









## Tests de Scan IPS & DoS – FortiGate

Ce tableau résume 5 tests de scan réalistes (Nmap & Masscan) pour démontrer les capacités de détection de FortiGate IPS et DoS Policy.

 Test	 Commande	 Objectif	 Détail technique	 IPS	 DoS
Test 1	sudo nmap -sS -T1 -p587,993 172.16.1.253	Simuler un scan furtif lent	Scan SYN discret, faible volume, évite DoS	✓ Log intrusion si signature activée	✗ Trop lent pour seuil
Test 2	sudo nmap -A -T4 -p587,993 172.16.1.253	Identifier OS et services	Empreinte OS, bannière SMTP, SSL cert	✓ os.fingerprint, vuln-type 14	✗ Volume trop faible
Test 3	sudo nmap -sS -T5 -p1-1000 172.16.1.253	Scan massif rapide (Nmap)	1000 ports, vitesse agressive	✗ Peut surcharger IPS	✓ tcp_port_scan, blocage rapide
Test 4	sudo masscan 172.16.1.1 -p1-1024 --rate=20000	Botnet/flood simulation	SYN ultra rapide, contournement IPS	✗ Trop rapide pour être inspecté	✓ Déclenche DoS immédiatement
Test 5	sudo nmap -sn 172.16.1.0/24	Cartographie réseau	ICMP sweep / Ping scan	✗ IPS ne couvre pas ICMP	✓ icmp_sweep (seuil conseillé : 1)