NAMA : Muhammad Zufar Badrus

NIM : 09011381722130

KELAS : ADMINISTRASI DAN MANAGEMENT SISTEM JARINGAN

RESUME

ArcOS + ArcIQ: Best-of-Breed Secured Networking

Latar Belakang

Bisnis saat ini menuntut perangkat lunak jaringan yang tangguh dan berkinerja tinggi ketika mereka membangun infrastruktur jaringan pintar mereka. Jika Anda mencari sistem operasi jaringan canggih untuk mendukung inisiatif transformasi jaringan organisasi Anda, lihat bagaimana solusi jaringan aman terbaik (ArcOS® + ArcIQ ™) memberikan visibilitas waktu nyata, dinamis kontrol, dan otomatisasi keamanan untuk berhasil mengurangi serangan DDoS.

ArcOS

ArcOS adalah perangkat lunak yang sepenuhnya dapat diprogram, modular, dan dapat diperpanjang yang melepaskan transisi dari integrasi vertikal ke segmentasi horizontal kelas terbaik di setiap lapisan dalam jaringan. Dibangun dari bawah ke atas menggunakan standar terbuka, ArcOS memungkinkan organisasi untuk secara efektif membangun infrastruktur yang dapat diskalakan secara besar-besaran di lingkungan jaringan fisik, virtual, dan cloud sambil memberikan kinerja yang unggul, keamanan, dan fleksibilitas penempatan.

Best-of-Breed Analytics

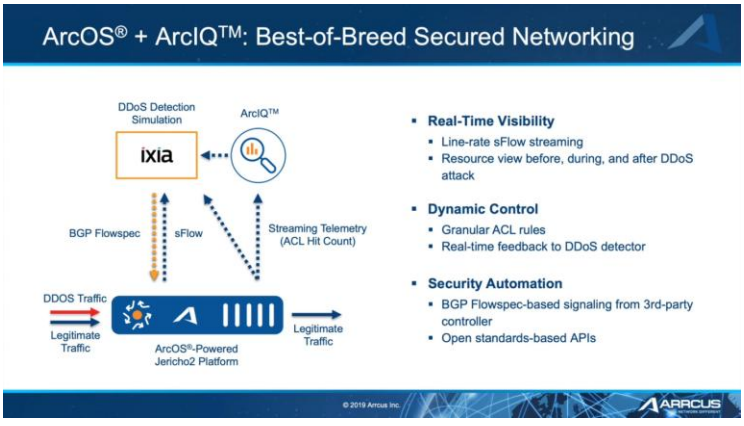
Apakah jaringan dikelola di tempat atau di cloud, operator perlu memvisualisasikan seluruh jaringan melalui analitik waktu nyata dengan Visibilitas Jauh. Perangkat lunak ArcOS menyediakan banyak operasi manajemen otomatis melalui FCAPS (Kesalahan, Konfigurasi, Akuntansi, Kinerja, Keamanan) yang dikendalikan oleh Kebijakan yang tersedia di luar kotak.

Selain itu, ia memiliki kemampuan telemetri streaming asli yang memungkinkan streaming dari bidang kontrol, bidang penerusan, dan data terkait lingkungan perangkat.

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 kemampuan telemetri streaming asli yang memungkinkan streaming bidang kontrol, bidang penerusan, dan data lingkungan perangkat. Semua data telemetri streaming diamankan melalui koneksi TLS.

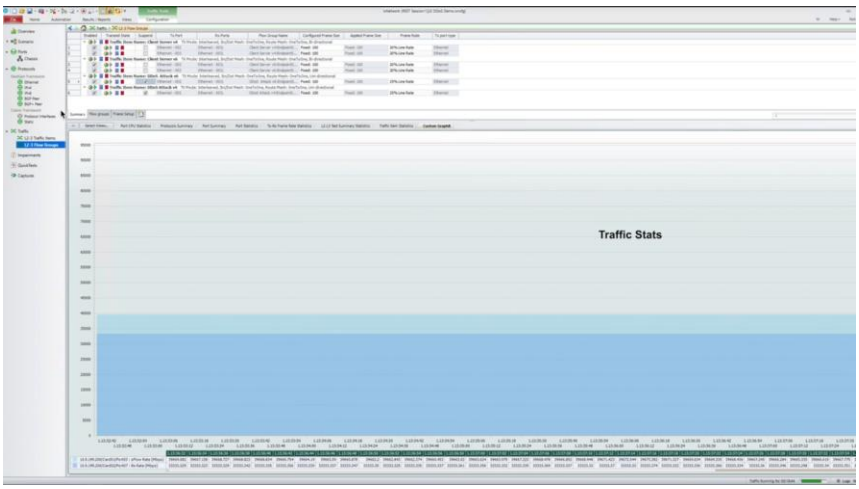
- Setiap gambar perangkat lunak adalah kunci pribadi yang ditandatangani oleh Arrcus untuk memastikan keaslian gambar pengguna akhir
- Sumber daya infrastruktur kritis seperti CPU, memori, proses, port, dan pengguna dimonitor melalui NetOps toolkit (ArcOpsTM)
- Peringatan dikeluarkan ketika pola penggunaan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

Dengan setup menggunakan ArcOS Power Jericho 2 Platform untuk menerima Legitimate DDOS Traffic menggunakan sFlow untuk memberikan sample traffic high rate menuju simulasi DDOS Detection, ArcOS detection Simulation menggunakan **IXIA.**

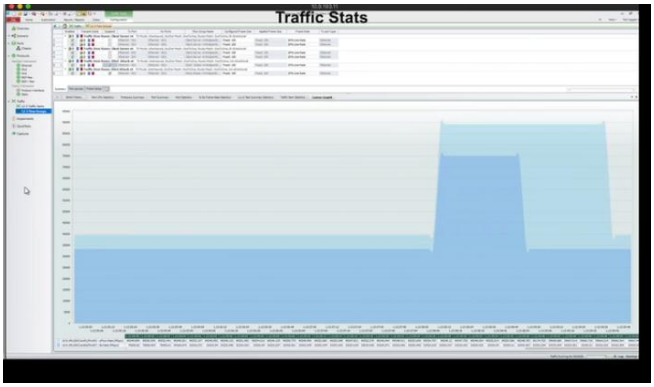


Simulasi DDOS detector ini mengirimkan ACL rules secara via kode BGP Flowspec untuk di instal di device ArcOS ini di desain untuk memblock DDOS traffic. Dengan ArcOS platform memiliki real time resource view yang memprioritaskan serangan DDOS itu memungkinkan kita untuk melihat impact dari DDOS Detection di network tersebut.Bersama-sama ArcIQ dan ArcOS mengirimkan *best of breed* Solusi DDOS Contoh Demo nya Sistem ini dengan menggunakan ArcIQ, ArcOS dan Traffic Stats

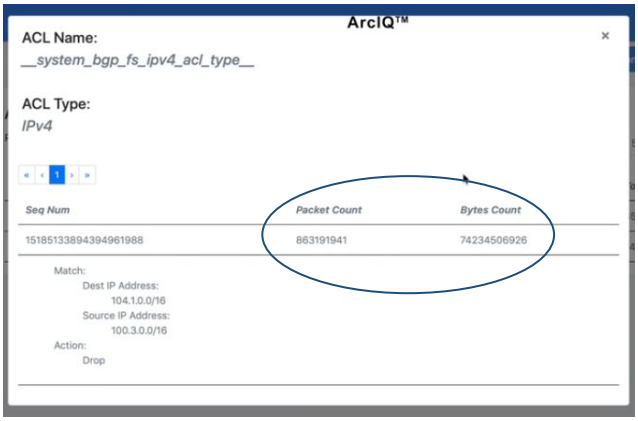
ArcOs banyak menggunakan 2 puluh ribu BGP Flowspec acl rules pada IPV4 4ribu dan IPV6 16 ribu dan menerima 3 Puluh ribu GB per detik yang tervisual di legitimate traffic pada apk *Traffic Stats* bewarna biru tua, 3 GB per detik itu merupakan sFlow sampel dari device ArcOS dengan termasuk sFlow bisa dilihat 4 puluh ribu GB per detik bewarna biru terang pada *Traffic Stats*



disini IXIA digunakan untuk meningkatkan traffic rate dari legitimate traffic dan serangan traffic dan melihat reaksi di sFlow sampel. Pada ArcOS sekarang BGP akan menerima lebih banyak dari flow spec rules untuk menangkal serangan ddos



Pada bagian traffic states bagian legitiamate traffic akan meningkat sebanyak 75 gb dan kemudian turun menjadi 3 gb setelah block serangan ddos didalam device ArcOS di ArcIQ device ArcOS akan mengganti count packet dan count bytes pada IPV4 dan IPV6 acl. Untuk menstop ddos attack dengan menghentikan traffic string dari IXIA danWidthdrawing BGP pada IXIA



Saat serangan sudah stop pada ArcIQ kita tidak akan lagi melihat Count dan Bytes nya berubah saat seperti sedang terkena DDOS

BrightTALK

Certificate of Attendance

This is to certify that:

muhammad zufar badrus

student, universtas

Viewed:

ArcOS + ArcIQ: Best-of-Breed Secured Networking

On: April 27, 2020
For: 5 of 5 minutes

Presented by:
Sri Paladgu

April 27, 2020
Date

www.brighttalk.com/webcast/17101/367356
Content link