Nama : Krisna Kapor

NIM : 09011381722109

Mata Kuliah : Administrasi dan Manajemen Jaringan

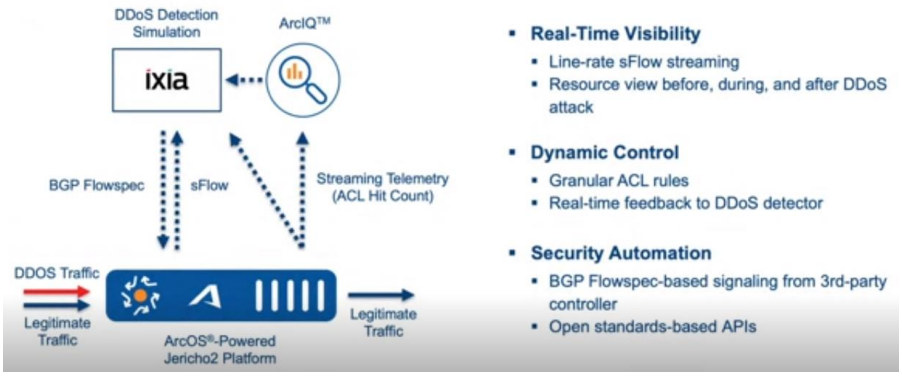
ArcOS + ArcIQ: Best-of-Breed Secured Networking

Perangkat lunak ArcOS menyediakan banyak operasi manajemen otomatis melalui kontrol FCAPS (*Fault, Configuration, Accounting, Performance, Security*) yang tersedia di luar kotak. Selain itu, ia menawarkan *native streaming telemetry* yang memungkinkan *streaming* pada *control plane, forwarding plane*, dan data lingkungan perangkat. Semua data telemetri streaming diamankan melalui koneksi TLS.

Keamanan ada dalam ArcOS DNA dan telah dibangun ke dalam produk sejak awal.

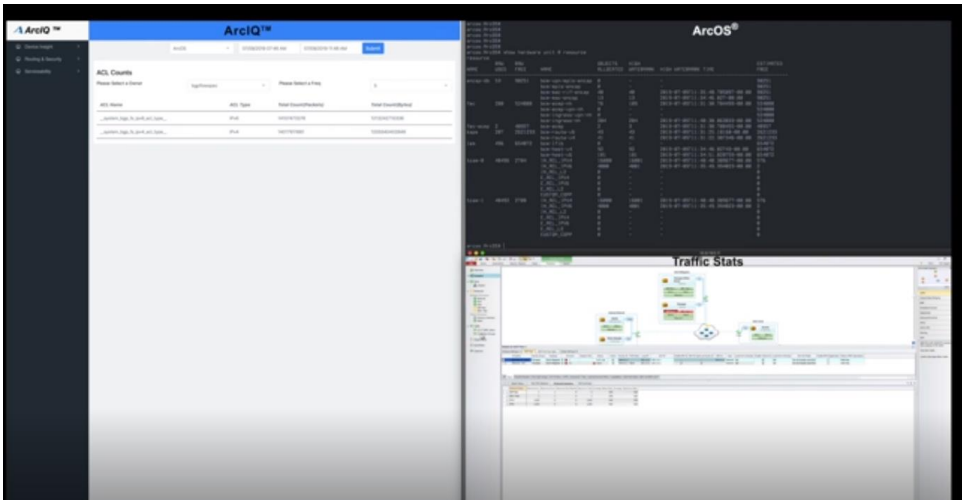
- Setiap *image* perangkat lunak adalah kunci pribadi yang ditandatangani oleh Arrcus untuk memastikan keaslian *end-user image.*
- Sumber daya infrastruktur kritis seperti CPU, memori, proses, port, dan pengguna dimonitor melalui NetOps toolkit (ArcOpsTM)
- Peringatan dikeluarkan ketika pola penggunaan yang tidak sah terdeteksi. Akses ArcOS dan *management plane* diamankan oleh SSH, TACACS +, dan panggilan *secure* REST.
- VRF manajemen memungkinkan pemisahan yang jelas antara jaringan manajemen out-of-band dan jaringan pesawat data in-band.

Dalam demo ini akan menampilkan solusi mitigasi jaringan DDOS menggunakan platform Arccus Flagship ArcOS dan ArcIQ. Berikut ini adalah pengaturan sederhana:



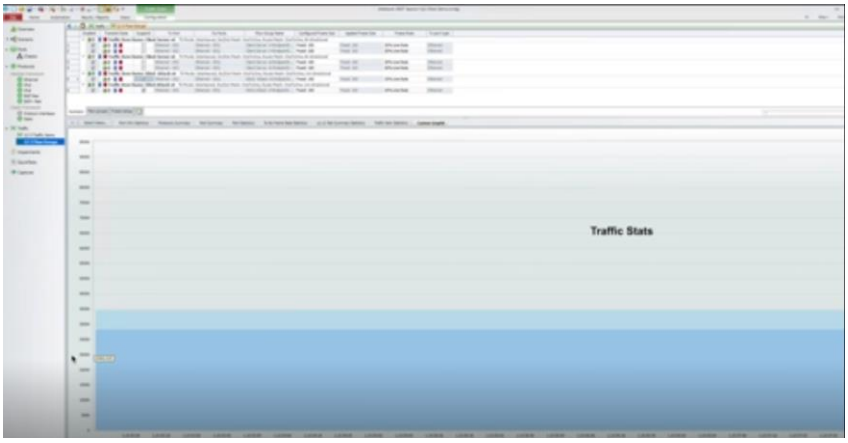
Gambar 1 *simple setup ArcOS* dan *ArcIQ*

Pada gambar 1 ialah Platform Jericho2 yang didukung oleh platform ArcOS yang dibuat untuk menerima lalu lintas yang sah dan DDOS menggunakan sflow Platform ArcOS mengirimkan sampel dengan tingkat kunjungan tinggi untuk mensimulasikan detektor DDOS. Untuk demo ini, akan menggunakan detektor DDOS yang disimulasikan. Detektor DDOS yang disimulasikan ini kemudian mengirimkan aturan ACL sebagai kebijakan dan diberi kode melalui EGP flows kembali untuk diinstal pada perangkat ArcOS. Ini dirancang untuk memblokir lalu lintas DDOS. Memanfaatkan Telemetri streaming ArcOS untuk ACL *hit count*. Detektor DDOS kemudian dapat mengukur efektivitas yang dikirim ke perangkat. Platform analitik ArcIQ yang menyediakan tampilan sumber daya sistem waktu-nyata sebelum dan selama serangan DDOS, ia menyediakan pandangan terpusat tentang dampak tindakan detektor DDOS di jaringan. Bersama-sama ArcOS dan ArcIQ memberikan yang terbaik dari solusi mitigasi DDOS berkembang biak 100 G dengan aliran line rate sflow dan aturan bgp flowpec skala tinggi. Sekarang, mari kita mulai demo.



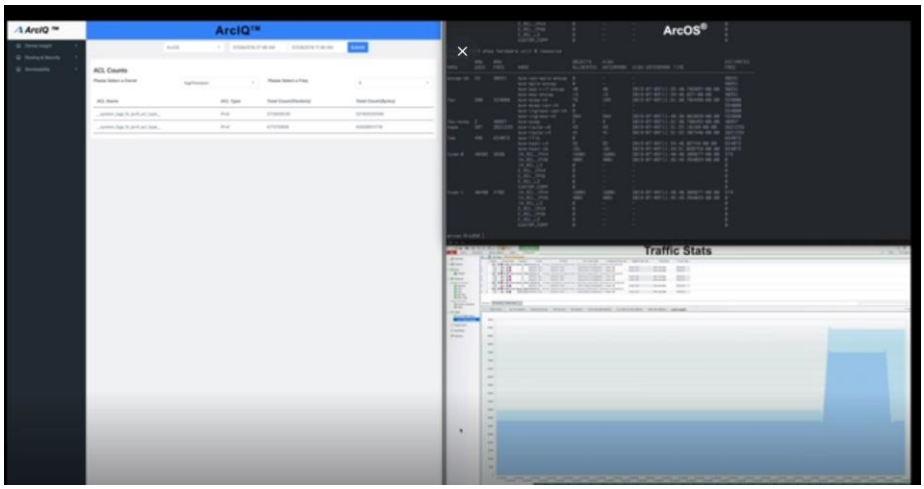
Gambar 2 ArcOS dan ArcIQ

Pada gambar 2 memiliki tiga Windows di sini, ArcIQ di sebelah kiri, ArcOS di kanan atas dan lalu lintas berhenti di kanan bawah. Dapat dilihat bahwa ArcOS sudah diisi sebelumnya dengan dua puluh ribu aturan EGP *Flowspec* ACL *Rules* dan menerima 33 gigabit per detik dari lalu lintas dan grafik 33 gigabit per detik lalu lintas ini diambil sampel oleh sflow pada perangkat ArcOS dengan termasuk sflow. Dapat dilihat total 40 gigabit per detik lalu lintas yang diarsir dan biru muda serta grafik.



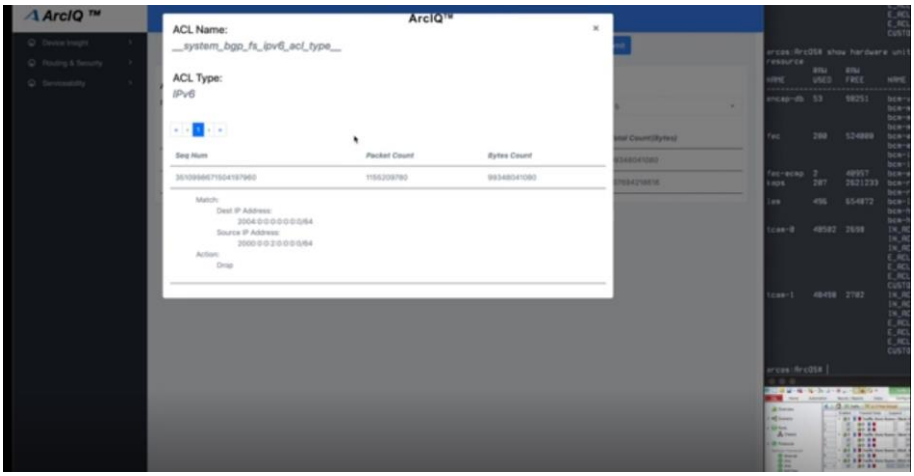
Gambar 3 lalu lintas traffic

Untuk mengalirkan 42 gigabit per detik dari server serangan lalu lintas DDOS dan jaringan ipv4. 104.1.0.0/24 dan jaringan IPv6 2004/64. Dapat dilihat peningkatan tingkat lalu lintas dan jendela statistik lalu lintas. Total 75 gigabit per detik lalu lintas sekarang diambil dari perangkat yang mencakup lalu lintas. Sebagai reaksi terhadap pengambilan sampel lalu lintas DDOS, sekarang mengeluarkan Aturan flowpec dari ixia. Di jendela ArcOS, dapat dilihat bahwa BGP diterima dengan benar dan diinstal aturan flowpec untuk memblokir serangan DDOS. Di jendela statistik lalu lintas di kanan bawah, Dapat dilihat bahwa tingkat lalu lintas sebentar meningkat menjadi 75 gigabit per detik dan kemudian turun kembali menjadi 33 gigabit per detik setelah serangan diblokir di dalam perangkat ArcOS.



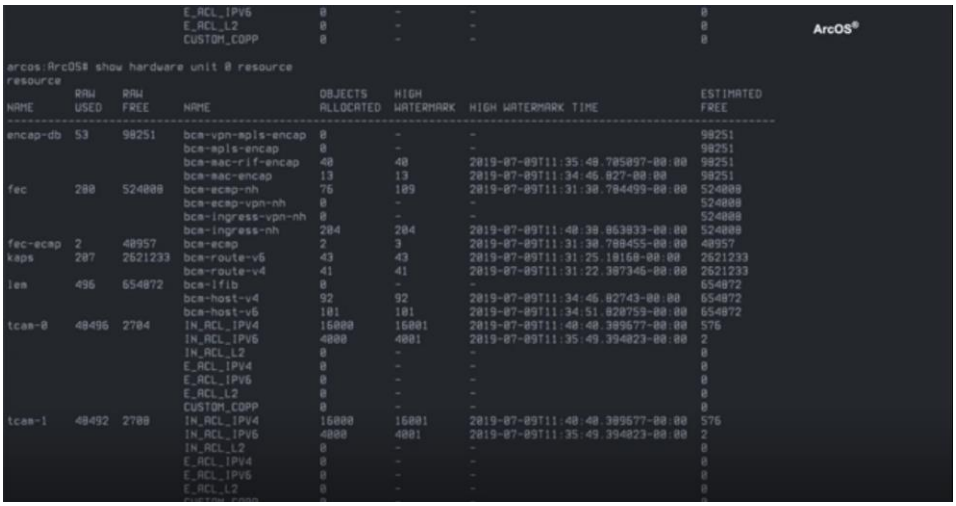
Gambar 4 ArcOS dan ArcIQ

Platform analitik Arccus atau ArcIQ di mana Dapat dilihat ArcOS terus *streaming* IPv4 dan IPv6 ACL. Ini dianggap sebagai ACL yang mendasarinya efektif dalam memblokir lalu lintas DDOS.



Gambar 5 ArcIQ

Sekarang menghentikan serangan DDOS dengan menghentikan string lalu lintas DDOS dari ixia dan dengan menarik Aturan BGP flowpec yang relevan dari ixia.



Gambar 6 ArcOS

Pada jendela ArcOS, perhatikan bahwa BGP telah menerima penarikan ACL dengan benar. Setelah serangan dihentikan pada ArcIQ, tidak lagi dilihat peningkatan ACL *hit count* karena ACL yang mendasarinya telah dihapus.

Jadi itulah demo perangkat ArcOS yang berhasil memitigasi serangan DDOS di lingkungan yang disimulasikan.