TUGAS MANAJEMEN JARINGAN

DESY MARITA

09011281320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA INDERALAYA

2016

Network Management: Big Data NetFlow Analysis

- Pejelasan NetFlow

NetFlow adalah teknologi Cisco IOS yang menyediakan statistik pada paket yang mengalir melalui router Cisco atau switch multilayer. NetFlow adalah standar untuk mengumpulkan data operasional IP dari jaringan IP. Teknologi NetFlow dikembangkan karena jaringan profesional diperlukan sebuah metode yang sederhana dan efisien untuk melacak TCP / IP mengalir dalam jaringan, dan SNMP tidak cukup untuk tujuan ini. Sementara SNMP mencoba untuk memberikan rentang yang sangat luas dari fitur manajemen jaringan dan pilihan, NetFlow difokuskan pada penyediaan statistik pada paket IP mengalir melalui perangkat jaringan. NetFlow menyediakan data untuk mengaktifkan jaringan dan pemantauan keamanan, perencanaan jaringan, analisis lalu lintas untuk memasukkan identifikasi kemacetan jaringan, dan akuntansi IP untuk tujuan penagihan. Misalnya, pada gambar, PC 1 terhubung ke PC 2 menggunakan aplikasi seperti HTTPS. NetFlow dapat memonitor koneksi aplikasi, pelacakan byte dan paket jumlah untuk itu aliran aplikasi individu. Ini kemudian mendorong statistik ke server eksternal yang disebut kolektor NetFlow.

NetFlow meningkatkan pada “asli NetFlow” dengan menambahkan kemampuan untuk menyesuaikan parameter analisis lalu lintas untuk kebutuhan spesifik dari administrator jaringan. Fleksibel NetFlow memfasilitasi penciptaan konfigurasi yang lebih kompleks untuk analisis lalu lintas dan data ekspor melalui penggunaan komponen konfigurasi dapat digunakan kembali. Ada banyak kegunaan potensial dari statistik yang NetFlow berikan; Namun, sebagian besar organisasi menggunakan NetFlow untuk beberapa atau semua tujuan pengumpulan data penting berikut:

- Mengukur yang menggunakan apa yang sumber daya jaringan untuk tujuan apa.
- Akuntansi dan pengisian kembali sesuai dengan tingkat pemanfaatan sumber daya.
- Menggunakan informasi diukur untuk melakukan perencanaan jaringan yang lebih efektif sehingga alokasi sumber daya dan penyebaran baik-selaras dengan kebutuhan pelanggan.
- Menggunakan informasi untuk struktur yang lebih baik dan menyesuaikan set aplikasi dan layanan untuk memenuhi kebutuhan pengguna dan persyaratan layanan pelanggan yang tersedia.

Ketika membandingkan fungsi SNMP untuk NetFlow, analogi untuk SNMP mungkin software remote control untuk kendaraan tak berawak; sedangkan analogi untuk NetFlow adalah, tagihan telepon belum rinci sederhana. Catatan telepon menyediakan call-by-call dan statistik dikumpulkan yang memungkinkan orang membayar tagihan untuk melacak panggilan panjang, panggilan yang sering, atau panggilan yang tidak seharusnya dilakukan. Berbeda dengan SNMP, NetFlow menggunakan "berbasis mendorong" model. Kolektor hanya mendengarkan lalu lintas NetFlow, dan perangkat jaringan yang bertanggung jawab atas pengiriman data NetFlow untuk kolektor, berdasarkan perubahan dalam cache aliran mereka. Perbedaan lain antara NetFlow dan SNMP adalah bahwa NetFlow hanya mengumpulkan statistik lalu lintas, seperti yang ditunjukkan pada gambar, sedangkan SNMP juga dapat mengumpulkan banyak indikator kinerja lainnya, seperti kesalahan antarmuka, penggunaan CPU, dan penggunaan memori. Di sisi lain, statistik lalu lintas yang dikumpulkan menggunakan NetFlow memiliki lebih banyak rincian daripada statistik lalu lintas yang dapat dikumpulkan dengan menggunakan SNMP.

Dari video tersebut Cisco 2016 memberikan kesempatan untuk berhubungan dengan sejumlah pengunjung ke stand, serta kesempatan untuk bertemu dengan BrightTalk untuk beberapa diskusi video yang direkam dengan topik operasi jaringan. Video ini berfokus pada dimana Kentik Jim Frey, alias VP Strategic, berbicara tentang komplikasi jaringan saat ini dan bagaimana analisis besar data NetFlow membantu operator mencapai wawasan tepat waktu ke lalu lintas mereka.

Kentik Jim Frey menjelaskan:

- Why Big Data NetFlow Analysis?

  Manajemen jaringan adalah salah satu daerah terakhir dari operasi TI untuk mengambil keuntungan dari Big Data. Untuk melihat efek dari Big Data terdapat pada manajemen jaringan dan analisis. Kentik berfikir bahwa manajemen jaringan adalah salah satu daerah terakhir dalam operasi digital dan IT yang telah mengambil keuntungan dari teknologi Big Data. Kentik telah membangun sebuah arsitektur Big Data pada inti dari solusi pemantauan jaringan. Yang membawa beberapa keuntungan nyata, karena Big Data besar tidak hanya tentang penanganan volume data yang besar, tetapi juga tentang membiarkan Anda menavigasi melalui dan menjelajahi data yang sangat cepat. Anda harus membangun arsitektur yang tepat untuk melakukan itu. Anda harus mengemasnya dengan cara yang membuatnya efektif dan efisien. itu menjadi

solusi yang sangat kuat. untuk memahami keadaan jaringan Anda dan kemudian mampu mengebor, menelusuri, bor kiri, bor kanan, dan poros analisis Anda.

Pelaksanaan Big Data juga memberi kita dasar untuk melakukan evaluasi otomatis metrik, sehingga kita dapat mulai melakukan hal-hal seperti menyiagakan otomatis. deteksi DDoS adalah kasus penggunaan besar bagi kami, dan Big Data memungkinkan kita untuk menjadi definitif dan jelas. Big analisis data benar-benar membantu dengan beberapa hal penting salah satunya adalah visibilitas yang jelas dalam aktivitas saat ini pada jaringan, sehingga Anda dapat melihat persis siapa yang bicara kepada siapa dan jenis aktivitas, lalu lintas, dan volume. Hal ini dapat membantu Anda melihat tren dalam aktivitas. Anda dapat menggunakannya untuk menyimak tren tersebut dan untuk membantu Anda mengenali apa yang normal dan apa yang tidak. Ketika Anda melihat sesuatu yang Anda tidak yakin tentang, Anda ingin bisa untuk turun ke dalamnya dan memahaminya secepat mungkin.

- Big Data Architectural Considerations

Organisasi yang tertarik Big Data sebagai arsitektur untuk manajemen jaringan harus berpikir tentang beberapa hal yaitu : Tidak semua arsitektur Big Data secara khusus dirancang untuk kasus penggunaan monitoring jaringan. Anda dapat mengambil alat Big Data lain dan mencoba untuk beradaptasi mereka, tapi itu sedikit adil bekerja untuk sampai ke tingkat fungsionalitas yang kebanyakan orang harapkan dari alat data non-Big yang di luar sana. Anda dapat mengambil alat Big Data lain dan mencoba untuk beradaptasi. apa yang Anda butuhkan untuk dicari adalah solusi yang mengambil keuntungan dari semua hal-hal besar yang Big Data dapat lakukan untuk Anda, tetapi yang telah disesuaikan dan dioptimalkan secara khusus untuk manajemen jaringan dan penggunaan manajemen keamanan kasus Anda. Anda memerlukan solusi dan memberikan manfaat tanpa harus membangun semuanya sendiri. Banyak sistem Big Data melakukan pekerjaan yang sangat baik dari semua data dan menyimpannya. Tapi ketika ingin menjalankan laporan, dapat mengambil puluhan menit, bahkan di jam kasus terburuk, untuk mendapatkan data kembali keluar yang diinginkan. Sulit untuk mengubah, menggeser dan mengajukan pertanyaan baru, karena itu berarti mulai dari awal. Jadi salah satu tantangan besar dengan solusi yang dibangun di arsitektur Big Data adalah untuk memberikan yang kemudahan akses, yang kecepatan akses, dengan kemampuan terbatas untuk mencapai semua data yang ada tersedia untuk Anda. Kentik menangani volume yang sangat besar data di backend, dengan miliaran catatan yang masuk ke SaaS setiap hari. Tapi hal lain mampu mendapatkan data kembali keluar

secepat mungkin. Sebagian besar - 95% dari permintaan dijalankan terhadap backend dengan pelanggan, kembali hasilnya waktu kurang dari dua detik. Jadi itu berarti bahwa Anda akan tahu apa yang terjadi atau Anda dapat mencari tahu.

- Other Interesting Trends

  SDN mengubah cara bahwa jaringan berperilaku. Jadi dapat memantau apa yang terjadi misalnya, bagaimana perilaku perubahan jaringan setelah perubahan telah dibuat melalui semacam penegakan kebijakan software-defined. Arsitektur Big Data dirancang untuk menjadi sangat fleksibel. Karena menggunakan API terbuka memungkinkan untuk menghubungkan ke sistem lain. Hal ini dapat terhubung dengan sangat sederhana dan mudah dengan apa pun macam sumber data lain yang telah datang atau output dimana Anda ingin menempatkannya. Kami juga memiliki rencana untuk terus memperluas platform ini, dan tumbuh, dan menyediakan layanan SaaS dari beberapa geografi. Jadi itu akan membantu menjaga dengan pertumbuhan geografis yang merupakan bagian alami dari segala macam sistem jaringan dan bisnis.

- What's Next for Big Data NetFlow Visibility

  Beberapa hal yang dilihat sekarang adalah untuk menambahkan penyelidikan keamanan yang lebih dalam, lebih kaya dan lebih spesifik, peringatan, dan anomali deteksi. Kami sedang dalam proses meningkatkan kemampuan kita untuk secara otomatis mengenali penyimpangan dari normal, sehingga kita dapat memahami anomali ketika mereka datang. Juga meningkatkan kemampuan untuk langsung mengintegrasikan dengan sistem eksternal untuk memicu respons untuk masalah. Anda dapat secara otomatis menyerahkan data ke sistem lain untuk tindakan, atau bahkan mengatur tindakan otomatis jika Anda berpikir hal itu dibenarkan. Ledakan mutlak dalam jumlah perangkat yang terhubung berarti bahwa ada akan peningkatan besar dalam jumlah lalu lintas yang menggunakan Internet, sumber yang perlu dilacak, dan perilaku yang perlu dipahami dan ditandai seperti biasa terhadap abnormal.