




# Tests de Scan IPS & DoS – Explication

Ce tableau décrit en détail les options de chaque commande Nmap/Masscan utilisée pour tester FortiGate IPS et DoS Policy.

 Commande	 Explication des options	 Objectif et comportement attendu
<code>sudo nmap -sS -T1 -p587,993 172.16.1.253</code>	<ul style="list-style-type: none"> <li>- `sudo` : nécessaire pour les sockets RAW</li> <li>- `nmap` : outil de scan</li> <li>- `-sS` : SYN scan (stealth)</li> <li>- `-T1` : timing très lent (furtif)</li> <li>- `-p587,993` : ports SMTP Submission et IMAPS</li> <li>- `172.16.1.253` : IP cible</li> </ul>	Scan furtif, faible volume, contourne la DoS Policy, déclenche IPS si signature `tcp.syn.scan` active
<code>sudo nmap -A -T4 -p587,993 172.16.1.253</code>	<ul style="list-style-type: none"> <li>- `-A` : active OS detection (`-O`), version (`-sV`), scripts NSE, traceroute</li> <li>- `-T4` : timing rapide modéré</li> <li>- `-p587,993` : ports mail</li> <li>- `172.16.1.253` : IP cible</li> </ul>	Fingerprint complet : bannière SMTP, cert SSL, OS guess. Déclenche IPS si vuln-type `14` (info disclosure) actif
<code>sudo nmap -sS -T5 -p1-1000 172.16.1.253</code>	<ul style="list-style-type: none"> <li>- `-sS` : SYN scan</li> <li>- `-T5` : timing agressif</li> <li>- `-p1-1000` : scan des 1000 premiers ports</li> <li>- `172.16.1.253` : IP cible</li> </ul>	Scan rapide de masse, risque de saturation. Pas toujours inspecté par IPS, déclenche `tcp_port_scan` dans DoS
<code>sudo masscan 172.16.1.253 -p1-1024 --rate=20000</code>	<ul style="list-style-type: none"> <li>- `masscan` : outil très rapide (scanner bas-niveau)</li> <li>- `-p1-1024` : 1024 ports</li> <li>- `--rate=20000` : 20 000 paquets/s</li> </ul>	Scan extrêmement rapide, contourne IPS, déclenche automatiquement la DoS Policy avec seuil bas
<code>sudo nmap -sn 172.16.1.0/24</code>	<ul style="list-style-type: none"> <li>- `-sn` : ping scan (pas de port scan)</li> <li>- `172.16.1.0/24` : balayage de 256 adresses</li> </ul>	Découverte réseau ICMP. Ne passe pas par IPS mais détecté comme `icmp_sweep` via la DoS Policy