

**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**

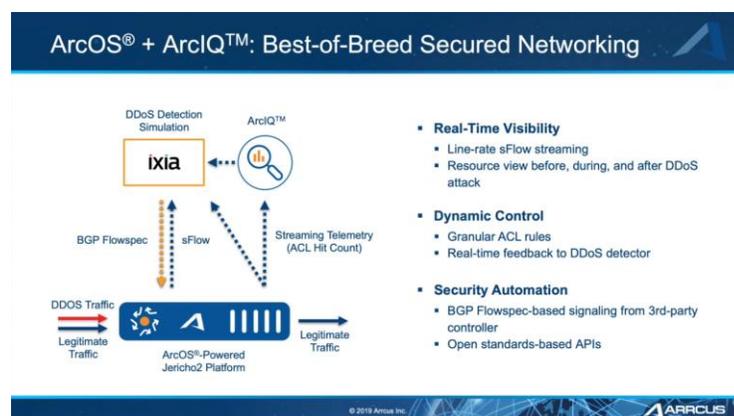
Apakah jaringan dikelola di tempat atau di cloud, operator perlu memvisualisasikan seluruh jaringan melalui analitik waktu nyata dengan Visibilitas Jauh. Perangkat lunak ArcOS menyediakan banyak operasi manajemen otomatis melalui FCAPS (Kesalahan, Konfigurasi, Akuntansi, Kinerja, Keamanan) yang dikendalikan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

Selain itu, ia memiliki kemampuan telemetry 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 telemetry streaming asli yang memungkinkan streaming bidang kontrol, bidang penerusan, dan data lingkungan perangkat. Semua data telemetry streaming diamankan melalui koneksi TLS.

- Setiap gambar perangkat lunak adalah kunci pribadi yang ditandatangani oleh Arcus untuk memastikan keaslian gambar pengguna akhir
- Sumber daya infrastruktur kritis seperti CPU, memori, proses, port, dan pengguna dimonitor melalui NetOps toolkit (ArcOps™)
- 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**.



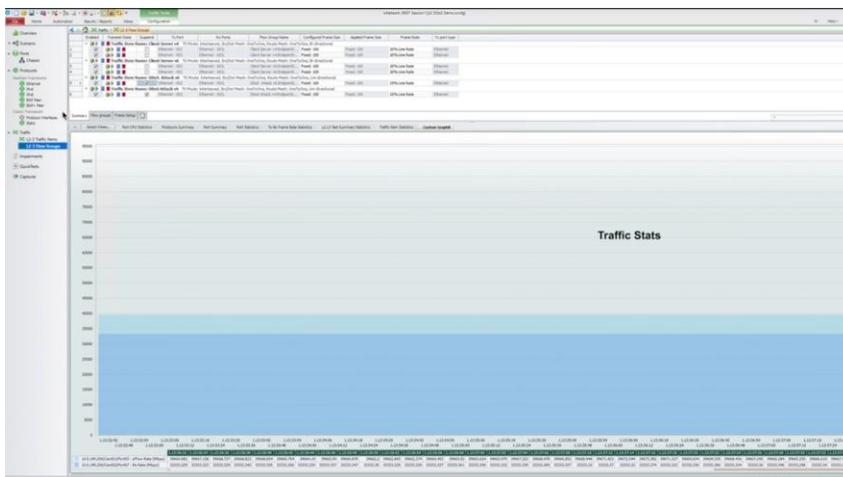
Simulasi DDOS detector ini mengirimkan ACL rules secara via kode BGP Flowspec untuk di instal di device ArcOS ini di desain untuk memblock DDOS traffic. Dengan ArcOS platform memiliki real time resource view yang memprioritaskan serangan DDOS itu memungkinkan kita untuk melihat impact dari DDOS Detection 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:ArcOS#
arcos:ArcOS#
arcos:ArcOS#
arcos:ArcOS# show hardware unit 0 resource
resource
```

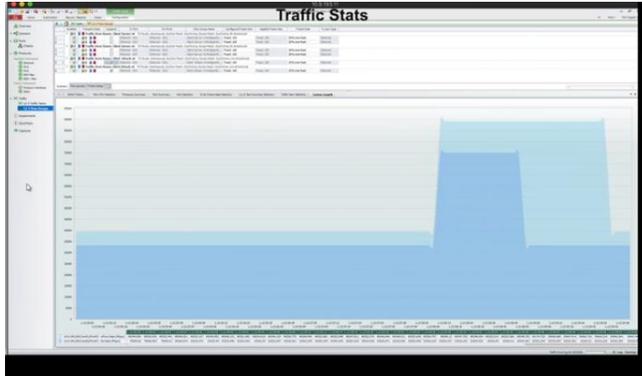
NAME	RAW USED	RAW FREE	NAME	OBJECTS ALLOCATED	HIGH WATERMARK	HIGH WATERMARK TIME	ESTIMATED FREE
encap-db	53	98251	bcm-vpn-mpis-encap	0	-	-	98251
			bcm-mpis-encap	0	-	-	98251
			bcm-mac-rif-encap	40	40	2019-07-09T11:35:40.705097-00:00	98251
fec	280	524000	bcm-mac-encap	13	13	2019-07-09T11:34:46.827-00:00	98251
			bcm-ecap-nh	76	109	2019-07-09T11:31:30.704499-00:00	524000
			bcm-ecap-vpn-nh	0	-	-	524000
			bcm-ingress-vpn-nh	0	-	-	524000
			bcm-ingress-nh	204	204	2019-07-09T11:40:30.063033-00:00	524000
fec-ecap	2	40957	bcm-ecap	2	3	2019-07-09T11:31:30.700455-00:00	40957
			bcm-route-v6	43	43	2019-07-09T11:31:25.10160-00:00	2621233
kaps	207	2621233	bcm-route-v4	41	41	2019-07-09T11:31:22.307346-00:00	2621233
			bcm-lfib	0	-	-	654872
lem	496	654872	bcm-host-v4	92	92	2019-07-09T11:34:46.82743-00:00	654872
			bcm-host-v6	101	101	2019-07-09T11:34:51.820759-00:00	654872
tcam-0	48496	2704	IN_ACL_IPV4	16000	16001	2019-07-09T11:40:40.309677-00:00	576
			IN_ACL_IPV6	4000	4001	2019-07-09T11:35:49.394023-00:00	2
			IN_ACL_L2	0	-	-	0
			E_ACL_IPV4	0	-	-	0
			E_ACL_IPV6	0	-	-	0
			E_ACL_L2	0	-	-	0
			CUSTOM_COPP	0	-	-	0
			IN_ACL_IPV4	16000	16001	2019-07-09T11:40:40.309677-00:00	576
			IN_ACL_IPV6	4000	4001	2019-07-09T11:35:49.394023-00:00	2
			IN_ACL_L2	0	-	-	0
tcam-1	48492	2700	E_ACL_IPV4	0	-	-	0
			E_ACL_IPV6	0	-	-	0
			E_ACL_L2	0	-	-	0
			CUSTOM_COPP	0	-	-	0
			IN_ACL_IPV4	16000	16001	2019-07-09T11:40:40.309677-00:00	576
			IN_ACL_IPV6	4000	4001	2019-07-09T11:35:49.394023-00:00	2

```
arcos:ArcOS#
```

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



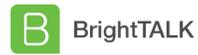
Pada bagian traffic states bagian legitimate traffic akan meningkat sebanyak 75 gb dan kemudian turun menjadi 3 gb setelah block serangan ddos didalam device ArcOS di ArcIQ device ArcOS akan mengganti count packet dan count bytes pada IPV4 dan IPV6 acl. Untuk menstop ddos attack dengan menghentikan traffic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

The screenshot shows the configuration for an ACL named '\_\_\_system\_bgp\_fs\_ipv4\_acl\_type\_\_'. The ACL Type is 'IPv4'. A table shows the traffic counts for a specific rule:

Seq Num	Packet Count	Bytes Count
15185133894394961988	863191941	74234506926

Match criteria:  
Dest IP Address: 104.1.0.0/16  
Source IP Address: 100.3.0.0/16  
Action: Drop

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



# 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](http://www.brighttalk.com/webcast/17101/367356)  
Content link