

DAFTAR GAMBAR

Gambar II.1 Contoh topologi yang telah di mikrosegmentasi (Basta et al., 2021)	15
Gambar II.2 Contoh ICMP <i>flood attack</i> pada sebuah LAN (kaalel, 2022)	18
Gambar II.3 Tahapan PPDIOO	21
Gambar III.1 Model Konseptual	24
Gambar III.2 Sistematisa Penelitian	26
Gambar III.3 Gambaran Penelitian	29
Gambar IV.1 Topologi <i>nonsegmented</i> yang akan digunakan	33
Gambar IV.2 Topologi <i>microsegmented</i> yang akan digunakan	34
Gambar IV.3 <i>Host</i> yang terlibat pada skenario 1	36
Gambar IV.4 Semua perangkat yang terlibat dalam skenario 1 topologi <i>non-microsegmented</i>	37
Gambar IV.5 Semua perangkat yang terlibat dalam skenario 1 topologi <i>microsegmented</i>	38
Gambar IV.6 <i>Host</i> yang terlibat pada skenario 2	39
Gambar IV.7 Perangkat yang terlibat pada skenario 2 topologi <i>non-microsegmented</i>	40
Gambar IV.8 Perangkat yang terlibat pada skenario 2 topologi <i>microsegmented</i>	40
Gambar IV.9 Konfigurasi <i>interface</i> Gi0/0	42
Gambar IV.10 Konfigurasi <i>interface</i> Gi0/1	42
Gambar IV.11 Konfigurasi <i>access list</i>	43
Gambar IV.12 Implementasi <i>access group/access list</i>	43
Gambar IV.13 Konfigurasi <i>rate-limit</i>	43
Gambar IV.14 Konfigurasi <i>interface</i> Gi0/0	44
Gambar IV.15 Menyimpan konfigurasi yang telah dilakukan	44
Gambar IV.16 <i>Dashboard</i> FortiGate	45
Gambar IV.17 Menu <i>Interfaces</i>	45
Gambar IV.18 Konfigurasi <i>interface</i> WAN	46
Gambar IV.19 Konfigurasi <i>interface</i> DMZ	47
Gambar IV.20 Konfigurasi <i>Switch</i> 2 dan 3	48
Gambar IV.21 Membuat <i>zone</i> baru	48
Gambar IV.22 Membuat <i>Internal Zone</i>	49

Gambar IV.23 Membuat <i>firewall policy</i>	49
Gambar IV.24 Konfigurasi <i>policy</i> WAN ke DMZ	50
Gambar IV.25 Konfigurasi <i>policy Internal Zone</i> ke DMZ	51
Gambar IV.26 Konfigurasi <i>policy</i> DMZ ke WAN	52
Gambar IV.27 Konfigurasi <i>policy</i> DMZ ke <i>Internal Zone</i>	53
Gambar IV.28 Konfigurasi <i>ICMP Flood Blocking</i> WAN	54
Gambar IV.29 Konfigurasi <i>ICMP Flood Blocking Internal Zone</i>	55
Gambar V.1 Hasil <i>ping</i> Attacker-PC1 ke PC-1	58
Gambar V.2 <i>Resource utilization server idle</i>	60
Gambar V.3 <i>Resource utilization server</i> dengan <i>traffic</i>	61
Gambar V.4 <i>CPU history firewall</i>	62
Gambar V.5 <i>Memory history firewall</i>	62
Gambar V.6 <i>Resource utilization</i> NGFW	63
Gambar V.7. <i>Flowchart</i> skenario 1 topologi <i>non-microsegmented</i>	64
Gambar V.8 Hasil penyerangan dari Attacker-PC01	65
Gambar V.9 Hasil penyerangan dari Attacker-PC02.....	65
Gambar V.10 <i>Broadcast message</i> untuk paket yang <i>di-drop</i>	65
Gambar V.11 Status <i>rate-limit</i> untuk <i>firewall</i>	66
Gambar V.12 <i>Chart conformed/exceeded</i>	66
Gambar V.13 <i>CPU usage firewall</i>	67
Gambar V.14 <i>CPU hog warning</i>	67
Gambar V.15 <i>Memory usage firewall</i>	68
Gambar V.16 <i>Resource utilization WebServer</i>	68
Gambar V.17 <i>Flowchart</i> skenario 1 <i>microsegmented</i>	69
Gambar V.18 Deteksi FortiGate untuk <i>ICMP flood</i>	70
Gambar V.19 <i>Detail log ICMP flood</i>	70
Gambar V.20 <i>Detail log</i> tambahan	71
Gambar V.21 <i>Resource utilization</i> FortiGate.....	72
Gambar V.22 <i>Resource utilization</i> WebServer	72
Gambar V.23 <i>Flowchart</i> skenario 2 <i>non-microsegmented</i>	73
Gambar V.24 Hasil penyerangan dari PC2	74
Gambar V.25 Hasil penyerangan dari PC3	74

Gambar V.26 <i>Rate-limit</i> skenario 2	74
Gambar V.27 <i>Resource utilization</i> WebServer	75
Gambar V.28 <i>CPU utilization firewall</i> skenario 2	76
Gambar V.29 <i>Memory utilization firewall</i> skenario 2	76
Gambar V.30 <i>Flowchart</i> skenario 2 <i>microsegmented</i>	77
Gambar V.31 <i>Detail log</i> skenario 2	78
Gambar V.32 <i>Resource utilization</i> WebServer skenario 2	79
Gambar V.33 <i>Resource utilization</i> FortiGate skenario 2	79
Gambar V.34 Pengujian <i>one-way delay non-microsegmented</i> normal	81
Gambar V.35 Pengujian <i>one-way delay non-microsegmented</i> skenario 1	82
Gambar V.36 Pengujian <i>one-way delay non-microsegmented</i> skenario 2	82
Gambar V.37 Pengujian <i>one-way delay microsegmented</i> normal	83
Gambar V.38 Pengujian <i>one-way delay microsegmented</i> skenario 1	84
Gambar V.39 Pengujian <i>one-way delay microsegmented</i> skenario 2	84
Gambar V.40 Hasil pengujian <i>ipdv non-microsegmented</i> normal	85
Gambar V.41 Hasil pengujian <i>ipdv non-microsegmented</i> skenario 1	86
Gambar V.42 Hasil pengujian <i>ipdv non-microsegmented</i> skenario 2	86
Gambar V.43 Hasil pengujian <i>ipdv microsegmented</i> normal	87
Gambar V.44 Hasil pengujian <i>ipdv microsegmented</i> skenario 1	87
Gambar V.45 Hasil pengujian <i>ipdv microsegmented</i> skenario 2	88
Gambar V.46 Hasil pengujian <i>packet loss non-microsegmented</i> normal	89
Gambar V.47 Hasil pengujian <i>packet loss non-microsegmented</i> skenario 1	90
Gambar V.48 Hasil pengujian <i>packet loss non-microsegmented</i> skenario 2	90
Gambar V.49 Hasil pengujian <i>packet loss microsegmented</i> normal.....	91
Gambar V.50 Hasil pengujian <i>packet loss microsegmented</i> skenario 1	91
Gambar V.51 Hasil pengujian <i>packet loss microsegmented</i> skenario 2	92
Gambar V.52 Hasil pengujian <i>capacity non-microsegmented</i> normal	93
Gambar V.53 Hasil pengujian <i>capacity non-microsegmented</i> skenario 1	93
Gambar V.54 Hasil pengujian <i>capacity non-microsegmented</i> skenario 2	94
Gambar V.55 Hasil pengujian <i>capacity microsegmented</i> normal.....	94
Gambar V.56 Hasil pengujian <i>capacity microsegmented</i> skenario 1	95
Gambar V.57 Hasil pengujian <i>capacity microsegmented</i> skenario 2	95

Gambar V.58 Perbandingan <i>one-way delay</i>	99
Gambar V.59 Perbandingan <i>ipdv</i>	100
Gambar V.60 Perbandingan <i>packet loss</i>	101
Gambar V.61 Perbandingan <i>capacity</i>	101
Gambar V.62 Perbandingan <i>firewall CPU utilization</i>	102
Gambar V.63 Perbandingan <i>firewall memory utilization</i>	103
Gambar V.64 Perbandingan <i>server CPU utilization</i>	103
Gambar V.65 Perbandingan <i>server memory utilization</i>	104