 3: Merencanakan

Pada tahap ini Anda telah memahami aset, subjek (pengguna), lalu lintas dan alur kerja. Kini Anda perlu mengubah pengetahuan ini menjadi kebijakan autentikasi dan keamanan untuk menerapkan arsitektur segmentasi mikro yang dibutuhkan. Sebagaimana disebutkan sebelumnya, untuk mendapatkan hasil terbaik Anda harus menyertakan kombinasi segmentasi makro dan mikro. Ingat bahwa dalam sebagian besar skenario brownfield, Anda akan terbatas oleh arsitektur yang telah ada.

Ada beberapa opsi untuk segmentasi makro, seperti VLAN, VRF, VPN SPB, terowongan VXLAN atau GRE dan fitur khusus seperti VLAN pribadi. Masing-masing memiliki kelebihan dan kekurangan serta dapat bermanfaat dalam situasi yang berbeda. Untuk segmentasi mikro, Anda perlu mengetahui kebijakan apa yang harus disertakan dalam profil untuk setiap pengguna atau jenis perangkat. Terakhir, Anda perlu menentukan cara memetakan pengguna dan perangkat ke segmen dan kebijakan tertentu mereka. Hal ini akhirnya akan meliputi autentikasi atau klasifikasi, yang dapat mencakup sidik jari perangkat.

Idealnya, Anda perlu berinvestasi dalam teknologi (segmentasi yang ditentukan perangkat lunak) yang memungkinkan Anda untuk membuat kebijakan autentikasi yang fleksibel sehingga akan mudah untuk memperbarui profil jaringan.

Kami menyarankan Anda merancang alur autentikasi dalam urutan berikut:

1. Autentikasi melalui sertifikat 802.1x menggunakan server RADIUS. Autentikasi akan menghasilkan catatan autentikasi berisi informasi yang dapat dibagikan dengan firewall.
2. Jika Anda tidak dapat mengautentikasi perangkat melalui sertifikat 802.1x, maka Anda harus mencoba autentikasi MAC selanjutnya. Autentikasi MAC kurang aman dari 802.1x namun lebih baik daripada tidak ada autentikasi sama sekali. Gunakan autentikasi MAC sampai Anda siap untuk maju ke 802.1x.

3. Jika tidak ada profil yang dikembalikan, Anda dapat mencoba sidik jari yang juga dapat Anda petakan ke segmen profil dan aturan. Hal ini tidak menghasilkan autentikasi atau catatan perakunan namun akan terdaftar di database inventaris IoT.
4. Terakhir, Anda dapat menerapkan "tangkap semua" bawaan jika profil tidak dikembalikan, atau jika semuanya gagal. Pada tahap awal Anda masih perlu memetakan perangkat ke profil yang kemudian berakhir di segmen dan aturan yang sama dan akan mencatat perangkat di basis data inventaris.

Alur ini harus terstruktur secara fleksibel sehingga Anda dapat menyesuaikannya saat menjalaninya. Sebagai contoh, Anda mungkin ingin menghilangkan autentikasi MAC dahulu dan menambahkannya nanti, setelah Anda memiliki daftar alamat MAC yang diperoleh dari laporan inventaris. Dan seiring Anda berproses menyempurnakan, Anda dapat, misalnya, mengubah segmen dan aturan yang terkait dengan profil bawaan menjadi aturan yang sangat membatasi yang memungkinkan akses ke *bastion host* saja.

Anda mungkin juga ingin berbagi peran perangkat dengan firewall sehingga aturan firewall dapat mengikuti peran perangkat dan bukan hanya subjaringan/alamat IP. Keuntungan dari integrasi ini ada dua. Pertama, firewall dapat menerapkan kebijakan terperinci ke perangkat IoT tersebut. Kedua, kebijakan firewall akan berbasis pengguna atau peran sehingga tidak lagi terikat pada subjaringan atau alamat IP, hal ini memungkinkan desain ulang dan segmentasi ulang jaringan di masa mendatang.

Prosesnya akan berulang-ulang dan Anda perlu menyesuaikan, menyetel dan menyempurnakannya seiring dengan Anda yang menjadi lebih sempurna dalam penggunaan autentikasi dan segmentasi.



Langkah 4: Mensimulasikan

Terlepas dari matangnya rencana Anda, kecil kemungkinannya untuk berjalan dengan benar untuk pertama kalinya. Setiap kesalahan dalam desain skema autentikasi, setiap kelalaian yang Anda buat dalam "daftar izin" kebijakan keamanan akan mengakibatkan proses bisnis yang rusak. Anda perlu menerapkan kebijakan autentikasi dan akses dalam mode "*fail-open*". Artinya, perangkat dan pengguna yang gagal melakukan autentikasi akan tetap diizinkan di jaringan, dan arus lalu lintas yang tidak terduga akan tetap diizinkan. Namun semuanya akan dicatat dan dengan catatan ini Anda dapat memperbaiki skema autentikasi dan kebijakan.

Langkah 5: Melaksanakan

Setelah beberapa penyesuaian, Anda tidak akan lagi mengalami kegagalan autentikasi atau penolakan aliran yang sah. Anda kemudian dapat memindahkan kebijakan tersebut dari "*fail-open*" ke "*fail-close*" yang berarti bahwa perangkat jahat akan diblokir, dan aliran tak terduga akan dihentikan.

Tentunya, Anda perlu terus memantau perangkat dan arus lalu lintas yang tidak terduga — mengulang seluruh siklus tadi seperlunya.



Hal lainnya

Sebagai bagian dari pemantauan, pencatatan dan karantina yang berkelanjutan, kami menyarankan Anda juga berinvestasi dalam *Intrusion Detection System* (IDS) eksternal. Walau ada beragam serangan *Distributed Denial of Service* (DDoS) yang dapat diidentifikasi secara langsung oleh sakelar itu sendiri, IDS eksternal juga dapat mendeteksi serangan yang lebih luas seperti virus, atau anomali lainnya. Anda mungkin ingat pada beberapa tahun yang lalu, sejumlah kamera pengintai video terinfeksi *malware* Mirai, atau hari ketika perangkat ini meluncurkan serangan terkoordinasi pada server DNS global yang memengaruhi layanan seperti Twitter, Spotify, atau Paypal. Serangan ini mungkin tidak akan terdeteksi oleh sakelar Anda, tetapi pasti akan terdeteksi oleh IDS khusus.

Setelah serangan terdeteksi, IDS akan memberi tahu sistem manajemen jaringan (NMS) Anda tentang alamat IP perangkat yang terkena dampaknya. Idealnya, NMS Anda dapat menemukan perangkat ini dalam basis data dan akan mengubah profilnya menjadi "peran karantina".

"Peran karantina" adalah peran yang sangat terbatas, biasanya peran ini hanya mengizinkan komunikasi dengan *bastion host* sehingga perangkat dapat diperbaiki, sebagai contoh, dengan menetapkan kata sandi yang kuat, atau memperbarui *firmware*-nya.



Mengapa ALE

Solusi [Digital Age Networking](#) Alcatel-Lucent Enterprise menggabungkan segmentasi kuat dan fleksibel yang ditentukan oleh perangkat lunak dengan kebijakan NAC DPI dinamis yang memungkinkan evolusi bertahap menuju arsitektur *zero trust*.

Digital Age Network adalah cetak biru Alcatel-Lucent Enterprise yang memungkinkan bisnis dan organisasi untuk memasuki era digital dan mengembangkan bisnis digital mereka. Hal ini berdasarkan tiga pilar:

- [Jaringan Otonom](#) yang dengan mudah, otomatis dan aman menghubungkan orang, proses, aplikasi dan objek. Jaringan Otonom ALE berdasarkan pada portofolio efisien yang lengkap dengan platform manajemen terpadu yang sejati, mengantarkan kebijakan keamanan umum di seluruh LAN dan WLAN kami. Jaringan Otonom juga menyediakan fleksibilitas penyebaran di dalam ruangan, di luar ruangan dan di lingkungan industri. Manajemen jaringan dapat dilakukan di tempat, di awan, atau dalam penerapan hibrida, tergantung pada preferensi pelanggan.
- [Orientasi perangkat IoT yang aman dan efisien](#): Segmentasi membuat perangkat tetap berada di segmen tertentu dan meminimalkan risiko gangguan pada perangkat dan jaringan. Segmentasi IoT dapat membantu bisnis agar dengan mudah dan otomatis memahami apakah perangkat berjalan baik atau tidak, dan membantu menjaga jaringan tetap aman.
- [Inovasi Bisnis](#) melalui otomatisasi alur kerja: Mengintegrasikan pengguna, aplikasi, dan metrik IoT secara *real-time*, dengan data geolokasi, ke dalam platform kolaborasi, menyederhanakan pembuatan dan peluncuran proses dan layanan bisnis digital otomatis yang baru termasuk menginformasikan kepada administrator keamanan dan jaringan tentang terjadinya pelanggaran.

Apa Anda memiliki alat untuk membuat inventaris IoT/perangkat? Apa Anda memiliki alat yang memungkinkan Anda untuk memantau alur aplikasi? Apakah sakelar dan titik akses nirkabel Anda saat ini siap untuk segmentasi yang ditentukan perangkat lunak? Jika saat ini Anda tidak memiliki alat ini, [hubungi kami](#) dan kami dapat membantu Anda mencapainya.



Yang kami tahu pasti

Mari kita rangkum dengan ringkasan inti:

- Untuk memiliki ZTA yang benar-benar efisien, Anda harus menggunakan segmentasi makro dan mikro.
- Terdapat lima langkah menuju ZTA: memantau, memvalidasi dan menilai, merencanakan, mensimulasikan dan melaksanakan
- ZTA yang berdasarkan segmentasi mikro bertumpu pada tiga pilar: Autentikasi, dengan 802.1x EAP-TLS sebagai acuan terpercaya; kebijakan yang berbeda terkait dengan peran pengguna atau perangkat yang merujuk ke prinsip hak istimewa paling rendah; dan pemantauan dan karantina berkelanjutan
- Dalam lingkungan hibrida dan bergerak, segmentasi mikro perlu ditentukan oleh perangkat lunak, artinya, harus bersifat dinamis dan berbasis kebijakan, bukan ditentukan secara statis, jika tidak maka tidak akan praktis

Migrasi ke ZTA melalui segmentasi mikro adalah sebuah proses, mustahil bagi perusahaan berukuran signifikan untuk sampai ke ZTA dalam satu siklus penyegaran. Namun dalam setiap siklus penyegaran atau desain ulang atau peningkatan berkelanjutan, Anda dapat mendekati tujuan tersebut jika Anda menempatkan infrastruktur dan desain yang tepat.

Alcatel-Lucent Enterprise berkomitmen untuk mengembangkan teknologi dan solusi jaringan yang membantu organisasi untuk mewujudkan potensi bisnis mereka melalui transformasi digital

